DOC 54 **3126/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

11 juni 2018

WETSONTWERP

betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

11 juin 2018

PROJET DE LOI

relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

INHOUD

SOMMAIRE

DE SPOEDBEHANDELING WORDT DOOR DE REGERING GEVRAAGD OVEREENKOMSTIG ARTIKEL 51 VAN HET REGLEMENT.

LE GOUVERNEMENT DEMANDE L'URGENCE CONFORMÉMENT À L'ARTICLE 51 DU RÈGLEMENT.

De regering heeft dit wetsontwerp op 11 juni 2018 ingediend.	*Le gouvernement a déposé ce projet de loi le 11 juin 2018.*
De "goedkeuring tot drukken" werd op 11 juni 2018 door de Kamer ontvangen.	*Le "bon à tirer" a été reçu à la Chambre le 11 juin 2018.*

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
DéFI	:	*Démocrate Fédéraliste Indépendant*
PP	:	*Parti Populaire*
Vuye&Wouters	:	*Vuye&Wouters*

Afkortingen bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*	*DOC 54 0000/000:*	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Schriftelijke Vragen en Antwoorden*	*QRVA:*	*Questions et Réponses écrites*
CRIV:	*Voorlopige versie van het Integraal Verslag*	*CRIV:*	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Beknopt Verslag*	*CRABV:*	*Compte Rendu Analytique*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*	*CRIV:*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Plenum*	*PLEN:*	*Séance plénière*
COM:	*Commissievergadering*	*COM:*	*Réunion de commission*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT:*	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

SAMENVATTING

Dit ontwerp van wet beoogt drie doelstellingen:

1) de omzetting van Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (hierna "Richtlijn");

2) de tenuitvoerlegging, voor de open clausules, van Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "AVG" of "Verordening");

3) het voorzien in afwijkende regelingen voor de overheden en verwerkingen buiten het toepassingsgebied van de EU (bijvoorbeeld de inlichtingen- en veiligheidsdiensten).

RÉSUMÉ

Ce projet de loi a trois objectifs:

1) Transposer la directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après "Directive");

2) Mettre en œuvre, pour les clauses ouvertes, le Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après "RGPD" ou "Règlement");

3) Prévoir des régimes dérogatoires pour les autorités et les traitements hors champ d'application de l'UE (par exemple les services de renseignement et de sécurité).

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

Algemeen kader

De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht.

In een meer algemeen kader werd het Verdrag van de Raad van Europa tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108 – hierna "Verdrag 108") op 28 januari 1981 voor ondertekening opengesteld. Het gaat om het eerste internationale juridisch bindende instrument op het gebied van de gegevensbescherming. Het Aanvullende Protocol bij het Verdrag (ETS nr. 181 van 8 november 2001) eist van de Staten die partij zijn bij het verdrag dat zij voorzien in toezichthoudende autoriteiten die volledig onafhankelijk optreden en heeft betrekking op het grensoverschrijdend verkeer van gegevens naar derde landen. Dat Verdrag 108 is dan ook van toepassing voor wat buiten het toepassingsgebied van de Europese Unie (hierna "EU") blijft zoals de verwerkingen door de inlichtingen- en veiligheidsdiensten als onderdeel van hun wettelijke opdrachten maar ook de militaire operaties van defensie. België heeft als partij bij het Verdrag 108 de verbintenis op zich genomen om in zijn intern recht de noodzakelijke maatregelen te nemen om uitvoering te geven aan de in het verdrag vervatte grondbeginselen.

Krachtens artikel 8, paragraaf 1, van het Handvest van de grondrechten van de Europese Unie en artikel 16, paragraaf 1, van het Verdrag betreffende de werking van de Europese Unie (hierna "VWEU") heeft eenieder recht op bescherming van zijn persoonsgegevens.

Artikel 16, paragraaf 2 van VWEU voorziet "Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. *Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten.".*

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

EXPOSÉ GÉNÉRAL

Cadre général

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental.

Dans un cadre plus général, la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108 – ci-après "la Convention 108") a été ouverte à la signature le 28 janvier 1981. Il s'agit du premier instrument international juridiquement contraignant dans le domaine de la protection des données. Le Protocole additionnel à la Convention (STE n° 181 du 08/11/2001) exige des États Parties à la Convention qu'ils mettent en place des autorités de contrôle, agissant de manière totalement indépendante, et porte sur les flux transfrontières de données vers des pays tiers. Cette Convention 108 est donc applicable pour ce qui reste hors champ d'application de l'Union Européenne (ci-après "UE") comme par exemple les traitements effectués par les services de renseignements et de sécurité dans le cadre de leurs missions légales mais aussi les opérations militaires de la Défense. En tant que partie à la Convention 108, la Belgique a pris l'engagement de prendre les mesures nécessaires au sein du droit interne afin de donner exécution aux principes fondamentaux repris dans la convention.

L'article 8, paragraphe premier, de la Charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe premier, du traité sur le fonctionnement de l'Union européenne (ci-après "TFUE") disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

L'article 16, paragraphe 2, du TFUE stipule que "*Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.".*

Het tweede lid voorziet onder meer het volgende: *"De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften.".*

Artikel 39 van de Verdrag betreffende de Europese Unie (hierna "VEU") voorziet: "Overeenkomstig artikel 16 van het Verdrag betreffende de werking van de Europese Unie en in afwijking van lid 2 daarvan stelt de Raad een besluit vast inzake de voorschriften betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van dit hoofdstuk vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. *Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten.".*

Tot op heden is nog geen uitvoering gegeven aan het artikel 39 VEU. Het nationale recht is daarvoor van toepassing.

Het recht op bescherming van persoonsgegevens heeft geen absolute gelding maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen.

Door snelle technologische ontwikkelingen en globalisering zijn nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. De mate waarin persoonsgegevens worden verzameld en gedeeld, is significant gestegen. Dankzij de technologie kunnen bedrijven en overheden bij het uitvoeren van hun activiteiten meer dan ooit tevoren gebruik maken van persoonsgegevens.

De Verordening is na meer dan vier jaar onderhandelen tot stand gekomen met het oog op de regeling van de stroom en van de verwerking van persoonsgegevens in de Europese Unie die een samenhangend nauwkeurig kader biedt dat gemeenschappelijk is voor alle verwerkingsverantwoordelijken en verwerkers op het grondgebied van de Europese Unie.

De Richtlijn is een regeling die afwijkt van de Verordening voor wat betreft hoofdzakelijk de politie- en justitiediensten en voorziet dan ook in specifieke regels voor die diensten die ten uitvoer moeten worden gelegd door de lidstaten van de Europese Unie bij het omzetten van de Richtlijn.

De hervorming van het Europees wetgevend kader inzake gegevensbescherming vervangt dus de oude

L'alinéa 2 prévoit en outre ce qui suit: *"Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne.".*

L'article 39 du traité sur l'Union européenne (ci-après "TUE") prévoit: "*Conformément à l'article 16 du traité sur le fonctionnement de l'Union européenne et par dérogation à son paragraphe 2, le Conseil adopte une décision fixant les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du présent chapitre, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.*".

A ce jour, l'article 39 TUE n'a toujours pas été exécuté. Le droit national doit alors s'appliquer.

Le droit à la protection des données à caractère personnel n'est pas un droit absolu; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité.

L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités.

Après plus de 4 ans de négociation, le Règlement a vu le jour afin de règlementer le flux et le traitement des données à caractère personnel dans l'Union européenne qui offre un cadre précis cohérent et commun à tous les responsables de traitement et sous-traitant sur le territoire de l'Union européenne.

La Directive est un régime dérogatoire au Règlement principalement pour les services de police et de justice et prévoit dès lors des règles spécifiques pour ces services qui doivent être mises en œuvre par les États membres de l'Union européenne à travers la transposition de la Directive.

La réforme du cadre législatif européen concernant la protection des données remplace donc l'ancienne

Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (hierna "kaderbesluit").

De beginselen inzake gegevensbescherming die in richtlijn 95/46 werden bekrachtigd, gelden nog steeds, maar de evolutie op technologisch vlak (internet web 2.0, cloud computing) en economisch vlak (oprichting van de grote digitale markt van de Europese Unie, internationalisering van de gegevensuitwisseling) vraagt om een herziening van die basisbeginselen. Er was nood aan een algemene harmonisatie van de regels ter zake.

Wat politie en justitie betreft, worden de beginselen van het kaderbesluit uitgebreid tot alle operationele gegevensverwerkingen door de betrokken diensten, terwijl het kaderbesluit enkel de overdrachten tussen bevoegde diensten via de politionele en justitiële samenwerking in strafzaken binnen de EU betrof.

Er moet niet alleen worden nagedacht over de omzetting van de Richtlijn, maar ook over de tenuitvoerlegging van de Verordening, aangezien beide instrumenten van toepassing zijn naargelang het om het ene of het andere toepassingsgebied gaat (doeleinden – bevoegde diensten). De moeilijkheid waarmee de wetgever wordt geconfronteerd bestaat erin dat de Richtlijn en de Verordening op veel punten op elkaar lijken maar op andere punten niet met elkaar overeenstemmen. Er moet dan ook worden voorzien in verschillende regels tenzij de Verordening voorziet in een uitzondering of beoordelingsmarge voor de publieke sector.

Die denkoefeningen die hebben geleid tot het huidige wetsontwerp moeten echter samengaan met de denkoefeningen die plaatsvinden over de oprichting van de Gegevensbeschermingsautoriteit (vroeger de Commissie voor de bescherming van de persoonlijke levenssfeer of kortweg Privacycommissie). Er werd rekening gehouden met verschillende praktijken die voortvloeien uit het ingetrokken wetgevingspakket door de Verordening en door de nationale wetten die de Verordening tenuitvoerleggen. Er werd eveneens rekening gehouden met de nieuwe bepalingen aangebracht door de Verordening en de nationale wetten die de Verordening tenuitvoerleggen, zoals bijvoorbeeld de uitbreiding van de bevoegdheden van de onafhankelijke toezichthoudende autoriteit (hierna "DPA") en het toezicht dat nodig is door onafhankelijke organen,

directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ainsi que la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (ci-après "décision-cadre").

Les principes de protection des données consacrés dans la directive 95/46 sont toujours valables mais l'évolution sur le plan technologique (internet web 2.0, Cloud computing) et économique (création du grand marché digital de l'union européenne, internationalisation de l'échange de données) exige que ces principes de base soient réévalués. Une harmonisation générale des règles en la matière était nécessaire.

En ce qui concerne la police et la justice, les principes de la décision-cadre sont étendus à tous les traitements de données opérationnelles effectués par les services concernés alors que la décision-cadre ne concernait que les transferts entre services compétents via la coopération policière et judiciaire en matière pénale au sein de l'UE.

La réflexion doit être menée non pas sur la transposition de la directive uniquement mais également sur la mise en œuvre du règlement car les deux instruments s'appliquent selon que l'on se trouve dans l'un ou l'autre champ d'application (finalités – services compétents). La difficulté à laquelle le législateur est confronté est que la Directive et le Règlement se ressemblent sur beaucoup de points mais divergent sur d'autres. Il y a donc lieu de prévoir des règles différentes sauf lorsque le règlement prévoit une exception ou une marge d'appréciation pour le secteur public.

Les réflexions qui ont abouties au présent projet de loi ont été menées en parallèle avec les réflexions qui ont lieu autour de la création de l'Autorité de protection des données (anciennement la Commission de la protection de la vie privée ou en abrégé la Commission vie privée). Il a été tenu compte de diverses pratiques découlant du corpus législatif abrogé par le Règlement et par les lois nationales qui le mettent en œuvre. Il a également été tenu compte des dispositions nouvelles apportées par le Règlement et les lois nationales qui le mettent en œuvre, comme par exemple l'augmentation des pouvoirs de l'autorité de contrôle indépendante (ci-après "DPA") et le nécessaire contrôle par des organes indépendants, les procédures de recours, la mise en place des délégués à la protection des données (ci-après "DPO"), la suppression de la déclaration des traitements remplacée

de beroepsprocedures, de invoering van functionarissen voor gegevensbescherming (hierna "DPO"), de afschaffing van de aangifte van de verwerkingen, die wordt vervangen door het bijhouden van registers, de invoering van effectbeoordelingen (hierna "DPIA"), de kennisgevingen inzake inbreuken op de beveiliging, de beveiligingsmaatregelen waarin voor alle verwerkingen moet worden voorzien, ...

De vraag van het toepassingsgebied van het ene en het andere wetgevend instrument is op het eerste gezicht niet evident als we het opschrift van de Richtlijn mogen geloven. De elementen van het toepassingsgebied, te weten de samenvoeging van een materieel element en van een persoonlijk element, moeten evenwel nader worden bekeken. Daarbij komt nog het beginsel van de restrictieve interpretatie van de uitzondering die de Richtlijn is ten aanzien van de algemene Verordening, alsmede de geschiedenis van die hervorming, te weten dat de Richtlijn het kaderbesluit van 2008 vervangt, zoals *supra* gezien.

Gelet op al die elementen en de veelvuldige besprekingen die ter zake werden gevoerd in de Raad van de Europese Unie kan de Richtlijn enkel worden gericht tot de diensten die uitsluitend en voornamelijk bevoegdheden inzake onderzoek en opsporing van strafbare feiten hebben, te weten traditioneel de politiediensten en de rechterlijke orde die zeer specifieke opdrachten hebben.

Er doet een veralgemeende overtuiging de ronde dat de algemene Verordening te strikt zou zijn voor die betrokken diensten. De Verordening voorziet evenwel zowel voor de inspectiediensten als voor enige andere overheidsdienst in beoordelingsruimte die de mogelijkheid biedt de verschillen tussen de Richtlijn en de Verordening te doen vervlakken, maar ook een zekere soepelheid te behouden voor de publieke sector.

Als voorbeelden van die beoordelingsruimte op het niveau van de publieke sector kunnen worden vermeld:

— geen rechtstreekse toepasbaarheid van de Verordening voor de verwerkingen van de publieke sector maar handhaving van de bestaande wetten (art. 6.2);

— de mogelijkheid om de toepassing van de Verordening aan te passen voor de verwerkingen van de publieke sector via nationale wetten (artt. 6.2 en 6.3);

— de mogelijkheid om verenigbare verdere verwerkingen te doen indien de wet daarin voorziet (art. 6.4);

— de uitzondering op het verbod om gevoelige gegevens te verwerken om redenen van algemeen belang bepaald in een wet (art. 9.2.g);

par la tenue de registres, la mise en place d'analyses d'impact (ci-après "DPIA"), les notifications des brèches de sécurité, les mesures de sécurité à prévoir pour tous les traitements, ….

La question du champ d'application de l'un et de l'autre instrument législatif n'est pas, au premier abord, évidente si l'on en croit le titre de la Directive. Pourtant, il y a lieu de regarder de plus près aux éléments du champ d'application, à savoir la réunion d'un élément matériel et d'un élément personnel. S'ajoute à cela le principe d'interprétation restrictive de l'exception qu'est la Directive par rapport au Règlement général, ainsi que l'historique de cette réforme rappelée ci-avant, à savoir que la Directive remplace la décision-cadre de 2008.

Au vu de tous ces éléments, et des discussions qui ont été abondantes sur le sujet au sein du Conseil de l'Union européenne, la directive ne peut être adressée qu'aux services ayant exclusivement et principalement des compétences de recherche, détection d'infraction pénales, à savoir classiquement les services de police et l'ordre judiciaire qui ont des missions très spécifiques.

Une croyance généralisée circule en ce que le Règlement général serait trop strict pour ces services concernés. Or, que ce soit pour les services d'inspection ou pour tout autre service public, le Règlement prévoit une marge de d'appréciation qui permet d'estomper les différences entre la Directive et le Règlement, mais également de maintenir une certaine souplesse pour le secteur public.

A titre d'exemples de ce marge d'appréciation au niveau du secteur public citons:

— pas d'applicabilité directe du Règlement pour les traitements du secteur public mais maintien des lois existantes (art. 6.2);

— possibilité d'adapter l'application du Règlement pour les traitements du secteur public via des lois nationales (art.6.2 et 6.3);

— la possibilité de faire des traitements ultérieurs compatibles si la loi le prévoit (art. 6.4);

— l'exception à l'interdiction de traiter des données sensibles pour des raisons d'intérêt public déterminé dans une loi (art. 9.2 .g);

— de uitzondering op het recht op vergetelheid (art. 17.3.b) en c));

— de uitzondering op het recht op overdraagbaarheid (art. 20.3);

— uitzondering op het recht op bezwaar (art. 21.1);

— de uitzondering op het verbod van profilering zonder menselijke tussenkomst (art. 22.2.b));

— de uitzonderingen op de rechten op informatie, inzage en rectificatie (art. 23);

— de uitzondering op de verplichting om de betrokkene in kennis te stellen van een inbreuk op de beveiliging (art. 23.1);

— een functionaris voor gegevensbescherming is verplicht voor de publieke sector behalve voor hoven en rechtbanken bij de uitoefening van hun rechterlijke taken (art. 37.1);

— de mogelijkheid van doorgiften aan derde landen op grond van een bilaterale overeenkomst (art. 46.2) of op grond van een in een wet erkend gewichtig algemeen belang (art.49.1.d);

— de uitzondering op de one-stop-shop (art. 55.2);

— de verwijzing naar het nationaal recht voor het opleggen van een geldboete voor de publieke sector (art. 83.7);

— de mogelijkheid om het nationaal identificatienummer te gebruiken (art. 87).

Die wetgevende instrumenten zijn evenwel beperkt tot de bevoegdheid van de Europese Unie, waardoor de vraagstukken met betrekking tot de bescherming van fundamentele rechten en vrijheden of het vrije verkeer van persoonsgegevens in verband met niet onder het EU-recht vallende activiteiten worden uitgesloten, zoals activiteiten met betrekking tot de nationale veiligheid. De Verordening is ook niet van toepassing op de verwerking van persoonsgegevens door de lidstaten van de Europese Unie binnen de context van hun activiteiten met betrekking tot het buitenlands- en veiligheidsbeleid van de Unie.

Artikel 52, paragraaf 1, van het Handvest van de Grondrechten van de Europese Unie bepaalt dat beperkingen op de uitoefening van het recht op gegevensbescherming kunnen opgelegd worden, voor zover zij voorzien worden bij wet, de wezenlijke inhoud van die rechten en vrijheden eerbiedigen, en dat, met

— l'exception au droit à l'oubli (art. 17.3.b) et c));

— l'exception au droit à la portabilité (art. 20.3);

— l'exception au droit d'objecter (art. 21.1);

— l'exception à l'interdiction de profilage sans intervention humaine (art. 22.2.b));

— les exceptions aux droits d'information, d'accès et de rectification (art. 23);

— l'exception à l'obligation de notifier une brèche de sécurité à la personne concernée (art. 23.1);

— un délégué à la protection des données est obligatoire pour le secteur public sauf pour les cours et tribunaux agissant dans l'exercice de leur fonction juridictionnelle (art. 37.1);

— la possibilité de transferts vers des pays tiers sur base de convention bilatérale (art. 46.2) ou sur base d'un intérêt public important reconnu dans une loi (art.49.1.d);

— l'exception au one-stop-shop (art. 55.2);

— le renvoi au droit national pour l'imposition d'amende pour le secteur public (art. 83.7);

— la possibilité d'utiliser le numéro d'identification national (art. 87).

Toutefois ces instruments législatifs se limitent à la compétence de l'Union européenne, en excluant les questions de protection des libertés et droits fondamentaux ou de libre flux des données à caractère personnel concernant des activités qui ne relèvent pas du champ d'application du droit de l'Union, telles que les activités relatives à la sécurité nationale. Le Règlement ne s'applique non plus au traitement des données à caractère personnel par les États membres de l'Union européenne dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union.

Conformément à l'article 52, paragraphe premier, de la Charte des droits fondamentaux de l'UE, des limitations peuvent être imposées à l'exercice du droit à la protection des données, dans la mesure où elles sont prévues par la loi, respectent le contenu essentiel des droits et libertés et, dans le respect du principe

inachtneming van het evenredigheidsbeginsel slechts beperkingen kunnen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

De activiteiten betreffende de nationale gemeenschappelijke veiligheid en de aanwending en paraatstelling met het oog op de aanwending van de krijgsmacht vallen onder het toepassingsgebied van Titel V, Hoofdstuk 2 van het VEU. Het gemeenschappelijk veiligheids- en defensiebeleid (hierna "GBVB") zorgt ervoor dat de EU beschikt over een operationeel vermogen dat op civiele en militaire middelen steunt. De EU kan deze middelen gebruiken voor de missies buiten het grondgebied van de Unie, zulks met het oog op handhaving van de vrede, conflictpreventie en versterking van de internationale veiligheid overeenkomstig de beginselen van het Handvest van de Verenigde Naties. Die missies bevatten de gemeenschappelijke acties inzake ontwapening, humanitaire en reddingsoperaties, adviserende en bijstandsverlenende militaire missies, missies voor conflictpreventie en vredeshandhaving, opdrachten van strijdkrachten op het gebied van crisisbeheersing, met inbegrip van het tot stand brengen van vrede en postconflict stabiliseringsoperaties. Al die missies kunnen bijdragen tot de strijd tegen terrorisme, ook door de steun geboden aan derde landen om terrorisme te bestrijden op hun grondgebied (Artt. 42-43 VEU).

In een meer algemeen kader is het Verdrag 108 van toepassing voor wat buiten het toepassingsgebied van de EU blijft zoals de verwerkingen verricht door de inlichtingen- en veiligheidsdiensten en de krijgsmacht.

Artikel 9 van het Verdrag 108 bepaalt dat kan afgeweken worden van de bepalingen inzake de hoedanigheid van de gegevens (art. 5), de bijzondere categorieën van gegevens (art. 6) en de bijkomende waarborgen voor de betrokkene (art. 8) indien de nationale wet in een dergelijke afwijking voorziet en het een maatregel betreft die in een democratische samenleving noodzakelijk is ten behoeve van:

a) "de bescherming van de veiligheid van de Staat, de openbare veiligheid, de geldelijke belangen van de Staat of de bestrijding van strafbare feiten";

b) "de bescherming van de betrokkene en van de rechten en vrijheden van anderen.".

De regels inzake gegevensbescherming zullen voortaan terug te vinden zijn in verschillende nationale wetgevingen:

de proportionnalité, sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui.

Les activités relatives à la sécurité nationale commune et la mise en œuvre et la mise en condition en vue de la mise en œuvre des forces armées tombent dans le champ d'application du titre V, chapitre 2 du TUE. La politique de sécurité et de défense commune (ci-après "PESC") assure à l'UE une capacité opérationnelle s'appuyant sur des moyens civils et militaires. L'UE peut y avoir recours dans des missions en dehors de son territoire afin d'assurer le maintien de la paix, la prévention des conflits et le renforcement de la sécurité internationale conformément aux principes de la charte des Nations unies. Ces missions incluent les actions conjointes en matière de désarmement, les missions humanitaires et d'évacuation, les missions de conseil et d'assistance en matière militaire, les missions de prévention des conflits et de maintien de la paix, les missions de forces de combat pour la gestion des crises, y compris les missions de rétablissement de la paix et les opérations de stabilisation à la fin des conflits. Toutes ces missions peuvent contribuer à la lutte contre le terrorisme, y compris par le soutien apporté à des pays tiers pour combattre le terrorisme sur leur territoire (Art. 42-43 TUE).

Dans un cadre plus général, la Convention 108 est applicable pour ce qui reste hors champ d'application de l'UE comme par exemple les traitements effectués par les services de renseignements et de sécurité et les forces armées.

L'article 9 de la Convention 108 détermine qu'il est possible de déroger aux dispositions en matière de qualité des données (art. 5), les catégories particulières de données (art.6) et les garanties complémentaires pour la personne concernée (art. 8) lorsqu'une telle dérogation est prévue par la loi nationale et qu'elle constitue une mesure nécessaire dans une société démocratique aux fins de:

a) "la protection de la sécurité de l'État, de la sûreté publique, des intérêts monétaires de l'État ou de répression des infractions pénales";

b) "la protection de la personne concernée et des droits et libertés d'autrui.".

Les règles relatives à la protection des données se retrouveront désormais dans différentes législations nationales:

— de Algemene Verordening 2016/679, die rechtstreeks van toepassing is in de Belgische wetgeving;

— het wetsontwerp;

— de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit,

— de verschillende sectorale wetten op dit gebied.

Toezichthoudende autoriteiten

De Verordening en de Richtlijn laten de lidstaten toe meerdere DPA's aan te duiden (Cf artikel 51.1 van de Verordening en artikel 41.1 van de Richtlijn).

De Privacycommisie, huidige toezichthoudende autoriteit, werd grondig hervormd om te beantwoorden aan de vereisten van de Verordening en de Richtlijn. Deze hervorming werd uitgevoerd door de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (GBA).

Huidig wetsontwerp ontwikkelt ook nieuwe bevoegdheden voor bepaalde bestaande organen teneinde rekening te houden met verschillende bijzonderheden.

De bevoegdheidsverdeling tussen de vier DPA's zal er als volgt uit zien:

Het C.O.C. wordt DPA voor:

— de politiediensten;

— de Algemene Inspectie van de federale en lokale politie;

— de Passagiersinformatie-eenheid, en dit voor verwerkingen van deze vier diensten die vallen onder titel 2 en/of onder Afdeling 2 van Hoofdstuk IV van titel 1 van het Ontwerp. Voor verwerkingen die onder de Verordening vallen en die uitgevoerd worden door de Passagiersinformatie-eenheid, is dus niet het C.O.C. maar de GBA bevoegd.

Comité I wordt DPA voor:

— de inlichtingen -en veiligheidsdiensten, voor zover het verwerkingen betreft die onder ondertitel 1 van titel 3 van het ontwerp vallen;

— verwerkingen van persoonsgegevens in het kader van veiligheidsmachtigingen, attesten en adviezen

— le Règlement général 2016/679, lequel est directement applicable en droit belge;

— le présent projet de loi;

— la loi du 3 décembre 2017 créant l'Autorité de protection des données,

— les différentes lois sectorielles en la matière.

Autorités de contrôle

Le Règlement et la directive permettent aux États membres de désigner plusieurs DPA (article 51.1 du Règlement et article 41.1 de la Directive).

La Commission vie privée, actuelle autorité de contrôle, a été transformée en profondeur pour répondre aux exigences du Règlement et de la Directive. Cette réforme a été mise en œuvre par la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (APD).

Le présent projet de loi établit également de nouvelles compétences de contrôles à certains organes existants afin de tenir compte des spécificités différentes.

La répartition des compétences entre les quatre DPA sera établie comme suit:

L'Organe de contrôle de l'information policière (le C.O.C.) devient la DPA pour:

— les services de police;

— l'Inspection générale de la police fédérale et locale;

— l'Unité d'information des passagers, et ce pour les traitements de ces quatre services qui relèvent du titre 2 et/ou de la Section 2 du Chapitre IV du titre 1er du projet. Pour les traitements qui relèvent du Règlement et qui sont réalisés par l'Unité d'information des passagers, ce n'est donc pas le C.O.C. mais l'APD qui est compétente.

Le Comité R devient la DPA pour:

— les services de renseignement et de sécurité, pour autant qu'il s'agisse de traitements relevant du sous-titre 1er dutitre 3 du projet;

— Les traitements de données à caractère personnel dans le cadre d'habilitations, d'attestations et d'avis de

(bedoeld in de wet van 11 december 1998) door vijf instanties/personen die in artikel 107 van het ontwerp worden opgesomd;

— de Passagiersinformatie-eenheid, voor zover het verwerkingen betreft die onder ondertitel 5 van titel 3 van het ontwerp vallen.

Comité P wordt samen met het Comité I DPA voor het OCAD, voor zover het verwerkingen van het OCAD betreft die onder ondertitel 4 van titel 3 van het ontwerp vallen.

De GBA is DPA voor alle andere gegevensverwerkingen die niet onder de bevoegdheid van C.O.C. of Comité I of Comité P vallen. *De facto* krijgt de GBA dus een residuaire bevoegdheid.

Als gevolg van deze verdeling zijn sommige organen onderworpen aan meerdere toezichthoudenden autoriteiten. Het Comité I en het Comité P worden bijvoorbeeld gezamenlijk bevoegd verklaard als zijnde DPA van het OCAD en dit enkel voor de verwerkingen van het OCAD die onder ondertitel 4 van titel 3 van het ontwerp vallen. Voor andere verwerkingen (bv. verwerkingen in het kader van het personeelsbeleid) van het OCAD is de GBA bevoegd. Ook voor de Passagiersinformatie-eenheid zijn er potentieel drie DPA's bevoegd. Het is daarom dat de term "bevoegde toezichthoudende autoriteit" gebruikt wordt.

Ter herinnering, de toezichtsrol van Comité P en Comité I staat los staat van de Verordening en van de Richtlijn zodat het Verdrag 108 aldus de enige norm betreft. Anderzijds, beschikken beide Comités vandaag reeds over heel wat bevoegdheden die in lijn liggen met die van een DPA, bijv. onderzoeksbevoegdheden, bevoegdheid om advies te verlenen op ontwerpen van regelgeving. In het ontwerp worden daar een aantal typische DPA-taken aan toegevoegd, zoals de behandeling van verzoeken tot onrechtstreekse toegang en van andere "*verzoeken"*. Ook wordt expertise inzake dataprotectie een vereiste om aangesteld te kunnen worden als lid van de Comités P & I.

Gezien de vermenigvuldiging van de toezichthoudende autoriteiten, worden deze uitgenodigd om nauw samen te werken wanneer dossiers overlappen. het sluiten van overeenkomsten tussen de verschillende gegevensbeschermingsautoriteiten en het "één loket principe" worden naar voren gebracht.

sécurité (viés dans la loi du 11 décembre 1998) par cinq instances/personnes énoncées à l'article 107 du projet;

— l'Unité d'information des passagers, pour autant qu'il s'agisse de traitements relevant du sous-titre 5 du titer 3 du projet.

Le Comité P devient, avec le Comité R, la DPA pour l'OCAM, pour autant qu'il s'agisse de traitements de l'OCAM relevant du sous-titre 4 du titre 3 du projet.

L'APD est la DPA pour tous les autres traitements de données qui ne relèvent pas de la compétence du C.O.C. ou du Comité R ou du Comité P. L'APD reçoit donc *de facto*, une compétence résiduaire.

Cette répartition a pour conséquence que certains organes soient soumis à plusieurs autorités de contrôle. Le Comité R et le Comité P sont en effet déclarés conjointement compétents pour être la DPA de l'OCAM et ce uniquement pour les traitements de l'OCAM relevant du sous-titre 4 du titre 3 du projet. Pour d'autres traitements (par exemple les traitements dans le cadre de la politique du personnel) de l'OCAM, c'est l'APD qui est compétente. Pour l'Unité d'information des passagers aussi, on compte potentiellement trois DPA. C'est la raison pour laquelle, il est utilisé les termes "autorité de contrôle compétente".

Pour rappel, le rôle de contrôle des Comités P et R est indépendant du Règlement et de la Directive, la Convention 108 ne constituant que la seule norme. Toutefois, ces deux Comités disposent déjà de compétences correspondant à celles d'une DPA, par exemple des compétences d'enquête, une compétence d'émettre des avis sur des projets de réglementation. Le projet y ajoute plusieurs tâches typiques d'une DPA, comme le traitement de demandes d'accès indirect et d'autres "requêtes". L'expertise en matière de protection des données devient également une exigence pour pouvoir être désigné en tant que membre des Comités P&R.

Vu la multiplication des autorités de contrôle, ces dernières sont invitées à collaborer lorsque des dossiers se chevauchent. La conclusion d'accords entre les différentes DPA et le principe de Guichet unique sont mis en avant.

ARTIKELSGEWIJZE TOELICHTING

VOORAFGAANDE TITEL

Artikel 1

Artikel 1 verduidelijkt de grondwettelijke grondslag inzake de bevoegdheid en behoeft geen bijzondere commentaar.

Art. 2

Dit artikel biedt de mogelijkheid de bepalingen van deze wet op algemene wijze te doen toepassen op enige verwerking, geheel of gedeeltelijk geautomatiseerd, alsmede op een niet-geautomatiseerde verwerking.

Zoals de Verordening zelf aangeeft dient bij de toepassing van de Verordening rekening te worden gehouden met de specifieke situatie van kleine, middelgrote en micro-ondernemingen. De Verordening verwijst daarvoor naar de definitie van het begrip kleine, middelgrote en micro- ondernemingen uit artikel 2 van de bijlage bij Aanbeveling 2003/361/EG van de Commissie. De Verordening voorziet immers in bepaalde verduidelijkingen voor organisaties met minder dan 250 werknemers. De regering meent dat ook bij de uitoefening van haar competenties, taken en bevoegdheden de Gegevensbeschermingsautoriteit rekening dient te houden met kleine, middelgrote en micro- ondernemingen. Het is bovendien niet uitgesloten dat de Europese Commissie bijzondere maatregelen zal treffen voor kleine, middelgrote en micro-ondernemingen zoals overweging 167 van de Verordening aangeeft. De regering zal aandachtig blijven voor deze ontwikkelingen.

Om te antwoorden op de opmerkingen van de Privacycommissie en de Raad van State wordt de uitsluiting van het toepassingsgebied van de Verordening voor wat betreft de titels 2 en 3 verwijderd vermits de Belgische wetgever inderdaad niet het toepassingsgebied van een Europese norm kan bepalen. Bovendien moet worden rekening gehouden met eventuele toekomstige rechtspraak van het Hof van Justitie van de Europese Unie die een impact kan hebben op het toepassingsgebied van de Verordening en de Richtlijn en dus ook op deze wet.

Anders dan wat de Raad van State voorstelt in zijn advies voeren de titels 4 tot 8 daarentegen niet alleen de Verordening uit. Het gaat daar ook soms om de omzetting van de Richtlijn of de implementatie van het Verdrag 108. Er kan dus geen bepaling in deze wet worden toegevoegd die de exclusieve uitvoering van

COMMENTAIRE DES ARTICLES

TITRE PRELIMINAIRE

Article 1er

L'article premier précise le fondement constitutionnel en matière de compétence et n'appelle pas de commentaire particulier.

Art. 2

Cet article permet de faire appliquer les dispositions de la loi de manière générale à tout traitement automatisé en tout ou en partie, ainsi qu'au traitement non automatisé.

Comme le Règlement l'indique lui-même, dans l'application du Règlement il y a lieu de tenir compte de la situation particulière des micro, petites et moyennes entreprises. A ces fins le Règlement réfère à la notion de micro, petites et moyennes entreprises reprise dans l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission. En effet, le Règlement prévoit certaines précisions pour les organisations occupant moins de 250 employés. Le gouvernement estime que dans l'exercice de ses compétences, missions et pouvoirs, l'Autorité de protection des données doit aussi tenir compte des micro, petites et moyennes entreprises. Il n'est d'ailleurs pas exclu que la Commission européenne envisagera des mesures spécifiques pour les micro, petites et moyennes entreprises comme l'indique le considérant 167 du Règlement. Le gouvernement restera attentif à ces développements.

Pour répondre aux remarques de la Commission vie privée et du Conseil d'État l'exclusion du champ d'application du Règlement en ce qui concerne les titres 2 et 3 a été supprimé puisqu'il est vrai que le législateur belge ne peut aucunement déterminer le champ d'application d'une norme européenne. En plus il faut tenir compte d'éventuelle jurisprudence future de la Cour de Justice de l'Union européenne qui peut avoir un impact sur le champ d'application du Règlement et de la Directive et donc aussi de la présente loi.

En revanche, contrairement à ce que le Conseil d'État suggère dans son avis, les titres 4 à 8 n'exécutent pas uniquement le Règlement. Il s'agit également de la transposition de la Directive ou de la mise en œuvre de la Convention 108. On ne peut donc pas rajouter une disposition dans la présente loi qui affirme l'exécution

de Verordening bevestigt, behalve voor wat betreft titel 1 zoals wordt aangegeven in artikel 6.

Hoewel de Verordening en de Richtlijn in een bepaald toepassingsgebied voorzien, moet in het kader van het nationaal recht in een ruimer toepassingsgebied worden voorzien omdat de Europese instrumenten bijvoorbeeld niet van toepassing zijn op het Gemeenschappelijk buitenlands en veiligheidsbeleid (hierna "GBVB"), dat in artikel 2 van de Verordening uit het toepassingsgebied ervan wordt uitgesloten. Men kan dus niet de Verordening enkel uitvoeren en zich ook beperken tot de omzetting van de Richtlijn. Andere domeinen moeten ook worden gedekt in ons nationaal recht. Om de regelgevingen niet te vermenigvuldigen, is dan ook beslist de bepalingen van de Verordening of sommige bepalingen van de Richtlijn te doen toepassen op enkele andere domeinen die niet worden gedekt door de Verordening teneinde ervoor te zorgen dat geen enkel domein buiten de regelgeving valt, wat rechtsonzekerheid zou creëren en een juridisch vacuüm ten opzichte van de situatie van vandaag alsook ten aanzien van onze verplichtingen krachtens het Verdrag 108.

Zo wordt er expliciet verwezen naar de toepassing van de Verordening ten aanzien van de bevoegdheden die opgenomen zijn in Hoofdstuk 2 van Titel V van het VEU om rechtszekerheid te bieden voor zover de Europese Unie nog geen eigen juridisch instrument heeft goedgekeurd. Er wordt dus verwezen naar de Verordening voor wat betreft de regels die van toepassing worden op deze domeinen. Het gaat dus niet zoals de Raad van State beweert om het uitbreiden van het toepassingsgebied van een bepaling van afgeleid Europees recht maar wel het voorzien van dezelfde regel voor de domeinen die anders zonder tussenkomst van de wetgever zonder regelgeving zouden vallen.

De wet voorziet daarom in de toepassing van de Verordening voor het GBVB-gebied, met uitzondering van de aanwending van de krijgsmacht, en de paraatstelling met het oog op de aanwending van de krijgsmacht zoals voorzien in ondertitel 2 van titel 3.

De Verordening is rechtstreeks toepasselijk en de bepalingen ervan moeten niet worden overgenomen in nationaal recht met uitzondering van bepaalde maatregelen die door de lidstaten moeten worden genomen aangezien de Verordening een zekere beoordelingsruimte laat. Het toepassingsgebied ervan sluit tevens de verwerkingen door de bevoegde overheden in de zin van de Richtlijn uit met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van

exclusive du Règlement, sauf pour le titre 1er tel qu'il est indiqué dans l'article 6.

Même si le Règlement et la directive prévoient un champ d'application déterminé, dans le cadre de la loi nationale, il y a lieu de prévoir un champ d'application plus large car les instruments européens ne s'appliquent pas à la Politique étrangère et de sécurité commune (ci-après "PESC") par exemple, exclu du champ d'application en son article 2 du Règlement. On ne peut donc pas uniquement exécuter le Règlement et se limiter également à la transposition de la Directive. D'autres domaines doivent également être couverts dans notre loi nationale. Afin de ne pas multiplier les règlementations, il est donc décidé de faire appliquer les dispositions du Règlement ou certaines dispositions de la Directive à certains domaines non couverts par le Règlement afin de ne pas laisser de domaine hors réglementation, ce qui engendrerait de l'insécurité juridique et des vides juridiques face à la situation d'aujourd'hui ainsi qu'à nos obligations en vertu de la Convention 108.

Ainsi il est fait mention expresse de l'application du Règlement aux compétences reprises dans le Chapitre 2 du titre V du TUE pour assurer une sécurité juridique tant qu'aucun instrument juridique propre n'est adopté par l'Union européenne. Il est dès lors fait référence au Règlement pour les règles applicables dans ces domaines. Il ne s'agit pas comme le prétend le Conseil d'État d'étendre le champ d'application d'un dispositif de droit européen dérivé, mais de prévoir la même règle pour des domaines qui sans intervention du législateur seraient dépourvus de toute règlementation.

La loi prévoit donc l'application du Règlement pour le domaine PESC à l'exception de la mise en œuvre des forces armées et de la mise en condition des forces armées en vue de leur mise en œuvre comme prévu dans le sous-titre 2 du titre 3.

Le Règlement est directement applicable et ses dispositions ne doivent pas être reprises dans une loi nationale à l'exception de certaines mesures qui doivent être prises par les États membres car le Règlement laisse une certaine marge d'appréciation. Son champ d'application exclut également les traitements effectués par les autorités compétentes au sens de la Directive aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la

gevaren voor de openbare veiligheid, alsmede wat niet tot de bevoegdheden van de Europese Unie behoort.

Bijvoorbeeld, de bepaling in artikel 3, § 2, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna "WVP"), waarin wordt gesteld: "*Deze wet is niet van toepassing op de verwerking van persoonsgegevens die door een natuurlijk persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht*", moet niet meer worden overgenomen in het nationale recht aangezien dit reeds wordt beoogd in artikel 2.2 van de Verordening.

De uitzondering bedoeld in artikel 3, § 3, WVP inzake de vrijheid van meningsuiting en de journalistiek wordt dan weer overgenomen in hoofdstuk V van titel 1 vermits de Verordening dit vereist.

De uitzondering bedoeld in artikel 3, § 4, WVP wordt geschrapt en vervangen door titel 3 inzake de verwerkingen door de inlichtingen- en veiligheidsdiensten.

De uitzondering bedoeld in artikel 3, § 5, WVP wordt geschrapt en vervangen door titel 2 inzake de verwerkingen door onder meer de politiediensten en de rechterlijke orde.

Artikel 3, § 5, 4°, WVP voorziet in een uitzondering voor de verwerkingen op grond van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme. Deze bepaling werd opgeheven door de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten welke zelf voorziet in een bijzonder regime inzake gegevensbescherming.

Artikel 3, § 5, 3°, WVP voorziet in de mogelijkheid van een breed uitzonderingsregime voor gegevensverwerking voor openbare overheden in de uitoefening van hun opdrachten van bestuurlijke politie. Daar werd bijvoorbeeld gebruik van gemaakt door het koninklijk besluit van 11 maart 2015 waarin de sociale inspecteurs en de ambtenaren van de openbare overheden die zijn vrijgesteld van bepaalde verplichtingen, worden aangewezen. Deze bepaling wordt voortaan gedekt door de uitzonderingen die mogelijk zijn op grond van artikel 23 van de Verordening maar die desalniettemin moeten worden voorzien door specifieke wetgeving zoals bedoeld in artikel 23.2 van de Verordening.

Artikel 3, § 6, WVP betreft de uitzondering voor Child Focus en voorziet in beperkingen inzake recht maar ook andere bijzondere maatregelen. De verwijzing naar

prévention de telles menaces, ainsi que ce qui n'entre pas dans les compétences de l'Union européenne.

Par exemple, la disposition de l'article 3, § 2, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après "LVP") qui prévoit que "*La présente loi ne s'applique pas au traitement de données à caractère personnel effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques*" ne doit plus être reprise dans la loi nationale, car elle est déjà visée par l'article 2.2 du Règlement.

En revanche, l'exception prévue à l'article 3, § 3, LVP sur la liberté d'expression et le journalisme est reprise dans le chapitre 5 du titre 1er puisque le Règlement l'exige.

L'exception prévue à l'article 3, § 4, LVP est supprimée et remplacée par le titre 3 sur les traitements par les services de renseignement et de sécurité..

L'exception prévue à l'article 3, § 5, LVP est supprimée et remplacée par le titre 2 sur les traitements par, entre autres, les services de police et l'ordre judiciaire.

L'article 3, § 5, 4°, LVP prévoit une exception pour les traitements faits en vertu de la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme. Cette disposition a été abrogée par la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces qui elle-même prévoit un régime particulier concernant la protection des données.

L'art. 3, § 5, 3°, LVP prévoit dans la possibilité d'un régime d'exceptions large pour les traitements de données par des autorités publiques pour des fins de police administrative. Ceci a été utilisé par exemple avec l'arrêté royal du 11 mars 2015 qui désigne les inspecteurs sociaux et les fonctionnaires des autorités publiques exemptées de certaines obligations. Cette disposition sera dorénavant couverte par les dérogations qui sont possibles en vertu de l'article 23 du Règlement mais qui doivent néanmoins être prévues par une législation spécifique tel que le prévoit l'article 23.2 du Règlement.

Article 3, § 6, LVP concerne l'exception pour Child Focus et prévoit des limitations en matière de droit mais également d'autres mesures particulières

Child focus wordt ingevoerd in titel 1 en meer bepaald in het hoofdstuk over de beginselen.

Artikel 3, § 7, WVP voorziet in een uitzondering op artikel 10 WVP voor de FOD Financië onderzoeksdienst. Zoals voor alle andere wetgevingen zijn de algemene uitzonderingen niet langer adequaat volgens de Verordening en de Richtlijn, dus de specifieke bepalingen inzake beperkingen van de rechten dienen in bijzondere wetgeving te worden ingevoegd.

Art. 3

Er dient herhaald te worden dat het eerste artikel, derde punt van de Verordening stelt dat "*Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.*". Dit betekent dat een verwerkingsverantwoordelijke een gegevensstroom niet kan blokkeren onder het voorwendsel van het garanderen van de bescherming van persoonsgegevens. Hij zal alleen dezelfde gegevensbeschermingsregels kunnen toepassen die het toepast voor zijn eigen gegevensverwerking. Een overheidsdienst mag vooral dus nooit tekort komen aan het volbrengen van zijn opdrachten om een reden gelinkt aan de gegevensbescherming. Elke overheidsdienst moet dus zijn opdrachten volbrengen met respect voor het wettelijk kader inzake de gegevensbescherming. Het is van essentieel belang dat de nodige gegevensstromen en proportioneel aan het volbrengen van zijn openbare opdrachten gebeuren in naleving van de Verordening en deze wet.

Het is niet de bedoeling van de wetgever om af te wijken van de geldende regels inzake gegevensbescherming, zoals de Privacycommissie beweert in zijn advies 33/2018. Integendeel, het gaat erom de uitwisseling en de bescherming van gegevens met behulp van efficiënte middelen te willen aanmoedigen. Maar de bescherming van persoonsgegevens kan geenszins een schild zijn om gegevensuitwisselingen te verhinderen en om af te wijken van andere principes van transparantie, veiligheid en effectiviteit. Deze bepaling bestaat overigens in het ontwerp tot modernisering van het Verdrag 108. De verwijzingen naar artikel 23 van de Verordening hebben niet anders tot doel dan te verwijzen naar een serie van doeleinden zonder deze evenwel in dit artikel op te lijsten, maar heeft niet tot doel om hier in afwijkingen te voorzien.

Voor wat betreft de herhaling van artikel 1.3. van de Verordening, het klopt zoals de Privacycommissie onderlijnt dat er geen overname van de bepalingen van de Verordening mag plaatsvinden. Echter, het betreft

La référence à Child Focus est introduite dans le titre 1er et notamment le chapitre sur les principes.

l'article 3, § 7, LVP prévoit une exception à l'article 10 LVP pour le SPF Finance service d'enquête. Comme pour toutes les autres législations, les exceptions générales ne sont plus adéquates selon le Règlement et la Directive, il y a donc lieu d'insérer les dispositions spécifiques de limitations des droits dans la légisation particulière.

Art. 3

Il convient de rappeler l'article premier troisième point du Règlement qui dispose que "*la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*". Cela signifie qu'un responsable de traitement ne peut faire obstacle à un flux de données sous prétexte de garantir la protection des données à caractère personnel. Il ne pourra appliquer que les mêmes règles de protection des données qu'il applique pour ses propres traitements de données. Il ne peut donc jamais être question notamment pour un service public de ne pas exercer ses missions pour des raisons liées à la protection des données. Il s'agira cependant pour chaque autorité publique de remplir ses missions en respectant le cadre législatif relatif à la protection des données. Il est crucial que les flux de données nécessaires et proportionnel à l'exécution des missions public aient lieu, dans le respect du Règlement et de la présente loi.

Il n'est pas dans l'intention du législateur de déroger aux règles en vigueur en matière de protection des données, comme le prétend la Commission vie privée dans son avis 33/2018. Au contraire, il s'agit d'encourager l'échange de données et la protection de ces données par des moyens efficaces. Mais la protection des données à caractère personnel ne peut être un bouclier à brandir à tout vents pour éviter les échanges de données et déroger à d'autres principes de transparence, de sécurité et d'effectivité. Cette disposition existe d'ailleurs dans le projet de modernisation de la Convention 108. Les références à l'article 23 du Règlement n'ont pour objectif que de faire référence à une série de finalités sans devoir la lister dans le présent article, mais n'a pas comme but de prévoir ici des dérogations.

S'agissant d'une redite de l'article 1er.3 du Règlement, il est vrai comme le soulève la Commissie vie privée qu'il n'y a pas lieu de copier les dispositions du Règlement. Toutefois, il s'agit ici d'appliquer le principe de la

hier het van toepassing maken van het principe van de uitwisseling van gegevens op de wet in zijn geheel en niet enkel voor de verwerkingen die onderworpen zijn aan de Verordening.

Art. 4

Het gaat om een bepaling waarin het territoriale toepassingsgebied wordt bepaald, waarin wordt opgenomen hetzij de vestiging op het Belgische grondgebied hetzij van de verwerkingsverantwoordelijke of de verwerker hetzij de betrokkene wanneer de verwerkingsverantwoordelijke en de verwerker gevestigd zijn buiten de Europese Unie. Gelet op de uniforme regels in de Europese Unie zal in beginsel een zekere samenhang worden behouden. In de gevallen waarin beoordelingsruimte voor de lidstaten van de Europese Unie bestaat, zou een dergelijke territoriale regeling tot een wetsconflict kunnen leiden. Het criterium van de verblijfplaats/het gegeven dat de betrokkene zich op het Belgische grondgebied bevindt, moet evenwel tevens behouden blijven teneinde de betrokkene eventueel tegen minder bindende regels te beschermen. Hierbij kan worden gedacht aan de leeftijd van het kind of de toestemming om gevoelige gegevens te verwerken, terwijl dat in België niet mogelijk is.

In antwoord op het advies 33/2018 van de Privacycommissie wordt er eveneens voorzien in een bepaling die de situatie regelt van een verwerkingsverantwoordelijke gevestigd op het grondgebied van een lidstaat van de Europese Unie en die beroep doet op een Belgische verwerker. Inderdaad, indien geen enkele regel wordt voorzien is er een risico op regelgevingsconflicten aangezien de twee wetten gelijktijdig van toepassing zouden zijn.

Art. 5

Dit artikel verduidelijkt dat de definities die in de wet gebruikt worden zich in de Verordening bevinden en in voorkomend geval moet ernaar worden verwezen. Ook andere definities worden in het wetsontwerp gebruikt en worden verduidelijkt in de betrokken bepalingen. Om te antwoorden op de opmerkingen van de Raad van State en van de Privacycommissie, de bedoeling van deze bepaling is om te voorzien dat, daar waar er definities voorzien worden, deze van toepassing zijn. Standaard zijn de definities van de Verordening van toepassing. In titel 1 zijn er geen specifieke definities dus zijn deze van de Verordening van toepassing net zoals de bijkomende definitie die in de voorlopige titel wordt voorzien voor de notie overheid, zoals de Raad van State aangeeft.

circulation des données à l'ensemble de la loi et non pas uniquement pour les traitements soumis au Règlement.

Art. 4

Il s'agit d'une disposition déterminant le champ d'application territorial, lequel reprend l'établissement sur le territoire belge, soit du responsable du traitement ou du sous-traitant, soit de la personne concernée alors que le responsable du traitement et le sous-traitant sont établis hors Union européenne.. En principe, vu les règles uniformes dans l'Union européenne, il sera maintenu une certaine cohérence. Dans les cas où il existe une marge d'appréciation pour les États membres de l'Union européenne, un tel régime territorial pourrait aboutir à un conflit de loi. Mais il est nécessaire de maintenir également le critère de résidence/se trouvant sur le territoire belge de la personne concernée afin de la protéger éventuellement contre des règles moins contraignantes. On peut penser à l'âge de l'enfant ou l'autorisation de traiter des données sensibles, alors que cela n'est pas possible en Belgique.

En réponse à l'avis 33/2018 de la Commission vie privée il est également prévu une disposition réglant la situation d'un responsable du traitement établi sur le territoire d'un État membre de l'Union européenne qui fait appel à un sous-traitant belge. En effet, si aucune règle n'est prévue, il y a un risque de conflit de loi puisque les deux lois s'appliqueraient concommittament.

Art. 5

Cet article précise que les définitions des termes repris dans la loi se retrouvent dans le Règlement, et qu'il y a lieu de s'y référer le cas échéant. D'autres définitions sont utilisées également dans le projet de loi et sont précisées dans les dispositions concernées. Pour répondre aux remarques du Conseil d'État et de la Commission vie privée, l'objectif de cette disposition est de prévoir que là où des définitions sont prévues, celles-ci s'appliquent. A défaut, les définitions du Règlement s'appliquent. Dans le titre 1er, il n'y a pas de définitions spécifiques, celles du Règlement s'appliquent donc bien, ainsi que la définition supplémentaire prévue dans le titre préliminaire, sur la notion d'autorité publique, comme le préconise le Conseil d'État.

De definitie van overheid wordt verduidelijkt en wordt hernomen van de wet van 4 mei 2016 inzake het hergebruik van overheidsinformatie, weliswaar uitgebreid tot de deelstaten en lokale overheden zoals de Raad van State het voorstelt. Inderdaad, het beperken van de definitie tot de Federale Staat zou een lacune teweegbrengen in de wet bijvoorbeeld voor wat betreft de sanctiebepalingen. Deze optie werd dus verkozen boven die van de Privacycommissie.

La définition d'autorité publique est précisée et est reprise de la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public tout en étant élargie aux entités fédérées et autorités locales, comme le propose le Conseil d'État. En effet limiter la définition à l'État fédéral engendrerait une lacune de la loi pour les dispositions relatives aux sanctions par exemple. Cette option a été préférée à celle proposée par la Commission vie privée.

TITEL 1

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

Titel 1 moet beschouwd worden als het hoofdzakelijke Verordening gedeelte. Dit deel herneemt natuurlijk niet de artikelen van de Verordening omdat de Verordening rechstreeks van toepassing is. Enkel de bepalingen die een beoordelingsruimte laten aan de lidstaten worden ingevuld.

TITRE 1ER

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel

Le titre 1er doit être considéré comme la partie principale liée au Règlement. Cette partie ne reprend bien évidemment pas les articles du Règlement car le Règlement est directement applicable. Uniquement les dispositions laissant de la marge de manoeuvre aux États membres sont complétées.

HOOFDSTUK I

Algemene bepalingen

Art. 6

Zoals hierboven vermeld, is de Verordening de algemene regel en van toepassing, met deze titel 1, op alle zaken die niet onder de titels 2, 3 en 7 vallen. Bijvoorbeeld, de verwerkingen door de politie die onder de doeleinden van titel 2 vallen behoren tot titel 2 maar wanneer de doeleinden niet onder titel 2 vallen, zijn deze titel en de Verordening van toepassing. Dit zal het geval zijn bijvoorbeeld voor wat betreft de personeelsdiensten van de politie.

Naast de bepalingen van deze wet, kunnen in uitvoering van de Verordening nog een aantal bepalingen genomen worden in nationale sectorale wetten. Met "bijzondere bepalingen" wordt naar deze wetsbepalingen verwezen.

Deze titel is eveneens van toepassing voor wat niet voorzien is in de Verordening via de uitbreiding van het toepassingsgebied voorzien in artikel 2, alinea 2 van deze wet. In die zin betreft het strikt gezien niet de uitvoering van de Verordening maar de toepassing ervan *mutatis mutandis*.

Zoals de Raad van State aanhaalt is deze bepaling strikt gezien niet noodzakelijk maar deze vermelding

CHAPITRE IER

Dispositions générales

Art. 6

Comme indiqué ci-avant, le Règlement est la règle générale et s'applique, avec le présent titre 1er, à tout ce qui n'est pas visé dans les titres 2, 3 et 7. Par exemple, les traitements de police aux fins du titre 2 sont concernés par le titre 2, mais lorsque les finalités n'entrent pas dans le titre 2, c'est le présent titre, et le Règlement qui s'applique. Ce sera le cas, par exemple de tout ce qui est service du personnel des services de police.

En plus des dispositions de cette loi, conformément au Règlement, un certain nombre de dispositions peuvent également être adoptées dans les lois sectorielles nationales. Il est renvoyé à ces dispositions légales par "dispositions particulières".

Ce titre s'applique également pour ce qui n'est pas prévu dans le Règlement via l'extension du champ d'application prévu à l'article 2, alinéa 2 de la loi. Dans ce sens il ne s'agit pas strictement d'une exécution du Règlement mais d'une application *mutatis mutandis*.

Comme le souligne le Conseil d'État, cette disposition n'est pas strictement nécessaire mais par soucis de

wordt behouden om redenen van klaarheid. Er mag hieruit ook niet worden afgeleid dat de andere titels de Verordening niet zouden uitvoeren. De andere titels, meer bepaald de titels 4 tot 6 en 8 voeren eveneens de Verordening uit maar zijn veel ruimer aangezien ze ook de omzetting van de Richtlijn en de implementatie van het Verdrag 108 beogen.

HOOFDSTUK II

Beginselen

Art. 7

Kinderen hebben met betrekking tot hun persoonsgegevens recht op specifieke bescherming, aangezien zij zich minder bewust kunnen zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens. Die specifieke bescherming moet met name gelden voor het gebruik van persoonsgegevens van kinderen voor marketingdoeleinden of voor het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. In de context van preventieve of adviesdiensten die rechtstreeks aan een kind van 13 jaar of ouder worden aangeboden, is de toestemming van de persoon die het ouderlijke gezag heeft of van de wettelijke vertegenwoordiger, niet vereist.

Artikel 8 van de Verordening bepaalt dat de minimumleeftijd voor kinderen om toestemming te geven 16 jaar is, maar de Verordening biedt de lidstaten van de Europese Unie de mogelijkheid te kiezen voor een lagere leeftijd, tot 13 jaar. Het betreft een beleidskeuze die tot de federale overheid behoort aangezien de bescherming van de persoonlijke levenssfeer een federale bevoegdheid is. De gemeenschappen komen daarna aan zet. De gemeenschappen kunnen dus in regelgeving voorzien met inachtneming van de federale wet. De gemeenschappen zijn, in overeenstemming met de bijzondere wetten tot hervorming der instellingen, bevoegd voor de preventie en voorlichting van jongeren over dit onderwerp.

Anderzijds is het van essentieel belang dat de verwerkingsverantwoordelijke een duidelijke en passende informatie voor het jonge publiek verstrekt en hen op de hoogte brengt van alle rechten die de jongere heeft, evenals alle gevolgen van het gebruik van deze diensten van de informatiemaatschappij op zijn privéleven en zijn persoonsgegevens.

clarté cette mention est maintenue. Il ne faudrait pas non plus déduire que les autres titres n'exécutent pas le Règlement. En effet, les autres titres, notammentles titres 4 à 6 et 8 exécutent également le Règlement mais sont beaucoup plus large car ils visent aussi la transposition de la Directive et la mise en œuvre de la Convention 108.

CHAPITRE II

Principes

Art. 7

Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. Le consentement du titulaire de l'autorité parentale ou du représentant légal ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseils proposés directement à un enfant âgé de 13 ans ou plus.

L'article 8 du Règlement détermine que l'âge de l'enfant pour le consentement est de 16 ans minimum mais le Règlement permet aux États membres de l'Union européenne d'opter pour un âge inférieur, jusque 13 ans. Il s'agit d'un choix politique relevant de l'autorité fédérale car la protection de la vie privée est une compétence fédérale. Les communautés interviennent ensuite. Les communautés peuvent dès lors réglementer en respectant la loi fédérale. Les communautés sont, conformément aux lois spéciales de réformes institutionnelles, compétentes pour la prévention et l'information des jeunes à ce sujet.

D'autre part, il est primordial que le responsable du traitement mette en œuvre une information claire et adaptée au jeune public en les informant de tous les droits que le jeune détient ainsi que de toutes les conséquences que comporte l'utilisation de ce service de société de l'information sur sa vie privée et ses données à caractère personnel.

Het is ook de verantwoordelijkheid van de verwerkingsverantwoordelijke die een rechtstreeks aanbod van diensten van de informatiemaatschappij levert aan de kinderen om een systeem te implementeren dat toegang verleent tot een dienst van de informatiemaatschappij door kinderen onder de 13 jaar met toestemming van een van de ouders of een andere persoon die het ouderlijk gezag heeft over het kind. Bijvoorbeeld, een controle van de leeftijd van het kind kan vereist zijn via de identiteitskaart of de Kids-ID identiteitskaart voor kinderen jonger dan 12 jaar.

Het toepassingscriterium is derhalve belangrijk aangezien bij de toepassing van de wet ofwel de wet van de woonplaats van het kind ofwel de wet van de zetel van de onderneming zal moeten worden toegepast. De kans bestaat dat erg verschillende regels zouden moeten worden toegepast indien de minimumleeftijd niet dezelfde zou zijn in de verschillende gemeenschappen van België. Coherentie met het oog op een gemakkelijkere toepasbaarheid is des te meer wenselijk ten aanzien van de verwerkingsverantwoordelijken, maar ook ten aanzien de ontvangers, die moeten weten welke regel op hen zal worden toegepast.

In dat verband heeft de staatssecretaris de verschillende Gemeenschappen om hun standpunt gevraagd. De Vlaamse Gemeenschap heeft zijn voorkeur al uitgesproken voor de verlaging van de leeftijd van het kind tot 13 jaar door goedkeuring van een resolutie van het Vlaams parlement, die gebaseerd is op het advies van de kinderrechtencommissaris van 22 april 2016 (advies 2016-2016/09).

Evenzo heeft de minister van Jeugdzaken van de Federatie Wallonië-Brussel bij brief van 13 juli 2017, aangegeven dat hij het advies deelt van de *Délégué général de la Communauté française aux droits de l'enfant*, waarin de leeftijd waarop kinderen in staat moeten zijn om vrij toegang te krijgen tot sociale netwerken op 13 jaar wordt vastgelegd. Een te restrictieve houding zou een averechts effect kunnen hebben van het omzeilen van regulering en zou kunnen leiden tot de ontwikkeling van parallelle praktijken die potentieel gevaarlijk zijn voor jongeren.

Onder ouderlijke verantwoordelijkheid moet worden verstaan ouderlijk gezag als bedoeld in de artikelen 371 en volgende van het Burgerlijk wetboek en de voogdij als bedoeld in de artikelen 389 en volgende van het Burgerlijk wetboek.

Onder "diensten van de informatiemaatschappij" wordt verstaan de diensten gedefinieerd in Richtlijn 2000/31/EG van het Europees Parlement en van de Raad van 8 juni 2000 betreffende bepaalde juridische

C'est également à la charge du responsable du traitement qui fournit une offre directe de services de la société de l'information aux enfants, de mettre en œuvre un système qui permette l'accès à un service de société de l'information par des enfants de moins de 13 ans moyennant l'accord d'un des parents ou personne ayant l'autorité parentale sur l'enfant. Une vérification de l'âge de l'enfant pourrait par exemple être exigée via la carte d'identité ou la carte d'identité Kids-ID pour les enfants âgés de moins de 12 ans.

Le critère d'application est dès lors d'importance car lors de l'application de la loi, il y aura lieu d'appliquer soit la loi de résidence de l'enfant, soit la loi du siège de l'entreprise. On risquerait de devoir appliquer des règles bien différentes si l'âge minimum n'était pas identique dans les différentes communautés en Belgique. Une cohérence pour une applicabilité plus aisée est d'autant plus souhaitable à destination des responsables du traitement mais également pour les destinataires qui doivent connaître quelle est la règle qui leur sera appliquée.

A cet égard, le Secrétaire d'État a envoyé une demande aux différentes Communautés pour connaître leur avis. La Communauté flamande a elle-même afficher sa préférence pour fixer le seuil à l'âge de 13 ans, en adoptant une résolution du Parlement flamand, laquelle est basée sur l'avis du 22 avril 2016 du *Kinderrechtencommissaris* (avis 2016-2016/09).

De même le ministre de la jeunesse de la Fédération Wallonie-Bruxelles a, par courrier du 13 juillet 2017, indiqué qu'il partage l'avis du Délégué général de la Communauté française aux droits de l'enfant qui fixe également à 13 ans l'âge à partir duquel les enfants devraient pouvoir librement accéder aux réseaux sociaux. Une attitude trop restrictive risquerait d'avoir des effets pervers de détournement de la réglementation et pourrait entraîner le développement de pratiques parallèles potentiellement dangereuses pour les jeunes.

Par responsabilité parentale, on entend l'autorité parentale visée dans les articles 371 et suivants du Code civil, et la tutelle visée aux articles 389 et suivants du Code civil.

Par "Service de la société de l'information", on entend les services définis dans la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de

aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt. Overweging 18 van die Richtlijn verduidelijkt namelijk dat de diensten van de informatiemaatschappij "*betrekking hebben op diensten waarvoor de afnemers niet betalen omvatten*".

Overeenkomstig het advies van de Privacycommissie werd de vermelding van de uitvoering van artikel 8.1 van de Verordening toegevoegd.

Zoals de Raad van State onderlijnt, gelet op de territoriale aanknopingspunten van artikel 4 zal deze bepaling niet van toepassing zijn op verwerkingen van persoonsgegevens van kinderen door verwerkingsverantwoordelijken die in een andere lidstaat van de Europese Unie gevestigd zijn. Jammer genoeg creëert de beoordelingsruimte die aan de lidstaten wordt gelaten over de leeftijd van kinderen een discordantie betreffende de toepasselijke wet binnen de Europese Unie zelf.

Art. 8

Het betreft een uitvoering van artikel 9.2.g van de Verordening, dat de lidstaten van de Europese Unie de mogelijkheid biedt te bepalen welke noodzakelijke verwerkingen van zwaarwegend algemeen belang van bijzondere of gevoelige persoonsgegevens zijn.

Er wordt in dit wetsontwerp beslist drie van deze verwerkingen vast te leggen: de instellingen voor de verdediging van de rechten van de mens, Child Focus alsook de instellingen die instaan voor de hulpverlening aan seksueel delinquenten. Deze domeinen van zwaarwegend algemeen belang zijn in de WVP opgenomen.

In antwoord op de opmerkingen van de Raad van State en de Privacycommissie acht de wetgever artikel 8, paragraaf 1, 1°, noodzakelijk. Deze bepaling valt immers niet binnen de categorie voorzien in artikel 9.2.d van de Verordening aangezien het ruimere verwerkingen voor oog heeft dan dit laatste artikel. Het oorspronkelijke artikel 6, § 1, k), WVP betreft verwerkingen met het oog op het maatschappelijk doel terwijl artikel 9.2.d van de Verordening enkel verwerkingen betreft met betrekking tot de leden of voormalige leden van de instantie. Bovendien wordt voorzien in een delegatie aan de Koning om dergelijke verwerkingen toe te laten. Het betreft dus wel degelijk de bijkomende waarborgen die worden gevraagd door beide instellingen. Hetzelfde geldt voor wat voorzien is in artikel 8, paragraaf 1, 3°.

De opsomming in dit artikel is exhaustief, maar brengt in geen geval de redenen van zwaarwegend algemeen

la société de l'information, et notamment du commerce électronique, dans le marché intérieur. Notamment, le considérant 18 de cette directive précise que les services de la société de l'information "*s'étendent également à des services qui ne sont pas rémunérés par ceux qui les reçoivent*".

Conformément à l'avis de la Commission vie privée il a été ajouté la mention d'exécution de l'article 8.1 du Règlement.

Comme le souligne le Conseil d'État, compte tenu des critères de rattachement territoriaux de l'article 4, la disposition ne sera pas applicable aux traitements de données à caractère personnel d'enfants par des responsables du traitement établis dans d'autres États membres de l'Union européenne. Malheureusement la marge de manœuvre laissée aux États membres sur l'âge de l'enfant crée une discordance de la loi applicable au sein même de l'Union européenne.

Art. 8

Il s'agit d'une exécution de l'article 9.2.g du Règlement qui permet aux États membres de l'Union européenne de déterminer quels sont les traitements de données particulières ou sensibles nécessaires pour motifs d'intérêt public important.

Il est décidé dans ce projet de loi d'en déterminer trois: les institutions de défense des droits de l'homme, Child Focus ainsi que les établissements chargés de l'aide aux délinquants sexuels. Ces domaines d'intérêt public important sont repris de la LVP.

En réponse aux commentaires du Conseil d'État et de la Commission vie privée le législateur estime que l'article 8, paragraphe 1er, 1°, est nécessaire. En effet, cette disposition n'entre pas dans la catégorie prévue à l'article 9.2.d du Règlement car il vise des traitements plus large que ce qui est prévu par ce dernier article. A l'origine l'article 6, § 1er, k), la loi vie privée concerne les traitements à des fins de l'objet social tandis que l'article 9.2.d du Règlement concerne uniquement les traitements relatifs aux membres ou anciens membres de l'organisme. De plus, il est prévu une délégation au Roi pour autoriser de tels traitements. Il s'agit donc bien de garanties supplémentaires réclamées par ces deux instances. Il en va de même pour ce qui est prévu à l'article 8, paragraphe 1er, 3°.

L'énumération dans cet article est exhaustive mais ne préjudicie en rien les motifs d'intérêt public important

belang in het gevaar, die belangrijk zijn en vastgesteld door het Recht van de Europese Unie overeenkomstig artikel 9.2.g van de Verordening. Dit is bijvoorbeeld het geval bij Verordening (EU) 2015/847 van het Europees Parlement en van de Raad van 20n mei 2015 betreffende bij geldovermakingen te voegen informatie en tot intrekking van Verordening (EG) nr. 1781/2006. Andere verwerkingen kunnen door de wet worden beschouwd als redenen van zwaarwegend algemeen belang.

Deze lijst wijst geen recht op zichzelf toe. Het is noodzakelijk om aan de andere voorwaarden van artikel 9.2.g), zelf te voldoen, namelijk dat de verwerking van bijzondere of gevoelige persoonsgegevens in verhouding moet staan tot het nagestreefde doel, het wezen van het recht op gegevensbescherming moet geeerbiedigd zijn en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

Om aan de Raad van State en de Privacycommissie te antwoorden, het is niet de bedoeling van de wetgever om in een “kaderwet” te bepalen welke de categorieën van gegevens, de categorieën van betrokkenen noch de gepaste en bijzondere maatregelen zijn. Aangezien deze “bijzonder” dienen te zijn, zoals artikel 9 van de Verordening het voorschrijft, komt het aan de wetgever toe om al dan niet bijzondere bepalingen te voorzien. Hier wordt slechts een lijst weergegeven van redenen van zwaarwegend algemeen belang die reeds in de huidige WVP gelden. Er wordt in deze dus niets nieuw voorzien. Er is echter beslist dezelfde waarborgen te hernemen die worden voorzien in artikel 10 § 2 van deze wet met betrekking tot de verplichting een lijst bijte houden alsook de vertrouwelijkheidsplicht. Wat betreft Child Focus, als antwoord op de Privacycommissie, werd besloten de waarborgen opnieuw in te voegen die voorheen in de WVP waren voorzien (verbod een bestand bij te houden over verdachte personen en benoeming van een DPO).

Wordt eveneens voorzien dat de verwerking van gevoelige gegevens door verenigingen, stichtingen bedoeld in dit artikel beperkt is en dat de verwerking van genetische en biometrische gegevens verboden is, behalve bij bijzondere wettelijke bepaling.

De delegatie aan de Koning met betrekking tot de individuele machtiging voor wat betreft de instellingen die instaan voor de hulpverlening aan seksueel delinquenten wordt behouden als aanvullende waarborg, zoals bedoeld in artikel 9.2.g) van de Verordening. In tegenstelling tot het advies van de Raad van State bevat deze wet wel de waarborgen.

déterminés par le droit de l’union européenne conformément à l’article 9.2.g du Règlement. C’est le cas par exemple du règlement (UE) 2015/847 du parlement européen et du conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (ce) n° 1781/2006. D’autres traitements peuvent être considérés par la loi comme motifs d’intérêt public important.

Cette liste n’attribue pas un droit. Il y a lieu en effet de satisfaire aux autres conditions prévues par l’article 9.2.g) lui-même à savoir que le traitement des données particulières ou sensibles doit être proportionné à l’objectif poursuivi, respecter l’essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêtes de la personne concernée.

Pour répondre au Conseil d’État et à la Commission vie privée, il n’est pas de l’intention du législateur de déterminer dans une “loi-cadre” quelles sont les catégories de données, catégories de personnes concernées, destinataires, ni les mesures appropriées et spécifiques. Celles-ci devant être “spécifiques”, tel que le prévoit l’article 9 du Règlement, il reviendra au législateur de prévoir ou non les dispositions spécifiques. Il n’est ici repris qu’une liste des motifs d’intérêt public important, étant ceux existant dans la LVP actuelle. Il n’y a donc rien de nouveau en l’occurence. Toutefois, il est décidé de reprendre les mêmes garanties prévues à l’article 10, § 2, de la présente loi relatives à l’obligation de tenir une liste, ainsi que l’obligation de confidentialité. En ce qui concerne Child Focus, en réponse à la Commission vie privée, il a été décidé de réinsérer les garanties précédemment prévues dans la LVP (interdiction de tenir un fichier de personnes suspectes et désignation d’un DPO).

Il est également prévu que le traitement des données sensibles par les associations, fondations visées au présent article est limité et que le traitement des données génétiques et biométriques est interdit, sauf disposition légale particulière.

La délégation au Roi concernant l’autorisation individuelle en ce qui concerne les établissements chargés de l’aide aux délinquants sexuels a été maintenue comme garantie complémentaire prévue à l’article 9.2.g du Règlement. Contrairement à l’avis du Conseil d’État, ces garanties sont bien parties intégrantes du présent projet de loi.

Art. 9

Teneinde te antwoorden op de opmerkingen van de Privacycommissie worden de waarborgen met betrekking tot de verwerking van gevoelige gegevens hernomen die werden vastgelegd in het oude artikel 25 van het koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Art. 10

§ 1. Het betreft de uitvoering van artikel 10 van de Verordening en de overname van artikel 8 WVP. Dit is vooral het strafregister en de personen die er toegang toe hebben. Het strafregister wordt geregeld door het Wetboek van strafvordering. Punt b van artikel 8 WVP is reeds vervat in artikel 10 van de Verordening en moet hier niet worden overgenomen. Er wordt niet langer nader bepaald dat de aangewezen personen tot geheimhouding verplicht zijn, aangezien zij daartoe door andere regelgevingen verplicht worden. De lijst is niet cumulatief.

De Privacycommissie stelt voor om het punt 3 van het artikel uit te breiden teneinde het van toepassing te maken op personen bepaald door of krachtens een wet, decreet of ordonnantie aangenomen om redenen van zwaarwegend algemeen belang ter verwenzenlijking van opdrachten van algemeen belang toevertrouwd door of krachtens een wet, decreet of ordonnantie.

In het punt 4° wordt rekening gehouden met de opmerking van de Raad van State tot toevoeging van verwerkingen met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Gelet op de wijzigingen die werden aangebracht in titel 4 is een verwijzing naar deze titel in dit punt niet op zijn plaats.

De Privacycommissie is van mening dat het punt 5° (betreffende Child Focus) van het oud artikel 9 § 1 (voortaan artikel 10) kan worden geschrapt omdat deze verwerkingen van gerechtelijke gegevens reeds gedekt worden door artikel 383*bis*/1 Strafwetboek dat reeds in een machtiging voorziet. De regering volgt de Privacycommissie op dit punt.

§ 2. Het betreft hier de overname van de aanvullende voorwaarden van artikel 25 van het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking

Art. 9

Afin de répondre au commentaire de la Commission vie privée, sont reprises ici les conditions relative aux traitements des données sensibles fixées à l'ancien article 25 de l'Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Art. 10

§ 1er. Il s'agit de l'exécution de l'article 10 du Règlement et l'introduction de l'article 8 LVP. Il s'agit notamment du casier judiciaire et des personnes qui y ont accès. Le casier judiciaire est réglé par le Code d'instruction criminel. Le point b de l'article 8 LVP est déjà prévu à l'article 10 du Règlement et ne doit pas être repris ici. Il n'est plus spécifié que les personnes désignées sont tenus au secret car ils le sont par d'autres règlementations. La liste n'est pas cumulative.

La Commission vie privée propose d'élargir le point 3° de l'article afin de viser les personnes déterminées par ou en vertu d'une loi, d'un décret, ou d'une ordonnance adopté pour des motifs d'intérêt public important pour l'accomplissement de tâches d'intérêt général confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

Au point 4° il est tenu compte de la remarque du Conseil d'État qui vise de rajouter les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Vu les modifications qui ont été faites dans le titre 4 une référence à ce titre dans ce point n'est plus à sa place.

La Commission vie privée est d'avis que le point 5° (concernant Child Focus) de l'ancien article 9, § 1er, (maintenant article 10) peut être supprimé puisque ces traitements de données judiciaires sont déjà couvertes par l'article 383*bis*/1 du Code pénal qui prévoit déjà une habilitation. Le gouvernement suit l'avis de la Commission vie privée sur ce point.

§ 2. Il s'agit ici de reprise des conditions supplémentaires de l'article 25 de l'Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. L'ensemble de l'article

van persoonsgegevens. Het artikel wordt niet volledig overgenomen aangezien de Verordening reeds in een aantal bepalingen voorziet, zoals de artikelen 14 en 15.

HOOFDSTUK III

Beperkingen op de rechten van de betrokkene

Dit hoofdstuk in de Verordening versterkt de rechten waarin reeds was voorzien in richtlijn 95/46 en in de WVP:

— de uitbreiding van het recht op informatie tot de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, het bestaan van profilering en de oorsprong van de gegevens;

— het recht op beknopte, transparante en begrijpelijke informatie die ook voor kinderen gemakkelijk toegankelijk is, die dadelijk en gratis wordt verstrekt, eventueel op een website;

— het recht op toegang tot en rechtzetting en schrapping van onjuiste gegevens;

— het recht op beperking van de verwerking in bepaalde gevallen;

— het recht om bezwaar te maken;

— het behoud van het recht om niet zonder menselijke tussenkomst geprofileerd te worden.

De Verordening voert echter nieuwe rechten in:

— het recht op vergetelheid;

— het recht op gegevensoverdraagbaarheid;

— het recht ingelicht te worden over inbreuken op de beveiliging.

Art. 11 à 17

De Verordening is de regel en de Richtlijn de uitzondering. De toepassing van de Richtlijnmoet restrictief geïnterpreteerd worden en beperkt tot de overheden die beantwoorden aan de voorziene definitie in artikel 3 van de Richtlijn en in het bijzonder de twee criteria (materieel en persoonlijk element), dat is de verwerking van persoonsgegevens door bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging

n'est pas repris car certaines dispositions sont déjà prévues par le Règlement, tels que les articles 14 et 15.

CHAPITRE III

Limitation aux droits de la personne concernée

Ce chapitre dans le Règlement, renforce les droits déjà contenus dans la directive 95/46 et la LVP:

— l'extension du droit à l'information à la durée de conservation, l'existence de profilage, l'origine des données;

— le droit à une information concise, transparente, intelligible, aisément accessible même aux enfants, fournie sans délai et sans frais, éventuellement sur un site internet;

— le droit d'accès, de rectification, et de suppression des données erronées;

— le droit de limiter le traitement dans certains cas;

— le droit d'objecter;

— le maintien du droit de ne pas être profilé sans intervention humaine.

Le Règlement crée toutefois de nouveaux droits:

— le droit à l'oubli;

— le droit à la portabilité des données;

— le droit d'être informé des brèches de sécurité.

Art. 11 à 17

Le Règlement étant la règle principale et la Directive l'exception, l'application de la directive doit être interprétée restrictivement et limitée aux autorités qui répondent à la définition prévue à l'article 3 de la Directive et notamment aux deux critères (élément matériel et personnel), c'est à dire le traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou

van straffen, met inbegrip van de bescherming tegen dreigingen voor de openbare veiligheid en het voorkomen van zulke dreigingen.

Dit betekent dat de Richtlijn zich enkel richt tot bepaalde overheden en op limitatieve wijze (zie de bevoegde autoriteiten in titel 2).

Er zijn talrijke diensten binnen openbare administratie met bevoegdheden gelinkt aan het voorkomen en het opsporen van strafbare feiten, onderzoek en vervolging ervan of de uitvoering van strafrechtelijke sancties. Dit is inderdaad het geval voor de sociale inspectiediensten, de economische inspectie, de inspectiediensten binnen de Federale Overheidsdienst Financiën voor wat betreft de inkomstenbelastingen bijvoorbeeld, of binnen de Nationale Bank van België, de FSMA, de gemeenten, … die onderworpen zijn aan de Verordening.

Andere overheidsdiensten hebben bevoegdheden die niet onder die definitie vallen, die eveneens onderworpen zijn aan de Verordening, maar die echter nood hebben aan een bijzondere regeling in verband met de rechten en plichten voor hun wettelijke opdrachten tot een goed einde te leiden.

Er doet een algemene overtuiging de ronde de GDPR te strikt zou zijn voor de betrokken diensten. Of het nu voor de inspectiediensten of voor elke andere overheidsdienst is, de algemene verordening voorziet in een bewegingsruimte speelruimte om de verschillen weg te werken tussen de richtlijn en de Verordening, maar ook om een bepaalde soepelheid te behouden voor de openbare sector.

Sommige bepalingen voorzien in artikel 12 tot 22 en 34 van de Verordening voorzien reeds rechtstreeks toepasbare afwijkingen. Dit is bijvoorbeeld het geval voor artikel 12.2, 12.4, 17.3, 19, 20.3, 21.1, 34.3.

Andere artikelen voorzien eveneens dat afwijkingen aan de vooropgestelde rechten en plichten mogelijk indien de nodige garanties vooropgesteld worden in de wet. Dit is het geval voor artikel 14.5, 22.2 et 22.4.

De Verordening biedt de lidstaten van de Europese Unie een zekere beoordelingsruimte met het artikel 23 dat beperkingen tot artikelen 12 tot 22 en 34 toelaat met inachtneming van bepaalde voorwaarden, vooral in zijn paragraaf 2.

Deze bepalingen moeten met een zekere precisie aangenomen worden. Er wordt dus verwezen naar

d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Cela signifie que la Directive ne s'adresse qu'à certaines autorités et de manière limitative (voir les autorités compétentes au titre 2).

Or il existe de nombreux services au sein de l'administration publique qui ont des compétences liées à la prévention et la détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. C'est en effet le cas des services d'inspection sociale, l'inspection économique, les services d'inspection au sein du Service public fédéral Finances en ce qui concerne les impôts sur le revenu par exemple, ou au sein de la Banque nationale de Belgique, la FSMA, les communes, …. Lesquelles sont soumises au Règlement.

D'autres administrations publiques ont des compétences qui n'entrent pas dans cette définition, lesquelles sont alors également soumises au Règlement, mais qui ont néanmoins besoin d'un régime particulier relativement aux droits et obligations pour mener à bien leurs missions légales.

Une croyance généralisée circule en ce que le Règlement général serait trop strict pour ces services concernés. Or, que ce soit pour les services d'inspection ou pour tout autre service public, le Règlement général prévoit une série de marge de manœuvre qui permettent d'estomper les différences entre la directive et le Règlement, mais également de maintenir une certaine souplesse pour le secteur public.

Certaines des dispositions prévues aux articles 12 à 22 et 34 du Règlement prévoient déjà des dérogations applicables directement. C'est le cas par exemple des articles 12.2, 12.4, 17.3, 19, 20.3, 21.1, 34.3.

D'autres articles prévoient également que des dérogations sont possibles aux droits et obligations prévus si des garanties nécessaires sont prévues dans une loi. C'est le cas des articles 14.5, 22.2 et 22.4.

Le Règlement permet toutefois une certaine marge d'appréciation pour les États membres de l'Union européenne avec un article 23 qui permet des restrictions aux articles 12 à 22 et 34 dans le respect de certaines conditions, notamment déterminées dans son paragraphe 2.

Ces dispositions doivent être prises avec une certaine précision. Il est donc renvoyé au Règlement pour les

de Verordening voor de direct van toepassing zijnde bepalingen alsook naar de bijzondere wetten voor wat betreft de uitvoeringsmaatregelen.

Het is nooit de bedoeling geweest van de regering om artikel 23.2 van de Verordening "om te zetten" in deze wet zoals de Privacycommisie en de Raad van State lijken te suggereren in hun adviezen. Het doel was om een kader te voorzien van minimale waarborgen geïnspireerd door artikel 3 § 7 WVP maar het spreekt voor zich dat het aan de wetgever toekomt om de gepaste waarborgen te bepalen in elke toepasselijke sectorale wet. Teneinde elke verwarring te vermijden heeft de regering de betrokken artikelen uit het wetsontwerp geschrapt.

Er worden wel nog bepalingen voorzien voor "koppelingen" tussen de titels van deze wetsontwerp. Inderdaad, de transparantie-, informatie- of toegangsverplichtingen van de verwerkingsverantwoordelijke in het kader van titel 1 konden redelijkerwijs niet worden toegepast in bepaalde situaties, met name wanneer gegevens worden doorgegeven door de in de titels 2 en 3 van dit wetsontwerp bedoelde autoriteiten of wanneer deze gegevens aan deze autoriteiten worden doorgegeven. Er worden daarom uitzonderingen voorzien in overeenstemming met artikel 23 van de Verordening.

Art. 11

Dit artikel bepaalt de verplichtingen van de verwerkingsverantwoordelijke wanneer hij over persoonsgegevens beschikt die rechtstreeks of onrechtstreeks van een overheid bedoeld in titel 3, zoals inlichtingen- en veiligheidsdiensten, OCAD, NVO, PIE in het kader van de doeleinden in artikel 8, § 1, 4°, van de wet van 25 december 2016…. afkomstig zijn. Omwille van evidente redenen van veiligheid en discretie krijgt de verwerkingsverantwoordelijke, en zijn personeel, zijn DPO of zijn verwerker, een verbod opgelegd om de betrokkene ervan op de hoogte te brengen dat hij over hem betreffende gegevens beschikt, wanneer deze van een overheid bedoeld in titel 3 afkomstig zijn.

Er moet echter verduidelijkt worden dat overheden slechts beschouwd worden als behorende tot titel 3 wanneer zij verwerkingen uitvoeren in het kader van opdrachten en doeleinden die verduidelijkt worden in elke ondertitel van titel 3. Bijvoorbeeld, de politie behoort tot de overheden van titel 3 wanneer zij tussenkomt als nationale veiligheidsoverheid in toepassing van artikel 22*ter* van de wet van 11 december 1998, maar zij maakt deel uit van titel 2 in de uitoefening van haar opdrachten bepaald in de wet op het politieambt.

dispositions directement applicable ainsi qu'aux lois particulières pour les mesures d'exécution.

Il n'a jamais été l'intention du gouvernement de "transposer" dans la présente loi l'article 23.2 du Règlement comme le semble suggérer la Commission vie privée et le Conseil d'État dans leurs avis. L'objectif a été de prévoir un cadre minimal de garanties inspirées de l'article 3, § 7, LVP mais il est évident qu'il appartient au législateur de déterminer les garanties appropriées dans chaque loi sectorielle applicable. Afin d'éviter toute confusion le gouvernement a supprimé les articles concernés du projet de loi.

Il est toujours prévu des dispositions "liens" entre les titres du présent projet de loi. En effet, les obligations en matière de transparence, d'information ou d'accès à charge du responsable de traitement visé par le titre 1er, ne pourrait raisonnablement être appliqué dans certains situations, notamment lorsqu'il s'agit de données qui ont été transmises par des autorités visées par les titres 2 et 3 de ce projet de loi, ou lorsque ces données sont transmises à ces autorités. Il est donc prévu des dérogations conformément à l'article 23 du Règlement.

Art. 11

Cet article détermine les obligations du responsable du traitement lorsqu'il dispose de données à caractère personnel émanant directement ou indirectement d'une autorité visée au titre 3, à savoir services de renseignement et de sécurité, OCAM, ANS, UIP dans le cadre des finalités de l'article 8, § 1er, 4°, de la loi du 25 décembre 2016, …. Pour des raisons évidentes de sécurité et de discrétion, le responsable du traitement, ainsi que son personnel, son DPO, ou son sous-traitant, a l'interdiction d'informer la personne concernée qu'il dispose de données la concernant lorsque celles-ci émanent d'une autorité visée au titre 3.

Il convient de préciser que les autorités ne sont considérées comme relevant du titre 3 que lorsqu'elles effectuent des traitements dans le cadre des missions et finalités précisées dans chaque sous-titre du titre 3. Par exemple, la police relève des autorités du titre 3 lorsqu'elle intervient comme autorité nationale de sécurité déléguée en application de l'article 22*ter* de la loi du 11 décembre 1998 mais elle relève du titre 2 dans l'exercice de ses missions fixées dans la loi sur la fonction de police.

De Privacycommissie, in punt 118 van haar advies, verwelkomt deze aanpassing die een lacune invult die de doctrine reeds twintig jaar terug heeft aangestipt. Om te antwoorden op haar verzoek worden de verwijzingen naar de artikelen 14, 16 en 19 van de wet van 30 november 1998 toegevoegd. De Nederlandstalige versie van oud artikel 12 verwees verkeerdelijk naar artikel 3 eerder dan naar titel 3, hetgeen de Privacycommissie heeft opgemerkt in het punt 120 van haar advies. Deze fout werd recht gezet.

Om te antwoorden op punt 122 van het advies van de Privacycommissie werd het artikel herformuleerd om uitdrukkelijk te bepalen dat de artikelen 12 tot 22 en 34 niet van toepassing zijn, hetgeen automatisch betekent dat enerzijds de betrokkenen niet genieten van deze rechten en anderzijds de verwerkingsverantwoordelijken niet gehouden zijn aan deze verplichtingen.

Om te antwoorden op de punten 138 en 139 van het advies van de Privacycommissie wordt verduidelijkt dat, zelfs indien het huidig artikel gegevens betreft die afkomstig zijn van autoriteiten bedoeld in titel 3, de beperking van de verplichting de betrokkene te informerenvan toepassing is op verwerkingsverantwoordelijken bedoeld in titel 1 die in het bezit zijn van deze gegevens en het dus logisch is deze in titel 1 in te voegen. Er wordt aan herinnerd dat het toepassingsgebied van titel 3 beperkt is tot de autoriteiten die erin worden bedoeld. Dit artikel hernemen onder titel 3 zou voor gevolg hebben dat het niet meer van toepassing zou zijn op verwerkingsverantwoordelijken van titel 1.

Hierop zijn twee uitzonderingen voorzien:

— wanneer de verwerkingsverantwoordelijke wettelijk verplicht is om alle gegevens die hem ter beschikking zijn gesteld, door te geven in het kader van een rechtsgeschil, of

— wanneer hij voorafgaande toestemming heeft gekregen van de overheid bedoeld in titel 3 waarvan de gegevens afkomstig zijn.

Om te antwoorden op het advies van het openbaar ministerie, de eerste uitzondering laat de doorgifte toe in het kader van een gerechtelijke procedure met respect voor de procedures die werden vastgelegd in sectorale wetten, in dit geval volgens de regels bepaald, in het bijzonder, in het Gerechtelijk wetboek en het Wetboek van strafvordering.

Deze uitzondering op de verplichtingen van de verwerkingsverantwoordelijke bedoeld in artikelen 12 tot 22 en 34 van de Verordening en op de transparantieverplichting bedoeld in punt 1.a) van artikel 5 van de

Au point 118 de son avis, la Commission vie privée salue cette adaptation qui comble une lacune que la doctrine a identifiée il y a vingt ans déjà. Pour répondre à sa demande, la référence aux articles 14, 16 et 19 de la loi du 30 novembre 1998 a été ajoutée. La version néerlandaise de l'ancien article 12 faisait référence, par erreur, à l'article 3 plutôt qu'au titre 3, ce que la Commission vie privée a fait remarquer au point 120 de son avis. Cette erreur a été corrigée.

Pour répondre au point 122 de l'avis de la Commission vie privée, l'article a été reformulé pour disposer expressément que les articles 12 à 22 et 34 ne s'appliquent pas, ce qui implique automatiquement que, d'une part, les personnes concernées ne bénéficient pas des droits et, d'autre part, les responsables du traitement ne sont pas tenus aux obligations.

Pour répondre aux points 138 et 139 de l'avis de la Commission vie privée, il est précisé que, même si le présent article traite des données émanant des autorités visées au titre 3, la restriction à l'obligation d'informer la personne concernée s'applique aux responsables du traitement visés dans le titre 1er en possession desdites données, il est donc logique de l'insérer dans le titre 1er. Il est rappelé que le champ d'application du titre 3 est limité aux autorités qui y sont visées. Reprendre le présent article sous le titre 3 aurait pour conséquence qu'il ne s'appliquerait plus aux responsables du traitement du titre 1er.

Deux exceptions sont prévues:

— lorsque le responsable du traitement est légalement tenu de transmettre toutes les données à sa disposition dans le cadre d'une procédure contentieuse, ou

— lorsqu'il obtient l'autorisation préalable de l'autorité visée au titre 3 dont proviennent les données.

Pour répondre à l'avis du ministère public, la première exception permet la transmission des données dans le cadre d'une procédure contentieuse dans le respect des procédures fixées dans les lois sectorielles, dans ce cas-ci selon les règles fixées notamment dans le Code judiciaire et le Code d'instruction criminelle.

Cette exception aux obligations du responsable du traitement visées aux articles 12 à 22 et 34 du Règlement et à l'obligation de transparence visée au point 1.a) de l'article 5 du Règlement est autorisée par

Verordening wordt toegestaan door artikel 23 van deze Verordening indien zij in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter bescherming van de nationale veiligheid, de landsverdediging en de openbare veiligheid. Gelet op de opdrachten zoals bepaald in de artikelen 7 en 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (wet van 30 november 1998) alsook van de ondersteunende diensten bedoeld in artikel 2, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, lijdt het geen twijfel dat het gaat om een noodzakelijke maatregel ter bescherming van de nationale veiligheid in het bijzonder.

Om alle bedreigingen tegen de Belgische staat en zijn burgers te kunnen bestrijden, moeten de inlichtingendiensten tot inlichtingenonderzoeken overgaan om de bedreigingen en de aanstichters ervan te kunnen identificeren. Er moet tot elke prijs vermeden worden dat deze laatsten dankzij hun recht op informatie bedoeld in artikelen 12 tot 22 en 34 van de Verordening ervan op de hoogte gebracht worden dat een inlichtingendienst hen “in de gaten houdt”. Om de doeltreffendheid en de geheim van de inlichtingenonderzoeken te garanderen, is de in dit artikel voorziene uitzondering noodzakelijk en evenredig.

In antwoord op punt 2 van artikel 23 van de Verordening omvatten deze wet, de Verordening alsook de wet van 30 november 1998 alle vereiste specifieke bepalingen:

— de doeleinden: artikelen 7 en 11 van de wet van 30 november 1998 alsook bepaalde doeleinden van de ontvanger van gegevens van een inlichtingendienst; artikel 3 van de wet van 10 juli 2006 alsook bepaalde doeleinden van de ontvanger van gegevens van het OCAD en van zijn ondersteunende diensten bedoeld in artikel 2, 2°, van de wet van 10 juli 2006;

— de categorieën van gegevens: de inlichtingendiensten maken in de uitvoering van hun opdrachten geen onderscheid tussen de categorieën van gegevens. Dit wordt in deze memorie van toelichting uitgelegd in de commentaar op titel 3; de gegevens die het OCAD ontvangt van zijn ondersteunende diensten bedoeld in artikel 2, 2°, van de wet van 10 juli 2006;

— het toepassingsgebied van de beperkingen: het gaat om een uitzondering op alle artikelen handelende over het recht op informatie van de betrokkene en aanverwante rechten (bijvoorbeeld het recht van verzet) die gerechtvaardigd is door het feit dat de betrokkenen van de inlichtingen en politionele onderzoeken absoluut niet mogen weten dat ze in de gaten worden gehouden om het onderzoek niet te belemmeren;

l’article 23 dudit Règlement si elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité nationale, la défense nationale et la sécurité publique. Au vu des missions des fixées aux articles 7 et 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (loi du 30 novembre 1998) ainsi que des services d’appui visés à l’article 2, 2°, de la loi du 10 juillet 2006 relative à l’analyse de la menace, portant entre autre sur la protection des sources il ne fait aucun doute qu’il s’agit d’une mesure nécessaire pour garantir notamment la sécurité nationale.

En effet, pour lutter contre toutes les menaces envers l’État belge et ses citoyens, les autorités visées au titre 3 doivent procéder à des enquêtes de renseignement afin d’identifier les menaces et leurs auteurs. Il faut à tout prix éviter que ces derniers grâce à leur droit d’information visé aux articles 12 à 22 et 34 du Règlement soient informés qu’un service de renseignement les a “repérés”. Pour assurer l’efficacité et la secret des enquêtes de renseignement, l’exception prévue dans le présent article est nécessaire et proportionnée.

En réponse au point 2 de l’article 23 du Règlement, la présente loi, le Règlement ainsi que la loi du 30 novembre 1998 contiennent toutes les dispositions spécifiques requises:

— les finalités: les articles 7 et 11 de la loi du 30 novembre 1998 ainsi que les finalités déterminées du destinataire des données d’un service de renseignement; l’article 3 de la loi du 10 juillet 2006 ainsi que les finalités déterminées du destinataire des données de l’OCAM et de ses services d’appui visés à l’article 2, 2°, de la loi du 10 juillet 2006;

— les catégories de données: les services de renseignement, dans l’exercice de leurs missions, ne font pas de distinction de catégories de données. Ceci est notamment expliqué dans le présent exposé des motifs dans le commentaire du titre 3; les données que l’OCAM reçoit de ses services d’appui visés à l’article 2, 2°, de la loi du 10 juillet 2006;

— l’étendue des limitations: il s’agit d’une exception à tous les articles traitant du droit à l’information de la personne concernée et des droits connexes (par exemple le droit d’opposition) justifiée par le fait que les personnes concernées des enquêtes de renseignement et de police ne peuvent absolument pas savoir qu’elles sont surveillées sous peine de griller la surveillance;

— de waarborgen ter voorkoming van misbruik of een onwettige toegang of doorgifte: zie de bepalingen van titel 3 van deze wet, en de bepalingen van de Verordening;

— de verwerkingsverantwoordelijke: de definitie is terug te vinden in artikel 4, 7°, van de Verordening;

— de opslagperiode: zie art. 5, 1.e) van de Verordening;

— de risico's voor de rechten en vrijheden van de betrokkene: er wordt een uitzondering gemaakt op het recht op informatie om de hierboven beschreven redenen. Wat de rest betreft, moeten de overheid bedoeld in titel 3 en de verdere verwerkingsverantwoordelijke alle in deze wet en de Verordening bepaalde waarborgen toepassen;

— het recht om van de beperking op de hoogte te worden gesteld: de personen worden van de beperking op de hoogte gesteld door de publicatie van deze wet in het *Belgisch Staatsblad*. Een bekendmaking van de toepassing van de beperking per geval zou daarentegen afbreuk doen aan het doel van de inlichting of de opdrachten van het OCAD en van zijn ondersteunende diensten bedoeld in artikel 2, 2°, van de wet van 10 juli 2006. Uit de loutere bekendmaking van de toepassing van artikel 23 van de Verordening zou de betrokkene kunnen afleiden dat een overheid bedoeld in titel 3 over hem betreffende gegevens beschikt.

Om te vermijden dat de verwerkings-verantwoordelijke van een gegeven van een overheid bedoeld in titel 3 argwaan wekt bij het personne concernée, verduidelijkt het tweede lid van paragraaf 2 van dit artikel dat de verantwoordelijke niets mag meedelen dat een aanwijzing zou kunnen zijn van het feit dat hij over gegevens van een overheid bedoeld in titel 3 beschikt.

In geen geval mag de verwerkings-verantwoordelijke aan de betrokkene melden dat dit artikel of artikel 23 van de Verordening toegepast werd. Hij mag de betrokkene ook niet verwijzen naar het Vast Comité van Toezicht op de inlichtingendiensten (Comité I). Hij moet verwijzen naar zijn bevoegde toezichthoudende autoriteit.

De derde paragraaf van dit artikel maakt de bescherming ook van toepassing op de logs en registraties van het raadplegen of van andere verwerkingen van een gegevensbank door een overheid bedoeld in titel 3. Wanneer een overheid bedoeld in titel 3 rechtstreeks toegang heeft tot een gegevensbank die hem niet toebehoort, worden deze raadplegingen geregistreerd (oplijsting/logs).

— les garanties destinées à prévenir les abus ou l'accès ou transfert illicites: voir les dispositions du titre 3 de la présente loi, et les dispositions du Règlement;

— le responsable du traitement: la définition se trouve à l'article 4, 7°, du Règlement;

— la durée de conservation: voir art. 5,1.e) du Règlement;

— les risques pour les droits et libertés de la personne concernée: il est fait exception au droit à l'information pour les raisons décrites ci-dessus. Pour le reste, l'autorité visée au titre 3 et le responsable de traitement ultérieur doivent appliquer toutes les garanties fixées par la présente loi et le Règlement;

— droit d'être informé de la limitation: les personnes sont informées de la limitation par la publication de la présente loi au *Moniteur belge*. Par contre, une information au cas par cas de l'application de la limitation nuirait à la finalité de renseignement ou aux missions de l'OCAM et de ses services d'appui visés à l'article 2, 2°, de la loi du 10 juillet 2006. En effet, par la simple information qu'il est fait application de l'article 23 du Règlement, la personne concernée pourrait en déduire qu'une autorité visée au titre 3 dispose de données la concernant.

Pour éviter que le responsable du traitement d'une donnée d'une autorité visée au titre 3 ne mette la puce à l'oreille de la personne concernée, l'alinéa 2 du paragraphe 2 du présent article précise que le responsable ne peut faire aucune mention qui serait susceptible de donner une indication sur le fait qu'il disposerait de données d'une autorité visée au titre 3.

A aucun moment, le responsable de traitement ne doit signaler à la personne concernée qu'il fait une application du présent article ou de l'article 23 du Règlement. Il ne peut pas non plus renvoyer la personne concernée vers le Comité permanent de contrôle des services de renseignement (Comité R). Il doit renvoyer vers sa propre autorité de contrôle compétente.

Paragraaf 3 du présent article rend également la protection applicable aux loggings et enregistrements de consultation ou d'autres traitements d'une banque de données par une autorité visée au titre 3. En effet, lorsqu'une autorité visée au titre 3 a un accès direct à une banque de données ne lui appartenant pas, ses consultations sont enregistrées (journalisation/logging).

Indien de persoon van wie de gegevens geraadpleegd zijn, ervan op de hoogte zou worden gesteld dat een overheid bedoeld in titel 3 zijn gegevens verzamelt, zou dit het inlichtingenonderzoek ernstig of de opdrachten van het OCAD en van zijn ondersteunende diensten bedoeld in artikel 2, 2°, van de wet van 10 juli 2006 in gevaar brengen. Bijgevolg krijgen de verwerkingsverantwoordelijken van de gegevensbanken waartoe de overheden bedoeld in titel 3 toegang hebben, een verbod opgelegd om de betrokkene op de hoogte te stellen van het raadplegen van zijn gegevens door een overheid bedoeld in titel 3, in toepassing van dit artikel.

Paragraaf 5 van artikel 11 bepaalt de verhoudingen tussen de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 en het Vast Comité I alsook de wijze waarop de toezichthoudende autoriteit de betrokkene antwoordt. Op vraag van de Privacycommissie, punt 123 van haar advies, worden de bevoegde toezichthoudende autoriteiten bepaald.

In antwoord op punt 124 van het advies van de Privacycommissie wordt bevestigd dat het altijd de Gegevensbeschermingsautoriteit is, de autoriteit die werd gevat, die de betrokkene antwoordt. De nieuwe formulering verduidelijkt de situatie. Trouwens, de term “beroep” wordt vervangen door de woorden “verzoek en klacht”.

In het punt 125 vraagt de Privacycommissie zich af in welke situatie een verwerkingsverantwoordelijke van titel 1 enkel over informatie zou beschikken afkomstig van een autoriteit van titel 3. Dat kan het geval zijn, bijvoorbeeld, indien een inlichtingendienst een Belgische onderneming informeert dat een persoon x die gekend is voor industriële spionage zich sterk interesseert in de onderneming.

Art. 12

Dit artikel bepaalt een beperkte toepassing van artikel 23 van de Verordening. Het heeft betrekking op het geval waarin een verwerkingsverantwoordelijke persoonsgegevens aan een overheid bedoeld in titel 3, ondertitels 2 en 4, bezorgt. In dat geval verbiedt dit artikel de verwerkingsverantwoordelijke om aan de betrokken persoon mee te delen dat de overheid ontvanger van de gegevens is, door te voorzien in een uitzondering op de artikelen 14.1.e en 15.1.c van de Verordening. Deze uitzondering beantwoordt aan de discretievereiste die eigen is aan de opdrachten van het OCAD en van zijn ondersteunende diensten bedoeld in artikel 2, 2°, van de wet van 10 juli 2006 en de Krijgsmacht.

Si la personne dont les données ont fait l’objet d’une consultation était informée qu’une autorité visée au titre 3 collecte ses données, cela mettrait sérieusement en péril l’enquête de renseignement ou les missions de l’OCAM et de ses services d’appui visés à l’article 2, 2°, de la loi du 10 juillet 2006. Par conséquent, les responsables du traitement des banques de données auxquelles les autorités visées au titre 3 ont accès, ont interdiction d’informer la personne concernée des consultations de ses données par une autorité visée au titre 3, en application du présent article.

Le paragraphe 5 de l’article 11 détermine les relations entre l’Autorité de protection de données visée dans la loi du 3 décembre 2017 et le Comité permanent R ainsi que la manière dont l’autorité de contrôle répond à la personne concernée. A la demande de la Commission vie privée, au point 123 de son avis, les autorités de contrôle compétentes ont été identifiées.

En réponse au point 124 de l’avis de la Commission vie privée, il est confirmé que c’est toujours l’Autorité de protection des données, l’autorité qui a été saisie, qui répond à la personne concernée. La nouvelle formulation clarifie la situation. Par ailleurs, le terme “recours” est remplacé par les mots “requête et plainte”.

La Commission vie privée, au point 125 de son avis, se demande dans quelle situation un responsable du traitement du titre 1er disposerait uniquement d’informations émanant d’une autorité du titre 3. Cela pourrait être le cas, par exemple, si un service de renseignement informe une entreprise belge qu’une personne x connue pour espionnage industriel s’intéresse très fortement à elle.

Art. 12

Cet article fait une application limitée de l’article 23 du Règlement. Il vise le cas où un responsable de traitement transmet des données à caractère personnel à une autorité visée au titre 3, sous-titres 2 et 4. Dans ce cas, l’ article interdit au responsable du traitement de communiquer à la personne concernée que l’autorité est destinataire des données, en prévoyant une exception aux articles 14.1.e et 15.1.c du Règlement. Cette exception répond à l’exigence de discrétion inhérente aux missions de l’OCAM et de ses services d’appui visés à l’article 2, 2°, de la loi du 10 juillet 2006 et des forces armées.

In punt 127 van het advies van de Privacycommissie en op pagina 18 van het advies van de Raad van State wordt aangehaald dat deze bepaling niet nuttig is omdat de autoriteiten bedoeld in titel 3 niet onder de definitie van “ontvanger” vallen in de zin van artikel 4.9 van de Verordening aangezien het overheden betreft die gegevens ontvangen in het kader van een bijzondere onderzoeksopdracht. Het is inderdaad zo dat de inlichtingen- en veiligheidsdiensten bedoeld in ondertitel 1 van titel 3 bijzondere onderzoeksopdrachten hebben en dus niet beschouwd worden als ontvangers in de zin van artikel 4.9 van de Verordening. Bijgevolg zijn de verplichtingen bedoeld in de artikelen 13.1.e, 14.1.e en 15.1.c. van de Verordening niet van toepassing wanneer een verwerkingsverantwoordelijke persoonsgegevens overmaakt aan een autoriteit bedoeld in de ondertitels 1 en 3 van titel 3. Geen enkele melding aan de betrokkene van de doorgifte van de persoonsgegevens kan dan ook gedaan worden, om evidente redenen van discretie. Het artikel wordt echter behouden voor de autoriteiten bedoeld in ondertitels 2 (Krijgsmacht) en 4 (OCAD) van titel 3 die geen bijzondere onderzoeken doen en dus onder de definitie van ontvanger vallen. Om te vermijden dat een autoriteit van titel 1 aan de betrokkene vermeldt dat zij gegevens heeft overgemaakt aan een autoriteit van de ondertitels 2 en 4 van titel 3 bepaalt huidig artikel dat de artikelen 14.1.e en 15.1.c van de Verordening niet van toepassing zijn. Deze uitzondering voldoet aan de vereiste discretie inherent aan de missies van OCAD en de Krijgsmacht.

La Commission vie privée, au point 127 de son avis, et le Conseil d’État, en page 18 de son avis, relèvent que cette disposition n’est pas utile car les autorités visées au titre 3 n’entrent pas dans la définition de “destinataire” au sens de l’article 4.9 du Règlement puisqu’il s’agit d’autorités publiques recevant des données dans le cadre d’une mission d’enquête particulière. Il est effectivement vrai que les services de renseignement et de sécurité visé au sous-titre 1er du titre 3 et les autorités visées au sous-titre 3 du titre 3 ont des missions d’enquête particulière et ne sont donc pas considérés comme des destinataires au sens de l’article 4.9. du Règlement. Par conséquent, les obligations visées aux articles 13.1.e, 14.1.e et 15.1.c. du Règlement ne s’appliquent pas quand un responsable du traitement transmet des données à caractère personnel à une autorité visée aux sous-titres 1 ou 3 du titre 3. Aucune mention ne peut dès lors être faite à la personne concernée de la transmission des données, pour des raisons évidentes de discrétion. L’article est cependant maintenu pour les autorités visées aux sous-titres 2 (les Forces armées) et 4 (l’OCAM) du titre 3 qui n’effectuent pas d’enquêtes particulières et donc relèvent de la définition de destinataire. Pour éviter qu’une autorité du titre 1er ne mentionne à la personne concernée qu’elle a transmis des données à une autorité des sous-titres 2 et 4 du titre 3, le présent article dispose que les articles 14.1.e et 15.1.c du Règlement ne s’appliquent pas. Cette exception répond à l’exigence de discrétion inhérente aux missions de l’OCAM et des forces armées.

Art. 13

Dit artikel kadert de toegang van de autoriteiten bedoeld in ondertitels 1 en 6 van titel 3 tot externe gegevensbanken voor hun eigen diensten (bijv. het rijksregister). In haar advies (punt 132) beveelt de Privacycommissie aan dat de specifieke wettelijke verwijzingen die de toegang tot deze externe gegevensbanken toelaten hernomen zouden worden in dit ontwerp. Het is echter niet mogelijk om aan dit verzoek te voldoen: enerzijds, de toegangen waarover autoriteiten als de inlichtingendiensten dienen te beschikken zijn talrijk en een volledige lijst is dus niet haalbaar in dit ontwerp zelf zonder deze bepaling onleesbaar te maken. Als voorbeeld kunnen de artikelen 14, 16/2, 16/3 en 16/4 aangehaald worden uit de organieke wet van de inlichtingendiensten maar ook buiten deze organieke wet zijn er de koninklijke besluiten die de toegang tot het rijksregister regelen en ook nog de machtigingen van de sectorale comités van de Privacycommissie. Anderzijds is deze lijst van wettelijke verwijzingen in constate evolutie hetgeen een voortdurende aanpassing van deze bepaling zou noodzaken.

Art. 13

Cet article encadre l’accès des autorités visées aux sous-titres 1 et 6 du titre 3 à des banques de données externes à leurs propres services (par ex., le registre national). Dans son avis (point 132), la Commission vie privée recommande que les références légales spécifiques permettant l’accès à ces banques de données externes soient reprises dans le projet. Il n’est cependant pas possible de satisfaire à cette demande: d’une part, les accès dont devraient disposer des autorités comme les services de renseignement sont nombreux et une liste exhaustive n’est pas envisageable dans le projet-même, sans compter qu’elle rendrait la disposition illisible. A titre d’exemple, on peut citer, dans la loi organique des services de renseignement les articles 14, 16/2, 16/3 et 16/4, mais aussi en dehors de cette loi organique, les arrêtés royaux autorisant l’accès au registre national, et encore les autorisations des comités sectoriels de la Commission vie privée. D’autre part, cette liste de références légales est en évolution constante, ce qui entraînerait une adaptation incessante de la présente disposition.

De overheden bedoeld in titel 3 zijn onderworpen aan verregaande beperkingen ter bescherming van hun bronnen, de identiteit van hun agenten en de vertrouwelijkheid van hun onderzoeken. Deze verplichtingen zijn uitdrukkelijk voorgeschreven bij voorbeeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en gaan gepaard met strafsancties in geval van niet-naleving:

— artikel 13 houdt de verplichting in om de bronnen van de inlichtingendiensten te beschermen. Het gaat hier natuurlijk niet enkel over informanten, buitenlandse inlichtingendiensten en de informatie die zij delen met een veiligheidsdienst. De bescherming heeft ook betrekking op de technische bronnen van de inlichtingendiensten. In het algemeen verplicht deze bepaling de inlichtingendiensten tot discretie en bescherming van de opdrachten;

— artikel 36 voorziet een plicht tot geheimhouding van de informatie waarvan de agenten van de inlichtingendiensten kennis hebben in het kader van functie;

— artikel 43 straft de kwaadwillige verspreiding van de identiteit van agenten van de inlichtingendiensten, evenals de schending van de twee voornoemde verplichtingen.

In het kader van hun onderzoeken moeten de agenten altijd rekening houden met het risico voor hun informanten of andere bronnen, door te trachten de informatie die ze ingewonnen hebben te toetsen aan andere informatie of ze verder uit te diepen. Wanneer de agenten er niet in slagen om hun bescherming te garanderen, moeten ze afzien van hun onderneming. Heel het inlichtingenwerk ondervindt hiervan de gevolgen of wordt zelfs onmogelijk gemaakt als het risico te groot is voor de bescherming die de inlichtingendiensten moeten bieden.

Dit artikel heeft als doelstelling de hiervoor beschreven bescherming te garanderen, door te waken over de vertrouwelijkheid van de opzoekingen die de overheden bedoeld in titel 3 kunnen doen in de externe databanken (vb. het Rijksregister) bij een on-line toegang. Het feit dat personen die vreemd zijn aan de betrokken overheid kennis kunnen krijgen van een opzoeking door deze dienst, zou een gevaar kunnen opleveren voor de bescherming waarvoor de inlichtingendiensten moeten zorgen. Wanneer, bijvoorbeeld, een buitenlandse dienst aan de Veiligheid van de Staat informatie geeft over een nakende dreiging met betrekking tot mijnheer XY, geboren op 01.01 2001 en met de Belgische nationaliteit, verifieert de Veiligheid van de Staat eerst of er een overeenkomst gevonden kan worden tussen de geseinde persoon en iemand in het Rijksregister

Les autorités visées au titre 3 ont des contraintes conséquentes pour assurer la protection de l'identité de leurs agents, la confidentialité de leurs enquêtes et la protection de leurs sources. Ces obligations sont expressément prescrites notamment dans la loi organique du 30 novembre 1998 des services de renseignement et de sécurité et sont assorties de sanctions pénales, en cas de non-respect:

— l'article 13 impose la protection des sources des services de renseignement. Cela ne concerne bien entendu pas que les informateurs, les services de renseignement étrangers et les informations qu'ils partagent avec les services de renseignement. La protection porte également sur les sources techniques des services de renseignement. De manière générale, cette disposition traduit une obligation de discrétion et de protection des missions dans le chef des services de renseignement;

— l'article 36 prescrit une obligation au secret portant sur les informations dont les agents des services de renseignement ont connaissance dans le cadre de leurs fonctions;

— l'article 43 punit la divulgation avec intention malveillante de l'identité des agents des services de renseignement, ainsi que le non-respect des deux obligations précédentes.

Dans le cadre de leurs enquêtes, les agents doivent toujours prendre en compte le risque qu'ils font courir à leur informateur ou à toute autre source, en tentant de recouper ou d'approfondir les informations obtenues de leur part. S'ils ne parviennent pas à garantir leur protection, les agents doivent renoncer à l'action entreprise. C'est tout le travail du renseignement qui s'en ressent, voire qui est rendu impossible, si le risque est trop grand à l'égard des protections que les services de renseignement ont l'obligation de garantir.

Cet article a pour objectif d'assurer les protections expliquées plus haut, en veillant à la confidentialité des recherches que les autorités visées au titre 3 peuvent effectuer dans les banques de données externes à leurs propres services (ex. le registre national), lorsqu'un accès en ligne est installé. En effet, le fait que des personnes extérieures à l'autorité concerné par la recherche peuvent prendre connaissance de celle-ci, est susceptible de mettre en péril les protections que les services de renseignement sont tenus de garantir. Par exemple, lorsqu'un service étranger informe la Sûreté de l'État d'une menace imminente en relation avec Monsieur XY, né le 01.01 2001, de nationalité belge, la Sûreté de l'État va notamment commencer par vérifier s'il y a concordance entre l'individu signalé et l'existence d'une telle personne au registre national,

en of er geen misverstand is met een andere persoon. Een correcte identificatie van de potentiële dreiging is natuurlijk primordiaal. De Veiligheid van de Staat moet trouwens de informatie van de buitenlandse inlichtingendienst beschermen. Deze informatie mag niet verspreid worden vooraleer ze steun vindt in de resultaten van het onderzoek.

De bescherming van de onderzoeken is tevens van belang voor de betrokkenen. Het feit dat een inlichtingendienst interesse toont in een persoon heeft immers, helaas regelmatig, tot gevolg dat wie niet bekend is met de inlichtingenwereld snel ongunstige conclusies trekt over de persoon in kwestie wat leidt tot reputatieschade voor hem of haar. Dit negatieve effect moet koste wat het kost worden vermeden.

Het is immers duidelijk dat men een risico neemt op het vlak van de vertrouwelijkheid, wanneer men weet, en dit is feitelijk zo, dat de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming zich moeten laten bijstaan door een ICT-dienst van tientallen personen om controle uit te oefenen op de voornamelijk organisatorische verplichtingen (bijvoorbeeld het naleven van het “need to know”-beginsel) bij de verwerking van persoonsgegevens. Het spreekt ook voor zich dat hoe vaker het bestaan van onderzoeken gedeeld wordt buiten de inlichtingendiensten, hoe hoger het risico is dat hun onderzoeken in het gedrang komen.

Om deze redenen mogen de opzoekingen die de overhden bedoeld in titel 3 verrichten voor hun onderzoeken enkel gekend zijn door een zeer beperkt aantal personen die niet tot deze diensten behoren. Het is in dat geval vanzelfsprekend dat het delen van gegevens beveiligd moet zijn (need to share securely). In het kader van een toegang tot een externe gegevensbank is het de verwerkingsverantwoordelijke in eigen persoon of de persoon die hij daartoe aanwijst die de wettelijke opdrachten van toezicht uitoefent (de “of” zijnde exclusief) op de door de inlichtingendiensten uitgevoerde verwerkingen in de externe gegevensbank waarvoor hij verantwoordelijk is. Het gaat om één enkele persoon. De functionaris voor gegevensbescherming van de betrokken externe gegevensbank heeft ook toegang tot de logs van de verwerkingen van de inlichtingendiensten in de gegevensbank waarvoor hij belast is met het toezicht op de naleving van de wetgeving. Hij moet immers zijn wettelijke opdracht van toezicht kunnen uitoefenen.

In het punt 129 is de Privacycommissie van mening dat het ontwerp duidelijk moet maken dat het altijd slechts om een en dezelfde fysieke persoon gaat. Er wordt dan ook in deze memorie van toelichting verduidelijkt dat de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming van de externe

et s’il n’existe pas de méprise avec un autre individu. L’identification correcte de la menace potentielle est évidemment primordiale. Par ailleurs, l’information transmise par le service de renseignement étranger doit être protégée par la Sûreté de l’État et ne peut être divulguée avant que les résultats de l’enquête ne cautionnent l’information transmise.

La protection des enquêtes est également importante pour les personnes concernées. En effet, le fait qu’un service de renseignement s’intéresse à une personne entraîne, malheureusement souvent, dans l’esprit de non-familiarisés avec le monde du renseignement, des conclusions rapides défavorables à la personne concernée qui lui cause un dommage réputationnel. Il faut évidemment éviter cet effet pervers à tout prix.

Sur le plan de la confidentialité, et du risque encouru pour celle-ci, c’est par ailleurs un état de fait que le responsable du traitement et le délégué à la protection des données doivent se faire assister d’une équipe ICT (composée de dizaines de personnes) pour exercer le contrôle sur le respect des obligations notamment organisationnelles (par exemple, pour le respect du need to know), lors de traitements de données à caractère personnel. De toute évidence, il est clair aussi que plus l’existence d’enquêtes est partagée en dehors des services de renseignement, plus le risque est grand que leurs enquêtes soient grillées.

Pour ces raisons, les recherches que font les autorités visées au titre 3 dans le cadre de leurs enquêtes ne peuvent être connues que d’un nombre très limité de personnes externes auxdits services. Dans ce cas, il va de soi que le partage de données doit être sécurisé (need to share securely). Dans le cadre d’un accès à une banque de données externe, il s’agit du responsable du traitement en personne ou la personne qu’il désigne à cet effet pour exercer ses missions légales de contrôle (le “ou” étant exclusif) sur les traitements effectués par les services de renseignement dans la banque de données externe dont il est le responsable. Il s’agit d’une seule personne. Le délégué à la protection des données de la banque de données externe concernée a également accès aux loggings des traitements des services de renseignement dans la banque de données pour laquelle il a la charge de veiller au respect de la législation. Il doit en effet pouvoir exercer sa mission légale de contrôle.

La Commission vie privée estime, dans son point 129, que le projet devrait spécifier clairement qu’il ne s’agit toujours que d’une seule et même personne physique. Il est dès lors précisé, dans le présent exposé des motifs, que le responsable du traitement et le délégué à la protection des données de la banque de données

gegevensbank slechts twee en enkel twee personen vertegenwoordigen. De beperking tot twee personen binnen de autoriteiten bedoeld in titel 3 kan niet gerechtvaardigd worden in de mate dat het de bescherming van de onderzoeken tegenover de buitenwereld is die in dit geval moet worden verzekerd. Dit sluit niet uit dat er ook binnen de autoriteiten bedoeld in titel 3 een beperking mogelijk is tot een team dat zich wijdt aan het beheer enerzijds en aan het controleren van de toegangen anderzijds. De leden van dit team worden in elk geval onderworpen aan zeer strikte regels van need to know en de geheimhoudingsplicht.

Om de vertrouwelijkheid van de verwerkingen in de betrokken externe gegevensbank te beschermen, wordt de toegang van deze personen verzekerd door de toepassing van technische, organisatorische en persoonlijke beveiligingsmaatregelen. Deze bepaling gaat niet in op de details van de technische maatregelen omdat het door de technologische vooruitgang niet mogelijk is om in een wet te bepalen welke middelen gebruikt worden. Dit zouden versleutelingsmethodes kunnen zijn, maar ook andere oplossingen. Organisatorische en persoonlijke maatregelen zijn bijvoorbeeld de vereiste van een veiligheidsmachtiging van ten minste het niveau geheim om toegang te krijgen tot de logs van de verwerkingen van de inlichtingendiensten.

Er moet ook benadrukt worden dat hun toegang enkel voor toezichtsdoeleinden gebruikt mag worden. Indien andere doeleinden nodig blijken (bijvoorbeeld, voor de facturatie van raadplegingen dient men toegang te hebben tot het aantal loggings), voorziet de bepaling dat deze in een protocolakkoord tussen de betrokken verwerkingsverantwoordelijken vastgesteld moeten worden.

De Privacycommissie (punt 130 van het advies) en de Raad van State (pagina 18 van het advies) uiten de bezorgdheid dat de bepaling de toegang mogelijk maakt tot de loggings voor andere doeleinden dan een controle, aan de hand van een protocol gesloten tussen betrokken verwerkingsverantwoordelijken. De Privacycommissie meent dat deze andere doeleinden in de wet zelf bepaald moeten worden. Het ontwerp werd aangepast in overeenstemming met deze opmerking. De andere doeleinden waarvoor een toegang zou kunnen worden voorzien buiten deze van de controle zullen enkel mogelijk zijn indien een wet dit toelaat. Het wettelijkheids- en een voorzienbaarheidsprincipe moeten in elk geval worden nageleefd.

Naast de verwerkingsverantwoordelijke van de betrokken externe gegevensbank en zijn functionaris voor gegevensbescherming wordt er ook op gewezen dat de verwerkingsverantwoordelijke van de betrokken externe ne représentent donc que deux et seulement deux personnes. La limitation à deux personnes au sein des autorités visées au titre 3 n'est pas justifiée dans la mesure où c'est la protection des enquêtes vis-à-vis de l'extérieur qui doit être assurée, en l'occurrence. Ce qui n'écarte pas une limitation également au sein des autorités visées sous le titre 3, à une équipe dédiée à la gestion, d'une part, et au contrôle des accès, d'autre part. Les membres de cette équipe sont de toute façon soumis à des règles très strictes de need to know et d'obligation au secret.

Pour protéger la confidentialité des traitements dans la banque de données externe concernée, l'accès de ces personnes sera assuré par la mise en œuvre de mesures de sécurité techniques, organisationnelles et personnelles. Cette disposition n'entre pas dans le détail des mesures techniques, parce l'évolution de la technologie ne permet pas de déterminer dans une loi quels seront les moyens utilisés. Il pourrait s'agir de méthodes de chiffrement mais aussi d'autres solutions. Pour les mesures organisationnelles et personnelles, on peut citer, par exemple, l'exigence d'une habilitation de sécurité d'un niveau au moins secret pour accéder aux loggings des traitements des services de renseignement.

Il est important aussi de souligner que leur accès ne pourra être utilisé qu'à des fins de contrôle. Si d'autres finalités s'avèrent nécessaires (par exemple, pour la facturation des consultations, il faut avoir accès au nombre de loggings), la disposition prévoit qu'elles doivent être définies dans un protocole d'accord entre les responsables du traitement concernés.

La Commission vie privée et le Conseil d'État s'inquiètent (point 130 de l'avis CPVP et page 18 de l'avis CE), que la disposition permette l'accès aux loggings pour d'autres finalités que celle du contrôle, par le biais d'un protocole conclu entre les responsables du traitement concernés. La Commission vie privée considère que ces autres finalités doivent être déterminées par la loi elle-même. Le projet a été adapté conformément à cette remarque. Les autres finalités pour lesquelles un accès pourrait être prévu en dehors de celle du contrôle ne pourront être visées que si une loi l'autorise. Les principes de légalité et de prévisibilité doivent en tout état de cause être respectés.

A côté du responsable du traitement de la banque de données externe concernée et de son délégué à la protection des données, il est également indiqué que le responsable du traitement de l'autorité visée au titre

overheid bedoeld in titel 3 en zijn functionaris voor gegevensbescherming uiteraard toegang hebben om de wettelijke conformiteit van de door de leden van de betrokken inlichtingen- en veiligheidsdienst uitgevoerde verwerkingen te kunnen controleren.

We kunnen niet uitsluiten dat het nodig is om toegang te verlenen aan een andere persoon dan zij die hierboven vermeld zijn, bijvoorbeeld voor technische ondersteuning. In dat geval voorziet dit artikel de mogelijkheid om een bijkomende persoon aan te wijzen in een protocolakkoord tussen de betrokken verwerkingsverantwoordelijken. De Privacycommissie uit een voorbehoud, in punt 130 van haar advies, voor wat betreft deze mogelijkheid voorzien in punt 5° om eenvoudig bij wijze van protocol de toegang uit te breiden tot derden voor andere doeleinden dan de controle. De Raad van State formuleert dezelfde opmerking voor een gelijkaardige bepaling van titel 2 (pagina 33 van het advies betreffende artikel 50). Om tegemoet te komen aan de Privacycommissie en de Raad van State verduidelijkt het ontwerp dat deze mogelijkheid om een derde persoon aan te duiden slechts toegelaten is om de controle effectief te maken. Het betreft dus a priori de ondersteuning door een lid van het informaticapersoneel.

Het is duidelijk dat naast het door de verschillende bovengenoemde actoren uitgeoefende toezicht de autoriteit die bevoegd is om toezicht uit te oefenen op de overheden bedoeld in titel 3 ook de logs en de desbetreffende verwerkingen tot haar beschikking moet hebben. Er moet benadrukt worden dat de toegangen tot de gegevensbanken intern altijd heel streng georganiseerd zijn. Vooreerst worden de toegangen enkel toegekend aan de agenten die het echt nodig hebben om hun werk te kunnen uitvoeren. De juridische dienst van de inlichtingendiensten heeft bijvoorbeeld geen toegang tot het Rijksregister. De opzoekingen worden daarenboven gevalideerd door de functionele chef van de agent die de opzoeking verricht. Bepaalde opzoekingen vereisen zelfs een beslissing van het diensthoofd. Ten slotte worden er periodiek steekproeven genomen om de wettelijkheid en de proportionaliteit van de verwerkingen te controleren. Dit is een solide basis. Dit moet gepaard gaan met een performante externe controle door de autoriteit die toezicht houdt op de inlichtingen- en veiligheidsdiensten zoals hiervoor vermeld. In overeenstemming met de wens van de Privacycommissie (algemene opmerking, en in het bijzonder punt 123) verduidelijkt dit ontwerp, telkens wanneer dit mogelijk is, welke toezichthoudende autoriteit bevoegd is. In dit geval is dat het Vast Comité I.

Om te antwoorden op de verzoeken van de Privacycommissie (punt 220 van het advies) en van de Raad van State (pagina 33 van het advies) over

3 concernée et son délégué à la protection des données ont bien entendu un accès pour pouvoir vérifier la conformité légale des traitements effectués par les membres du service de renseignement et de sécurité concerné.

On ne peut exclure qu'il soit nécessaire d'accorder un accès à une autre personne que celles qui sont visées plus haut, par exemple pour un support technique. Dans ce cas, cet article prévoit la possibilité de désigner la personne supplémentaire dans un protocole d'accord entre les responsables du traitement concernés. La Commission vie privée émet une réserve, dans le point 130 de son avis, quant à cette faculté prévue dans le 5°, d'élargir, par simple protocole, l'accès à des tiers pour d'autres finalités que celle du contrôle. Le Conseil d'État formule la même remarque pour une disposition similaire du titre 2 (page 33 de l'avis CE concernant l'article 50). Pour apaiser la Commission vie privée et le Conseil d'État, le projet précise que cette possibilité de désigner une tierce personne n'est permise que pour rendre effectif le contrôle. Il s'agit a priori de l'appui d'un membre du personnel informatique.

Il est évident que parallèlement au contrôle exercé par les différents acteurs cités plus haut, l'autorité compétente pour exercer un contrôle sur les autorités visées au titre 3 doit également avoir à sa disposition les loggings et les traitements qui y sont liés. Il faut souligner que les accès aux banques de données sont déjà organisés en interne de manière très rigoureuse. En premier lieu, les accès ne sont accordés qu'aux agents qui en ont réellement besoin pour accomplir leur travail. Par exemple, le service juridique des services de renseignement n'a pas accès au registre national. Ensuite, les recherches effectuées sont couvertes par le chef fonctionnel des agents qui y procèdent. Certaines recherches nécessitent même une décision du dirigeant du service. Enfin, des contrôles aléatoires périodiques sont réalisés pour vérifier la légalité et la proportionnalité des traitements effectués. C'est une base solide. Il convient de la coupler avec un contrôle extérieur performant de l'autorité de contrôle des services de renseignement et de sécurité, comme développé plus haut. Conformément au souhait de la Commission vie privée (remarque générale, et notamment point 123), chaque fois que cela est possible le projet précise quelle autorité de contrôle est compétente. En l'occurrence, c'est le Comité permanent R.

Pour répondre aux demandes de la Commission vie privée (point 220 de son avis) et du Conseil d'État (page 33 de son avis) sur le manque de définition de la notion

het gebrek aan definitie van de notie controlesysteem werden de termen geschrapt en vervangen door meer duidelijke termen. Zo wordt er verduidelijkt dat het de logbestanden en de technische, organisatorische en individuele beveiligingsmaatregelen betreft die ter beschikking worden gesteld van het Vast Comité I.

Tot slot wordt er bepaald dat de overheden bedoeld in titel 3 mogen afwijken van de technische, organisatorische en individuele beveiligingsmaatregelen ter bescherming van hun verwerkingen, indien zij van mening zijn dat de belangen (bronnen, identiteit van agenten, discretie van onderzoeken) niet bedreigd zijn door een kennisname van hun verwerkingen. Om te antwoorden op de opmerkingen van de Privacycommissie (punt 131) en de Raad van State (pagina 18), volgens dewelke de afwijking niet kan berusten op een arbitraire beoordelingsmacht van de autoriteiten, werd het ontwerp aangepast om te verduidelijken dat de afwijking slechts kan volgen uit een situatieanalyse waarbij tot het besluit wordt gekomen dat er geen gevaar is voor de te beschermen belangen. Gemeenschappelijke gegevensbanken zijn een duidelijk voorbeeld waarbij alle maatregelen niet noodzakelijk van toepassing zijn. Gegeven het feit dat ze deze gegevensbanken aanvullen en dat er een spoor van elke transactie zichtbaar moet zijn voor de andere gebruikers, heeft de beperking van de toegang tot de verwerkingen van de betrokken dienst weinig zin. In de eerste plaats hebben de betrokken autoriteiten bedoeld in titel 3 beschouwd dat het delen van niet-geclassificeerde informatie met andere autoriteiten die deelnemen aan gemeenschappelijke gegevensbanken niet de te beschermen belangen in gevaar brengt.

Het OCAD verwerkt de gegevens die het overeenkomstig artikel 6 van de wet van 10 juli 2006 ontvangt van zijn ondersteunende diensten bedoeld in artikel 2, 2°, van de wet van 10 juli 2006, waaronder de inlichtingen en veiligheidsdiensten bedoeld in titel 3 van deze wet. Voor de rechtvaardiging van deze beperking wordt verwezen naar de commentaar betreffende artikel 11. Overeenkomstig artikel 13 van de wet van 10 juli 2006 moet ieder lid van het OCAD de geheimen bewaren die hem zijn toevertrouwd in de uitoefening van zijn opdracht of zijn medewerking. Het geheim blijft bestaan zelfs wanneer het lid het OCAD heeft verlaten of zijn medewerking heeft stopgezet. Deze verplichtingen gaan gepaard met strafsancties in geval van niet-naleving.

Wanneer zij de gegevensbanken raadplegen, dienen de leden van het OCAD de reden van hun opzoeking schriftelijk te motiveren in een intern document van het OCAD. Bovendien hebben slechts bepaalde leden van het OCAD toegang tot bepaalde gegevensbanken. Zo kunnen bijvoorbeeld enkel personeelsleden gedetacheerd van de politie bij het OCAD het RRN raadplegen

de système de contrôle, les termes ont été supprimés pour être remplacés par des termes plus précis. Ainsi, il est précisé que ce sont les journaux et les mesures de sécurité techniques, organisationnelles et individuelles qui sont mis à disposition du Comité permanent R.

Enfin, il est précisé que les autorités visées au titre 3 peuvent déroger aux mesures de sécurité techniques, organisationnelles et individuelles visant à protéger leurs traitements, si elles considèrent que les intérêts (sources, identité des agents, discrétion des enquêtes) ne sont pas menacés par une prise de connaissance de leurs traitements. Pour répondre aux remarques de la Commission vie privée (point 131) et du Conseil d'État (page 18), selon lesquelles la dérogation ne pouvait pas reposer sur un pouvoir d'appréciation arbitraire des autorités, le projet a été adapté pour préciser que la dérogation ne pouvait découler que d'une analyse de la situation concluant à l'absence de danger pour les intérêts à protéger. Les banques de données communes sont un exemple évident où toutes les mesures ne sont pas nécessairement d'application. Dès lors qu'ils alimentent ces banques de données et qu'une trace de chaque transaction doit être visible pour les autres utilisateurs, la limitation de l'accès aux traitements du service concerné n'a pas beaucoup de sens. A la base, les autorités concernées visées au titre 3 ont considéré que le partage d'informations non classifiées avec d'autres autorités qui participent aux banques de données communes ne mettaient pas les intérêts à protéger en danger.

Conformément à l'article 6 de la loi du 10 juillet 2006, l'OCAM reçoit des données de ses services d'appui visés à l'article 2, 2°, de la loi du 10 juillet 2006, dont les services de renseignement et de sécurité visés au titre 3 de la présente loi. Pour la justification de cette limitation, il est renvoyé au commentaire portant sur l'article 11. Conformément à l'article 13 de la loi du 10 juillet 2006, chaque membre de l'OCAM est tenu de garder les secrets qui lui sont confiés dans l'exercice de sa mission ou de sa collaboration. L'obligation de secret subsiste, même lorsque le membre a quitté l'OCAM ou a mis un terme à sa collaboration. Ces obligations sont assorties de sanctions pénales, en cas de non-respect.

Lorsqu'ils consultent ces banques de données, les membres de l'OCAM doivent systématiquement notifier par écrit dans un document interne à l'OCAM la raison de leur recherche. Ensuite, seuls certains membres de l'OCAM ont accès à certaines banques de données. Par exemple, seuls les membres détachés par la police à l'OCAM ont l'autorisation de consulter le RRN.

Art. 14

Dit artikel bepaalt de verplichtingen van de verwerkingsverantwoordelijke wanneer hij over persoonsgegevens beschikt die aanvankelijk door de gerechtelijke overheid, de politiediensten, de Algemene Inspectie van de federale politie en de lokale politie, de Cel voor Financiële Informatieverwerking, de Algemene Administratie van de Douane en Accijnzen en de Passagiersinformatie-eenheid (hierna de "organen") verwerkt worden. Om evidente redenen van veiligheid en discretie mag de verwerkingsverantwoordelijke, en zijn personeel, zijn DPO of zijn verwerker, de betrokken persoon er niet van op de hoogte brengen dat hij over op hem betrekking hebbende gegevens beschikt wanneer deze van die organen afkomstig zijn. Het spreekt voor zich dat de transparantieverplichting bedoeld in punt 1.a) van dit artikel 5 niet van toepassing is.

Deze uitzondering op de verplichtingen van de verwerkingsverantwoordelijke bedoeld in de artikelen 12 tot 22 en 34 van de Verordening wordt toegestaan door artikel 23 van deze Verordening indien zij in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de belangrijke doelstellingen van algemeen belang die worden opgesomd in artikel 23.1 van deze Verordening waaronder de nationale veiligheid, de openbare veiligheid, de voorkoming en opsporing van strafbare feiten alsook de onderzoeken en de vervolgingen in dat verband of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Gelet op de operationele opdrachten van die verschillende diensten die vermeld zijn in artikel XX (de doelstellingen van titel 2 beogen) van de wet, lijdt het geen twijfel dat het gaat om een noodzakelijke maatregel ter waarborging van die belangrijke doelstellingen van algemeen belang. Om de doeltreffendheid en de discretie die nodig zijn voor de verwezenlijking van die operationele doelstellingen door die organen immers te verzekeren, is de in dit artikel vastgelegde uitzondering noodzakelijk en evenredig.

In haar advies nr. 33/2018 wenst de Privacycommissie dat alle betrokken partijen in deze wet worden vermeld. De betrokken overheden, organen en organismen zijn vermeld in verschillende bijzondere wetten, decreten en ordonnaties.

Bijvoorbeeld:

— voor de politidiensten de artikelen 44/1 tot 44/11/13 van de wet op het politieambt, die voorzien in de overzending van informatie aan bepaalde overheden, organen, organismen en diensten alsook aan iedere

Art. 14

Cet article détermine les obligations du responsable du traitement lorsqu'il dispose de données à caractère personnel initialement traitées par l'autorité judiciaire, des services de police, de l'Inspection générale de la police fédérale et de la police locale, de la Cellule de Traitement des Informations Financières, de l'Administration générale des douanes et accises, et de l'Unité d'information des passagers (ci après, les "organes"). Pour des raisons évidentes de sécurité et de discrétion, le responsable du traitement, ainsi que son personnel, son DPO, ou son sous-traitant, a interdiction d'informer la personne concernée qu'il dispose de données la concernant lorsque celles-ci émanent de ces organes. Il va de soi que l'obligation de transparence visée au point 1.a) de l'article 5 n'est pas d'application.

Cette exception aux obligations du responsable du traitement visées aux articles 12 à 22 et 34 du Règlement est autorisée par l'article 23 dudit Règlement si elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs importants d'intérêt public énumérés à l'article 23.1. dudit Règlement, dont la sécurité nationale, la sécurité publique et la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Au vu des missions opérationnelles de ces différents services qui sont d'ailleurs reprises à l'article XX XX de la loi et viser les finalités du titre 2, il ne fait aucun doute qu'il s'agit d'une mesure nécessaire pour garantir ces objectifs importants d'intérêt public. En effet, pour assurer l'efficacité et la discrétion liées à la réalisation de ces finalités opérationnelles poursuivies par ces organes, l'exception prévue dans le présent article est nécessaire et proportionnée.

Dans son avis n°33/2018, la Commission vie privée souhaite voir énoncé dans la présente loi l'ensemble des "acteurs concernés". Les autorités publiques, les organes et organismes concernés sont ceux visés dans les différentes lois organiques ainsi que dans des lois particulières, décrets et ordonnances.

A titre illustratif:

— pour les services de police, les articles 44/1 à 44/11/13 de la loi sur la fonction de police qui prévoient la transmission d'information à certaines autorités, organes, organismes et services ainsi que tout autre

andere ontvanger van politionele informatie bepaald in de bijzondere wetten, decreten en ordonnanties;

— de maatregelen ter bestrijding van de sociale fraude, waarvoor informatie moet worden gedeeld met overheden die persoonsgegevens verwerken in het kader van titel 1 of de Dienst voor Inschrijvingen van Voertuigen die informatie van de politiediensten ontvangt en deze meedeelt aan de organismen die verantwoordelijk zijn voor de autokeuring;

— of ook artikel 81, § 1, van de wet van 18 september 2017 die voorziet immers dat wanneer de CFI meldingen van vermoedens analyseert, zij alle bijkomende inlichtingen die zij nuttig acht voor de vervulling van haar opdracht mag opvragen, in het bijzonder bij de onderworpen entiteiten, hun toezichtautoriteiten, de administratieve diensten van de Staat, de openbare centra voor maatschappelijk welzijn, de curatoren in een faillissement of de voorlopige bewindvoerders. In dat geval vindt er dus een transfer van gegevens van persoonlijke aard plaats tussen de CFI, opgenomen in titel 2 van de huidige wet en de personen en entiteiten opgenomen in titel 1 van de huidige wet.

Aangezien laatstgenoemden niet allemaal tot de overheid behoren zoals bepaald in artikel 5 van deze wet, is het noodzakelijk om een ruime definitie op te nemen waardoor de informatie die afkomstig is van de organen bedoeld in paragraaf 1 ook beschermd wordt wanneer ze verwerkt wordt door een privéorgaan.

In overeenstemming met punt 2 van artikel 23 van de Verordening moeten de wettelijke en reglementaire teksten over de mededeling van gegevens aan deze ontvangers alle vereiste specifieke bepalingen bevatten.

Een minimum is evenwel bepaald in de wet. Ze moeten immers in de eerste plaats de gepaste technische of organisatorische maatregelen nemen om ervoor te zorgen dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt zijn tot hetgeen de personen nodig hebben om hun functies uit te oefenen of tot hetgeen nodig is voor de behoeften van de dienst. Vervolgens moeten ze de gepaste technische en organisatorische maatregelen nemen om de persoonsgegevens te beschermen tegen toevallige of niet-toegestane vernietiging, tegen toevallig verlies en tegen wijziging of elke andere niet-toegestane verwerking van die gegevens. Tot slot zijn de leden van de overheden, organen of instellingen die de gegevens bedoeld in de eerste paragraaf verwerken, bovendien gebonden door de discretieplicht.

Het spreekt bijgevolg voor zich dat een geadresseerde zich niet op die bepaling zal kunnen beroepen

récipiendaire d'informations policières identifiés dans des lois particulières, décrets et ordonnances;

— les dispositions visant à lutter contre la fraude sociale qui requièrent un partage d'information avec des autorités traitant des données à caractère personnel dans le cadre du titre 1er ou encore la Direction de l'immatriculation des véhicules qui reçoit des informations des services de police et qui les communique aux organismes en charge du contrôle technique;

— ou encore l'article 81, § 1er, , de la loi du 18 septembre 2017 qui prévoit en effet que lorsqu'elle analyse les déclarations de soupçon, la CTIF peut requérir tous les renseignements complémentaires qu'elle juge utile à l'accomplissement de sa mission, notamment auprès des entités assujetties, de leurs autorités de contrôle, des services administratifs de l'État, des centres publics d'action sociale, des curateurs de faillite ou des administrateurs provisoires. Il s'opère donc, dans ce cas, un transfert de données à caractère personnel entre la CTIF, visée au titre 2 de la présente loi, et des personnes et entités visées au titre 1er de la présente loi.

Ces récipiendaires ne relevant pas tous de l'autorité publique telle que définie à l'article 5 de la présente loi, il est nécessaire de reprendre une définition large permettant également de protéger l'information provenant des organes visés au paragraphe premier lorsqu'elle est traitée par un organisme privé.

Conformément au point 2 de l'article 23 du Règlement, les textes légaux et réglementaires concernant la communication de données vers ces récipiendaires devront contenir toutes les dispositions spécifiques requises.

Un minimum est cependant prévus dans la loi. En effet, ils devront tout d'abord adopter des mesures techniques ou organisationnelles appropriées pour assurer que l'accès aux données et les possibilités de traitement soient limités à ce dont les personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service. Ils devront ensuite adopter des mesures techniques ainsi que les mesures organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données. Enfin, les membres des autorités publiques, organes ou organismes qui traitent les données visées au paragraphe premier sont en outre tenus au devoir de discrétion.

Il est dès lors évident qu'un récipiendaire ne pourra se prévaloir de cette disposition pour recourir au profilage

om over te gaan tot profilering zonder de bepalingen van artikel 22 van de Verordening in acht te nemen.

De toepassing van dezelfde beperkingen op de logbestanden van de door in paragraaf 1 bedoelde organen uitgevoerde verwerkingen in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in titel 1 is vooral bedoeld om ervoor te zorgen dat de informatie volgens dewelke deze organen een administratieve gegevensbank hebben geraadpleegd voor onderzoek of bescherming tegen de gevaren van de openbare veiligheid, zoals het Rijksregister van de natuurlijke personen, niet aan de betrokken persoon kan worden meegedeeld.

De wettelijke en reglementaire teksten moeten beantwoorden aan de voorschriften van artikel 23.2 van de Verordening. Dat is al het geval voor talrijke teksten. We illustreren dit met de gegevens die doorgegeven worden door de politiediensten.

De koninklijke besluiten ter uitvoering van de artikelen 44/1 tot 44/11/13 van de wet van 5 augustus 1992 op het politieambt zijn op de dag van de goedkeuring van onderhavige wet: het koninklijk besluit van 14 maart 2006 tot uitvoering van artikel 44/11/11 van de wet van 5 augustus 1992 op het politieambt met het oog op de doorzending van bepaalde gegevens aan bpost en houdende de administratieve behandeling van de onmiddellijk inningen, de drie koninklijke besluiten van 30 oktober 2015 betreffende de rechtstreekse toegang van het Controleorgaan tot de gegevens en de informatie van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt, de rechtstreekse toegang van het Vast Comité van toezicht op de politiediensten en van de Dienst Enquêtes ervan tot de gegevens en de informatie van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt en de rechtstreekse toegang van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten en de Dienst Enquêtes ervan tot de gegevens en de informatie van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt, het koninklijk besluit van 28 april 2016 betreffende de rechtstreekse bevraging van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt door de aangewezen personeelsleden van de Dienst Vreemdelingenzaken en het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Foreign Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling 1*bis* "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt.

Die bepaling heeft echter geen betrekking op het koninklijk besluit van 30 oktober 2015 betreffende

sans respecter les dispositions de l'article 22 du Règlement.

L'application des mêmes limitations à la journalisation des traitements effectués par les organes visés au paragraphe premier dans les banques de données des responsables du traitement visés au titre 1er est essentiellement destinée à faire en sorte que l'information selon laquelle ces organes ont consulté une banque de données administrative à des fins d'enquête ou de protection contre la menace pour la sécurité publique, telle que par exemple le Registre national des personnes physiques, ne puisse être communiquée à la personne concernée.

Les textes légaux et réglementaires devront répondre aux prescrits de l'article 23.2 du Règlement. C'est déjà la cas pour de nombreux textes. Illustrons ce propos avec les données transmises par les services de police.

Les arrêtés royaux pris en exécution des articles 44/1 à 44/11/13 du 5 août 1992 sur la fonction de police sont, au jour de l'adoption de la présente loi, l'arrêté royal du 14 mars 2006 portant exécution de l'article 44/11/11 de la loi du 5 août 1992 sur la fonction de police dans le cadre de la transmission de certaines données à bpost en vue du traitement administratif des perceptions immédiates, les trois arrêtés royaux du 30 octobre 2015 respectivement relatif à l'accès direct de l'Organe de contrôle aux données et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police et relatif à l'accès direct du Comité permanent de contrôle des services de police et de son Service d'enquêtes aux données et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police et relatif à l'accès direct du Comité permanent de contrôle des services de renseignement et de sécurité et de son Service d'enquêtes aux données et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police, l'arrêté royal du 28 avril 2016 relatif à l'interrogation directe de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police par les membres du personnel désignés de l'Office des étrangers et l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters et portant exécution de certaines dispositions de la section 1er*bis* "de la gestion des informations" du chapitre IV de la loi sur la fonction de police.

L'arrêté royal du 30 octobre 2015 relatif aux conditions afférentes à la communication des données à caractère

de voorwaarden verbonden aan de mededeling van persoonsgegevens en informatie door de Belgische politiediensten aan de leden van Interpol en Interpol.

Elk verzoek dat betrekking heeft op de uitoefening van de in de artikelen 12 tot 22 en 34 van de Verordening vastgelegde rechten betreffende politiegegevens en dat aan een geadresseerde wordt gericht, wordt zo snel mogelijk en in elk geval binnen een maand na de ontvangst van het verzoek aan de Gegevensbeschermingsautoriteit bezorgd. Zij is als enige bevoegd om een antwoord aan de betrokken persoon te geven.

Als laatstgenoemde rechtstreeks gevat wordt door de verwerkingsverantwoordelijke van titel 1 (de geadresseerde), zal ze vanzelfsprekend niets meedelen aan de betrokken persoon maar zal ze de nodige verificaties verrichten. Als ze daarentegen gevat wordt door de betrokken persoon, zal ze volgens de geldende wettelijke bepalingen antwoorden. Aangezien een ad hoc controleautoriteit opgericht is voor de politiediensten en de gerechtelijke overheid, zal de gegevensbeschermingsautoriteit het verzoek tot verificatie van de verwerkingsverantwoordelijke of de betrokken persoon aan deze autoriteit doorgeven. Het uiteindelijke antwoord aan de betrokken persoon zal echter steeds via de Gegevensbeschermingsautoriteit worden bezorgd.

Art. 15

Dit artikel bepaalt de verplichtingen van de verwerkingsverantwoordelijke wanneer de Passagiersinformatie-eenheid persoonsgegevens verwerkt.

Omwille van evidente redenen van veiligheid en discretie hebt de verwerkingsverantwoordelijke het verbod om de betrokkene te informeren dat hij beschikt over dergelijke gegevens.

Paragraaf 2 voorziet een uitzondering: wanneer de verwerkingsverantwoordelijke wettelijk ertoe gehouden is om alle gegevens, die hij ter beschikking heeft, over te maken.

Deze uitzondering op de verplichtingen van de verwerkingsverantwoordelijke bedoeld in de artikelen 12 tot 22 en 34 van de Verordening en aan de verplichting van transparantie bedoeld in punt 1.a) van artikel 5 van de Verordening is toegestaan door artikel 23 van voormelde Verordening indien zij binnen een democratische samenleving een noodzakelijke en proportionele maatregel vormt voor de garantie van de nationale veiligheid te garanderen en voor de garantie van het voorkomen en het opsporen van strafbare feiten alsook

personnel et des informations des services de police belges aux membres d'Interpol et à Interpol n'est en revanche pas visé par cette disposition.

Toute demande portant sur l'exercice des droits visés aux articles 12 à 22 et 34 du Règlement, concernant des données policières, adressée à un destinataire de ces données est transmise, par ce dernier, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, à l'Autorité de protection des données, seule habilitée à adresser une réponse à la personne concernée.

Si cette dernière est saisie directement par le responsable du traitement du titre 1er (le destinataire), elle ne communiquera bien entendu rien à la personne concernée mais opèrera les vérifications nécessaires. Si par contre, elle est saisie par la personne concernée, elle répondra selon les dispositions légales en vigueur. Comme une autorité de contrôle ad hoc est instituée pour les services de police et l'autorité judiciaire, l'autorité de protection des données lui transmettra la demande de vérification émanant du responsable du traitement ou de la personne concernée. La réponse finale vers la personne concernée sera cependant toujours transmise via l'Autorité de protection des données.

Art. 15

Cet article détermine les obligations du responsable du traitement lorsque l'Unité d'information des passagers traite de données à caractère personnel.

Pour des raisons évidentes de sécurité et de discrétion, le responsable du traitement a l'interdiction d'informer la personne concernée qu'il dispose de telles données.

Une exception est prévue par le paragraphe 2: lorsque le responsable du traitement est légalement tenu de transmettre toutes les données à sa disposition.

Cette exception aux obligations du responsable du traitement visées aux articles 12 à 22 et 34 du Règlement et à l'obligation de transparence visée au point 1.a) de l'article 5 du Règlement est autorisée par l'article 23 dudit Règlement si elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité nationale, et pour garantir la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection

het onderzoeken en het vervolgen in het kader van de uitvoering van strafsancties, daarin begrepen de bescherming tegen de bedreigingen voor de openbare veiligheid en het voorkomen van dergelijke bedreigingen.

Er bestaat geen twijfel dat het een noodzakelijke maatregel betreft voor de garantie van het voorkomen en het opsporen van strafbare feiten alsook het onderzoeken en het vervolgen in het kader van de uitvoering van strafsancties. De passagiersgegevens worden in feite verwerkt met als doel het onderzoeken en vervolgen van de inbreuken opgesomd in artikel 8 van de wet van 25 december 2016. Het moet ten alle koste vermeden worden dat de betrokkenen hiervan verwittigd worden.

Met het oog op de opdrachten in de artikelen 7 en 11 van de wet van 30 november 1998 en waarvoor de passagiersgegevens verwerkt kunnen worden door de PIE, is er geen twijfel dat dit een maatregel betreft voor de garantie van de openbare veiligheid. Om te strijden tegen alle bedreigingen ten aanzien van de Belgische Staat en diens burgers, worden inlichtingenonderzoeken uitgevoerd teneinde de bedreigingen en hun auteurs te identificeren. Er moet ten alle koste vermeden worden dat deze laatsten geïnformeerd worden dat zij geïdentificeerd werden. Teneinde de efficiëntie en de discretie van de inlichtingenonderzoeken te verzekeren, is de uitzondering voorzien in huidig artikel noodzakelijk en proportioneel.

Teneinde te vermijden dat de verwerkingsverantwoordelijke de betrokkene alarmeert, specifieert paragraaf 3 van huidig artikel dat de verwerkingsverantwoordelijke geen enkele vermelding mag maken die een indicatie kan geven aangaande het feit dat deze over dergelijke gegevens zou beschikken.

Paragraaf 4, die dezelfde beperkingen toepast voor wat betreft de oplijsting van de uitgevoerde verwerkingen door de PIE binnen de gegevensbanken van de verwerkingsverantwoordelijke bedoeld in deze titel, is er voornamelijk op gericht om ervoor te zorgen dat de informatie, volgens dewelke de PIE een administratieve gegevensbank heeft geraadpleegd, zoals bijvoorbeeld het Rijksregister van de natuurlijke personen, niet gecommuniceerd zou kunnen worden aan betrokkene.

Art. 16

Indien de persoonsgegevens in het kader van een strafrechtelijk onderzoek en een strafrechtelijke procedure worden verwerkt, wordt erin voorzien dat het recht op informatie, inzage en op rectificatie of wissing van persoonsgegevens en op verwerkingsbeperking overeenkomstig het nationaal procesrecht wordt

contre les menaces pour la sécurité publique et la prévention de telles menaces.

Il ne fait aucun doute qu'il s'agit d'une mesure nécessaire pour garantir la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales. En effet, les données des passagers sont traitées aux fins de recherche et poursuite d'infractions énumérées à l'article 8 de la loi du 25 décembre 2016, et il faut éviter à tout prix que les personnes concernées en soient averties.

Au vu des missions fixées aux articles 7 et 11 de la loi du 30 novembre 1998, et pour lesquelles des données des passagers peuvent être traitées par l'UIP, il ne fait aucun doute qu'il s'agit d'une mesure nécessaire pour garantir notamment la sécurité nationale. En effet, pour lutter contre toutes les menaces envers l'État belge et ses citoyens, des enquêtes de renseignement sont effectuées afin d'identifier les menaces et leurs auteurs. Il faut à tout prix éviter que ces derniers soient informés qu'ils ont été "repérés". Pour assurer l'efficacité et la discrétion des enquêtes de renseignement, l'exception prévue dans le présent article est nécessaire et proportionnée.

Pour éviter que le responsable du traitement ne mette la puce à l'oreille de la personne concernée, le paragraphe 3 du présent article précise que le responsable du traitement ne peut faire aucune mention qui serait susceptible de donner une indication sur le fait qu'il disposerait de telles données.

Le paragraphe 4, appliquant les mêmes limitations à la journalisation des traitements effectués par l'UIP dans les banques de données des responsables du traitement visés dans ce titre est essentiellement destiné à faire en sorte que l'information selon laquelle l'UIP a consulté une banque de données administrative, comme par exemple le Registre national des personnes physiques, ne puisse être communiquée à la personne concernée.

Art. 16

Lorsque les données à caractère personnel sont traitées dans le cadre d'une enquête pénale ou d'une procédure judiciaire en matière pénale, il est prévu que le droit à l'information, le droit d'accès aux données à caractère personnel, de rectification ou d'effacement de celles-ci, et le droit de limitation du traitement sont

uitgeoefend. Voor het overige wordt verwezen naar de toelichtingen bij de bepalingen betreffende de vordering tot staking (artikel 209 ev).

Art. 17

Dit artikel voorzag in de toepassing van de rechten van personen die betrokken zijn bij een gemeenschappelijke behandeling van hun persoonsgegevens, rechtstreeks of onrechtstreeks afkomstig van ten minste één bevoegde autoriteit van titel 2 of ten minste één autoriteit bedoeld in titel 3. De Privacycommissie vraagt zich af, in punt 144 van haar advies, welke de meerwaarde is van deze bepaling en welke de verhouding is tot de andere voorziene afwijkingen, zoals deze in artikel 12. In de afwijking van de rechten van de betrokkene voorzien in artikel 12 betreft het enkel het beschermen van gegevens die aangeleverd werden door autoriteiten bedoeld in titel 3 wanneer deze zich bevinden in een gegevensbank die behoort tot andere autoriteiten die onderworpen zijn aan titel 1. Daar waar dit artikel verschilt van het artikel 12 is dat het tot doel heeft te voorkomen dat de autoriteit die onderworpen is aan titel 1 zijn verwerking in de gezamenlijke gegevensbank moet onthullen aan de betrokkene en, tegelijkertijd, het bestaan van een verwerking door de autoriteiten bedoeld in titel 2 of 3.

Ter illustratie kunnen we de terrorist fighters aanhalen die het voorwerp uitmaken van een gemeenschappelijke verwerking van hun gegevens door autoriteiten onderworpen aan titel 1, alsook door autoriteiten onderworpen aan titel 2 en nog door andere bedoeld in titel 3. Naar gelang de omstandigheden is het niet altijd wenselijk dat de betrokkene op de hoogte wordt gesteld dat hij de aandacht heeft getrokken van de politie- of inlichtingendiensten. Huidig artikel heeft tot doel de autoriteiten onderworpen aan titel 1 en die deelnemen aan de gemeenschappelijke gegevensbank terrorist fighters te verbieden aan de betrokkene te onthullen dat de gegevens die het verwerkt in het kader van de eigen doeleinden ook worden verwerkt in de gemeenschappelijke gegevensbank terrorist fighters, en alzo ook een verwerking te onthullen door de politie- of inlichtingendiensten.

Deze uitzondering tast niet de rechten van de betrokkene aan ten opzichte van de verwerking van zijn gegevens door de autoriteit onderworpen aan titel 1 voor de eigen doeleinden. Deze autoriteit kan gewoonweg niet onthullen aan de betrokkene dat het deze gegevens gevoed heeft aan de gezamenlijke gegevensbank.

De Privacycommissie heeft desalniettemin gelijk te benadrukken dat het ontwerp van artikel 18 een

exercés conformément aux règles nationales relatives à la procédure judiciaire. Pour le surplus, il est renvoyé aux explications données pour les dispositions relatives à l'action en cessation (art. 209 et suivants).

Art. 17

Cet article prévoyait l'application des droits de personnes concernées par un traitement commun de leurs données à caractère personnel, émanant directement ou indirectement d'au moins une autorité compétente du titre 2 ou d'au moins une autorité du titre 3. La Commission vie privée s'interroge, dans le point 144 de son avis, sur la plus-value de cette disposition et sur son articulation avec les autres exceptions prévues, comme celle de l'article 12. Dans l'exception aux droits de la personne concernée prévue à l'article 12, il s'agit de protéger uniquement les données fournies par les autorités visées sous le titre 3 lorsqu'elles se trouvent dans une banque de données appartenant à d'autres autorités soumises au titre 1er. A la différence de l'exception prévue à l'article 12, cet article-ci tend à empêcher que l'autorité soumise au titre 1er ne dévoile son traitement dans la banque de données conjointe à la personne concernée et par la même occasion, l'existence d'un traitement des autorités visées au titre 2 ou 3.

A titre d'illustration, citons les terrorist fighters qui font l'objet d'un traitement commun de leurs données par des autorités soumises au titre 1er, ainsi que par des autorités visées au titre 2 et par d'autres encore visées au titre 3. En fonction des circonstances, il n'est pas toujours souhaitable que la personne concernée soit mise au courant qu'elle a attiré l'attention des services de police ou des services de renseignement. Le présent article vise à interdire à une autorité soumise au titre 1er, qui participe à la banque de données commune terrorist fighters, de révéler à la personne concernée que les données qu'elle traite à son égard dans le cadre de ses finalités propres, le sont aussi dans la banque de données communes terrorist fighters, dévoilant ainsi un traitement par les services de police ou par les services de renseignement.

Cette exception n'empiète pas sur les droits de la personne concernée à l'égard des données traitées par l'autorité soumise au titre 1er pour ses propres finalités. Cette autorité ne peut simplement pas dévoiler à la personne concernée qu'elle a fourni ces données à la banque de données conjointe.

Néanmoins, la Commission vie privée a raison de souligner que le projet d'article 18 avait un champ

toepassingsgebied had dat deels overlapte met dat van artikel 12. Daarom wordt vorig artikel 18 nieuw artike 17 ingekort en beperkt het zich nu tot een verbod voor autoriteiten van titel 1 om de betrokkene te informeren over het feit dat zijn gegevens werden meegedeeld aan een gezamenlijke gegevensbank.

De termen “gezamenlijke gegevensbank” worden verkozen boven de termen “gemeenschappelijke verwerkingen” om het toepassingsgebied van dit artikel te beperken en om verwarring te vermijden met de “gemeenschappelijke gegevensbanken” bedoeld in artikel 44/11/3*bis* wet op het politieambt.

Om te antwoorden op het verzoek van de Privacycommissie (punt 144 van haar advies) enerzijds en van de Raad van State (pagina 19 van het advies) anderzijds, werd een definitie van gezamenlijke gegevensbank toegevoegd aan het ontwerp. Er moet verduidelijkt worden dat de gemeenschappelijke gegevensbanken in de zin van artikel 44/11/3*bis* wet op het politieambt binnen de definitie van “gezamenlijke gegevensbank” vallen maar deze laatste definitie beperkt zich niet tot de eerste. Trouwens, het spreekt voor zich dat de gegevensbanken van het OCAD en de Passagiersinformatie-eenheid geen gezamenlijke gegevensbanken zijn omdat het niet een gemeenschappelijke oefening van meerdere autoriteiten betreft.

d’application qui recoupait partiellement celui de l’article 12. Dès lors, l’article anciennement 18, nouvellement 17, a été restreint et se limite maintenant à une interdiction pour une autorité du titre 1er d’informer la personne concernée que ses données ont été communiquées à une banque de données conjointe.

Les termes “banque de données conjointe” ont été préférés aux termes “traitements communs” pour restreindre le champ d’application du présent article et pour éviter une confusion avec les “banques de données communes” visées à l’article 44/11/3*bis* de la loi sur la fonction de police.

Pour répondre à la demande de la Commission vie privée (point 144 de son avis), d’une part, et du Conseil d’État (page 19 de son avis), d’autre part, une définition de “banque de données conjointe” a été ajoutée dans le projet. Il convient de préciser que les banques de données communes au sens de l’article 44/11/3*bis* de la loi sur la fonction de police entrent dans la définition de “banque de données conjointe” mais cette dernière définition ne se limite pas aux premières. Par ailleurs, il va de soi que les banques de données de l’OCAM et de l’Unité d’information des passagers ne sont pas des banques de données conjointes car il ne s’agit pas d’un exercice commun par plusieurs autorités.

HOOFDSTUK IV

Verwerkingsverantwoordelijke en verwerker

Afdeling 1

Algemene bepalingen

Art. 18

Dit artikel voert artikel 43 van de Verordening uit, dat de mogelijkheid biedt te kiezen welke instantie de certificeringsorganen accrediteert. Er is beslist dat die instantie de nationale accreditatie-instantie wordt die is aangewezen in overeenstemming met verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad, te weten BELAC, de Belgische accreditatie-instantie.

Afdeling 2

Publieke sector

Er wordt beslist om met de invoeging van deze afdeling de gegevensstromen afkomstig van de federale overheidsdiensten te vergemakkelijken en instrumenten

CHAPITRE IV

Responsable du traitement et sous-traitant

Section 1re

Dispositions générales

Art. 18

Cet article exécute l’article 43 du Règlement qui permet de choisir quel sera l’organisme qui accrédite les organismes de certification. Il est décidé que cet organisme sera l’organisme national d’accréditation désigné conformément au règlement (CE) no 765/2008 du Parlement européen et du Conseil , à savoir BELAC, l’organisme belge d’Accréditation.

Section 2

Secteur public

Il est décidé par l’insertion de cette section de faciliter les flux de données en provenance des administrations fédérales et de présenter des outils qui aideront

voor te stellen die de administratie moeten helpen haarde verplichtingen te vervullen, zowel voor de voorbereiding en de opmaak van de registers als voor de controle a posteriori en het opzoeken van informatie in geval van verzoeken van de betrokkene aan de verwerkingsverantwoordelijke of de verwerker.

Deze afdeling is enkel van toepassing op de federale overheid overeenkomstig de algemene definitie zoals voorzien in artikel 5.

Sommige van de bepalingen die volgen, leggen aanvullende verplichtingen op voor de verwerkingsverantwoordelijken van de federale publieke sector.

Zo bevatten de artikelen 20 e.v. maatregelen die de Verordening op adequate wijze aanvullen teneinde de verwerkingsverantwoordelijken van de federale publieke sector in een systeem te kunnen laten stappen waarin er geen onduidelijkheden meer kunnen zijn rond hun verantwoordelijkheid.

De twee voorwaarden die de wetgever zichzelf heeft opgelegd bij het opstellen van deze aanvullende maatregelen zijn enerzijds het respect voor de filosofie van de Verordening – namelijk het beginsel van de verantwoordelijkheid van iedere verwerkingsverantwoordelijke – en anderzijds het verschil in meerwaarde voor de gegevensbescherming. De wetgever is immers van mening dat de principes van de Verordening, op voorwaarde dat zij goed ten uitvoer worden gelegd, volstaan om de persoonsgegevens te beschermen. Het mag niet de bedoeling zijn om verplichtingen op te leggen die de uitwisseling van gegevens afremmen, wel integendeel. Het moet de bedoeling zijn om instrumenten aan te bieden die de tenuitvoerlegging vergemakkelijken; bijvoorbeeld door de doeltreffendheid van de gegevensuitwisselingen te verbeteren, door kennis te ontwikkelen en te delen, door de tenuitvoerleggingsmaatregelen te uniformeren, enz.

Art. 19

Deze afdeling is enkel van toepassing op de federale overheid overeenkomstig de algemene definitie zoals voorzien in artikel 5 en de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus die als een overheid worden beschouwd. Doorgeven van informatie tussen politie-entiteiten zullen daarom niet worden beschouwd als uitwisselingen tussen verschillende overheden.

l'administration à remplir ses obligations tant dans la préparation et la rédaction des registres, que dans le contrôle a posteriori et la recherche d'information lors de demandes par la personne concernée auprès du responsable du traitement ou du sous-traitant.

Cette section s'applique uniquement à l'autorité publique fédérale, conformément à la définition générale prévue à l'article 5.

Certaines des dispositions qui suivent posent des obligations supplémentaires pour les responsables du traitement du secteur public fédéral.

Ainsi, il est disposé dans les articles 20 et suivants des mesures qui complémentent adéquatement le Règlement afin d'offrir aux responsables du traitement du secteur public fédéral une transition vers un système où leur responsabilité ne peut plus souffrir de confusions.

Les deux conditions que le législateur s'est imposé pour rédiger ces mesures complémentaires sont d'une part le respect de la philosophie du Règlement – à savoir le principe de responsabilité et de chaque responsable du traitement – et d'autre part la plus-value différente de la protection des données. Le législateur estime en effet que les principes du Règlement sont suffisantes, lorsqu'elles sont bien mises en œuvre, pour protéger les données à caractère personnel. Il ne doit pas s'agir de créer des obligations qui freinent l'échange de données mais au contraire de proposer des outilsqui facilitent la mise en œuvre; par exemple en améliorant l'efficacité des échanges de données, en développant et en partageant des connaissances, en uniformisant les mesures de mise en œuvre…

Art. 19

Cette section s'applique uniquement à l'autorité publique fédérale, conformément à la définition générale prévue à l'article 5 et aux sevices de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police structuré à deux niveaux qui sont considérés comme une autorité intégrée. Les transferts d'information entre entités de police ne seront donc pas visés comme des échanges entre autorités publiques différentes.

Art. 20

In dat verband voorziet dit artikel erin dat protocollen moeten worden opgemaakt om de modaliteiten van de uitwisseling van gegevens, die zijn oorsprong in een wettelijke grondslag vindt, te formaliseren. Het hoofddoel daarvan is te waarborgen dat alle beveiligingsmaatregelen worden genomen bij die doorgiften.

Deze protocollen bieden de mogelijkheid te waarborgen dat de doorgegeven gegevens zullen worden verwerkt volgens de regels die zijn vastgelegd tussen de verwerkingsverantwoordelijken.

Deze protocollen zijn enkel bedoeld voor de doorgiften van gegevens door een federale overheid aan een andere overheid, of privéorgaan. Soortgelijke protocollen kunnen niet worden geëist door andere overheidsniveaus, ook niet voor stromen intern bij de politie opgenomen in de zin van artikel 2, 2°, van de wet van 7 december 1998 en evenmin noch voor stromen van en naar het buitenland. Hiertoe herinneren we opnieuw aan het eerste artikel, derde punt van de Verordening die stelt dat "*Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens*". Er kan echter opgemerkt worden dat Vlaamse regering eveneens van plan is dit type van protocol verplicht te maken.

Deze bepaling voldoet aan beide voormelde voorwaarden. Enerzijds respecteert zij de geest van de Verordening door de verwerkingsverantwoordelijken ertoe aan te zetten na te denken over de conformiteit van hun gegevensuitwisselingen en anderzijds biedt zij de mogelijkheid de uitwisseling van gegevens te verbeteren door de formalisering ervan. Hiertoe wordt een reeds elementen voorzien.

Wat betreft de categorie van ontvangers moet herhaald worden, zoals de Raad van State het aanhaalt in zijn advies, pagina 18, dat de inlichtingen- en veiligheidsdiensten en de autoriteiten bedoeld in ondertitel 3 van titel 3 geen ontvangers zijn in de zin van de definitie van de Verordening. De verwerking van deze gegevens door deze autoriteiten stemt in zekere mate overeen met de toepasselijke regels met betrekking tot de bescherming van gegevens in functie van de doeleinden van de verwerking. Bijgevolg worden de inlichtingen- en veiligheidsdiensten en de autoriteiten bedoeld in ondertitel 3 van titel 3 uitgesloten van de vermelding in het protocol. Trouwens, het derde punt heeft betrekking op de naam van de functionaris voor gegevensbescherming. In elk geval geniet de naam van de functionaris voor gegevensbescherming van de inlichtingendiensten, als

Art. 20

A ce titre, cet article prévoit que des protocoles doivent être rédigés pour formaliser les modalités de l'échange de données, qui trouve son origine dans une base légale. L'objectif étant principalement de garantir que toutes les mesures de sécurité sont prises lors de ces transferts.

Ces protocoles permettent de fixer des garanties selon lesquelles les données transférées seront traitées selon les règles qui ont été fixées entre les responsables du traitement.

Ces protocoles sont prévus uniquement pour les transferts de données à partir d'une autorité publique fédérale vers une autre autorité publique, ou organisme privé. Ces protocoles ne peuvent pas être exigés par d'autres niveaux de pouvoirs, non plus pour des flux interne à la police intégrée au sens de l'article 2, 2°, de la loi du 07 décembre 1998, et également pas pour des flux de et vers l'étranger. A cet égard, on rappelle à nouveau l'article premier troisième point du Règlement qui dispose que "*la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*". Toutefois, on peut noter que le gouvernement flamand compte également rendre obligatoire ce type de protocole.

Cette disposition répond aux deux conditions énumérées ci-avant. Elle respecte l'esprit du Règlement en invitant les responsables du traitement à s'interroger sur la conformité de leurs échanges de données d'une part, et d'autre part elle permet d'améliorer l'échange de données en les formalisant. A cet effet, une série d'éléments est prévue.

En ce qui concerne la catégorie de destinataires, il doit être répété, comme le remarque le Conseil d'État dans son avis, page 18, que les services de renseignement et de sécurité et les autorités visées au sous-titre 3 du titre 3 ne sont pas des destinataires, au sens de la définition du Règlement. Le traitement de ces données par ces autorités concorde de la sorte avec les règles applicables en matière de protection des données en fonction des finalités du traitement. Par conséquent, les services de renseignement et de sécurité et les autorités visées au sous-titre 3 du titre 3 sont exclus de la mention dans le protocole. Par ailleurs, le troisième point vise le nom du délégué à la protection des données. En tout état de cause, le nom du délégué à la protection des données des services de renseignement, en tant qu'agent de ces services, bénéficie d'une protection

agent van deze diensten, van een bijzondere bescherming in toepassing van de artikele, 36 en 43 van de organieke wet van 30 november 1998 betreffende de inlichtingen- en veiligheidsdiensten. Dit verantwoordt terdege en wettelijk het niet publiekelijk maken van deze informatie.

Onder wettelijke grondslag wordt begrepen elke nationale of *supra*nationale wettekst die een administratie kan opleggen om gegevens te verwerken om zijn missies te volbrengen in brede zin. Zo wordt wettelijke grondslag niet gedefinieerd als een tekst die specifiek een gegevensverwerking of -overdracht voorschrijft, maar algemener een wettelijke bepaling die niet anders kan verwezenlijkt worden dan door gegevens te verwerken. Evenzo, de doeleinde moet precies zijn. Daaronder moet worden verstaan een doel op zich en zich niet beperken tot de vermelding van "vervulling van wettelijke overheidsopdrachten".

In het belang van duidelijkheid en om de bezorgdheid van de Privacycommissie en de Raad van State te beantwoorden voorziet het punt 11 dat het protocol de bestaande wettelijke afwijkingen van de rechten van de betrokkenen oplijst. Het gaat zeker niet om het toekennen van bijkomende afwijkingen.

Wordt eveneens gesteld dat het protocol eventueel de sancties voorziet die van toepassing zijn in geval van niet naleven van dit protocol. Het gaat er hier om bijzondere sancties te voorzien tussen partners. Het is bijvoorbeeld te verwachten dat de autoriteit die de gegevens goorgift, de gegevens niet langer zal doorgeven.. Titel 6 blijft van toepassing voor de overtredingen op dit artikel.

De Raad van State en de Privacycommissie stellen ook voor om andere elementen in het protocol toe te voegen.

— de beschrijving van de precieze doeleinden waarvoor de gegevens oorspronkelijk werden ingezameld. De wetgever meent dat dit element niet zinvol is voor een gegevensstroom tussen autoriteiten aangezien er altijd een wettelijke basis nodig is;

— de vermelding van de verenigbaarheidsanalyse van de doeleinden in geval van verdere verwerking. De wetgever meent dat dit element in contradictie is met de vereiste van wettelijke grondslag en dus niet dient te worden toegevoegd;

— controle op de naleving van het beginsel "inzameling bij de authentieke gegevensbron". Deze vereiste is niet essentieel wanneer er een wettelijke grondslag bestaat en vloeit overigens niet voort uit de Verordening.

particulière en application des articles 36 et 43 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Ceci justifie pertinamment et légalement de ne pas rendre publique cette information.

Par base légale, il faut entendre tout texte de loi national ou *supra*national qui peut amener une administration à devoir traiter des données pour remplir ses missions au sens large. Ainsi, il ne faut pas entendre par base légale un texte qui prescrirait spécifiquement un traitement de données ou un transfert de données, mais plus généralement une disposition légale qui ne peut être réalisée autrement qu'en traitant des données. De même, la finalité doit être précise. Il faut entendre une fin en soi, et ne pas se limiter à la mention "exécution des missions légales de l'autorité publique".

Pour un souci de clarté et afin de répondre à la préoccupation de la Commission vie privée et du Conseil d'État, le point 11 prévoit que le protocole liste les dérogations légales aux droits des personnes concernées existantes. Il ne s'agit certainement pas d'accorder des dérogations supplémentaires.

Il est également stipulé que le protocole prévoit éventuellement des sanctions applicables en cas de non-respect de ce protocole. Il s'agit ici de prévoir des sanctions particulières entre les partenaires, par exemple, il peut être prévu que l'autorité qui transmet les données ne transmette plus les données. Le titre 6 reste applicable pour les violations à cet article.

Le Conseil d'État et la Commission vie privéeproposent également d'insérer d'autres éléments relevant du protocole:

— la description des finalités précises pour lesquelles les données ont été collectées à l'origine. Le législateur estime que cet élément n'a pas d'utilité pour un flux de données entre autorités, étant entendu qu'une base légale est toujours nécessaire;

— la mention de l'analyse de compatibilité des finalités en cas de traitement ultérieur. Le législateur estime que cet élément est en contradiction avec l'exigence de base légale et qu'il n'y a donc pas lieu de l'insérer;

— la vérification du respect du principe de "collecte auprès de la source authentique des données". Cette exigence n'est pas essentielle lorsqu'une base légale existe et de plus ne découle pas du Règlement.

Het laatste element kan worden ingevoegd, het heeft betrekking op alle specifieke maatregelen die de gegevensflux omkaderen conform het proportionaliteitsbeginsel en de vereisten inzake gegevensbescherming by design en default (keuze van het formaat van de mededeling, logging van de toegangen zodat men kan controleren wie wanneer toegang had tot welke gegevens en waarom, invoering van een verwijzingsrepertorium ingeval van automatische mededeling van de wijzigingen aan de gegevens om zich ervan te verzekeren dat enkel de noodzakelijke gegevens worden bijgewerkt en dit voor de nodige termijn, …).

De Raad van State en de Privacycommissie menen ook dat er een publiciteit moet voorzien worden voor het protocol. Teneinde het principe van de voorzienbaarheid van de wet na te leven wordt besloten een publiciteit te voorzien op de website van elk van de verwerkingsverantwoordelijken, hetgeen een brede visibiliteit moet toelaten.

De Raad van State (pagina 23 van het advies) meent eveneens dat de wet de situaties zou moeten voorzien in dewelke een protocol niet moet worden aangenomen. Dit is niet meer pertinent aangezien de regering beslist heeft het protocol verplicht te maken.

Zoals de Privacycommissie aanhaalt, aangezien de elektronische gegevensuitwisselingen verbonden aan E-government van nature niet beperkt zijn tot stromen tussen federale openbare of private instellingen zou een samenwerkingsakkoord nodig kunnen zijn om dit types van stromen te omkaderen.

Art. 21

Binnen de federale overheidmoet zonder uitzondering een functionaris voor gegevensbescherming worden aangewezen. De Verordening en de Richtlijn zijn op dit punt duidelijk en vereisen dit. Er wordt ook opgelegd dat een verwerker die voor de federale overheidgegevens verwerkt een functionaris voor gegevensbescherming aanwijst. Deze bepaling voorziet eveneens dat, wanneer de overheid beroep doet op een verwerker uit de privésector of persoonsgegevens doorgeeft aan een verantwoordelijke voor de verwerking uit de privésector, zij ook een functionaris voor gegevensbescherming dienen te hebben aangeduid als een van de minimale waarborgen. Het betreft een bijkomende bescherming die het advies van de Privacycommissie niet voorziet. Rekening houdend met de opmerkingen van de Privacycommissie wordt wel een zekere flexibiliteit toegevoegd aan deze voorwaarde. De verantwoordelijke voor de verwerking of de verwerker dient namelijk enkel een functionaris voor gegevensbescherming aan te duiden wanneer

Le dernier élément peut être inséré lequel concerne les mesures spécifiques encadrant le flux conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut (choix du format de la communication, journalisation des accès de manière telle que l'on puisse savoir qu a eu accès à quoi quand et pourquoi, mise en place d'un répertoire de références en cas de communication automatique des actualisations des données afin d'assurer que seules les données nécessaires soient actualisées et pour la durée nécessaire, ...).

Le Conseil d'État et la Commission vie privée estiment également qu'une publicité du protocole doit être organisée. Afin de rencontrer le principe de prévisibilité de la loi il est décidé de prévoir une publicité sur le site internet de chacun des responsables du traitement ce qui permettra une visibilité large.

Le Conseil d'État estime également que la loi devrait prévoir les situations dans lesquelles un protocole n'est pas adopté. Ceci n'est plus pertinent puisque le gouvernement a décidé de rendre le protocole obligatoire.

Comme l'indique la Commission vie privée, dans la mesure où les échanges électroniques de données liés à l'e-government ne sont par nature pas limités aux flux entre les organismes fédéraux publics ou privés, un accord de coopération pourrait être nécessaire afin d'encadrer ce type de flux.

Art. 21

Un délégué à la protection des données doit être désigné dans les autorités publiques fédérales, et ici il n'y a pas d'exception possible. Le Règlement et la Directive sont claires et exigeants sur ce point. Il est également exigé qu'un sous-traitant qui traite des données pour le compte de ces autorités publiques fédérales désigne obligatoirement un délégué à la protection des données. Cette disposition prévoit également que lorsque l'autorité publique fait appel à un sous-traitant du secteur privé ou transmet des données à un responsable du traitement du secteur privé, il doit également avoir désigné un délégué à la protection des données comme étant l'une des garantie minimale. Il s'agit d'une protection supplémentaire que n'entrevoit pas l'avis de la Commission vie privée. Compte tenu des remarques de la Commissie vie privée, une certaine flexibilité est apportée à cette condition. En effet, ce responsable du traitement ou sous-traitant doit désigner un délégué à la protection des données uniquement lorsque suite à une

volgende op een gegevensbeschermingseffectbeoordeling blijkt dat het een verwerking betreft die een hoog risico inhoudt voor de betrokkenen.

Een functionaris voor gegevensbescherming heeft een strengere en ruimere rol dan de veiligheidsadviseur. Hij is voor gegevensbescherming de referentiepersoon voor de verwerkingsverantwoordelijke en is tevens het contactpunt voor het publiek, of dat nu de burger is of de bevoegde toezichthoudende autoriteit.

Dit ontwerp van wet wil de nadruk leggen op de belangrijke rol van de functionaris voor gegevensbescherming, die ook een belangrijke speler zal zijn bij de effectbeoordelingen die zullen moeten worden verricht vóór elk ontwerp van wet en vóór de uitvoering van elke gegevensverwerking.

De Verordening, net als de Richtlijn, benadrukken dat de verwerkingsverantwoordelijke en de verwerker de functionaris voor gegevensbescherming moeten ondersteunen bij de vervulling van de taken bedoeld in artikel 39 van de Verordening, en in artikel 34 van de Richtlijn, door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid. De functionaris voor gegevensbescherming mag geen instructies ontvangen met betrekking tot de uitvoering van zijn taken en mag door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft worden voor de uitvoering van zijn taken. De functionaris voor gegevensbescherming brengt daarom rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker. Bij de aanwijzing van de functionaris voor gegevensbescherming zou dan ook rekening moeten worden gehouden met zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de hem toegewezen taken te vervullen. De verwerkingsverantwoordelijke en de verwerker zouden dus alles in het werk moeten stellen en organisatorische maatregelen moeten nemen teneinde het wezen van de Verordening en de Richtlijn te kunnen respecteren.

Zij zouden onder andere een voorbeeld kunnen nemen aan Verordening 45/2001 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, dat erin voorziet dat de functionaris benoemd wordt voor een termijn van ten minste twee jaar en ten

analyse d'impact relative à la protection des données il s'avère qu'il s'agit d'un traitement à risque élevé pour les personnes concernées.

Un délégué à la protection des données a un rôle plus contraignant et plus large que le conseiller en sécurité. Il est la personne ressource pour le responsable du traitement en matière de protection des données et également le point de contact pour le public, que ce soit le citoyen ou l'autorité de protection des données compétente.

Ce projet de loi souhaite mettre l'accent sur le rôle crucial de ce délégué à la protection des données qui sera également un acteur majeur lors des analyses d'impact qui devront être effectuées avant chaque projet de loi et avant la mise en œuvre de chaque traitement des données.

Le Règlement, ainsi que la Directive, insistent pour que le responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 39 du Règlement, et 34 de la Directive, en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées. Le délégué à la protection des données ne peut recevoir aucune instruction en ce qui concerne l'exercice de ses missions, et ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. A ce titre, le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant. La désignation du délégué à la protection des données devrait donc tenir compte des qualités professionnelles et en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions qui lui sont attribuées. Le responsable du traitement et le sous-traitant devraient donc mettre tout en œuvre et instaurer des mesures organisationnelles qui permettent de respecter l'essence du Règlement et de la Directive.

Il pourrait par exemple prendre l'exemple du Règlement 45/2001 du parlement européen et du conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, lequel prévoit que le délégué à la protection des données est nommé pour une période de deux à

hoogste vijf jaar. Hij kan worden herbenoemd, maar de totale duur van zijn mandaat mag niet meer dan tien jaar bedragen.

Art. 22

Er wordt voorzien dat de verwerkingsverantwoordelijke het advies van de functionaris voor gegevensbescherming verzoekt alvorens de verwerking uit te voeren overeenkomstig de risicobenadering. In geval van een negatief advies van de functionaris voor gegevensbescherming of wanneer aanbevelingen niet gevolgd zouden zijn, door de verwerkingsverantwoordelijke of de verwerker, die niet door dat advies gebonden zijn, dienen zij alsnog hun beslissing om de verwerking ten uitvoer te brengen te motiveren. Deze bepaling laat ook toe de vrijheid van de verwerkingsverantwoordelijke en de verwerker te vrijwaren om het advies en de aanbevelingen van de functionaris voor gegevensbescherming al dan niet op te volgen.

Ook de effectbeoordeling bedoeld in artikel 35 van de Verordening moet verplicht voor advies worden voorgelegd aan de functionaris voor gegevensbescherming, ofwel bij de uitwerking van het juridisch instrument dat in de verwerking voorziet, ofwel bij het ten uitvoer brengen van de verwerking.

Art. 23

Het is de bedoeling dat vóór de uitvoering van de verwerkingsactiviteit een gegevensbeschermingseffectbeoordeling wordt uitgevoerd, ook al werd reeds een effectbeoordeling uitgevoerd bij de opstelling van de wet of de reglementering die haar uitvoert teneinde te zorgen voor een efficiënte en tijdige analyse wanneer alle elementen onder de aandacht van de verwerkingsverantwoordelijke worden gebracht.

Alle elementen van de impactanalyse worden voorzien in artikel 35 van Verordening. De analyse moet op zijn minst een systematische beschrijving van de verwerkingshandelingen bevatten, evenals de doeleinden, met desgevallend inbegrip van het nagestreefde rechtmatig belang, een beoordeling van de noodzaak en de proportionaliteit van de verwerkingshandelingen tegenover de doeleinden, een risicobeoordeling voor de rechten en vrijheden van de betrokken personen, de beoogde maatregelen om tegemoet te komen aan die risico's, met inbegrip van de garanties, maatregelen en mechanismen voor de veiligheid met het oog op het verzekeren van de bescherming van de persoonsgegevens en om het bewijs van naleving van de Verordening te leveren, rekening houdend met de rechten en

cinq ans. Son mandat pourra être renouvelé, la durée totale du mandat ne pouvant toutefois dépasser dix ans.

Art. 22

Il est prévu que le responsable du traitement sollicite l'avis du délégué à la protection des données avant la mise en œuvre du traitement conformément à l'approche par le risque. En cas d'avis négatif du délégué à la protection des données, ou de recommandations qui ne seraient pas suivies par le responsable du traitement ou le sous-traitant, ce dernier n'étant pas tenu par cet avis, devra néanmoins motiver sa décision de mettre en œuvre le traitement. Cette disposition permet de maintenir également la liberté du responsable du traitement et du sous-traitant de suivre ou ne pas suivre les avis et recommandations du délégué à la protection des données.

De même, l'analyse d'impact visé à l'article 35 du Règlement devra obligatoirement recevoir l'avis du délégué à la protection des données, que ce soit lors de l'élaboration de l'instrument juridique qui le prévoit, ou lors de la mise en œuvre de ce traitement.

Art. 23

Il est prévu qu'une analyse d'impact relative à la protection des données doit être effectuée avant la mise en œuvre de l'activité de traitement, et ce même si une analyse d'impact a déjà été menée lors de l'élaboration de la loi ou de la réglementation qui la met en place afin d'assurer une analyse efficace et ponctuelle lorsque tous les éléments sont portés à la connaissance du responsable du traitement.

Tous les éléments de l'analyse d'impact sont prévus dans l'article 35 du Règlement. L'analyse doit contenir au moins une description systématique des opérations de traitement, les finalités, y compris le cas échéant, l'intérêt légitime poursuivi, une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du Règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. Lors de l'élaboration de la base

rechtmatige belangen van de betrokken personen en de andere getroffen personen. Bij de uitwerking van de rechtsgrondslag is het vaak moeilijk om in detail te weten welke praktische en technische veiligheidsmaatregelen en -mechanismen het best beantwoorden op de gedetecteerde risico's in de analyse. Ook bij het opstellen van de verwerking kan het voorkomen dat de opgestelde maatregelen en mechanismen bijkomende risico's met zich meebrengen waarbij geen rekening gehouden werd in de eerste analyse.

légale, il est souvent difficile de voir dans les détails quels seront les mesures et mécanismes de sécurité pratiques et techniques qui seront les plus à mêmes de répondre aux risques décelés dans l'analyse. De même, lors de la mise en place du traitement, il peut s'avérer que les mesures et mécanismes mis en place génèrent des risques supplémentaires qui n'avaient pas été pris en compte lors de la première analyse.

HOOFDSTUK V

CHAPITRE V

Verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen

Traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire

Art. 24

Art. 24

Artikel 85 van de Verordening stelt dat "*De lidstaten brengen het recht op bescherming van persoonsgegevens overeenkomstig deze verordening wettelijk in overeenstemming met het recht op vrijheid van meningsuiting en van informatie, daaronder begrepen de verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen*" waarvan de verwerking ten behoeven van academische, artistieke of literaire uitdrukkingsvormen deel uitmaken.

L'article 85 du Règlement dispose que "*les États membres doivent concilier par la loi le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, y compris les traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire."* dont le traitement à des fins d'expression universitaire, artistique ou littéraire fait partie.

Artikel 85, § 2, van de Verordening gaat in het bijzonder door op de doeleinden bedoeld in de eerste paragraaf en bepaalt het volgende: *"Voor verwerking voor journalistieke doeleinden of ten behoeve van academische, artistieke of literaire uitdrukkingsvormen stellen de lidstaten uitzonderingen of afwijkingen vast* […]".

L'article 85, § 2, du Règlement continue spécifiquement sur les finalités visées dans le paragraphe premier et dispose que "*Dans le cadre du traitement réalisé à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, les États membres prévoient des exemptions ou des dérogations* […].".

De Raad van State lijkt aan te geven dat dit artikel het artikel 85 in zijn geheel zou moeten uitvoeren en dus een draagwijdte zou moeten hebben die veel ruimer is dan de verwerkingen voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen. Maar dat is niet het opzet van deze wet en de Verordening vereist ook niet in zijn artikel 85 § 1 een specifieke uitvoering door middel van een welbepaalde wet die tot doel zou hebben de verhouding te regelen tussen de vrijheid van meningsuiting en de bescherming van de persoonsgegevens. Er wordt eerder algemeen aan de wetgever gevraagd te waken over de verzoening van deze verhouding in elke reglementering die zou kunnen raken aan dit delicate evenwicht.

Le Conseil d'État semble indiquer que cet article devrait mettre en oeuvre l'article 85 dans son entièreté et devrait donc avoir une portée plus large que les traitements à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire. Or, ce n'est pas le but du présent projet de loi et le Règlement n'exige non plus dans son article 85 § 1er une mise en oeuvre spécifique par le biais d'une loi déterminée qui aurait pour objet de régler la relation entre la liberté d'expression et la protection des données à caractère personnel. Il est plutôt demandé au législateur de façon générale de veiller à la conciliation de cette relation dans toute règlementation qui pourrait toucher à cette équilibre délicate.

Definitie

De Verordening geeft geen definitie van verwerkingen voor journalistieke doeleinden.

Deze wet definieert de verwerking voor journalistieke doeleinden als "*de voorbereiding, het verzamelen, opstellen, voortbrengen, verspreiden of archiveren ten behoeve van het informeren van het publiek, met behulp van elke media en waarbij de verwerkingsverantwoordelijke zich de naleving van journalistieke deontologische regels tot taak stelt.*".

De Raad voor de Journalistiek heeft op 16 oktober 2013 de deontologische code voor de journalistiek goedgekeurd waarin de doeleinden van de journalistieke verwerking gedefinieerd worden als zijnde "*De plicht om het publiek te informeren over aangelegenheden van algemeen belang".*

De informatie van algemeen belang is "een informatie die één of meer kwesties oproept voor het leven in de samenleving als geheel of voor één van haar componenten*"*.

Wat betreft de notie van informatie van algemeen belang meent de Raad van State *Volgens een vaste rechtspraak van het Europees Hof voor de Rechten van de Mens is de toegenomen bescherming inzake de vrijheid van meningsuiting die aan journalisten is toegekend gerechtvaardigd gezien hun rol van "waakhond" van de democratie die ze in hoofdzaak vervullen wanneer zij verslag uitbrengen over onderwerpen van algemeen belang of wanneer zij bijdragen tot een openbaar debat over een kwestie van algemeen belang. Daaruit vloeit echter niet voort dat alleen de verwerking van gegevens die op zich reeds "van algemeen belang" zouden zijn, deel uitmaakt van de journalistieke activiteit.* De Raad van State verzoekt dit artikel te herzien in het licht van de overweging 153 van de Verordening teneinde een brede interpretatie te weerhouden van de noties verbonden aan deze vrijheden, zoals de journalistiek.

Op dit punt heeft de regering de definitie voorzien in dit artikel dus gewijzigd om tegemoet te komen aan de opmerkingen van de Raad van State.

In verband met het begrip van media, meent de rechtspraak betreffende artikel 25 van de Grondwet waarin de persvrijheid verzekerd wordt, dat de pers zich niet beperkt tot de geschreven pers, maar "*dat een evolutionaire interpretatie moet worden gegeven aan de notie van de pers en (...) dat een telecommunicatiemiddel zoals het internet waarschijnlijk ook een pers in de zin van de Grondwet zal vormen"* (Cass, 6 mars 2012, P. 11 1374 N*).*

Définition

Le Règlement ne donne pas de définition des traitements à des fins de journalisme.

La présente loi définit le traitement à des fins journalistiques comme *"la préparation, la collecte, la rédaction, la production , la diffusion ou l'archivage à des fins d'informer le public, par le biais de tout média et dont le responsable du traitement s'impose des règles de déontologie journalistique*.

Le conseil de déontologie journalistique a adopté le 16 octobre 2013 le code de déontologie des journalistes qui définit la finalité du traitement journalistique comme étant "*le devoir d'informer le public des sujets d'intérêt général".*

L'information d'intérêt général est "*une information qui évoque un ou plusieurs enjeux pour la vie en société dans son ensemble ou pour une de ses composantes"*.

Concernant la notion d'information d'intérêt général, l'avis du Conseil d'État dispose que "*selon une jurisprudence constante de la Cour européenne des Droits de l'homme, la protection accrue en matière de liberté d'expresssion reconnue aux journalistes se justifie en raison de leur rôle de "chien de garde" de la démocratcie qui s'exprime essentiellement lorsqu'ils traitent de sujets d'intérêts général ou lorsqu'ils apportent une contribution à un débat public relatif à une quesiton d'intérêt général. Il ne s'en déduit pas toutefois que seuls les traitements d'information qui seraient eux-mêmes directement d'intérêt général participe à l'exercice de l'activité journalistique."* Le Conseil d'État demande de revoir cet article à la lumière du considérant 153 du Règlement afin de retenir une interprétation large des notions liées à cette liberté, telles le journalisme.

Sur ce point, le gouvernement a donc modifié la définition reprise dans cet article afin de répondre aux remarques du Conseil d'État.

Concernant la notion de média, la jurisprudence relative à l'article 25 de la Constitution garantissant la liberté de la presse, considère que la presse ne se limite pas à la presse imprimée mais "*qu'il y a lieu de conférer une interprétation évolutive à la notion de presse et (…) qu'un moyen de télécommunication comme internet est également susceptible de constituer une presse au sens de la constitution"* (Cass., 6 mars 2012, P. 11 1374 N*).*

Zoals de Raad van State het onderlijnt viseert de notie "media" niet enkel de geschreven pers maar elk orgaan dat informatie verspreid bestemd voor een onbepaald publiek, welke ook het communicatiemiddel of de vorm mag zijn die dit aanneemt.

De Privacycommissie stelt voor om aan het einde van de definitie toe te voegen "*en waarbij de verwerkingsverantwoordelijke zich de naleving van journalistieke deontologische regels tot taak stelt.*". De regering volgt dit voorstel.

Huidig recht

Vrijheid van meningsuiting, persvrijheid en verbod op censuur

In België is het recht op vrije meningsuiting neergelegd in artikel 19 van de Grondwet, die bepaalt dat "*De vrijheid van eredienst, de vrije openbare uitoefening ervan, alsmede de vrijheid om op elk gebied zijn mening te uiten, zijn gewaarborgd, behoudens bestraffing van de misdrijven die ter gelegenheid van het gebruikmaken van die vrijheden worden gepleegd.*"

De persvrijheid is eveneens neergelegd in artikel 25 van de Grondwet, die bepaalt dat: "*De drukpers is vrij; de censuur kan nooit worden ingevoerd".*

Het verbod op censuur werd geïnterpreteerd volgens de vaste rechtspraak, zowel van het Europees Hof voor de Rechten van de Mens (EHRM, 29 maart 2011, *aff. RTBF c/ Belgique)* als de hoven en rechtbanken (Appel, Bxl, 20 sept. 2011; Civ. Namur, réf , 1er décembre 2015, *JLMB*, 26 fév. 2016, p. 1) als verbod op de controles en voorafgaand verbod op publicatie van een artikel.

De bestraffing van misbruik door een journalist bij de uitoefening van zijn vrije meningsuiting kan enkel a posteriori gelden(Cass., 29 juin 2000, C, 98 0530 F).

Deze rechtspraak heeft als gevolg dat om de gegevensbescherming te harmoniseren met de persvrijheid, zoals opgelegd door artikel 85 van de Verordening, de verwerkingen met journalistieke doeleinden vrijgesteld moeten worden van alle bepalingen van de Verordening waarvan de toepassing een controle a priori van de verwerkingen met journalistieke doeleinden kan inhouden.

Dit artikel onderzoekt dus één voor één alle bepalingen van de Verordening om te onderzoeken of hun toepassing een controle a priori kan inhouden en in dat geval stelt het de verwerkingen met journalistieke doeleinden en verwerkingen ten behoeve van academische, artistieke of literaire uitdrukkingsvormen vrij.

Comme le Conseil d'État le souligne la notion de média ne vise pas uniquement la presse écrite mais tout organe qui diffuse des informations à destination d'un public indéterminé, quelque soit le mode de communication et la forme que celle-ci adopte.

La Commission vie privée suggère de rajouter à la fin de la définition "*et dont le reponsable du traitement s'impose des règles de déontologies journalistiques"*. Le gouvernement suit cette suggestion.

Droit actuel

Liberté d'expression, liberté de la presse et Interdiction de la censure

En Belgique, le droit à la liberté d'expression est consacré par l'article 19 de la constitution, qui dispose que "*la liberté des cultes, celle de leur exercice public, ainsi que la liberté de manifester ses opinions en toute matière, sont garanties, sauf la répression des délits commis à l'occasion de l'usage de ces libertés.*"

La liberté de presse est également consacrée par l'article 25 de la Constitution qui dispose que: "*la presse est libre; la censure ne pourra jamais être établie*".

L'interdiction de la censure a été interprétée par la jurisprudence constante, tant de la Cour européenne des Droits de l'Homme (CEDH, 29 mars 2011, *aff. RTBF c/ Belgique*) que des cours et tribunaux (Appel, Bxl, 20 sept. 2011; Civ. Namur, réf , 1er décembre 2015, *JLMB*, 26 fév. 2016, p. 1) comme interdisant les contrôles et interdictions préalables à la publication d'un article.

La répression des abus effectuées par un journaliste dans l'exercice de sa liberté d'expression ne peut intervenir qu'a posteriori (Cass., 29 juin 2000, C, 98 0530 F).

Cette jurisprudence a pour conséquence que pour réconcilier la protection des données avec la liberté de la presse, comme l'impose l'article 85 du Règlement, les traitements à des fins journalistiques doivent être exonérés de toutes les dispositions du règlement dont l'application pourrait constituer un contrôle a priori des traitements à des fins journalistiques.

Cet article examine donc une par une tous les dispositions du règlement pour examiner si leur application peut constituer un contrôle a priori et dans ce cas , il exempte les traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire.

Bescherming van de bronnen

De wet van 7 april 2005 tot bescherming van journalistieke bronnen bepaalt dat de journalisten niet mogen gedwongen worden hun document vrij te geven die de identiteit van hun informateur zou kunnen vrijgeven of de aard en de afkomst van hun informatie, behalve op vraag van en rechter en indien het van die aard is om de Commissie te waarschuwen voor een ernstige inbreuk met bedreiging voor de fysieke integriteit van personen.

Deze wet heeft als gevolg dat de verwerkingen met journalistieke doeleinden vrijgesteld moeten worden van alle bepalingen van de Verordening waarvan de toepassing een inbreuk zou kunnen inhouden op de bescherming van de bronnen.

Dit artikel onderzoekt dus één voor één alle bepalingen van de Verordening om te onderzoeken of hun toepassing een inbreuk inhoudt op de bescherming van de bronnen en in dat geval stelt het de verwerkingen met journalistieke doeleinden en verwerkingen ten behoeve van academische, artistieke of literaire uitdrukkingsvormen vrij.

Rechtsgrondslag

Er bestaan twee wettelijke grondslagen binnen de Verordening voor verwerkingen voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen: artikel 6.1.a) van de Verordening (toestemming van de betrokkene, zoals bijvoorbeeld tijdens een interview) en artikel 6.1.f) van de Verordening (afweging van belangen).

Artikel 6.1 f) van de Verordening bepaalt dat een verwerking plaats kan vinden wanneer het noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke, mits de belangen, vrijheden en fundamentele rechten van de betrokken persoon niet boven dat belang prevaleren.

De behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke is hier het recht de vrije meningsuiting neergelegd in artikel 10 van het Europees Verdrag inzake de Rechten van de Mens, erkend door artikel 85 van de Verordening, verzekerd door artikel 19 en 25 van de Grondwet.

Deze rechtsgrondslag staat de verwerkingsverantwoordelijke voor journalistieke, academische of literaire doeleinden toe om de gegevens van de betrokken persoon te verwerken los van zijn toestemming. De journalist kan *under cover* onderzoeken voeren of de verwerking verder zetten zelfs indien de betrokken persoon zijn oorspronkelijke toestemming intrekt.

Protection des sources

La loi du 7 avril 2005 *relatives à la protection des sources des journalistes* dispose que les journalistes ne peuvent être contraints à révéler leur document susceptible de révéler l'identité de leur informateur ou la nature et la provenance de leur information, sauf à la requête d'un juge et si cela est de nature à prévenir la commission d'infraction grave constituant une menace pour l'intégrité physique de personnes.

Cette loi a pour conséquence que les traitements à des fins journalistiques doivent être exonérés de toutes les dispositions du règlement dont l'application qui pourrait constituer une infraction à la protection des sources.

Cet article examine donc une par une tous les dispositions du règlement pour examiner si leur application peut constituer une infraction à la protection des sources et dans ce cas, il exempte les traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire.

Base légale

Il existe deux bases légales possibles au sein du Règlement pour les traitements à des fins de journalisme et à des fins d'expression universitaire, artistique ou littéraire: l'article 6.1.a) du Règlement (le consentement de la personne concernée, comme par exemple lors d'un interview) et l'article 6.1.f) du Règlement (la pondération d'intérêt).

L'article 6.1. f) du Règlement dispose qu'un traitement peut avoir lieu lorsqu'il est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement, à moins que ne prévalent les intérêts, libertés et droits fondamentaux de la personne concernée.

Les intérêts légitimes poursuivis par le responsable du traitement sont ici le droit à la liberté d'expression consacré par l'article 10 de la Convention européenne des droits de l'homme, reconnus par l'article 85 du règlement, garanti par les articles 19 et 25 de la Constitution.

Cette base légale autorise le responsable du traitement à des fins de journalisme, académique, artistique ou littéraire à traiter les données de la personne concernée indépendamment du consentement de celle-ci. Le journaliste peut mener des enquêtes *under cover* ou continuer son traitement même si la personne concernée retire son consentement initial.

§ 2. Zoals de Raad van State het aangeeft, wanneer een verwerking van gegevens voor journalistieke doeleinden gebaseerd is op toestemming, is het artikel 7 van de Verordening en in het bijzonder de mogelijkheid van de betrokkene om zijn toestemming op elk moment in te trekken, niet van toepassing op deze verwerkingen. Het huidig ontwerp van wet heeft dit dus in die zin gewijzigd. De uitzondering werd eveneens voor het artikel 8 van de Verordening toegevoegd.

Deze paragraaf stelt de verwerkingsverantwoordelijke voor journalistieke, academische, artistieke of literaire doeleinden ook vrij van het verbod op de verwerking van gevoelige gegevens (art. 9 et 10 van de Verordening).

Deze paragraaf stelt de verwerkingsverantwoordelijke voor journalistieke, academische, artistieke of literaire doeleinden eveneens vrij van de verplichting om toegangsrecht te verlenen aan de betrokkene terwijl die hem bijkomende gegevens geeft waardoor hij geïdentificeerd kan worden (artikel 11 van de Verordening).

Die vrijstelling is nieuw tegenover de huidige WVP, in die zin dat deze verplichting eveneens nieuw is.

De Privacycommissie meent dat deze uitzondering geschrapt zou moeten worden want “indien de hypothese bedoeld in artikel 11.2 van de Verordening zich voordoet kan de betrokkene slechts de rechten kunnen uitoefenen die hem door de AVG worden verleend binnen de strikte grenzen bepaald in de uitvoeringsreglementering van de AVG”. Om redenen van helderheid wordt het advies van de Privacycommissie niet gevolgd.

Deze paragraaf stelt de verwerkingsverantwoordelijke voor journalistieke, academische, artistieke of literaire doeleinden ook vrij van de verplichting om de betrokkene te informeren, terwijl hij de gegevens verzamelt bij hem (artikel 13 van de Verordening) of bij een derde (artikel 14 van de Verordening).

Artikel 3, § 3, b), WVP wordt overgenomen in dit artikel, die onderzoeken beoogt toe te staan die op anonieme wijze worden uitgevoerd, zoals undercoveronderzoeken of onderzoeken waarbij het doel van de reportage niet wordt vermeld.

Deze paragraaf stelt vervolgens de verwerkingsverantwoordelijke voor journalistieke, academische, artistieke of literaire doeleinden vrij van de verplichting om toegang te verlenen aan de betrokkene (artikel 15 van de Verordening) om dezelfde redenen dan de voorgaande uitzonderingen.

§ 2. Comme le suggère le Conseil d’État, lorsqu’un traitement de données à des fins de journalisme est basée sur le consentement, l’article 7 du Règlement, en particulier la possibilité pour la personne concernée de retirer son consentement à tous moments, ne s’applique pas à ces traitements. Le présent projet de loi a donc été modifié dans ce sens. L’exemption pour l’article 8 du Règlement a également été rajouté.

Ce paragraphe exempte aussi le responsable du traitement à des fins de journalisme, académique, artistique ou littéraire de l’interdiction de traiter des données sensibles (art. 9 et 10 du Règlement)

Ce paragraphe exempte également le responsable du traitement à des fins de journalisme, académique, artistique ou littéraire de l’obligation de donner un droit d’accès à la personne concernée lorsque celle-ci lui fournit des données supplémentaires qui permettent de l’identifier (article 11 du Règlement).

Cette exemption est nouvelle par rapport à la LVP, dans la mesure où cette obligation est également nouvelle.

La Commission vie privée estime que cette exemption devrait être supprimé car “si l’hypothèse visée à l’article 11.2 RGPD se réalise, la personne ne pourra exercer les droits que lui confèrent le RGPD dans la stricte mesure d’exécution du RGPD.”. Par souci de clarté l’avis de la Commission vie privée n’est pas suivi.

Ce paragraphe exempte aussi le responsable du traitement à des fins de journalisme, académique, artistique ou littéraire de l’obligation d’informer la personne concernée lorsqu’il collecte des informations auprès d’elle (article 13 du Règlement) ou auprès d’un tiers (article 14 du Règlement).

L’article reprend ici l’article 3, § 3, b), LVP qui vise à permettre les enquêtes effectuées dans l’anonymat telles que les enquêtes sous couverture d’une identité fictive, ou enquêtes en omettant de présenter l’objectif du reportage.

Ensuite ce paragraphe exempte le responsable du traitement à des fins de journalisme, académique, artistique ou littéraire de l’obligation de donner accès à la personne concernée (article 15 du Règlement) pour les mêmes motifs que les exemptions précédentes.

Deze paragraaf stelt de verwerkingsverantwoordelijke voor journalistieke, academische, artistieke of literaire doeleinden ook vrij van de verplichting om een recht tot verbetering te verlenen aan de betrokkene (art. 16 van de Verordening).

Oorspronkelijk voorzag dit artikel er ook in dat verwerkingen voor journalistieke doeleinden uitgezonderd werden van het recht op verbetering voor zover de uitoefening van dit recht een ontwerp van publicatie zou hinderen en voor ozver de betrokkene over een recht van antwoord beschikte. De Raad van State meende dat deze bepaling verwarring teweeg bracht tussen het recht op bescherming van gegevens en de persvrijheid. Inderdaad, het recht van antwoord is geen recht op verbetering. De uitzondering op artikel 16 van de Verordening dient dus aan geen enkele voorwaarde onderworpen te zijn. De regering deelt in deze de mening van de Raad van State. In de mate dat het recht is verworven om te verzoeken dat een antwoord wordt verspreid zou de mogelijkheid om het recht op verbetering toe te laten in bepaalde omstandigheden het evenwicht kunnen schaden tussen de vrijheid om te informeren en het recht van antwoord.

Het wetsontwerp stelt de verwerkingsverantwoordelijke voor journalistieke, academische, artistieke of literaire doeleinden niet vrij van de verplichting om het recht om vergeten te worden te verlenen aan de betrokken persoon (artikel 17 van de Verordening). Artikel 17.3 van de Verordening stelt zelf dat het recht om vergeten te worden niet van toepassing is op verwerkingen voor doeleinden van vrije meningsuiting en vrije informatie. De verordening is dus rechtstreeks van toepassing en het is dus niet nodig dat de wet die vrijstelling opnieuw aanmaakt.

De Privacycommissie stelt voor het artikel te wijzigen, stellen dat het artikel 17 van de Verordening van toepassing is op verwerkingen voor journalistieke doeleinden wanneer hun inhoud niet langer in het algemeen belang is of indien hun bewaring in de originele toestand niet aangewezen is gelet op de repercussies van hun informatieve inhoud op de betrokkene.

De Raad van State voegt zich daarentegen bij de positie van de regering door te stellen dat "*in artikel 29 terecht niet* [wordt] *bepaald dat het niet van toepassing is op de verwerking van gegevens voor journalistieke, academische, artistieke of literaire doeleinden, aangezien reeds in die uitsluiting wordt voorzien in paragraaf 3, a), zelf van dat artikel 17.".*

Deze paragraaf stelt de verwerkingsverantwoordelijke voor journalistieke, doeleinden eveneens vrij van de verplichting om een recht op beperking van de

Ce paragraphe exempte aussi le responsable du traitement à des fins de journalisme, académique, artistique ou littéraire de l'obligation de donner un droit de rectification à la personne concernée (art. 16 du Règlement).

Initialement cet article prévoyait aussi que les traitements à des fins journalistiques étaient exemptés du droit de rectification pour autant que l'exercice de ce droit compromettait une publication en projet et dans la mesure où la personne concernée avait un droit de réponse. Le Conseil d'État considère que cette précision révèlait une confusion entre le droit à la protection des données et la liberté de la presse. En effet, le droit de réponse n'est pas un droit de rectification. L'exemption de l'article 16 du Règlement ne devrait dès lors être soumis à aucune condition. Le gouvernement partage l'avis du Conseil d'État. Dans la mesure où le droit de solliciter la diffusion d'une réponse est acquis, le fait de permettre le droit de rectification dans certaines conditions pourrait atteindre l'équilibre entre la liberté d'information et le droit de réponse.

Le projet de loi n'exempte pas le responsable du traitement à des fins de journalisme, académique, artistique ou littéraire de l'obligation de donner un droit à l'oubli à la personne concernée (article 17 du Règlement). En effet l'article 17.3 du Règlement dispose lui-même que le droit à l'oubli n'est pas applicable aux traitements à des fins de liberté d'expression et d'information. Le règlement étant directement applicable, il n'est donc pas nécessaire de que la loi recrée cette exemption.

La Commission vie privée suggère de modifier l'article en disant que l'article 17 du Règlement est applicable aux traitements à des fins journalistiques si leur contenu ne présente plus d'intérêt général ou si leur préservation en l'état n'est pas indiquée au vu des répercussions de leur contenu informatif sur la personne concernée.

Le Conseil d'État rejoint par contre la position du gouvernement en déclarant que "*c'est à bon escient que le projet de loi ne déclare pas l'article 17 inapplicable aux traitments effectués aux fins de journalisme dès lors que cette exclusion est déjà prévue par le paragraphe 3. a) lui-même de cet article 17.".*

Ce paragraphe exempte également le responsable du traitement à des fins de journalisme de l'obligation de donner un droit de limitation du traitement à la personne

verwerking te verlenen aan de betrokkene indien de uitoefening van dit recht een voorgenomen publicatie in het gevaar brengt.

Indien de betrokkene de juistheid van de gegevens betwist, dan dwingt artikel 18 van de Verordening inderdaad de verwerkingsverantwoordelijke om de publicatie op te schorten voor de tijd die nodig is om de juistheid van de gegevens na te gaan.

Zoals het Europees Hof voor de Rechten van de Mens benadrukt "*l'information est un bien périssable et en retarder la publicatio , même pour un brève période, risque fort de la priver de toute valeur et de tout intérêt*" (CEDH, 29 maart 2011, *Aff. RTBF c/ Belgique, § 108).* Artikel 18.1 a) van de Verordening is dus niet verenigbaar met de vrije meningsuiting en de verwerkingsverantwoordelijke voor journalistieke doeleinden moet dus vrijgesteld worden.

De Privacycommissie meent dat het recht op beperking van de gegevens behouden zou moeten blijven in de hypotheses voorzien door de artikelen 18.1.b) van de Verordening (de verwerking is niet rechtmatig en de betrokkene eist er de beperking van eerder dan de wissing) en 18.1.c) van de Verordening (de verwerkingsverantwoordelijke heeft de gegevens niet meer nodig maar de betrokkene heeft ze nog nodig ter uitoefening van een rechtsvordering).

De verplichting van de verwerkingsverantwoordelijke om derden in te lichten over de rechtzettingen (artikel 19 van de Verordening) is niet van toepassing op verwerkingen voor journalistieke, academische, artistieke of literaire doeleinden voor zover het recht op rechtzetting en om vergeten te worden van toepassing is op die verwerkingen.

Tot slot stelt deze paragraaf de verwerkingsverantwoordelijke voor journalistieke doleinden vrij van de verplichting om aan de betrokkene een recht te geven om de verwerking te weigeren (artikel 21.1 van de Verordening).

Dit recht is inderdaad tegenstrijdig aan artikel 25 van de Grondwet die censuur verbiedt.

Het verbod op censuur werd geïnterpreteerd door de vaste rechtspraak, zowel van het Europees Hof voor de Rechten van de Mens (CEDH, 29 maart 2011, *Aff. RTBF c/ Belgique*) als de hoven en rechtbanken (Brussel, 20 sept. 2011; Civ. Namur, 1er december 2015, *JLMB*, 26 feb. 2016, p. 1) als verbod om controles te voeren en verbod vooraf aan de publicatie van een artikel. De bestraffing van misbruiken begaan door een journalist in de uitoefening van zijn vrije meningsuiting kan slechts

concernée si l'exercice de ce droit compromet une publication en projet.

Lorsque la personne concernée conteste l'exactitude des données, l'article 18 du Règlement contraint en effet le responsable du traitement à suspendre la publication le temps nécessaire pour vérifier l'exactitude des données.

Comme le souligne la Cour européenne des droits de l'Homme "*l'information est un bien périssable et en retarder la publication, même pour un brève période, risque fort de la priver de toute valeur et de tout intérêt*" (CEDH, 29 mars 2011, *Aff. RTBF c/ Belgique, § 108)*. L'article 18.1 a) du Règlement n'est donc pas compatible avec la liberté d'expression et d'information et il convient d'en exempter le responsable du traitement à des fins journalistiques.

La Commission vie privée estime que le droit à la limitation des données devrait être maintenu dans les hypothèes prévues par les articles 18.1. b) du Règlement (le traitement est illicite et la personne concernée en exige la limitation au lieu de son effacement) et 18.1.c) du Règlement (le responsable du traitement n'a plus besoin des données mais elles sont encore nécessaires pour la personne concernée pour l'exercice de droits en justice).

L'obligation du responsable du traitement de notifier aux tiers les rectifications (article 19 du Règlement) ne s'applique aux traitements à des fins de journalisme, académique, artistique ou littéraire de l'obligation que dans la mesure où le droit à la rectification et à l'oubli s'appliquent à ces traitements.

Enfin, ce paragraphe exempte le responsable du traitement à des fins de journalisme de l'obligation de donner à la personne concernée un droit d'objection au traitement (article 21.1 du Règlement).

Ce droit est en effet contraire à l'article 25 de la Constitution qui interdit la censure.

L'interdiction de la censure a été interprétée par la jurisprudence constante, tant de la Cour européenne des Droits de l'Homme (CEDH, 29 mars 2011, *Aff. RTBF c/ Belgique*) que des cours et tribunaux (Appel, BXL, 20 sept. 2011; Civ. Namur, 1er décembre 2015, *JLMB*, 26 fév. 2016, p. 1) comme interdisant les contrôles et interdiction préalables à la publication d'un article. La répression des abus effectuées par un journaliste dans l'exercice de sa liberté d'expression ne peut intervenir

a posteriori gelden op basis van artikel 1382 van het burgerlijk wetboek (Cass. 29 juin 2000, C, 98 0530 F).

De Privacycommissie onderlijnt dat het onevenredig is om er zonder beperking van af te wijken. Naar het voorbeeld van wat reeds voorzien is in de WVP dient te worden verduidelijkt dat deze vrijstelling enkel geldt indien de uitoefening van het recht op bezwaar dreigt een ontwerp van publicatie in gedrang te brengen. De regering volgt het advies van de Privacycommissie op dit punt.

§ 3. De verplichting van de verwerkingsverantwoordelijke om het activiteitenregister mee te delen aan de Gegevensbeschermingsautoriteit (artikel 30.4 van de Verordening), om samen te werken met de Gegevensbeschermingsautoriteit, om een gegevenslek te melden aan de Gegevensbeschermingsautoriteit (artikel 33 van de Verordening) of om te vragen om de Gegevensbeschermingsautoriteit voorafgaandelijk aan de publikatie te raadplegen (artikel 36 van de Verordening) is niet van toepassing op de verwerkingen voor journalistieke doeleinden in de mate dat deze ertoe kunnen leiden dat de Gegevensbeschermingsautoriteit maatregelen neemt die een publicatie verhinderen, hetgeen een handeling van censuur zou uitmaken die verboden wordt door de Grondwet.

§ 4. Het hoofdstuk over internationale doorgiften is niet van toepassing op doorgiften van persoonsgegevens voor uitsluitend journalistieke, academische, artistieke of literaire doeleinden aan derde landen of internationale organisaties in de mate dat de toepassing ervan nodig is om het recht op privacy te verzoenen met de regels betreffende de vrijheid van meningsuiting.

§ 5. De bevoegdheden toegekend door de Verordening aan de Gegevensbeschermingsautoriteit, zoals de bevoegdheid toegang te hebben tot de verwerking, om de wijziging ervan te bevelen of om ze te verbieden, zijn niet van toepassing op de verwerkingen voor journalistieke, academische, artistieke of literaire doeleinden voor zover ze handelingen kunnen teweegbrengen die tegenstrijdig zijn met artikel 25 van de Grondwet, die censuur verbiedt, of met de wet van 7 april 2005 inzake de bescherming van journalistieke bronnen.

qu'a posteriori sur base de l'article 1382 du Code civil (Cass. 29 juin 2000, C, 98 0530 F).

La Commission vie privée souligne qu'il est disproportionné d'y déroger sans limite. A l'instar de ce qui est déjà prévu dans la LVP, il convient de préciser que cette dispense vaut uniquement si l'exercice du droit d'oppostion est susceptible de compromettre une publication en projet. Le gouvernement suit l'avis de la Commssion vie privée sur ce point.

§ 3. L'obligation du responsable du traitement de communiquer le registre des activités à l'Autorité de protection des données (article 30.4 du Règlement), de collaborer avec l'Autorité de protection des données), de notifier une fuite de données à l'Autorité de protection des données (article 33 du Règlement) ou de demander à consulter l'Autorité de protection des données préalablement à une publication (article 36 du Règlement) n'est pas applicable aux traitements à des fins de journalismes dans la mesure où ils peuvent amener l'Autorité de protection des données à prendre une mesure qui empêche une publication ce qui constituerait un acte de censure interdit par la Constitution.

§ 4. Le chapitre sur les transferts internationaux ne s'applique pas aux transferts de données à caractère personnel effectués aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire vers des pays tiers ou à des organisations internationales, dans la mesure où son application est nécessaire pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

§ 5. Les pouvoirs accordés par le Règlement à l'Autorité de protection des données, comme le pouvoir d'accéder au traitement, d'ordonner sa modification ou de l'interdire ne sont pas applicables aux traitements à des fins de journalisme, académique, artistique ou littéraire dans la mesure où ils peuvent constituer des actes contraires à l'article 25 de la Constitution, qui prohibe la censure, ou à la loi du 7 avril 2005 relative à la protection des sources des journalistes.

TITEL 2

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid

Het vrije verkeer van persoonsgegevens tussen bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid binnen de Europese Unie en de doorgifte van dergelijke persoonsgegevens aan derde landen en internationale organisaties, moet worden vergemakkelijkt, en tegelijk moet een hoge mate van bescherming van persoonsgegevens worden gewaarborgd. Die ontwikkelingen vereisen een solide en coherenter kader voor de bescherming van persoonsgegevens, gepaard gaand met een strikte toepassing van de regels.

Teneinde de Richtlijn zo goed mogelijk om zetten, maar ook met het oog op de invoering van de mechanismen waarin de Verordening voorziet, zijn verschillende pistes van aanpak onder de loep genomen. De werkgroep heeft inzonderheid gereflecteerd over de volgende vragen:

Hoe verhoudt ons huidig Belgisch wetgevend kader zich ten opzichte van de Verordening *en de richtlijn? Zijn er tekortkomingen? Moet onze wetgeving worden gewijzigd of aangevuld (privacywet, Gerechtelijk Wetboek of Wetboek van Strafvordering)?*

— Het onderscheid tussen de burgerlijke rechtbank en de strafrechtbank enerzijds en tussen bestuurlijke politie en gerechtelijke politie anderzijds is van essentieel belang bij deze denkoefening.

Wat zijn de verschillen tussen de Verordening en de Richtlijn?

— Naargelang de toepasselijke rechtsregels (burgerlijk recht of strafrecht)?

— Naargelang het gaat om de bestuurlijke politie of de gerechtelijke politie?

TITRE 2

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces

Il convient de faciliter le libre flux des données à caractère personnel entre les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union européenne, et le transfert de telles données vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel. Ces évolutions obligent de mettre en place un cadre pour la protection des données à caractère personnel solide et plus cohérent, assorti d'une application rigoureuse des règles.

Afin de transposer au mieux la Directive, mais également la mise en place des mécanismes prévus par le Règlement, plusieurs axes d'attaques ont été survolés. Les réflexions en groupe de travail ont porté notamment sur les questions suivantes:

Comment se rapporte notre cadre législatif belge actuel au Règlement *et à la directive? Est-ce qu'il y a des lacunes? Faut-il modifier ou compléter notre législation (que ce soit la loi vie privée, le Code judiciaire ou le Code d'instruction criminelle)?*

— la distinction entre le tribunal civil et pénal d'une part, et police administrative et police judiciaire, est essentielle dans cette réflexion.

Quelles sont les différences entre le Règlement et la Directive?

— Selon le régime judiciaire qui s'applique (civil ou pénal)?

— Selon qu'il s'agisse de la police administrative ou de la police judiciaire?

— Naargelang de verplichtingen voor de verwerkingsverantwoordelijke/verwerker?

Wie is de verwerkingsverantwoordelijke voor welke soort verwerking?

— Vindt de verwerking plaats in het kader van het gerechtelijk dossier (de aard van de procedure is bepalend voor de keuze van het toepasselijke instrument en dus voor de verantwoordelijkheden)?

— Vindt de verwerking plaats in het kader van een informaticatoepassing (Waar bevindt de toepassing zich? Wie is de beheerder/verwerker? Met welke doeleinden vinden de verwerkingen plaats?)?

Wat is het controleorgaan voor welke soort verwerking?

— Vindt de verwerking plaats in het kader van het gerechtelijk dossier?

— Vindt de verwerking plaats in het kader van een informaticatoepassing?

— Rechtstreekse/onrechtstreekse toegang (politie)?

Daaruit vloeit dan ook voort dat de verwerkingen door de gerechtelijke overheden of de politiediensten voor andere doeleinden dan die bepaald in deze titel dus niet worden beoogd door die bepalingen. Op die verwerkingen is de Verordening dus rechtstreeks van toepassing, evenals de bepalingen waarin het nationaal recht voorziet.

HOOFDSTUK I

Algemene bepalingen

Art. 25

Dit artikel bepaalt dat deze wet de omzetting beoogt van de Richtlijn 2016/680/EU van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Het Belgisch recht voldoet grotendeels aan de vereisten van de Richtlijn. Op federaal niveau zal de omzetting

— Selon les obligations pour le responsable du traitement/sous-traitant?

Qui est le responsable du traitement pour quel type de traitement?

— le traitement a lieu dans le cadre du dossier judiciaire (la nature de la procédure définit le choix de l'instrument qui s'applique et donc les responsabilités)?

— le traitement a lieu dans le cadre d'une application informatique (où se situe l'application? Qui est le gestionnaire/sous-traitant? Les traitements ont lieu pour quelles finalités?)?

Quel est l'organe de contrôle pour quel type de traitement?

— le traitement a lieu dans le cadre du dossier judiciaire?

— le traitement a lieu dans le cadre d'une application informatique?

— Accès direct-indirect (police)?

Il en résulte donc que les traitements faits par les autorités judiciaires ou les services de police à des fins autres que les fins déterminées par le présent titre ne sont donc pas visés par ces dispositions. Ces traitements sont donc soumis au Règlement directement applicable ainsi qu'aux dispositions mises en œuvre par le droit national.

CHAPITRE I^ER

Dispositions générales

Art. 25

Cet article dispose que la présente loi transpose la Directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Le droit belge répond en grande partie aux exigences de la Directive. Au niveau fédéral, la transposition de

van de Richtlijn integraal zijn met de aanneming van dit wetsontwerp.

Art. 26

Dit artikel neemt de definities over die in de Richtlijn zijn opgenomen. De gemeenschappelijke definities tussen de Richtlijn en de Verordening zijn identiek.

We kunnen het volgende specificeren:

3° Het markeren zoals vermeld in de definitie van behandelingsbeperking (artikel 3.3 van de Richtlijn) heeft als doel om bijvoorbeeld metadata toe te voegen.

7° In artikel 3.7 van de Richtlijn wordt het begrip bevoegde overheid gedefinieerd teneinde op ruime wijze de rechterlijke en politiële overheden te beogen, evenals andere entiteiten die door de lidstaat zijn gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen (overweging 11), om rekening te houden met de verschillende systemen van de lidstaten van de Europese Unie.

De Richtlijn bepaalt de "bevoegde autoriteit" (art. 3.7 van de Richtlijn) als volgt:

a) iedere overheidsinstantie die bevoegd is voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; of

b) ieder ander orgaan dat of iedere andere entiteit die krachtens het lidstatelijke recht is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

De term "bevoegde autoriteiten" wordt hier vervangen door de term "bevoegde overheden", wat de term is die in België wordt gebruikt, terwijl de vertaling van de Richtlijn naar het Nederlands de voorkeur geeft aan de woordenschat die in Nederland wordt gebruikt.

Volgende bevoegde overheden worden in deze wet aangewezen:

— de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus

la Directive sera intégrale avec l'adoption du présent projet de loi.

Art. 26

Cet article reprend les définitions inclues dans la Directive. Les définitions communes entre la Directive et le Règlement sont identiques.

On peut spécifier ce qui suit:

3° Le marquage tel que mentionné dans la définition de limitation de traitement (art. 3.3 de la Directive) vise par exemple l'ajout de métadonnées.

7° L'article 3.7 de la Directive définit la notion d'autorité compétente, afin de viser de manière large les autorités judiciaires et policières ainsi que d'autres entités à qui l'État membre a confié l'exercice de l'autorité publique et des prérogatives de puissance publique (considérant 11), pour respecter les différents systèmes des États membres de l'Union européenne.

La Directive détermine l'"*autorité compétente*" (art. 3.7 de la Directive) comme suit:

a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou

b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Le terme en néerlandais "bevoegde autoriteiten" est ici remplacé par le terme "bevoegde overheden" qui est le terme utilisé en Belgique, alors que la traduction de la Directive en langue néerlandaise privilégie le vocabulaire utilisé aux Pays-Bas.

Les autorités compétentes suivantes sont désignées dans la présente loi:

— les services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (qui est la

(dit is ook de referte in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit);

— de gerechtelijke overheden waaronder wordt verstaan de gemeenrechtelijke hoven en rechtbanken en het openbaar ministerie;

— de Dienst Enquêtes van het Vast Comité van Toezicht op de politiediensten in het kader van zijn rechtelijke missies zoals bedoeld in artikel 16, § 3, van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse (de Dienst Enquête P);

— de Algemene Inspectie van de federale politie en van de lokale politie (AIG);

— de Algemene administratie van de douane en accijnzen, in het kader van haar taak inzake opsporing, vaststelling en vervolging van de misdrijven die onder haar bevoegdheid vallen zoals bepaald in de Algemene Wet inzake douane en accijnzen van 18 juli 1977, en desgevallend in de Wet van 22 april 2003 houdende toekenning van de hoedanigheid van officier van gerechtelijke politie aan bepaalde ambtenaren van de administratie der douane en accijnzen;

— de Passagiersinformatie-eenheid zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens;

— de Cel voor financiële informatieverwerking bedoeld in artikel 76 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

— de Dienst Enquêtes van het het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van zijn gerechtelijke opdrachten zoals bedoeld in artikel 40, 3e lid van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

Er wordt verstaan onder gemeenrechtelijke hoven en rechtbanken en het openbaar ministerie: alle instellingen die tot taak hebben de wet te handhaven door geschillen te beslechten. Het betreft dus de magistraten, rechtbanken en organen die bijdragen aan het recht spreken binnen de rechterlijke macht, zoals de griffiers, de colleges van hoven en rechtbanken en het openbare ministerie.

référence faite dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données);

— les autorités judiciaires entendues comme les cours et tribunaux du droit commun et le ministère public;

— le Service d'enquêtes du Comité permanent de contrôle des services de police dans le cadre de ses missions judiciaires telles que prévues à l'article 16, § 3, de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (Service d'enquêtes P);

— l'Inspection générale de la police fédérale et de la police locale (AIG);

— l'Administration générale des douanes et accises, dans le cadre de sa mission relative à la recherche, la constatation et la poursuite des infractions déterminée par la Loi générale du 18 juillet 1977 sur les douanes et accises et, le cas échéant, par la Loi du 22 avril 2003 octroyant la qualité d'officier de police judiciaire à certains agents de l'Administration des douanes et accises;

— l'Unité d'information des passagers, telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers;

— la Cellule de traitement des informations financières visée à l'article 76 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

— le Service d'enquêtes du Comité permanent de contrôle des services de renseignement dans le cadre de ses missions judiciaires telles que prévues à l'article 40, alinéa 3, de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

On entend par cours et tribunaux du droit commun et le ministère public l'ensemble des institutions dont la fonction est de faire appliquer la loi en tranchant les litiges. Il s'agit donc des magistrats, des juridictions, des organes concourant à l'exercice du pouvoir de juger dans l'ordre judiciaire, tels que les greffes, les collèges des cours et tribunaux et du parquet.

De Algemene wet inzake douane en accijnzen definieert de bevoegdheden en de werkwijze van de Algemene Administratie van de douane en accijnzen (AADA). Deze wet is de basis voor alle taken die door de AADA moeten worden uitgevoerd, niet alleen voor de taken inzake douane en accijnzen (fiscaal en penaal) die aan een aangifteplicht verbonden zijn, maar ook voor alle taken waarvoor in diverse wetgeving vaststellings- en onderzoekstaken worden opgelegd aan de AADA, voornamelijk bij handel van, naar en door de Europese Unie. Als voorbeelden zijn te noemen de taken van de AADA inzake drugsprecursoren, economische vergunningen (wapenhandel, diamant, …), voedselveiligheid, namaak, afval, CITES, … Douanemisdrijven worden opgespoord en vastgesteld door de AADA die vervolgens de strafvordering op gang zal brengen zoals bepaald in de artikelen 279 tot 285 van de algemene wet inzake douane en accijnzen van 18 juli 1977 (B.S. 21 september 1977 – hierna AWDA). Ten aanzien van douane en accijnzen behoort de strafvordering aan de AADA alleen of aan de Administratie en aan het openbaar ministerie gezamenlijk (wanneer twee vorderingen, namelijk een gemeenrechtelijke vordering en een vordering inzake douane- en accijnszaken, gelijktijdig uitgeoefend moeten worden, of wanneer het openbaar ministerie tussenkomt voor de vordering van een gevangenisstraf). Het recht van initiatief behoort wel alleen aan de AADA. Het openbaar ministerie kan niet op eigen initiatief een opsporingsonderzoek voeren bij schendingen van de douane- en accijnzenwetgeving. Als de politiedienst een douane- of accijnzenmisdrijf vaststelt, dan licht hij de AADA in.

De Algemene wet inzake douane en accijnzen van 28 juli 1977 deelt aan de Algemene administratie van de douane en accijnzen de bevoegdheid toe om elke strafrechtelijke vervolging van douane- en accijnsmisdrijven zelf te vervolgen (met uitsluiting van het Openbaar Ministerie, behalve voor de gevangenisstraf) voor de correctionele rechtbank (artikel 281), dan wel om zelf (wederom met uitsluiting voor het Openbaar Ministerie) voor die misdrijven een minnelijke schikking te stellen (artikel 263). In Hoofdstuk II (in zonderheid artikelen 8 t/m 10) van het Ministeriële besluit van 27 februari 1979 inzake douane en accijnzen wordt deze bevoegdheid toegekend aan de directeur-generaal en de Gewestelijke directeurs van de douane en accijnzen (rekening houdende met de wet van 27 APRIL 2016 tot aanpassing van de bepalingen tot toekenning van titels en graden in de fiscale wetboeken en de wettelijke bepalingen met betrekking tot de douane en accijnzen, en houdende diverse andere bepalingen en rekening houdende met het besluit van de Administrateur-generaal van de Douane en Accijnzen van 25 april 2017 houdende aanduiding van ambtenaren in het kader

La Loi générale sur les douanes et accises définie les compétences et les méthodes de travail de l'Administration générale des douanes et accises (AGDA). Cette loi constitue la base pour toutes les missions qui doivent être exécutées par l'AGDA, non seulement pour les missions relatives aux douanes et accises (fiscal et pénal) pour lesquelles il existe une obligation de déclaration, mais également pour toute mission pour laquelle de diverses législations imposent des missions de constatation et de recherche à l'AGDA, notamment en cas de commerce depuis, vers ou par l'Union européenne. Peuvent être cités comme exemples, les missions de l'AGDA relatives aux précurseurs de drogues, permis économiques (traffic d'armes, diamant, …), sécurité alimentaire, contrefaçon, déchets, CITES, … L'AGDA recherche et constate des infractions douanières et initie ensuite l'action pénale déterminée dans les articles 279 à 285 de la Loi générale sur les douanes et accises (MB. 21 septembre 1977 – ci-après LGDA). Vis-à-vis les douanes et accises l'action pénale appartient à l'AGDA seule ou à l'Administration et au ministère public conjointement (lorsque deux actions, à savoir une action de droit commun et une action relative aux matières douanières et d'accises, doivent être exercées en même temps ou lorsque le ministère public intervient pour réclamer l'emprisonnement). Mais, le droit d'initiative appartient seul à l'AGDA. Le ministère public ne peut pas de leur propre initiative mener une enquête de recherche en cas de violation de la législation relative aux douanes et accises. Lorsqu'un service de police constate une infraction douanière ou d'accises il en informe l'AGDA.

La loi générale sur les douanes et accises du 18 juillet 1977 accorde la compétence à l'Administration Générale des Douanes et Accises de poursuivre elle-même toute poursuite pénale d'infractions en matière de douane et d'accises (à l'exception du ministère public, sauf pour la peine d'emprisonnement) pour le tribunal correctionnel (article 281), et de proposer une solution à l'amiable pour ces infractions (de nouveau sauf le ministère public) (article 263). Dans le chapitre II (en particulier l'article 8 à 10) de l'Arrêté ministériel du 27 février 1979 en matière des douanes et accises, cette compétence est attribuée au directeur général et aux directeurs régionaux des douanes et accises (en tenant compte de loi du 27 avril 2016 adaptant les dispositions attributives de titres et de grades dans les codes fiscaux et les dispositions légales relatives aux douanes et accises et portant diverses autres dispositions et tenant compte de l'arrêté de l'Administrateur général du 25 avril 2017 portant désignation de fonctionnaires dans le cadre de certaines dispositions légales relatives aux douanes et accises, le directeur général et le directeur régional doivent respectivement être lus

van sommige wettelijke bepalingen met betrekking tot douane en accijnzen dient de directeur-generaal en de gewestelijk directeur respectievelijk gelezen te worden als adviseur-generaal hoofd van de dienst geschillen en de adviseur-generaal regionaal centrum directeur).

Deze bevoegdheid geldt uitsluitend voor douane- en accijnsmisdrijven. De Algemene administratie van de douane en accijnzen kan geen andere misdrijven vervolgen waarvoor ze wel vaststellings- en/of opsporingsbevoegdheid heeft, zoals misdrijven inzake verdovende middelen, mensenhandel, namaakgoederen, enzovoort. Op al deze andere domeinen beslist de Procureur des Konings, na het dossier te hebben ontvangen, over het gevolg dat aan de feiten moet worden gegeven.

De verwerkingen in het kader van de finaliteiten bedoeld in artikel 8, § 1, 1°, 2°, 3° et 5°, van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens vallen onder het toepassingsgebied van titel 2 vermits het de verwerking van persoonsgegevens (passagiersgegevens) verricht door de overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Verwerkingen verricht voor andere finaliteiten bedoeld in de wet van 25 december 2016 vallen niet onder het toepassingsgebied van titel 2. Ze zullen, naar gelang het geval, vallen onder hetzij titel 1 hetzij titel 3.

Andere administratieve overheden, ook indien zij bevoegd zijn tot controle, inspectie of vervolging van bepaalde strafbare feiten, worden niet als bevoegde overheden in de zin van deze titel beschouwd.

8° Verwerkingsverantwoordelijke: Art. 3.8 van de Richtlijn en art. 3.7 van de Verordening. Het betreft de klassieke definitie van verwerkingsverantwoordelijke, die hier wordt gedifferentieerd op grond van het toepassingsgebied. De vraag wie de verwerkingsverantwoordelijke is, is dus een feitelijke vraag en moet voor ieder geval afzonderlijk worden onderzocht. In de wet kan echter precies worden vastgelegd wie de verwerkingsverantwoordelijke is. Deze vraag is niet onbeduidend en kan vaak aanleiding geven tot discussies. Binnen het strafrechtelijke kader bestaan er verschillende gemeenschappelijke gegevensbanken, wat het probleem niet eenvoudiger maakt. Als er daadwerkelijk meerdere verwerkingsverantwoordelijken zijn, zullen die als medeverantwoordelijken worden beschouwd.

comme conseiller général à la tête du service litiges et le conseiller général directeur du centre régional).

Cette compétence est uniquement valable pour les infractions en matière des douanes et accises. L'Administration Générale des Douanes et Accises ne peut pas poursuivre d'autres infraction pour lesquelles elle peut effectuer des enquêtes administratives et/ou judiciaires, comme les infractions en matière de substances stupéfiantes, traite des êtres humains, contrefaçon, etc. sur tous les autres domaines, le Procureur du Roi décide, après réception du dossier, de la suite à donner aux faits.

Les traitements dans le cadre des finalités visées à l'article 8, § 1er, 1°, 2°, 3° et 5°, de la loi du 25 décembre 2016 tombent dans l'application du titre 2 puisqu'il s'agit de traitements de données à caractère personnel (données des passagers) effectués par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Les traitements faits pour les autres finalités visées par la loi du 25 décembre 2016 ne tombent pas dans l'application du titre 2. Ils seront soumis selon le cas, soit au titre 1er, soit au titre 3.

Les autres autorités administratives, même si elles ont des compétences de contrôle, d'inspection ou de poursuite de certaines infractions, ne sont pas considérées comme des autorités compétentes au sens du présent titre.

8° Le responsable du traitement: Art. 3.8 de la Directive et 3.7 du Règlement. Il s'agit de la définition classique du responsable du traitement modalisée ici en fonction du champ d'application. La question de savoir qui est le responsable du traitement est donc une question de fait et doit être analysée au cas par cas. Toutefois, la loi peut déterminer précisément qui est le responsable du traitement. Cette question n'est pas anodine et pourra souvent être confrontée à discussions. Dans le cadre pénal, plusieurs banques de données communes existent, ce qui ne simplifie pas la question. S'il y a effectivement plusieurs responsables du traitement, ceux-ci seront considérés comme co-responsables.

In bepaalde gevallen, en inzonderheid bij de federale overheidsdiensten, blijkt dat de verwerkingsverantwoordelijken in de praktijk op vrij uiteenlopende wijzen worden aangewezen. Zo wordt in bepaalde wetten bijvoorbeeld de voorzitter van de FOD, de bevoegde minister of een specifieke dienst aangewezen. Er is evenwel geen vaste regel. Het is hier ook niet de bedoeling om deze aangelegenheid te regelen, aangezien elk departement eigen bijzondere kenmerken heeft. Eenieder moet zich baseren op de definitie en er zich zo goed mogelijk naar richten.

Voor die vragen moet noodzakelijkerwijs intern een oplossing worden gevonden, want die bijzonderheden zijn er elders niet.

Het concept van verwerkingsverantwoordelijk moet worden onderscheiden van het concept van bevoegde overheid. Inderdaad, in de interne organisatie kunnen de twee begrippen verschillend zijn. Bijvoorbeeld: de federale politie is een bevoegde overheid, maar de verwerkingsverantwoordelijk kan de minister van Binnenlandse Zaken en/of Justitie zijn.

10° Ontvanger: art. 3.10 van de Richtlijn en art. 3.9 van de Verordening. Overheidsinstanties waaraan ingevolge een wettelijke verplichting persoonsgegevens worden bekendgemaakt voor het vervullen van een officiële taak, zoals belasting- of douane-overheden, financiële onderzoeksdiensten, onafhankelijke bestuurlijke overheden of financiële marktoverheden die belast zijn met de regulering van en het toezicht op de effectenmarkten, moeten niet als ontvangers worden beschouwd indien zij persoonsgegevens ontvangen die noodzakelijk zijn voor de uitvoering van een bepaald onderzoek in het algemeen belang, overeenkomstig het Unierecht of het nationale recht. Verzoeken om bekendmaking vanwege overheidsinstanties dienen in ieder geval schriftelijk te worden ingediend, gemotiveerd te worden en incidenteel te zijn, en mogen geen volledig bestand betreffen of resulteren in de koppeling van bestanden. De verwerking van persoonsgegevens door die overheidsinstanties moet stroken met de voor het doel van de verwerking toepasselijke gegevensbeschermingsregels.

11° Inbreuk op de beveiliging: Art. 3.11 van de Richtlijn en art. 3.12 van de Verordening. In de richtlijn wordt de term “data breach” gebruikt, die in het Nederlands vertaald wordt door “inbreuk in verband met persoonsgegevens” en in het Frrans “violation de données à caractère personnel”. Die vertalingen geven echter onvoldoende weer dat de inbreuk zowel opzettelijk als toevallig kan

Dans certains cas, et particulièrement les services publics fédéraux, il ressort que la désignation du responsable du traitement est assez différente selon les pratiques. On voit par exemple être désigné dans certaines lois, soit le président du SPF, soit le ministre compétent, soit un service particulier. Mais il n’y a pas de règle fixe. Et ce n’est pas l’objectif ici de régler cette question car chaque département a ses propres particularités. A chacun de se référer à la définition et de s’y prêter le plus fidèlement.

Ces questions doivent nécessairement trouver une solution en interne car ces particularités ne se retrouvent pas ailleurs.

La notion de responsable du traitement doit être différenciée de la notion d’autorité compétente. En effet, dans l’organisation interne, les deux notions peuvent être distinctes. Par exemple: la police fédérale est une autorité compétente, mais le responsable du traitement pourra être le ministre de l’Intérieur et/ou de la Justice.

10° Destinataire: art. 3.10 de la Directive et art. 3.9 du Règlement. Les autorités publiques auxquelles des données à caractère personnel sont communiquées conformément à une obligation légale pour l’exercice de leurs fonctions officielles, telles que les autorités fiscales et douanières, les cellules d’enquête financière, les autorités administratives indépendantes ou les autorités des marchés financiers responsables de la réglementation et de la surveillance des marchés de valeurs mobilières ne doivent pas être considérées comme des destinataires si elles reçoivent des données à caractère personnel qui sont nécessaires pour mener une enquête particulière dans l’intérêt général, conformément au droit de l’Union ou au droit national. Les demandes de communication adressées par les autorités publiques devraient toujours être présentées par écrit, être motivées et revêtir un caractère occasionnel, et elles ne devraient pas porter sur l’intégralité d’un fichier ni conduire à l’interconnexion de fichiers. Le traitement des données à caractère personnel par les autorités publiques en question doit être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement.

11° Brèche de sécurité: Art. 3.11 de la Directive et art. 3.12 du Règlement. La Directive utilise le terme de “data breach” traduit en français par “violation de données à caractère personnel” et en néerlandais par “inbreuk in verband met persoonsgegeven”. Mais ces traductions ne reflètent pas assez que la violation puisse être intentionnelle mais également accidentelle. On préfèrera

zijn. Daarom wordt de voorkeur eraan gegeven om de termen “inbreuk op de beveiliging” in het Nederlands en “brèche de sécurité” in het Frans te gebruiken.

12° Genetische gegevens: Art. 3.12 van de Richtlijn en art. 3.13 van de Verordening. Genetische gegevens worden gedefinieerd als persoonsgegevens met betrekking tot de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie geven over de fysiologie of de gezondheid van die natuurlijke persoon, die voortkomen uit een analyse van een biologisch monster van de betrokken persoon, met name een chromosoomanalyse, een analyse van desoxyribonucleïnezuur (DNA) of van ribonucleïnezuur (RNA) of een analyse van een ander element waarmee soortgelijke informatie kan worden verkregen. Gezien de complexe en gevoelige aard van genetische informatie kunnen het misbruik en hergebruik voor uiteenlopende doeleinden bijzonder schadelijk zijn voor de betrokken persoon. Discriminatie op grond van genetische kenmerken moet in beginsel worden verboden.

14° Gegevens over gezondheid: Art. 3.14 van de Richtlijn en art. 3.15 van de Verordening. Als persoonsgegevens over gezondheid worden beschouwd alle gegevens die betrekking hebben op de gezondheidstoestand van een betrokkene en die informatie geven over de lichamelijke of geestelijke gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst. Zij omvatten informatie over de natuurlijke persoon die is verzameld in het kader van de registratie voor of de verlening van gezondheidszorgdiensten aan die natuurlijke persoon als bedoeld in Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg, alsmede een aan een natuurlijke persoon toegekend nummer, symbool of kenmerk dat uitsluitend als identificatie van die natuurlijke persoon geldt voor gezondheidsdoeleinden, de informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel of lichaamseigen stof, met inbegrip van genetische gegevens en biologische monsters, en alle informatie over bijvoorbeeld ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de fysiologische of biomedische staat van de betrokkene, ongeacht de bron, bijvoorbeeld een arts of andere gezondheidswerker, een ziekenhuis, een medisch hulpmiddel of een in-vitro diagnostische test.

15° Toezichthoudende autoriteit: Art. 3.15 van de Richtlijn. Het betreft de in de wet aangewezen onafhankelijke toezichthoudende autoriteit. Het toezicht op de

utiliser les termes de “brèches de sécurité” en français et “inbreuk op de beveiliging” en néerlandais.

12° Données génétiques: Art. 3.12 de la Directive et art. 3.13 du Règlement. Les données génétiques sont définies comme les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d’une personne physique, qui donnent des informations uniques sur la physiologie ou l’état de santé de cette personne et qui résultent de l’analyse d’un échantillon biologique de la personne physique en question, notamment une analyse des chromosomes, de l’acide désoxyribonucléique (ADN) ou de l’acide ribonucléique (ARN), ou de l’analyse d’un autre élément permettant d’obtenir des informations équivalentes. Compte tenu du caractère complexe et sensible des informations génétiques, les conséquences engendrées par un usage abusif ou une réutilisation des données à diverses fins peuvent être particulièrement nocives pour la personne concernée. Il y a lieu d’interdire en principe toute discrimination fondée sur des caractéristiques génétiques.

14° Données concernant la santé: Art. 3.14 de la Directive et art. 3.15 du Règlement. Les données à caractère personnel concernant la santé comprennent l’ensemble des données se rapportant à l’état de santé d’une personne concernée qui révèlent des informations sur l’état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l’inscription de cette personne en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l’application des droits des patients en matière de soins de santé transfrontaliers au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l’identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l’examen d’une partie du corps ou d’une substance corporelle, y compris à partir de données génétiques et d’échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, des antécédents médicaux, un traitement clinique ou l’état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu’elle provienne par exemple d’un médecin ou d’un autre professionnel de la santé, d’un hôpital, d’un dispositif médical ou d’un test de diagnostic in vitro.

15° L’autorité de contrôle: Art. 3.15 de la Directive. Il s’agit de l’autorité de contrôle indépendante visée par la loi. Il peut y en avoir plusieurs. En ce qui concerne le

rechterlijke orde kan niet worden uitgeoefend door de toezichthoudende autoriteit bedoeld in de Verordening, maar er moet wel toezicht worden georganiseerd. In rechtsoverweging 80 van de Richtlijn is aldus het volgende vermeld: *"Hoewel deze richtlijn ook van toepassing is op de activiteiten van nationale gerechten en andere rechterlijke autoriteiten, dient de competentie van de toezichthoudende autoriteiten zich niet uit te strekken tot de verwerking van persoonsgegevens door gerechten in het kader van hun taken, teneinde de onafhankelijkheid van rechters bij de uitvoering van hun gerechtelijke taken te vrijwaren. Die vrijstelling dient beperkt te blijven tot gerechtelijke activiteiten in het kader van rechtszaken en niet te gelden voor andere activiteiten die rechters overeenkomstig het lidstatelijke recht verrichten. De lidstaten moeten ook kunnen bepalen dat de bevoegdheid van de toezichthoudende autoriteit zich niet uitstrekt tot de verwerking van persoonsgegevens door andere onafhankelijke rechterlijke autoriteiten in het kader van hun gerechtelijke taken, bijvoorbeeld het openbaar ministerie. De naleving van de regels van deze richtlijn door gerechten en andere onafhankelijke rechterlijke autoriteiten is in elk geval altijd onderworpen aan onafhankelijk toezicht in overeenstemming met artikel 8, lid 3, van het Handvest."*

16° Internationale organisatie: Art. 3.16 van de Richtlijn en art. 3.26 van de Verordening. België is, net als alle lidstaten van de Europese Unie, aangesloten bij de Internationale organisatie van Criminele Politie (Interpol). Om haar taak te kunnen uitvoeren, zorgt Interpol voor het ontvangen, opslaan en verspreiden van persoonsgegevens om bevoegde overheden bij te staan in het voorkomen en bestrijden van internationale criminaliteit. Daarom is het passend de samenwerking tussen de Europese Unie en Interpol te versterken door een efficiënte uitwisseling van persoonsgegevens te bevorderen, zulks met eerbiediging van de grondrechten en fundamentele vrijheden met betrekking tot de automatische verwerking van persoonsgegevens. Wanneer persoonsgegevens worden doorgegeven van de Unie aan Interpol, en aan landen die vertegenwoordigers naar Interpol hebben afgevaardigd, is deze wet, met name de bepalingen inzake internationale doorgiften, van toepassing.

Er komen ook nog andere internationale organisaties potentieel in aanmerking om mee samen te werken met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Voor de politiediensten is deze mogelijkheid voorzien in de wet op het politieambt: de Belgische

contrôle de l'ordre judiciaire, celui ne peut se faire par l'autorité de contrôle visée par le Règlement, mais un contrôle doit néanmoins être organisé. C'est ainsi que le considérant 80 de la Directive stipule ce qui suit: *"Bien que la présente directive s'applique également aux activités des juridictions nationales et autres autorités judiciaires, la compétence des autorités de contrôle ne devrait pas s'étendre au traitement des données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle, afin de préserver l'indépendance des juges dans l'accomplissement de leurs missions judiciaires. Il convient que cette exception soit limitée aux activités judiciaires dans le cadre d'affaires portées devant les juridictions et qu'elle ne s'applique pas aux autres activités auxquelles les juges pourraient être associés conformément au droit d'un État membre. Les États membres devraient aussi pouvoir prévoir que la compétence de l'autorité de contrôle ne s'étend pas aux traitements de données à caractère personnel effectués par d'autres autorités judiciaires indépendantes dans l'exercice de leur fonction juridictionnelle, par exemple le ministère public. En tout état de cause, le respect des règles de la présente directive par les juridictions et autres autorités judiciaires indépendantes fait toujours l'objet d'un contrôle indépendant conformément à l'article 8, paragraphe 3, de la Charte."*

16° Organisation internationale: Art. 3.16 de la Directive et art. 3.26 du Règlement. Tous les États membres de l'Union européenne sont affiliés à l'Organisation internationale de police criminelle (Interpol). Pour exécuter sa mission, Interpol reçoit, conserve et diffuse des données à caractère personnel pour aider les autorités compétentes à prévenir et à combattre la criminalité internationale. Il est dès lors approprié de renforcer la coopération entre l'Union européenne et Interpol en favorisant un échange efficace de données à caractère personnel tout en garantissant le respect des libertés et droits fondamentaux en ce qui concerne le traitement automatique des données à caractère personnel. Lorsque des données à caractère personnel sont transférées de l'Union vers Interpol, et vers des pays qui ont délégué des membres à Interpol, la présente loi, en particulier ses dispositions relatives aux transferts internationaux, s'appliquent.

D'autres organisations internationales sont également susceptibles de coopérer à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Pour les services de police, cette possibilité est prévue par la loi sur la Fonction de police: la

geïntegreerde politie kan, onder bepaalde voorwaarden uiteraard, persoonsgegevens overmaken “aan de buitenlandse politiediensten, aan de internationale organisaties voor gerechtelijke en politionele samenwerking en aan de internationale rechtshandhavingdiensten”. Tot op heden is van die mogelijkheid nog amper of geen gebruik gemaakt naast de samenwerking met Interpol, maar bepaalde organisaties komen potentieel zeker in aanmerking. Zo hebben de Verenigde Naties een “Office on Drugs and Crime” (UNODC) die onder andere analyses opstelt van criminaliteitsfenomenen, analyses die gebaat kunnen zijn met informatie van de Belgische politie. Met de VN wordt trouwens al actief samengewerkt in het kader van het Civiel Crisisbeheer, zij het tot nog toe zonder uitwisseling van persoonsgegevens. Een ander voorbeeld is de Wereldbank, een instituut voor ontwikkelingssamenwerking dat leningen verstrekt aan ontwikkelingslanden ter bestrijding van armoede. Binnen de Wereldbank is een Integrity Department actief in de strijd tegen corruptie, in het bijzonder door onderzoek te doen naar de projecten die het financiert.

17° Internationale overeenkomst: het betreft hier de overeenkomsten op het gebied van justitiële en politiële samenwerking afgesloten tussen België en een niet-lidstaat van de Europese Unie, zoals gedefinieerd in artikel 39.2 van de Richtlijn. Het betreft overeenkomsten met sensu stricto een wettelijke waarde. Memorandum of understanding, protocollen, ministeriële akkoorden, … zijn dus uitgesloten. De grensakkoorden voldoen a priori aan de algemene beginselen, aangezien daarin op praktische wijze de verplichtingen van het Kaderbesluit 2008/977 ten uitvoer worden gelegd, dat de voorganger is van Richtlijn 2016/680 die wordt omgezet in deze titel van dit wetsontwerp. Er moet evenwel geval per geval worden nagegaan of die overeenkomsten in overeenstemming zijn met de nieuwe bepalingen. Het gaat immers om een harmonisering van de beginselen die moeten worden toegepast in alle lidstaten. Niets verhindert de lidstaten echter om overeenkomsten af te sluiten met het oog op de tenuitvoerlegging van die beginselen.

Art. 27

Het betreft de materiële werkingssfeer van deze titel. Het doeleinde van de verwerking is niet alleen bepalend voor het gegeven of de bevoegde overheid optreedt, maar ook voor de toepassing van deze titel. Wanneer het doeleinde niet binnen de in deze titel bepaalde werkingssfeer valt, zijn de Verordening en de uitvoeringsmaatregelen ervan van toepassing.

Deze titel is dus beperkt tot de politiediensten, de rechterlijke overheden, en de andere overheden bedoeld

police intégrée belge peut, sous certaines conditions, transférer des données personnelles “aux services de police étrangers, aux organisations internationales de coopération judiciaire et policière et aux services de répression internationaux”. À ce jour, cette possibilité n’a pratiquement pas été utilisée, voire jamais, en plus de la coopération avec Interpol, mais certaines organisations sont certainement éligibles. Par exemple, l’ONU dispose d’un “Office des NU contre la drogue et le crime” (ONUDC) qui, entre autres, effectue des analyses sur les phénomènes criminels, analyses qui pourraient bénéficier des informations de la police belge. En outre, l’ONU coopère déjà activement dans le cadre de la gestion des crises civiles, mais sans échanger de données personnelles jusqu’à présent. Un autre exemple est la Banque mondiale, institut de coopération au développement qui accorde des prêts aux pays en développement pour lutter contre la pauvreté. Au sein de la Banque Mondiale, un service sur les questions d’Intégrité est actif dans la lutte contre la corruption, notamment en enquêtant sur les projets qu’elle finance.

17° Accord international: il s’agit ici des conventions de coopération judiciaire et policière établies entre la Belgique et un État non-membre de l’Union Européenne dont la définition est prévue à l’article 39.2 de la Directive. Il s’agit donc des conventions avec une valeur légale sensu stricto. Sont donc exclus les Memorandum of Understanding, protocoles, accords ministériels, … En ce qui concerne les accords transfrontaliers, dans la mesure où ils mettent en œuvre de manière pratique les obligations de la Décision-cadre 2008/977, prédécesseur de la Directive 2016/680 transposée par le présent titre de ce projet de loi, les principes généraux sont a priori remplis. Mais il y aura lieu de vérifier au cas par cas si ces conventions sont conformes aux nouvelles dispositions. Il s’agit en effet d’une harmonisation des principes qui doivent s’appliquer dans tous les États membres. Mais rien n’empêche chaque État membre de procéder à des accords pour mettre en œuvre ces principes.

Art. 27

Il s’agit du champ d’application matériel du présent titre. C’est la finalité du traitement qui déterminera en outre du fait que c’est l’autorité compétente qui agit, l’application du présent titre. Lorsque la finalité n’entre pas dans le champ d’application prévu au présent titre, c’est le Règlement est ses mesures d’exécution qui s’appliquent.

Le présent titre est donc limité aux services de police, aux autorités judiciaires, et aux autres autorités tels que

in het vorige artikel. Dat vloeit voort uit een restrictieve interpretatie overeenkomstig de overwegingen 10 en 11 van de Richtlijn. De Verordening is het beginsel, de Richtlijn de uitzondering. Een uitzondering moet steeds restrictief worden geïnterpreteerd. Bovendien is de Richtlijn de opvolger van het Kaderbesluit. Er moet dus zo nauw mogelijk worden aangesloten bij de daarin vastgelegde personele werkingssfeer.

Zowel de Verordening als de Richtlijn zijn van toepassing op de dossiers van de rechterlijke orde, naargelang van het doeleinde van de verwerkingen. Overweging 20 van de Verordening bepaalt het volgende: *"Hoewel de onderhavige verordening onder meer van toepassing is op de activiteiten van gerechten en andere rechterlijke autoriteiten, zouden in het Unierecht of het lidstatelijke recht de verwerkingen en verwerkingsprocedures met betrekking tot het verwerken van persoonsgegevens door gerechten en andere rechterlijke autoriteiten nader kunnen worden gespecificeerd."* Overweging 80 van de Richtlijn bepaalt het volgende: *"Hoewel deze richtlijn ook van toepassing is op de activiteiten van nationale gerechten en andere rechterlijke autoriteiten [...]."*

Dat verschilt enigszins van het vorige systeem dat werd ingevoerd bij de WVP, die ruime uitzonderingen toestond voor de rechterlijke macht en de politiële sector.

In het Gerechtelijk Wetboek of het Wetboek van Strafvordering kan evenwel worden voorzien in oplossingen die soortgelijk zijn aan de ratio legis van de WVP en die soortgelijke garanties kunnen bieden.

Overeenkomstig hetgeen hiervoor reeds werd aangegeven, werd dan ook beslist om de toepassing van deze Richtlijn te beperken tot enkel de politiediensten, de rechterlijke overheden, en de andere overheden bepaald in het vorige artikel.

Deze wet spreekt niet over openbare orde op zich omdat in de Richtlijn *"de regels [worden] vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid."*

Overweging 12 van de Richtlijn biedt opheldering:

"De door de politie of andere rechtshandhavingsautoriteiten verrichte activiteiten zijn hoofdzakelijk gericht op de voorkoming, het onderzoek, de opsporing of

définis à l'article précédent. C'est le résultat d'une interprétation restrictive, conformément aux considérants 10 et 11 de la Directive. Le Règlement est le principe, la Directive l'exception. Une exception doit toujours s'interpréter restrictivement. De plus, la Directive succède à la Décision-cadre. Il y a donc lieu de rester au plus près du champ d'application personnel qui y était faite.

Tant le Règlement que la Directive s'appliquent aux dossiers de l'ordre judiciaire en fonction de la finalité des traitements. Le considérant 20 du Règlement précise ce qui suit: *" …le présent règlement s'applique entre autres aux activités des juridictions et autres autorités judiciaires,(…) le droit de l'Union ou le droit national pourrait préciser les opérations et procédures de traitement de données à caractère personnel dans le cadre des juridictions et autres autorités judiciaires".* Le considérant 80 de la Directive précise ce qui suit: "*la présente directive s'applique également aux activités des juridictions nationales et autres autorités judiciaires…".*

Ce qui diffère un peu du système précédent mis en place dans la LVP qui permettait de larges exceptions au pouvoir judiciaire et au secteur policier.

Le Code judiciaire ou le Code d'instruction criminelle peuvent toutefois prévoir des solutions similaires à la ratio legis de la LVP et assurer des garanties similaires.

Conformément à ce qui a déjà été indiqué ci-dessus, il a donc été décidé de limiter l'application de la présente Directive aux seuls services de police, aux autorités judiciaires et aux autorités énumérées à l'article précédent.

La présente loi ne parle pas d'ordre public en tant que tel car la Directive "*établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces."*

Le considérant 12 de la Directive apporte un éclaircissement:

"Les activités menées par la police ou d'autres autorités répressives sont axées principalement sur la prévention et la détection des infractions pénales et les

de vervolging van strafbare feiten, met inbegrip van politieactiviteiten waarbij vooraf niet bekend is of een voorval al dan niet een strafbaar feit is. Tot die activiteiten behoren ook de uitoefening van gezag door het nemen van dwangmaatregelen zoals politieactiviteiten bij demonstraties, belangrijke sportevenementen en rellen. Zij omvatten ook de rechts- en ordehandhaving als een, zo nodig, aan de politie of andere rechtshandhavingsautoriteiten toevertrouwde taak ter bescherming tegen en voorkoming van gevaren voor de openbare veiligheid en voor bij wet beschermde fundamentele belangen van de samenleving, die tot strafbare feiten kunnen leiden. De lidstaten kunnen de bevoegde autoriteiten belasten met andere taken die niet noodzakelijkerwijs worden verricht met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, zodat de verwerking van persoonsgegevens voor die andere doeleinden, voor zover zij binnen het toepassingsgebied van het Unierecht valt, binnen het toepassingsgebied van Verordening (EU) 2016/679 valt.".

Voor de duidelijkheid wordt ook bevestigd dat dit, naast de taken van de gerechtelijke politie, ook de taken van bestuurlijke politie omvat. Klassiek kan verwezen worden naar de handhaving van de openbare orde. De openbare orde omvat de klassieke trilogie bestaande uit openbare rust, veiligheid en gezondheid. De openbare rust beoogt de afwezigheid van wanordelijkheden en onlusten in openbare plaatsen. De openbare veiligheid beoogt de afwezigheid van gevaarlijke toestanden voor personen en goederen en omvat o.m. de voorkoming van de criminaliteit en de bijstand van de personen in gevaar. De openbare gezondheid beoogt de afwezigheid van ziekten door de handhaving van de hygiëne en door het vrijwaren van een kwalitatief leefmilieu. Dit begrip openbare orde wordt aldus bepaald als leidraad van en maatstaf voor het optreden van de politiediensten en legt de nadruk op de noodzaak van het daadwerkelijk behoud van de openbare orde

Voorts is er het gegeven dat de politie alsmaar meer dient op te reden in het zogenaamde administratief sanctierecht waarvan de gemeentelijke administratieve sancties wetgeving (GAS-wet 24 juni 2013) het meest gekend is. Het gaat om een door of krachtens de wet vastgestelde maatregel met een repressief karakter, die door een bestuursorgaan wordt opgelegd door middel van een eenzijdige, individuele bestuurshandeling, als reactie op een inbreuk op een rechtsnorm. Dit zal met een eventuele verdere depenalisering alsmaar toenemen. We verwijzen trouwens ook naar de bestuurlijke

enquêtes et les poursuites en la matière, y compris les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non. Ces activités peuvent également comprendre l'exercice de l'autorité par l'adoption de mesures coercitives, par exemple les activités de police lors de manifestations, de grands événements sportifs et d'émeutes. Parmi ces activités figure également le maintien de l'ordre public lorsque cette mission est confiée à la police ou à d'autres autorités répressives lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société protégés par la loi, et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale. Les États membres peuvent confier aux autorités compétentes d'autres missions qui ne sont pas nécessairement menées à des fins de prévention et de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, de sorte que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application du droit de l'Union, relève du champ d'application du règlement (UE) 2016/679.".

Dans un souci de clarté, il est également confirmé que, outre les tâches de police judiciaire, cela inclut également les tâches de police administrative. Il peut traditionnellement être renvoyé au maintien de l'ordre public. L'ordre public consiste en la trilogie classique, comprenant la tranquillité, la sécurité et la santé publiques. La tranquillité publique vise l'absence de troubles et d'émeutes dans les endroits publics. La sécurité publique vise l'absence de situations dangereuses pour les personnes et les biens, et comprend entre autres la prévention de la criminalité et l'assistance aux personnes en danger. La santé publique vise l'absence de maladies en maintenant l'hygiène et en préservant un cadre de vie qualitatif. Cette notion d'ordre public est donc définie comme fil conducteur et norme pour les interventions des services de police et met l'accent sur la nécessité de maintenir effectivement l'ordre public.

Il y a ensuite le fait que la police doit de plus en plus intervenir dans le cadre des règles de sanction relevant du droit administratif dont la législation relative aux sanctions administratives communales (loi SAC du 24 juin 2013) est la plus connue. Il s'agit d'une mesure à caractère répressif fixée par ou en vertu de la loi, imposée par un organe d'administration au moyen d'un acte administratif unilatéral et individuel en réaction à la violation d'une norme juridique. Elle ne fera qu'augmenter avec une éventuelle plus grande dépénalisation. Nous renvoyons d'ailleurs également aux mesures

maatregelen die mogelijk zijn op basis van diverse bijzondere wetten zoals de Nieuwe Gemeentewet (inzonderheid artikel 130, 134-134 *sexies*, 135).

In de praktijk is er een behoefte van het verzamelen en verwerken van gegevens die vallen onder de ruime noemer van "bestuurlijke politie". Voorbeelden: persoonsgegevens over supporters, persoonsgegevens over bedelaars die zorgen voor overlast, personen actief in het digitaal landschap, portiers,….

Het is nuttig erop te wijzen dat de verwerkingen door de in deze titel bedoelde politiediensten en rechterlijke overheden voor andere doeleinden dan die bepaald in deze titel dus niet worden beoogd door die bepalingen. Op die verwerkingen is de Verordening dus rechtstreeks van toepassing, evenals de bepalingen waarin het nationale recht voorziet, inzonderheid titel 1 van deze wet.

Bijvoorbeeld, de verwerking van strikt persoonlijke administratieve gegevens, zoals het personeel van de politiediensten, is onderworpen aan de Verordening. Dgegevensbank kansspelen is ook onderworpen aan de Verordening.

Artikel 9.2 van de Richtlijn bepaalt immers in het bijzonder: *"Wanneer aan bevoegde autoriteiten krachtens het lidstatelijke recht andere taken dan die ter verwezenlijking van de in artikel 1, lid 1, omschreven doeleinden worden toevertrouwd, is Verordening (EU) 2016/679 van toepassing op verwerking voor die doeleinden, waaronder archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, tenzij de verwerking geschiedt in het kader van een activiteit die buiten de werkingssfeer van het Unierecht valt.".*

Deze titel geldt enkel voor de activiteiten die binnen het toepassingsgebied van het Europese Unierecht vallen. Activiteiten die de nationale veiligheid betreffen, activiteiten van agentschappen of eenheden die zich met nationale veiligheidsvraagstukken bezighouden en de verwerking van persoonsgegevens door de lidstaten in het kader van activiteiten die binnen de werkingssfeer van hoofdstuk 2 van titel V van het VEU vallen, worden niet als binnen het toepassingsgebied van deze titel vallende activiteiten beschouwd (overweging 14). Die bevoegdheden worden beoogd in de titels 1 en 3 van deze wet.

De door deze titel geboden bescherming ten opzichte van de verwerking van hun persoonsgegevens is van

administratives possibles sur la base de diverses lois particulières telles que la nouvelle loi communale (en particulier aux articles 130, 134-134*sexies*, 135).

Dans la pratique, il y a un besoin de collecter et de traiter les données qui tombent sous la vaste appellation de "police administrative". Exemples: données à caractère personnel sur les supporters, données à caractère personnel sur les mendiants qui sont à l'origine de nuisances, sur des personnes actives dans le paysage numérique, sur les portiers...

Il est utile de rappeler que les traitements faits par les services de police, les autorités judiciaires visés par le présent titre à des fins autres que les fins déterminées par le présent titre ne sont donc pas visés par ces dispositions. Ces traitements sont donc soumis au Règlement directement applicable ainsi qu'aux dispositions mises en œuvre par le droit national et donc notamment le titre 1er de la présente loi.

Par exemple, les traitements de données à caractère personnel strictement administratifs tels que les ressources humaines des services de police, sont soumis au Règlement. La banque de donnée relative aux jeux de hasard est également soumise au Règlement.

En effet, l'article 9.2 de la Directive prévoit notamment: *"Lorsque les autorités compétentes sont chargées par le droit d'un État membre d'exécuter des missions autres que celles exécutées pour les finalités énoncées à l'article 1er, paragraphe 1er, le règlement (UE) 2016/679 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.".*

Le présent titre ne s'applique que pour les activités relevant du champ d'application du droit de l'Union européenne. Les activités relatives à la sécurité nationale, les activités des agences ou des services responsables des questions de sécurité nationale et le traitement de données à caractère personnel par les États membres dans le cadre d'activités relevant du champ d'application du titre V, chapitre 2, du TUE ne sont pas considérées comme des activités relevant du champ d'application du présent titre (considérant 14). Ces compétences sont visées par les titres 1 et 3 de la présente loi.

La protection conférée par le présent titre s'applique aux personnes physiques, indépendamment de leur

toepassing op natuurlijke personen, ongeacht hun nationaliteit of verblijfplaats.

HOOFDSTUK II

Beginselen van de verwerking

Art. 28

(Artikel 4 van de Richtlijn)

Iedere verwerking van persoonsgegevens dient ten aanzien van de natuurlijke personen in kwestie rechtmatig, behoorlijk en transparant te zijn en uitsluitend te geschieden met het oog op specifieke, bij wet vastgestelde doeleinden. Dit belet als zodanig niet dat de rechtshandhavingsinstanties activiteiten verrichten zoals onderzoeken, met of zonder bijzonder opsporingsmethoden, of videobewaking. Die activiteiten kunnen worden verricht met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, voor zover de activiteiten bij wet zijn vastgelegd en in een democratische samenleving, met inachtneming van de legitieme belangen van de betrokken natuurlijke persoon, een noodzakelijke en evenredige maatregel vormen.

Natuurlijke personen moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten in verband met de verwerking van hun persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot de verwerking kunnen uitoefenen.

Met name dienen de specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt expliciet en legitiem te zijn, en te worden vastgesteld op het ogenblik dat de persoonsgegevens worden verzameld. Het punt waarop de Richtlijn en de Verordening verschillen, is dat er geen verplichte transparantie is. Dat houdt verband met de mogelijke uitzonderingen voor het recht op informatie.

De persoonsgegevens moeten toereikend en ter zake dienend zijn voor de doeleinden waarvoor zij worden verwerkt. Meer bepaald moet ervoor worden gezorgd dat niet bovenmatig veel gegevens worden verzameld en dat zij niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor zij worden verwerkt. Persoonsgegevens mogen alleen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere manier kan worden verwezenlijkt.

nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel.

CHAPITRE II

Principes de traitement

Art. 28

(Article 4 de la Directive)

Tout traitement de données à caractère personnel doit être licite, loyal et transparent à l'égard des personnes physiques concernées et n'être effectué qu'aux fins spécifiques fixées par la loi. Cela n'interdit pas en soi aux autorités répressives de mener des activités telles que des enquêtes, avec ou sans méthodes particulières, ou de la vidéosurveillance. Ces activités peuvent être menées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, pour autant qu'elles soient déterminées par la loi et qu'elles constituent une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des intérêts légitimes de la personne physique concernée.

Les personnes physiques devraient être informées des risques, règles, garanties et droits en ce qui concerne le traitement de données à caractère personnel les concernant et des modalités d'exercice de leurs droits par rapport au traitement.

En particulier, les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées au moment de la collecte des données à caractère personnel. Là où diffère la Directive et le Règlement c'est qu'il n'y a pas d'obligation de transparence. Ce qui est en lien avec les exceptions possibles pour le droit à l'information.

Les données à caractère personnel devraient être adéquates et pertinentes au regard des finalités pour lesquelles elles sont traitées. Il convient notamment de veiller à ce que les données à caractère personnel collectées ne soient pas excessives, ni conservées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens.

Om ervoor te zorgen dat gegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan.

Om de veiligheid in verband met de verwerking te handhaven en te voorkomen dat met een verwerking inbreuk wordt gemaakt op deze Richtlijn, dienen persoonsgegevens te worden verwerkt met inachtneming van een passend niveau van beveiliging en vertrouwelijkheid, wat onder meer inhoudt dat ongeoorloofde toegang tot of het gebruik van persoonsgegevens en de voor de verwerking gebruikte apparatuur wordt voorkomen, en dit met inachtneming van de stand van de techniek, de uitvoeringskosten in verband met de risico's en de aard van de te beschermen persoonsgegevens.

De beginselen zijn grotendeels overgenomen uit richtlijn 95/46, wat betekent dat het Belgisch recht met enkele aanpassingen voldoet aan de Europese vereisten:

— Finaliteitsbeginsel (art. 4, § 1, 2°, WVP): welbepaald, uitdrukkelijk omschreven en gerechtvaardigd;

— Eerlijkheids- en rechtmatigheidsbeginsel (art. 4, § 1, 1°, WVP);

— Beginsel van verenigbare verdere verwerking (art. 4, § 1, 2°, WVP);

— Nauwkeurige, toereikende en bijgewerkte gegevens (art. 4, § 1, 4°, WVP);

— Ter zake dienende en niet-overmatige gegevens (art. 4, § 1, 3°, WVP);

— Bewaringstermijn (art. 4, § 1, 5°, WVP).

Er is hier geen verplichte transparantie (punt a), wat verantwoord is in het licht van de doeleinden. De uitzonderingen op het recht op informatie vloeien daaruit voort.

Art. 29

De tekst verduidelijkt dat het gaat om verdere verwerking. Een verdere verwerking is een verwerking door dezelfde of een andere verwerkingsverantwoordelijke voor doeleinde vermeld in artikel 27 dat verschilt van de doeleinden waarvoor de gegevens werden verzameld of voor een ander doeleinde dat niet onder de doeleinden vermeld in artikel 27 valt.

Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais doivent être fixés par le responsable du traitement en vue de leur effacement ou d'un examen périodique.

Afin de préserver la sécurité entourant le traitement et de prévenir tout traitement effectué en violation de la présente Directive, il convient que les données à caractère personnel soient traitées de manière à garantir un niveau de sécurité et de confidentialité approprié, notamment en empêchant l'accès non autorisé à ces données et à l'équipement servant à leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement, et à tenir compte de l'état des connaissances et de la technologie disponible, des coûts de mise en œuvre au regard des risques et de la nature des données à caractère personnel à protéger.

Les principes sont, en grande partie, repris de la directive 95/46 ce qui signifie que le droit belge répond aux exigences européennes, moyennant quelques adaptations:

— Principe de finalité (art. 4, § 1er, 2°, LVP): déterminé, explicite et légitime;

— Principe de loyauté et de licéité (art. 4, § 1er, 1°, LVP);

— Principe de traitement ultérieur compatible (art. 4, § 1er, 2°, LVP);

— Données exactes, adéquates et mises à jour (art. 4, § 1er, 4°, LVP);

— Données pertinentes et non excessives (art.4, § 1er, 3°, LVP);

— Durée de conservation (art. 4, § 1er, 5°, LVP).

Il n'y a ici pas d'obligation de transparence (point a), ce qui se justifie par rapport aux finalités. De là découlent les exceptions au droit à l'information.

Art. 29

Le texte précise qu'il s'agit de traitement ultérieur. Un traitement ultérieur est un traitement par le même ou par un autre responsable du traitement, pour l'une des finalités énoncées à l'article 27, autre que celles pour lesquelles les données ont été collectées ou pour une autre finalité qui n'est pas visée par l'article 27.

Artikel 4.2 van de Richtlijn voorziet: "*verwerking door dezelfde of een andere verwerkingsverantwoordelijke voor een doel opgesomd in artikel 1, lid 1, dan dat waarvoor de persoonsgegevens worden verzameld, is toegelaten voor zover:*

a) de verwerkingsverantwoordelijke overeenkomstig het Unierecht of het lidstatelijke recht gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en

b) de verwerking noodzakelijk is *en in verhouding staat tot dat andere doel overeenkomstig het Unierecht of het lidstatelijke recht."*

(Artikel 9 van de Richtlijn)

De door de bevoegde overheden verzamelde gegevens mogen niet worden verwerkt voor andere doeleinden deze voorzien in artikel 27, tenzij die verwerking krachtens, de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst is toegestaan.

Indien deze verdere verwerking gebeurt door een bestemmeling in een andere lidstaat van de Europese Unie, dan dient deze verdere verwerking te zijn toegestaan volgens het nationale recht van die lidstaat.

Gebeurt de verdere verwerking door een bestemmeling buiten de Europese Unie die ontvanger is van de persoonsgegevens overgemaakt door een Belgische bevoegde overheid, dan dient deze verdere verwerking te zijn toegestaan door het rechtsinstrument dat de juridische basis vormt voor de overmaking van de betrokken persoonsgegevens aan deze bestemmeling.

Wanneer persoonsgegevens voor een ander doeleinde worden verwerkt dan de in deze titel vastgelegde doeleinden, is de Verordening van toepassing, tenzij de verwerking geschiedt in het kader van een activiteit die buiten de werkingssfeer van het Unierecht valt.

Er mogen geen extra specifieke voorwaarden betreffende de bescherming van persoonsgegevens worden opgelegd voor de overmaking van gegevens aan ontvangers in de andere lidstaten van de Europese Unie dan de voorwaarden die kunnen worden opgelegd in het geval van een vergelijkbare overmaking van persoonsgegevens aan ontvangers binnen België. Er moet benadrukt worden dat het hier enkel voorwaarden betreft die betrekking hebben op de bescherming van persoonsgegevens, aangezien vermoed wordt dat alle landen binnen de Europese Unie dezelfde hoge standaarden inzake gegevensbescherming hanteren.

L'article 4.2 de la Directive prévoit: "*le traitement, par le même ou par un autre responsable du traitement, pour l'une des finalités énoncées à l'article 1er, paragraphe 1er, autre que celles pour lesquelles les données ont été collectées, est autorisé à condition que:*

a) le responsable du traitement soit autorisé à traiter ces données à caractère personnel pour une telle finalité conformément au droit de l'Union ou au droit d'un État membre; et

b) le traitement soit nécessaire et proportionné à cette autre finalité conformément au droit de l'Union ou au droit d'un État membre."

(Article 9 de la Directive)

Les données à caractère personnel collectées par les autorités compétentes ne peuvent être traitées à des fins autres que celles prévues à l'article 27, à moins qu'un tel traitement ne soit autorisé par la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international.

Si ce traitement ultérieur est effectué par un destinataire dans un autre État membre de l'Union européenne, ce traitement ultérieur doit être autorisé en vertu de la législation nationale de cet État membre.

En cas de traitement ultérieur par un destinataire extérieur à l'Union européenne destinataire des données personnelles transmises par une autorité compétente belge, ce traitement ultérieur doit être autorisé par l'instrument juridique constituant la base juridique du transfert des données à caractère personnel concernées à ce destinataire.

Lorsque des données à caractère personnel sont traitées pour une autre fin que celle déterminée par le présent titre, le Règlement s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.

Aucune condition particulière supplémentaire en ce qui concerne la protection des données personnelles peuvent être imposées pour le transfert de données à des destinataires dans d'autres États membres de l'Union européenne autre que les conditions qui peuvent être imposées en cas d'un transfert similaire des données personnelles à des destinataires en Belgique. Il convient de souligner que cela ne concerne que les conditions relatives à la protection des données à caractère personnel, car il est supposé que tous les pays de l'Union européenne appliquent les mêmes normes élevées de protection des données. Cependant,

Andere voorwaarden, die geen betrekking hebben op de bescherming van persoonsgegevens, mogen echter wel nog worden opgelegd. Zo heeft het verbod om tussen de politiediensten uitgewisselde persoonsgegevens niet als bewijs in strafzaken te gebruiken ("*for police use only*") zonder toestemming daartoe van het openbaar ministerie niet als doel om persoonsgegevens te beschermen vanuit een privacy-optiek: deze voorwaarde wordt opgelegd om redenen van politiële en gerechtelijke samenwerking en de betrouwbaarheid van het bewijs. Een dergelijke voorwaarde kan dus nog steeds opgelegd worden bij de uitwisseling van persoonsgegevens tussen politiediensten binnen de Europese Unie.

De doelstelling van deze voorwaarde is het waarborgen van het vrije verkeer van persoonsgegevens binnen de Europese Unie zoals voorzien in artikel 1.3 van de Verordening en artikel 3 van deze wet en dit wetsontwerp heeft niet de bedoeling om ruimer te zijn dan de Richtlijn. Andere voorwaarden dan deze die van toepassing zijn op gelijkaardige doorgiften van gegevens binnen het Belgisch grondgebied zijn niet aanvaardbaar voor de doorgiften van bevoegde overheden naar ontvangers van andere lidstaten van de Europese Unie.

Art. 30

Er worden passende termijnen vastgelegd voor het wissen van persoonsgegevens of bij het verstrijken van de vastgelegde termijn of voor een periodieke evaluatie van de noodzaak van de opslag of het wissen van persoonsgegevens. De naleving van die termijnen wordt met procedurele maatregelen gewaarborgd.

Het betreft overweging 26, waarin staat dat de verwerkingsverantwoordelijke een maximale termijn dient vast te stellen, hoewel dat niet is weergegeven in de tekst van artikel 5 van de Richtlijn. De maximale duur kan een aantal jaren zijn, maar ook het optreden van een factor, zoals het overlijden van de betrokken persoon.

Deze bepaling wordt thans reeds toegepast (zie artikel 4 WVP). Er wordt dus verder gegaan dan in artikel 5 van de Richtlijn terwijl, deze bepaling niet als dusdanig in de Verordening bestaat.

Er wordt eveneens voorzien dat er bij het verlopen van de termijn een analyse uitgevoerd wordt op basis van de proportionaliteits- en noodzaelijkheidscriteria om te bepalen of de bewaring nog nodig is. Indien blijkt dat de bewaring nog nodig en proportioneel is, dan wordt het gegeven bewaard gedurende een nieuwe termijn. De wettelijke grondslag moet echter de maximumtermijn

d'autres conditions qui ne concernent pas la protection des données à caractère personnel peuvent encore être imposées. Par exemple, l'interdiction de l'utilisation de données personnelles échangées entre les services de police comme preuve en matière pénale ("*for police use only*") sans le consentement du procureur général, ne vise pas à protéger les données à caractère personnel du point de vue de la vie privée: cette condition est imposée pour des raisons de la coopération policière et judiciaire et la fiabilité des preuves. Une telle condition peut donc encore être imposée à l'échange de données personnelles entre les forces de police au sein de l'Union européenne.

L'objectif de cette condition est de garantir la libre circulation des données à caractère personnel au sein de l'Union européenne, tel que le prévoit l'article 1er.3 du Règlement et l'article 3 de la présente loi et le présent projet de loi n'a pas l'intention d'être plus large que la Directive. Des conditions différentes de celles applicables aux transferts de données similaires à l'intérieur du territoire belge ne sont pas acceptables pour le transferts par des autorités compétentes vers des destinataires d'autres États membres de l'Union européenne.

Art. 30

Des délais appropriés sont fixés pour l'effacement des données à caractère personnel à l'échéance du délai fixé ou pour la vérification régulière de la nécessité de conserver ou effacer les données à caractère personnel. Des règles procédurales garantissent le respect de ces délais.

Il s'agit du considérant 26 qui stipule que le responsable du traitement devrait fixer un délai maximum même si ce n'est pas dans le texte de l'article 5 de la Directive. La durée maximale peut être un nombre d'année, mais également l'apparition d'un facteur, tel que le décès de la personne concernée.

Cette disposition est déjà appliquée actuellement (voir article 4 LVP). On va donc plus loin que l'art. 5 de la directive, tandis que cette disposition n'existe pas comme telle dans le Règlement.

Il est également prévu qu'à l'échéance du délai une analyse soit effectuée sur base de critères de proportionnalité et de nécessité afin de déterminer si la conservation est encore nécessaire. S'il s'avère que la conservation est encore nécessaire et proportionnelle, la donnée est conservée pour un nouveau délai. La base légale doit néanmoins prévoir le délai maximum dans

voorzien waarbinnen de gegevens bewaard kunnen worden, zelfs indien er een analyse uitgevoerd werd.

Zoals de Raad van State aangeeft kan deze wet geen bepalingen beslissen die zouden moeten voorzien worden in een Europese of internationaalrechtelijke bepaling. De tekst wordt dus in die zin aangepast.

Art. 31

(Artikel 6 van de Richtlijn)

Het is inherent aan de verwerking van persoonsgegevens op het gebied van justitiële samenwerking in strafzaken en politiële samenwerking dat persoonsgegevens betreffende verschillende categorieën van betrokkenen worden verwerkt. Daarom moet in voorkomend geval en zoveel mogelijk een onderscheid worden gemaakt tussen persoonsgegevens betreffende verschillende categorieën van betrokkenen, zoals verdachten, personen die zijn veroordeeld wegens een strafbaar feit, slachtoffers en derden, zoals getuigen, personen die over relevante informatie beschikken of personen die contact hebben of banden onderhouden met verdachten en veroordeelde misdadigers. Dit mag geen afbreuk doen aan de toepassing van het recht op het vermoeden van onschuld zoals gewaarborgd bij het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag voor de Rechten van de mens zoals uitgelegd in de rechtspraak van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens.

De verwerking van persoonsgegevens op het gebied van justitiële samenwerking in strafzaken en politiële samenwerking omvat noodzakelijkerwijs de verwerking van persoonsgegevens over verschillende categorieën van betrokkenen. Het is daarom van belang om, waar passend en voor zover mogelijk, een duidelijk onderscheid te maken tussen de persoonsgegevens van verschillende categorieën betrokkenen, zoals de verdachten, de personen die zijn veroordeeld voor een strafbaar feit, de slachtoffers en andere partijen, zoals getuigen, mensen die nuttige informatie of contacten hebben, en de handlangers van verdachte personen en veroordeelde criminelen.

De tenuitvoerlegging van de bepalingen van de Richtlijn vormt een uitdaging voor de lidstaten en dit is niet aan de aandacht van het Europees Parlement en de Raad ontsnapt. Daarom, als het artikel het doel bepaalt waarnaar we moeten streven, moet dit doel zoveel als mogelijk worden bereikt. Dit biedt onder meer

lequel ces données peuvent être conservées même si une analyse a été effectuée.

Comme le souligne le Conseil d'État, la présente loi ne peut déterminer des dispositions qu'il y a lieu de prévoir dans un dispositif légal européen ou international. Le texte est donc adapté en ce sens.

Art. 31

(Article 6 de la Directive)

Le traitement des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière implique nécessairement le traitement de données à caractère personnel concernant différentes catégories de personnes concernées. Il importe dès lors d'établir une distinction claire, le cas échéant et dans la mesure du possible, entre les données à caractère personnel de différentes catégories de personnes concernées, telles que: les suspects; les personnes reconnues coupables d'une infraction pénale; les victimes et les autres parties, tels que les témoins; les personnes détenant des informations ou des contacts utiles; et les complices de personnes soupçonnées et de criminels condamnés. Cela ne devrait pas empêcher l'application du droit à la présomption d'innocence garanti par la Charte des droits fondamentaux de l'Union européenne et par la Convention européenne des droits de l'homme, telles qu'elles ont été interprétées respectivement par la Cour de justice de l'Union européenne et par la Cour européenne des droits de l'homme dans leur jurisprudence.

Le traitement des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière implique nécessairement le traitement de données à caractère personnel concernant différentes catégories de personnes concernées. Il importe dès lors d'établir une distinction claire, le cas échéant, et dans la mesure du possible, entre les données à caractère personnel de différentes catégories de personnes concernées, telles que les suspects, les personnes reconnues coupables d'une infraction pénale, les victimes et les autres parties, tels que les témoins, les personnes détenant des informations ou des contacts utiles, et les complices de personnes soupçonnées et de criminels condamnés.

La mise en œuvre des dispositions de la Directive constitue un défi pour les États membres et cela n'a pas échappé au Parlement et au Conseil européens. Par conséquent, si l'article fixe l'objectif vers lequel il faut tendre, il doit néanmoins être atteint dans la mesure du possible. Il laisse ainsi, entre autres, la possibilité

de mogelijkheid aan de betrokken diensten om zich geleidelijk aan aan te passen om het beoogde doel te bereiken. Het is niet omdat iets vandaag niet meteen mogelijk is dat dit morgen ook niet het geval zal zijn.

Art. 32

(Artikel 8.1 van de Richtlijn)

Het betreft de toepassing in overeenstemming met artikel 22 van de Grondwet waarin is bepaald dat "*Ieder recht heeft op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald. De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht.*"

De Privacycommissie heeft meerdere adviezen in die zin uitgebracht:

— Advies 13/2006 betreffende de elektronische handtekening in het informatiesysteem Phenix;

— Advies 11/2004 betreffende het ontwerp van wet Phenix;

— Advies 42/1997 betreffende de verspreiding van rechterlijke beslissingen.

Zonder afbreuk te doen aan het vermoeden van onschuld is het in een voortdurende stroom van informatievergaring niet altijd mogelijk om de juistheid hiervan na te gaan. Er kan bijvoorbeeld naar aanleiding van een aangifte van meerdere getuigen een ernstig vermoeden zijn dat iemand in aanmerking komt als verdachte van een misdrijf (bv. zedendelict) wat dan later weer na verder onderzoek kan worden weerlegd. Personen die aangeven slachtoffer of getuige te zijn van een misdrijf kunnen bij verder onderzoek ook in aanmerking komen als verdachte (bv. dossiers van wederzijdse slagen en verwondingen, tipgever blijkt effectief medeverdachte te zijn, boekhouder die geen besef had dat hij zich schuldig maken aan een misdrijf, melder van een brand komt in aanmerking voor brandstichting/oplichting van de verzekering, bij verkeersongeval is niet altijd duidelijk wie finaal verdachte zal zijn van de onopzettelijke slagen…). Om die reden kan het opdelen van de persoonsgegevens in verschillende categorieën voor de politiediensten geen resultaatverbintenis zijn maar de bevoegde overheden moeten zo goed mogelijk dit doel trachten te bereiken.

Er wordt eveneens voorzien dat de bevoegde overheden alle redelijke maatregelen nemen om te verzekeren dat de persoonsgegevens die onjuist, onvolledig of niet

aux services concernés de s'adapter progressivement pour atteindre l'objectif prévu. Ce n'est donc pas parce qu'une chose n'est pas immédiatement possible aujourd'hui qu'elle ne le sera pas demain.

Art. 32

(Article 8.1 de la Directive)

Il s'agit là de l'application conforme de l'article 22 de la Constitution qui stipule que "*Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit.*"

Plusieurs avis de la Commission vie privée ont été émis en ce sens:

— Avis 13/2006 relatif à la signature électronique dans le système Phénix;

— Avis 11/2004 relatif au projet de loi Phénix;

— Avis 42/1997 relatif à la diffusion des décisions juridictionnelles.

Sans préjudice de la présomption d'innocence, il n'est pas toujours possible de vérifier l'exactitude des données dans un flux continu de collecte d'informations. Par exemple, suite aux déclarations de témoins multiples, il y a des soupçons sérieux qu'une personne soit considérée comme suspecte d'un crime (par exemple, une infraction sexuelle) alors que ces soupçons, après une enquête plus approfondie peuvent plus tard être réfutées. Des personnes indiquées comme victime ou témoin d'un crime peuvent, après des recherches approfondies, aussi être considérées comme un suspect (par exemple, dossiers d'agression mutuelle, un indicateur qui semble le suspect effectif, un comptable qui ne se rend pas compte qu'il est coupable d'un crime pour incendie criminel/escroquerie à l'assurance, un accident de la route n'est pas toujours clair qui est suspect des coups et blessures accidentels ...). Pour cette raison, diviser les données personnelles en différentes catégories pour les services de police ne peut pas être une obligation de résultat, mais les autorités compétentes doivent tendre à cet objectif dans la mesure du possible.

Il est également prévu que les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui

meer actueel zijn, niet overgemaakt worden of ter beschikking gesteld worden. Hiertoe gaat elke bevoegde overheid, in de mate van het mogelijke, de kwaliteit van de persoonsgegevens na vooraleer ze overgemaakt worden ter beschikking gesteld worden. Indien na de verificatie de toezichthoudende overheid merkt dat de overgemaakte of ter beschikking gestelde gegevens niet juist of onvolledig zijn, dan informeert ze onmiddellijk de bestemmeling van die gegevens.

Art. 33

Een verwerking van persoonsgegevens geldt slechts als rechtmatig indien zij noodzakelijk is om een bevoegde overheid in staat te stellen op grond van het Unierecht of het Belgisch recht een taak in het algemeen belang uit te voeren met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Die activiteiten dienen de bescherming van vitale belangen van de betrokkene te omvatten. Het uitvoeren van de bij wet aan de bevoegde overheden toegewezen taken in verband met de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten, stelt hen in staat van natuurlijke personen te verlangen of te eisen dat zij aan de gedane verzoeken gevolg geven. In dit geval mag de toestemming van de betrokkene als omschreven in de Verordening geen rechtsgrond vormen voor de verwerking van persoonsgegevens door bevoegde overheden. Wanneer van de betrokkene wordt verlangd dat hij aan een wettelijke verplichting voldoet, heeft hij geen echte, vrije keuze, en kan zijn reactie derhalve niet als een spontane blijk van zijn wil worden uitgelegd. Dit mag niet beletten om in de wetgeving te bepalen dat de betrokkene kan instemmen met de verwerking van zijn persoonsgegevens voor de doeleinden van deze richtlijn, zoals DNA-tests in strafrechtelijke onderzoeken of het toezicht, met behulp van elektronische enkelbanden, op de locatie waar de betrokkene zich bevindt met het oog op de tenuitvoerlegging van straffen.

In artikel 8.2 van de Richtlijn is het moeilijk het onderscheid te maken tussen de verwerkingsdoeleinden en de finaliteiten van de verwerking, reden waarvoor dat we alleen de verplichting om de doeleinden te vermelden behouden .

Onder “wet” wordt een wetgevende maatregel verstaan. Dit betekent niet noodzakelijk dat een wetgevende handeling goedgekeurd door het parlement nodig is, onverminderd de constitutionele vereisten. Dit recht, die rechtsgrond of die wetgevende maatregel moet evenwel

sont inexactes, incomplètes ou ne sont plus à jour ne soient pas transmises ou mises à disposition. À cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition. Si, à l’issue de sa vérification, l’autorité de contrôle s’aperçoit que des données transmises ou mises à disposition, ne sont plus exactes ou complètes, elle en informe sans délai le destinataire de ces données.

Art. 33

Pour être licite, le traitement des données à caractère personnel doit être nécessaire à l’exécution d’une mission d’intérêt général par une autorité compétente, fondée sur le droit de l’Union européenne ou le droit belge, à des fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière ou d’exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Ces activités devraient couvrir la protection des intérêts vitaux de la personne concernée. Dans le cadre de l’exécution des missions de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière ou d’exécution de sanctions pénales qui leur sont confiées de manière institutionnelle par la loi, les autorités compétentes peuvent demander ou ordonner aux personnes physiques de donner suite aux demandes qui leur sont adressées. Dans ce cas, le consentement de la personne concernée, au sens du Règlement, ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes. Lorsqu’elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d’une véritable liberté de choix; sa réaction ne pourrait dès lors être considérée comme une manifestation libre de sa volonté. Cela ne devrait pas empêcher de prévoir par la loi que la personne concernée peut consentir au traitement de données à caractère personnel la concernant aux fins de la présente directive, par exemple pour des tests ADN dans des enquêtes pénales ou le suivi de sa localisation au moyen de dispositifs électroniques dans le cadre de l’exécution de sanctions pénales.

A l’article 8.2 de la Directive, il existe une difficulté de cerner la différence entre les objectifs et les finalités du traitement, raison pour laquelle on ne maintien que l’obligation de mentionner les finalités du traitement.

On entend par “loi”, une mesure législative. Cela ne signifie pas nécessairement que l’adoption d’un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l’ordre constitutionnel. Cependant, ce droit, cette base juridique ou

duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is, zoals vereist door de rechtspraak van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens.

Wanneer het op de overmakende bevoegde overheid toepasselijke Unierecht of recht voorziet in specifieke voorwaarden die in specifieke omstandigheden op de verwerking van persoonsgegevens van toepassing zijn, zoals het gebruik van behandelingscodes, dient de overmakende bevoegde overheid de ontvanger van die persoonsgegevens van die voorwaarden en van de noodzaak tot eerbiediging ervan in kennis te stellen. Die voorwaarden kunnen bijvoorbeeld voorzien in een verbod om de persoonsgegevens aan anderen door te zenden, of deze voor andere doeleinden te gebruiken dan deze waarvoor zij aan de ontvanger werden doorgezonden, of de betrokkene niet in kennis te stellen in geval van een beperking van het recht op informatie zonder de voorafgaande toestemming van de overmakende bevoegde overheid. Die verplichtingen dienen ook te gelden voor doorgiften van de overmakende bevoegde overheid aan ontvangers in derde landen of internationale organisaties. De overmakende bevoegde overheid mag geen andere voorwaarden toepassen op ontvangers in andere lidstaten van de Europese Unie dan die welke van toepassing zijn op vergelijkbare doorzending van gegevens binnen de staat zelf.

De wettelijke mogelijkheid tot verwerking kan eveneens voortvloeien uit een internationale overeenkomst, die dan de elementen voorzien in paragraaf 2 moet bevatten.

Art. 34

(Artikel 10 van de Richtlijn)

Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden verdienen specifieke bescherming aangezien de context van de verwerking ervan aanzienlijke risico's voor de grondrechten en fundamentele vrijheden kan meebrengen. Die persoonsgegevens omvatten de persoonsgegevens waaruit ras of etnische afkomst blijkt, waarbij het gebruik van de term "ras" niet impliceert dat theorieën worden aanvaard die erop gericht zijn vast te stellen dat er verschillende menselijke rassen bestaan. Dergelijke persoonsgegevens mogen slechts worden verwerkt indien bij de verwerking passende bij wet vastgelegde waarborgen gelden wat de rechten en

cette mesure législative devrait être clair et précis et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme.

Lorsque le droit de l'Union ou le droit applicable à l'autorité compétente qui transmet les données soumet le traitement de données à caractère personnel à des conditions spécifiques applicables dans certaines situations particulières, telles que l'utilisation de codes de traitement, l'autorité compétente qui transmet les données devrait informer le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter. Ces conditions pourraient, par exemple, comprendre une interdiction de transmission ultérieure des données à caractère personnel à autrui, une interdiction d'utilisation desdites données à des fins autres que celles pour lesquelles elles ont été transmises au destinataire, ou une interdiction d'informer la personne concernée lorsque le droit à l'information est limité en l'absence d'autorisation préalable de l'autorité compétente qui transmet les données. Ces obligations devraient également s'appliquer aux transferts de données par l'autorité compétente qui transmet les données à des destinataires dans des pays tiers ou des organisations internationales. L'autorité compétente qui transmet les données ne doit pas appliquer aux destinataires dans les autres États membres de l'Union européenne des conditions différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État lui-même.

La possibilité légale de traitement peut également résulter d'un accord international, qui doit alors contenir les éléments prévus au paragraphe 2.

Art. 34

(Article 10 de la Directive)

Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits. Ces données à caractère personnel comprennent les données à caractère personnel qui révèlent l'origine raciale ou ethnique, étant entendu que l'utilisation de l'expression "origine raciale" n'implique pas que l'adhérence à des théories tendant à établir l'existence de races humaines distinctes. Ces données à caractère personnel ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne s'accompagne de

vrijheden van de betrokkene betreft en zij is toegelaten in bij wet bepaalde gevallen; bij ontstentenis van zulke wet, indien de verwerking noodzakelijk is om de vitale belangen van de betrokkene of een andere persoon te beschermen; of indien de verwerking betrekking heeft op gegevens die de betrokkene zelf kennelijk openbaar heeft gemaakt. Passende waarborgen voor de rechten en vrijheden van de betrokkene kunnen bijvoorbeeld inhouden dat die gegevens enkel mogen worden verzameld in samenhang met andere gegevens over de natuurlijke persoon in kwestie, dat de verzamelde gegevens afdoende kunnen worden beveiligd, dat strengere regels gelden voor de toegang van het personeel van de bevoegde overheid tot de gegevens, en dat de doorzending van die gegevens wordt verboden. De verwerking van die gegevens dient ook bij wet toegelaten te zijn wanneer de betrokkene uitdrukkelijk heeft toegestemd met de verwerking die een ingrijpende inbreuk vormt op zijn privacy. De toestemming van de betrokkene op zich mag evenwel geen rechtsgrond vormen voor de verwerking van die gevoelige persoonsgegevens door bevoegde overheden.

De wet in de brede zin kan gepaste bijkomende garanties voorzien.

Art. 35

(Artikel 11 van de Richtlijn)

De betrokkene dient het recht te hebben niet te worden onderworpen aan een besluit waaraan voor hem negatieve rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking die bedoeld is om een beeld te krijgen van bepaalde van zijn persoonlijke aspecten. Voor die verwerking moeten in ieder geval passende waarborgen worden geboden, waaronder specifieke voorlichting van de betrokkene en het recht op menselijke tussenkomst, met name om zijn standpunt kenbaar te maken, om uitleg over het genomen besluit te krijgen na een dergelijke beoordeling en om op te komen tegen het besluit. Profilering die leidt tot discriminatie van natuurlijke personen op grond van persoonsgegevens die door de aard ervan bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, is verboden overeenkomstig de bepalingen van de artikelen 21 en 52 van het Handvest van de grondrechten van de Europese Unie.

garanties appropriées pour les droits et libertés de la personne concernée fixées par la loi et ne soit permis dans des cas autorisés par la loi; lorsqu'il n'est pas déjà autorisé par une telle loi, qu'il ne soit nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne; ou qu'il ne porte sur des données manifestement rendues publiques par la personne concernée. Des garanties appropriées pour les droits et libertés de la personne concernée pourraient comprendre la possibilité de ne collecter ces données qu'en rapport avec d'autres données relatives à la personne physique concernée, la possibilité de sécuriser les données collectées de manière adéquate, des règles plus strictes pour l'accès du personnel de l'autorité compétente aux données et l'interdiction de la transmission de ces données. Il convient également que le traitement de pareilles données soit autorisé par la loi lorsque la personne concernée a expressément marqué son accord au traitement qui est particulièrement intrusif pour elle. Toutefois, l'accord de la personne concernée ne devrait pas constituer en soi une base juridique pour le traitement de ces données à caractère personnel sensibles par les autorités compétentes.

La loi au sens large peut prévoir des garanties supplémentaires adéquates.

Art. 35

(Article 11 de la Directive)

La personne concernée devrait avoir le droit de ne pas faire l'objet d'une décision impliquant l'évaluation de certains aspects personnels la concernant, qui est prise sur le seul fondement d'un traitement automatisé et qui produit des effets juridiques défavorables la concernant ou qui l'affecte de manière significative. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, y compris la fourniture d'informations spécifiques à la personne concernée et le droit d'obtenir une intervention humaine, en particulier d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision. Tout profilage qui entraîne une discrimination à l'égard de personnes physiques sur la base de données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux, sont interdits en application des conditions établies aux articles 21 et 52 de la Charte des droits fondamentaux de l'Union européenne.

HOOFDSTUK III

Rechten van de betrokkene

Net als de basisvoorwaarden worden de rechten die voortvloeien uit richtlijn 95/46 overgenomen en versterkt.

Wat de Verordening betreft, wordt in artikel 23 de mogelijkheid geboden om in beperkingen te voorzien voor inzonderheid de gerechtelijke procedures (alsook de nationale veiligheid, de defensie, de openbare veiligheid, enz.). De Richtlijn legt een aantal verplichtingen op, maar afwijkingen zijn mogelijk via de artikelen 13.3, 15 en 16.4. Artikel 18 van de Richtlijn biedt de lidstaten de mogelijkheid in voorkomend geval de uitoefening van die rechten vast te leggen in het Gerechtelijk Wetboek.

Teneinde de betrokkene in staat te stellen zijn rechten uit te oefenen moet alle informatie die aan de betrokkene wordt verstrekt, eenvoudig toegankelijk te zijn, met inbegrip van de website van de verwerkingsverantwoordelijke, begrijpelijk te zijn, en in duidelijke en eenvoudige taal gesteld te worden. Die informatie dient aangepast te zijn aan de behoeften van kwetsbare personen, zoals kinderen.

Art. 36

(Artikel 12 van de Richtlijn)

De modaliteiten zijn nauw gelinkt met de rechten van de betrokkene. Zo is het algemeen recht om geïnformeerd te worden, het recht om op de hoogte gehouden te worden van het vervolg, en om bijvoorbeeld makkelijk toegang te hebben tot de website. Onder “begrijpelijk” moet verstaan worden als aangepast zijn aan kinderen.

Zoals aangehaald door de Raad van State wordt het lid aangevuld om artikel 12 van de Richtlijn correct om te zetten.

Er moeten modaliteiten voorzien worden voor het faciliteren van de betrokkene bij de uitoefening van de rechten die hem zijn toegekend door deze titel, met inbegrip van de middelen om te verzoeken en, in voorkomend geval, het zonder bijkomende kosten verkrijgen van de toegang tot zijn persoonsgegevens, de rectificatie of de wissing ervan en de verwerkingsbeperking. De verwerkingsverantwoordelijke is gehouden om op de verzoeken van de betrokkene te antwoorden binnen een redelijke termijn, zonder beperkingen te stellen aan de rechten van de betrokkene conform deze titel. Bovendien, indien de verzoeken kennelijk ongegrond of buitensporig zijn, bijvoorbeeld omdat de betrokkenen

CHAPITRE III

Droits de la personne concernée

De même que pour les conditions de fond, les droits découlant de la directive 95/46 sont repris et renforcés.

L’article 23 du Règlement permet des restrictions pour les procédures judiciaires notamment (ainsi que la sécurité nationale, la défense, la sécurité publique, ...). La Directive impose un certain nombre d’obligations mais des dérogations sont possibles via les articles 13.3, 15 et 16.4. L’article 18 de la Directive permet quant à lui de laisser aux états membres la possibilité de déterminer l’exercice de ces droits entre autre par le Code judiciaire.

Afin de permettre aux personnes concernées d’exercer leurs droits, toute information qui leur est communiquée devrait être aisément accessible, y compris sur le site internet du responsable du traitement, et facile à comprendre, et formulée en des termes clairs et simples. Ces informations devraient être adaptées aux besoins des personnes vulnérables telles que les enfants.

Art. 36

(Article 12 de la Directive)

Les modalités sont liées étroitement aux droits de la personne concernée. En effet, le droit à l’information de manière générale est le droit d’être tenu au courant du suivi, d’avoir facilement accès aux informations via un site web par exemple. Le caractère compréhensible doit également être compris comme étant adapté aux enfants.

Comme soulevé par le Conseil d’État, l’alinéa est complété pour transposer correctement l’article 12 de la Directive.

Des modalités doivent être prévues pour faciliter l’exercice par la personne concernée des droits qui lui sont conférés par le présent titre, y compris les moyens de demander et, le cas échéant, d’obtenir, sans frais, notamment l’accès aux données à caractère personnel, et leur rectification ou leur effacement et la limitation du traitement. Le responsable du traitement devrait être tenu de répondre aux demandes de la personne concernée dans les meilleurs délais, à moins qu’il n’applique des limitations aux droits de la personne concernée conformément au présent titre. En outre, si les demandes sont manifestement infondées ou excessives, par exemple lorsque la personne concernée présente de

repetitieve en onredelijke verzoeken tot info stelt of misbruik maakt van zijn recht om informatie te ontvangen, bijvoorbeeld door valse of misleidende info te voegen bij zijn verzoek, kan de verwerkingsverantwoordelijke een redelijke vergoeding aanrekenen of weigeren gevolg te geven aan het verzoek.

Wanneer de verwerkingsverantwoordelijke om aanvullende informatie verzoekt die noodzakelijk is ter bevestiging van de identiteit van de betrokkene, dient die informatie uitsluitend voor deze specifieke finaliteit te worden verwerkt en mag die informatie niet langer worden opgeslagen dan voor dat doel noodzakelijk is.

Art. 37

(Artikel 13 van de Richtlijn)

Ten minste de volgende informatie moet ter beschikking van de betrokkene worden gesteld:

— de identiteit van de verwerkingsverantwoordelijke;

— het bestaan van de verwerking;

— de doeleinden van de verwerking;

— het recht klacht in te dienen;

— en het bestaan van het recht om van de verwerkingsverantwoordelijke toegang tot en rectificatie of wissing van persoonsgegevens of verwerkingsbeperking te verlangen;

— de rechtsgrond voor de verwerking en hoe lang de gegevens zullen worden opgeslagen;

— de categorieën van ontvangers van de persoonsgegevens, ook in derde landen of internationale organisaties;

en voor zover die nadere informatie noodzakelijk is om, met inachtneming van de specifieke omstandigheden waarin de persoonsgegevens worden verwerkt, met betrekking tot de betrokkene een behoorlijke verwerking te waarborgen. Dit kan worden gedaan op de website van de bevoegde overheid.

Er kunnen bijzondere wetten worden aangenomen om de informatieverstrekking aan de betrokkenen uit te stellen, te beperken of achterwege te laten, of de inzage in hun persoonsgegevens volledig of gedeeltelijk

façon répétée et déraisonnable des demandes d'information ou fait une utilisation abusive de son droit de recevoir des informations, par exemple en fournissant des informations fausses ou trompeuses lorsqu'elle présente sa demande, le responsable du traitement doit pouvoir exiger le paiement de frais raisonnables ou refuser de donner suite à la demande.

Lorsque le responsable du traitement demande que des informations supplémentaires lui soient fournies pour confirmer l'identité de la personne concernée, il convient que ces informations fassent l'objet d'un traitement uniquement pour cette finalité précise et qu'elles ne soient pas conservées pendant une durée excédant celle nécessaire au regard de ladite finalité.

Art. 37

(Article 13 de la Directive)

Les informations suivantes, au moins, devraient être communiquées à la personne concernée:

— l'identité du responsable du traitement;

— l'existence d'un traitement;

— les finalités du traitement;

— le droit d'introduire une réclamation;

— l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement ou la limitation du traitement;

— la base juridique du traitement et de la durée pendant laquelle les données seront conservées:

— les catégories de destinataires y compris dans les pays tiers ou au sein d'organisations internationales;

et dans la mesure où ces informations complémentaires sont nécessaires pour assurer un traitement loyal des données à l'égard de la personne concernée, compte tenu des circonstances particulières dans lesquelles les données sont traitées. Ces informations pourraient figurer sur le site internet de l'autorité compétente.

Des lois particulières peuvent être adoptées visant à retarder ou à limiter l'information des personnes concernées ou à ne pas leur accorder cette information, ou à leur limiter, complètement ou partiellement, l'accès aux

te beperken, voor zover en zolang die maatregel in een democratische samenleving, met inachtneming van de grondrechten en van de legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen, om ervoor te zorgen dat de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen niet in het gedrang komt, om de openbare veiligheid of de nationale veiligheid te beschermen, of om de rechten en vrijheden van anderen te beschermen. De verwerkingsverantwoordelijke dient door middel van een concreet en individueel onderzoek van elk geval te beoordelen of het inzagerecht gedeeltelijk dan wel volledig moet worden beperkt.

Hetzelfde geldt voor wat betreft de hoven en rechtbanken evenals het parket, waarvoor de bepalingen van het Wetboek van Strafvordering, het Gerechtelijk Wetboek, of de bijzondere wetten van toepassing zijn. Deze bepalingen houden rekening met een evenwicht tussen de fundamentele rechten en legitieme belangen van de betrokken natuurlijke persoon en de basisbeginselen van de werking van een democratische Staat.

Zoals het openbaar ministerie aangeeft in zijn advies is de tekst vertrokken van de basisgedachte dat eens een strafonderzoek aan de gang is de betrokkene zijn rechten enkel kan uitoefenen middels de binnen het strafprocesrecht bestaande procedures, zoals bijvoorbeeld de procedure van inzage enafschrift van artikel 21*bis* Strafwetboek. Er moet immers ook rekening worden gehouden met andere instanties en in het bijzonder de politiediensten voor dewelke er geen wettelijke reden bestaat die hen uitsluit van elke controle simpelweg omdat zij houder zijn van gerechtelijke gegevens.

Een dergelijke ruime formulering biedt de mogelijkheid de bijzondere wetten, waarin de verwerkingscategorieën kunnen worden vastgelegd waarvoor een informatiebeperking is toegestaan, te behouden.

Elke weigering of beperking van de inzage dient in principe schriftelijk aan de betrokkene te worden toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen.

Elke beperking van de rechten van de betrokkene dient in overeenstemming te zijn met het Handvest van de grondrechten van de Europese Unie en met het Europees Verdrag voor de Rechten van de Mens, zoals uitgelegd in de rechtspraak van respectievelijk het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens, en met name de wezenlijke inhoud van die rechten en vrijheden te eerbiedigen.

données à caractère personnel les concernant, dès lors qu'une telle mesure constitue une mesure nécessaire et proportionnée dans une société démocratique, compte dûment tenu des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, pour éviter de nuire à la prévention et à la détection des infractions pénales, aux enquêtes et poursuites en la matière ou à l'exécution de sanctions pénales, pour sauvegarder la sécurité publique ou la sécurité nationale, ou pour protéger les droits et libertés d'autrui. Le responsable du traitement devrait apprécier, en examinant chaque cas de façon concrète et individuelle, s'il y a lieu de limiter le droit d'accès partiellement ou complètement.

Il en est de même pour ce qui concerne les cours et tribunaux ainsi que le parquet, pour lesquels les dispositions du Code d'Instruction criminelle, le Code judiciaire, ou les lois particulières s'appliquent. Ces dispositions tiennent compte d'un équilibre entre les droits fondamentaux et les intérêts légitimes de la personne physique concernée et les principes fondamentaux de fonctionnement d'un État démocratique.

Comme le mentionne le ministère public dans son avis, le texte s'écarte de l'idée fondamentale qu'une fois qu'une enquête criminelle est en cours, ses droits ne peuvent être exercés que par les procédures prévues par la loi de procédure pénale, comme la procédure d'inspection et l'article 21*bis* du Code pénal. En effet, il y a lieu également de tenir compte des autes instances et notamment des services de police pour lesquels il n'existe pas de raison légitime qui les exluerait de tout contrôle simplement par ce qu'il détienne des données judiciaires.

Un tel libellé large permet de maintenir les lois particulières, lesquelles peuvent déterminer les catégories de traitement pour lesquelles une restriction de l'information est permise.

Tout refus d'accès ou toute limitation de l'accès devrait en principe être présenté par écrit à la personne concernée et indiquer les motifs factuels ou juridiques sur lesquels la décision est fondée.

Toute limitation des droits de la personne concernée doit respecter la Charte des droits fondamentaux de l'Union européenne et la Convention européenne des droits de l'homme, telles qu'elles sont interprétées respectivement par la Cour de justice de l'Union européenne et par la Cour européenne des droits de l'homme dans leur jurisprudence, et notamment respecter l'essence desdits droits et libertés.

Art. 38

(Artikel 14 van de Richtlijn)

Dit artikel is gelijkaardig aan artikel 15 van de Verordening.

Een natuurlijke persoon moet beschikken over het recht op inzage van de gegevens die over hem zijn verzameld, en moet dit recht gemakkelijk en met redelijke tussenpozen kunnen uitoefenen, zodat hij kennis kan nemen van de verwerking en de rechtmatigheid daarvan kan nagaan. Iedere betrokkene moet dan ook het recht hebben om op de hoogte te zijn van, en mededelingen te verkrijgen over, de doeleinden waarvoor de gegevens worden verwerkt, de periode waarin deze gegevens worden verwerkt, en de ontvangers van de gegevens, ook in derde landen. Wanneer die mededelingen informatie behelzen over de oorsprong van de persoonsgegevens, mag die informatie de identiteit van natuurlijke personen, met name van vertrouwelijke bronnen, niet onthullen. Om aan dit recht te voldoen, volstaat het dat aan de betrokkene in een begrijpelijke vorm een volledig overzicht van die gegevens wordt verstrekt, dat wil zeggen in een vorm die de betrokkene in staat stelt kennis te nemen van deze gegevens en na te gaan of deze juist zijn en overeenkomstig deze richtlijn zijn verwerkt, zodat hij in voorkomend geval de hem, uit hoofde van deze Dichtlijn toegekende rechten, kan uitoefenen. Dat overzicht kan worden verstrekt in de vorm van een kopie van de persoonsgegevens die worden verwerkt.

In de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst kunnen categorieën van gegevensverwerkingen worden bepaald waarop die beperkingen van de rechten van toepassing kunnen zijn.

Teneinde de bezorgdheden van het openbaar ministerie, zoals geuit in hun advies, te beantwoorden, is het duidelijk dat wanneer de gegevens zich in een gerechtelijk dossier bevinden, de regels inzake de strafprocedure van toepassing zijn zoals wordt voorzien in artikel 44 van deze wet.

Art. 39

(Artikel 16 van de Richtlijn)

Een natuurlijke persoon dient het recht te hebben om de hem betreffende onjuiste persoonsgegevens te laten rectificeren en te vervolledigen, vooral wanneer het gaat om feiten, en deze te laten wissen indien de verwerking van die gegevens inbreuk maakt op deze titel. Rekening

Art. 38

(Article 14 de la Directive)

Cet article est similaire à l'article 15 du Règlement.

Une personne physique doit avoir le droit d'accéder aux données qui ont été collectées la concernant et d'exercer ce droit facilement, à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité. En conséquence, chaque personne concernée doit avoir le droit de connaître et de se faire communiquer les finalités du traitement des données, la durée pendant laquelle les données sont traitées, ainsi que l'identité des destinataires, y compris les destinataires se trouvant dans des pays tiers. Lorsque ces communications comportent des informations relatives à l'origine des données à caractère personnel, ces informations ne doivent pas révéler l'identité des personnes physiques, en particulier les sources confidentielles. Pour que ce droit soit respecté, il suffit que la personne concernée dispose d'un aperçu complet de ces données sous une forme intelligible, c'est-à-dire une forme qui lui permette de prendre connaissance de ces données et de vérifier si elles sont exactes et traitées conformément à la présente Directive, de sorte qu'elle puisse exercer les droits que lui confère la présente directive. Cet aperçu pourrait être fourni sous la forme d'une copie des données à caractère personnel faisant l'objet du traitement.

La loi, le décret, l'ordonnance, le droit de l'Union européenne ou la convention internationale peut déterminer des catégories de traitements de données qui sont susceptibles de relever de ces limitations des droits.

Afin de répondre aux inquiétudes du Ministère public, telles qu'exprimées dans leur avis, il est évident que lorsque les données se trouvent dans un dossier judiciaire, les règles de procédure pénale s'applique, ainsi qu'il est prévu à l'article 44 de la présente loi.

Art. 39

(Article 16 de la Directive)

Une personne physique doit avoir le droit de faire rectifier et compléter des données à caractère personnel inexactes la concernant, en particulier lorsque cela touche aux faits, et disposer d'un droit d'effacement lorsque le traitement de ces données constitue une

houdend met de finaliteiten van de verwerking heeft de betrokkene het recht om onvolledige persoonsgegevens te laten vervolledigen, onder meer via een aanvullende verklaring.

Het recht op rectificatie mag echter geen invloed hebben op, bijvoorbeeld, de inhoud van een getuigenverklaring. Een natuurlijke persoon dient tevens recht te hebben op verwerkingsbeperking wanneer hij de juistheid van persoonsgegevens betwist en de juistheid of onjuistheid niet kan worden vastgesteld, of wanneer de persoonsgegevens moeten worden bewaard als bewijsmateriaal. Meer bepaald moeten persoonsgegevens niet worden gewist maar moet de verwerking worden beperkt indien in een specifiek geval redelijkerwijs kan worden aangenomen dat het wissen van de gegevens de legitieme belangen van de betrokkene zou kunnen schaden. In een dergelijk geval moeten de aan beperkingen onderworpen gegevens alleen worden verwerkt voor de finaliteit die die het wissen ervan verhinderd heeft. De verwerking van persoonsgegevens zou onder meer kunnen worden beperkt door het overbrengen van de geselecteerde gegevens naar een ander verwerkingssysteem, bijvoorbeeld voor archivering, of door het niet-beschikbaar maken van de geselecteerde gegevens. In geautomatiseerde bestanden moet de verwerking in beginsel met technische middelen worden beperkt. Het feit dat de verwerking van persoonsgegevens wordt beperkt, dient in het bestand duidelijk te worden aangegeven. Die rectificatie of wissing van persoonsgegevens of die verwerkingsbeperking moet worden meegedeeld aan de ontvangers aan wie de gegevens zijn bekendgemaakt en aan de overheden van wie de onjuiste data afkomstig waren. De verwerkingsverantwoordelijke dient er tevens voor te zorgen dat verdere verspreiding van die gegevens achterwege blijft.

In de Nederlandse versie wordt voortaan de term “rectificatie” gebruikt terwijl in de WVP de term “verbeteren” werd gebruikt.

Art. 40

Het betreft in dit artikel een modaliteitvan het verzoek. Er wordt van de verwerkingsverantwoordelijke verlangd dat hij onverwijld een ontvangstbevestiging bezorgt en in ieder geval binnen een maand na ontvangst van het verzoek om één van de rechten uit te oefenen waarin deze titel voorziet.

violation du présent titre. Compte tenu des finalités du traitement, la personne concernée a le droit d’obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant à cet effet une déclaration complémentaire.

Cependant, le droit de rectification ne doit pas affecter, par exemple, la teneur d’une déposition. Une personne physique doit également avoir le droit d’obtenir la limitation du traitement lorsqu’elle conteste l’exactitude des données à caractère personnel et qu’il ne peut être déterminé si ces données sont exactes ou non, ou lorsque les données à caractère personnel doivent être conservées à des fins probatoires. Plus particulièrement, les données à caractère personnel doivent faire l’objet d’une limitation du traitement plutôt qu’être effacées si, dans un cas déterminé, il existe des motifs raisonnables de penser que l’effacement pourrait nuire aux intérêts légitimes de la personne concernée. En pareil cas, les données faisant l’objet d’une limitation du traitement ne doivent être traitées que pour la finalité qui a empêché leur effacement. Les méthodes visant à limiter le traitement de données à caractère personnel peuvent consister, entre autres, à déplacer les données sélectionnées vers un autre système de traitement, par exemple à des fins archivistiques, ou à rendre les données sélectionnées inaccessibles. Dans les fichiers automatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques. Le fait que le traitement des données à caractère personnel est limité devrait être indiqué de manière claire dans le fichier. Cette rectification ou cet effacement des données à caractère personnel ou cette limitation du traitement doivent être communiqués aux destinataires auxquels les données ont été communiquées et aux autorités à l’origine des données inexactes. Les responsables du traitement doivent alors cesser de continuer à diffuser ces données.

Dans la version néerlandaise, le terme “rectificatie” est désormais utilisé alors qu’était utilisé dans la LVP, le terme “verbeteren”.

Art. 40

Il s’agit dans cet article d’une modalité de la demande. Il est demandé au responsable du traitement de délivrer un accusé de réception dans les meilleurs délais et en tout état de cause dans un délai d’un mois à compter de la réception de la demande d’exercice d’un des droits prévus par le présent titre.

Art. 41, 42 en 43

(Artikellen 13.3, 15, 16.4 en 17 van de Richtlijn)

Het betreft het systeem van de onrechtstreekse toegang bedoeld in artikel 13 WVP. Bij de onderhandelingen over de Richtlijn werd deze bepaling toegevoegd onder druk van onder meer België, die een systeem wensten te behouden dat voldoet aan de beginselen van het recht op de bescherming van de gegevens. Ter herinnering, in artikel 13 WVP was het volgende bepaald: *"Eenieder die zijn identiteit bewijst, is gerechtigd zich kosteloos tot de Commissie voor de bescherming van de persoonlijke levenssfeer te wenden, teneinde de in de artikelen 10 en 12 bedoelde rechten uit te oefenen ten aanzien van de verwerkingen van persoonsgegevens bedoeld in artikel 3, §§ 4, 5, 6 en 7.*" Die mogelijkheid is er enkel in de Richtlijn en niet in de Verordening.

Het is de bedoeling om het systeem van de onrechtstreekse toegang als mogelijkheid te behouden voor de overheden die dat wensen.

Er wordt ook bepaald dat wanneer de onrechtstreekse toegang wordt toegepast, het verzoek wordt ingediend bij de bevoegde toezichthoudende autoriteit.

Deze artikelen voeren de mogelijkheid uit tot zogenaamde onrechtstreekse toegang voor de lidstaten bepaald in artikel 17 van de Richtlijn in de volgende bewoordingen:

"*1. In de in artikel 13, lid 3, artikel 15, lid 3, en artikel 16, lid 4, bedoelde gevallen treffen de lidstaten maatregelen die ertoe strekken dat de betrokkene zijn rechten ook via de bevoegde toezichthoudende autoriteit kan uitoefenen.*

2. De lidstaten schrijven voor dat de verwerkingsverantwoordelijke de betrokkene in kennis stelt van de mogelijkheid uit hoofde van lid 1 zijn rechten via de toezichthoudende autoriteit uit te oefenen.

3. Wanneer het in lid 1 bedoelde recht wordt uitgeoefend, stelt de toezichthoudende autoriteit de betrokkene er ten minste van in kennis dat alle noodzakelijke controles of een evaluatie door de toezichthoudende autoriteit hebben plaatsgevonden. De toezichthoudende autoriteit stelt de betrokkene tevens in kennis van zijn recht om beroep in te stellen bij de rechter".

De onrechtstreekse toegang werd in België tot op heden geregeld door artikel 13 WVP.

Art. 41, 42 et 43

(Articles 13.3, 15, 16.4 et 17 de la Directive)

Il s'agit du système de l'accès indirect visé à l'article 13 LVP. Lors des négociations de la directive, cette disposition a été ajoutée sous la pression de entre autre la Belgique qui souhaitaient maintenir un système répondant aux principes de droit à la protection des données. Pour rappel, l'article 13 LVP stipulait: *"1er. Toute personne justifiant de son identité a le droit de s'adresser sans frais à la Commission de la protection de la vie privée pour exercer les droits visés aux articles 10 et 12 à l'égard des traitements de données à caractère personnel visés à l'article 3, §§ 4, 5, 6 et 7.*" Cette possibilité n'existe que dans la Directive et pas dans le Règlement.

Il s'agit de laisser le système de l'accès indirect une option pour les autorités qui le souhaitent.

Il est également prévu que lorsqu'il est fait application de l'accès indirect, la demande se fait via l'autorité de contrôle compétente.

Ces articles mettent en œuvre la faculté dite d'accès indirect réservée aux États membres par l'article 17 de la Directive en ces termes:

"*1. Dans les cas visés à l'article 13, paragraphe 3, à l'article 15, paragraphe 3, et à l'article 16, paragraphe 4, les États membres adoptent des mesures afin que les droits de la personne concernée puissent également être exercés par l'intermédiaire de l'autorité de contrôle compétente.*

2. Les États membres prévoient que le responsable du traitement informe la personne concernée de la possibilité qu'elle a d'exercer ses droits par l'intermédiaire de l'autorité de contrôle en application du paragraphe 1er.

3. Lorsque le droit visé au paragraphe 1er est exercé, l'autorité de contrôle informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. L'autorité de contrôle informe également la personne concernée de son droit de former un recours juridictionnel".

L'accès indirect était jusqu'ici consacré en Belgique par l'article 13 LVP.

De voorbereidende werkzaamheden van deze wet geven aan dat "*ingevolgde de bijzondere taken van die diensten [o.a. politie] kan er geen sprake van zijn aan eenieder een rechtstreeks recht van toegang te verlenen tot de geregistreerde gegevens die op hen betrekking hebben. Eenieder kan de Commissie voor de bescherming van de persoonlijke levenssfeer evenwel vragen in zijn plaats het recht van toegang en het recht op verbetering uit te oefenen. (…) Die door de Franse wet ingegeven procedure is bekend onder de benaming "onrechtstreekse toegang". Zij beoogt een billijk evenwicht tot stand te brengen tussen de gewettigde rechten van iedere persoon en de niet minder gewettigde noodzaak van opsporing en vervolging van de overtredingen, alsmede van het voorkomen van inbreuken op de veiligheid van de Staat*" (Parl. St. Kamer, 48-1610/1, buitengewone zitting, 1991-1992, bz.19).

Het oude artikel 39 van de Franse wet nr. 78-17 van 6 januari 1978 betreffende de bestanden, de informatica en de vrijheden bepaalde reeds dat het recht op toegang tot de bestanden van de politie en de gendarmerie, op een verwerking teneinde misdrijven te voorkomen, op te sporen of te controleren of belastingen te innen, wordt uitgeoefend door bemiddeling van een commissaris van de "Commission nationale de l'informatique et des libertés" (CNIL).

Dergelijke beperkingen van de rechten van de persoon die betrokken is bij de verwerking van zijn persoonsgegevens zijn in overeenstemming met de aanbeveling nr. R (87) 15 tot regeling van het gebruik van persoonsgegevens op politieel gebied. Deze Aanbeveling van de Raad van Europa somt een aantal principes op die op dit gebied moeten worden toegepast, in het bijzonder om de naleving van artikel 8 van het Europees Verdrag voor de Rechten van de Mens te garanderen. Op 15 februari 2018, meer dan twee jaren na de goedkeuring van de Richtlijn 2016/680, heeft de adviescommissie van het Verdrag 108 een praktische gids voor het gebruik van persoonsgegevens op politieel gebied gepubliceerd. Deze gids herinnert eraan dat "*sinds de goedkeuring ervan, heeft de Aanbeveling (87)15 het voorwerp uitgemaakt van verschillende evaluaties (in 1993, 1998 en 2002), zowel wat de toepassing als de relevantie ervan betreft. In 2010 heeft de adviescommissie van het Verdrag 108 beslist om een studie uit te voeren over het gebruik van persoonsgegevens op politieel gebied in heel Europa. Deze evaluatie heeft aangetoond dat de principes van de Aanbeveling (87)15 nog steeds een geschikt uitgangspunt vormden om reglementeringen uit te werken die op nationaal vlak hierop betrekking hebben (…)*" (blz.2). Punt 6 van deze gids van 2017 vermeldt evenwel dat "*in het geval van een onrechtstreekse toegang, de betrokken persoon zijn verzoek aan de toezichthoudende autoriteit kan*

Les travaux préparatoires de cette loi indiquent "*qu'en raison des missions particulières de ces services [e.a. de police], il ne saurait être question de donner à toute personne un droit d'accès direct aux données enregistrées à leur égard. Toute personne pourra toutefois demander à la Commission de la protection de la vie privée d'exercer pour elle le droit d'accès et de rectification. (…) Cette procédure, qui s'inspire de la loi française est connue sous le nom d'"accès indirect". Elle vise à établir un juste équilibre entre les droits légitimes de l'individu et les nécessités, tout aussi légitimes, de la recherche et de la poursuite des infractions ainsi que de la prévention des atteintes à la sûreté de l'État"* (Doc. Parl. Ch., 48-1610/1, session extraordinaire, 1991-1992, p.19).

En effet, tout comme en Belgique, la loi française du 6 janvier 1978 relative aux fichiers, à l'informatique et aux libertés prévoyait déjà que le droit d'accès aux fichiers de police et de gendarmerie, à un traitement visant à prévenir, rechercher ou contrôler des infractions ou encore à recouvrer des impositions s'exerce par l'intermédiaire d'un commissaire de la "Commission nationale de l'informatique et des libertés" (CNIL).

De telles restrictions aux droits de la personne concernée par le traitement de ses données à caractère personnel sont conformes à la recommandation no R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Cette Recommandation du Conseil de l'Europe énonce un ensemble de principes applicables à ce secteur, notamment pour garantir le respect de l'article 8 de la Convention européenne des droits de l'homme. Le 15 février 2018, soit près de deux ans après l'adoption de la Directive 2016/680, le Comité consultatif de la Convention 108 a publié un guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police. Ce guide rappelle que "*depuis son adoption, la Recommandation (87)15 a fait l'objet de plusieurs évaluations (en 1993, 1998 et 2002) sur le plan tant de son application que de sa pertinence. En 2010, le Comité consultatif de la Convention 108 a décidé de réaliser une étude sur l'utilisation de données à caractère personnel dans le secteur de la police dans l'ensemble de l'Europe. Cette évaluation a montré que les principes de la Recommandation (87)15 constituaient toujours un point de départ approprié pour élaborer des réglementations s'appliquant à cette matière au niveau national (…)"* (p.2). Or, le point 6 de ce guide indique que "*Si le droit d'accès prévu est indirect, la personne concernée peut adresser sa demande à l'autorité de contrôle qui, après avoir été*

richten. Deze autoriteit zal, na daartoe behoorlijk te zijn gemachtigd, het verzoek in zijn naam behandelen en de nodige verificaties verrichten met betrekking tot de beschikbaarheid en de rechtmatigheid van de verwerking van de persoonsgegevens. De toezichthoudende autoriteit zal de betrokkene vervolgens antwoorden (op basis van de gegevens die kunnen worden verspreid, onverminderd de beperkingen of wettelijk toegestane afwijkingen)." (blz. 9).

Tijdens de voorbereidende werkzaamheden waren verschillende landen er voorstander van om de lidstaten de mogelijkheid te bieden het principe van onrechtstreekse toegang op te nemen in hun nationale wetgeving, zoals reeds het geval is in bepaalde landen waaronder België.

In tegenstelling tot hetgeen de Raad van State oordeelde, had de Europese wetgever dus wel degelijk de bedoeling om de lidstaten in staat te stellen de bestaande situatie te behouden.

Voor wat betreft de politiediensten, in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, zal het verzoek om de rechten van de betrokkenen, bedoeld in dit hoofdstuk, worden gericht aan de toezichthoudende autoriteit, bedoeld in artikel 71, namelijk het *Controleorgaan op de politionele informatie* (of het COC).

Voor de betrokkene garandeert de uitoefening van dit recht via de toezichthoudende autoriteit dat er daadwerkelijk een controle zal plaatsvinden. Voor zijn antwoord zal het Controleorgaan op de politionele informatie zich immers tot de bevoegde verwerkingsverantwoordelijke wenden en/of, naargelang van het geval, tot de politiedienst belast met de verwerking van de informatie.

Wat betreft het antwoord van het Controleorgaan op de politionele informatie aan de betrokkene, zal het meedelen dat "*de nodige verificaties werden verricht*".

dûment mandatée, la traitera en son nom et procédera à des vérifications sur la disponibilité et la licéité du traitement des données à caractère personnel. L'autorité de contrôle répondra ensuite à la personne concernée (en fonction des données qu'il est possible de diffuser, sous réserve des restrictions ou dérogations autorisées légalement)." (p.9).

Lors des travaux préparatoires, différents pays ont soutenu la possibilité pour les États membres d'introduire dans leurs législations nationales le principe de l'accès indirect" tels qu'il existe déjà dans certains pays dont la Belgique.

Contrairement à ce que le Conseil d'État estime, l'intention du législateur européen a donc bien été de permettre aux États Membre de maintenir la situation existante.

Pour ce qui concerne les services de police, au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant la police intégrée, structurée à deux niveaux, la demande d'exercer les droits des personnes concernées visées au présent chapitre sera adressée à l'autorité de contrôle visée à l'article 71, soit *l'Organe de Contrôle de l'information policière* (ou le COC).

Pour la personne concernée, l'exercice de ce droit via l'autorité de contrôle lui permet d'avoir l'assurance qu'un contrôle effectif sera effectué vu que, pour répondre, l'Organe de contrôle de l'information policière se retournera vers le responsable de traitement compétent et/ou suivant les cas vers le service de police en charge du traitement de l'information.

Concernant la réponse que l'Organe de contrôle de l'information policière donnera à la personne concernée, elle communiquera "*qu'il a été procédé aux vérifications nécessaires"*.

Art. 44

(Artikel 18 van de Richtlijn)

Art. 44

(Article 18 de la Directive)

Indien de persoonsgegevens in het kader van een strafrechtelijk onderzoek en een strafrechtelijke procedure worden verwerkt, wordt erin voorzien dat het recht op informatie, inzage en op rectificatie of wissing van persoonsgegevens en op verwerkingsbeperking

Lorsque les données à caractère personnel sont traitées dans le cadre d'une enquête pénale ou d'une procédure judiciaire en matière pénale, il est prévu que le droit à l'information, le droit d'accès aux données à caractère personnel, de rectification ou d'effacement

overeenkomstig het nationaal procesrecht wordt uitgeoefend.

Het advies van het openbaar ministerie laat uitschijnen dat dit principe uitgebreid wordt naar alle bestaande rechten in dit hoofdstuk. Maar de Richtlijn is in deze duidelijk en de toepassing van dit principe mag niet worden veralgemeend. Het dient te worden beperkt tot enkele rechten.

Teneinde de bezorgdheden van het openbaar ministerie, zoals geuit in hun advies, te beantwoorden, is het duidelijk dat wanneer de gegevens zich in een gerechtelijk dossier bevinden, de regels inzake de strafprocedure van toepassing zijn zoals wordt voorzien in artikel 44 van deze wet.

Art. 45

Dit artikel bepaalt de verplichtingen van de in deze titel bedoelde verwerkings-verantwoordelijke en bevoegde overheid wanneer zij beschikken over persoonsgegevens die rechtstreeks of onrechtstreeks van een overheid bedoeld in titel 3, zoals inlichtingen- en veiligheidsdienst, NVO, OCAD, …. afkomstig zijn.

Omwille van evidente redenen van veiligheid en discretie krijgen de verwerkingsverantwoordelijke en de bevoegde overheid een verbod opgelegd om de betrokkene ervan op de hoogte te brengen dat zij over hem betreffende gegevens beschikken, wanneer deze van een inlichtingendienst afkomstig zijn.

Om te antwoorden op het punt 217 van het advies van de Privacycommissie: deze uitzondering op het recht van de betrokkene op informatie moet in titel 2 hernomen worden omdat de bevoegde autoriteiten bedoeld in deze titel niet over een algemeen verbod beschikken om de betrokkene te informeren. De controleregels en de verhoudingen tussen de toezichthoudende autoriteiten dienen eveneens te worden bepaald.

De formulering van artikel 45 werd in dezelfde zin aangepast als artikel 11 om op het punt 122 van het advies van de Privacycommissie te antwoorden. Zo voorziet het artikel uitdrukkelijk dat de artikelen 36 tot 44 en 62 niet van toepassing zijn, hetgeen automatisch inhoudt dat enerzijds de betrokkenen niet van deze rechten genieten en anderzijds dat de verwerkingsverantwoordelijken niet tot de verplichtingen gehouden zijn.

Hierop zijn twee uitzonderingen voorzien:

de celles-ci, et le droit de limitation du traitement sont exercés conformément aux règles nationales relatives à la procédure judiciaire.

L'avis du ministère public prétend étendre ce principe à tous les droits existants dans ce chapitre. Or la Directive est claire à ce sujet et l'application de ce principe ne peut pas être général. Il doit être limité à certains droits.

Afin de répondre aux inquiétudes du ministère public, telles qu'exprimées dans leur avis, il est évident que lorsque les données se trouvent dans un dossier judiciaire, les règles de procédure pénale s'applique, ainsi qu'il est prévu à l'article 44 du présent projet de loi.

Art. 45

Cet article détermine les obligations du responsable du traitement et de l'autorité compétente visés dans le présent titre lorsqu'ils disposent de données à caractère personnel émanant directement ou indirectement d'une autorité visée au titre 3, tel qu'un service de renseignement et de sécurité, l'ANS, OCAM, ….

Pour des raisons évidentes de sécurité et de discrétion, le responsable du traitement et l'autorité compétente ont l'interdiction d'informer la personne concernée qu'ils disposent de données la concernant lorsque celles-ci émanent d'un service de renseignement.

Pour répondre au point 217 de l'avis de la Commission vie privée: cette exception au droit d'être informé de la personne concernée doit être reprise dans le titre 2 car les autorités compétentes visées dans ce titre n'ont pas une interdiction générale d'informer la personne concernée. Les règles de contrôle et les liens entre les autorités de contrôle doivent également être fixés.

La formulation de l'article 45 a été adaptée dans le même sens que celle de l'article 11 pour répondre au point 122 de l'avis de la Commission vie privée. Ainsi, l'article dispose expressément que les articles 36 à 44 et 62 ne s'appliquent pas, ce qui implique automatiquement que, d'un côté, les personnes concernées ne bénéficient pas des droits et, de l'autre, les responsables du traitement ne sont pas tenus aux obligations.

Deux exceptions sont prévues:

— wanneer de verwerkingsverantwoordelijke of de bevoegde overheid wettelijk verplicht is om alle gegevens die hem ter beschikking zijn gesteld in het kader van een rechtsgeschil, door te geven, of

— wanneer hij de voorafgaande toestemming heeft gekregen van de overheid bedoeld in titel 3 waarvan de gegevens afkomstig zijn.

Deze uitzondering op de verplichtingen van de verwerkingsverantwoordelijke bedoeld in artikelen 12 tot 22 en 34 van de Verordening en op de transparantieverplichting bedoeld in punt 1.a) van artikel 5 van de Verordening wordt toegestaan door artikel 23 van deze Verordening indien zij in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborgingbescherming van de nationale veiligheid, de landsverdediging en de openbare veiligheid.

Gelet op de opdrachten van de beide inlichtingen- en veiligheidsdiensten zoals bepaald in de artikelen 7 en 11 van de wet van 30 november 1998, lijdt het geen twijfel dat het gaat om een noodzakelijke maatregel ter bescherming van de nationale veiligheid in het bijzonder. Om alle bedreigingen tegen de Belgische staat en zijn burgers te kunnen bestrijden, moeten de inlichtingendiensten tot inlichtingenonderzoeken overgaan om de bedreigingen en de aanstichters ervan te kunnen identificeren. Er moet tot elke prijs vermeden worden dat deze laatsten dankzij hun recht op informatie bedoeld in artikelen 36 tot 44 en 62 van deze wet ervan op de hoogte gebracht worden dat een inlichtingendienst hen “in de gaten houdt”. Om de doeltreffendheid en de discretie van de inlichtingenonderzoeken te garanderen, is de in dit artikel voorziene uitzondering noodzakelijk en evenredig.

Gelet op de opdrachten van het OCAD, zoals bepaald in de wet van 10 juli 2006 betreffende de analyse van de dreiging, lijdt het geen twijfel dat het gaat om een noodzakelijke maatregel ter bescherming van de nationale veiligheid in het bijzonder. Om, overeenkomstig artikelen 3 en 8 van de wet van 10 juli 2006 de dreigingen die uitgaan van terrorisme en extremisme te kunnen evalueren, moet het OCAD de gegevens uitgaande van al zijn ondersteunende diensten, bedoeld in artikel 2, 2°, van de wet van 10 juli 2006, kunnen verwerken, onder meer gegevens van inlichtingen- en veiligheidsdiensten. Er moet tot elke prijs vermeden worden dat deze laatsten dankzij hun recht op informatie bedoeld in artikelen 12 tot 22 en 34 van de Verordening ervan op de hoogte gebracht worden dat een inlichtingendienst hen “in de gaten houdt”. Om de doeltreffendheid en de discretie van de inlichtingenonderzoeken te garanderen, is de in dit artikel voorziene uitzondering noodzakelijk en evenredig.

— lorsque le responsable du traitement ou l’autorité compétente est légalement tenu de transmettre toutes les données à sa disposition dans le cadre d’une procédure contentieuse, ou

— lorsqu’il obtient l’autorisation préalable de l’autorité visée au titre 3 dont proviennent les données.

Cette exception aux obligations du responsable du traitement visées aux articles 12 à 22 et 34 du Règlement et à l’obligation de transparence visée au point 1.a) de l’article 5 du Règlement est autorisée par l’article 23 dudit Règlement si elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité nationale, la défense nationale et la sécurité publique.

Au vu des missions des deux services de renseignement et de sécurité fixées aux articles 7 et 11 de la loi du 30 novembre 1998, il ne fait aucun doute qu’il s’agit d’une mesure nécessaire pour garantir notamment la sécurité nationale. En effet, pour lutter contre toutes les menaces envers l’État belge et ses citoyens, les services de renseignement doivent procéder à des enquêtes de renseignement afin d’identifier les menaces et leurs auteurs. Il faut à tout prix éviter que ces derniers soient informés qu’un service de renseignement les a “repérés” grâce à leur droit d’information visé aux articles 36 à 44 et 62 de la présente loi. Pour assurer l’efficacité et la discrétion des enquêtes de renseignement, l’exception prévue dans le présent article est nécessaire et proportionnée.

Au vu des missions de l’OCAM fixées dans la loi du 10 juillet 2006 relative à l’analyse de la menace, il ne fait aucun doute qu’il s’agit d’une mesure nécessaire pour garantir notamment la sécurité nationale. En effet, conformément à l’article 3 de la loi du 10 juillet 2006, pour pouvoir évaluer, conformément à l’article 8 de la loi du 10 juillet 2006, toutes les menaces émanant du terrorisme et extrémisme, envers l’État belge et ses citoyens, l’OCAM doit pouvoir procéder au traitement des données émanant de tous ses services d’appui, visé dans l’article 2, 2°, de la loi du 10 juillet 2006, dont des données des services de renseignement et de sécurité. Il faut à tout prix éviter que ces derniers grâce à leur droit d’information visé aux articles 12 à 22 et 34 du Règlement soient informés qu’un service de renseignement les a “repérés”. Pour assurer l’efficacité et la discrétion des enquêtes de renseignement, l’exception prévue dans le présent article est nécessaire et proportionnée.

Om te vermijden dat de verwerkings-verantwoordelijke van een gegeven van een overheid bedoeld in titel 3 argwaan wekt bij de betrokkene, verduidelijkt paragraaf 3 van dit artikel dat de verantwoordelijke niets mag meedelen dat een aanwijzing zou kunnen zijn van het feit dat hij over gegevens van een inlichtingendienst beschikt.

In geen geval mag de verwerkings-verantwoordelijke aan de betrokkene melden dat dit artikel toegepast werd. Hij mag de betrokkene ook niet verwijzen naar het Comité I. Hij moet verwijzen naar zijn bevoegde toezichthoudende autoriteit.

De paragraaf 5 van dit artikel maakt de bescherming ook van toepassing op de logs en registraties van het raadplegen en van andere verwerkingen van een gegevensbank door een overheid bedoeld in titel 3. Wanneer een overheid bedoeld in titel 3 rechtstreeks toegang heeft tot een gegevensbank die hem niet toebehoort, worden deze raadplegingen geregistreerd (oplijsting/logs). Indien de persoon van wie de gegevens geraadpleegd zijn, door de verantwoordelijke van de gegevensbank ervan op de hoogte zou worden gesteld dat een inlichtingendienst zijn gegevens verzamelt, zou dit het inlichtingenonderzoek en de opdrachten van het OCAD of van zijn ondersteunende diensten bedoeld in artikel 2, 2°, van de wet van 10 juli 2006, ernstig in gevaar brengen. Bijgevolg krijgen de verwerkingsverantwoordelijken van de gegevensbanken waartoe de inlichtingendiensten toegang hebben, een verbod opgelegd om de betrokkene op de hoogte te stellen van het raadplegen van zijn gegevens door een inlichtingendienst, in toepassing van dit artikel.

De paragraaf 6 van artikel 45 bepaalt de verhoudingen tussen de bevoegde toezichthoudende autoriteit en het Vast Comité I alsook de wijze waarop de autoriteit die gevat wordt de betrokkene antwoordt. Op verzoek van de Privacycommissie werd verduidelijkt dat het Vast Comité I de bevoegde autoriteit is voor de gegevens afkomstig van titel 3. De andere bevoegde toezichthoudende autoriteiten die kunnen gevat worden kunnen, al naar gelang het geval, het COC zijn of het controlemechanisme voor de gerechtelijke overheden. Trouwens, de term “beroep” werd vervangen door de woorden “verzoek en klacht”.

Art. 46

Dit artikel heeft betrekking op het geval waarbij een verwerkingsverantwoordelijke of een bevoegde overheid persoonsgegevens aan een overheid bedoeld in titel 3, ondertitels 2 en 4 bezorgt. In dat geval verbiedt dit artikel de verwerkingsverantwoordelijke en de bevoegde

Pour éviter que le responsable du traitement d’une donnée d’une autorité visée au titre 3 ne mette la puce à l’oreille de la personne concernée, paragraphe 3 du présent article précise que le responsable ne peut faire aucune mention qui serait susceptible de donner une indication sur le fait qu’il disposerait de données d’un service de renseignement.

A aucun moment, le responsable du traitement ne doit signaler à la personne concernée qu’il fait une application du présent article. Il ne peut pas non plus renvoyer la personne concernée vers le Comité R. Il doit renvoyer vers sa propre autorité de contrôle compétente.

Le paragraphe 5 du présent article rend également la protection applicable aux loggings et enregistrements de consultation et d’autres traitements d’une banque de données par une autorité visée au titre 3. En effet, lorsqu’une autorité visée au titre 3 a un accès direct à une banque de données ne lui appartenant pas, ses consultations sont enregistrées (journalisation/logging). Si la personne dont les données ont fait l’objet d’une consultation était informée par le responsable de la banque de données qu’un service de renseignement collecte ses données, cela mettrait sérieusement en péril l’enquête de renseignement et les missions de l’OCAM ou de ses services d’appui visés à l’article 2, 2°, de la loi du 10 juillet 2006. Par conséquent, les responsables du traitement des banques de données auxquelles les services de renseignement ont accès, ont interdiction d’informer la personne concernée des consultations de ses données par un service de renseignement, en application du présent article.

Le paragraphe 6 de l’article 45 détermine les relations entre l’autorité de contrôle compétente saisie et le Comité permanent R ainsi que la manière dont l’autorité saisie répond à la personne concernée. A la demande de la Commission vie privée, il a été précisé que l’autorité compétente pour les données émanant du titre 3 est le Comité permanent R. Les autres autorités de contrôle compétentes qui peuvent être saisies peuvent, en fonction des cas, être le COC ou le mécanisme de contrôle pour les autorités judiciaires. Par ailleurs, le terme “recours” est remplacé par les mots “requête et plainte”.

Art. 46

Cet article vise le cas où un responsable du traitement ou une autorité compétente transmet des données à caractère personnel à une autorité visée au titre 3, sous-titres 2 et 4. Dans ce cas, l’article interdit au responsable du traitement et à l’autorité compétente de

overheid om aan de betrokkene mee te delen dat de inlichtingendienst ontvanger van de gegevens is, door te voorzien in een uitzondering op de artikelen 37, eerste paragraaf, 8°) en 38, eerste praragraaf, 4°)van deze wet. Deze uitzondering beantwoordt aan de discretievereiste die eigen is aan de opdrachten van het OCAD en van haar ondersteunende diensten bepaald in artikel 2, 2°, van de wet van 10 juli 2006 en de Krijgsmacht.

In het punt 128 van haar advies haalt de Privacycommissie aan dat deze bepaling niet nuttig is omdat de autoriteiten bedoeld in titel 3 niet onder de definitie van "ontvanger" vallen in de zin van artikel 31, 10°, van deze wet aangezien het overheden betreft die gegevens ontvangen in het kader van een bijzondere onderzoeksopdracht. Het is inderdaad zo dat de inlichtingen- en veiligheidsdiensten bedoeld in ondertitel 1 van titel 3 en de autoriteiten bedoeld in ondertitel 3 van titel 3 bijzondere onderzoeksopdrachten hebben en dus niet beschouwd worden als ontvangers in de zin van artikel 26, 10°, van deze wet. Bijgevolg zijn de verplichtingen bedoeld in de artikelen 37, eerste paragraaf, 8°) en 38, eerste praragraaf, 4°) van deze wet niet van toepassing wanneer een verwerkingsverantwoordelijke persoonsgegevens overmaakt aan een autoriteit bedoeld in de ondertitels 1 en 3 van titel 3. Geen enkele melding aan de betrokkene van de doorgifte van de persoonsgegevens naar een autoriteit bedoeld in de ondertitels 1 en 3 van titel 3 kan dan ook gedaan worden, om evidente redenen van discretie. Het artikel wordt echter behouden voor de autoriteiten bedoeld in ondertitels 2 (Krijgsmacht) en 4 (OCAD) van titel 3 die geen bijzondere onderzoeken doen en dus onder de definitie van ontvanger vallen. Om te vermijden dat een autoriteit van titel 2 aan de betrokkene vermeldt dat zij gegevens heeft overgemaakt aan een autoriteit van de ondertitels 2 en 4 van titel 3 bepaalt huidig artikel dat de artikelen 37, eerste paragraaf, 8°) en 38, eerste praragraaf, 4°) van deze wet niet van toepassing zijn.

Art. 47

De inlichtingen- en veiligheidsdiensten zijn onderworpen aan verregaande beperkingen ter bescherming van de identiteit van hun agenten, de vertrouwelijkheid van hun onderzoeken en de bescherming van hun bronnen. Deze verplichtingen zijn uitdrukkelijk voorgeschreven in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en gaan gepaard met strafsancties in geval van niet-naleving:

— artikel 13 houdt de verplichting in om de bronnen van de inlichtingendiensten te beschermen. Het gaat hier natuurlijk niet enkel over informanten, buitenlandse inlichtingendiensten en de informatie die zij delen met

communiquer à la personne concernée que le service de renseignement est destinataire des données, en prévoyant une exception aux articles 37, paragraphe premier, 8°) et 38, paragraphe premier, 4°) de la présente loi. Cette exception répond à l'exigence de discrétion inhérente aux missions de l'OCAM et de ses services d'appui visés à l'article 2, 2°, de la loi du 10 juillet 2006, et aux Forces armées.

La Commission vie privée, au point 218 de son avis, relève que cette disposition n'est pas utile car les autorités visées au titre 3 n'entrent pas dans la définition de "destinataire" au sens de l'article 31.10° de la présente loi puisqu'il s'agit d'autorités publiques recevant des données dans le cadre d'une mission d'enquête particulière. Il est effectivement vrai que les services de renseignement et de sécurité visé au sous-titre 1er du titre 3 et les autorités visées au sous-titre 3 du titre 3 ont des missions d'enquête particulière et ne sont donc pas considérés comme des destinataires au sens de l'article 26, 10°. Par conséquent, les obligations visées aux articles 37, paragraphe premier, 8°) et 38, paragraphe premier, 4°)) de la présente loi ne s'appliquent pas quand un responsable du traitement ou une autorité compétente visés dans le titre 2 transmet une donnée à caractère personnel à une autorité visée aux sous-titres 1 ou 3 du titre 3. Aucune mention ne peut dès lors être faite à la personne concernée de la transmission de données vers une autorité visée aux sous-titres 1 ou 3 du titre 3, pour des raisons évidentes de discrétion. L'article est cependant maintenu pour les autorités visées aux sous-titres 2 (les Forces armées) et 4 (l'OCAM) du titre 3 qui n'effectuent pas d'enquêtes particulières et donc relèvent de la définition de destinataire. Pour éviter qu'une autorité du titre 2 ne mentionne à la personne concernée qu'elle a transmis des données à une autorité des sous-titres 2 et 4 du titre 3, le présent article dispose que les 37, paragraphe premier, 8°) et 38, paragraphe premier, 4°) ne s'appliquent pas.

Art. 47

Les services de renseignement et de sécurité ont des contraintes conséquentes pour assurer la protection de l'identité de leurs agents, la confidentialité de leurs enquêtes et la protection de leurs sources. Ces obligations sont expressément prescrites dans la loi organique du 30 novembre 1998 des services de renseignement et de sécurité et sont assorties de sanctions pénales, en cas de non-respect:

— l'article 13 impose la protection des sources des services de renseignement. Cela ne concerne bien entendu pas que les informateurs, les services de renseignement étrangers et les informations qu'ils

de Veiligheid van de Staat en de ADIV. De bescherming heeft ook betrekking op de technische bronnen van de inlichtingendiensten. In het algemeen verplicht deze bepaling de inlichtingendiensten tot discretie en bescherming van de opdrachten;artikel 36 voorziet een plicht tot geheimhouding van de informatie waarvan de agenten van de inlichtingendiensten kennis hebben in het kader van functie;

— artikel 43 straft de kwaadwillige verspreiding van de identiteit van agenten van de inlichtingendiensten, evenals de schending van de twee voornoemde verplichtingen.

In het kader van hun onderzoeken moeten de agenten altijd rekening houden met het risico voor hun informanten of andere bronnen, door te trachten de informatie die ze ingewonnen hebben te toetsen aan andere informatie of ze verder uit te diepen. Wanneer de agenten er niet in slagen om hun bescherming te garanderen, moeten ze afzien van hun onderneming. Heel het inlichtingenwerk ondervindt hiervan de gevolgen of wordt zelfs onmogelijk gemaakt als het risico te groot is voor de bescherming die de inlichtingendiensten moeten bieden.

Dit artikel heeft als doelstelling de hiervoor beschreven bescherming te garanderen, door te waken over de vertrouwelijkheid van de opzoekingen die de inlichtingen- en veiligheidsdiensten kunnen doen in de externe databanken (vb. een terro-databank) bij een online toegang. Het feit dat personen die vreemd zijn aan de betrokken inlichtingendienst kennis kunnen krijgen van een opzoeking door deze dienst, zou een gevaar kunnen opleveren voor de bescherming waarvoor de inlichtingendiensten moeten zorgen. Wanneer, bijvoorbeeld, een buitenlandse dienst aan de Veiligheid van de Staat informatie geeft over een nakende dreiging met betrekking tot mijnheer XY, geboren op 01.01 2001 en met de Belgische nationaliteit, verifiëert de Veiligheid van de Staat eerst of er een overeenkomst gevonden kan worden tussen de geseinde persoon en iemand in een gespecialiseerde databank, bijv. terro, en of er geen misverstand is met een andere persoon. Een correcte identificatie van de potentiële dreiging is natuurlijk primordiaal. De Veiligheid van de Staat moet trouwens de informatie van de buitenlandse inlichtingendienst beschermen. Deze informatie mag niet verspreid worden vooraleer ze steun vindt in de resultaten van het onderzoek.

De bescherming van de onderzoeken die de inlichtingendiensten uitvoeren is tevens van belang voor de betrokkenen. Het feit dat een inlichtingendienst interesse toont in een persoon heeft immers, helaas regelmatig, tot gevolg dat wie niet bekend is met de

partagent avec la Sûreté de l'État et le SGRS. La protection porte également sur les sources techniques des services de renseignement. De manière générale, cette disposition traduit une obligation de discrétion et de protection des missions dans le chef des services de renseignement; – l'article 36 prescrit une obligation au secret portant sur les informations dont les agents des services de renseignement ont connaissance dans le cadre de leurs fonctions;

— l'article 43 punit la divulgation avec intention malveillante de l'identité des agents des services de renseignement, ainsi que le non- respect des deux obligations précédentes.

Dans le cadre de leurs enquêtes, les agents doivent toujours prendre en compte le risque qu'ils font courir à leur informateur ou à toute autre source, en tentant de recouper ou d'approfondir les informations obtenues de leur part. S'ils ne parviennent pas à garantir leur protection, les agents doivent renoncer à l'action entreprise. C'est tout le travail du renseignement qui s'en ressent, voire qui est rendu impossible, si le risque est trop grand à l'égard des protections que les services de renseignement ont l'obligation de garantir.

Cet article a pour objectif d'assurer les protections expliquées plus haut, en veillant à la confidentialité des recherches que les services de renseignement et de sécurité peuvent effectuer dans les banques de données externes à leurs propres services (ex. une banque de données terro), lorsqu'un accès en ligne est installé. En effet, le fait que des personnes extérieures au service de renseignement concerné par la recherche peuvent prendre connaissance de celle-ci, est susceptible de mettre en péril les protections que les services de renseignement sont tenus de garantir. Par exemple, lorsqu'un service étranger informe la Sûreté de l'État d'une menace imminente en relation avec Monsieur XY, né le 01.01 2001, de nationalité belge, la Sûreté de l'État va notamment commencer par vérifier s'il y a concordance entre l'individu signalé et l'existence d'une telle personne dans une banque de données spécialisée, par exemple terro, et s'il n'existe pas de méprise avec un autre individu. L'identification correcte de la menace potentielle est évidemment primordiale. Par ailleurs, l'information transmise par le service de renseignement étranger doit être protégée par la Sûreté de l'État et ne peut être divulguée avant que les résultats de l'enquête ne cautionnent l'information transmise.

La protection des enquêtes menées par les services de renseignement est également importante pour les personnes concernées. En effet, le fait qu'un service de renseignement s'intéresse à une personne entraîne, malheureusement souvent, dans l'esprit de

inlichtingenwereld snel ongunstige conclusies trekt over de persoon in kwestie wat leidt tot reputatieschade voor hem of haar. Dit negatieve effect moet koste wat het kost worden vermeden.

Het is immers duidelijk dat men een risico neemt op het vlak van de vertrouwelijkheid, wanneer men weet, en dit is feitelijk zo, dat de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming zich moeten laten bijstaan door een ICT-dienst van tientallen personen om controle uit te oefenen op de voornamelijk organisatorische verplichtingen (bijvoorbeeld het naleven van het "need to know"-beginsel) bij de verwerking van persoonsgegevens.

Het spreekt ook voor zich dat hoe vaker het bestaan van onderzoeken gedeeld wordt buiten de inlichtingendiensten, hoe hoger het risico is dat hun onderzoeken in het gedrang komen.

Om deze redenen mogen de opzoekingen die de inlichtingen- en veiligheidsdiensten verrichten voor hun onderzoeken enkel gekend zijn door een zeer beperkt aantal personen die niet tot deze diensten behoren. Het is in dat geval vanzelfsprekend dat het delen van gegevens beveiligd moet zijn (need to share securely). In het kader van een toegang tot een externe gegevensbank is het de verwerkingsverantwoordelijke in eigen persoon of de persoon die hij daartoe aanwijst die de wettelijke opdrachten van toezicht uitoefent (de "of" zijnde exclusief) op de door de inlichtingendiensten uitgevoerde verwerkingen in de externe gegevensbank waarvoor hij verantwoordelijk is. Het gaat om één enkele persoon. De functionaris voor gegevensbescherming van de betrokken externe gegevensbank heeft ook toegang tot de logs van de verwerkingen van de inlichtingendiensten in de gegevensbank waarvoor hij belast is met het toezicht op de naleving van de wetgeving. Hij moet immers zijn wettelijke opdracht van toezicht kunnen uitoefenen. Om op de opmerking in het punt 129 van het advies van de Privacycommissie te antwoorden waarin zij meent dat het ontwerp duidelijk moet maken dat het altijd slechts om een en dezelfde fysieke persoon gaat, wordt verduidelijkt dat de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming van de externe gegevensbank slechts twee en enkel twee personen vertegenwoordigen.

Om de vertrouwelijkheid van de verwerkingen in de betrokken externe gegevensbank te beschermen, wordt de toegang van deze personen verzekerd door de toepassing van technische, organisatorische en persoonlijke beveiligingsmaatregelen. Deze bepaling gaat niet in op de details van de technische maatregelen omdat het door de technologische vooruitgang niet mogelijk is om

non-familiarisés avec le monde du renseignement, des conclusions rapides défavorables à la personne concernée qui lui cause un dommage réputationnel.

Il faut évidemment éviter cet effet pervers à tout prix. Sur le plan de la confidentialité, et du risque encouru pour celle-ci, c'est par ailleurs un état de fait que le responsable du traitement et le délégué à la protection des données doivent se faire assister d'une équipe ICT (composée de dizaines de personnes) pour exercer le contrôle sur le respect des obligations notamment organisationnelles (par exemple, pour le respect du need to know), lors de traitements de données à caractère personnel.

De toute évidence, il est clair aussi que plus l'existence d'enquêtes est partagée en dehors des services de renseignement, plus le risque est grand que leurs enquêtes soient grillées.

Pour ces raisons, les recherches que font les services de renseignement et de sécurité dans le cadre de leurs enquêtes ne peuvent être connues que d'un nombre très limité de personnes externes auxdits services. Dans ce cas, il va de soi que le partage de données doit être sécurisé (need to share securely). Dans le cadre d'un accès à une banque de données externe, il s'agit du responsable du traitement en personne ou la personne qu'il désigne à cet effet (le "ou" étant exclusif) pour exercer ses missions légales de contrôle sur les traitements effectués par les services de renseignement dans la banque de données externe dont il est le responsable. Il s'agit d'une seule personne. Le délégué à la protection des données de la banque de données externe concernée a également accès aux loggings des traitements des services de renseignement dans la banque de données pour laquelle il a la charge de veiller au respect de la législation. Il doit en effet pouvoir exercer sa mission légale de contrôle. Pour rencontrer la remarque de la Commission vie privée qui estime, dans son point 129, que le projet devrait spécifier clairement qu'il ne s'agit toujours que d'une seule et même personne, il est précisé que le responsable du traitement et le délégué à la protection des données de la banque de données externe ne représentent donc que deux et seulement deux personnes.

Pour protéger la confidentialité des traitements dans la banque de données externe concernée, l'accès de ces personnes sera assuré par la mise en œuvre de mesures de sécurité techniques, organisationnelles et personnelles. Cette disposition n'entre pas dans le détail des mesures techniques, parce l'évolution de la technologie ne permet pas de déterminer dans une loi

in een wet te bepalen welke middelen gebruikt worden. Dit zouden versleutelingsmethodes kunnen zijn, maar ook andere oplossingen. Organisatorische en individuele maatregelen zijn bijvoorbeeld de vereiste van een veiligheidsmachtiging van ten minste het niveau geheim om toegang te krijgen tot de logs van de verwerkingen van de inlichtingendiensten.

Er dient te worden opgemerkt dat de bescherming niet gerechtvaardigd is voor de verwerkingen van het OCAD in de gegevensbanken bedoeld in artikel 44/2 § 1 wet op het politieambt aangezien het OCAD geen orgaan is dat gegevens verzameld en geen onderzoeken uitvoert. Het doet dus geen opsporingen of enig andere verwerking in de hogerbedoelde externe gegevensbanken op basis van gegevens die de inlichtingendiensten hen zouden overgemaakt hebben. Het OCAD coördineert de analyse van de overgemaakt inlichtingen.

Er moet ook benadrukt worden dat hun toegang enkel voor toezichtsdoeleinden gebruikt mag worden. Indien andere doeleinden nodig blijken (bijvoorbeeld, voor de verrekening van de raadplegingen dient men toegang te hebben tot het aantal loggings, voorziet de bepaling dat deze in een protocolakkoord tussen de betrokken verwerkingsverantwoordelijken vastgesteld moeten worden. Naar het voorbeeld van de wijzigingen aangebracht aan artikel 13, volgend op de opmerking van de Privacycommissie (punt 130) en de Raad van State (pagina 18) over het feit dat de bepaling de toegang mogelijk maakt tot de loggings voor andere doeleinden dan een controle, aan de hand van een protocol gesloten tussen betrokken verwerkingsverantwoordelijken, werd het ontwerp aangepast in overeenstemming met deze opmerking. De andere doeleinden waarvoor een toegang zou kunnen worden voorzien buiten deze van de controle zullen enkel mogelijk zijn indien een wet dit toelaat. Het wettelijkheids- en een voorzienbaarheidsprincipe moeten in elk geval worden nageleefd.

Naast de verwerkingsverantwoordelijke van de betrokken externe gegevensbank en zijn functionaris voor gegevensbescherming wordt er ook op gewezen dat de verwerkingsverantwoordelijke van de betrokken overheden bedoeld in titel 3 en zijn functionaris voor gegevensbescherming uiteraard toegang hebben om de wettelijke conformiteit van de door de leden van de betrokken inlichtingen- en veiligheidsdienst uitgevoerde verwerkingen te kunnen controleren.

We kunnen niet uitsluiten dat het nodig is om toegang te verlenen aan een andere persoon dan zij die hierboven vermeld zijn, bijvoorbeeld voor technische ondersteuning. In dat geval voorziet dit artikel de mogelijkheid om een bijkomende persoon aan te wijzen in een protocolakkoord tussen de betrokken

quels seront les moyens utilisés. Il pourrait s'agir de méthodes de chiffrement mais aussi d'autres solutions. Pour les mesures organisationnelles et individuelles, on peut citer, par exemple, l'exigence d'une habilitation de sécurité d'un niveau au moins secret pour accéder aux loggings des traitements des services de renseignement.

Il convient de préciser que la protection ne se justifie pas pour les traitements de l'OCAM dans les banques de données visées à l'article 44/2, § 1er, de la loi sur la fonction de police car l'OCAM n'est pas un organe de collecte de données et n'effectue pas d'enquête. Dès lors, il ne fait pas de recherches ou tout autre traitement dans les banques de données externes susvisées, à partir de données que les services de renseignement lui auraient transmises. L'OCAM coordonne l'analyse des renseignements transmis.

Il est important aussi de souligner que leur accès ne pourra être utilisé qu'à des fins de contrôle. Si d'autres finalités s'avèrent nécessaires (par exemple, pour la facturation des consultations, il faut avoir accès au nombre de loggings), la disposition prévoit qu'elles doivent être définies dans un protocole d'accord entre les responsables du traitement concernés. A l'instar des adaptations apportées à l'article 13, à la suite de la remarque de la Commission vie privée (point 130) et du Conseil d'État (page 18), sur le fait que la disposition permette l'accès aux loggings pour d'autres finalités que celle du contrôle, par le biais d'un protocole conclu entre les responsables du traitement concernés, le projet a été adapté conformément à cette remarque. Les autres finalités pour lesquelles un accès pourrait être prévu en dehors de celle du contrôle ne pourront être visées que si une loi l'autorise. Les principes de légalité et de prévisibilité doivent en tout état de cause être respectés.

A côté du responsable du traitement de la banque de données externe concernée et de son délégué à la protection des données, il est également indiqué que le responsable du traitement pour l'autorité visée au titre 3 concerné et son délégué à la protection des données ont bien entendu un accès pour pouvoir vérifier la conformité légale des traitements effectués par les membres du service de renseignement et de sécurité concerné.

On ne peut exclure qu'il soit nécessaire d'accorder un accès à une autre personne que celles qui sont visées plus haut, par exemple pour un support technique. Dans ce cas, cet article prévoit la possibilité de désigner la personne supplémentaire dans un protocole d'accord entre les responsables du traitement concernés. La

verwerkingsverantwoordelijken. De Privacycommissie uit een voorbehoud, in punt 130 van haar advies, voor wat betreft deze mogelijkheid voorzien in punt 5° om eenvoudig bij wijze van protocol de toegang uit te breiden tot derden voor andere doeleinden dan de controle. De Raad van State formuleert dezelfde opmerking voor een gelijkaardige bepaling van deze titel (pagina 33). Om tegemoet te komen aan de Privacycommissie en de Raad van State verduidelijkt het ontwerp dat deze mogelijkheid om een derde persoon aan te duiden slechts toegelaten is om de controle effectief te maken. Het betreft dus a priori de ondersteuning door een informaticus personeelslid.

Het is duidelijk dat naast het door de verschillende bovengenoemde actoren uitgeoefende toezicht de autoriteit die bevoegd is om toezicht uit te oefenen op de inlichtingendiensten ook de logs en de desbetreffende verwerkingen tot haar beschikking moet hebben.

Er moet benadrukt worden dat de toegangen tot de gegevensbanken intern altijd heel streng georganiseerd zijn. Vooreerst worden de toegangen enkel toegekend aan de agenten die het echt nodig hebben om hun werk te kunnen uitvoeren. De juridische dienst van de inlichtingendiensten heeft bijvoorbeeld geen toegang tot de gegevensbank van de penitentiaire inrichtingen. De opzoekingen worden daarenboven gevalideerd door de functionele chef van de agent die de opzoeking verricht. Bepaalde opzoekingen vereisen zelfs een beslissing van het diensthoofd. Ten slotte worden er periodiek steekproeven genomen om de wettelijkheid en de proportionaliteit van de verwerkingen te controleren. Dit is een solide basis. Dit moet gepaard gaan met een performante externe controle door de autoriteit die toezicht houdt op de inlichtingen- en veiligheidsdiensten zoals hiervoor vermeld. In overeenstemming met de wens van de Privacycommissie (algemene opmerking, en in het bijzonder punt 123) verduidelijkt het ontwerp telkens dat mogelijk is welke toezichthoudende autoriteit bevoegd is. In dit geval, het Vast Comité I.

Om te antwoorden op de verzoeken van de Privacycommissie (punt 220 van het advies) en van de Raad van State (pagina 33 van het advies) over het gebrek aan definitie van de notie controlesysteem werden de termen geschrapt en vervangen door meer duidelijke termen. Zo wordt er verduidelijkt dat het de logbestanden en de technische, organisatorische en individuele beveiligingsmaatregelen betreft die ter beschikking worden gesteld van het Vast Comité I.

Tot slot wordt er bepaald dat de overheden bedoeld in titel 3 mogen afwijken van de technische, organisatorische en individuele beveiligingsmaatregelen ter bescherming van hun verwerkingen, indien zij van mening

Commission vie privée émet une réserve, dans le point 130 de son avis, quant à cette faculté prévue dans le 5°, d'élargir, par simple protocole, l'accès à des tiers pour d'autres finalités que celle du contrôle. Le Conseil d'État formule la même remarque pour une disposition similaire de ce titre (page 33). Pour apaiser la Commission vie privée et le Conseil d'État, le projet précise que cette possibilité de désigner une tierce personne n'est permise que pour rendre effectif le contrôle. Il s'agit a priori de l'appui d'un membre du personnel informatique.

Il est évident que parallèlement au contrôle exercé par les différents acteurs cités plus haut, l'autorité compétente pour exercer un contrôle sur les services de renseignement doit également avoir à sa disposition les loggings et les traitements qui y sont liés.

Il faut souligner que les accès aux banques de données sont déjà organisés en interne de manière très rigoureuse. En premier lieu, les accès ne sont accordés qu'aux agents qui en ont réellement besoin pour accomplir leur travail. Par exemple, le service juridique des services de renseignement n'a pas accès à la banque de données des établissements pénitentiaires. Ensuite, les recherches effectuées sont couvertes par le chef fonctionnel des agents qui y procèdent. Certaines recherches nécessitent même une décision du dirigeant du service. Enfin, des contrôles aléatoires périodiques sont réalisés pour vérifier la légalité et la proportionnalité des traitements effectués. C'est une base solide. Il convient de la coupler avec un contrôle extérieur performant de l'autorité de contrôle des services de renseignement et de sécurité, comme développé plus haut. Conformément au souhait de la Commission vie privée (remarque générale, et notamment point 123), chaque fois que cela est possible le projet précise quelle autorité de contrôle est compétente. En l'occurrence, c'est le Comité permanent R.

Pour répondre aux demandes formulées par la Commission vie privée (point 220 de son avis) et par le Conseil d'État (page 33 de son avis) sur le manque de définition de la notion de système de contrôle, les termes ont été supprimés pour être remplacés par des termes plus précis. Ainsi, il est précisé que ce sont les journaux et les mesures de sécurité techniques, organisationnelles et individuelles qui sont mis à disposition du Comité permanent R.

Enfin, il est précisé que les autorités visées au titre 3 peuvent déroger aux mesures de sécurité techniques, organisationnelles et personnelles visant à protéger leurs traitements, si elles considèrent que les intérêts

zijn dat de belangen (bronnen, identiteit van agenten, discretie van onderzoeken) niet bedreigd zijn door een kennisname van hun verwerkingen. Om te antwoorden op de opmerkingen van de Privacycommissie (punt 131) en de Raad van State (pagina 18), volgens dewelke de afwijking niet kan berusten op een arbitraire beoordelingsmacht van de autoriteiten, werd het ontwerp aangepast om te verduidelijken dat de afwijking slechts kan volgen uit een situatieanalyse waarbij tot het besluit wordt gekomen dat er geen gevaar is voor de te beschermen belangen. Gemeenschappelijke gegevensbanken zijn een duidelijk voorbeeld waarbij alle maatregelen niet noodzakelijk van toepassing zijn. Gegeven het feit dat ze deze gegevensbanken aanvullen en dat er een spoor van elke transactie zichtbaar moet zijn voor de andere gebruikers, heeft de beperking van de toegang tot de verwerkingen van de betrokken dienst weinig zin. In de eerste plaats hebben de betrokken autoriteiten bedoeld in titel 3 beschouwd dat het delen van niet-geclassificeerde informatie met andere autoriteiten die deelnemen aan gemeenschappelijke gegevensbanken niet de te beschermen belangen in gevaar brengt.

Art. 48

Zoals de Privacycommissie opmerkt in punt 221 van haar advies, is huidige bepaling een weerspiegeling van artikel 17 in titel 1. Zij beoogt de beperking van de rechten van de betrokkene ten opzichte van gemeenschappelijke verwerkingen die rechtstreeks of onrechtstreeks afkomstig zijn van een bevoegde autoriteit van titel 2 en een autoriteit van titel 3. Daar waar dit artikel verschilt van het artikel 17 is dat er hier geen medewerking is van autoriteiten van titel 1 in de gezamenlijke gegevensbanken. Naar het voorbeeld van artikel 17 wordt huidig artikel ook gewijzigd om zijn toepassingsgebied te beperken tot een verbod voor een autoriteit van titel 2 om de betrokkene te informeren over het feit dat zijn gegevens werden overgemaakt aan een gezamenlijke gegevensbank. Deze uitzondering tast niet de rechten van de betrokkene aan ten opzichte van de verwerking van zijn gegevens door de autoriteit onderworpen aan titel 2 voor de eigen doeleinden. Deze autoriteit kan gewoonweg niet onthullen aan de betrokkene dat het deze gegevens geleverd heeft aan de gezamenlijke gegevensbank.

Om te antwoorden op het verzoek van de Privacycommissie (punt 222 van haar advies) enerzijds en van de Raad van State (pagina 19 van het advies) anderzijds, werd een definitie van gezamenlijke gegevensbank toegevoegd aan het ontwerp. Het kan gaan om gemeenschappelijke gegevensbanken in de zin van artikel 44/11/3*bis* wet op het politieambt maar ook om andere oefeningen van gemeenschappelijke

(sources, identité des agents, discrétion des enquêtes) ne sont pas menacés par une prise de connaissance de leurs traitements. Pour répondre aux remarques de la Commission vie privée (point 131) et du Conseil d'État (page 18), selon lesquelles la dérogation ne pouvait pas reposer sur un pouvoir d'appréciation arbitraire des autorités, le projet a été adapté pour préciser que la dérogation ne pouvait découler que d'une analyse de la situation concluant à l'absence de danger pour les intérêts à protéger. Les banques de données communes sont un exemple évident où toutes les mesures ne sont pas nécessairement d'application. Dès lors qu'ils alimentent ces banques de données et qu'une trace de chaque transaction doit être visible pour les autres utilisateurs, la limitation de l'accès aux traitements du service concerné n'a pas beaucoup de sens. A la base, les autorités concernées visées au titre 3 ont considéré que le partage d'informations non classifiées avec d'autres autorités qui participent aux banques de données communes ne mettaient pas les intérêts à protéger en danger.

Art. 48

Comme l'observe la Commission vie privée, dans le point 221 de son avis, la présente disposition est le reflet de l'article 17, dans le titre 1er. Elle vise la limitation des droits de la personne concernée à l'égard des traitements communs de données émanant directement ou indirectement d'une autorité compétente du titre 2 et d'une autorité du titre 3. A la différence de l'article 17, il n'y a pas de participation d'autorités du titre 1er dans la banque de données conjointe. A l'instar de l'adaptation opérée à l'article 17, le présent article est également modifié pour limiter son champ d'application à une interdiction pour une autorité du titre 2 d'informer la personne concernée que ses données ont été communiquées à une banque de données conjointe. Cette exception n'empiète pas sur les droits de la personne concernée à l'égard des données traitées par l'autorité soumise au titre 2 pour ses propres finalités. Cette autorité ne peut simplement pas dévoiler à la personne concernée qu'elle a fourni ces données à la banque de données conjointe.

Pour répondre à la demande de la Commission vie privée (point 222 de son avis), d'une part, et du Conseil d'État (page 19 de son avis), d'autre part, une définition de banque de données conjointe a été ajoutée dans le projet. Il peut s'agir des banques de données communes telles que visées à l'article 44/11/3*bis* de la loi sur la fonction de police, mais aussi d'autres exercices communs de traitements de données à

gegevensverwerkingen. Het is dus niet pertinent om hen aan te duiden in deze wet. Trouwens, het spreekt voor zich dat de gegevensbanken van het OCAD en de Passagiersinformatie-eenheid geen gezamenlijke gegevensbanken zijn omdat het niet een gemeescnhappelijke oefening van meerdere autoriteiten betreft.

Art. 49

Zoals artikel 15 betreft het hier bepalingen die tot doel hebben de verplichtingen te bepalen van de verantwoordelijke voor de verwerking en de bevoegde autoriteit bedoeld in de huidige titel wanneer zij beschikken over persoonsgegevens afkomstig van een verwerking door de Passagiersinformatie-eenheid.

Omwille van evidente redenen van veiligheid en discretie hebt de verwerkingsverantwoordelijke het verbod om de betrokkene te informeren dat zij beschikken over dergelijke gegevens.

Paragraaf 2 voorziet een uitzondering: wanneer de verwerkingsverantwoordelijke wettelijk ertoe gehouden is om alle gegevens, die zij ter schikking heeft, over te maken.

Teneinde te vermijden dat de verwerkingsverantwoordelijke de betrokkene alarmeert, specifieert paragraaf 3 van huidig artikel dat de verwerkingsverantwoordelijke geen enkele vermelding mag maken die een indicatie kan geven aangaande het feit dat deze over dergelijke gegevens zou beschikken.

Paragraaf 4, die dezelfde beperkingen toepast voor wat betreft de oplijsting van de uitgevoerde verwerkingen door de PIE binnen de gegevensbanken van de verwerkingsverantwoordelijke bedoeld in deze titel, is er voornamelijk op gericht om ervoor te zorgen dat de informatie, volgens dewelke de PIE een dergelijke gegevensbank heeft geraadpleegd, niet gecommuniceerd zou kunnen worden aan de betrokkene.

HOOFDSTUK IV

Verwerkingsverantwoordelijke en verwerker

De reflecties over het vastleggen van de verwerkingsverantwoordelijke, de verwerker, de medeverantwoordelijken voor de verwerking, de gezamenlijke verantwoordelijkheid voor de verschillende verwerkingen op grond van de aard en doeleinden ervan zijn aan de gang. De toenemende informatisering van de “law enforcement” en de verschijning van allerlei soorten gegevensbanken en computertoepassingen doet nieuwe

carcatère personnel. Il n’est donc pas pertinent de les désigner dans la présente loi. Par ailleurs, il va de soi que les banques de données de l’OCAM et de l’Unité d’information des passagers ne sont pas des banques de données conjointes car il ne s’agit pas d’un exercice commun par plusieurs autorités.

Art. 49

Comme l’article 15, il s’agit ici de dispositions qui visent à déterminer les obligations du responsable du traitement et de l’autorité compétente visés dans le présent titre lorsqu’ils disposent de données à caractère personnel émanant d’un traitement de données à caractère personnel par l’Unité d’information des passagers.

Pour des raisons évidentes de sécurité et de discrétion, le responsable du traitement a l’interdiction d’informer la personne concernée qu’ils disposent de telles données.

Une exception est prévue par le paragraphe 2 : lorsque le responsable du traitement est légalement tenu de transmettre toutes les données à sa disposition.

Pour éviter que le responsable du traitement ne mette la puce à l’oreille de la personne concernée, le paragraphe 3 du présent article précise que le responsable du traitement ne peut faire aucune mention qui serait susceptible de donner une indication sur le fait qu’il disposerait de telles données.

Le paragraphe 4, appliquant les mêmes limitations à la journalisation des traitements effectués par l’UIP dans les banques de données des responsables du traitement visés dans ce titre est essentiellement destiné à faire en sorte que l’information selon laquelle l’UIP a consulté une telle banque de données ne puisse être communiquée à la personne concernée.

CHAPITRE IV

Responsable du traitement et sous-traitant

Les réflexions sur la détermination du responsable du traitement / sous-traitant / co-responsables du traitement/responsabilité commune des différents traitements en fonction de leur nature et finalités sont en cours. L’informatisation grandissante du law enforcement et l’apparition de toutes sortes de banques de données et applications informatiques fait naître de nouvelles préoccupations. Avec l’autonomisation de

bezorgdheden ontstaan. Met de verzelfstandiging van de rechterlijke orde moet noodzakelijkerwijs een verschuiving van de verantwoordelijkheid plaatsvinden. De verwerkingsverantwoordelijke en voortaan ook de verwerker moeten verplichtingen in acht nemen (recht op inzage, beveiligingsmaatregelen, beveiligingsplan, mededeling van de inbreuken op de beveiliging ...) en zijn verantwoordelijk voor enige inbreuk op deze wet. In vergelijking met de WVP werden verschillende aanvullende verplichtingen toegevoegd inzonderheid inzake de in te voeren technische en organisatorische maatregelen, alsmede het houden van een register, logbestanden, effectbeoordeling ...

Afdeling 1

Technische en organisatorische maatregelen

Art. 50

(Artikel 19 van de Richtlijn)

Bij die maatregelen moet rekening worden gehouden met de aard, de reikwijdte, de context en de finaliteiten van de verwerking alsook het risico die zij stellen voor de rechten en vrijheden van natuurlijke personen. De door de verwerkingsverantwoordelijke genomen maatregelen dienen onder meer te bestaan in het opstellen en implementeren van specifieke waarborgen inzake de behandeling van persoonsgegevens van kwetsbare natuurlijke personen, zoals kinderen.

Zoals gewenst door de Raad van State wordt het artikel aangevuld teneinde artikel 19 van de Richtlijn in zijn geheel om te zetten.

Art. 51

(Artikel 20 van de Richtlijn)

Hier wordt verduidelijkt wat wordt verstaan onder organisatorische en technische maatregelen. De tenuitvoerlegging van die maatregelen mag niet alleen van economische overwegingen afhangen. Om de naleving van deze titel te kunnen aantonen, dient de verwerkingsverantwoordelijke interne regels vast te leggen en maatregelen te implementeren die in het bijzonder voldoen aan de beginselen van “privacy by design” en “privacy by default”. Wanneer de verwerkingsverantwoordelijke ingevolge deze titel een gegevensbeschermingseffectbeoordeling heeft uitgevoerd, dienen de resultaten daarvan in acht te worden genomen bij de ontwikkeling van die maatregelen en procedures. Die maatregelen

l’ordre judiciaire, un déplacement de la responsabilité doit nécessairement avoir lieu. Le responsable du traitement, et désormais le sous-traitant, ont des obligations à respecter (droit d’accès, mesures de sécurité, plan de sécurité, communication des brèches de sécurité, …) et sont responsables pour toutes infractions à la présente loi. Par rapport à la LVP, plusieurs obligations supplémentaires ont été ajoutées notamment dans les mesures organisationnelles et techniques à mettre en place, ainsi que la tenue de registre, de fichiers de journalisation, d’analyse d’impact, …

Section 1

Mesures organisationnelles et techniques

Art. 50

(Article 19 de la Directive)

Ces mesures doivent tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que ceux-ci présentent pour les droits et libertés des personnes physiques. Les mesures prises par le responsable du traitement doivent comprendre l’établissement et la mise en œuvre de garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes physiques vulnérables telles que les enfants.

Comme souhaité par le Conseil d’État, l’article est complété afin de transposer complètement l’article 19 de la Directive.

Art. 51

(Article 20 de la Directive)

Il est ici précisé ce qu’on entend par mesures techniques et organisationnelles. La mise en œuvre de telles mesures ne doit pas dépendre uniquement de considérations économiques. Afin d’être en mesure de démontrer qu’il respecte le présent titre, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut, avec d’autres mots “privacy by design” en “privacy by default”. Lorsque le responsable du traitement a procédé à une analyse d’impact relative à la protection des données en vertu du présent titre, les résultats doivent être pris en compte

kunnen onder meer inhouden dat zo spoedig mogelijk wordt overgegaan tot pseudonimisering.

Die organisatorische en technische maatregelen moeten worden geëvalueerd rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, de reikwijdte, de context en de finaliteiten van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, welke aan de verwerking zijn verbonden.

Onder risico's wordt verstaan, lichamelijke, materiële of immateriële schade, met name:

— wanneer de verwerking kan leiden tot discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde gegevens, ongeoorloofde ongedaan making van pseudonimisering, of enig ander aanzienlijk economisch of maatschappelijk nadeel;

— wanneer de betrokkenen hun rechten en vrijheden of de controle over hun persoonsgegevens dreigen te verliezen;

— wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt;

— wanneer genetische gegevens of biometrische gegevens worden verwerkt met het oog op de unieke identificatie van een persoon of wanneer gegevens over gezondheid of gegevens over seksueel gedrag en seksuele geaardheid of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen worden verwerkt;

— wanneer persoonlijke aspecten worden geëvalueerd, om met name aspecten van beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of belangstellingssferen, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;

— wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt;

— of wanneer de verwerking een grote hoeveelheid persoonsgegevens en een groot aantal betrokkenen betreft.

lors de l'élaboration desdites mesures et procédures. Les mesures pourraient consister notamment dans le recours à la pseudonymisation le plus tôt possible.

Ces mesures techniques et organisationnelles doivent être évaluées compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques.

On entend par risques, des dommages physiques matériels ou un préjudice moral, en particulier:

— lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important;

— lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel;

— lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques ou l'appartenance syndicale;

— lorsque des données génétiques ou biométriques sont traitées afin d'identifier une personne de manière unique ou lorsque des données concernant la santé ou des données concernant la vie sexuelle et l'orientation sexuelle, ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes sont traitées;

— lorsque des aspects personnels sont évalués, en particulier dans le cadre de l'analyse et de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels;

— lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants;

— ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.

De waarschijnlijkheid en ernst van het risico moet worden bepaald op basis van de aard, de reikwijdte, de context en de finaliteiten van de gegevensverwerking. Het risico moet worden beoordeeld op basis van een objectieve evaluatie, aan de hand waarvan wordt bepaald of de gegevensverwerking een hoog risico inhoudt. Een hoog risico is een bijzonder risico op aantasting van de rechten en vrijheden van betrokkenen.

Afdeling 2

Gezamelijke verwerkingsverantwoordelijken

Art. 52

(artikel 24 van de Richtlijn)

Voor de bescherming van de rechten en vrijheden van de betrokkenen en de verantwoordelijkheid en aansprakelijkheid van verwerkingsverantwoordelijken en verwerkers, onder meer wat de monitoring door en de maatregelen van toezichthoudende autoriteiten betreft, is het noodzakelijk dat de bij deze titel vastgestelde verantwoordelijkheden op duidelijke wijze worden toegekend, onder meer voor het geval waarin een verwerkingsverantwoordelijke de doeleinden en de middelen voor de verwerking samen met andere verwerkingsverantwoordelijken vaststelt, of wanneer een verwerking namens een verwerkingsverantwoordelijke wordt uitgevoerd.

Afdeling 3

Verwerker

Art. 53 en 54

(Artikelen 22 tot 23 van de Richtlijn)

De uitvoering van een verwerking door een verwerker dient te worden geregeld door een rechtshandeling, of een overeenkomst die de verwerker bindt aan de verwerkingsverantwoordelijke, en waarin met name is bepaald dat de verwerker uitsluitend op instructie van de verwerkingsverantwoordelijke dient te handelen, bij gebrek hieraan neemt de verwerker zijn verantwoordelijkheid op zich als een verantwoordelijke, in voorkomend geval, door de initiële verantwoordelijke van zijn verantwoordelijkheid vrij te pleiten. De verwerker dient de beginselen van gegevensbescherming van “privacy by design” en “privacy by default” in acht te nemen.

Deze bepaling creëert geen rechten maar verplichtingen en een verantwoordelijkheid van de verwerkers die hun bevoegdheden op grond van de overeenkomst

Il convient de déterminer la probabilité et la gravité du risque en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque doit faire l’objet d’une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque élevé. On entend par risque élevé un risque particulier de porter atteinte aux droits et aux libertés des personnes concernées.

Section 2

Responsables conjoints du traitement

Art. 52

(article 21 de la Directive)

La protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et des sous-traitants, y compris dans le cadre de la surveillance exercée par les autorités de contrôle et des mesures prises par celles-ci, exige une répartition claire des responsabilités fixées dans le présent titre, y compris dans le cas où le responsable du traitement détermine les finalités et les moyens du traitement conjointement avec d’autres responsables du traitement, ou lorsqu’un traitement est effectué pour le compte d’un responsable du traitement.

Section 3

Sous-traitant

Art. 53 et 54

(Articles 22 à 23 de la Directive)

La réalisation du traitement par un sous-traitant doit être régie par un acte juridique ou un contrat liant le sous-traitant au responsable du traitement et prévoyant notamment que le sous-traitant ne devrait agir que sur instruction du responsable du traitement, à défaut, le sous-traitant engage sa responsabilité comme tout responsable du traitement, le cas échéant en exonérant le responsable du traitement initial de sa responsabilité. Le sous-traitant doit tenir compte du principe de protection des données “dès la conception” et “par défaut”.

Cette disposition ne crée pas de droits mais des obligations et une responsabilité des sous-traitants qui auraient outrepassé leurs pouvoirs en vertu du contrat

met de verwerkingsverantwoordelijke zouden hebben overschreden. De vraag rijst des te meer wanneer de verwerker een particulier orgaan is. De bevoegde toezichthoudende autoriteit voor de verantwoordelijke zal ook de opvolging bij de verwerker moeten verzekeren. Het principe van "bijzaak volgt hoofdzaak" zou moeten gelden. Alleen de bevoegde toezichthoudende autoriteit van de verwerkingsverantwoordelijke heeft een duidelijk beeld van de algehele behandeling en de bijbehorende risico's.

Om de door de betrokkene uitgeoefende rechten te vergemakkelijken, kan het akkoord voorzien in één enkel contactpunt.

Een verwerking van persoonsgegevens kan ook plaatsvinden onder het gezag van een Belgische bevoegde overheid samen met een buitenlandse bevoegde overheid of een internationale organisatie, bijvoorbeeld bij de creatie van gezamenlijk bestand. In voorkomend geval zullen de Belgische en de buitenlandse verwerkingsverantwoordelijken samen de gezamenlijke verwerkingsverantwoordelijken zijn.

Het kan inderdaad voorkomen dat er een gemeenschappelijke databank wordt opgezet, die wordt beheerd door twee politiediensten van twee verschillende landen. Dit is het geval bij de Centra voor Politie- en Douanesamenwerking (CPDS). Artikel 7 van de Belgisch-Franse Akkoord inzake politiesamenwerking (Doornik II) brengt een dergelijk "gemeenschappelijk bestand" tot stand in het CPDS te Doornik (BE-FR), net als artikel 4 van het Verdrag dat het CPDS (BE-FR-DE-LUX) in Luxemburg opricht. Men kan verder ook denken aan gemengde databanken in een grensstreek, bijvoorbeeld een bestand dat de informatie bevat over de inbraken die zich gedurende de laatste jaren hebben voorgedaan aan beide kanten van de grens, gezamenlijk beheerd door de korpschef aan Belgische kant en zijn ambtsgenoot aan de andere kant van de grens.

Afdeling 4

Verplichtingen

Art. 55

De verklaring bij de toezichthoudende autoriteit wordt geschrapt.

De verwerkingsverantwoordelijke of de verwerker moet een register bijhouden van alle categorieën van verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Het gaat om een register van

qui les lient au responsable du traitement. La question se posera d'autant plus lorsque le sous-traitant est un organisme privé. L'autorité de contrôle compétente pour le responsable du traitement devra également assurer le suivi auprès des sous-traitant. Le principe comme quoi "l'accessoire suit le principal" devra s'appliquer. Seule l'autorité de contrôle du responsable du traitement aura une vue claire de l'ensemble du traitement et des risques y associés.

Pour faciliter les droits exercés par la personne concernée, l'accord peut prévoir un seul point de contact.

Un traitement de données à caractère personnel peut également avoir lieu sous l'autorité d'une autorité compétente belge conjointement avec une autorité compétente étrangère ou une organisation internationale, par exemple lors de la création d'un dossier conjoint. Le cas échéant, les responsables du traitement belges et étrangers seront ensemble les responsables du traitement conjoints.

Il peut en effet être créé une banque de données commune, géré par deux services de police de deux différents pays. C'est le cas dans le cadre des Centres de Coopération Policière et Douanière (CCPD). L'article 7 de l'accord de coopération policière FR-BE (Tournai II) met en place un tel "fichier commun" dans le CCPD de Tournai (BE-FR), ainsi que l'art 4 du Traité qui établit le CCPD Luxembourg (BE-FR-DE-LUX). On peut en outre envisager des banques de données communes dans une région frontalière, par exemple un fichier qui contient les informations sur les cambriolages des dernières années des deux côtés de la frontière, géré ensemble par le chef de corps du côté belge et par son homologue de l'autre côté de la frontière.

Section 4

Obligations

Art. 55

La déclaration auprès de l'autorité de contrôle est supprimée.

Le responsable du traitement ou le sous-traitant doit tenir des registres pour toutes les catégories d'activités de traitement relevant de sa responsabilité. Il s'agit d'un registre de catégories de traitement ou d'activités

verwerkingscategorieën of verwerkingsactiviteiten en niet om een register van individuele verwerkingen.

Iedere verwerkingsverantwoordelijke en verwerker wordt ertoe verplicht met de toezichthoudende autoriteit samen te werken en haar dat register te verstrekken zodat zij dat kan gebruiken om op die verwerkingen toe te zien. De verwerkingsverantwoordelijke of de verwerker die persoonsgegevens verwerkt in systemen voor niet-geautomatiseerde verwerking dient te beschikken over efficiënte methoden, zoals logbestanden of andere vormen van registers, om de rechtmatigheid van de verwerking aan te tonen, om interne controle mogelijk te maken en om de integriteit en de beveiliging van gegevens te waarborgen.

In dit gedeelte worden de elementen vermeld die in het register moeten worden opgenomen. De elementen zijn identiek aan die van titel 1 van toepassing tot alle andere openbare diensten, omwille consistentie in de teksten en de systemen. Het register wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit. De elementen hernemen dus hetgeen gemeenschappelijk is aan de instrumenten en specifiek voor de openbare sector. Uiteraard, als men niet in het bezit is van zulke informatie, dan moet die niet overgenomen worden.

Wat betreft de categorie van ontvangers moet herhaald worden, zoals de Raad van State het aanhaalt in zijn advies, pagina 18, dat de inlichtingen- en veiligheidsdiensten en de autoriteiten bedoeld in ondertitel 3 van titel 3 geen ontvangers zijn in de zin van de definitie van de Verordening. De verwerking van deze gegevens door deze autoriteiten stemt in zekere mate overeen met de toepasselijke regels met betrekking tot de bescherming van gegevens in functie van de doeleinden van de verwerking. Bijgevolg worden de inlichtingen- en veiligheidsdiensten en de autoriteiten bedoeld in ondertitel 3 van titel 3 uitgesloten van de vermelding in het protocol. Trouwens, het tweede punt heeft betrekking op de naam van de functionaris voor gegevensbescherming. In elk geval geniet de naam van de functionaris voor gegevensbescherming van de inlichtingendiensten van een bijzondere bescherming in toepassing van de artikele, 36 en 43 van de organieke wet van 30 november 1998 betreffende de inlichtingen- en veiligheidsdiensten. Dit verantwoordt terdege en wettelijk het niet publiekelijk maken van deze informatie.

de traitement et non pas d'un registre de traitements individuels.

Chaque responsable du traitement et sous-traitant est tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à sa disposition pour qu'ils puissent servir au contrôle de ces opérations de traitement. Le responsable du traitement ou le sous-traitant qui traite des données à caractère personnel dans des systèmes de traitement non automatisés devrait s'être doté des moyens effectifs de démontrer la licéité du traitement, de pratiquer l'autocontrôle et de garantir l'intégrité et la sécurité des données, tels que des journaux ou d'autres formes de registres.

Le présent article prévoit les éléments qui doivent être inclus dans le registre. Les éléments sont identiques à ce qui est prévu dans le titre 1er applicable à tous les autres services publics dans l'objectif de la cohérence du texte et des systèmes. Le registre est mis à la disposition de l'autorité de contrôle compétente. Les éléments reprennent donc ce qui est commun aux instruments et spécifiques pour le secteur public. Il bien entendu que lorsqu'on n'est pas en possession de telle information, celle-ci ne doit pas être reprise.

En ce qui concerne la catégorie de destinataires, il doit être répété, comme le remarque le Conseil d'État dans son avis, page 18, que les services de renseignement et de sécurité et les autorités visées au sous-titre 3 du titre 3 ne sont pas des destinataires, au sens de la défintion du Règlement. Le traitement de ces données par ces autorités concorde de la sorte avec les règles applicables en matière de protection des données en fonction des finalités du traitement. Par conséquent, les services de renseignement et de sécurité et les autorités visées au sous-titre 3 du titre 3 sont exclus de la mention dans le registre. Par ailleurs, le deuxième point vise le nom du délégué à la protection des données. En tout état de cause, le nom du délégué à la protection des données des services de renseignement, en tant qu'agent de ces services, bénéficie d'une protection particulière en application des articles 36 et 43 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Ceci justifie pertinemment et légalement de ne pas rendre publique cette information.

Art. 56

(Artikel 25 van de Richtlijn)

Het gaat om een bijzondere verplichting die niet bestaat in de Verordening.

Er dienen logbestanden te worden bijgehouden van ten minste de volgende activiteiten in systemen voor geautomatiseerde verwerking: verzameling, wijziging, raadpleging, samenvoeging en wissing. De logbestanden van raadplegingen en bekendmakingen moeten het mogelijk maken de redenen, de datum en het tijdstip van die handelingen te achterhalen, de categorieën van personen die persoonsgegevens hebben geraadpleegd of bekendgemaakt, en de categorieën van ontvangers. De identificatie van de persoon die persoonsgegevens heeft geraadpleegd of het system die heeft deze gegevens bekendgemaakt dient, indien mogelijk, te worden geregistreerd in de logbestanden. Het is hetzelfde voor de identificatie van de ontvangers. De logbestanden dienen uitsluitend te worden gebruikt om te controleren of de gegevensverwerking rechtmatig is, om interne controle uit te oefenen, om de integriteit en de beveiliging van de gegevens te garanderen en om strafrechtelijke procedures of in deze titel bedoelde finaliteiten te waarborgen. Interne controle dient interne tuchtprocedures van bevoegde overheden te omvatten.

De verzameling impliceert noodzakelijkerwijs een record in het geval van logbestanden.

Art. 57

(Artikel 26 van de Richtlijn)

Er wordt tevens voorzien dat de verwerkingsverantwoordelijke en de verwerker, ieder wat hem betreft, met de toezichthoudende autoriteit samenwerkt.

Art. 58

Artikel 27 van de Richtlijn voorziet in de volgende verplichting: “Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de reikwijdte, de context of de doeleinden daarvan, waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert, voorzien de lidstaten erin dat de verwerkingsverantwoordelijke vóór de verwerking een beoordeling verricht van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens”. De gegevensbeschermingseffectbeoordeling moet

Art. 56

(Article 25 de la Directive)

Il s’agit d’une obligation particulière qui n’existe pas dans le Règlement.

Des fichiers de journalisation doivent être établis au moins pour les opérations effectuées dans des systèmes de traitement automatisé telles que la collecte, la modification, la consultation, l’interconnexion ou l’effacement. Les journaux des opérations de consultation et de communication doivent permettre d’établir le motif, la date et l’heure de celles-ci, les catégories de personnes qui ont consulté ou communiqué les données à caractère personnel, et les catégories de destinataires. L’identification de la personne qui a consulté ou le système qui a communiqué les données à caractère personnel devrait, si possible, apparaître dans le fichier de journalisation. Il en est de même pour l’identification des destinataires. Les fichiers de journalisation devraient être utilisés uniquement à des fins de vérification de la licéité du traitement, d’autocontrôle, de garantie de l’intégrité et de la sécurité des données et pour les besoins de procédures pénales ou des finalités visées au présent titre. L’autocontrôle comprend aussi les procédures disciplinaires internes des autorités compétentes.

La collecte implique nécessairement un enregistrement dans le cas des fichiers de journalisation.

Art. 57

(Article 26 de la Directive)

Il est prévu également que le responsable du traitement, et le sous-traitant, chacun en ce qui le concerne, coopère avec l’autorité de contrôle.

Art. 58

L’article 27 de la Directive impose que “*Lorsqu’un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d’engendrer un risque élevé pour les droits et les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue préalablement au traitement une analyse de l’impact des opérations de traitement envisagées sur la protection des données à caractère personnel*”. L’analyse d’impact relative à la protection des données

betrekking hebben op de relevante systemen en processen van de verwerkingsactiviteiten en niet op individuele gevallen.

Het is dus verplicht over te gaan tot een gegevensbeschermingseffectbeoordeling, die moet worden uitgevoerd door de verwerkingsverantwoordelijke. Zoals door de Privacycommissie werd benadrukt zal de DPO deze daar uiteraard in kunnen ondersteunen, maar daarbij mag niet uit het oog worden verloren dat de effectbeoordeling uiteindelijk aan deze laatste zal worden voorgelegd voor advies en dat deze moet worden verricht vóór elke verwerkingsactiviteit, ook al werd reeds een gegevensbeschermingseffectbeoordeling uitgevoerd in het kader van de vaststelling van de rechtsgrond.

Dit dient met name te gelden voor grootschalige verwerkingen die bedoeld zijn voor de verwerking van een aanzienlijke hoeveelheid persoonsgegevens op regionaal, nationaal of *supra*nationaal niveau, waarvan een groot aantal betrokkenen gevolgen zou kunnen ondervinden en die bijvoorbeeld vanwege hun gevoelige aard een hoog risico met zich kunnen brengen, wanneer conform het bereikte niveau van technologische kennis een nieuwe technologie op grote schaal wordt gebruikt, alsmede voor andere verwerkingen die een groot risico voor de rechten en vrijheden van de betrokkenen inhouden, met name wanneer betrokkenen als gevolg van die verwerkingen hun rechten moeilijker kunnen uitoefenen. Een gegevensbeschermingseffectbeoordeling dient ook te worden gemaakt wanneer persoonsgegevens worden verwerkt met het oog op het nemen van besluiten met betrekking tot specifieke natuurlijke personen na een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen die is gebaseerd op de profilering van deze gegevens, of na de verwerking van bijzondere categorieën van persoonsgegevens, biometrische gegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Een gegevensbeschermingseffectbeoordeling is tevens nodig voor de grootschalige bewaking van openbaar toegankelijke ruimten, met name wanneer optisch-elektronische apparatuur wordt gebruikt, of voor alle andere verwerkingen wanneer de bevoegde toezichthoudende autoriteit oordeelt dat zij waarschijnlijk een groot risico inhouden voor de rechten en vrijheden van betrokkenen, met name omdat betrokkenen als gevolg van deze verwerkingen een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst, of omdat deze verwerkingen systematisch op grote schaal worden uitgevoerd.

Wanneer die beoordeling het hoge risico voor de rechten en vrijheden van de betrokkenen bevestigt, moet

doit porter sur les systèmes et processus pertinents des opérations de traitement, et non sur des cas individuels.

Il y a donc obligation de procéder à une analyse d'impact, laquelle devra être effectuée par le responsable du traitement. Comme le souligne la Commision vie privée, le DPO pourra bien évidemment assister celui-ci tout en étant attentif que l'analyse d'impact lui sera soumise pour avis et que celle-ci doit être effectuée avant toute activité de traitement même si une analyse d'impact a déjà été réalisée dans le cadre de l'adoption de la base juridique.

Cela devrait s'appliquer en particulier aux opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou *supra*national, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, en conformité avec l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle, ainsi qu'à d'autres opérations de traitement qui engendrent un risque élevé pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces personnes d'exercer leurs droits. Une analyse d'impact relative à la protection des données devrait également être effectuée lorsque des données à caractère personnel sont traitées en vue de prendre des décisions relatives à des personnes physiques spécifiques à la suite d'une évaluation systématique et approfondie d'aspects personnels propres à des personnes physiques sur la base du profilage desdites données ou à la suite du traitement de catégories particulières de données à caractère personnel, de données biométriques ou de données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes. Une analyse d'impact relative à la protection des données est de même requise aux fins de la surveillance à grande échelle de zones accessibles au public, en particulier lorsque des dispositifs optoélectroniques sont utilisés, ou pour toute autre opération pour laquelle l'autorité de contrôle compétente considère que le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, en particulier parce qu'elles empêchent ces personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat, ou parce qu'elles sont effectuées systématiquement à grande échelle.

Lorsque cette analyse confirme le risque élevé pour les droits et libertés des personnes, le responsable du

de verwerkingsverantwoordelijke vóór de verwerking de toezichthoudende autoriteit raadplegen.

Onder bepaalde omstandigheden kan het redelijk en nuttig zijn dat de gegevensbeschermingseffectbeoordeling zich niet beperkt tot een enkel project, bijvoorbeeld wanneer overheidsinstanties of -organen een gemeenschappelijke verwerkingsapplicatie of -platform willen opzetten of wanneer meerdere verwerkingsverantwoordelijken van plan zijn een gemeenschappelijke verwerkingsapplicatie of -omgeving in te voeren voor een hele bedrijfstak, of een segment daarvan, of voor een gangbare horizontale activiteit.

Art. 59

(Artikel 28 van de Richtlijn)

Wanneer een gegevensbeschermingseffectbeoordeling uitwijst dat de verwerking, bij afwezigheid van de waarborgen, beveiligingsmaatregelen en risicobeperkende mechanismen, met een hoog risico voor de rechten en vrijheden van natuurlijke personen gepaard zou gaan, en de verwerkingsverantwoordelijke van mening is dat het niet mogelijk is dat risico te beperken door middel van maatregelen die met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn, dient de bevoegde toezichthoudende autoriteit van de verwerkingsverantwoordelijke voorafgaandelijk aan de verwerking te worden geraadpleegd. Bepaalde types van persoonsgegevensverwerking en de omvang en frequentie van deze verwerkingen, hebben een dermate hoog risico om te leiden tot schade of aantasting van de rechten en vrijheden van natuurlijke personen. Als onderdeel van die raadplegingsprocedure kan het resultaat van een gegevensbeschermingseffectbeoordeling die voor de verwerking in kwestie wordt uitgevoerd, aan de toezichthoudende autoriteit worden voorgelegd, meer bepaald wat betreft de voorgenomen maatregelen om het risico voor de rechten en vrijheden van natuurlijke personen te beperken. Het is wel te verstaan dat de vereiste formaliteit de raadpleging van de toezichthoudende autoriteit is en niet de ontvangst van haar advies.

De bevoegde toezichthoudende autoriteit van de verwerkingsverantwoordelijke dient tevens te worden geraadpleegd tijdens de voorbereiding van een wetgevende of regelgevende maatregel houdende verwerking van persoonsgegevens, om ervoor te zorgen dat de voorgenomen verwerking strookt met deze titel, en met name om de risico's daarvan voor betrokkenen te beperken. Overeenkomsten tussen de verschillende toezichthoudende autoriteiten moeten worden afgesloten als

traitement doit consulter préalablement au traitement l'autorité de contrôle.

Il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée.

Art. 59

(Article 28 de la Directive)

Lorsqu'il ressort d'une analyse d'impact relative à la protection des données que, en l'absence des garanties, de mesures de sécurité et de mécanismes pour atténuer le risque, le traitement engendrerait un risque élevé pour les droits et libertés des personnes physiques et que le responsable du traitement est d'avis que le risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts de mise en œuvre, il y a lieu de consulter l'autorité de contrôle compétente du responsable du traitement avant le début des opérations de traitement. Certains types de traitements et l'ampleur et la fréquence des traitements sont susceptibles d'engendrer un tel risque élevé et peuvent également causer un dommage ou porter atteinte aux droits et libertés d'une personne physique. Dans le cadre de ce processus de consultation, les résultats d'une analyse d'impact relative à la protection des données réalisée en ce qui concerne le traitement en question peuvent être soumis à l'autorité de contrôle, notamment les mesures envisagées pour atténuer le risque pour les droits et libertés des personnes physiques. Il est bien entendu que la formalité exigée est la consultation de l'autorité de contrôle et non la réception de son avis.

L'autorité de contrôle compétente du responsable du traitement devrait également être consultée au stade de la préparation d'une mesure législative ou réglementaire qui prévoit le traitement de données à caractère personnel, afin d'assurer que le traitement prévu respecte le présent titre et, en particulier, d'atténuer le risque qu'il comporte pour la personne concernée. Des accords devront être établit entre les différentes autorités de contrôle si le dossier est introduit par plusieurs autorités

het dossier wordt ingediend bij verschillende bevoegde toezichthoudende autoriteiten, gelet op de verschillende doeleinden die dezelfde verwerking kan hebben.

Wanneer het om een verwerker gaat en hij de toezichthoudende autoriteit vóór een verwerking moet raadplegen, moet laatstgenoemde de voor de Richtlijn aangewezen toezichthoudende autoriteit raadplegen, zelfs indien de verwerker aan de door de Verordening aangewezen toezichthoudende autoriteit is onderworpen, zulks vanaf het tijdstip waarop hij gegevens verwerkt die door een toezichthoudende autoriteit worden verzameld voor de in deze titel omschreven doeleinden.

Het in paragraaf vier bedoelde advies is niet bindend.

Onverminderd de operationele vereisten, hoewel het advies is gevraagd aan de toezichthoudende autoriteit, kan de verwerking onmiddellijk plaatsvinden. Er zijn feitelijk noodsituaties die, om operationele redenen, gegevenscontroleurs de mogelijkheid moeten bieden om de gegevens onmiddellijk te verwerken, wanneer ze hun verantwoordelijkheden nemen.

Art. 60

Artikel 29 van de Richtlijn voorziet in de verplichting passende technische en organisatorische maatregelen te nemen rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, de reikwijdte, de context en de finaliteiten van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, om een op het risico afgestemd beveiligingsniveau te waarborgen. Zij kunnen gemeenschappelijk zijn voor Justitie en politiediensten.

De beveiliging van de informatie strekt ertoe het volgende te waarborgen:

— de authenticiteit van de gegevens (worden de gegevens door de bevoegde personen ingevoerd?), cf. ISO 27000; – betrouwbaarheid

— de integriteit van de gegevens (zijn de gegevens intact en beschermd tegen vernietiging en verlies? Cf. ISO 27000); – integriteit / herstel / opslag;

— de vertrouwelijkheid van de gegevens (zijn de gegevens beschermd tegen ongeoorloofde toegang, wijziging of verspreiding?), inzonderheid dankzij de pseudonimisering en de versleuteling van de gegevens; -controle op de toegang tot de apparatuur / tot de gegevens / invoercontrole

de contrôle compétentes au vu des finalités différentes qu'un même traitement peut avoir.

Lorsqu'il s'agit d'un sous-traitant et qu'il doit consulter l'autorité de contrôle préalablement à un traitement, ce dernier doit consulter l'autorité de contrôle désignée pour la Directive, même si le sous-traitant est soumis à l'autorité de contrôle désigné par le Règlement, et ce, dès le moment où il traite des données collectées par une autorité de contrôle pour les finalités définies au présent titre.

L'avis visé au paragraphe 4 n'est pas contraignant.

Sans préjudice des nécessités opérationnelles, bien que l'avis ait été demandé à l'autorité de contrôle, le traitement peut avoir lieu immédiatement. En effet, il y a des situations d'urgence, qui pour des motifs opérationnels, doivent permettre aux responsables du traitement de traiter les données immédiatement, tout en prenant leurs responsabilités.

Art. 60

L'article 29 de la Directive prévoit l'obligation de prendre des mesures techniques et organisationnelles appropriées compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque. Celles-ci peuvent être communes à la Justice et aux services de police.

La sécurité de l'information a pour objet de garantir :

— l'authenticité des données (les donnée sont-elles introduites par les personnes habilitées?), cf.ISO 27000; – fiabilité

— l'intégrité des données (les données sont-elles intactes et protégées contre la destruction et la perte?), cf. ISO 27000; – intégrité / restauration / conservation;

— la confidentialité des données (les données sont-elles protégées des accès, modification ou diffusion non autorisés?), notamment grâce à la pseudonymisation et au cryptage des données; -contrôle de l'accès aux installations / aux données / contrôle de l'introduction

— de beschikbaarheid van de gegevens (zijn de gegevens toegankelijk en beschikbaar voor de bevoegde personen?); – beschikbaarheid

— de toerekenbaarheid (worden de verschillende acties getraceerd?); – controle op de gegevensdragers

— het beginsel van data minimization (worden de gegevens beperkt tot het strikt noodzakelijke?); – noodzaak

— de beveiliging van de doorgifte en van het vervoer; – transmissiecontrole / transportcontrole

— de gebruikerscontrole (logs). – gebruikerscontrole.

De vermelde beoordeling van de risico's is niet noodzakelijkerwijs een gegevensbeschermingseffectbeoordeling bedoeld in artikel 60 maar kan ervan deel uitmaken.

Art. 61

(Artikel 30.1 van de Richtlijn)

Een inbreuk op de beveiliging kan, wanneer deze niet tijdig en adequaat wordt aangepakt, resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens of beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie.

Daarom moet de verwerkingsverantwoordelijke, zodra hij weet dat een inbreuk op de beveiliging heeft plaatsgevonden, de toezichthoudende autoriteit zonder onnodige vertraging en waar mogelijk niet meer dan 72 uur nadat hij er kennis van heeft genomen, in kennis stellen van de inbreuk op de beveiliging, tenzij de verwerkingsverantwoordelijke conform het verantwoordingsbeginsel kan aantonen dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich brengt.

Wanneer ze niet binnen 72 uur kan plaatsvinden, dient de kennisgeving vergezeld te gaan van een toelichting bij de vertraging en kan informatie zonder verdere onnodige vertraging in fasen worden verstrekt, en in ieder geval binnen 72 uur na de kennisgeving.

— la disponibilité des données (les données sont-elles accessibles et disponibles pour les personnes autorisées?); – disponibilité

— l'imputabilité (les différentes actions sont-elles tracées?); – contrôle des supports de données

— le principe de data minimization (les données sont-elles limitées au strict nécessaire?); – nécessité

— la sécurité de la transmission et du transport; – contrôle de la transmission / contrôle du transport

— le contrôle des utilisateurs (logs). – contrôle des utilisateurs.

L'évaluation des risques mentionnée n'est pas nécessairement une analyse d'impact relative à la protection des données visée à l'article 60 mais peut en faire partie.

Art. 61

(Article 30.1 de la Directive)

Une brèche de sécurité risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important pour la personne physique concernée.

En conséquence, dès que le responsable du traitement apprend qu'une brèche de sécurité s'est produite, il convient qu'il notifie cette brèche de sécurité à l'autorité de contrôle dans les meilleurs délais et, lorsque c'est possible, dans les 72 heures au plus tard après en avoir pris connaissance, à moins qu'il ne puisse démontrer, conformément au principe de responsabilité, qu'il est peu probable que brèche de sécurité en question engendre un risque pour les droits et les libertés des personnes physiques.

Si une telle notification ne peut avoir lieu dans ce délai de 72 heures, la notification devrait être assortie des motifs du retard et des informations peuvent être fournies de manière échelonnée sans autre retard indu, et en tout cas dans les 72 heures de la notification.

Art. 62

(Artikel 31 van de Richtlijn)

Wanneer de inbreuk op de beveiliging waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen met zich meebrengt, dienen de natuurlijke personen daarvan zonder onnodige vertraging in kennis te worden gesteld, zodat zij de nodige voorzorgsmaatregelen kunnen treffen. De kennisgeving moet melding maken van de aard van de inbreuk op de beveiliging en aanbevelingen bevatten over hoe de persoon in kwestie mogelijke negatieve gevolgen kan beperken. Betrokkenen dienen zo snel als redelijkerwijs mogelijk is, in nauwe samenwerking met de toezichthoudende autoriteit en met inachtneming van de door deze laatste of andere relevante bevoegde overheden aangereikte richtsnoeren, in kennis te worden gesteld. Zo zouden de betrokkenen onverwijld in kennis moeten worden gesteld wanneer een onmiddellijk risico op schade moet worden beperkt, terwijl een langere termijn gerechtvaardigd kan zijn wanneer passende maatregelen moeten worden genomen tegen aanhoudende of soortgelijke inbreuken op de beveiliging.

Wanneer door het uitstellen of beperken van de kennisgeving inzake een inbreuk op de beveiliging aan de natuurlijke persoon in kwestie niet kan worden belet dat officiële of gerechtelijke onderzoeken of procedures worden belemmerd, dat de voorkoming, de opsporing, het onderzoek of de vervolging van strafbare feiten in het gedrang komen, dat straffen niet ten uitvoer worden gelegd, dat de openbare veiligheid, de nationale veiligheid of de rechten en vrijheden van anderen niet worden beschermd, zou die kennisgeving in uitzonderlijke omstandigheden achterwege kunnen worden gelaten.

De sectorale wetten kunnen die voorwaarden verduidelijken.

Die kennisgeving is niet noodzakelijk indien de verwerkingsverantwoordelijke passende technische en organisatorische beschermingsmaatregelen, zoals versleuteling, heeft genomen.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 63 tot 65

(Artikelen 32 tot 34 van de Richtlijn)

Artikel 32 van de Richtlijn voorziet in de verplichting een functionaris voor gegevensbescherming (DPO) aan

Art. 62

(Article 31 de la Directive)

Lorsqu'une brèche de sécurité est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, celle-ci devrait être informée dans les meilleurs délais afin qu'elle puisse prendre les précautions qui s'imposent. La communication devrait décrire la nature de la brèche de sécurité et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. Il convient que de telles communications aux personnes physiques concernées soient effectuées aussi rapidement qu'il est raisonnablement possible et en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la brèche de sécurité ou la survenance de violations similaires peut justifier un délai plus long pour la communication.

Lorsque le fait de retarder ou de limiter la communication à la personne physique concernée d'une brèche de sécurité ne permet pas d'éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, d'éviter de nuire à la prévention et à la détection des infractions pénales, aux enquêtes et poursuites en la matière ou à l'exécution de sanctions pénales, de sauvegarder la sécurité publique ou la sécurité nationale, ou de protéger les droits et libertés d'autrui, la communication pourrait, dans des circonstances exceptionnelles, être omise.

Les lois sectorielles pourront préciser ces conditions.

Cette communication n'est pas nécessaire si le responsable du traitement a mis en œuvre des mesures de protection techniques et organisationnelles appropriées telles que le chiffrement par exemple.

Section 5

Délégué à la protection des données

Art. 63 à 65

(Articles 32 à 34 de la Directive)

L'article 32 de la Directive impose de désigner un délégué à la protection des données (DPO), lequel a

te wijzen die een uitgebreidere en ruimere rol heeft dan de veiligheidsadviseur die wij thans kennen.

Het gaat er dan ook om één of meerdere personen aan te wijzen die de verwerkingsverantwoordelijke bijstaat of bijstaan bij het toezicht op de interne naleving van de krachtens deze titel vastgestelde bepalingen, [*"behalve wanneer een lidstaat beslist om gerechten en andere onafhankelijke rechterlijke autoriteiten daarvan vrij te stellen in het kader van hun gerechtelijke taken"]*. Die persoon kan een lid van het bestaande personeel van de verwerkingsverantwoordelijke zijn die een speciale opleiding inzake gegevensbeschermingswetgeving en -praktijk heeft genoten om deskundigheid op dat gebied te verwerven. Het vereiste expertiseniveau dient met name te worden bepaald op grond van de uitgevoerde gegevensverwerking en de bescherming die voor de door de verwerkingsverantwoordelijke verwerkte persoonsgegevens wordt vereist. De aangewezen persoon kan zijn taken op deeltijdse of voltijdse basis uitvoeren. Verschillende verwerkingsverantwoordelijken kunnen, rekening houdend met hun organisatiestructuur en omvang, samen een functionaris voor gegevensbescherming benoemen, bijvoorbeeld in het geval van gezamenlijke middelen in centrale eenheden of tussen verwerkingsverantwoordelijken. Binnen de structuur van de verwerkingsverantwoordelijken in kwestie kunnen aan deze persoon ook verschillende functies worden toegewezen. Die persoon dient de verwerkingsverantwoordelijke en de werknemers die persoonsgegevens verwerken bij te staan door hen te informeren en te adviseren over de nakoming van hun relevante verplichtingen inzake gegevensbescherming. Deze functionarissen voor gegevensbescherming dienen in staat te zijn hun taken en verplichtingen onafhankelijk in overeenstemming met de wetgeving uit te voeren.

De Richtlijn biedt de lidstaten de mogelijkheid "*gerechten en andere onafhankelijke rechterlijke autoriteiten van die verplichting vrij [te] stellen bij de uitoefening van hun rechterlijke taken.*"Voor die optie wordt niet gekozen om verschillende redenen.

1. De keuze betreft enkel gerechten en andere onafhankelijke rechterlijke overheden bij de uitoefening van hun rechterlijke taken. Dat betekent dat in ieder geval een DPO moet worden aangewezen voor de andere taken.

2. Nut om één contactpunt in de rechterlijke orde te hebben, voor alle taken samen.

3. De Richtlijn maakt het mogelijk dat verschillende verwerkingsverantwoordelijken één en dezelfde DPO aanwijzen.

un rôle plus étendu et plus large que le conseiller en sécurité, que nous connaissons actuellement.

Il s'agit donc de désigner une ou plusieurs personne qui aiderait le responsable du traitement à vérifier le respect, au niveau interne, des dispositions adoptées en vertu du présent titre, [*"sauf lorsqu'un État membre décide que des tribunaux et d'autres autorités judiciaires indépendantes en sont dispensés dans l'exercice de leur fonction juridictionnelle."]* Cette personne peut être un membre du personnel du responsable du traitement ayant reçu une formation spéciale dans le domaine du droit et des pratiques en matière de protection des données afin d'acquérir des connaissances spécialisées dans ce domaine. Le niveau de connaissances spécialisées requis doit être déterminé notamment en fonction du traitement des données effectué et de la protection exigée pour les données à caractère personnel traitées par le responsable du traitement. Cette personne peut exercer cette fonction à temps plein ou à temps partiel. Un délégué à la protection des données peut être désigné conjointement par plusieurs responsables du traitement, compte tenu de leur structure organisationnelle et de leur taille, par exemple en cas de partage des ressources au sein d'unités centrales ou entre responsables du traitement. Cette personne peut également être désignée pour occuper différents postes au sein de la structure des responsables du traitement concernés. Elle doit aider le responsable du traitement et les employés traitant des données à caractère personnel en les informant et en les conseillant sur le respect des obligations leur incombant en matière de protection des données. Ces délégués à la protection des données devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance conformément à la législation.

La Directive permet aux États membres de dispenser *les tribunaux et d'autres autorités judiciaires indépendantes de cette obligation lorsqu'elles agissent dans l'exercice de leur fonction juridictionnelle."* Il n'est pas fait le choix de cette option pour plusieurs raisons.

1. Le choix ne porte que sur les tribunaux et autres autorités judiciaires indépendantes lorsqu'elles agissent dans l'exercice de leur fonction juridictionnelle. Ce qui signifie qu'un DPO doit en tout état de cause être désigné pour les autres tâches.

2. Utilité d'avoir un seul point de contact au sein de l'ordre judiciaire, pour toutes tâches confondues.

3. La Directive permet la désignation d'un seul et même DPO par plusieurs responsables de traitement.

Er moet worden opgemerkt dat er ter zake dan ook een verschil is tussen de Richtlijn en de Verordening. De Verordening maakt immers veeleer een uitzondering op de verplichting om een DPO aan te wijzen. Bovendien wordt in de Verordening enkel verwezen naar de gerechten bij de uitoefening van hun rechterlijke taken. Daar vloeien twee interpretaties uit voort: in het kader van de Verordening gaat het dan ook ofwel om een verbod om een DPO aan te wijzen, ofwel om een beperking op de verplichting om een DPO aan te wijzen, wat betekent dat dat een mogelijkheid blijft. In de Richtlijn gaat het om een mogelijkheid. Met het oog op de harmonisatie van de regels in de rechterlijke orde wordt evenwel ervoor gekozen slechts één regel te doen toepassen, zulks los van de finaliteit van de verwerking, te weten de verplichting om een DPO aan te wijzen, zelfs voor de gerechten bij de uitoefening van hun rechterlijke taken.

Een koninklijk besluit van 6 december 2015 regelt momenteel de taken en bevoegdheden van de adviseur voor beveiliging en gegevensbescherming. Een hervorming van dit systeem moet worden gerealiseerd om de missies van de DPO in het bestaande juridische corpus te integreren.

In artikel 32.4 van de Richtlijn wordt erin voorzien dat de verwerkingsverantwoordelijke de contactgegevens van de DPO openbaar maakt zonder nadere verduidelijking. De informatie moet gemakkelijk worden gevonden om de betrokkene de mogelijkheid te bieden zijn rechten te doen gelden. Dat zal bijvoorbeeld het geval zijn op de website van de verwerkingsverantwoordelijke.

Er wordt voorzien in een delegatie aan de Koning voor de praktische details, de werkwijze en de vereiste competenties.

In artikel 41 wordt erin voorzien dat een wet de mogelijkheid biedt af te wijken van de rechtstreekse toegang tot de DPO. Het gaat in zekere zin om de verlenging van het recht op informatie, wat bepaalde verwerkingsverantwoordelijken die het systeem van onrechtstreekse toegang invoeren dan de mogelijkheid biedt een coherent systeem te hebben. Als antwoord op het voorstel van het openbaar ministerie, er kan voor de toepassing van dit artikel niet worden afgeweken van het contactpunt. Daarvoor dient men een onrechtstreekse toegang te organiseren. In de mate dat er toepassing wordt gemaakt van de procedureregels wordt er niet afgeweken van het principe van het contactpunt van de functionaris voor gegevensbescherming.

De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.

A noter qu'il y a donc une différence entre la Directive et le Règlement sur ce point. En effet le Règlement fait plutôt d'une exception à l'obligation de désigner un DPO. De plus, le Règlement ne fait référence qu'aux seules juridictions agissant dans l'exercice de leur fonction juridictionnelle. De là découlent deux interprétations: dans le cadre du Règlement, il s'agit donc soit d'une interdiction de désigner un DPO, soit une restriction à l'obligation d'en désigner un, ce qui signifie que cela reste une faculté. Dans la Directive, il s'agit d'une faculté. Mais afin d'harmoniser les règles au sein de l'ordre judiciaire, il est opté de ne faire appliquer qu'une et même règle quel que soit la finalité du traitement, à savoir l'obligation de désigner un DPO, même pour les juridictions agissant dans l'exercice de leur fonctions juridictionnelles.

Un arrêté royal du 6 décembre 2015 règle actuellement les missions et compétences du Conseiller en sécurité et en protection des données. Une réforme de ce dispositif doit être réalisé et intégrer les missions du DPO dans le corpus légal existant.

Il est prévu à l'article 32.4 de la Directive, que le responsable du traitement publie les coordonnées du DPO sans autre précision. L'information doit être facilement trouvée pour permettre à la personne concernée de faire valoir ses droits. Ce sera le cas par exemple sur le site web du responsable du traitement.

Une délégation au Roi est prévue pour les détails pratiques, mode de fonctionnement ainsi que les compétences requises.

A l'article 41, il est prévu qu'une loi permette de déroger à l'accès direct vers le DPO. Il s'agit en quelque sorte du prolongement du droit à l'information, ce qui permet alors pour certains responsables du traitement qui mettent en place le système d'accès indirect d'avoir un système cohérent. En réponse à la proposition du ministère public, il ne peut être dérogé pour l'application de cet article au point de contact. Il faut pour cela organiser un accès indirect. Dans la mesure où il est fait application des règles de procédure, il n'est pas dérogé au principe de point de contact du délégué à la protection des données.

Le délégué à la protection des données est soumis au secret ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.

Zoals de Raad van State opmerkt wordt de verplichting tot geheimhouding of vertrouwelijkheid strafrechtelijk bestraft rekening houdende met de formulering van het artikel 458 Strafwetboek.

HOOFDSTUK V

Doorgiften van persoonsgegevens aan derde landen of internationale organisaties

Art. 66

(Artikel 35 van de Richtlijn)

Doorgifte aan een derde land of aan een internationale organisatie kan enkel plaatsvinden indien die specifieke doorgifte noodzakelijk is met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten, of de tenuitvoerlegging van straffen, waaronder de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, en indien de verwerkingsverantwoordelijke in het derde land of de internationale organisatie een bevoegde overheid is in de zin van Richtlijn.

Doorgifte kan enkel worden verricht door bevoegde overheden die als verwerkingsverantwoordelijken optreden, behalve wanneer verwerkers expliciet wordt opgedragen om namens verwerkingsverantwoordelijken gegevens door te geven. Een dergelijke doorgifte kan plaatsvinden in gevallen waarin de Europese Commissie heeft besloten dat het derde land of de internationale organisatie in kwestie een adequaat beschermingsniveau waarborgt, of in gevallen waarin passende waarborgen worden geboden of waarin afwijkingen voor specifieke situaties van toepassing zijn.

Wanneer persoonsgegevens van de Europese Unie aan verwerkingsverantwoordelijken, verwerkers of andere ontvangers in derde landen of internationale organisaties worden doorgegeven, mag dit niet ten koste gaan van het beschermingsniveau waarin voor natuurlijke personen wordt voorzien, ook in gevallen van verdere doorgiften van persoonsgegevens door het derde land of de internationale organisatie aan verwerkingsverantwoordelijken of verwerkers in hetzelfde of een ander derde land dan wel in dezelfde of een andere internationale organisatie.

Al die voorwaarden zijn cumulatieve voorwaarden en er bestaat een hiërarchie tussen de soorten doorgiften afhankelijk van hun grondslag op grond van een adequaatheidsbesluit, van passende waarborgen in of specifieke situaties.

Comme le mentionne le Conseil d'État, l'obligation de secret ou de confidentialité est sanctionnée pénalement compte tenu du libellé de l'article 458 du Code pénal.

CHAPITRE V

Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

Art. 66

(Article 35 de la Directive)

Un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que s'il est nécessaire à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, et si le responsable du traitement dans le pays tiers ou dans l'organisation internationale est une autorité compétente au sens de la Directive.

Un transfert ne peut être effectué que par les autorités compétentes agissant en qualité de responsables du traitement, sauf dans le cas où les sous-traitants sont expressément chargés de procéder au transfert pour le compte des responsables du traitement. Un tel transfert peut avoir lieu lorsque la Commission européenne a décidé que le pays tiers ou l'organisation internationale en question garantit un niveau adéquat de protection, lorsque des garanties appropriées ont été prévues ou lorsque des dérogations pour des situations particulières s'appliquent.

Lorsque des données à caractère personnel sont transférées de l'Union européenne à des responsables du traitement, à des sous-traitants ou à d'autres destinataires dans des pays tiers ou à des organisations internationales, il importe que le niveau de protection des personnes physiques ne soit pas compromis, y compris en cas de transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale à des responsables du traitement ou à des sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale.

Toutes ces conditions sont des conditions cumulatives et il existe une hiérarchie entre les types de transferts quant à ceux qui sont effectués sur base d'une décision d'adéquation, de garanties appropriées, ou de situations particulières.

Doorgifte van persoonsgegevens vanuit een lidstaat van de Europese Unie aan derde landen of internationale organisaties is in beginsel enkel toegestaan nadat de lidstaat waarvan de gegevens zijn verkregen daarin heeft toegestemd. Wanneer de bedreiging voor de openbare veiligheid van een lidstaat of derde land of voor de fundamentele belangen van een lidstaat zo onmiddellijk is dat de voorafgaande toestemming niet tijdig kan worden verkregen, dient de bevoegde overheid met het oog op een doeltreffende samenwerking op het gebied van rechtshandhaving de mogelijkheid te hebben de desbetreffende persoonsgegevens zonder voorafgaande toestemming aan het derde land of de internationale organisatie in kwestie door te geven.

Eventuele specifieke voorwaarden met betrekking tot de doorgifte moeten worden meegedeeld aan de ontvangende derde landen of internationale organisaties. Aan verdere doorgiften van persoonsgegevens naar andere derde landen of internationale organisaties dient de Belgische bevoegde overheid die de oorspronkelijke doorgifte heeft verricht voorafgaand haar toestemming te verlenen.

Wanneer de bevoegde overheid die de oorspronkelijke doorgifte heeft verricht, beslist over een verzoek om toestemming voor een verdere doorgifte, dient deze naar behoren rekening te houden met alle relevante factoren, waaronder de ernst van het strafbare feit, de specifieke voorwaarden voor en de finaliteit van de oorspronkelijke gegevensdoorgifte, de aard en de modaliteiten van de uitvoering van de strafrechtelijke sanctie, en het beschermingsniveau van de persoonsgegevens in het derde land of de internationale organisatie waaraan de persoonsgegevens verder worden doorgegeven. De bevoegde overheiddie de oorspronkelijke doorgifte heeft verricht, moet ook specifieke voorwaarden kunnen stellen aan de verdere doorgifte. Dergelijke specifieke voorwaarden kunnen worden beschreven in, bijvoorbeeld, verwerkingscodes.

Art. 67

(Artikel 36 van de Richtlijn)

De paragrafen 2 tot 6 en 8 van de Richtlijn moeten niet worden omgezet aangezien zij enkel betrekking hebben op de Europese Commissie.

De Europese Commissie heeft de bevoegdheid om te beslissen met rechtskracht voor de gehele Europese Unie, dat bepaalde derde landen, een gebied of één of

Lorsque des données à caractère personnel sont transférées d'un État membre de l'Union européenne vers des pays tiers ou à des organisations internationales, un tel transfert ne devrait en principe avoir lieu qu'après que l'État membre auprès duquel les données ont été collectées a autorisé le transfert. Il est dans l'intérêt d'une coopération efficace en matière répressive que lorsque le caractère immédiat de la menace pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre est tel qu'il rend impossible l'obtention d'une autorisation préalable en temps utile, l'autorité compétente puisse transférer les données à caractère personnel pertinentes vers le pays tiers concerné ou à l'organisation internationale concernée sans cette autorisation préalable.

Des éventuelles conditions particulières applicables au transfert doivent être communiquées aux pays tiers ou organisations internationales destinataires. Les transferts ultérieurs de données à caractère personnel vers des autres États tiers ou organisations internationales doivent être soumis à l'autorisation préalable de l'autorité compétente belge qui a procédé au transfert initial.

Lorsqu'elle statue sur une demande d'autorisation d'un transfert ultérieur, l'autorité compétente qui a procédé au transfert initial devrait prendre dûment en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, les conditions particulières applicables au transfert initial des données et la finalité pour laquelle les données ont été transférées initialement, la nature et les conditions de l'exécution de la sanction pénale, et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel ou laquelle les données à caractère personnel sont transférées ultérieurement. L'autorité compétente qui a effectué le transfert initial devrait aussi pouvoir assortir le transfert ultérieur de conditions particulières. Ces conditions particulières peuvent être décrites, par exemple, dans des codes de traitement.

Art. 67

(Article 36 de la Directive)

Les paragraphes 2 à 6 et 8 de la Directive ne doivent pas être transposés car ils ne concernent que la Commission européenne.

La Commission européenne a le pouvoir de décider, avec effet dans l'ensemble de l'Union européenne, que certains pays tiers, un territoire ou un ou plusieurs

meerdere nader bepaalde sectoren in een derde land, of een internationale organisatie een adequaat niveau van persoonsgegevensbescherming bieden, en daarmee in de gehele Unie rechtszekerheid en eenvormigheid verschaffen ten aanzien van derde landen of internationale organisaties die worden geacht een dergelijk beschermingsniveau te bieden. In die gevallen kunnen doorgiften van persoonsgegevens aan die landen zonder specifieke toestemming plaatsvinden, behalve wanneer een andere lidstaat waarvan de gegevens zijn verkregen zijn toestemming aan de doorgifte moet verlenen.

Art. 68

(Artikel 37 van de Richtlijn)

Doorgiften die niet plaatsvinden op grond van een adequaatheidsbesluit worden enkel toegestaan indien in een juridisch bindend instrument passende waarborgen voor de persoonsgegevensbescherming worden geboden, of indien de verwerkingsverantwoordelijke alle omstandigheden in verband met de gegevensdoorgifte heeft beoordeeld en op basis van die beoordeling van oordeel is dat passende waarborgen voor de bescherming van persoonsgegevens worden geboden. Dergelijke juridisch bindende instrumenten zouden bijvoorbeeld juridisch bindende bilaterale overeenkomsten kunnen zijn die zijn gesloten en in de rechtsorde zijn geïmplementeerd en waarop de betrokkenen van die lidstaten zich zouden kunnen beroepen, en die de naleving van gegevensbeschermingsvoorschriften en de rechten van de betrokkenen waarborgen, waaronder het recht om administratief beroep of beroep in rechte in te stellen.

De “internationale rechtsregels die België verbinden”, zoals vermeld in artikel 44/11/13 van de wet van 5 augustus 1992 op het politieambt, zijn dergelijke juridisch bindende instrumenten. Deze overeenkomsten zullen daarom moeten voorzien in passende waarborgen voor de bescherming van persoonsgegevens, indien ze een juridische basis vormen voor informatie-uitwisseling met politiediensten uit landen buiten de Europese Unie of internationale organisaties.

De verwerkingsverantwoordelijke moet rekening kunnen houden met tussen Europol of Eurojust en derde landen geslotensamenwerkingsovereenkomsten die de uitwisseling van persoonsgegevens mogelijk maken wanneer de beoordeling van alle omstandigheden omtrent de gegevensdoorgifte wordt verricht. De verwerkingsverantwoordelijke moet ook rekening kunnen houden met het feit dat de doorgifte van persoonsgegevens

secteurs déterminés dans un pays tiers, ou une organisation internationale offrent un niveau adéquat de protection des données, assurant ainsi une sécurité juridique et une uniformité dans l’ensemble de l’Union en ce qui concerne les pays tiers ou les organisations internationales qui sont réputés offrir un tel niveau de protection. Dans ces cas, les transferts de données à caractère personnel vers ces pays peuvent avoir lieu sans qu’il soit nécessaire d’obtenir une autorisation spécifique, sauf lorsqu’un autre État membre auprès duquel les données ont été collectées doit autoriser le transfert.

Art. 68

(Article 37 de la Directive)

Les transferts qui ne sont pas fondés sur une décision d’adéquation ne sont autorisés que lorsque des garanties appropriées ont été offertes dans un instrument juridiquement contraignant assurant la protection des données à caractère personnel, ou lorsque le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et estime, au vu de cette évaluation, qu’il existe des garanties appropriées en matière de protection des données à caractère personnel. Ces instruments juridiquement contraignants pourraient, par exemple, être des accords bilatéraux juridiquement contraignants conclus et mis en œuvre dans l’ordre juridique et que les personnes concernées pourraient faire exécuter, qui respectent les exigences en matière de protection des données et les droits des personnes concernées, y compris le droit à un recours administratif ou juridictionnel effectif.

Les “règles internationales de droit qui lient la Belgique”, telles qu’énoncées à l’article 44/11/13 de la loi du 5 août 1992 sur la fonction de police, sont considérés comme de tels instruments juridiquement contraignants. Ces accords devront donc prévoir des garanties appropriées pour la protection des données à caractère personnel s’ils fournissent une base légale pour l’échange d’informations avec les services de police d’un pays tiers à l’Union européenne ou d’organisations internationales.

Lorsqu’il évalue toutes les circonstances entourant le transfert de données, le responsable du traitement devrait pouvoir tenir compte des accords de coopération conclus entre Europol ou Eurojust et des pays tiers qui permettent un échange de données à caractère personnel. Le responsable du traitement devrait aussi pouvoir prendre en compte le fait que le transfert de données à caractère personnel sera soumis à des obligations

zal worden onderworpen aan verplichtingen inzake vertrouwelijkheid en aan het specialiteitbeginsel, om ervoor te zorgen dat de gegevens niet worden verwerkt voor andere doeleinden dan die waarvoor zij worden doorgegeven. Verder dient de verwerkingsverantwoordelijke in acht te nemen dat de persoonsgegevens niet zullen worden gebruikt om de doodstraf of enige vorm van vrede of onmenselijke behandeling te vorderen, uit te spreken of uit te voeren. Hoewel die voorwaarden kunnen worden bezien als passende waarborgen voor de overdracht van gegevens, moet de verwerkingsverantwoordelijke bijkomende waarborgen kunnen eisen.

Art. 69

(Artikel 38 van de Richtlijn)

Wanneer er geen adequaatheidsbesluit voorhanden is en geen passende waarborgen worden geboden, zou een doorgifte of een categorie van doorgiften slechts in specifieke situaties kunnen plaatsvinden, indien zulks noodzakelijk is:

— om de vitale belangen van de betrokkene of een andere persoon te beschermen of om legitieme belangen van de betrokkene te waarborgen indien de wet het voorziet;

— om een onmiddellijke en ernstige bedreiging van de openbare veiligheid van een lidstaat van de Europese Unie of een derde land te voorkomen;

— in een bijzonder geval, met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten, de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;

— of, in een bijzonder geval, met het oog op de vaststelling, de uitoefening of de onderbouwing van rechtsvorderingen.

Die afwijkingen moeten beperkend worden opgevat en mogen geen frequente, massale en structurele doorgifte van persoonsgegevens mogelijk maken en evenmin een grootschalige doorgifte van gegevens, maar dienen tot de strikt noodzakelijke gegevens te worden beperkt. Dergelijke doorgiften worden gedocumenteerd en op verzoek ter beschikking van de toezichthoudende autoriteit gesteld zodat deze de rechtmatigheid van de doorgifte kan controleren.

de confidentialité et au principe de spécificité, ce qui garantit que les données ne seront pas traitées à des fins autres que celles pour lesquelles elles ont été transférées. En outre, le responsable du traitement devrait prendre en compte le fait que les données à caractère personnel ne seront pas utilisées pour demander, prononcer ou mettre à exécution une condamnation à la peine de mort ou toute forme de traitement cruel et inhumain. Si ces conditions peuvent être considérées comme des garanties appropriées permettant le transfert de données, le responsable du traitement devrait pouvoir exiger des garanties supplémentaires.

Art. 69

(Article 38 de la Directive)

En l'absence de décision d'adéquation ou de garanties appropriées, un transfert ou une catégorie de transferts ne peuvent être effectués que dans des situations particulières, s'ils sont nécessaires :

— à la sauvegarde des intérêt vitaux de la personne concernée ou d'une autre personne ou à la sauvegarde des intérêts légitimes de la personne concernée lorsque la loi le prévoit;

— à la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre de l'Union européenne ou d'un pays tiers;

— dans un cas particulier, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

— ou, dans un cas particulier, à la constatation, l'exercice ou la défense de droits en justice.

Ces dérogations doivent être interprétées de manière restrictive et ne doivent pas permettre des transferts fréquents, massifs et structurels de données à caractère personnel ni des transferts de données à grande échelle, mais des transferts limités aux données strictement nécessaires. Ces transferts sont documentés et mis à la disposition de l'autorité de contrôle, sur demande, afin qu'elle puisse en vérifier la licéité.

Art. 70

(Artikel 39.1 van de Richtlijn)

Het betreft een bepaling die enkel in de om te zetten Richtlijn staat en derhalve enkel de rechtshandhavingsoverheden aangaat.

De bevoegde overheden passen de vigerende bilaterale of multilaterale internationale overeenkomsten met derde landen op het gebied van justitiële samenwerking in strafzaken of politiële samenwerking toe met het oog op de uitwisseling van relevante informatie voor het uitvoeren van de hun bij wet opgedragen taken. Deze uitwisseling vindt in beginsel plaats door samenwerking met, of ten minste met de medewerking van, de overheden die in de betrokken derde landen bevoegd zijn voor de toepassing van deze titel, in voorkomend geval zelfs zonder bilaterale of multilaterale internationale overeenkomst.

Het is echter niet steeds eenvoudig om de bevoegde overheden in derde landen te identificeren. Binnen de Europese Unie zal elk land aanduiden wie haar bevoegde overheden zijn in het kader van de implementatie van de Richtlijn. Derde landen zijn echter niet gebonden door deze Richtlijn, zullen deze daarom ook niet omzetten, en bijgevolg geen bevoegde overheden aanduiden. Het zal er daarom op neerkomen dat de betrokken Belgische diensten, alvorens zij persoonsgegevens kunnen overmaken aan een bestemmeling in een derde land, zelf zullen moeten identificeren of deze bestemmeling al dan niet een bevoegde overheid betreft zoals bedoeld in deze wet, en aldus welk regime op de overmaking van toepassing is: artikel 66 indien het een bevoegde overheid betreft of artikel 70 indien het een andere bestemmeling betreft.

Om deze inschatting te kunnen maken, zal de overmakende Belgische dienst, meer bepaald de verantwoordelijke voor de verwerking van de betrokken persoonsgegevens, informatie moeten inwinnen over de concrete taken en opdrachten van de bestemmeling in het derde land om deze te vergelijken met de doeleinden voorzien in artikel 32 van deze wet. Men beschikt daarbij over een zekere inschattingsvrijheid, al moet de geldende interpretatie van de doeleinden voorzien in artikel 32 van deze wet uiteraard worden gerespecteerd.

In specifieke individuele gevallen kunnen de normale procedures die het contacteren van die overheid in het derde land voorschrijven, echter inefficiënt of ongepast zijn, met name omdat de doorgifte niet tijdig kon worden verricht of omdat de bevoegde overheid in het derde land de rechtsstatelijkheid of de internationale mensenrechtennormen en -regels niet eerbiedigt, zodat de

Art. 70

(Article 39.1 de la Directive)

Il s'agit d'une disposition qui n'existe que dans la Directive qui doit être transposée et ne concerne dès lors que les autorités répressives.

Les autorités compétentes appliquent les accords internationaux bilatéraux ou multilatéraux conclus avec des pays tiers qui sont en vigueur dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, aux fins d'échanger les informations nécessaires pour leur permettre d'accomplir les missions que leur confie la loi. En principe, ce processus se déroule moyennant, ou tout au moins avec, la coopération des autorités compétentes dans les pays tiers concernés aux fins du présent titre, parfois même en l'absence d'un accord international bilatéral ou multilatéral.

Cependant, il n'est pas toujours facile d'identifier les autorités compétentes dans les pays tiers. Au sein de l'Union européenne, chaque pays indiquera qui sont ses autorités compétentes dans le contexte de la mise en œuvre de la Directive. Toutefois, les pays tiers ne sont pas liés par cette directive et ne les transposeront donc pas, et ne désignent donc pas les autorités compétentes. Cela signifie donc que les services belges concernés, avant de pouvoir transférer des données à caractère personnel à un destinataire dans un pays tiers, devront s'identifier, que ce destinataire soit ou non une autorité compétente au sens de la présente loi, et donc quel régime de transfert s'applique: article 66 s'il concerne une autorité compétente ou article 70 s'il concerne un autre destinataire.

Afin de pouvoir procéder à cette estimation, le service belge transférant, en particulier le responsable du traitement des données à caractère personnel concernées, devra obtenir des informations sur les tâches et missions spécifiques du destinataire dans le pays tiers afin de les comparer avec les objectifs prévus dans l'article 32 de la présente loi. Un certain degré de discrétion est possible, bien qu'il y a lieu d'interpréter correctement les objectifs prévus à l'article 32 de la présente loi.

Cependant, dans certains cas particuliers, il se peut que les procédures normales exigeant de contacter ladite autorité dans le pays tiers soient inefficaces ou inappropriées, notamment parce que le transfert ne pourrait être effectué en temps opportun ou parce que cette autorité compétente dans le pays tiers ne respecte pas l'état de droit ou n'observe pas les règles et

Belgische bevoegde overheden zouden kunnen beslissen de persoonsgegevens rechtstreeks aan in die derde landen gevestigde ontvangers door te geven. Dit kan het geval zijn wanneer doorgifte van persoonsgegevens dringend noodzakelijk is om het leven van een persoon die het slachtoffer van een strafbaar feit dreigt te worden, te redden of om het plegen van een dreigend misdrijf, waaronder terrorisme, te voorkomen.

Hoewel dat een dergelijke vorm van uitwisseling tussen bevoegde overheden en in derde landen gevestigde ontvangers voorbehouden moet blijven voor specifieke individuele gevallen, voorziet deze titel in voorwaarden om dergelijke gevallen te regelen. Die bepalingen worden niet beschouwd als afwijkingen van bestaande bilaterale of multilaterale internationale overeenkomsten op het gebied van justitiële samenwerking in strafzaken of politiële samenwerking. Die regels gelden naast de overige bepalingen van deze titel, met name de bepalingen betreffende de rechtmatigheid van de verwerking en de bepalingen van hoofdstuk V.

Gegevens kunnen uitzonderlijk worden verzonden naar ontvangers die geen bevoegde overheden zijn. Het moet daarom mogelijk zijn om alle gevallen te behandelen.

Artikel 40 van de Richtlijn moet niet worden omgezet.

HOOFDSTUK VI

Onafhankelijke toezichthoudende autoriteiten

Art. 71

(Artikelen 41 tot 49 van de Richtlijn)

Dit hoofdstuk wordt omgezet in titel 7 van deze wetsontwerp voor wat betreft sommige overheden bedoeld in deze titel.

1. Algemene beschouwingen

Het volgende artikel heeft betrekking op het Controleorgaan op de Politionele Informatie (hierna afgekort als "Controleorgaan" dan wel "C.O.C.") ingesteld bij de "*Wet van 18 maart 2014 betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van*

normes internationales dans le domaine des droits de l'homme de sorte que les autorités compétentes belges pourraient décider de transférer les données à caractère personnel directement à des destinataires établis dans ces pays tiers. C'est notamment le cas lorsqu'il est urgent de transférer des données à caractère personnel afin de sauver la vie d'une personne qui risque de devenir la victime d'une infraction pénale ou pour éviter la commission imminente d'un crime, y compris d'un acte de terrorisme.

Même si ce transfert entre autorités compétentes et destinataires établis dans des pays tiers ne devrait avoir lieu que dans certains cas précis, le présent titre prévoit les conditions qui réglementent ces cas. Ces dispositions ne sont pas considérées comme constituant des dérogations aux accords internationaux bilatéraux ou multilatéraux en vigueur dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière. Ces règles s'appliquent en complément des autres règles énoncées dans le présent titre, en particulier celles sur la licéité du traitement et celles du chapitre V.

Des données peuvent être envoyées exceptionnellement à des destinataires qui ne sont pas autorité compétente. Il faut donc pouvoir couvrir tous les cas.

L'article 40 de la Directive ne doit pas être transposé.

CHAPITRE VI

Autorités de contrôle indépendantes

Art. 71

(Articles 41 à 49 de la Directive)

Ce chapitre est transposé dans le titre 7 du présent projet de loi pour ce qui concerne certaines autorités visées au présent titre uniquement.

1. Généralités

L'article suivant porte sur l'Organe de Contrôle de l'Information policière (ci-après l'Organe de contrôle ou C.O.C.) instauré par "*la loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle"* (ci-après, Loi Organe de contrôle 2014). L'Organe de contrôle précité,

strafvordering" (hierna afgekort als "Wet Controleorgaan 2014"). Voormeld Controleorgaan, dat thans een collaterale parlementaire instelling is, was op zijn beurt de rechtsopvolger van het vroegere Controleorgaan dat vóór 7 april 2014 nog onder de voogdij van de minister van Binnenlandse Zaken en Justitie ressorteerde. De opdrachten van het Controleorgaan staan actueel omschreven in het hoofdstuk VIIter ("*Controleorgaan van het politioneel informatiebeheer*") van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna afgekort als "WVP") en inhoudende de artikelen 36*ter* tot en met 36*ter*/14. In essentie komt het erop neer dat het Controleorgaan actueel de instelling is die in het Belgische politie- en veiligheidslandschap belast is met de controle op het beheer en gebruik van persoonsgegevens en van informatie door de politiediensten en dus van de hele politionele informatiehuishouding. Het belang van het Controleorgaan en van zijn fundamentele opdrachten werd recent herhaaldelijk benadrukt door het Grondwettelijk Hof (hierna "GwH") in zijn arrest 108/2016 van 14 juli 2016 in diverse overwegingen. Er kan immers verwezen worden naar de overwegingen B.22, B.26.2, B.49, B.67.4, B.85, B.91, B.92, B.97, B.98.4.3, B.99.3.3, B.99.3.4, B.107.3, B.112.6, B.115.9, B.113.2, B.124.2, B.133 en B.155. In al deze overwegingen werd verwezen naar het bestaan en de bevoegdheden van het Controleorgaan om zo goed als alle bezwaren van beweerde ongrondwettigheid tegen de artikelen 44/1 e.v. van de Wet op het Politieambt ('WPA') van tafel te vegen. Het ging hem dan over thema's als fenomenen van bestuurlijke politie, de begrippen gegevens en persoonsgegevens, de problematiek van de mededeling van de gegevens uit de ANG, het beweerde onevenredig karakter van de te verwerken gegevens, de verwerking van gevoelige gegevens en foto's/vingerafdrukken, de rechtstreekse toegang tot en bevraging van de ANG, de internationale doorgifte van de gegevens, de bewaartermijnen van de gegevens, enz … Telkens opnieuw verwees het Hof naar de controle door het Controleorgaan teneinde de (grond) wettelijkheid van deze bepalingen te rechtvaardigen.

De belangrijke rol die het Controleorgaan in het huidige systeem van politionele informatiehuishouding speelt en zelfs meer algemeen in de hele veiligheidsarchitectuur werd tot slot zeer recentelijk in de verf gezet door de parlementaire onderzoekscommissie "*belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging*" (hierna "POC Aanslagen") en meer bepaald in zijn 3e tussentijds verslag over het onderdeel veiligheidsarchitectuur (Parl.

qui est actuellement un organe collatéral du parlement, était quant à lui le successeur en droit de l'ancien organe de contrôle qui, avant le 7 avril 2014, relevait encore de la tutelle du ministre de l'Intérieur et de la Justice. Les missions de l'Organe de contrôle sont actuellement définies dans le chapitre VIIter *("Organe de Contrôle de l'Information policière"*) de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, (ci-après "LVP") et contenant les articles 36*ter*/14 inclus. En synthèse on constate que l'Organe de contrôle est l'institution qui dans le paysage policier et de sécurité Belge est responsable pour le contrôle de la gestion des données à caractère personnel et des informations par les services de police et donc de toute la gestion de l'information policière. L'importance de l'Organe de contrôle et de ses missions fondamentales ont été récemment soulignés à maintes reprises par la Cour Constitutionnelle (ci-après "C.C.") dans son arrêt 108/2016 du 14 juillet 2016 dans diverses considérations. En effet, il convient de renvoyer aux considérants B.22, B.26.2, B.49, B.67.4, B.85, B.91, B.92, B.97, B.98.4.3, B.99.3.3, B.99.3.4, B.107.3, B.112.6, B.115.9, B.113.2, B.124.2, B.133 et B.155. Dans tous ces considérants, il est fait référence à l'existence et aux compétences de l'Organe de contrôle afin de dissiper ainsi également tous les griefs de prétendue inconstitutionnalité contre les articles 44/1 e.s. de la Loi sur la Fonction de Police ('LFP'). Il s'agissait alors de thèmes tels que des phénomènes de police administrative, des notions données et données à caractère personnel, la problématique de la communication des données (extraites) de la BNG, le caractère prétendument disproportionné des données à traiter, le traitement de données sensibles et de photos et empreintes digitales, l'accès direct et l'interrogation directe à la BNG, le transfert international des données, les délais de conservation des données , etc… A chaque fois, la Cour renvoyait au contrôle par l'Organe de contrôle afin de justifier la constitutionalité de ces dispositions.

Le rôle important que l'Organe de Contrôle joue dans l'actuel système de gestion de l'information policière et même plus général dans toute l'architecture de la sécurité, était mis en avant par la commission d'enquête parlementaire "*chargée d'examiner les circonstances qui ont conduit auxattentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste"* (ci-après "CEP Attentats") et plus particulièrement dans sons 3ième rapport intermédiaire sur le volet architecture de de la sécurité (Doc.Parl.Chambre, 2016-2017, n° 1752/008). Le sujet de l'information (policière)

St., Kamer, 2016-2017, n° 1752/008). Het thema van de (politionele) informatiehuishouding stond mede centraal in de werkzaamheden van de POC (zie voornamelijk het hoofdstuk IV, "*De informatiehuishouding*").

De POC aanslagen heeft niet alleen het C.O.C gehoord (cf. verslag p. 34), gebruik gemaakt van de resultaten van haar onderzoeken (cf. p. 189) en de hulp van het C.O.C. ingeroepen (cf. p. 206), maar heeft het ook aangemoedigd zijn inspanningen op het vlak van de controle op de politionele informatie verder te zetten. De essentiële rol van het C.O.C. werd door de POC bijvoorbeeld ook benadrukt rond de thematiek van de bijzondere gegevensbanken: *"De onderzoekscommissie dringt aan op een actief nastreven van uitsluitend bij het COC geregistreerde bijzondere gegevensbanken (bij voorkeur eenzelfde toepassing voor alle componenten van de gerechtelijke politie)"* (p. 207).

Er kan in het algemeen verwezen worden naar de pagina's 208, 212, 257 en 441 van het verslag waar telkens gewezen wordt op de belangrijke rol van het Controleorgaan en de opdrachten die het in de toekomst nog dient te uit te voeren of bezig is uit te voeren. Een aparte afdeling IV.2.6 van het verslag (p. 219 tot en met 221) werd gewijd aan het C.O.C. waarin aangemoedigd wordt haar werkzaamheden verder te zetten. Een aanbeveling tot slot van de POC luidt als volgt: "*Het COC moet voorts kunnen toezien op de globale veiligheid van de informatiehuishouding en niet enkel op onderdelen ervan*." (p. 252).

De doelstelling van dit wetsontwerp bestaat erin het Controleorgaan te voorzien van een eigen juridisch kader, wat om meerdere redenen noodzakelijk is geworden. Deze redenen kunnen als volgt worden samengevat:

— de nakende inwerkingtreding van de Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;

— de noodzaak tot omzetting van de Richtlijn 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. Elke lidstaat dient overeenkomstig artikel 44 van de Richtlijn bij wet een "toezichthoudende

était un des thèmes centraux dans les travaux de la CEP (voir principalement le chapitre IV, "*La gestion des informations*").

Le CEP Attentats n'a pas seulement entendu le C.O.C. (rapport p. 34), utilisé les résultats de ses enquêtes et fait appel à l'aide du C.O.C. (p. 206), mais l'a aussi encouragé à poursuivre ses efforts sur le plan du contrôle de l'information policière. Le rôle essentiel du C.O.C. a par exemple été mis en exergue concernant le thème des banques de données particulières: *"La commission d'enquête insiste afin que l'on tende activement vers des banques de données particulières exclusivement enregistrées au COC (de préférence, une application identique pour toutes les composantes de la police judiciaire)" (p. 207).*

On peut renvoyer aux pages 208, 212, 257 et 441 du rapport où la CEP illustre le rôle important que joue l'Organe de Contrôle et les tâches qu'il doit exécuter dans le futur ou est en train d'exécuter. Une section spécifique IV.2.6 du rapport (p. 219 – 221) a été prévue sur le C.O.C. dans laquelle il est encouragé de suivre ses travaux. La CEP fait enfin la recommandation suivante: "*Le COC doit par ailleurs pouvoir contrôler la sécurité globale de la gestion de l'information et non plus seulement certains aspects de celle-ci*." (p. 252).

L'objectif de ce projet de loi est d'encadrer l'Organe de contrôle avec un cadre juridique propre, ce qui est devenu nécessaire pour plusieurs raisons. Ces raisons peuvent être résumées comme suit:

— l'entrée en vigueur imminente 2018 du Règlement 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et relatif à la libre circulation de ces données et abrogeant la Directive 95/46/CE;

— la nécessité de transposition de la Directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et relative à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JBZ du Conseil. Chaque état membre doit conformément à l'article 44 de la directive créer une

autoriteit" of een Gegevensbeschermingsautoriteit (hierna "DPA") op te richten;

— het herbekijken, herijken en stroomlijnen van de structuur en samenstelling van het Controleorgaan, het statuut van zijn leden en diens opdrachten en bevoegdheden in functie van enerzijds de toekomstige inwerkingtreding van de hogervermelde EU-instrumenten en anderzijds in functie van de ervaringen die het Controleorgaan in zijn nieuwe samenstelling heeft opgedaan sinds het medio 2014 (in de praktijk vanaf 1 oktober 2015) een collaterale parlementaire instelling is geworden en een nieuw wetgevend kader kreeg met de Wet Controleorgaan 2014.

Het lot van Controleorgaan is noodzakelijkerwijze verbonden aan de nakende hervorming van de Commissie voor de bescherming van de persoonlijke levenssfeer ('hierna CBPL') die inderdaad dient hervormd te worden door de voormelde inwerkingtreding, medio 2018, van de Verordening 2016/679. In dat verband moet worden gewezen op de wet van 3/12/2017 tot oprichting van een gegevensbeschermingsautoriteit.

"Noodzakelijkerwijze" vermits de lege lata het Controleorgaan verankerd zit in de WVP die met dit ontwerp wordt opgeheven. Zo bepaalt het huidig artikel 36*ter* § 1 en 2 WVP dat er bij de Privacycommissie een Controleorgaan op de politionele informatie wordt opgericht, dat voor de uitoefening van zijn opdrachten onafhankelijk is van de Privacycommissie. Het deelt enkel het secretariaat van de Privacycommissie. Het spreekt evenwel voor zich dat, in de mate dat de Privacycommissie zoals voorzien in de WVP wordt opgeheven en vervangen door een totaal nieuwe instelling, met name de nieuwe Gegevensbeschermingsautoriteit, ook het Controleorgaan, zo niet (impliciet) wordt opgeheven, minstens in een juridisch vacuüm terechtkomt. Temeer het Controleorgaan actueel onder meer is samengesteld uit een lid van de Privacycommissie dat, een keer de Privacycommissie opgeheven, niet noodzakelijk nog lid zal zijn van de GBA, opvolger van de Privacycommissie.

Om al deze redenen opteert dit wetsontwerp ervoor een eigen juridisch kader vast te leggen tot instelling, organisatie, taakstelling en werking van het Controleorgaan op de politionele informatie.

2. Doel en krachtlijnen van de hervorming

Zoals in de inleiding uiteengezet streeft het voorstel diverse doelstellingen na. Deze worden hiernavolgend meer in detail besproken.

autorité de contrôle ou une autorité de protection des données ci-après "DPA");

— revoir, redéfinir et rationaliser la structure et la composition de l'Organe de contrôle, le statut de ses membres et leurs missions et compétences en fonction d'une part de l'entrée en vigueur prochaine des instruments-UE précités et d'autre part en fonction des expériences que l'Organe de contrôle a acquises dans sa nouvelle composition depuis qu' il est devenu un organe collatéral du parlement mi-2014 (en pratique depuis le 1 octobre 2015) et a reçu un nouveau cadre légal avec la Loi Organe de contrôle 2014.

Le sort de l'Organe de contrôle est nécessairement lié à la réforme imminente de la Commission de la Protection de la vie privée (ci-après "CPVP") qui doit en effet être réformée par l'entrée en vigueur précitée du Règlement 2016/679 mi-2018. A cet égard, on se référera au loi du 3/12/2017 portant la création d'une autorité de protection des données.

"Nécessairement" puisque, de lege lata, l'Organe de contrôle est inscrit dans la LVP dont les dispositions seront abrogées par ce projet de loi. Ainsi, l'actuel article 36*ter* § 1er et 2 LVP prévoit qu'il est créé auprès de la Commission de la protection de la vie privée un Organe de contrôle de l'information policière qui est indépendant de la Commission vie privée dans l'exercice de ses missions. Il partage uniquement le secrétariat avec la Commission vie privée. Cependant, il est évident que, dans la mesure où la Commission vie privée comme prévu dans la LVP est abrogée et remplacée par une toute nouvelle institution, à savoir la nouvelle autorité de protection des données, l'Organe de contrôle est (implicitement) abrogé ou se retrouve au moins dans un vide juridique. D'autant plus que l'Organe de contrôle actuel est composé entre autres d'un membre de la Commission vie privée qui, une fois la Commission vie privée abrogée, ne sera pas encore nécessairement membre de l'APD, successeure de la Commission vie privée.

Pour tous ces motifs, ce projet de loi opte pour fixer un cadre juridique propre à l'organe, aux tâches, organisation et au fonctionnement de l'Organe de contrôle de l'information policière.

2. Objectif et lignes de force de la réforme

A l'instar de ce qui est expliqué dans l'introduction, la proposition poursuit divers objectifs. Ceux-ci sont exposés plus en détail ci-après.

2.1. Aanduiding van het Controleorgaan als politionele Gegevensbeschermingsautoriteit of toezichthoudende autoriteit

Zoals in de inleiding aangegeven treden de volgende instrumenten in werking in mei 2018. De Verordening treedt in werking op 25 mei 2018 en heeft uiteraard geen omzetting nodig behoudens een reeks bepalingen die de concrete toepassing op het terrein in de Belgische rechtsorde moeten mogelijk maken. De Verordening is in beginsel rechtstreeks toepasselijk in de Belgische rechtsorde en is ook voor de geïntegreerde politie van belang nu zij ook op deze entiteiten van toepassing zal zijn voor wat betreft hun niet operationele opdrachten en de daarmee verband houdende gegevensverwerkingen (bijv. in de materie van het human resources management, de rekrutering, de opleiding, enz …).

Ingevolge de opmerking van de Privacycommissie (punten 456 en 464), werd ervoor geopteerd de bevoegdheid van het Controleorgaan op de politionele informatie te beperken tot een controletaak in het kader van de Richtlijn. In de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit werd er nog beslist om het Controleorgaan aan te duiden als DPA in uitvoering van de Verordening voor wat de verwerkingen van de politiediensten van de geïntegreerde politie betreft voor de finaliteiten van titel 1. Er wordt echter beslist aan de hand van dit wetsontwerp deze bevoegdheid te schrappen en het artikel 4 § 2, 3e lid van de wet van 3 december 2017 op te heffen.

Voor wat betreft de operationele taken en bevoegdheden van bestuurlijke en gerechtelijke politie van de politiediensten is daarentegen de Richtlijn 2016/680 van toepassing en van essentieel belang. De omzettingstermijn voor deze Richtlijn liep af op 6 mei 2018. Het huidig wetsontwerp wil hieraan, voor wat de diensten van de geïntegreerde politie betreft, t.t.z. de federale politie en de korpsen van de lokale politie, voor wat de dienst enquêtes van het Vast Comité P betreft, voor wat de algemene inspectie van de federale en de lokale politie (afgekort als AIG) betreft en voor wat de Passagiersinformatie-eenheid (en afgekort als PIE) zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens betreft en meer specifiek voor wat de aanwijzing van de Belgische toezichthoudende autoriteiten (of "*Data Protection Authority*" (DPA)) betreft, uitvoering geven. Dit ontwerp duidt het Controleorgaan dan ook aan als DPA voor wat de politionele sector van de reguliere politie betreft voor zijn operationele gegevensverwerkingen, naast de drie andere vermelde specifieke diensten wiens activiteiten nauw aansluiten bij die sector.

2.1. Désignation de l'Organe de contrôle comme autorité de protection des données policières ou Autorité de contrôle

Comme indiqué dans l'introduction, les instruments suivants entrent en vigueur en mai 2018. Le Règlement sera applicable le 25 mai 2018 et n'a évidemment pas besoin de transposition sauf une série de dispositions qui doivent permettre l'application concrète sur le terrain dans l'ordre juridique belge. Le Règlement est en principe directement applicable dans l'ordre juridique belge et est également capital pour la police intégrée maintenant que ces entités y sont également soumises pour qui ce concerne leurs tâches non opérationnelles et les traitements de données y afférentes (par exemple en matière de ressources humaines, management, recrutement, formation, etc.

Suite à la remarque de la Commission vie privée (points 456 et 464), il a été décidé de limiter la compétence de l'Organe de contrôle de l'information policière à une tâche de contrôle dans le cadre de la Directive. Dans la loi du 3 décembre 2017 portant la création d'une autorité de protection des données il avait encore été décidé de désigner l'Organe de contrôle comme DPA en exécution du règlement 2016/679 pour ce qui concerne les traitements par les services de police de la police intégrée pour les finalités du titre 1er. Cependant, par le biais de ce projet de loi il est décidé de supprimer cette compétence et d'abroger l'article 4 § 2, alinéa 3 de la loi du 3 décembre 2017.

Par contre, pour ce qui concerne les tâches opérationnelles et les compétences de la police administrative et judiciaire des services de police, la Directive 2016/680 s'applique et est primordiale. Le délai de transposition pour cette Directive a expiré le 6 mai 2018. Le projet de loi actuel veut la mettre en œuvre pour ce qui concerne les services de police intégrée, c'est-à-dire la police fédérale et les corps de la police locale, pour ce qui concerne le service d'enquête du Comité permanent P, pour ce qui concerne l'Inspection de la police fédérale et de la police locale (en abrégé l'AIG) et pour ce qui concerne l'Unité d'information des passagers (en abrégé UIP), telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers et plus particulièrement pour ce qui concerne la désignation des autorités de contrôle belges (ou "*Data Protection Authority*" DPA). Ce projet désigne ainsi l'Organe de contrôle comme DPA pour ce qui concerne le secteur policier de la police régulière pour les traitements des données opérationnels, à côté des trois autres services mentionnés dont les activités sont étroitement liées à ce secteur.

Door de oprichting van het C.O.C. als onafhankelijk parlementair orgaan met de *Wet Controleorgaan 2014* werd *de facto* reeds in grote mate aan de verplichting tot oprichting van een GBA voor de politiesector voldaan en dit nog vóór er sprake was van de Richtlijn 2016/680. Er was en is immers reeds voldaan aan de voorwaarden van onafhankelijkheid van het C.O.C., zoals voorzien in artikel 42 van de Richtlijn, evenals aan de voorwaarden betreffende de leden van de DPA, zoals voorzien in artikel 43 van diezelfde richtlijn.

Deze onafhankelijkheid van het Controleorgaan werd trouwens bevestigd in het recente arrest 180/2016 van het Grondwettelijk Hof: *"(…)Krachtens artikel 36ter/2 van de Privacywet oefenen die leden hun ambt voltijds uit, wat met zich meebrengt dat zij niet tegelijkertijd lid van het Controleorgaan en lid van de politie kunnen zijn. Artikel 36ter/1, § 8, van die wet bepaalt overigens uitdrukkelijk dat de leden van het Controleorgaan geen openbare of particuliere betrekking of activiteit mogen uitoefenen die de onafhankelijkheid of de waardigheid van hun ambt in gevaar zou kunnen brengen. De wetgever heeft bovendien voor de betrokken leden van het Controleorgaan voorzien in bepalingen betreffende hun statuut tijdens en na het uitoefenen van hun mandaat, die hun onafhankelijkheid tijdens de uitoefening van het mandaat mede waarborgen. Zo is voorzien in een detachering tijdens het uitoefenen van het mandaat, een reaffectatie na het beëindigen van het mandaat en een voorrangsregeling voor betrekkingen bij de politiediensten bij het naderen van het einde van het mandaat (artikelen 36ter/4, 36ter/5 en 36ter/6 van de Privacywet) (…)"* (Overweging B.120.3).

2.2. Aanduiding van het Controleorgaan als toezichthouder of controle-instantie inzake politionele informatiehuishouding en de bestendiging van die rol.

Gelet op hogervermelde redenen waarbij de rechtsbasis van het Controleorgaan, met name de (desbetreffende bepalingen van de) WVP, verdwijnt dient er een nieuwe wettelijk kader te worden gecreëerd voor het Controleorgaan. In essentie betreft het hier de voortzetting van de huidige opdrachten, taken en bevoegdheden van het C.O.C. Er wordt echter van de gelegenheid gebruikt gemaakt een reeks van verbeteringen aan te brengen die de voorbije periode overigens ook gedeeltelijk reeds zijn voorgesteld in het parlement of in de adviezen van de Privacycommissie en die het C.O.C. meer efficiëntie en slagkracht moeten geven.

Verbeteringen die ook noodzakelijk zijn gebleken in de praktijk sinds het C.O.C. vanaf oktober 2015 daadwerkelijk van start is gegaan en die nu, gezien de nieuwe

Par la création du C.O.C. en tant qu'organe indépendant du parlement avec *la loi Organe de contrôle 2014*, il est *de facto* déjà amplement satisfait à l'obligation de création d'un APD pour le secteur police et ceci avant qu'il ne soit question de la directive 2016/680. Les conditions d'indépendance du C.O.C., telles que prévues à l'article 42 de la Directive étaient et sont en effet déjà remplies, ainsi que les conditions concernant les membres de la DPA, telles que prévues à l'article 43 de la même Directive.

Cette indépendance de l'Organe de contrôle est d'ailleurs confirmée dans le récent arrêt 180/2016 de la Cour Constitutionnelle *"(…) En vertu de l'article 36ter/2 de la loi sur la protection de la vie privée, ces membres exercent leur fonction à temps plein, ce qui signifie qu'ils ne peuvent pas être simultanément membre de l'Organe de contrôle et membre de la police. Article 36ter/1, § 8, de cette loi dispose du reste expressément que les membres de l'Organe de contrôle ne peuvent exercer aucun (d') emploi ou activité public ou privé qui pourrait mettre en péril l'indépendance ou la dignité de leur (la) fonction. De plus, le législateur a pour les membres concernés de l'Organe de contrôle des dispositions concernant leur statut pendant et après l'exercice de leur mandat, qui contribuent à garantir leur indépendance pendant l'exercice de leur mandat. Ainsi, un détachement est prévu pendant l'exercice de leur mandat, une réaffectation au terme du mandat et un régime de priorité pour les emplois dans les services de police à l'approche de la fin de leur mandat (articles 36ter/4, 36ter/6 et 36ter/6 de la loi sur la protection de la vie privée (…)"* (considérant B.120.3).

2.2. Désignation de l'Organe de contrôle comme autorité de contrôle ou instance de contrôle en matière de gestion de l'information policière et la pérennisation de ce rôle

Pour les raisons susmentionnées où la base légale de l'Organe de contrôle, à savoir (les dispositions applicables/concernées de) la LVP, disparaît, un nouveau cadre légal doit être créé pour l'Organe de contrôle. Il s'agit essentiellement ici de la poursuite des missions actuelles, tâches et compétences du C.O.C. Cependant, il convient de profiter de l'occasion d'apporter une série d'améliorations qui, au cours de la période écoulée, ont d'ailleurs été aussi en partie déjà proposées au Parlement ou dans les avis de la Commission vie privée et qui doivent donner au C.O.C. plus d'efficacité et de moyens d'action.

Des améliorations qui se sont aussi avérées nécessaires en pratique depuis que le C.O.C. est opérationnel depuis octobre 2015 et qui maintenant, vu les nouvelles

bevoegdheden als DPA, des te meer nodig zullen blijken te zijn. Het gaat meer in het bijzonder om:

— het herbekijken van de organisatie en samenstelling van het Controleorgaan met onder meer een afslanking en gewijzigde samenstelling, de creatie van een dienst onderzoeken en een iets uitgebreidere ondersteuning;

— een beter, eenvormiger en duidelijker statuut voor de leden van het Controleorgaan waarbij de analogie wordt doorgetrokken met andere vergelijkbare collaterale parlementaire instellingen zoals het Comité P, het Comité I en de toekomstige Gegevensbeschermingsautoriteit (cf. wetsvoorstel DOC 54 n° 2913-001);

— het beter omschrijven van een aantal bevoegdheden waarover het Controleorgaan minimaal dient te beschikken om zijn taken en opdrachten efficiënt te kunnen uitoefenen.

2.3. Aanduiding van het Controleorgaan als toezichthouder in andere domeinen

Daarnaast en tot slot voorziet het ontwerp ook de mogelijkheid dat het Controleorgaan in de toekomst ook nog met andere toezichtstaken zou kunnen worden belast. In dat opzicht kan gedacht worden aan een specifieke controle op bepaalde mogelijke (niet zichtbare) cameratoepassingen door de eenheden van de geïntegreerde politie (zie DOC 54 n° 2855-001).

In het kader van een voorgenomen wijziging van de WPA besliste de regering immers het Controleorgaan aan te duiden als toezichthouder op het gebruik van camera's voor bestuurlijk politionele doeleinden. De keuze voor het Controleorgaan is logisch vermits het Controleorgaan reeds belast is met de controle op de verwerking van politionele persoonsgegevens en informatie. Een dergelijke bijkomende toezichtfunctie ligt ook in het verlengde van de in dit ontwerp voorziene rol voor het Controleorgaan als DPA op de politie-entiteiten en de drie voornoemde bijzondere diensten (Dienst Enquêtes P, de AIG en de PIE).

De Richtlijn laat de lidstaten trouwens de vrijheid om naast de rol van DPA ook nog andere of parallelle rollen aan die toezichthoudende autoriteit te geven voor zover die daarmee uiteraard verenigbaar zijn. Meer algemeen is het samengaan van de rol van DPA met de rol van politoneel toezichthouder met een focus op efficiënte en effectiviteit van het politieoptreden in het algemeen en politionele informatiehuishouding in het bijzonder ten zeerste aangewezen. Het Controleorgaan belasten met

compétences en tant que DPA, seront d'autant plus nécessaires. Il s'agit plus particulièrement de:

— revoir l'organisation et la composition de l'Organe de contrôle avec entre autres une réduction des effectifs et une composition modifiée, la création d'un service d'enquête et un soutien plus important;

— un meilleur statut, plus homogène et plus clair pour les membres de l'Organe de contrôle par analogie avec d'autres organes collatéraux du parlement comparables tels que le Comité P, le Comité R et le future Autorité de protection des données;

— mieux définir un nombre de compétences dont l'Organe de contrôle doit au minimum disposer pour exercer efficacement ses tâches et missions.

2.3. Désignation de l'Organe de contrôle comme autorité de contrôle dans d'autres domaines

De plus et enfin, le projet prévoit aussi la possibilité pour l'Organe de contrôle de pouvoir à l'avenir être investi encore d'autres missions de contrôle. A cet égard, on peut penser à un contrôle spécifique de certaines applications caméra (non visibles) possibles par les unités de la police intégrée (cf. DOC 54 n° 2855-001).

Dans le cadre d'un projet de modification de la LFP, le gouvernement à décidé en effet de désigner l'Organe de contrôle comme autorité de contrôle de l'utilisation de caméras à des fins policières administratives. Le choix de l'Organe de contrôle est logique puisque l'Organe de contrôle est déjà chargé du contrôle du traitement des données à caractère personnel et des informations policières. Une telle fonction de contrôle supplémentaire s'inscrit aussi dans la continuité du rôle prévu dans ce projet pour l'Organe de contrôle en tant que DPA sur les entités de la police et les trois services spéciaux mentionnés (Service d'enquête P, l'AIG et l'UIP) l'AIG.

La Directive laisse toutefois aux états membres la liberté de donner en plus du rôle de DPA encore d'autres rôles ou d'autres rôles parallèles à ce de l'autorité de contrôle pour autant qu'ils soient évidemment compatibles avec celui-ci. Plus généralement, la combinaison du rôle de DPA avec le rôle d'autorité de contrôle policière axé sur l'efficacité et l'efficience de l'intervention policière en général et de la gestion de l'information policière est donc tout indiquée. Confier à l'Organe de

deze laatste (meer operationele) opdrachten, naast die van DPA, is dus de logica zelve om meerdere redenen:

— de expertise inzake politionele gegevensverwerkingen bevindt zich nu reeds bij het Controleorgaan en wordt daar verder uitgebouwd;

— aspecten en vraagstukken van privacy/gegevensbescherming enerzijds en efficiëntie/effectiviteit anderzijds zitten voortdurend verweven in politionele gegevensverwerkingen en zijn in de praktijk niet uit elkaar te halen;

— dergelijke (a priori of a posteriori) bijkomende controlebevoegdheden liggen volledig in lijn en maken zelfs onderdeel uit van de actuele controlebevoegdheid van het C.O.C. en, sterker nog, laten haar toe haar rol van DPA met meer kennis van zaken en dus beter, uit te oefenen (vb. bij de klachtenbehandeling) en is dus én in het belang van de burger/betrokkene én in het belang van de politie;

— de keuze van het Controleorgaan getuigt van een rationeel gebruik van middelen en is voor de politie ook veel eenduidiger en eenvoudiger vermits zij met slechts één controle-instantie te maken krijgt onafgezien van het thema (ofwel een operationele gegevensverwerking ofwel een niet operationele gegevensverwerking);

— het toebedelen van ook andere meer operationele opdrachten die focussen op efficiëntie en effectiviteit vermijdt een DPAGBA die zich uitsluitend zou toespitsen op de privacyaspecten van de politionele informatiehuishouding. Het is belangrijk dat een toezichthoudende autoriteit ook de kennis, ervaring en problemen van de politionele realiteit kent en de daarmee gepaard gaande verplichtingen en beperkingen. Een DPA die zich alleen maar focust op privacy en gegevensbescherming zonder met die andere politionele realiteit en handhavingsnoden rekening te houden moet worden vermeden.

Het artikel 71 creëert het Controleorgaan en somt de opdrachten en taken uit waarmee het wordt belast. Het betreffen:

1° het toezicht op de toepassing van de Richtlijn door de federale politie en de korpsen van de lokale politie. Dit is de verplichting voorzien in artikel 46.1. a) van de Richtlijn die bepaalt dat de lidstaten er moeten voor zorgen dat elke toezichthoudende autoriteit op zijn grondgebied toeziet op de toepassing van de krachtens de richtlijn vastgestelde bepalingen en de omzettingsmaatregelen daarvan, en deze ook moet handhaven. Dit

contrôle ces dernières missions (plus opérationnelles), en plus de celles d'une DPA, est donc parfaitement/tout à fait logique pour plusieurs raisons:

— l'expertise relative en matière de traitements des données policières est déjà à présent de la compétence de l'Organe de contrôle et continue à s'y développer;

— les aspects et questions de respect de la vie privée et de protection des données d'une part et efficacité/efficience d'autre part sont continuellement imbriqués dans les traitements d'informations policières et en pratique ne peuvent pas être dissociés;

— de telles compétences de contrôle supplémentaires (a priori ou a posteriori) s'inscrivent pleinement et font même partie intégrante de la compétence de contrôle actuelle du C.O.C. et, à dire vrai, lui permettent d'exercer son rôle de DPA en meilleure connaissance de cause et donc mieux (par exemple le traitement des plaintes) et est donc dans l'intérêt du citoyen/de la personne concernée et dans l'intérêt de la police;

— le choix de l'Organe de contrôle témoigne d'une utilisation rationnelle des moyens et est pour la police aussi beaucoup plus clair et plus simple puisqu'elle n'est confrontée qu'à une seule instance de contrôle indépendamment du thème (ou bien un traitement de données opérationnel ou bien un traitement de données non opérationnel);

— attribuer encore d'autres tâches plus opérationnelles qui se mettent l'accent sur l'efficacité et l'efficience évite une DPA qui se focaliserait exclusivement sur les aspects liés à la protection de la vie privée de la gestion de l'information policière. Il est important qu'une autorité de contrôle ait aussi la connaissance, l'expérience et connaisse les problèmes de la réalité policière ainsi que les obligations et limitations y afférentes. Une dPA qui se concentre uniquement sur la vie privée et la protection des données sans tenir compte de cette autre réalité policière et les contraintes répressives, doit être évité.

L'article 71 crée l'Organe de contrôle et énumère les missions et tâches dont il est chargé. Elles concernent:

1° le contrôle de l'application de la Directive par la police fédérale et les corps de la police locale. Ceci est l'obligation prévue à l'article 46.1. a) de la Directive qui précise que les états membres doivent veiller à ce que, sur son territoire, chaque autorité de contrôle, contrôle l'application des dispositions adoptées en application de la présente directive et de ses mesures d'exécution et veille au respect de celles-ci. De plus ce contrôle

toezicht strekt zich bovendien ook uit tot de algemene Inspectie van de federale en de lokale politie en de Passagiersinformatie-eenheid.

De bevoegdheid van het C.O.C. strekt zich niet uit tot alle mogelijke andere handhavingsorganen ("*Law Enforcement Authorities*" of LEA) of inspectiediensten die belast zijn met de toepassing van bepaalde sectorale wetgeving (zoals bijvoorbeeld de sociale inspectie, de economische inspectie, inspectiediensten die afhangen van de deelstaten, enz …). Dat zou inderdaad volstrekt onhaalbaar zijn voor een beperkte controledienst als het C.O.C. Ook thans is de bevoegdheid van het C.O.C. beperkt tot de reguliere politie en daarin wenst dit ontwerp geen wijzigingen aan te brengen, behoudens de drie voormelde specifieke diensten. Wel nieuw is uiteraard het materieel toepassingsgebied van haar opdrachten waarbij het C.O.C. de opdracht van volwaardige DPA wordt verleend ten opzichte van de politiediensten, de AIG en de PIE in hun operationele gegevensverwerkingen. Er wordt herhaald dat de Richtlijn er niet aan in de weg staat dat de DPA nog bijkomende andere rollen zou opnemen, uiteraard voor zover niet onverenigbaar met de rol als DPA. Dat is in casu evenwel niet het geval vermits deze opdracht als DPA integendeel volledig in het verlengde ligt van de algemene toezichtsopdracht van het C.O.C. die het actueel reeds voor zijn rekening neemt. Het moet trouwens gezegd dat het Controleorgaan ook thans reeds in zijn werking een aantal taken van DPA op zich neemt zoals bijvoorbeeld het adviseren rond privacyaspecten, het waarschuwen wanneer bepaalde gegevensverwerkingen niet conform de WVP en/of de WPA zijn, enz …;

2° de controle van de verwerking van de informatie en de persoonsgegevens bedoeld in artikel 44/1 tot en met 44/11/13 WPA. Dit is niet meer dan de voortzetting van de actuele opdrachten van het Controleorgaan (cf. art. 36*ter* § 1 WVP).

3° elke andere opdracht haar door of krachtens andere wetten verleend. Deze opdrachten moeten natuurlijk compatibel zijn met de rol van een DPA. Hoger wezen we bijvoorbeeld naar de toekomstige bijzondere toezichtsopdracht op het niet zichtbaar bestuurlijk politioneel cameragebruik. Zo zullen bepaalde toepassingen van niet zichtbaar cameragebruik aan een voorafgaande notificatieverplichting aan het C.O.C. kunnen worden onderworpen en het Controleorgaan de bevoegdheid worden gegeven, indien het oordeelt dat niet is voldaan aan de voorwaarden voor het gebruik, de beslissing tot gebruik, de verlenging of de uitvoering van de maatregel, het cameragebruik te schorsen of stop te zetten en te verbieden dat de verkregen gegevens verder worden geëxploiteerd.

devrait aussi s'appliquer à l'Inspection générale de la police fédérale et locale et à l'Unité d'information des passagers.

La compétence du C.O.C. ne s'applique pas à tous les autres organes répressifs (*"Law enforcement Authoritiess"* ou LEA) ou services d'inspection qui sont chargés de l'application de certaines législations sectorielles (comme par exemple l'inspection sociale, l'inspection économique, les services d'inspection qui dépendent des entités fédérées, etc). En effet, cela serait totalement irréalisable pour un service de contrôle limité comme le C.O.C. A l'heure actuelle, la compétence du C.O.C. est également limitée à la police régulière et le projet ne souhaite pas y apporter des modifications, sauf les trois services spécifiques mentionnés. Ce qui est nouveau, c'est évidemment le champ d'application matériel de ses missions où le C.O.C. reçoit la mission de DPA à part entière par rapport aux services de police, l'AIG et le UIP dans ses traitements de données opérationnelles. Il est répété que la Directive n'interdit pas que la DPA assumerait encore d'autres rôles supplémentaires, évidemment pour autant qu'ils ne soient pas incompatibles avec le rôle de DPA. Cependant, ce n'est in casu pas le cas puisque cette mission en tant que DPA s'inscrit au contraire pleinement dans le prolongement de la mission de contrôle générale que le C.O.C. compte déjà actuellement à son actif. Cependant, il convient de rappeler que l'Organe de contrôle assume déjà actuellement un nombre de tâches de DPA dans son fonctionnement comme par exemple donner des avis sur des aspects de la protection de la vie privée, avertir quand certains traitements de données ne sont pas conformes à la LVP et/ou LFP, etc.;

2° le contrôle du traitement de l'information et des données à caractère personnel visé à l'article 44/1 à 44/11/13 LFP inclus. Ce n'est pas plus que la continuité des missions actuelles de l'Organe de contrôle (cf. art. 36*ter* § 1er LVP).

3° toute autre mission qui lui est accordée par ou en vertu d'autres lois. Ces missions doivent naturellement être compatibles avec le rôle d'une DPA. Précédemment nous avons par exemple indiqué la future mission particulière de contrôle sur l'utilisation de caméras policières administratives non visibles. Certaines applications d'utilisation de caméras non visibles avec une obligation de notification préalable seront ainsi être soumises au C.O.C. et l'Organe de contrôle va recevoir la compétence, s'il juge qu'il n'est pas satisfait aux conditions pour l'utilisation, la décision d'utilisation, la prolongation ou l'exécution de la mesure, de suspendre ou de supprimer l'utilisation de caméras et interdire que les données obtenues continuent à être exploitées (utilisées).

Het belang van het Controleorgaan in het toezicht op de grondrechten en zijn opdrachten zou daarmee extra in de verf worden gezet, wat zoals gezegd eerder al door het Grondwettelijk Hof werd gedaan in zijn arrest 108/2016. Vermits dit soort van opdrachten in essentie evenzeer gaat over persoonsgegevensverwerkingen en de rechtmatigheid ervan, en zelfs zeer gevoelige gegevens, is het Controleorgaan als toezicht houdende autoriteit ook het best geplaatst om dit soort van bijkomende opdrachten op zich te nemen. De zetel van het C.O.C. is, zoals *de facto* al het geval is, is gevestigd te Brussel.

Evident treden de leden van het Controleorgaan onafhankelijk op (zie ook artikel 42.1 van de Richtlijn die de onafhankelijkheid van de toezichthoudende autoriteit benadrukt). In het artikel 36*ter* WVP werd deze onafhankelijkheid al ingeschreven ten aanzien van de Privacycommissie, maar in werkelijkheid was zij algemeen. Deze onafhankelijkheid dient nog te worden versterkt.

TITEL 3

De bescherming van natuurlijke personen met betrekking tot de verwerking door andere overheden dan die bedoeld in titels 1 en 2

ONDERTITEL 1

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

ALGEMEEN DEEL

Zoals bepaald in artikel 2 van de Verordening, is deze niet van toepassing op de verwerking van persoonsgegevens in het kader van een activiteit die niet binnen het toepassingsgebied van het Europees Recht valt. Gezien de activiteiten van de inlichtingen- en veiligheidsdiensten (de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid) niet tot de bevoegdheden van de Unie behoren (cf. art. 4 Verdrag betreffende de Europese Unie), zijn de bepalingen uit de Verordening niet op hen van toepassing. De verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten werd geregeld door de wet van 8 december 1992. Deze wet voorzag in een toepassing van algemene principes en enkele uitzonderingen die voortvloeiden uit de specifieke opdrachten van deze diensten. Gelet op de opheffing

L'importance de l'Organe de contrôle dans le contrôle des droits fondamentaux et ses missions serait ainsi mis en évidence, ce qui, comme déjà indiqué plus haut, a été fait par la Cour Constitutionnelle dans son arrêt 108/2016. Puisque ce type de missions concerne aussi pour l'essentiel des traitements de données à caractère personnel et leur légalité ainsi que le traitement de données très sensibles, l'Organe de contrôle en tant que autorité de contrôle est le mieux placé pour assumer ce type de missions supplémentaires. Le siège du C.O.C. est, comme c'est déjà le cas, établi à Bruxelles.

Evidemment, les membres de l'Organe de contrôle agissent de manière indépendante (voir aussi l'article 42.1 de la Directive qui insiste sur l'indépendance de l'autorité de contrôle). Dans l'article 36*ter* LVP, cette indépendance est déjà inscrite à l'égard de la Commission vie privée, mais en réalité elle était générale. Cette indépendance doit encore être renforcée.

TITRE 3

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par d'autres autorités que celles visées aux titres 1 et 2

SOUS-TITRE 1ER

DE LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL PAR L'ORGANE DE COORDINATION POUR L'ANALYSE DE LA MENACE

PARTIE GENERALE

Comme le précise l'article 2 du Règlement, celui-ci ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union européenne. Les activités de l'OCAM n'entrant pas dans les compétences de l'Union (cf. art. 4 TUE), les dispositions du Règlement ne leur sont pas applicables. Le traitement des données à caractère personnel de l'OCAM était réglementé par la loi du 8 décembre 1992. Cette loi prévoyait une application des principes généraux et quelques exceptions en raison des spécificités des finalités de l'OCAM. La loi du 8 décembre 1992 étant abrogée par la présente loi, un nouveau régime est prévu dans le sous-titre 4. Celui-ci détermine donc de nouvelles règles applicables à tout traitement de

van de wet van 8 december 1992 door onderhavige wet, wordt een nieuw regime ingevoerd door ondertitel 1. Deze titel bepaalt aldus de toepasselijke regels voor elke verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten en hun verwerkers in het belang van de uitoefening van de opdrachten van voornoemde diensten.

De ondertitel volgt vier richtsnoeren:

1. Overname van de bepalingen van de wet van 8 december 1992 die van toepassing zijn op de inlichtingen- en veiligheidsdiensten.

2. Naleving van de Conventie voor de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa van 28 januari 1981 (het zogeheten Verdrag 108);

3. Bekrachtiging van bepaalde verplichtingen van de verwerkingsverantwoordelijken;

4. Specifieke bepalingen voor het gebruik van persoonsgegevens van de inlichtingendiensten voor historische, wetenschappelijke of statistische doeleinden.

I. — **STATUS QUO IN VERGELIJKING MET DE WET VAN 8 DECEMBER 1992**

Toen de wet van 8 december 1992 werd aangenomen, heeft de wetgever de beslissing genomen de twee inlichtingen- en veiligheidsdiensten te onderwerpen aan de algemene principes voor de verwerking van persoonsgegevens en de uitzonderingen te beperken tot degene die absoluut noodzakelijk zijn om hun opdrachten in alle discretie te vervullen.

De wetgever verklaarde zijn keuze als volgt:

"Ten slotte wordt een speciale regeling getroffen met betrekking tot de verwerking beheerd door het Bestuur Veiligheid van de Staat van het Ministerie van Justitie en door de Algemene dienst Inlichting en Veiligheid van het Ministerie van Landsverdediging, ofschoon die niet volledig uitgesloten zijn van de werkingssfeer van de wet. De aard zelf van de taken die zij volbrengen, rechtvaardigt dat die autoriteiten deze taken met de nodige geheimhouding verder zouden kunnen uitvoeren. De belangrijkheid van de uitzonderingen welke die diensten genieten, is overigens met de nodige zorg afgewogen, en alleen die bepalingen welke volstrekt onverenigbaar zijn met hun taken, zijn eruit geweerd. Evenwel valt op te merken dat de betrokken personen toch nog over een aantal controlemiddelen ter zake données à caractère personnel par l'OCAM et ses sous-traitants dans l'intérêt de l'exercice des missions desdits services.

Le titre suit quatre lignes directrices:

1. reprise des mêmes dispositions que celles applicables à l'OCAM dans la LVP;

2. respect de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe du 28 janvier 1981 (dite Convention 108);

3. renforcement de certaines obligations des responsables du traitement;

4. dispositions particulières pour l'utilisation des données à caractère personnel de l'OCAM à des fins historiques, scientifiques ou statistiques.

I. — **STATU QUO PAR RAPPORT À LA LOI DU 8 DÉCEMBRE 1992**

Lors de l'adoption de la loi du 8 décembre 1992, le législateur a pris la décision de soumettre les deux services de renseignement aux principes généraux de traitement des données à caractère personnel et de limiter les exceptions à celles absolument nécessaires pour permettre l'accomplissement de leurs missions en toute discrétion.

Le législateur a expliqué son choix en ces termes:

"Enfin, les traitements gérés par la Sûreté de l'État du Ministère de la Justice et le Service général du Renseignement et de la Sécurité du Ministère de la Défense nationale, sans être complètement exclus du champ d'application de la loi seront soumis à un sort spécifique. La nature même des tâches qu'ils accomplissent justifie qu'ils puissent continuer à l'accomplir avec toute la discrétion nécessaire. L'importance des exceptions dont bénéficieront ces services a d'ailleurs été pesée avec soin et seules les dispositions absolument incompatibles avec leurs missions ont été écartées. Il est à noter cependant que les personnes concernées ne seront pas dépourvues de tout moyen de contrôle à leur égard, puisqu'elles pourront bénéficier d'un "droit d'accès indirect" aux données enregistrées

zullen beschikken omdat zij voor de geregistreerde gegevens een onrechtstreeks recht van toegang genieten dat wordt uitgeoefend door tussenkomst van de Commissie voor de bescherming van de persoonlijke levenssfeer." (Doc, Kamer, 1990-1991, n° 1610, pp. 7 en 8).

Deze ondertitel maakt dezelfde principes toepasselijk op de inlichtingen- en veiligheidsdiensten en voorziet dezelfde uitzonderingen om dezelfde redenen van discretie.

II. — **NALEVING VAN DE PRINCIPES VAN DE CONVENTIE 108**

De inlichtingen- en veiligheidsdiensten zijn onderworpen aan de Conventie voor de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa van 28 januari 1981 (Verdrag 108). Deze ondertitel houdt de rechten en verplichtingen in vastgelegd door de Conventie 108 en voorziet geen juridische uitzonderingen dan wanneer toegelaten door de Conventie zelf.

III. — **BEKRACHTIGING VAN BEPAALDE VERPLICHTINGEN**

In vergelijking met de verplichtingen vastgelegd door de wet van 8 december 1992, gaat deze ondertitel verder en voorziet deze in nieuwe verplichtingen. Aldus wordt gesteld dat de inlichtingen- en veiligheidsdiensten registers moeten bijhouden van hun verwerkingsactiviteiten. De diensten hebben eveneens de verplichting om melding te maken aan de bevoegde toezichthoudende autoriteit van elke inbreuk op de beveiliging van persoonsgegevens die een risico voor de rechten en vrijheden van natuurlijke personen inhoudt. De ondertitel legt aan de inlichtingen- en veiligheidsdiensten ook op een functionaris voor gegevensbescherming aan te duiden. Deze verplichting bestond niet in de wet van 8 december 1992 maar werd niettemin al opgelegd door het Koninklijk Besluit van 12 oktober 2010 ter uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende de regeling van de inlichtingen- en veiligheidsdiensten. De rol van deze functionaris voor gegevensbescherming wordt uitgebreid in deze ondertitel.

IV. — **VERWERKING VOOR HISTORISCHE, WETENSCHAPPELIJKE EN STATISTISCHE DOELEINDEN**

Het raadplegen van persoonsgegevens van de inlichtingen- en veiligheidsdiensten en diens personeel

qui s'exercera auprès de la Commission de la protection de la vie privée." (Doc, La Chambre, 1990-1991, n° 1610, pp. 7 et 8).

Le pésent sous-titre rend les mêmes principes applicables aux services de renseignement et prévoit les mêmes exceptions pour les mêmes raisons de discrétion.

II. — **RESPECT DES PRINCIPES DE LA CONVENTION 108**

Les services de renseignement et de sécurité sont soumis à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe du 28 janvier 1981 (Convention 108). Le présent sous-titre contient tous les droits et obligations fixés dans la Convention 108 et n'y prévoit d'exceptions légales expresses que lorsque la Convention elle-même les autorise.

III. — **RENFORCEMENT DE CERTAINES OBLIGATIONS**

Par rapport aux obligations fixées par la loi du 8 décembre 1992, le présent sous-titre va plus loin et prévoit de nouvelles obligations. Ainsi, il dispose que les services de renseignement et de sécurité doivent tenir des registres de leurs activités de traitement. Les services ont également l'obligation de notifier à l'autorité de contrôle compétente toute brèche de sécurité portant sur des données à caractère personnel et présentant un risque pour les droits et libertés des personnes physiques. Le sous-titre impose aussi aux services de renseignement et de sécurité de désigner un délégué à la protection des données. Cette obligation qui n'existait pas dans la loi du 8 décembre 1992 était néanmoins déjà fixée dans l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le rôle du délégué à la protection des données est renforcé dans le présent sous-titre.

IV. — **TRAITEMENT À DES FINS HISTORIQUES, SCIENTIFIQUES OU STATISTIQUES**

La consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel des

voor historische, wetenschappelijke en statistische doeleinden wordt gereglementeerd. Deze raadpleging is slechts mogelijk indien zij geen weerslag heeft op de opdrachten van de inlichtingendiensten en indien zij geen gevaar vormt voor een bron of een derde die zijn medewerking aan de inlichtingendiensten verleent, en indien zij geen weerslag heeft op een lopend opsporings- of gerechtelijk onderzoek of op de relaties die België onderhoudt met andere Staten of internationale organisaties. De verwerking van geclassificeerde documenten dient natuurlijk ook de bepalingen van de wet van 11 december 1998 te respecteren.

Deze specifieke reglementering is noodzakelijk gezien een aanvraag tot verwerking van gegevens komende van de inlichtingen- en veiligheidsdiensten voor historische, wetenschappelijke of statistische doeleinden kan plaatsvinden op elk moment, zelfs wanneer een inlichtingenonderzoek nog lopende is. Het is te vermijden dat een personne concernée van een dienst, onder het voorwendsel dat hij student is, kennis kan nemen van het feit dat hij het voorwerp uitmaakt van een opvolging, wat het gehele onderzoek in het gedrang zou brengen.

ARTIKELSGEWIJZE TOELICHTING

HOOFDSTUK I

Definities

Art. 72

De eerste paragraaf wijst naar de definities die gehanteerd worden in titel 2, met uitzondering van diegene die betrekking hebben op de gerechtelijke overheden of de politie en hun toezichthoudende autoriteit. Paragraaf 2 voert hieraan enkele definities toe die eigen zijn aan deze ondertitel en die enkel relevant zijn voor de inlichtingen- en veiligheidsdiensten.

Om te antwoorden op het advies van de Raad van State, pagina 10, worden de woorden "*teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met verwerking te beschermen*" geschrapt van de definitie van toezichthoudende autoriteit in punt 6°. Toezichthoudende autoriteit wordt op een neutrale wijze gedefinieerd omdat het kan wijzen op meerdere autoriteiten (Gegevensbeschermingsautoriteit, het COC,…). Een punt 7° wordt toegevoegd om het Vast Comité I te definiëren.

services de renseignement et de sécurité et de leur personnel est réglementée. Elle n'est possible que si elle ne porte pas atteinte aux missions des services de renseignement, ni ne met en danger une source ou un tiers qui prête son concours, et ne porte pas atteinte à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales. Le traitement des données classifiées doit bien entendu aussi respecter les dispositions de la loi du 11 décembre 1998.

Cette réglementation spécifique est nécessaire car une demande de consultation des données des services de renseignement et de sécurité à des fins historiques, scientifiques ou statistiques peut avoir lieu à tout moment, alors même qu'une enquête de renseignement est encore en cours. Il faut éviter qu'une personne concernée d'un service, sous prétexte qu'elle est étudiante, puisse prendre connaissance du fait qu'elle fait l'objet d'un suivi, ce qui mettrait en péril toute l'enquête.

COMMENTAIRE DES ARTICLES

CHAPITRE IER

Définitions

Art. 72

Le premier paragraphe renvoie aux définitions prévues dans le titre 2, à l'exception de celles qui visent les autorités judiciaires ou de police et leur autorité de contrôle. Le paragraphe 2 y ajoute quelques notions qui sont propres au présent sous-titre et qui ne sont pertinentes que pour les services de renseignement et de sécurité.

Pour répondre à l'avis du Conseil d'État en page 10, les mots "*afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement"* sont supprimés de la définition d'autorité de contrôle visée au 6°. Autorité de contrôle est définie de manière neutre car elle peut viser plusieurs autorités (l'Autorité de protection des données, le C.O.C, …). Il est ajouté un 7° pour définir le Comité permanent R.

HOOFDSTUK II

Toepassingsgebied

Art. 73

De verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten wordt momenteel geregeld door de wet van 8 december 1992. Deze wet sluit de toepassing van enkele artikelen uit voor deze diensten en onder andere enkele verplichtingen en rechten van betrokken personen. Gezien "nationale veiligheid" uitgesloten is van de toepassing van de Algemene Verordening Gegevensbescherming (AVG), is een aparte regeling nodig voor de gegevensverwerking door de inlichtingen- en veiligheidsdiensten. Dit regime is geïnspireerd op de huidige wet van 8 december 1992 en beantwoordt aan de standaarden van het Verdrag 108 van de Raad van Europa.

Het eerste lid verduidelijkt het toepassingsgebied van deze ondertitel. Dit zijn de verwerkingen die worden uitgevoerd in het kader van de wettelijke missies van de inlichtingen- en veiligheidsdiensten. Deze missies vloeien voort uit de artikelen 7 en 11 van de wet van 30 november 1998, evenals uit andere bijzondere rechtsgrondslagen.

Het tweede lid verduidelijkt dat de andere titels van deze wet niet van toepassing zijn op de verwerkingen door de inlichtingen- en veiligheidsdiensten. De ondertitel omvat het geheel van bepalingen dat van toepassing is op de inlichtingen- en veiligheidsdiensten voor hun verwerking van persoonsgegevens bij de uitoefening van hun wettelijke opdrachten (rechten, verplichtingen, archivering, controle,…), de toepassing van andere titels van deze wet met uitzondering van sommige straf- en slotbepalingen is dus niet te rechtvaardigen.

CHAPITRE II

Champ d'application

Art. 73

Le traitement de données à caractère personnel par les services de renseignement et de sécurité est actuellement réglé par la loi du 8 décembre 1992. Cette loi exclut l'application de certains articles à ces services et notamment de certains droits et obligations des personnes concernées. Vu que la "sécurité nationale" est exclue du champ d'application du Règlement général sur la protection des données (RGPD), une règlementation séparée est nécessaire pour le traitement des données par les services de renseignement et de sécurité. Ce régime est inspiré de la loi actuelle du 8 décembre 1992 et répond aux normes de la Convention 108 du Conseil de l'Europe.

L'alinéa permier précise le champ d'application du présent sous-titre. Il s'agit des traitements effectués dans le cadre des missions légales des services de renseignement et de sécurité. Ces missions découlent des articles 7 et 11 de la loi du 30 novembre 1998, ainsi que d'autres bases légales particulières.

L'alinéa 2 précise que les autres titres ne s'appliquent pas aux traitements des données à caractère personnel par les services de renseignement et de sécurité. Le sous-titre couvre l'ensemble des dispositions applicables aux services de renseignement et de sécurité dans leur traitement de données à caractère personnel dans l'exercice de leurs missions légales (droits, obligations, archivage, contrôle, …). L'application d'autres titres de la présente loi à l'exception de certaines dispositions pénales et finales ne se justifie donc pas.

HOOFDSTUK III

Algemene voorwaarden voor de verwerking

Art. 74

Dit artikel beschrijft in welke gevallen een verwerking van persoonsgegevens rechtmatig is.

Deze gevallen zijn deze zoals ze vervat waren in artikel 5 van de wet van 8 december 1992. De inlichtingen- en veiligheidsdiensten kunnen aldus persoonsgegevens verwerken indien dit nuttig is voor de uitvoering van hun opdrachten zoals voorzien in de wet van 30 november 1998, voor de uitvoering van een

CHAPITRE III

Conditions générales du traitement

Art. 74

Cet article décrit les cas dans lesquels le traitement de données à caractère personnel est légitime.

Ces cas sont ceux qui étaient repris à l'article 5 de la loi du 8 décembre 1992. Ainsi, les services de renseignement et de sécurité peuvent traiter des données à caractère personnel si cela est utile pour l'exercice de leurs missions prévues dans la loi du 30 novembre 1998, pour l'exécution d'un contrat ou pour d'autres obligations.

contract of voor andere verplichtingen. Een verwerking van persoonsgegevens is eveneens toegelaten wanneer dit noodzakkelijk is voor de uitvoering van een opdracht van openbaar belang.

Er valt op te merken dat de term “noodzakelijk” vervangen werd door de term “nuttig” in punt d). Dit wordt verklaard door de aard van de inlichtingenonderzoeken zelf, die past in het kader van de preventie en de voorziening. Vóór het inzamelen van gegevens is het moeilijk om reeds te weten of het resultaat hiervan noodzakelijk zal zijn om een taak van algemeen belang te vervullen. Het betreft een bevestiging van het standpunt dat de wetgever heeft ingenomen, met name in artikel 13 van de wet van 30 november 1998 dat stelt dat de inlichtingendiensten “informatie en persoonsgegevens [mogen] […] verwerken die nuttig kunnen zijn om hun opdrachten te vervullen”.

De behandeling van persoonsgegevens is eveneens steeds mogelijk met de instemming van de betrokken persoon, op voorwaarde dat de toestemming vrij en geïnformeerd is zoals de rechtspraak bepaalt.

Art. 75

Iedere verwerking van persoonsgegevens dient rechtmatig en eerlijk te geschieden met het oog op specifieke, vastgestelde doeleinden. De betrokkenen moeten kennis kunnen nemen van de regels, waarborgen en rechten in verband met de verwerking van hun persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot de verwerking kunnen uitoefenen.

De specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt dienen welbepaald, expliciet en legitiem te zijn. De persoonsgegevens dienen niet verder te worden verwerkt op een wijze die onverenigbaar is met deze doeleinden. Er wordt verduidelijkt dat verdere verwerking voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd wordt.

De persoonsgegevens dienen toereikend, ter zake dienend en niet overmatig te zijn voor de doeleinden waarvoor zij worden verwerkt.

De persoonsgegevens dienen nauwkeurig te zijn. De onjuiste persoonsgegevens dienen verbeterd of verwijderd te worden. Deze beginselen zijn overgenomen uit artikel 5 van het Verdrag 108 en artikel 4 van de wet van 8 december 1992.

Un traitement de données à caractère personnel est également autorisé s’il est nécessaire pour l’exécution d’une mission d’intérêt public.

Il est précisé que le terme “nécessaire” a été remplacé par le terme “utile” au point c). Cela s’explique par la nature-même des enquêtes de renseignement qui s’inscrit dans la prévention et l’anticipation. Avant la collecte des données, il est difficile de déjà savoir si le résultat de celle-ci sera nécessaire pour l’exécution d’une mission d’intérêt public. Il s’agit d’une confirmation de la position que le législateur a prise notamment à l’article 13 de la loi du 30 novembre 1998 qui dispose que les services de renseignement peuvent “*traiter des informations et des données à caractère personnel qui peuvent être utiles à l’exécution de leurs missions*”.

Le traitement de données à caractère personnel est également toujours possible avec l’accord de la personne concernée pour autant que le consentement soit libre et éclairé tel que la jurisprudence le prévoit.

Art. 75

Chaque traitement de données à caractère personnel doit être effectué licitement et loyalement, en lien avec des finalités spécifiques et déterminées. Les personnes concernées doivent pouvoir prendre connaissance des règles, garanties et droits en lien avec le traitement de leurs données à caractère personnel, ainsi que de la manière dont elles peuvent exercer leurs droits relatifs au traitement.

Les finalités spécifiques pour lesquelles les données à caractère personnel sont traitées doivent être déterminées, explicites et légitimes. Les données ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités. Il est précisé qu’un traitement ultérieur à des fins historiques, scientifiques ou statistiques n’est pas réputé incompatible.

Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

Les données à caractère personnel doivent être exactes. Les données inexactes doivent être rectifiées ou effacées. Ces principes sont repris de l’article 5 de la Convention 108 et de l’article 4 de la loi du 8 décembre 1992.

Wat betreft de bewaring van de gegevens, worden de modaliteiten in artikel 79 bepaald.

HOOFDSTUK IV

Types van persoonsgegevens

Art. 76

Dit artikel laat de inlichtingen- en veiligheidsdiensten toe om persoonsgegevens te verwerken die gevoelig zijn vanwege hun aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of geaardheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen.

Deze uitzondering was voor de inlichtingen-en veiligheidsdiensten reeds voorzien in de WVP (artikel 3, § 4). Hoewel deze verwerking in principe verboden is, voorziet het Verdrag 108 in haar artikel 9, § 2, een uitzondering op het verbod deze gegevens te verwerken in het belang van de nationale veiligheid indien dit uitdrukkelijk voorzien is in een wet, wat de bestaansreden is van dit artikel. Deze mogelijkheid om gevoelige gegevens te verwerken wordt gerechtvaardigd door het feit dat de inlichtingendiensten in staat moeten zijn om elk type gegeven, zonder onderscheid, te verwerken om te kunnen anticiperen op elke bedreiging van de nationale veiligheid.

Zo kunnen bijvoorbeeld politieke, godsdienstige of levensbeschouwelijke overtuigingen belangrijke indicatoren vormen voor het inschatten van de bedreiging die een persoon kan vormen voor de nationale veiligheid, onder andere als indicator voor radicalisering. Biometrische gegevens laten dan weer een formele identificatie toe van vreemdelingen wanneer hun identiteitsdocumenten niet betrouwbaar zijn, wat extreem nuttig is in het kader van de veiligheidsverificaties die de ADIV uitvoert in het buitenland om de veiligheid van de troepen te verzekeren. Gegevens betreffende ras en etniciteit maken het mogelijk om lidmaatschap tot welbepaalde groeperingen te bepalen en bepaalde fenomenen te onderzoeken die een bedreiging vormen voor de nationale veiligheid.

Eender welk gegeven kan nuttig zijn op elk moment. De inlichtingendiensten moeten elk type van gegeven kunnen verwerken zonder beperkingen om naar best vermogen hun opdrachten te kunnen uitvoeren, dit met

En ce qui concerne la conservation des données, les modalités sont fixées à l'article 79.

CHAPITRE IV

Types de données à caractère personnel

Art. 76

Cet article autorise les services de renseignement et de sécurité à traiter des données à caractère personnel qui sont sensibles de par leur nature, notamment celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

Cette possibilité pour les services de renseignement et de sécurité de traiter ces données était déjà adoptée par la LVp (article 3, § 4). La Convention 108 autorise d'ailleurs dans son article 9, § 2, une exception à l'interdiction de traiter ces données dans l'intérêt de la sécurité nationale si elle est expressément prévue dans une loi, raison d'être de cet article. Cette possibilité de traiter des données sensibles est justifiée par le fait que pour anticiper toute menace contre la sécurité nationale, les services de renseignement doivent pouvoir collecter tout type de données, sans distinction.

Par exemple, les opinions politiques, les convictions religieuses ou philosophiques peuvent former des indicateurs importants pour l'évaluation de la menace qu'une personne peut former pour la sécurité nationale, par exemple un indicateur de radicalisation. Les données biométriques permettent l'identification formelle des étrangers là où leurs documents d'identité ne sont pas fiables, ce qui est extrêmement utile notamment dans le cadre des vérifications de sécurité effectuées à l'étranger par le SGRS pour assurer la sécurité des troupes. Les données sur la race et l'ethnie permettent de déterminer l'appartenance à certains groupes et d'étudier certains phénomènes présentant une menace pour la sécurité nationale.

N'importe quelle donnée peut être nécessaire à tout moment. Les services de renseignement doivent pouvoir traiter tout type de données sans limitation pour pouvoir exercer au mieux leurs missions, en respectant

naleving van het principe van proportionaliteit en met onderwerping aan een diepgaande controle.

De Privacycommissie merkt op dat de inlichtingendiensten de noodzaak en evenredigheid van het verwerken van bijzondere gegevens niet rechtvaardigt. Het betreft nochtans een status quo met betrekking tot de wet van 1992. De onderliggende redenen voor deze verwerking van bijzondere gegevens zijn altijd, op evidente wijze, gerechtvaardigd wegens het anticiperen op bedreigingen voor de nationale veiligheid. Wat betreft de verwerking van genetische persoonsgegevens, deze kan onmisbaar blijken voor een onbetwistbare identificatie van slachtoffers / betokkenen die een onderlinge band hebben. We denken bijvoorbeeld aan een aanslag met behulp van explosieven waarbij de inlichtingendiensten vanop de eerste rij betrokken zijn ter verduidelijking van de scène van het gebeuren en ter identificatie van de personen die een bedreiging vormen, in het bijzonder voortvluchtigen.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 77

Voor de bewaring van de persoonsgegevens verwijst dit artikel naar artikel 21 van de wet van 30 november 1998.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 78

Dit algemeen principe, met name dat elke natuurlijke persoon recht heeft op de bescherming van zijn persoonsgegevens, is overgenomen van artikel 2 van de wet van 8 december 1992.

Art. 79

Dit artikel bevat een opsomming van de rechten van de persoon wiens gegevens verwerkt worden door de inlichtingen- en veiligheidsdiensten. De uitoefening van deze rechten wordt verder uitgewerkt in artikelen 79 en 8082. Het Verdrag 108 voorziet in diens artikelen 8 en 9 dat er uitzonderingen mogelijk zijn op het recht op informatie, rectificatie en vergetelheid van de betrokkene, indien de wet hierin voorziet en het om een maatregel gaat die in een

bien entendu l'exigence de proportionnalité et en étant soumis à un contrôle approfondi.

La Commission vie privée constate que les services de renseignement ne justifient pas la nécessité et la proportionnalité de traiter des catégories particulières de données. Il s'agit pourtant d'un statu quo par rapport à la loi de 1992. Les raisons qui sous-tendent ce traitement de données particulières sont toujours, de manière évidente, justifiées par l'anticipation de menaces pour la sécurité nationale. En ce qui concerne le traitement de données à caractère personnel génétiques, celui-ci peut se révéler indispensable pour une identification indiscutable de victimes / personnes concernées qui ont un lien entre elles. On songe par exemple à un attentat à l'aide d'explosifs, où les services de renseignement sont impliqués en première ligne par l'explication de la scène du drame et l'identification des personnes qui représentent la menace, notamment de fugitifs.

CHAPITRE V

Conservation des données à caractère personnel

Art. 77

Pour la conservation des données à caractère personnel, cet article renvoie à l'article 21 de la loi du 30 novembre 1998.

CHAPITRE VI

Droits de la personne concernée

Art. 78

Ce principe général, à savoir que toute personne physique a droit au respect de sa vie privée, est repris de l'article 2 de la loi du 8 décembre 1992.

Art. 79

Cet article contient une énumération des droits de la personne dont les données sont traitées par les services de renseignement et de sécurité. Les modalités d'exercice de ces droits sont précisées dans les articles 79 et 80. La Convention 108 prévoit en ses articles 8 et 9 combinés que des exceptions aux droits de la personne concernée à l'information, à la rectification et à l'effacement sont possibles, pour autant qu'elles soient prévues par la loi et qu'il s'agisse de

democratische samenleving noodzakelijk is ten behoeve van de bescherming van de veiligheid van de staat. Deze uitzonderingen werden al vastgelegd in artikel 3, § 4, van de wet van 8 december 1992.

Om de discretie van hun inlichtingenonderzoeken te vrijwaren, verzamelen en verwerken de inlichtingen- en veiligheidsdiensten persoonsgegevens zonder goedkeuring en buiten medeweten van de betrokkenen. Teneinde deze discretie te verzekeren is de toegang van de betrokkene een onrechtstreekse toegang uitgeoefend met tussenkomst van het Vast Comité I die diens rechten in zijn plaats uitoefent.

Om te antwoorden op punt 232 van het advies van de Privacycommissie werden de artikelen betreffende het recht op toegang gewijzigd of geschrapt.

Art. 80

Op vraag van de burger controleert het Vast Comité I de rechtmatigheid van de gegevensverwerking door de inlichtingen- en veiligheidsdiensten. Na controle deelt het aan de betrokkene mee dat de nodige verificaties werden verricht. Indien nodig gaan de inlichtingen- en veiligheidsdiensten over tot de verbetering of verwijdering van onjuiste of niet-pertinente gegevens. De procedure wordt verder uitgewerkt in de wet.

Art. 81

Deze bepaling is de weerspiegeling van artikel 11, § 2, in titel 1 van deze wet die het Vast Comité I en de autoriteiten bedoeld in titel 3 ook toelaten een logbestand bij te houden van de verzoeken tot het uitoefenen van de rechten bedoeld in de artikelen 12 tot 22 en 34 van de Verordening.

Art. 82

Net zoals het artikel 12*bis* van de wet van 8 december 1992, stelt deze bepaling dat de inlichtingen- en veiligheidsdiensten geen besluit mogen nemen met negatieve of ingrijpende rechtsgevolgen voor de betrokken persoon, voor zover dit gebeurt louter op grond van een geautomatiseerde verwerking die bedoeld is om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid. Dit verbod geldt niet indien dergelijke verwerking door of krachtens een wet wordt toegelaten of indien dit noodzakelijk is voor redenen van zwaarwegend openbaar belang, zoals de veiligheid van de Staat.

mesures nécessaires dans une société démocratique à la protection de la sécurité de l'État. Ces exceptions étaient déjà établies dans l'article 3, § 4, de la loi du 8 décembre 1992.

Pour assurer la discrétion de leurs enquêtes de renseignement, les services de renseignement et de sécurité collectent et traitent des données à caractère personnel sans le consentement et à l'insu des personnes concernées. Pour assurer cette discrétion, l'accès de la personne concernée est un accès indirect exercé par l'intermédiaire du Comité permanent R qui est subrogé dans les droits de celle-ci.

Pour répondre au point 232 de l'avis de la Commission vie privée, les articles concernant l'accès ont été adaptés ou supprimé.

Art. 80

Le Comité permanent R vérifie, à la demande de la personne concernée, la licéité du traitement des données par le service de renseignement et de sécurité. Après contrôle, il communique à celle-ci que les vérifications nécessaires ont été faites. Si nécessaire, les services de renseignement et de sécurité procèdent à la correction ou l'effacement des données inexactes ou non pertinentes. Les modalités de la procédure sont précisées dans la loi.

Art. 81

Cette disposition est le reflet de l'article 11, § 2, dans le titre 1er de la présente loi, permettant au Comité permanent R et aux autorités visées au titre 3 de tenir aussi un journal des demandes d'exercice des droits visés aux articles 12 à 22 et 34 du Règlement.

Art. 82

A l'instar de ce que faisait l'article 12*bis* de la loi du 8 décembre 1992, cette disposition prescrit que les services de renseignement et de sécurité ne peuvent prendre aucune décision produisant des effets juridiques dommageables ou lourds de conséquence pour la personne concernée, sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects de sa personnalité. Cette interdiction ne s'applique pas lorsqu'un tel traitement est autorisé par ou en vertu d'une loi ou lorsqu'il est nécessaire en raison d'un intérêt public important, tel que la sécurité de l'État.

Wat betreft de besluiten, is het de norm dat de inlichtingendiensten in principe geen besluiten nemen met directe rechtsgevolgen voor de burgers. De voornaamste rol van de inlichtingendiensten is het informeren van de overheidsinstanties, in hoofdzaak naar aanleiding van dreigingen uitgaande van individuen, voor zover deze dreigingen gelinkt zijn aan de opdrachten van de geïnformeerde instanties. Het zijn deze bevoegde overheidsinstanties die de nodige besluiten nemen (bijvoorbeeld de Dienst Vreemdelingenzaken).

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 83

Dit artikel bepaalt de verplichtingen van de verwerkingsverantwoordelijke van de inlichtingen- en veiligheidsdiensten. Hij moet waken over de juistheid van de persoonsgegevens. Hij moet ook zorgen dat voor de personen die onder hun gezag handelen, de toegang tot de gegevens beperkt blijft tot wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst. De inlichtingen- en veiligheidsdiensten zien erop toe dat personen die onder hun gezag handelen kennis hebben van de verplichtingen en voorschriften die hen door deze ondertitel worden opgelegd.

Deze verplichtingen zijn conform de verplichtingen voor de verantwoordelijke van de verwerking vervat in artikel 16, § 2, 1°, van de wet van 8 december 1992, met een kleine aanpassing om de tekst in overeenstemming te brengen met artikel 13 van de wet van 30 november 1998 dat bepaalt dat de inlichtingendiensten “informatie en persoonsgegevens [mogen][…] verwerken die nuttig kunnen zijn om hun opdrachten te vervullen”.

Art. 84

Het gaat over een overname van artikel 16, § 2, van de wet van 8 december 1992. Voor de bescherming van de rechten van betrokkenen en om de verantwoordelijkheid en aansprakelijkheid van de inlichtingen- en veiligheidsdiensten en hun verwerkers te bepalen, is het noodzakelijk dat verantwoordelijkheden op duidelijke

Au sujet des décisions, la règle est que les services de renseignement ne prennent en principe pas de décisions ayant des effets juridiques directs à l’égard des citoyens. Le rôle principal des services de renseignement est d’informer les autorités publiques, essentiellement, à propos de menaces véhiculées par des individus, dès lors que ces menaces ont un lien avec les missions des autorités averties. Ce sont ces autorités publiques compétentes qui prennent les décisions qui s’imposent (par exemple l’Office des étrangers).

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 83

Le présent article détermine certaines obligations pour le responsable du traitement des services de renseignement et de sécurité. Il doit veiller à la justesse des données à caractère personnel. Il doit également veiller à ce que, pour les personnes agissant sous leur autorité, l’accès aux données soit limité à ce qui est utile pour l’exercice de leurs fonctions ou pour les besoins du service. Les services de renseignement et de sécurité font également en sorte que les personnes agissant sous leur autorité aient connaissance des obligations et prescriptions qui leur sont imposées par le présent sous-titre.

Ces obligations sont conformes à celles du responsable du traitement contenues dans l’article 16, § 2, 1°, de la loi du 8 décembre 1992, avec une petite adaptation pour rendre le texte conforme à l’article 13 de la loi du 30 novembre 1998 qui dispose que les services de renseignement peuvent “*traiter des informations et des données à caractère personnel qui peuvent être utiles à l’exécution de leurs missions*”.

Art. 84

Il s’agit d’une reprise de l’article 16, § 2, de la loi du 8 décembre 1992. Pour la protection des droits des personnes concernées et pour déterminer les responsabilités des services de renseignement et de sécurité et celles des sous-traitants, il est nécessaire que des responsabilités soient fixées de manière claire quand

wijze worden vastgesteld wanneer een verwerking namens een inlichtingen- en veiligheidsdienst wordt uitgevoerd.

De verwerkingsverantwoordelijke moet een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking. De uitvoering van een verwerking door een verwerker dient te worden geregeld door een overeenkomst die de verwerker bindt aan de verwerkingsverantwoordelijke, en waarin met name is bepaald dat de verwerker uitsluitend op instructie van de inlichtingen- en veiligheidsdienst dient te handelen, dat hij de voorziene technische beveiligingsmaatregelen naleeft en dat hij door dezelfde verplichtingen als deze van de betrokken inlichtingendienst is gebonden.

Deze overeenkomst bepaalt ook de verantwoordelijkheden van de verwerker.

Art. 85

Dit artikel legt aan de verwerker dezelfde verplichtingen op als deze waartoe de verwerkingsverantwoordelijken zijn gehouden.

Gelet op de opdrachten van de inlichtingen- en veiligheidsdiensten en de gevoeligheid van sommige persoonsgegevens, mag de verwerker de verwerking niet aan een andere verwerker doorgeven zonder de uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Art. 86

Dit artikel is een overname van artikel 16, § 3, van de wet van 8 december 1992. Een verwerker of eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker zelf verwerkt de persoonsgegevens slechts in opdracht van de verwerkingsverantwoordelijke, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 87

Wanneer meerdere verwerkingsverantwoordelijken worden aangesteld voor éénzelfde verwerking, worden zij de gezamenlijke verwerkingsverantwoordelijken

un traitement est effectué au nom d'un service de renseignement et de sécurité.

Le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements. L'exécution d'un traitement par un sous-traitant doit être réglée par un accord qui lie le sous-traitant au responsable du traitement et dans lequel il est notamment fixé que le sous-traitant agit exclusivement sur instruction du service de renseignement et de sécurité, qu'il respecte les mesures de sécurité techniques prévues et qu'il est tenu aux mêmes obligations que le service de renseignement concerné.

Cet accord détermine aussi les responsabilités du sous-traitant.

Art. 85

Cet article impose au sous-traitant les mêmes obligations que celles qui incombent aux responsables de traitement.

Vu les missions des services de renseignement et de sécurité et la sensibilité de certaines données à caractère personnel, le sous-traitant ne peut pas confier le traitement à un autre sous-traitant sans l'autorisation expresse du responsable du traitement.

Art. 86

Cet article est une reprise de l'article 16, § 3, de la loi du 8 décembre 1992. Un sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant lui-même ne traite des données à caractère personnel que sur instruction du responsable du traitement, sauf en cas d'obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 87

Lorsque plusieurs responsables du traitement sont désignés pour un même traitement, on appelle ceux-ci responsables conjoints du traitement. Cet article

genoemd. Dit artikel beoogt de hypothese waarbij er meerdere verwerkingsverantwoordelijken voor één persoonsgegevensbank zijn, waarin verwerkingen van een inlichtingen- en veiligheidsdienst vervat zijn. De verplichtingen van de verwerkingsverantwoordelijken ten aanzien van de betrokken personen en de mededeling van gegevens, zijn in het algemeen gedefinieerd door of krachtens de wet. Gezien er in dit geval meerdere verwerkingsverantwoordelijken zijn, moeten hun respectievelijke verplichtingen gepreciseerd worden. Indien dit niet voorzien is door of krachtens de wet, biedt dit artikel de mogelijkheid om de verplichtingen vast te leggen in een akkoord. Voor het gemak van de betrokken personen kan in het akkoord één contactpunt aangewezen worden voor de verschillende verwerkingsverantwoordelijken.

Om te antwoorden op het punt 233 van het advies van de Privacycommissie werd het derde lid aangepast om het aanduiden van een enkel contactpunt op te leggen.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 88

Dit artikel herneemt artikel 16, § 4, WVP. Het vermeldt de passende technische en organisatorische maatregelen die de verwerkingsverantwoordeljke moet treffen. Dit artikel stelt dat er hierbij steeds een belangenafweging gemaakt wordt. Zo worden de stand van de techniek (technologische evoluties), de kosten van de toe te passen maatregelen, de aard van de te beveiligen gegevens en de mogelijke risico's mee in overweging genomen om het passende karakter van de maatregelen vast te stellen.

Om haar wettelijke verplichtingen inzake het beschermen van haar bronnen en de derden die hun medewerking verlenen, van de identiteit van haar agenten en van de inlichtingenonderzoeken te waarborgen, is het cruciaal voor een inlichtingen- en veiligheidsdienst dat de technische en organisatorische maatregelen op deze verplichtingen aansluiten. Daarnaast bepaalt artikel 13 van de wet van 30 november 1998 dat de agenten van de inlichtingen- en veiligheidsdiensten toegang hebben tot de ingewonnen en verwerkte persoonsgegevens, voor zover deze nuttig zijn voor hun opdracht.

Buiten deze interne maatregelen, zijn er ook tal van externe maatregelen die in het belang van de uitoefening van hun opdrachten reeds opgelegd worden aan de inlichtingen-en veiligheidsdiensten:

vise l'hypothèse où il y a plusieurs responsables du traitement pour une banque de données à caractère personnel,dans laquelle il y a des traitements d'un service de renseignement et de sécurité. De manière générale, les obligations des responsables du traitement à l'égard des personnes concernées et de la communication des données sont définies par ou en vertu de la loi. Compte tenu qu'en l'espèce, il y a plusieurs responsables du traitement, il faut que leurs obligations respectives soient précisées. Si ce n'est pas prévu par ou en vertu de la loi, cet article permet que ces obligations respectives soient définies dans un accord. Pour la facilité des personnes concernées, l'accord peut aussi désigner un seul point de contact pour les différents responsables du traitement.

Pour répondre au point 233 de l'avis de la Commission vie privée, l'alinéa 3 a été adapté pour imposer la désignation d'un seul point de contact.

Section 3

Sécurité des données à caractère personnel

Art. 88

Cet article reprend l'article 16, § 4, LVP. Il mentionne les mesures techniques et organisationnelles adéquates que le responsable du traitement doit prendre. Cet article suppose toujours une mise en balance des intérêts. Ainsi, l'état de la technique (les progrès technologiques), les coûts des mesures à appliquer, la nature des données à protéger et les risques encourus doivent être pris en considération pour déterminer le caractère adéquat des dispositions à prendre.

Il est crucial pour un service de renseignement et de sécurité que ces mesures techniques et organisationnelles correspondent à ses obligations légales en matière de protection de ses sources, des tiers qui lui prêtent leur concours, de l'identité de ses agents et des enquêtes de renseignement. Par ailleurs, l'article 13 de la loi du 30 novembre 1998 prescrit que les agents des services de renseignement et de sécurité n'ont accès aux données à caractère personnel recueillies et traitées que pour autant qu'elles soient utiles à l'exécution de leur mission.

En dehors de ces mesures internes, il existe aussi nombre de mesures externes qui ont déjà été imposées aux services de renseignement et de sécurité dans l'intérêt de l'exercice de leurs missions:

1. De classificatieregels zoals bepaald in de wet van 11 december 1998, die onder andere een veiligheidsmachtiging voor de agenten van de inlichtingen- en veiligheidsdiensten voorzien;

2. NAVO-veiligheidsregels;

3. Richtlijnen van de Nationale Veiligheidsraad;

4. Richtlijnen van de Nationale Veiligheidsoverheid.

Art. 89

Om het toezicht op de inlichtingendiensten daadkrachtiger te maken, voert dit artikel een nieuwe verplichting in voor de verwerkingsverantwoordelijke. Zo moet de verwerkingsverantwoordelijke zo snel mogelijk het Vast Comité I, op de hoogte brengen indien er een inbreuk op de beveiliging plaatsvindt die een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Om te antwoorden op de aanbeveling van de Privacycommissie (punt 234 van het advies) en van de Raad van State (pagina 34 van het advies) werd het ontwerp aangepast om het respecteren van een termijn toe te voegen van 72 uur ten laatste na kennis te hebben genomen van de inbreuk op de beveiliging, indien dit mogelijk is. Er is echter geen sprake van een kennisgeving aan de betrokkene, gezien dit in het belang van de uitvoering van de opdrachten van de inlichtingen- en veiligheidsdiensten niet mogelijk is. Het beschermen van de nationale veiligheid laat het uitblijven van deze kennisgeving toe.

De verwerker moet elke inbreuk op de beveiliging melden aan de verwerkingsverantwoordelijke die het risico voor de rechten en vrijheden van personen zal beoordelen. Opnieuw is er hier echter geen sprake van een kennisgeving aan de betrokkene. De te vermelden gegevens worden opgesomd in het wetsartikel. Om de inlichtingenonderzoeken, de bronnen van de inlichtingen- en veiligheidsdiensten en derden die hun medewerking aan de diensten verlenen te beschermen, worden deze gegevens beperkt.

Afdeling 4

Registers

Art. 90

Eveneens om een meer doeltreffend toezicht toe te laten, introduceert dit artikel een nieuwe verplichting voor de verwerkingsverantwoordelijke van de

1. les règles de classification telles que définies dans la loi du 11 décembre 1998, qui prévoient entre autres une habilitation de sécurité pour les agents des services de renseignement et de sécurité;

2. les règles de sécurité de l'OTAN;

3. les directives du Conseil national de sécurité;

4. les directives de l'Autorité nationale de sécurité.

Art. 89

Cet article introduit une nouvelle obligation à charge du responsable du traitement afin de rendre plus efficace le contrôle exercé sur eux. Le responsable du traitement doit dans les meilleurs délais mettre au courant le Comité permanent R, d'une brèche de sécurité si elle recèle un risque élevé pour les droits et libertés de personnes physiques. Pour répondre à la recommandation de la Commission vie privée (point 234 de son avis) et du Conseil d'État (page 34 de son avis), le projet a été adapté pour ajouter le respect d'un délai de 72 heures au plus tard après avoir pris connaissance de la brèche de sécurité, si cela est possible. Par contre, il n'est pas question d'une notification à la personne concernée, vu que ce n'est pas possible dans l'intérêt de l'exercice des missions des services de renseignement et de sécurité. La protection de la sécurité nationale permet l'omission de cette notification.

Le sous-traitant doit notifier toute brèche de sécurité au responsable du traitement qui évaluera le risque pour les droits et libertés des personnes. Ici non plus il n'est pas question de notification à la personne concernée. Le texte légal énumère les informations à communiquer. Ces informations sont limitées en vue de protéger les enquêtes de renseignement, les sources des services de renseignement et de sécurité et les tiers qui leur prêtent leur concours.

Section 4

Registres

Art. 90

Pour permettre un contrôle plus efficace, cet article introduit une nouvelle obligation dans le chef du responsable du traitement des services de renseignement.

inlichtingendiensten. Deze dienen een register bij te houden van hun gegevensbanken en van deze die hen ter beschikking worden gesteld.

De keuze werd gemaakt om het bijhouden van een register van gegevensbanken op te leggen en niet van de verwerkingsactiviteiten. Deze keuze wordt verantwoord door het feit dat de gegevensbanken het resultaat van het geheel van de verwerkingsactiviteiten door de inlichtingendienst inhoudt (behalve wanneer het gegeven niet werd ingegeven of verwijderd wegens niet pertinent). Omgekeerd is het moeilijk om de verschillende verwerkingsactiviteiten van de diensten op te sommen aangezien deze praktisch enkel gegevensverwerking doen en al hun activiteiten verweven zijn. Indien de verwerkingsactiviteiten van de inlichtingendiensten zouden moeten worden "afgegrensd", dan zouden zij bestaan uit "verzameling" en "analyse". Dit heeft echter geen zin aangezien deze betrekking hebben op dezelfde gegevens. Bovendien zouden de registers in dat geval vaag en algemeen zijn. Een register met de verschillende gegevensbanken lijkt meer aangewezen om een gerichtere controle toe te laten.

Ter informatie, de activiteiten van collecte van de inlichtingendiensten maken reeds het voorwerp uit van een controle door het Comité I (en in bepaalde gevallen door de BIM-Commissie) op grond van de wetten van 30 november 1998 en van 18 juli 1991.

Het register moet geclassificeerd zijn in de zin van de wet van 11 december 1998 want de meeste gegevensbanken van de inlichtingendiensten zijn zelf geclassificeerd.

Dit artikel somt de informatie op die vermeld moet worden in het register. Voor de gegevensbanken van de diensten werden dezelfde vermeldingen als die uit het artikel 30 van de Verordening hernomen, met uitzondering van de categorieën van personen en categorieën van persoonsgegevens, zonder onderscheid. Strikt genomen is er trouwens geen sprake van categorieën van personen en gegevens in het werk van de inlichtingendiensten. Er is geen slachtoffer of getuige. Er zijn eenvoudigweg enkel betrokkenen en hun omgeving. De gegevensbanken houden alle persoonsgegevens bij die noodzakelijk zijn voor de uitvoering van de opdrachten van de inlichtingendiensten.

In de punten 235 en 236 van haar advies uit de Privacycommissie haar verbazing over het feit dat de inlichtingendiensten in hun register niet de categorieën van personen en gegevens moeten opnemen. Een

Ceux-ci doivent tenir un registre de leurs banques de données et de celles mises à leur disposition.

Il a été fait le choix d'imposer la tenue d'un registre portant sur les banques de données et non sur les activités de traitement. Ce choix est motivé par le fait que les banques de données contiennent le résultat de l'ensemble des activités de traitement des services de renseignement (sauf si la donnée n'est pas introduite ou est effacée pour cause de non pertinence). A l'inverse, il est difficile d'énumérer différentes activités de traitement des services puisque ceux-ci ne font pratiquement que du traitement de données à caractère personnel et que toutes leurs activités sont indissociables. S'il fallait "délimiter" les activités de traitement des services de renseignement, elles consisteraient en "collecte" et "analyse". Mais cela n'a pas de sens de séparer les deux puisqu'elles portent sur les mêmes données. En outre, les registres ne pourraient être que vagues et généraux. Un registre portant sur les différentes banques de données paraît plus judicieux pour permettre un contrôle plus pointu.

Pour information, les activités de collecte des services de renseignement font déjà l'objet d'un contrôle du Comité R (et dans certains cas aussi de la Commission BIM) en application des lois du 30 novembre 1998 et du 18 juillet 1991.

Le registre doit être classifié au sens de la loi du 11 décembre 1998 car la plupart des banques de données des services de renseignement sont elles-mêmes classifiées.

Cet article énumère les informations qui doivent être mentionnées dans le registre. Pour les banques de données des services, les mêmes mentions que celles prévues à l'article 30 du Règlement sont reprises, à l'exception des catégories de personnes concernées et des catégories de données à caractère personnel. La raison en est que les services de renseignement traitent indifféremment de toutes les catégories de personnes et de données, sans distinction. Il n'existe d'ailleurs pas à proprement parler de catégories de personnes ou de données dans le travail de renseignement. Il n'y a pas de victime ou de témoin. Il y a simplement des personnes concernées et leur environnement. Les banques de données contiennent toutes les données à caractère personnel nécessaires pour exécuter les missions des services de renseignement.

Aux points 235 et 236 de son avis, la Commission vie privée exprime son étonnement quant au fait que les services de renseignement ne doivent pas reprendre dans leur registre les catégories de personnes et de

herinnering van het wettelijk kader dringt zich dus op: de inlichtingendiensten worden wettelijk door geen enkele reglementering verplicht een register te bij houden. De wetgever beslist desondanks hen het houden van een register op te leggen waarvan het doel, we herhalen, is om de controle te faciliteren. De wetgever meent dat een register van de gegevensbanken de controle van de verwerkingen door de inlichtingendiensten makkelijker en efficienter maakt dan een register van de verwerkingsactiviteiten die de categorieën van personen of gegevens vermelden. Deze keuze wordt overigens hierboven verklaard, in het bijzonder de afwezigheid van werkelijke categorieën van personen en het feit dat elk type van gegevens wordt verzameld. De Privacycommissie stelt als categorieën van personen de extremisten, geradicaliseerden, salafisten,… voor. Het is echter niet altijd mogelijk noch wenselijk om personen in categorieën onder te brengen en hen in vakjes te steken (in het bijzonder het milieu van een betrokkene). Bovendien zijn de voorgestelde categorieën in werkelijkheid de doeleinden van de inlichtingendiensten. Deze doeleinden maken deel uit van de vermeldingen die zich in het register moeten bevinden.

Wat betreft de gegevensbanken waartoe de inlichtingendiensten toegang hebben, zijn de vermeldingen gelimiteerd aangezien alle informatie vervat in deze banken zich bevinden in de registers bijgehouden door de verantwoordelijke van de verwerking van voornoemde banken. Indien het om een gegevensbank in het buitenland gaat, is het overigens mogelijk dat de inlichtingendienst niet over de precieze contactgegevens van de verwerkingsverantwoordelijke beschikt of dat hij niet dezelfde definitie van de term “verwerkingsverantwoordelijke” hanteert, of zelfs geen functionaris voor gegevensbescherming heeft. Om te antwoorden op het punt 237 van het advies van de Privacycommissie wordt duidelijker aangegeven dat de inlichtingendienst, voor de landen buiten de Europese Unie, de contactgegevens van de “dienst die de gegevensbank beheert” moet vermelden, indien deze gekend zijn.

De verwerker heeft eveneens de verplichting om een geclassificeerd register met alle categorieën van verwerkingsactiviteiten, uitgevoerd voor rekening van de inlichtingendiensten, bij te houden. Het register heeft hier wel betrekking op de verwerkingsactiviteiten aangezien de opdracht die werd toevertrouwd aan een verwerker steeds betrekking heeft op de een of andere gepreciseerde activiteit. Integendeel, de categorieën van personen of gegevens kunnen niet op voorhand bepaald worden vermits zij slechts gekend zullen worden op het moment van de verwerking (bijvoorbeeld een onderzoek in open bronnen, een analyse van een

données. Un petit rappel du contexte légal s’impose: les services de renseignement ne sont légalement obligés par aucune règlementation de tenir un registre. Le législateur décide néanmoins de leur imposer la tenue d’un registe, dont le but, rappelons-le, est de faciliter le contrôle. Le législateur estime qu’un registre des banques de données rend plus facile et plus efficace le contrôle des traitements des services de renseignement qu’un registre des activités de traitement mentionnant des catégories de personnes ou de données. Ce choix est d’ailleurs expliqué ci-dessus, notamment l’absence de réelles catégories de personnes et le fait que tout type de données sont collectées. La Commission vie privée propose comme catégories de personnes les extrémistes, les radicalistes, les salafistes, … Il n’est cependant pas toujours possible, ni souhaitable de catégoriser des personnes et de les mettre toutes dans des cases (notamment le milieu d’une personne concernée). En outre, les catégories proposées sont en réalité les finalités des services de renseignement. Ces finalités font partie des mentions devant se trouver dans le registre.

Pour les banques de données auxquelles les services ont accès, les mentions sont limitées car toutes les informations portant sur ces banques se trouvent dans le registre tenu par le responsable du traitement desdites banques. Par ailleurs, s’il s’agit d’une banque de données à l’étranger, il est possible que le service de renseignement ne dispose pas des coordonnées exactes du responsable du traitement, ou même qu’il n’y ait pas une même définition des termes “responsable du traitement”, voir pas de délégué à la protection des données. Pour répondre au point 237 de l’avis de la Commission vie privée, il est indiqué plus précisément que le service de renseignement doit mentionner, pour les pays hors Union européenne, les coordonnées du “service gestionnaire de la banque de données” si celles-ci sont connues.

Le sous-traitant a également l’obligation de tenir un registre classifié de toutes les catégories d’activités de traitement effectuées pour le compte du service de renseignement concerné. Le registre porte ici sur les activités de traitement car la mission confiée au sous-traitant portera toujours sur l’une ou l’autre activité précise. Par contre, les catégories de personnes ou de données ne peuvent pas être déterminées à l’avance puisqu’elles ne seront connues qu’à l’issue du traitement (par exemple une recherche dans les sources ouvertes, une analyse d’un phénomène sur les média sociaux). Aucun destinataire n’est mentionné car c’est le service concerné,

fenomeen op sociale media). Geen enkele bestemmeling wordt vermeld aangezien het de betrokken dienst is, en niet de verwerker, die de verzamelde gegevens zal doorgeven.

De derde paragraaf voorziet een schriftelijke vorm, met inbegrip van elektronische vorm, voor het register.

De vierde paragraaf bepaalt dat de registers ter beschikking worden gesteld op vraag van de bevoegde toezichthoudende autoriteit. Het register van de verwerker wordt steeds ter beschikking gesteld van de verwerkingsverantwoordelijke.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 91

Dit artikel legt de aanduiding van een functionaris voor gegevensverwerking op door de verwerkingsverantwoordelijke en, in voorkomend geval de verwerker. Deze moet titularis zijn van een veiligheidsmachtiging zeer geheim want de inlichtingendiensten kunnen classificeren tot en met dit niveau. Hij mag niet worden ontzet uit zijn functies omwille van de uitvoering van zijn opdrachten.

Om rekening te houden met een waarneming van de Raad van State (pagina 35 van het advies) wordt het ontwerp aangepast om de mogelijkheid te beogen voor de verwerkingsverantwoordelijke om tot het stopzetten van het mandaat van de functionaris voor gegevensbescherming te kunnen beslissen indien hij een zware fout heeft begaan of de voorwaarden noodzakelijk voor het uitoefenen van zijn functie niet langer vervult. De betrokkene zal zich tot het Vast Comité I kunnen richten om deze beslissing aan te vechten.

Zijn functie herneemt deze van de raadgever informatieveiligheid vervat in artikel 4 van het Koninklijk Besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 en wordt uitgebreid. De functionaris wordt betrokken bij alle vragen betreffende de bescherming van persoonsgegevens.

Hij oefent zijn functie in volledige onafhankelijkheid uit en moet beschikken over de nodige middelen. De Koning kan indien nodig, andere modaliteiten voor de werking vastleggen en de bevoegdheden van de functionaris uitbreiden.

et non le sous-traitant, qui transmettra éventuellement les renseignements collectés.

Le paragraphe 3 prévoit une forme écrite, y compris la forme électronique pour le registre.

Le paragraphe 4 dispose que les registres sont mis à la disposition de l'autorité de contrôle compétente à sa demande. Le registre du sous-traitant est en permanence mis à la disposition du responsable du traitement.

Section 5

Délégué à la protection des données

Art. 91

Cet article impose la désignation d'un délégué à la protection des données par le responsable du traitement, et le cas échéant, par le sous-traitant. Celui-ci doit être titulaire d'une habilitation de sécurité du niveau très secret car les services de renseignement peuvent classifier jusqu'à ce niveau. Il ne peut pas être relevé de ses fonctions en raison de l'exercice de ses missions.

Pour tenir compte d'une observation du Conseil d'État (page 35 de son avis), le projet est adapté pour viser la possibilité pour le responsable du traitement de décider de la cessation de fonctions du délégué à la protection des données concerné, en raison de l'exercice gravement fautif de ses fonctions ou parce qu'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions. L'intéressé pourra s'adresser au Comité permanent R pour contester cette décision.

Sa fonction reprend celle du conseiller en sécurité de l'information visé à l'article 4 de l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique et est étendue. Le délégué doit être associé à toutes les questions relatives à la protection des données à caractère personnel.

Il exerce ses fonctions en toute indépendance et doit disposer des ressources nécessaires. Le Roi peut fixer, si nécessaire, d'autres modalités de fonctionnement et étendre les compétences du délégué.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van gegevens aan de publieke sector en de privésector

Art. 92

De uitwisseling van gegevens tussen de inlichtingen- en veiligheidsdiensten, en de publieke en private sector wordt geregeld in de artikelen 14, 16 en 19 van de wet van 30 november 1998. Betrokken bepalingen bevatten de wettelijke modaliteiten voorde informatie-uitwisseling in dit kader.

Artikel 14 van de wet van 30 november 1998 organiseert de informatie-uitwisseling met de publieke sector. Deze bepaling stelt:

"De gerechtelijke overheden, de ambtenaren en agenten van de openbare diensten, die van de politiediensten inbegrepen, kunnen uit eigen beweging aan de betrokken inlichtingen- en veiligheidsdienst de informatie meedelen die nuttig is voor de uitvoering van zijn opdrachten. Op verzoek van een inlichtingen- en veiligheidsdienst, delen de gerechtelijke overheden, de ambtenaren en agenten van de openbare diensten, die van de politiediensten inbegrepen, aan de betrokken inlichtingen- en veiligheidsdienst, de informatie mee die nuttig is voor de uitvoering van zijn opdrachten. Wanneer de gerechtelijke overheden, de ambtenaren en de agenten van de openbare diensten, die van de politiediensten inbegrepen, van oordeel zijn dat het meedelen van de informatie bedoeld in het tweede lid van aard is afbreuk te doen aan een lopend opsporings- of gerechtelijk onderzoek, of aan de verzameling van gegevens overeenkomstig de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, of iemand in zijn persoonlijke fysieke integriteit kan schaden, kunnen zij binnen vijf werkdagen na ontvangst van de aanvraag deze mededeling weigeren en delen zij de redenen hiervan schriftelijk mee. Met inachtneming van de geldende wetgeving kunnen de inlichtingen- en veiligheidsdiensten, overeenkomstig de door de Koning vastgelegde algemene nadere regels, toegang krijgen tot de gegevensbanken van de openbare sector die nuttig zijn voor de uitoefening van hun opdrachten."

Artikel 16 van de wet van 30 november 1998 organiseert de informatie-uitwisseling met de private sector.

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données avec le secteur public et le secteur privé

Art. 92

L'échange de données entre les services de renseignement et de sécurité et les secteurs public et privé est réglée dans les articles 14, 16 en 19 de la loi du 30 novembre 1998. Les dispositions concernées contiennent les modalités légales de l'échange d'informations dans ce cadre.

L'article 14 de la loi du 30 novembre 1998 organise l'échange d'informations avec le secteur public et dispose:

"Les autorités judiciaires, les fonctionnaires et les agents des services publics, y compris des services de police, peuvent communiquer d'initiative au Service de Renseignement et de Sécurité concerné les informations utiles à l'exécution de ses missions. A la requête d'un service de renseignement et de sécurité, les autorités judiciaires, les fonctionnaires et les agents des services publics, y compris des services de police, communiquent au service de renseignement et de sécurité concerné, les informations utiles à l'exécution de ses missions. Lorsque les autorités judiciaires, les fonctionnaires et les agents des services publics, y compris les services de police, estiment que la communication des informations visées à l'alinéa 2 est de nature à porter atteinte à une information ou à une instruction judiciaire en cours ou à la récolte d'informations visée par la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, ou qu'elle est susceptible de nuire à l'intégrité physique d'une personne, ils peuvent refuser cette communication dans les cinq jours ouvrables de la demande, en exposant leurs raisons par écrit. Dans le respect de la législation en vigueur, les services de renseignement et de sécurité peuvent selon les modalités générales fixées par le Roi, avoir accès aux banques de données du secteur public utiles à l'exécution de leurs missions."

L'article 16 de la loi du 30 novembre 1998 organise l'échange d'information avec le secteur privé et dispose:

Deze bepaling stelt:

"De personen en organisaties die behoren tot de privésector kunnen, onverminderd artikel 2, § 2, uit eigen beweging aan de inlichtingen- en veiligheidsdiensten de informatie en persoonsgegevens meedelen die nuttig zijn voor de uitvoering van hun opdrachten. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, onverminderd artikel 2, § 2, informatie en persoonsgegevens inwinnen bij personen en organisaties die behoren tot de privésector."

Artikel 19 van de wet van 30 november 1998 bepaalt de voorwaarden waaronder de inlichtingen- en veiligheidsdiensten gegevens aan de publieke en private sector meedelen.

De twee eerstvermelde bepalingen werden recent gewijzigd door de wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek. Meer in het bijzonder werden voor wat betreft artikel 14 van de wet van 30 november 1998 de woorden "*op basis van de eventueel afgesloten akkoorden*" geschrapt. De memorie van toelichting geeft volgende verduidelijking:

"Artikel 14 betreft de mededeling door de gerechtelijke autoriteiten en openbare diensten, met inbegrip van de politiediensten, van informatie die nuttig is voor de uitvoering van de opdrachten van de inlichtingendiensten. Deze bepaling voorziet dat eventueel akkoorden kunnen worden afgesloten om deze mededeling te regelen. Een protocolakkoord is evenwel nooit verplicht. Het spreekt daarentegen voor zich dat als een inlichtingendienst een akkoord ondertekent met een overheid, dat akkoord moet worden toegepast. Die woorden zijn dus onnodig en kunnen tot verwarring leiden, aangezien sommige overheden enkel op grond van een bestaand akkoord informatie willen meedelen. Zij worden dan ook geschrapt."

Dit artikel ligt in lijn met de recente keuze van de wetgever om de samenwerking en informatie-uitwisseling tussen de inlichtingen- en veiligheidsdiensten en de publieke sector niet te laten afhangen van het bestaan van een protocolakkoord.

Dit geldt eveneens voor de uitwisselingen met de privésector. De wet van 30 maart 2017 creëerde, in artikel 16 van de wet van 30 november 1998, een spreekrecht in hoofde van de personen en instanties die behoren tot de privésector. De memorie van toelichting geeft volgende verduidelijking: *"Er wordt voorgesteld artikel 16 te wijzigen om de mogelijkheid te voorzien*

"Sans préjudice de l'article 2, § 2, les personnes et organisations relevant du secteur privé peuvent communiquer d'initiative aux services de renseignement et de sécurité, les informations et les données à caractère personnel utiles à l'exercice de leurs missions. Dans l'intérêt de l'exercice de leurs missions, sans préjudice de l'article 2, § 2, les services de renseignement et de sécurité peuvent collecter auprès des personnes et organisations relevant du secteur privé des informations et des données à caractère personnel."

L'article 19 de la loi du 30 novembre 1998 fixe les conditions dans lesquelles les services de renseignement et de sécurité communiquent des données aux secteurs public et privé.

Les deux premières dispositions ont été récemment modifiées par la loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal. Plus précisément en ce qui concerne l'article 14 de la loi du 30 novembre 1998, les mots *"sur la base des accords éventuellement conclus*" ont été supprimés. L'exposé des motifs donne la précision suivante:

"L'article 14 concerne la communication par les autorités judiciaires et les services publics, y compris les services de police, d'informations utiles à l'exécution des missions des services de renseignement. La disposition prévoit que des accords peuvent éventuellement être conclus pour régler cette communication. Néanmoins, un protocole d'accord n'est jamais obligatoire. Par contre, il est évident que si un service de renseignement signe un accord avec une autorité, cet accord sera appliqué. Ces termes sont donc inutiles et peuvent prêter à confusion. En effet, certaines autorités exigent l'existence d'un accord pour communiquer des informations. Ces termes sont donc supprimés."

Le présent article va dans le sens du choix récent du législateur de ne pas faire dépendre la collaboration et l'échange d'informations entre les services de renseignement et de sécurité et le secteur public de l'existence d'un protocole d'accord.

Ceci vaut également pour les échanges avec le secteur privé. La loi du 30 mars 2017 a créé, dans l'article 16 de la loi du 30 novembre 1998, un droit de parler dans le chef des personnes et entités qui appartiennent au secteur privé. L'exposé des motifs donne la précision suivante: *"Il est proposé de modifier l'article 16 afin de prévoir la possibilité pour les personnes et instances*

voor privépersonen en instanties om uit eigen beweging informatie, zelfs persoonsgegevens, mee te delen aan een inlichtingen- en veiligheidsdienst.". Ook hier heeft de wetgever de keuze gemaakt om geen voorafgaand protocolakkoord te verplichten voor verwerkingen in het kader van de detectie van potentiële dreigingen voor de veiligheid van het land en de bevolking.

Dit artikel bepaalt ook dat een raadpleging van de functionaris voor gegevensbescherming of de bevoegde toezichthoudende autoriteit of een impactanalyse geen voorafgaande vereiste kunnen zijn voor de mededeling van informatie. De gegevensuitwisseling met de inlichtingendiensten, welke een loutere toepassing is van de artikelen 14, 16 en 19 van de wet van 30 november 1998 en beantwoordt aan de operationele vereisten van de nationale veiligheid en hoogdringendheid, mag niet vertraagd worden door een adviesaanvraag of een anlyse voor een pure toepassing van de wet. Als er overgegaan wordt tot een beoordeling van de belangen, dan spreekt voor zich dat de opdrachten tot nationale veiligheid waarmee de Belgische inlichtingendiensten belast zijn van hoger belang zijn dan andere belangen, voor zover ze een collectief belang beschermen en geen individuele belangen.

De uitzondering van artikel 23 van de Verordening op de impactanalyse is bovendien een toepassing van de uitzondering in artikel 35.10 van de Verordening:

"Wanneer verwerking uit hoofde van artikel 6, lid 1, onder c) of e), haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is, de specifieke verwerking of geheel van verwerkingen in kwestie daarbij wordt geregeld, en er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een gegevensbeschermingseffectbeoordeling is uitgevoerd, zijn de leden 1 tot en met 7 niet van toepassing, tenzij de lidstaten het noodzakelijk achten om voorafgaand aan de verwerkingen een dergelijke beoordeling uit te voeren."

De wetgever heeft de impactanalyse uitgevoerd wanneer de wet van 30 november 1998 werd aangenomen. Een impactanalyse voor elke uitwisseling is dus niet nodig.

Dit weerhoudt een overheidsinstantie of een particulier orgaan er logischerwijs niet van om een protocolakkoord te sluiten met een inlichtingen- en veiligheidsdienst of om het advies van de functionaris voor gegevensbescherming of van de bevoegde toezichthoudende autoriteit te vragen of een impactanalyse,

privées de communiquer d'initiative des informations, même des données à caractère personnel, à un service de renseignement et de sécurité.". Ici aussi le législateur a fait le choix de ne pas prévoir l'obligation d'un protocole d'accord préalable lors des traitements dans le cadre de la détection de menaces potentielles pour la sécurité du pays et de la population.

Le présent article dispose également qu'une consultation du délégué à la protection des données ou de l'autorité de contrôle compétente ou une analyse d'impact ne peuvent pas être exigées comme préalable à la transmission des informations. Les échanges de données avec les services de renseignement étant une simple application des articles 14, 16 et 19 de la loi du 30 novembre 1998 et répondant à des exigences opérationnelles de sécurité nationale et d'urgence, l'échange ne peut pas être retardé par la demande d'un avis ou d'une analyse sur une pure application de la loi. Lorsque l'on procède à une appréciation des intérêts en présence, il va de soi que les missions de sécurité nationale dont sont chargés les services de renseignement belges constituent un intérêt supérieur à d'autres intérêts, dans la mesure où elles protègent un intérêt collectif et non des intérêts individuels.

L'exception à l'article 23 du Règlement sur l'analyse d'impact est d'ailleurs une application de l'exception visée à l'article 35.10 du Règlement:

"Lorsque le traitement effectué en application de l'article 6, paragraphe 1er, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement."

Le législateur a fait l'analyse d'impact lorsqu'il a adopté la loi du 30 novembre 1998. Une analyse d'impact pour chaque échange n'est donc plus nécessaire.

Cela n'empêche évidemment pas l'autorité publique ou l'organisme privé de conclure un protocole d'accord avec un service de renseignement et de sécurité ou de demander l'avis de son délégué à la protection des données ou de l'autorité de contrôle compétente ou de procéder à une analyse d'impact, mais le résultat de

maar dit mag geen voorafgaande voorwaarde voor de informatie-uitwisseling zijn die er toe kan leiden dat de mededeling van belangrijke informatie die gericht is een zwaarwegender belang te beschermen vertraagd wordt.

Het derde lid van dit artikel wijkt af van artikel 22 § 1, tweede lid voor wat betreft de verplichte vermeldingen in het protocol. Dit is om evidente redenen van discretie over de *modus operandi* van inlichtingendiensten en meer bepaald de manier waarop zij informatie beschermen. Het derde lid van dit artikel legt minimum zes onontbeerlijke vermeldingen op.

Er wordt een vierde lid toegevoegd dat beoogt te verduidelijken dat, zelfs indien men acht dat het protocol niet moet worden geclassificeerd, een beperking van de verspreiding zich opdringt om evidente veiligheidsredenen. Het protocol zal daarom tenminste de markering "BEPERKTE VERSPREIDING" dragen in de zin van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998.

Afdeling 2

Doorgifte van gegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 93

Het eerste en tweede lid van dit artikel zijn een exacte reproductie van de eerste paragraaf van artikel 21 WVP. Zij hernemen het criteria van het adequate beschermingsniveau dat de niet-lidstaat van de Europese Unie moet waarborgen opdat de betrokken inlichtingendienst persoonsgegevens mag doorgeven. Enkel de termen "internationale organisatie" wordt toegevoegd omdat een internationale organisatie eveneens de bestemmeling kan zijn van persoonsgegevens. De derde alinea bepaalt dat het adequaat beschermingsniveau gewaarborgd kan worden door veiligheidsclausules waarop de betrokken inlichtingendienst en de bestemmeling zich afstemmen. Dit lid herneemt de idee van lid 2 van artikel 22 WVP.

Art. 94

Dit artikel voorziet uitzonderingen op de vereiste van een adequaat beschermingsniveau:

— na instemming van de betrokken persoon (kopij van artikel 22, 1°, van de wzet van 8 december 1992);

ces consultations ne peut pas être une condition préalable à l'échange d'informations qui serait susceptible de retarder la transmission d'une information dont le besoin peut être urgent et qui vise à protéger un intérêt supérieur et collectif.

L'alinéa 3 du présent article déroge à l'article 22 § 1er, alinéa 2 en ce qui concerne les mentions que doit contenir le protocole. Cela s'explique pour des raisons évidentes de discrétion du *modus operandi* des services de renseignement et notamment de la manière dont ils protègent les informations. L'alinéa 3 du présent article impose un minimum de six mentions indispensables.

Il est ajouté un 4ème alinéa visant à préciser que, même s'il est estimé que le protocole ne doit pas être classifié, une limitation de diffusion s'impose pour des raisons évidentes de sécurité. Dès lors, le protocole aura au minimum le marquage "DIFFUSION RESTREINTE" au sens de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998.

Section 2

Transfert des données vers des pays non membres de l'Union européenne ou à des organisations internationales

Art. 93

Les alinéas premier et 2 du présent article sont l'exacte reproduction du premier paragraphe de l'article 21 LVP. Ils reprennent le critère du niveau de protection adéquat que doit assurer le pays non membre de l'Union européenne pour que le service de renseignement concerné puisse lui transférer une donnée à caractère personnel. Seuls les termes "organisation internationale" ont été ajoutés puisqu'une organisation internationale peut également être le destinataire de données à caractère personnel. Le troisième alinéa fixe que le niveau de protection adéquat peut être assuré par des clauses de sécurité sur lesquelles s'accordent le service de renseignement concerné et le destinataire. Cet alinéa reprend l'idée de l'alinéa 2 de l'article 22 LVP.

Art. 94

Cet article prévoit des exceptions à l'exigence d'un niveau de protection adéquat:

— avec le consentement de la personne concernée (copie de l'article 22, 1°, de la loi du 8 décembre 1992);

— indien de doorgifte noodzakelijk of wettelijk verplicht is voor de bescherming van de fysieke integriteit van een persoon of van een belangrijk openbaar belang (fusie van 4° en 5°, van artikel 22 van de wet van 8 december 1992;

— indien de doorgifte noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend openbaar belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

Zelfs indien het voor de hand ligt dat de inlichtingen en veiligheidsdiensten de doorgifte van persoonsgegevens aan landen die niet een adequaat beschermingsniveau waarborgen, trachten te voorkomen, kan het gebeuren dat zij hiertoe verplicht zijn in het kader van de nationale veiligheid, de strijd tegen terrorisme, de bescherming van Belgische troepen in het buitenland, … Ter informatie, de samenwerking tussen de inlichtingen- en veiligheidsdiensten en hun buitenlandse partners wordt gereglementeerd in een door de Nationale Veiligheidsraad goedgekeurde richtlijn.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 95 tot 98

Het Vast Comité I is, in toepassing van de wet van 18 juli 1991 tot regeling van de controle op de politie- en inlichtingendiensten en op het OCAD, reeds belast met de controle op de twee inlichtingendiensten. Artikel 1 bepaalt dat "*het toezicht voornamelijk betrekking heeft op de bescherming die de Grondwet of de wet aan personen toebedeelt*".

Een groot deel van de gegevens die inlichtingendiensten verzamelen, zowel voor hun inlichtingen- als veiligheidsopdrachten, zijn persoonsgegevens.

Hieruit volgt dat de controle door het Vast Comité I al in grote mate betrekking heeft op de naleving, door beide inlichtingendiensten, van de regels die de verwerking van persoonsgegevens regelen.

Om een dubbele controle op dezelfde verwerking te vermijden, werd de optie geponeerd om het Comité I aan te stellen als toezichthoudende autoriteit wat de bescherming van persoonsgegevens betreft.

Deze aanstelling heeft als voordeel dat de verantwoordelijkheid wordt toegewezen aan een onafhankelijke instelling die reeds bekend is met het inlichtingenmilieu

— si le transfert est nécessaire ou légalement obligatoire à la sauvegarde de l'intégrité physique d'une personne ou d'un intérêt public important (fusion des 4° et 5°, de l'article 22 de la loi du 8 décembre 1992);

— si le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

Même s'il est évident que les services de renseignement et de sécurité essaient d'éviter de transférer des données à caractère personnel à des pays n'assurant pas un niveau de protection adéquat, il arrive qu'ils y soient contraints dans un objectif de sécurité nationale, de lutte contre le terrorisme, de protection des troupes belges à l'étranger, … A titre d'information, une directive approuvée par le Conseil national de sécurité règlemente la collaboration des services de renseignement et de sécurité avec leurs partenaires étrangers.

CHAPITRE X

Autorité de contrôle

Art. 95 à 98

Le Comité permanent R est déjà chargé, en application de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'OCAM, de contrôler les deux services de renseignement. L'article premier dispose que "*le contrôle porte en particulier sur la protection des droits que la Constitution et la loi confèrent aux personnes*".

Une grande partie des données collectées par les services de renseignement, tant dans leurs missions de renseignement que dans celles de sécurité, sont des données à caractère personnel.

Par conséquent, le contrôle exercé par le Comité R porte déjà très largement sur le respect, par les deux services de renseignement, des règles régissant le traitement des données à caractère personnel.

Pour éviter un double contrôle sur le même traitement, le choix est posé de désigner le Comité R comme autorité de protection des données.

Cette désignation a l'avantage de confier cette responsabilité à une institution indépendante qui connaît déjà le milieu du renseignement et qui répond aux

en die beantwoordt aan de vereisten van beveiliging voor de behandeling van geclassificeerde gegevens in de zin van de wet van 11 december 1998.

De controlebevoegdheid van het Comité I op de verwerking van persoonsgegevens door de inlichtingendiensten wordt bevestigd door middel van een aanpassing van de wet van 18 juli 1991.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden

Art. 99

Zoals uiteengezet in de inleiding, is de raadpleging van persoonsgegevens van de inlichtingen -en veiligheidsdiensten of zijn personeel door een verdere verwerkingsverantwoordelijke voor historische, wetenschappelijke of statistische doeleinden slechts mogelijk indien dit geen weerslag heeft op de opdrachten van de inlichtingendiensten, noch een bron of een derde die zijn medewerking verleent in gevaar brengt, en indien dit geen weerslag heeft op een lopend opsporings- of gerechtelijk onderzoek of op de relaties die België onderhoudt met vreemde Staten of internationale organisaties.

De behandeling van geclassificeerde documenten moet vanzelfsprekend de bepalingen van de wet van 11 december 1998 respecteren. Deze specifieke reglementering is nodig aangezien een aanvraag tot raadpleging van persoonsgegevens van de inlichtingen -en veiligheidsdiensten voor historische, wetenschappelijke en statistische doeleinden op elk moment kan gebeuren, zelfs wanneer een inlichtingenonderzoek nog steeds lopende is. Het is nodig te vermijden dat een betrokkene van een dienst, onder het voorwendsel dat zij studente is, kennis kan nemen van het feit dat zij het voorwerp uitmaakt van een opvolging, wat het gehele onderzoek in het gedrang zou brengen. Dit regiem is niet van toepassing tot Rijksarchief.

Zelfs indien titel 4 van onderhavige wet niet van toepassing is op de inlichtingen- en veiligheidsdiensten, is het aangeraden om er een expliciete afwijking op te voorzien voor de andere organismen die hun gegevens verwerken alsook deze van hun personeel. Bepaalde persoonsgegevens van de diensten bevinden zich immers bij de Staatsarchieven; hun personeel wordt beheerd door andere algemene secretariaten van hun FOD/Ministerie, …

exigences de sécurité pour traiter des données classifiées au sens de la loi du 11 décembre 1998.

Les pouvoirs de contrôle du Comité R sur les traitements des données à caractère personnel par les services de renseignement sont renforcés par l'adaptation de la loi du 18 juillet 1991.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 99

Comme expliqué dans l'introduction, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel des services de renseignement et de sécurité et de leur personnel par un responsable du traitement ultérieur n'est possible que si elle ne porte pas atteinte aux missions des services de renseignement, ni ne met en danger une source ou un tiers qui prête son concours, et ne porte pas atteinte à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales.

Le traitement des données classifiées doit bien entendu aussi respecter les dispositions de la loi du 11 décembre 1998. Cette réglementation spécifique est nécessaire car une demande de consultation des données des services de renseignement à des fins historiques, scientifiques ou statistiques peut avoir lieu à tout moment, alors même qu'une enquête de renseignement est encore en cours. Il faut éviter qu'une personne concernée d'un service, sous prétexte qu'elle est étudiante, puisse prendre connaissance du fait qu'elle fait l'objet d'un suivi, ce qui mettrait en péril toute l'enquête. Ce régime n'est pas applicable aux Archives de l'État.

Même si le titre 4 de la présente loi n'est pas applicable aux services de renseignement et de sécurité, il convient d'y faire une dérogation expresse pour les autres organismes qui traitent leurs données ainsi que celles de leur personnel. En effet, certaines données à caractère personnel des services se trouvent aux Archives de l'État; la gestion de leur personnel se fait par d'autres directions générales de leur SPF/Ministère, …

De gegevens van het personeel van de inlichtingendiensten zijn beschermd om te vermijden dat de leden van deze diensten druk ondervinden, of zelfs bedreigingen moeten ondergaan omdat hun identiteit en hun hoedanigheid werd onthuld. Bijgevolg is het aangeraden te verduidelijken dat de bescherming van de gegevens van hun personeel deel uitmaakt van de opdrachten van de inlichtingendiensten. Dit geldt eveneens voor de bronnen en derden die hun medewerking verlenen aan de inlichtingendiensten. De betrokken dienst heeft de verplichting om ook hun gegevens te beschermen (art. 13, al. 3 en art. 13/4, al.2 van de wet van 30 november 1998).

De toelating tot raadpleging moet gegeven worden door de inlichtingendienst, zelfs indien het gegeven niet meer in haar bezit is , omdat deze het beste kan evalueren of een raadpleging een weerslag kan hebben op één van de te beschermen belangen.

Hiertoe, wanneer de persoonsgegevens van de inlichtingen- en veiligheidsdiensten overgedragen zijn naar het Algemeen Rijksarchief, dan zou het kunnen dat er een vraag tot raadpleging (latere verwerking) zonder historische, statistische of wetenschappelijke doeleinden gericht wordt aan de algemeen archivist. Die mogelijkheid wordt in acht genomen om desgevallend een vergunning te bekomen buiten de reeds voorziene gevallen, eerder dan een systematische weigering.

Om te antwoorden op het advies van de Raad van State (pagina 35) wordt het tweede lid van dit artikel opnieuw geformuleerd: er wordt verduidelijkt dat een verdere verwerking zonder historische, statistische of wetenschappelijke doeleinden geweigerd wordt behalve indien het doeleinde wettelijk is en de raadpleging geen afbreuk kan doen aan de belangen bedoeld in het eerste lid. Zo moet het duidelijk zijn dat er geen sprake is van het toelaten van een doeleinde – deze dient op zich en voorafgaand wettelijk te zijn – maar wel een raadpleging van gegevens in bepaalde gevallen. Aangezien de criteria vastliggen betreft het geenzins een discretionaire bevoegdheid. De modaliteiten zijn deze die zijn vastgelegd in huidig hoofdstuk en, desgevallend, in andere wetten (bijvoorbeeld de wet van 11 december 1998).

Uiteraard is deze toelating niet noodzakelijk voor de eigen raadplegingsnoden van de Algemene Rijksarchivaris na overdracht van de archieven van de inlichtingen- en veiligheidsdiensten naar het Algemeen Rijksarchief zoals bepaald in artikel 21/1 van de wet van 30 november 1998.

Les données du personnel des services de renseignement sont protégées pour éviter que des membres desdits services ne subissent des pressions, voire des menaces car leur identité et qualité sont dévoilées. Par conséquent, il convient de préciser que la protection des données de leur personnel par les services de renseignement fait partie de leurs missions. Il en va de même des sources et des tiers qui prêtent leur concours à un service de renseignement. Le service concerné a d'ailleurs l'obligation de protéger leurs données (art. 13, al. 3 et 13/4, al. 2 de la loi du 30 novembre 1998).

L'autorisation de consulter doit émaner du service de renseignement concerné, même si la donnée n'est pas entre ses mains, car c'est lui qui est le plus à même d'évaluer si la consultation est susceptible de porter atteinte à un des intérêts à protéger.

A cet égard, lorsque les données à caractère personnel des services de renseignement et de sécurité sont transférées aux Archives générales du Royaume, il se peut qu'une demande de consultation (traitement ultérieur) sans finalités historiques, statistiques ou scientifiques soit présentée à l'archiviste général. Cette éventualité est prise en considération pour permettre d'obtenir, le cas échéant, une autorisation en dehors des cas déjà prévus, plutôt qu'un refus systématique.

Pour répondre à l'avis du Conseil d'État, en page 35, l'alinéa 2 de cet article est reformulé: il est précisé qu'un traitement ultérieur sans finalités historiques, statistiques ou scientifiques est refusé sauf si la finalité est légitime et que la consultation n'est pas susceptible de porter aux intérêts à protéger qui sont visés à l'alinéa premier. Ainsi, il est clair qu'il n'est pas question d'autoriser une finalité – celle-ci devant en elle-même et au préalable être légitime – mais bien une consultation de données dans certains cas. Les critères étant déterminés, il ne s'agit pas d'un pouvoir discrétionnaire. Les modalités sont celles fixées dans le présent chapitre et, le cas échéant, dans d'autres lois (par exemple la loi du 11 décembre 1998).

Bien entendu, cette autorisation n'est pas nécessaire pour les besoins propres de consultation de l'Archiviste général du Royaume, après le transfert des archives des services de renseignement et de sécurité aux Archives générales du Royaume comme précisé dans l'article 21/1 de la loi de 30 novembre 1998.

Art. 100

Om de aandacht van de gebruiker te vestigen op het bijzondere regime toepasselijk op de verdere verwerking van het gegeven, vereist dit artikel dat dit gegeven gemarkeerd wordt met de vermelding “Bescherming van persoonsgegevens – artikelen 99 tot 104 van de wet van xx/xx/2018” .

Art. 101

Omwille van evidente redenen voor de bescherming van het privéleven, moeten de gegevens anoniem worden gemaakt. Indien dit het niet mogelijk maakt om het doel van de verdere verwerking te bereiken, kan de betrokken inlichtingendienst pseudonimisering toestaan.

De filosofie van dit artikel beantwoord aan wat is voorzien in hoofdstuk II van het Koninklijk Besluit van 13 februari 2001 betreffende de uitvoering van de wet van 8 december 1992. De term pseudonymisering werd toegevoegd als gevolg van de nieuwe Europese reglementering. Indien de anonimisering of de pseudonimisering de identificatie niet onmogelijk maakt, laat de inlichtingendienst slecht een consultatie toe indien er geen disproportionele weerslag is op het privéleven. In dezelfde zin, indien de latere verwerking van gepseudonimiseerde gegevens het niet toelaat om de historische, wetenschappelijke of statistische doeleinden te bereiken, kan de betrokken inlichtingendienst niet-gepseudonimiseerde gegevens toelaten indien er geen disproportionele weerslag is op het privéleven.

Art. 102

Omwille van redenen van bescherming van het privéleven en de belangen in de zin van artikel 99, kan geen enkele communicatie of publicatie van niet-geanonimiseerde en niet-gepseudonimiseerde gegevens plaatsvinden zonder toelating van de betrokken inlichtingen- en veiligheidsdienst.

Art. 103

Dit artikel legt de verwerkingsverantwoordelijke op een logbestand betreffende de verdere verwerking te bewaren. Deze verwerkingsverantwoordelijke zijn meer bepaald de inlichtingen- en veiligheidsdiensten, de Staatsarchieven, het DGHR van het Ministerie van Defensie, de Stafdienst Personeel en Organisatie van de FOD Justitie en elke andere entiteit die beschikt over gegevens van de inlichtingendiensten.

Art. 100

Pour attirer l’attention de l’utilisateur sur le régime particulier applicable à la donnée lors du traitement ultérieur, exige cet article que cette donnée soit marquée de la mention “Protection des données à caractère personnel – articles 99 à 104 de la loi du xx/xx/2018”.

Art. 101

Pour des raisons évidentes de protection du droit à la vie privée, les données doivent être rendues anonymes. Si cela ne permet pas d’atteindre le but du traitement ultérieur, le service de renseignement concerné peut autoriser la pseudonymisation.

La philosophie de cet l’article correspond à ce qui était prévu dans le chapitre II de l’arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992. Le terme pseudonymisation est ajouté suite à la nouvelle règlementation européenne. Si l’anonymisation ou la pseudonymisation ne rend pas l’identification impossible, le service de renseignement concerné n’autorise la consultation que si cela ne constitue pas une atteinte disproportionnée à la vie privée. Dans le même sens, si un traitement ultérieur de données pseudonymisées ne permet pas d’atteindre les fins historiques, statistiques ou scientifiques, le service concerné peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 102

Pour des raisons de protection du droit à la vie privée et des intérêts visés à l’article 99, toute communication et toute publication des données consultées non anonymisées et non pseudonymisées ne peuvent avoir lieu qu’avec l’autorisation du service de renseignement et de sécurité concerné.

Art. 103

Cet article impose la tenue d’un journal du traitement ultérieur par le responsable de traitement. Celui-ci est notamment les services de renseignement et de sécurité, les Archives de l’État, la DGHR du Ministère de la Défense, le service d’encadrement Personnel & Organisation du SPF Justice et toute autre entité disposant de données des services de renseignement.

Het begrip logbestand dat hier gebruikt wordt beoogt het bijhouden van een lijst concreet uitgevoerde verwerkingen in het kader van latere verwerkingen. Dit begrip differerntieert zich van dat in het register elders gebruikt in de kaderwet om elke verwarring te voorkomen.

Naast het logbestand dat wordt bijgehouden door de verantwoordelijke voor de verdere verwerking, moet de Algemene Rijksarchivaris een spoor bij van de raadplegingen uitgevoerd door elke verantwoordelijke voor de verdere verwerking houden.

Dit logbestand is logischerwijze geclassificeerd indien de latere verwerking betrekking heeft op geclassificeerde gegevens.

Dit logbestand helpt identificeren wie doet wat en moet vermelden:

1. de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van hun functionaris voor gegevensbescherming van de laatste;

2. de doeleinden van de verdere verwerking;

3. de gegevens die later verwerkt worden;

4. de eventuele voorwaarden voor de verdere verwerking vastgelegd door de betrokken inlichtingen- en veiligheidsdienst;

5. de eventuele ontvangers toegestaan door de betrokken inlichtingen- en veiligheidsdienst.

Dit logbestand laat toe de traceerbaarheid van de verdere verwerkingen en in het bijzonder de controle door de bevoegde toezichthoudende autoriteit te vergemakkelijken.

Art. 104

Dit artikel verduidelijkt dat elke persoon die gegevens verwerkt voor historische, wetenschappelijke of statistische doeleinden verantwoordelijk is voor deze verwerking. Dit houdt een verbod in om geanonimiseerde, of gepseudonimiseerde gegevens in persoonsgegevens om te omzetten. Dit verbod is overgenomen van het artikel 6 van het Koninklijk Besluit van 13 februari 2001 houdende uitvoering van de wet van 8 december 1992.

Le terme de journal, utilisé ici, vise la tenue d'une liste des traitements effectués concrètement et sur quelles données, dans le cadre des traitements ultérieurs. Ce terme se différencie de celui de registre utilisé ailleurs dans la loi-cadre pour éviter toute confusion.

A côté du journal tenu par le responsable du traitement ultérieur, l'Archiviste général du Royaume doit également garder une trace des consultations effectuées par chaque responsable du traitement ultérieur.

Ce journal est bien entendu classifié si le traitement ultérieur porte sur des données classifiées.

Ce journal permet d'identifier qui fait quoi et doit mentionner:

1. les coordonnées du responsable du traitement initial, du responsable ultérieur et du délégué à la protection des données de ce dernier;

2. les finalités du traitement ultérieur;

3. les données faisant l'objet du traitement ultérieur;

4. les éventuelles conditions du traitement ultérieur fixées par le service de renseignement et de sécurité concerné;

5. les éventuels destinataires autorisés par le service de renseignement et de sécurité concerné.

Ce journal permet de faciliter la traçabilité des traitements ultérieurs et notamment le contrôle par l'autorité de contrôle compétente.

Art. 104

Cet article précise que toute personne qui traite des données à des fins historiques, scientifiques ou statistiques est responsable dudit traitement. Elle a interdiction de convertir des données anonymes ou pseudonymisées en données à caractère personnel. Cette interdiction est reprise de l'article 6 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992.

ONDERTITEL 2

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR DE KRIJGSMACHT

Art. 105

Defensie is onderworpen aan het Verdrag van de Raad van Europa tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens op 28 januari 1981. Het Aanvullende Protocol bij het Verdrag (ETS nr. 181 van 8 november 2001) eist van de Staten die partij zijn bij het verdrag dat zij voorzien in toezichthoudende autoriteiten die volledig onafhankelijk optreden en heeft betrekking op het grensoverschrijdend verkeer van gegevens naar derde landen. Dat Verdrag 108 is dan ook van toepassing voor wat buiten het toepassingsgebied van de EU blijft zoals de verwerkingen door de inlichtingen en veiligheidsdiensten als onderdeel van hun wettelijke opdrachten maar ook de militaire operaties van Defensie. België heeft als partij bij het Verdrag 108 de verbintenis op zich genomen om in zijn intern recht de noodzakelijke maatregelen te nemen om uitvoering te geven aan de in het verdrag vervatte grondbeginselen.

Het oogmerk van dit artikel is om de verwerking van persoonsgegevens door de Krijgsmacht bij de aanwending en de paraatstelling met het oog op de aanwending te ontrekken aan de bepalingen van Titel 1. De begrippen “aanwending” en “paraatstelling” dienen begrepen te worden zoals bedoeld in de wet van 20 mei 1994 betreffende de perioden en de standen van de militairen van het reservekader alsook betreffende de aanwending en de paraatstelling van de Krijgsmacht.

Het advies van de Raad van State werd gevolgd om deze verwijzing in de wettekst op te nemen.

De inzet van de krijgsmacht is op basis van artikel 2 van de Verordening uitgesloten uit het materieel toepassingsgebied van de Verordening. Dergelijke mogelijkheid tot afwijking van het algemeen kader inzake gegevensbescherming was reeds in de richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, ingeschreven. Deze richtlijn werd met de wet van 11 december 1998 omgezet in nationaal recht en geïntegreerd in de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, echter zonder deze afwijking invulling te geven.

SOUS-TITRE 2

LA PROTECTION DES PERSONNES PHYSIQUES CONCERNANT LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL PAR LES FORCES ARMEES

Art. 105

La Défense est soumise à la Convention du Conseil de l’Europe pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel a été ouverte à la signature le 28 janvier 1981. Le Protocole additionnel à la Convention (STE n° 181 du 08/11/2001) exige des États Parties à la Convention qu’ils mettent en place des autorités de contrôle, agissant de manière totalement indépendante, et porte sur les flux transfrontières de données vers des pays tiers. Cette Convention 108 est donc applicable pour ce qui reste hors champ d’application de l’UE comme par exemple les traitements effectués par les services de renseignements et de sécurité dans le cadre de leurs missions légales. En tant que partie à la Convention 108, la Belgique a pris l’engagement de prendre les mesures nécessaires au sein du droit interne afin de donner exécution aux principes fondamentaux repris dans la convention.

L’objet de cet article est de soustraire le traitement des données à caractère personnel par les forces armées lors de la mise en œuvre et de la mise en condition aux fins de la mise en œuvre du titre 1er. Les termes “mise en œuvre” et “mise en condition” sont à interpréter comme visés par la loi du 20 mai 1994 relative aux périodes et aux positions des militaires du cadre de réserve, ainsi qu’à la mise en œuvre et à la mise en condition des Forces armées.

L’avis du Conseil d’État a été suivi afin d’inclure cette référence dans le texte de la loi.

Sur base de l’article 2 du Règlement, l’engagement des forces armées est exclu du champ d’application matériel du Règlement. De telles possibilités de dérogation du cadre général sur la protection des données étaient déjà inscrites dans la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relatif à la protection des personnes physiques en matière du traitement des données à caractère personnel et relatif à la libre circulation de ces données. Cette directive a été transposée par la loi du 11 décembre 1998 en droit national et intégrée dans la loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel, mais sans concrétiser cette dérogation.

Tijdens een operationele inzet / aanwending zijn de verwerking van (ook “gevoelige”) persoonsgegevens en de vereiste van discretie absoluut noodzakelijke voorwaarden. Met het oog op de goede afloop van een missie moet de commandant immers het geheel van gegevens, zowel persoonsgegevens als andere (situationele, menselijke, geografische, …) verwerken die hem een inzicht moeten verschaffen in de precieze omstandigheden op het strijdtoneel met betrekking tot zijn eenheid alsook de gebieden waar hij effectief operaties voert en die waar hij er eventueel nog zal moeten voeren, om hem in staat te stellen om op het terrein zijn manschappen en hun posities te beschermen evenals de hem toevertrouwde opdrachten en zo de te ondernemen acties tot een goed einde te kunnen brengen.

Vandaag zijn de soorten inzet en de wijze waarop operaties worden gevoerd fundamenteel veranderd. Rekening houdend met de diversiteit en de onberekenbaarheid van de nieuwe dreigingen enerzijds en de technologische vooruitgang anderzijds, worden persoonsgegevens nodig voor de bevelvoering als voor de eenheden op het terrein een steeds belangrijker onderdeel van de noodzakelijke informatie. Eenmaal in onderlinge samenhang te zijn geëvalueerd, nagetrokken en geanalyseerd, stelt deze informatie de commandant in staat om de risico’s in te schatten die zijn eenheid loopt in het kader van de missie en dienovereenkomstig actiemiddelen in te zetten, in het bijzonder tijdens de voorbereiding en het voeren van gevechtsoperaties.

De persoonsgegevens vormen daarbij een onderdeel van de te verwerken gegevens en krijgen ten gevolge de aard van de activiteiten van de krijgsmacht een gevoelig karakter waardoor de vereisten van discretie en geheimhouding absolute randvoorwaarden vormen niet alleen voor het welslagen van de missie maar ook voor de veiligheid van zowel het eigen militair personeel als het militair personeel waarmee de Belgische krijgsmacht samen optreedt als de lokale bevolking.

De wet voorziet daarom in de toepassing van de regels voor het GBVB-gebied, met uitzondering van de aanwending van de krijgsmacht, en de paraatstelling met het oog op de aanwending van de krijgsmacht.

Voornoemde uitzondering ingeval van aanwending en paraatstelling met het oog op de aanwending ontslaat België niet aan de verplichtingen die ontspruiten uit het Verdrag 108. In het bijzonder moet het rechtsregime opgelegd worden dat van toepassing is voor die militaire operaties.

In geval van aanwending van de krijgsmacht of paraatstelling met het oog op aanwending van de krijgsmacht dient de krijgsmacht passende operationele

Lors de l’engagement / la mise en œuvre opérationnelle, le traitement de données à caractère personnel (en ce compris les données “sensibles”) et l’exigence de discrétion sont des conditions absolument nécessaires. En vue d’un bon déroulement d’une mission, le commandant doit d’ailleurs traiter toutes les données, aussi bien les données à caractère personnel que les autres (situationnelles, humaines, géographiques, …) qui devraient lui donner une vue sur les circonstances précises sur le champ de bataille concernant l’unité et les régions où il mène effectivement des opérations et celles où il devrait encore en mener, pour lui permettre de protéger ces troupes sur le terrain et leur positions, ainsi que les missions qui lui ont été confiées et de cette manière mener à bien les actions à entreprendre.

Actuellement, les types d’engagement et la manière dont les opérations sont menées ont changé fondamentalement. En tenant compte de la diversité et du caractère imprévu des nouvelles menaces d’un côté et le progrès technologique d’un autre côté, les données à caractère personnel nécessaires pour le commandement ainsi que pour les unités sur le terrain deviennent de plus en plus partie intégrante de l’information nécessaire. Une fois évaluée, contrôlée et analysée conjointement, cette information permet au commandant d’évaluer les risques que son unité court dans le cadre de la mission et des moyens d’action en conséquence, en particulier en préparant et en menant des opérations de combat.

Les données à caractère personnel forment une partie des données à traiter et reçoivent, suite à la nature des activités des forces armées, un caractère sensible, ce qui fait que les exigences de discrétion et de confidentialité deviennent des conditions absolument nécessaires non seulement pour le bon déroulement de la mission, mais aussi tant pour la sécurité du personnel militaire, que pour le personnel militaire avec lequel les forces armées belges opèrent et la population locale.

La loi prévoit donc l’application du Règlement pour le domaine PESC à l’exception de la mise en œuvre des forces armées et de la mise en condition des forces armées en vue de leur mise en œuvre.

L’exception mentionnée en cas de la mise en œuvre et la mise en condition aux fins de la mise en œuvre, ne libère pas la Belgique des obligations qui émergent de la Convention 108. Il convient en particulier que le régime juridique doit être imposé qui est d’application pour ces opérations militaires.

En cas de la mise en œuvre ou la mise en condition en vue de la mise en œuvre des forces armées, les forces armées devraient prendre des mesures appropriées

maatregelen te treffen tot bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens en dit in overeenstemming met het voor de aanwending toepasselijke mandaat.

Daarbij dienen de volgende beginselen in ieder geval in acht te worden genomen:

— Persoonsgegevens van alle aard mogen worden verwerkt voor zover ze noodzakelijk zijn voor de uitoefening van hun opdrachten;

— De verwerking moet verband houden met de aanwending en de paraatstelling met het oog op de aanwending van de krijgsmacht;

— De bewaring is begrensd tot wat noodzakelijk is;

— Eenheden in operaties mogen de persoonsgegevens doorgeven naar hun coalitiepartners in de mate dat dit noodzakelijk is voor operationele redenen;

— De aard van militaire operaties noopt tot het beperken van een aantal rechten doch slechts die beperking een noodzakelijke en evenredige maatregel vormt voor de aanwending van de krijgsmacht of paraatstelling met het oog op aanwending van de krijgsmacht;

— Voornoemd regime wordt onderworpen aan het toezicht van de bevoegde toezichtshoudende autoriteit. Het spreekt vanzelf dat dit toezicht niet kan uitgevoerd ter plaatse noch in de operatiezone noch in iedere zone die verbonden is met de aanwending en de paraatstelling met het oog op aanwending. Naast de veiligheidsrisico's van dergelijk toezicht, zou dit een impact hebben op het internationaal humanitair rechtelijk statuut van deze personen.

ONDERTITEL 3

DE BESCHERMING VAN NATUURLIJKE PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS IN HET KADER VAN DE WET VAN 11 DECEMBER 1998 BETREFFENDE DE CLASSIFICATIE EN DE VEILIGHEIDSMACHTIGINGEN, VEILIGHEIDSATTESTEN EN VEILIGHEIDSADVIEZEN

ALGEMEEN DEEL

Deze ondertitel handelt over verwerkingen in het kader van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen,

pour la protection des personnes physiques relative à la protection des données à caractère personnel et ceci conformément au mandat qui est d'application.

Pour cela, il faut respecter en tout cas les principes suivants:

— Des données à caractère personnel de toute nature sont traitées pour autant qu'elles sont nécessaires pour l'exécution de leur missions;

— Le traitement doit se rapporter à la mise en œuvre et à la mise en condition en vue de la mise en œuvre des forces armées;

— La conservation est limitée à ce qui est nécessaire;

— Les unités en opération peuvent transférer les données à caractère personnel à leurs partenaires dans la mesure où cela est nécessaire pour des raisons opérationnelles;

— La nature des opérations militaires nécessite la limitation de certains droits, mais seulement si cette limitation a un caractère nécessaire et proportionné en vue de l'utilisation des forces armées;

— Le régime précité est soumis à la supervision de l'autorité de contrôle compétente. Il est évident que cette supervision ne peut pas être exécutée sur le terrain, ni dans la zone d'opération ni dans chaque zone qui est lié avec la mise en œuvre et à la mise en condition en vue de la mise en œuvre. Outre les risques en matière de sécurité d'un tel suivi, ceci aurait un impact sur le statut international humanitaire de droit de ces personnes.

SOUS-TITRE 3

DE LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL DANS LE CADRE DE LA LOI DU 11 DECEMBRE 1998 RELATIVE À LA CLASSIFICATION ET AUX HABILITATIONS, ATTESTATIONS ET AVIS DE SÉCURITÉ

PARTIE GENERALE

Ce sous-titre traite du traitement des données dans le cadre de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis

veiligheidsattesten en veiligheidsadviezen (hierna "de wet van 11 december 1998"). De verwerkingen die beoogt worden in deze ondertitel dienen begrepen te worden als de verwerking van persoonsgegevens in het kader van veiligheidsmachtigingen en veiligheidsverificaties, uitgevoerd door de veiligheidsoverheid (hierna "NVO") bedoeld in artikel 15, eerste lid, de veiligheidsofficieren bedoeld in artikel 13, 1°, en de overheden bedoeld in artikel 15, tweede lid en 22*ter* van de wet van 11 december 1998. Dit toepassingsgebied wordt gedefinieerd in het artikel 107. De overheden die het veiligheidsonderzoek bedoeld in artikel 18 en de veiligheidsverificatie bedoeld in artikel 22*sexies* van de wet van 11 december uitvoeren verwerken persoonsgegevens in het kader van deze activiteiten onder deze titel omdat zij optreden als collegiale overheid van de NVO.

Deze ondertitel is ook van toepassing op elke verwerking van persoonsgegevens door het beroepsorgaan in het kader van de beroepsprocedures bedoeld in de wet van 11 december 1998 tot oprichting van het beroepsorgaan (hierna "wet van 11 december 1998 op het beroepsorgaan").

Zoals bepaald in artikel 2 van de Verordening, is deze niet van toepassing op de verwerking van persoonsgegevens in het kader van een activiteit die niet binnen het toepassingsgebied van het Europees Recht valt.

Gezien de verwerkingen in het kader van artikel 107 niet tot de bevoegdheden van de Unie behoren (cf. art. 4 VEU), zijn de bepalingen uit de Verordening niet op haar van toepassing.

De verwerking van persoonsgegevens in het kader van artikel 107 werd geregeld door de WVP. Deze wet voorzag in een toepassing van algemene principes en enkele uitzonderingen die voortvloeiden uit de specifieke opdrachten in de wet van 11 december 1998.

Gelet op de opheffing van de WVP door onderhavige wet, wordt een nieuw regime ingevoerd door deze ondertitel. Deze titel bepaalt aldus de toepasselijke regels voor elke verwerking van persoonsgegevens in het kader van artikel 107 en hun verwerkers in het belang van de uitoefening van de opdrachten van voornoemde overheden, organen en personen.

De titel volgt vier richtsnoeren:

1. Overname van de bepalingen van de WVP die van toepassing zijn op de NVO, de veiligheidsofficieren bedoeld in artikel 13, 1°, en de overheden bedoeld in artikel 15, tweede lid en 22*ter* van de wet van 11 december 1998;

de sécurité (ci-après "la loi du 11 décembre 1998"). Le traitement des données qui est visé dans ce sous-titre doit être compris comme le traitement des données à caractère personnel dans le cadre des habilitations et vérifications de sécurité effectuées par l'autorité de sécurité (ci-après dénommée "ANS") visée à l'article 15, paragraphe 1er, les officiers de sécurité visés à l'article 13, 1°, et les autorités visées à l'article 15, deuxième alinéa et 22*ter* de la loi du 11 décembre 1998. Ce champ d'application est défini à l'article 107. Les autorités effectuant l'enquête de sécurité visée à l'article 18 et la vérification de sécurité visée à l'article 22*sexies* de la loi du 11 décembre 1998, traitent des données personnelles dans le cadre de leurs activités relevant de ce titre car ils agissent comme autorité collégiale de l'ANS.

Ce sous-titre s'applique également à tout traitement de données à caractère personnel par l'organe de recours dans le cadre de la procédure d'appel prévue par la loi du 11 décembre 1998 portant création d'un organe de recours (ci-après "Loi du 11 décembre 1998 sur l'organe de recours").

Comme le précise l'article 2 du Règlement, celui-ci ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union européenne.

Vu que les traitements dans le cadre de l'article 107 n'entrant pas dans les compétences de l'Union (cf. art. 4 TUE), les dispositions du Règlement ne leur sont pas applicables.

Le traitement des données à caractère personnel dans le cadre de l'article 107 étaient réglementés par la LVP. Cette loi prévoyait une application des principes généraux et quelques exceptions en raison des spécificités des missions dans la loi du 11 décembre 1998.

Vu l'abrogation de la LVP par la présente loi, un nouveau régime est prévu dans le présent sous-titre. Celui-ci détermine donc de nouvelles règles applicables à tout traitement de données à caractère personnel dans le cadre de l'article 107 et leurs sous-traitants dans l'intérêt de l'exercice des missions desdits autorités, organes et personnes.

Le titre suit quatre lignes directrices:

1. Reprise des mêmes dispositions de la LVP applicables à l'ANS, aux officiers de sécurité visés à l'article 13, 1°, et les autorités visées à l'article 15, second alinéa en 22*ter* de la loi du 11 décembre 1998;

2. Naleving van de Conventie voor de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa van 28 januari 1981 (het zogeheten Verdrag 108);

3. Bekrachtiging van bepaalde verplichtingen van de NVO als verwerkingsverantwoordelijke;

4. Specifieke bepalingen voor het gebruik van persoonsgegevens van de NVO voor historische, wetenschappelijke of statistische doeleinden.

I. — STATUS QUO IN VERGELIJKING MET DE WET VAN 8 DECEMBER 1992

Onder de WVP waren de verwerkingen in het kader van artikel 107 onderworpen aan de algemene principes voor de verwerking van persoonsgegevens. De wetgever heeft echter via de *wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens* de verwerkers in het kader van artikel 109 uitzonderingen voor de verwerking van persoonsgegevens toegekend (DOC, Kamer, 1997-1998, n°1566, p. 24).

De wetgever besliste hiermee de NVO dezelfde uitzonderingen toe te kennen als aan de inlichtingendiensten: *"Ten slotte wordt een speciale regeling getroffen met betrekking tot de verwerking beheerd door het Bestuur Veiligheid van de Staat van het Ministerie van Justitie en door de Algemene dienst Inlichting en Veiligheid van het Ministerie van Landsverdediging, ofschoon die niet volledig uitgesloten zijn van de werkingssfeer van de wet. De aard zelf van de taken die zij volbrengen, rechtvaardigt dat die autoriteiten deze taken met de nodige geheimhouding verder zouden kunnen uitvoeren. De belangrijkheid van de uitzonderingen welke die diensten genieten, is overigens met de nodige zorg afgewogen, en alleen die bepalingen welke volstrekt onverenigbaar zijn met hun taken, zijn eruit geweerd. Evenwel valt op te merken dat de betrokken personen toch nog over een aantal controlemiddelen ter zake zullen beschikken omdat zij voor de geregistreerde gegevens een onrechtstreeks recht van toegang genieten dat wordt uitgeoefend door tussenkomst van de Commissie voor de bescherming van de persoonlijke levenssfeer."* (DOC, Kamer, 1990-1991, n° 1610, pp. 7 en 8).

Deze ondertitel van onderhavige wet maakt dezelfde principes toepasselijk op de verwerkingen in het kader

2. Respect de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe du 28 janvier 1981 (dite Convention 108);

3. Renforcement de certaines obligations de l'ANS en tant que responsables du traitement;

4. Dispositions particulières pour l'utilisation des données à caractère personnel de l'ANS à des fins historiques, scientifiques ou statistiques.

I. — STATU QUO PAR RAPPORT À LA LOI DU 8 DÉCEMBRE 1992

En vertu de la LVP, le traitement prévu par l'article 107 était soumis aux principes généraux du traitement des données à caractère personnel. Le législateur a cependant, par la *loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relatif à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, les sous-traitants ont été accordé des dérogations pour le traitement des données à caractère personnel en vertu de l'article 109 (DOC, Chambre, 1997-1998, n° 1566, page 24).

Le législateur a décidé d'accorder à l'ANS les mêmes exemptions qu'aux services de renseignements: "*Enfin, les traitements gérés par la Sûreté de l'État du Ministère de la Justice et le Service général du Renseignement et de la Sécurité du Ministère de la Défense nationale, sans être complètement exclus du champ d'application de la loi seront soumis à un sort spécifique. La nature même des tâches qu'ils accomplissent justifie qu'ils puissent continuer à l'accomplir avec toute la discrétion nécessaire. L'importance des exceptions dont bénéficieront ces services a d'ailleurs été pesée avec soin et seules les dispositions absolument incompatibles avec leurs missions ont été écartées. Il est à noter cependant que les personnes concernées ne seront pas dépourvues de tout moyen de contrôle à leur égard, puisqu'elles pourront bénéficier d'un "droit d'accès indirect"* aux données enregistrées qui s'exercera auprès de la Commission de la protection de la vie privée." (Doc, La Chambre, 1990-1991, n° 1610, pp. 7 et 8).

Le présent sous-titre de la présente loi rend les mêmes principes applicables aux traitements dans le

van artikel 107 en voorziet dezelfde uitzonderingen om dezelfde redenen van discretie.

II. — **NALEVING VAN DE PRINCIPES VAN HET VERDRAG 108**

De verwerking in het kader van artikel 107 is onderworpen aan de principes van het Verdrag 108.

Deze ondertitel houdt de rechten en verplichtingen in vastgelegd door het Verdrag 108 en voorziet geen juridische uitzonderingen dan wanneer toegelaten door het Verdrag zelf.

III. — **BEKRACHTIGING VAN BEPAALDE VERPLICHTINGEN**

In vergelijking met de verplichtingen vastgelegd door de WVP, gaat deze ondertitel verder en voorziet deze in nieuwe verplichtingen. Aldus wordt gesteld dat de verwerkers in het kader van artikel 107 registers moet bijhouden van hun verwerkingsactiviteiten.

De verwerkers in het kader van artikel 107 hebben eveneens de verplichting om melding te maken aan de bevoegde toezichthoudende autoriteit van elke inbreuk op de beveiliging van persoonsgegevens die een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt.

De ondertitel legt ook op een functionaris voor gegevensbescherming aan te duiden voor de verwerkingen in het kader van artikel 107. Deze verplichting bestond niet in de WVP. De rol van deze functionaris voor gegevensbescherming wordt ingevoerd via deze ondertitel.

IV. — **VERWERKING VOOR HISTORISCHE, WETENSCHAPPELIJKE EN STATISTISCHE DOELEINDEN**

Het raadplegen van persoonsgegevens in het kader van de verwerkingen gebeurd onder deze ondertitel voor historische, wetenschappelijke en statistische doeleinden wordt gereglementeerd. Deze raadpleging is slechts mogelijk indien zij geen weerslag heeft op de opdrachten in het kader van de wet van 11 december 1998 en indien zij geen gevaar vormt voor een bron of een derde die zijn medewerking in het kader van de wet van 11 december 1998 verleent, en indien zij geen weerslag heeft op een lopend opsporings- of gerechtelijk onderzoek of op de relaties die België onderhoudt met andere Staten of internationale organisaties.

cadre de l'article 107 et prévoit les mêmes exceptions pour les mêmes raisons de discrétion.

II. — **RESPECT DES PRINCIPES DE LA CONVENTION 108**

Le traitement dans le cadre de l'article 107 est soumis aux principes de la Convention 108.

Le présent sous-titre contient tous les droits et obligations fixés dans la Convention 108 et n'y prévoit d'exceptions légales expresses que lorsque la Convention elle-même les autorise.

III. — **RENFORCEMENT DE CERTAINES OBLIGATIONS**

Par rapport aux obligations fixées par la LVP, le présent sous-titre va plus loin et prévoit de nouvelles obligations. Ainsi, il dispose que les sous-traitants dans le cadre de l'article 107 doivent tenir des registres de leurs activités de traitement.

Les sous-traitants dans le cadre de l'article 107 ont également l'obligation de notifier à l'autorité de contrôle compétente toute brèche de sécurité portant sur des données à caractère personnel et représentant un risque pour les droits et libertés des personnes physique.

Le sous-titre précise également qu'un délégué à la protection des données devrait être désigné pour le traitement dans le cadre de l'article 107. Cette obligation n'existait pas dans la LVP. Le rôle de ce délégué à la protection des données est introduit via le présent sous-titre.

IV. — **TRAITEMENT À DES FINS HISTORIQUES, SCIENTIFIQUES OU STATISTIQUES**

La consultation des données personnelles dans le cadre du traitement effectué sous ce sous-titre à des fins historiques, scientifiques et statistiques est réglementée. Cette consultation n'est possible que si elle n'affecte pas les missions prévues par la loi du 11 décembre 1998 et si elle ne met pas en danger une source ou un tiers qui collabore dans le cadre de la loi du 11 décembre 1998, et si cela n'a aucune incidence sur une enquête en cours ou une enquête judiciaire ou sur les relations que la Belgique entretient avec d'autres États ou organisations internationales.

De verwerking van geclassificeerde documenten dient natuurlijk ook de hierop betrekking hebbende bepalingen van de wet van 11 december 1998 te respecteren.

Deze specifieke reglementering is noodzakelijk gezien, een aanvraag tot verwerking van gegevens komende van de NVO, de veiligheidsofficieren bedoeld in artikel 13, 1°, en de overheden bedoeld in artikel 15, tweede lid en 22*ter* van de wet van 11 december 1998 en het beroepsorgaan bedoeld in de wet van 11 december 1998 op het beroepsorgaan voor historische, wetenschappelijke of statistische doeleinden steeds betrekking zal hebben op documenten en dragers waar de persoonsgegevens van de betrokkene een prominente rol spelen. Het valt te vermijden dat gegevens waar de identiteit en andere persoonsgegevens over de betrokkene niet te beschermen zijn door anonimiseren in dit kader gecommuniceerd worden.

HOOFDSTUK I

Definities

Art. 106

De eerste paragraaf verwijst naar sommige definities van titel 2.

Paragraaf 2 voegt hieraan enkele definities toe die eigen zijn aan deze ondertitel en die enkel relevant zijn voor verwerking van persoonsgegevens in het kader van de wet van 11 december 1998.

Naar aanleiding van de opmerking geformuleerd in punten 238 en 242 door de Privacycommissie in haar advies nr. 33/2018 werd het punt 7° ingevoegd dat de toezichthoudende autoriteit uitdrukkelijk benoemt.

HOOFDSTUK II

Toepassingsgebied

Art. 107

De verwerking van persoonsgegevens in het kader van de wet van 11, december 1998 wordt momenteel geregeld door de wet van 8 december 1992. Deze wet sluit de toepassing van enkele artikelen uit voor deze diensten (onder andere enkele verplichtingen en rechten van betrokken personen). Gezien het toepassingsveld van de wet van 11 december 1998 uitgesloten is van de toepassing van deVerordening, is een aparte regeling nodig voor de gegevensverwerking in het kader van de

Le traitement des documents classifiés doit bien entendu également respecter les dispositions de la loi du 11 décembre 1998.

Cette réglementation spécifique est nécessaire car une demande de consultation des données de l'ANS, des officiers de sécurité visés à l'article 13, 1°, des autorités visées à l'article 15, deuxième alinéa et 22*ter* de la loi du 11 décembre 1998 et de l'organe de recours visé dans la loi du 11 décembre 1998 relatif à l'organe de recours à des fins historiques, scientifiques ou statistiques se rapportera toujours aux documents et médias dans lesquels les données à caractère personnel de la personne concernée jouent un rôle prépondérant. Il faut éviter que des données où l'identité et d'autres informations personnelles sur la personne concernée non protégées par anonymisation soient communiquées dans ce contexte.

CHAPITRE I^ER

Définitions

Art. 106

Le premier paragraphe renvoie à certaines définitions du titre 2.

Le paragraphe 2 ajoute quelques définitions qui sont propres au présent sous-titre et qui ne sont pertinentes que pour le traitement des données personnelles dans le cadre de la loi du 11 décembre 1998.

Suite à la remarque formulée dans les points 238 et 242 par la Commission vie privée dans son avis n°33/2018, le point 7°, qui designe explicitement l'autorité de contrôle, a été inséré.

CHAPITRE II

Champ d'application

Art. 107

Le traitement de données à caractère personnel dans le cadre de la loi du 11 décembre 1998 est actuellement réglé par la loi du 8 décembre 1992. Cette loi exclut l'application de certains articles à ces services (notamment de certains droits et obligations des personnes concernées). Vu que la loi du 11 décembre 1998 est exclue du champ d'application du Règlement, une règlementation séparée est nécessaire pour le traitement des données dans le cadre de la loi du 11 décembre 1998.

wet van 11 december 1998. Dit regime is geïnspireerd op de huidige WVP en beantwoordt aan de standaarden van het Verdrag 108.

In punt 239 stelt de Privacycommissie in haar advies nr. 33/2018 vast dat de overheden, organen en personen bedoeld in dit artikel krachtens artikel 110 gemachtigd worden om bijzondere categorieën van persoonsgegevens te verwerken, zonder te onderzoeken in welke mate dit noodzakelijk en proportioneel is, en dat deze noodzaak en proportionaliteit niet meer in de sectorale wetgeving onderzocht dient te worden. Het dient bendrukt te worden dat zij deze verwerking enkel kunnen in het kader van veiligheidsmachtigingen en veiligheidsverificaties. Deze worden beheerst door de wet van 11 december 1998 en haar uitvoeringsbesluiten. Allereerst voorziet de wet van 11 december 1998 reeds in een beperking van het toepassingsveld. Alvorens een veiligheidsmachtiging kan worden aangevraagd dient aangetoond te worden dat er een noodzaak is tot kennisname van geclassificeerde informatie. Dit hangt dus niet af van sectorale wetgeving, maar wel van het feit of er al dan niet een mogelijk contact met geclassificeerde informatie zal plaatsvinden. Dit is een duidelijk criterium dat geldt over alle sectoren heen. Wat betreft de veiligheidsadviezen dient er een aanvraagdossier te worden voorgelegd alvorens veiligheidsadviezen kunnen worden opgelegd voor toegang tot bepaalde zones of functies. Deze verplichting tot veiligheidsverificatie wordt steeds geformaliseerd in de vorm van een administratieve beslissing, sectorale regelgeving…

Veiligheidsmachtigingen en veiligheidsverificaties kaderen dus steeds in de nationale veiligheid en de openbare orde en worden pas toegestaan/toegepast na een grondige afweging.

Daarnaast dient benadrukt te worden dat de betrokkene wiens persoonsgegevens verwerkt worden in dit kader er steeds van op de hoogte wordt gebracht. Meer nog, deze verwerking kan niet plaatsvinden zonder dat de betrokkene hiervoor zijn toestemming heeft verleend.

De communicatie en verwerking in het kader van de veiligheidsmachtigingen en veiligheidsverificaties verloopt steeds via veiligheidsofficieren. Dit zijn steeds personen die over een veiligheidsmachtiging beschikken en aan een strikte geheimhouding gebonden zijn.

Het is noodzakelijk voor het functioneren van dit systeem dat de veiligheidsofficier van elke overheid, orgaan of persoon bedoeld in artikel 110 kennis kan nemen, van deze ruime categorieën van persoonsgegevens (en dus persoonsgegevens verwerkt). Een voorbeeld hiervan is: de veiligheidsofficier van een rechtspersoon signaleert aan de NVO dat één van de werknemers

Ce régime est inspiré de la LVP et répond aux normes de la Convention 108.

Au point 239 la Commission vie privée, dans son avis n° 33/2018 du 11 avril 2018, constate que les autorités, organes et personnes visés à cet article sont autorités en vertu de l'article 110 à traiter des catégories particulières de données à caractère personnel, sans vérifier dans quel mésure cela est nécessaire ou proportionnel, et que cette nécessité et proportionalité ne doit plus être examiné dans la législation sectorielle. Il convient de souligner qu'ils ne peuvent effectuer ce traitement que dans le cadre des habilitations de sécurité et des vérifications de sécurité. Celles-ci sont régies par la loi du 11 décembre 1998 et ses arrêtés d'exécution. D'abord, la loi prévoit déjà une limitation du champ d'apllication. Avant qu'une habilitation de sécurité puis être demandée il doit être démontré qu'il y a une néccesité de prendre connaissance des informations classifiées. Ceci ne dépend donc pas de la législation sectorielle, mais du fait ou non qu'il y aura lieu un contact possible avec des informations classifiées. Ceci est un critère précis qui s'applique de tous les secteurs. En ce qui concerne les avis de sécurité il doit être soumis un dossier de demande avant que les avis de sécurité puissent être imposés pour l'accès à certains zones ou fonctions. Cette obligation de vérification de sécurité est toujours formulée sous forme d'une décision administrative, de la législation sectorielle…

Des habilitations de sécurité et des vérifications de sécurité s'inscrivent toujours dans la sécurité nationale et l'orde public et ne sont autorisés/appliqués que après une évaluation approfondie.

En outre il convient de souligner que la personne concernée dont les données à caractère personnel sont traitées dans ce cadre en est toujours avertie. En plus, ce traitement ne peut pas avoir lieu sans que la personne concernée ait donné son consentement.

La communication et le traitement dans le cadre des habilitations de sécurité et des vérifications de sécurité passent toujours pas des officiers de sécurité. Ceux-ci sont des personnes qui disposent d'une habilitation de sécurité et qui sont tenus à une confidentialité stricte.

Il est indispensable pour la fonctionnement du système que les officiers de sécurité de chaque autorité, organe ou personne visé à l'article 110 puissent prendre connaissance de cette large catégorie de données à caractère personnel, (et donc puissent traiter des données à caractère personnel). Un exemple : l'officier de sécurité d'une personne morale signale à l'ANS qu'un

tekenen van radicalisme vertoont. Dit is een verplichting die aan de veiligheidsofficier wordt opgelegd in de wet van 11 december 1998, waardoor hij verplicht wordt om in deze verwerking ook rekening te houden met persoonsgegevens waaruit de elementen bedoeld in artikel 110 blijken.

In de communicatieketen voorzien voor veiligheidsmachtigingen of veiligheidsverificaties is het daarom noodzakelijk dat, in het belang van de nationale veiligheid en de openbare orde, elke overheid, orgaan of persoon bedoeld in artikel 107 de gegevens bedoeld in artikel 110 mag verwerken.

Het eerste lid verduidelijkt het toepassingsgebied van deze ondertitel. Het somt de overheden en entiteiten op, die in de behandeling met betrekking tot de veiligheidsmachtigingen en veiligheidsattesten en -adviezen, zoals bedoeld in de wet van 11 december 1998, persoonsgegevens conform deze titel moeten verwerken.

Het tweede lid bepaalt dat de verwerking van persoonsgegevens door het beroepsorgaan, in het kader van de beroepsprocedures bedoeld in de wet van 11 december 1998 tot oprichting van het beroepsorgaan, ook conform deze titel moeten gebeuren. De beroepsprocedures die verband houden met de veiligheidsmachtigingen en veiligheidsverificaties hernemen de persoonsgegevens die door het vorige lid onder deze titel geplaatst worden. Het is dan ook logisch dat op deze persoonsgegevens hetzelfde regime wordt toegepast.

Het derde lid bepaalt dat de andere titels van deze wet niet van toepassing zijn op de verwerkingen in het kader van de wet van 11 december 1998. Deze ondertitel omvat het geheel van bepalingen dat van toepassing is op de verwerking van persoonsgegevens bedoeld in het eerste en tweede lid. De toepassing van andere titels van deze wet met uitzondering van de straf- en slotbepalingen is dus niet te rechtvaardigen.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 108

Dit artikel beschrijft in welke gevallen een verwerking van persoonsgegevens rechtmatig is. Deze gevallen zijn deze zoals ze vervat waren in artikel 5 WVP.

De behandeling van persoonsgegevens is steeds mogelijk met de instemming van de betrokken persoon, op voorwaarde dat de toestemming vrij en geïnformeerd is zoals de rechtspraak bepaalt. Deze instemming wordt

employé manifeste des signes de radicalisme. Ceci est une obligation qui est mis sur l'officier de sécurité par la loi du 11 décembre 1998, ce qui fait qu'il est obligé dans ce traitement d'aussi tenir compte des données à caractère personnel qui affichent des éléments visés à l'article 110.

Il est donc necéssaire dans la chaîne de communication prévue pour les habilitations de sécurité ou des vérifications de sécurité que, dans l'intérêt de la sécurité national ou de l'ordre public, chaque autorité, organe ou personne visé à l'article 107 peut traiter les données visées à l'article 110.

L'alinéa premier clarifie le champ d'application du sous-titre. Il énumère les autorités et entités qui doivent traiter les données à caractère personnel conformément au présent titre lorsqu'elles traitent des habilitations de sécurité, des attestations et avis de sécurité, comme indiqué dans la loi du 11 décembre 1998.

Le deuxième alinéa prévoit que le traitement des données à caractère personnel par l'organe de recours, dans le cadre des procédures de recours prévues par la loi du 11 décembre 1998 portant création de l'organe de recours, doit également avoir lieu conformément au présent titre. Les procédures de recours relatives aux habilitations de sécurité et aux vérifications de sécurité reprennent les données personnelles placées sous ce titre par l'alinéa précédent. Il est donc logique que le même régime soit appliqué à ces données personnelles.

Le troisième alinéa dispose que les autres titres de la présente loi ne s'appliquent pas aux traitements dans le cadre de la loi du 11 décembre 1998. Le présent sous-titre comprend l'ensemble des dispositions applicables au traitement des données à caractère personnel visées au premier et deuxième alinéa. L'application d'autres titres de la présente loi à l'exception des dispositions pénales et finales ne se justifie donc pas.

CHAPITRE III

Conditions générales du traitement

Art. 108

Cet article décrit les cas dans lesquels le traitement de données à caractère personnel est légitime. Ces cas sont ceux qui étaient repris à l'article 5 LVP.

Le traitement des données personnelles est toujours possible avec le consentement de la personne concernée, à condition que l'autorisation soit libre et informée comme déterminé par la jurisprudence. Ce consentement

ook wettelijk vereist in artikelen 16, 22*bis*, tweede lid, 22*quinquies*/*1*, § 1, tweede lid en §§ 5 en 6 van de wet 11 december 1998. De verwerking bedoeld in artikel 94/3 kan plaatsvinden indien dit noodzakelijk is voor de uitvoering van de procedures veiligheidsmachtiging en veiligheidsverificatie bedoeld in de wet van 11 december 1998, voor de uitvoering van een contract of voor andere verplichtingen. Een verwerking van persoonsgegevens is eveneens toegelaten wanneer dit noodzakelijk is voor de uitvoering van een opdracht van openbaar belang.

Art. 109

Iedere verwerking van persoonsgegevens dient rechtmatig en eerlijk te geschieden met het oog op specifieke, vastgestelde doeleinden. Betrokkene personen moeten kennis kunnen nemen van de regels, waarborgen en rechten in verband met de verwerking van hun persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot de verwerking kunnen uitoefenen.

De specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt dienen welbepaald, expliciet en legitiem te zijn. De persoonsgegevens dienen niet verder te worden verwerkt op een wijze die onverenigbaar is met deze doeleinden. Er wordt verduidelijkt dat verdere verwerking voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd wordt.

De persoonsgegevens dienen toereikend, ter zake dienend en niet overmatig te zijn voor de doeleinden waarvoor zij worden verwerkt. De persoonsgegevens dienen nauwkeurig te zijn. De onjuiste persoonsgegevens dienen verbeterd of verwijderd te worden. Deze beginselen zijn overgenomen uit artikel 5 van het Verdrag 108 en artikel 4 WVP.

HOOFDSTUK IV

Aard van de persoonsgegevens

Art. 110

Dit artikel laat de overheden, organen en personen bedoeld in artikel 107 toe om persoonsgegevens te verwerken die gevoelig zijn vanwege hun aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens

est également légalement requis aux articles 16, 22*bis*, deuxième alinéa, 22*quinquies*/1, § 1er, deuxième alinéa et §§ 5 et 6 de la loi du 11 décembre 1998. Le traitement visé à l'article 94/3 peut avoir lieu si cela est nécessaire pour la mise en œuvre des procédures d'habilitation de sécurité et de vérification de la sécurité prévues par la loi du 11 décembre 1998, pour l'exécution d'un contrat ou pour d'autres obligations. Un traitement de données à caractère personnel est également autorisé s'il est utile pour l'exécution d'une mission d'intérêt public.

Art. 109

Chaque traitement de données à caractère personnel doit être effectué licitement et loyalement, en lien avec des finalités spécifiques et déterminées. Les personnes concernées doivent pouvoir prendre connaissance des règles, garanties et droits en lien avec le traitement de leurs données à caractère personnel, ainsi que de la manière dont elles peuvent exercer leurs droits relatifs au traitement.

Les finalités spécifiques pour lesquelles les données à caractère personnel sont traitées doivent être déterminées, explicites et légitimes. Les données ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités. Il est précisé qu'un traitement ultérieur à des fins historiques, scientifiques ou statistiques n'est pas réputé incompatible.

Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées. Les données à caractère personnel doivent être exactes. Les données inexactes doivent être rectifiées ou effacées. Ces principes sont repris de l'article 5 de la Convention 108 et de l'article 4 LVP.

CHAPITRE IV

Types de données à caractère personnel

Art. 110

Cet article autorise les autorités, organes et personnes visés à l'article 107 à traiter des données à caractère personnel qui sont sensibles de par leur nature, notamment celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la

die het seksuele gedrag of geaardheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen. Deze uitzondering was reeds voorzien in de WVP (artikel 3, § 4).

Hoewel deze verwerking in principe verboden is, voorziet het Verdrag 108 in haar artikel 9, § 2, een uitzondering op het verbod deze gegevens te verwerken in het belang van de nationale veiligheid indien dit uitdrukkelijk voorzien is in een wet, wat de bestaansreden is van dit artikel.

Deze mogelijkheid om gevoelige gegevens te verwerken wordt gerechtvaardigd door het feit dat de verwerkingsverantwoordelijke in staat moet zijn om elk type gegeven, zonder onderscheid, te verwerken om te kunnen anticiperen op elke bedreiging van de nationale veiligheid.

Zo kunnen bijvoorbeeld politieke, godsdienstige of levensbeschouwelijke overtuigingen belangrijke indicatoren vormen voor het inschatten van de bedreiging die een persoon kan vormen voor de nationale veiligheid, onder andere als indicator voor radicalisering.

Biometrische gegevens laten dan weer een formele identificatie toe van vreemdelingen wanneer hun identiteitsdocumenten niet betrouwbaar zijn, wat extreem nuttig is in het kader van de veiligheidsverificaties die de ADIV uitvoert in het buitenland om de veiligheid van de troepen te verzekeren.

Gegevens betreffende ras en etniciteit maken het mogelijk om lidmaatschap tot welbepaalde groeperingen te bepalen en bepaalde fenomenen te onderzoeken die een bedreiging vormen voor de nationale veiligheid.

Eender welk van de in dit artikel vermelde gegevens kan nuttig zijn op elk moment. De verwerkingsverantwoordelijke moet elk van deze gegevens kunnen verwerken zonder beperkingen om naar best vermogen haar opdrachten te kunnen uitvoeren, dit met naleving van het principe van proportionaliteit en met onderwerping aan een diepgaande controle.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 111

Voor de bewaring van de persoonsgegevens verwijst dit artikel naar artikel 25 van de wet van 11 december 1998 dat in het kader van de procedures

vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes. Cette exception était déjà adoptée par la LVP (article 3, § 4).

La Convention 108 autorise d'ailleurs dans son article 9, § 2, une exception à l'interdiction de traiter ces données dans l'intérêt de la sécurité nationale si elle est expressément prévue dans une loi, raison d'être de cet article.

Cette possibilité de traiter des données sensibles est justifiée par le fait que le responsable du traitement devrait être en mesure de traiter chaque type de données, sans distinction, pour anticiper toute menace contre la sécurité nationale.

Par exemple, les opinions politiques, les convictions religieuses ou philosophiques peuvent former des indicateurs importants pour l'évaluation de la menace qu'une personne peut former pour la sécurité nationale, par exemple un indicateur de radicalisation.

Les données biométriques permettent l'identification formelle des étrangers là où leurs documents d'identité ne sont pas fiables, ce qui est extrêmement utile notamment dans le cadre des vérifications de sécurité effectuées à l'étranger par le SGRS pour assurer la sécurité des troupes.

Les données sur la race et l'ethnie permettent de déterminer l'appartenance à certains groupes et d'étudier certains phénomènes présentant une menace pour la sécurité nationale.

N'importe quelle donnée peut être nécessaire à tout moment. Le responsable du traitement doit pouvoir traiter tout type de données sans limitation pour pouvoir exercer au mieux sa missions, en respectant bien entendu l'exigence de proportionnalité et en étant soumis à un contrôle approfondi.

CHAPITRE V

Conservation des données à caractère personnel

Art. 111

Pour la conservation des données à caractère personnel, cet article renvoie à l'article 25 de la loi du 11 décembre 1998 qui détermine les modalités de

veiligheidsmachtiging en veiligheidsverificatie reeds de modaliteiten van bewaring van persoonsgegevens bepaalt.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 112

Dit algemeen principe, met name dat elke natuurlijke persoon recht heeft op de bescherming van zijn persoonsgegevens, is overgenomen van artikel 2 WVP.

Art. 113

Dit artikel bevat een opsomming van de rechten van de persoon wiens gegevens verwerkt worden. De uitoefening van deze rechten wordt verder uitgewerkt in de volgende paragrafen en artikelen. Het Verdrag 108 voorziet in diens artikelen 8 en 9 dat er uitzonderingen mogelijk zijn op het recht op informatie, rectificatie en vergetelheid van de betrokkene, indien de wet hierin voorziet en het om een maatregel gaat die in een democratische samenleving noodzakelijk is ten behoeve van de bescherming van de veiligheid van de staat. Deze uitzonderingen werden al vastgelegd in artikel 3, § 4, WVP.

Art. 114

§ 1. Het eerste lid bepaalt welke persoonsgegevens de betrokkene kan raadplegen. In het kader van artikel 107, eerste lid, beperkt dit zich tot de informatie die de betrokkene, conform de wet van 11 december 1998, zelf aanlevert in het kader hiervan.

Op vraag van de burger controleert de bevoegde toezichthoudende autoriteit de rechtmatigheid van de gegevensverwerking door de verwerkingsverantwoordelijke. Na controle deelt de toezichthoudende autoriteit aan de betrokkene mee dat de nodige verificaties werden verricht. Indien nodig gaat de verwerkingsverantwoordelijke over tot de verbetering of verwijdering van onjuiste of niet-pertinente gegevens.

§ 2. In het geval de betrokkene een beroep zou aantekenen tegen een weigering van een veiligheidsmachtiging of -advies of tegen een negatief veiligheidsattest beperkt de toegang tot zijn verwerkte persoonsgegevens zich tot de persoonsgegevens bedoeld in artikel 6 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan.

stockage des données personnelles dans le cadre des procédures d'habilitation de sécurité et de vérification de sécurité.

CHAPITRE VI

Droits de la personne concernée

Art. 112

Ce principe général, à savoir que toute personne physique a droit au respect de sa vie privée, est repris de l'article 2 LVP.

Art. 113

Cet article contient une énumération des droits de la personne dont les données sont traitées. Les modalités d'exercice de ces droits sont précisés dans les paragraphes et articles suivants. La Convention 108 prévoit en ses articles 8 et 9 combinés que des exceptions aux droits de la personne concernée à l'information, à la rectification et à l'effacement sont possibles, pour autant qu'elles soient prévues par la loi et qu'il s'agisse de mesures nécessaires dans une société démocratique à la protection de la sécurité de l'État. Ces exceptions étaient déjà établies dans l'article 3, § 4, LVP.

Art. 114

§ 1er. L' alinéa premier détermine les données personnelles que la personne concernée peut consulter. Dans le cadre de l'article 107, alinéa premier, celles-ci sont limitées aux informations que l'intéressé fournit lui-même conformément à la loi du 11 décembre 1998.

L'autorité de contrôle compétente vérifie, à la demande de la personne concernée, la licéité du traitement des données par le responsable du traitement. Après contrôle, l'autorité de contrôle communique à celle-ci que les vérifications nécessaires ont été faites. Si nécessaire, le responsable du traitement procède à la correction ou l'effacement des données inexactes ou non pertinentes.

§ 2. En cas de recours de l'intéressé contre un refus d'habilitation ou d'avis ou contre une attestation de sécurité négative, l'accès à ses données personnelles traitées se limitera aux données personnelles visées à l'article 6 de la loi du 11 décembre 1998 portant création d'un organe de recours.

Art. 115

Net zoals het artikel 12*bis* WVP, stelt deze bepaling dat de verwerkingsverantwoordelijke geen besluit mag nemen met negatieve rechtsgevolgen voor de betrokken persoon, voor zover dit gebeurt louter op grond van een geautomatiseerde verwerking die bedoeld is om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid. Dit verbod geldt niet indien dergelijke verwerking door of krachtens een wet wordt toegelaten of indien dit noodzakelijk is voor redenen van zwaarwegend openbaar belang, zoals de veiligheid van de Staat.

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 116

Dit artikel bepaalt de verplichtingen van de verwerkingsverantwoordelijke. Hij moet waken over de juistheid van de persoonsgegevens. Hij moet ook zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de gegevens beperkt blijft tot wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst.

De verwerkingsverantwoordelijke zien erop toe dat personen die onder hun gezag handelen kennis hebben van de verplichtingen en voorschriften die hen door deze ondertitel worden opgelegd.

Deze verplichtingen zijn conform de verplichtingen voor de verantwoordelijke van de verwerking vervat in artikel 16, § 2, 1°, LVP.

Art. 117

Het gaat over een overname van artikel 16, § 2, WVP. Voor de bescherming van de rechten van betrokkenen en om de verantwoordelijkheid en aansprakelijkheid van de verwerkingsverantwoordelijke en haar verwerkers te bepalen, is het noodzakelijk dat verantwoordelijkheden op duidelijke wijze worden vastgesteld wanneer een verwerking namens de verwerkingsverantwoordelijke wordt uitgevoerd.

De verwerkingsverantwoordelijke moet een verwerker kiezen die voldoende waarborgen biedt ten aanzien van

Art. 115

A l'instar de ce que faisait l'article 12*bis* LVP, cette disposition prescrit que le responsable du traitement ne peut prendre aucune décision produisant des effets juridiques dommageables ou lourds de conséquence pour la personne concernée, sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects de sa personnalité. Cette interdiction ne s'applique pas lorsqu'un tel traitement est autorisé par ou en vertu d'une loi ou lorsqu'il est nécessaire en raison d'un intérêt public important, tel que la sécurité de l'État.

CHAPITRE VII

Obligations du responsable de traitement et du sous-traitant

Section 1re

Obligations générales

Art. 116

Cet article détermine les obligations du responsable du traitement. Il doit veiller à la justesse des données à caractère personnel. Il doit également veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données soit limité à ce qui est utile pour l'exercice de leurs fonctions ou pour les besoins du service.

Le responsable du traitement fait également en sorte que les personnes agissant sous son autorité aient connaissance des obligations et prescriptions qui leur sont imposées par le présent sous-titre.

Ces obligations sont conformes à celles du responsable du traitement contenues dans l'article 16, § 2, 1°, WVP.

Art. 117

Il s'agit d'une reprise de l'article 16, § 2, LVP. Pour la protection des droits des personnes concernées et pour déterminer les responsabilités du responsable du traitement et de leurs sous-traitants, il est nécessaire que des responsabilités soient fixées de manière claire lorsqu'un traitement est effectué pour le compte du responsable de traitement.

Le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes au regard

de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking.

De uitvoering van een verwerking door een verwerker dient te worden geregeld door een overeenkomst die de verwerker bindt aan de verwerkingsverantwoordelijke, en waarin met name is bepaald dat de verwerker uitsluitend op instructie van de verwerkingsverantwoordelijke dient te handelen, dat hij de voorziene technische beveiligingsmaatregelen naleeft en dat hij door dezelfde verplichtingen als deze van de verwerkingsverantwoordelijke is gebonden. Deze overeenkomst bepaalt ook de verantwoordelijkheden van de verwerker.

Art. 118

Dit artikel legt aan de verwerker dezelfde verplichtingen op als deze waartoe de verwerkingsverantwoordelijken zijn gehouden. Gelet op de opdrachten van de verwerkingsverantwoordelijke en de gevoeligheid van sommige persoonsgegevens, mag de verwerker de verwerking niet aan een andere verwerker doorgeven zonder de uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Art. 119

Dit artikel is een overname van artikel 16, § 3, WVP. Een verwerker of eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker zelf verwerkt de persoonsgegevens slechts in opdracht van de verwerkingsverantwoordelijke, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 120

Wanneer meerdere verwerkingsverantwoordelijken worden aangesteld voor éénzelfde persoonsgegevensverwerking, worden zij de gezamenlijke verwerkingsverantwoordelijken genoemd. Dit artikel beoogt de hypothese van één persoonsgegevensbank met meerdere verwerkingsverantwoordelijken.

De verplichtingen van de verwerkingsverantwoordelijken ten aanzien van de betrokkenen en de mededeling van gegevens, zijn in het algemeen gedefinieerd door of krachtens de wet. Gezien er in dit geval meerdere verwerkingsverantwoordelijken zijn, moeten hun respectievelijke verplichtingen gepreciseerd worden. Indien dit

des mesures de sécurité technique et d'organisation relatives aux traitements.

L'exécution d'un traitement par un sous-traitant doit être réglée par un accord qui engage le sous-traitant au responsable du traitement et dans lequel il est notamment fixé que le sous-traitant agit exclusivement sur instruction du responsable du traitement, qu'il respecte les mesures de sécurité techniques prévues et qu'il est tenu aux mêmes obligations que celles du responsable du traitement. Cet accord détermine aussi les responsabilités du sous-traitant.

Art. 118

Cet article impose au sous-traitant les mêmes obligations que celles qui incombent aux responsables du traitement. Vu les missions du responsable du traitement et la sensibilité de certaines données à caractère personnel, le sous-traitant ne peut pas confier le traitement à un autre sous-traitant sans l'autorisation expresse du responsable du traitement.

Art. 119

Cet article est une reprise de l'article 16, § 3, LVP. Un sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant lui-même ne traite des données à caractère personnel que sur instruction du responsable du traitement, sauf en cas d'obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 120

Lorsque plusieurs responsables du traitement sont désignés pour un même traitement de données à caractère personnel, on appelle ceux-ci responsables conjoints du traitement. Cet article vise l'hypothèse où une banque de données à caractère personnel a plusieurs responsables du traitement.

De manière générale, les obligations des responsables du traitement à l'égard des personnes concernées et de la communication des données sont définies par ou en vertu de la loi. Compte tenu qu'en l'espèce, il y a plusieurs responsables du traitement, il faut que leurs obligations respectives soient précisées. Si ce n'est pas

niet dit niet voorzien is door of krachtens de wet, biedt dit artikel de mogelijkheid om de verplichtingen vast te leggen in een akkoord.

Voor het gemak van de betrokkenen kan in het akkoord één contactpunt aangewezen worden voor de verschillende verwerkingsverantwoordelijken.

Naar aanleiding van de opmerking geformuleerd in punt 242 door de Privacycommissie in haar advies nr. 33/2018 werd de verplichting tot het opnemen van een gezamenlijk contactpunt in het register ingevoegd.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 121

Dit artikel herneemt artikel 16, § 4, WVP. Het vermeldt de passende technische en organisatorische maatregelen die de verwerkingsverantwoordelijke moet treffen. Dit artikel stelt dat er hierbij steeds een belangenafweging gemaakt wordt. Zo worden de stand van de techniek (technologische evoluties), de kosten van de toe te passen maatregelen, de aard van de te beveiligen gegevens en de mogelijke risico's mee in overweging genomen om het passende karakter van de maatregelen vast te stellen.

Er zijn tal van maatregelen die in het belang van de uitoefening van haar opdrachten reeds opgelegd worden aan de verwerkingsverantwoordelijke in het kader van de wet van 11 december 1998:

1. de classificatieregels zoals bepaald in de wet van 11 december 1998;

2. de regels in de wet van 30 november 1998;

3. de NAVO-veiligheidsregels (en van de Europese Unie);

4. de richtlijnen van de Nationale Veiligheidsraad;

5. de richtlijnen van de Nationale Veiligheidsoverheid.

Art. 122

Om het toezicht op de verwerking bedoeld in artikel 107 daadkrachtiger te maken, voert dit artikel een nieuwe verplichting in voor de verwerkingsverantwoordelijke.

prévu par ou en vertu de la loi, cet article permet que ces obligations respectives soient définies dans un accord.

Pour la facilité des personnes concernées, l'accord peut aussi désigner un seul point de contact pour les différents responsables du traitement.

Suite à la remarque formulée dans le point 242 par la Commission vie privée dans son avis n°33/2018, l'obligation de reprendre un point de contact commun dans le régistre a été inséré.

Section 3

Sécurité des données à caractère personnel

Art. 121

Cet article reprend l'article 16, § 4, LVP. Il mentionne les mesures techniques et organisationnelles adéquates que le responsable du traitement doit prendre. Cet article suppose toujours une mise en balance des intérêts. Ainsi, l'état de la technique (les progrès technologiques), les coûts des mesures à appliquer, la nature des données à protéger et les risques encourus doivent être pris en considération pour déterminer le caractère adéquat des dispositions à prendre.

Il existe nombre de mesures qui ont déjà été imposées au responsable du traitement dans l'intérêt de l'exercice de ses missions dans le cadre de la loi du 11 décembre 1998:

1. les règles de classification telles que définies dans la loi du 11 décembre 1998;

2. les règles dans la loi du 30 novembre 1998;

3. les règles de sécurité de l'OTAN (et de l'Union européenne);

4. les directives du Conseil national de sécurité;

5. les directives de l'Autorité nationale de Sécurité.

Art. 122

Cet article introduit une nouvelle obligation à charge du responsable du traitement afin de rendre plus efficace le contrôle sur le traitement visé à l'article 107.

Zo moet de verwerkingsverantwoordelijke zo snel mogelijk haar toezichthoudende autoriteit, op de hoogte brengen indien er een inbreuk op de beveiliging plaatsvindt die een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Er is echter geen sprake van een kennisgeving aan de betrokkene, gezien dit in het belang van de uitvoering van de verwerking niet mogelijk is. Het beschermen van de nationale veiligheid laat het uitblijven van deze kennisgeving toe. De verwerker moet elke inbreuk op de beveiliging melden aan de verwerkingsverantwoordelijke die het risico voor de rechten en vrijheden van personen zal beoordelen. Opnieuw is er hier echter geen sprake van een kennisgeving aan de betrokkene.

De te vermelden gegevens worden opgesomd in het wetsartikel. Om de verwerkingen en derden die hun medewerking hieraan verlenen te beschermen, worden deze gegevens beperkt.

Naar aanleiding van de opmerking geformuleerd in punt 242 door de Privacycommissie in haar advies nr. 33/2018 werd de verplichting ingevoegd om inbreuken te melden binnen 72 uur na kennisname ervan.

Afdeling 4

Registers

Art. 123

Eveneens om een meer doeltreffend toezicht toe te laten, introduceert dit artikel een nieuwe verplichting voor de verwerkingsverantwoordelijke, en desgevallend zijn verwerker, voor de verwerking bedoeld in artikel 107.

Deze dient een register bij te houden van zijn verwerkingsactiviteiten.

Dit artikel somt de informatie op die vermeld moet worden in dat register. Er werden dezelfde vermeldingen als die uit titel 1 hernomen.

Er dient echter genuanceerd te worden dat deze vermeldingen slechts gemaakt kunnen worden wanneer ze toepasselijk en mogelijk zijn. Indien het om een verwerkingsactiviteit in het buitenland gaat, is het bijvoorbeeld mogelijk dat de verwerkingsverantwoordelijken niet over de precieze contactgegevens van de verwerkingsverantwoordelijke beschikt. Om deze reden is de vermelding van deze contactgegevens onderworpen aan de voorwaarde dat deze gekend zijn.

Le responsable du traitement doit dans les meilleurs délais mettre au courant son autorité de contrôle, d'une brèche de sécurité si elle recèle un risque élevé pour les droits et libertés de personnes physiques. Par contre, il n'est pas question d'une notification à la personne concernée, car cela n'est pas possible dans l'intérêt de la mise en œuvre du traitement. La protection de la sécurité nationale permet l'omission de cette notification. Le sous-traitant doit notifier toute brèche de sécurité au responsable du traitement qui évaluera le risque pour les droits et libertés des personnes. Ici non plus il n'est pas question de notification à la personne concernée.

Le texte légal énumère les informations à communiquer. Afin de protéger les opérations de traitement et les tiers qui coopèrent avec cela, ces données sont limitées.

Suite à la remarque formulé dans le point 242 par la Commission vie privée dans son avis n°33/2018, l'obligation de notifier des brèches de sécurité dans le délai de 72 heures après la prise de connaissance a été inséré.

Section 4

Registres

Art. 123

Pour également permettre un contrôle plus efficace, cet article introduit une nouvelle obligation dans le chef du responsable du traitement et, le cas échéant, son sous-traitant, pour le traitement visé à l'article 107.

Ceux-ci doivent tenir un registre de leurs activités de traitement.

Cet article énumère les informations qui doivent être mentionnées dans ce registre. Les mêmes mentions que celles du titre 1er ont été répétées.

Cependant, il faut nuancer que ces mentions ne peuvent être faites que lorsqu'elles sont applicables et possibles. Par exemple, s'il s'agit d'une activité de traitement à l'étranger, il est possible que les responsables du traitement n'aient pas les coordonnées exactes du responsable du traitement. Pour cette raison, la mention de ces données de contact est soumise à la condition que celles-ci soient connues.

De tweede paragraaf voorziet een schriftelijke vorm, met inbegrip een elektronische vorm begrepen wordt, voor het register.

De derde paragraaf bepaalt dat het register ter beschikking worden gesteld op vraag van de bevoegde toezichthoudende autoriteit. Het register van de verwerker wordt steeds ter beschikking gesteld van de verwerkingsverantwoordelijke.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 124

Dit artikel legt de aanduiding van een functionaris voor gegevensverwerking op door de verwerkingsverantwoordelijke en, in voorkomend geval door de verwerker.

De functionaris wordt betrokken bij alle vragen betreffende de bescherming van persoonsgegevens.

Deze moet titularis zijn van een veiligheidsmachtiging zeer geheim want overheden kunnen classificeren tot en met dit niveau.

Hij oefent zijn functie in volledige onafhankelijkheid uit en moet beschikken over de nodige middelen. Hij mag niet worden ontzet uit zijn functies.

De Koning kan indien nodig, andere modaliteiten voor de werking vastleggen en de bevoegdheden van de functionaris uitbreiden.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van persoonsgegevens aan de publieke sector en de private sector

Art. 125

De uitwisseling van persoonsgegevens verwerkt in het kader van artikel 107 vindt plaats in het kader van de procedures veiligheidsmachtiging en veiligheidsattesten en -adviezen bedoeld in de wet van 11 december 1998. De uitwisseling van persoonsgegevens is dus onderhevig aan wettelijk bepaalde procedures waaraan reeds analyses voorafgaan.

Le second paragraphe prévoit une forme écrite, y compris la forme électronique pour le registre.

Le troisième paragraphe dispose que les registres sont mis à la disposition de l'autorité de contrôle compétente à sa demande. Le registre du sous-traitant est en permanence mis à la disposition du responsable de traitement.

Section 5

Délégué à la protection des données

Art. 124

Cet article impose la désignation d'un délégué à la protection des données par le responsable du traitement, et le cas échéant, par le sous-traitant.

Le délégué est impliqué dans toutes les questions concernant la protection des données personnelles.

Celui-ci doit être titulaire d'une habilitation de sécurité du niveau très secret car les autorités peuvent classifier jusqu'à ce niveau.

Il exerce ses fonctions en toute indépendance et doit disposer des ressources nécessaires. Il ne peut être renvoyé de ses fonctions.

Le Roi peut fixer, si nécessaire, d'autres modalités de fonctionnement et étendre les compétences du délégué.

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données avec le secteur public et le secteur privé

Art. 125

L'échange de données à caractère personnel traitées dans le cadre de l'article 107 intervient dans le cadre des procédures d'habilitation de sécurité et des attestations et avis de sécurité visés par la loi du 11 décembre 1998. L'échange de données à caractère personnel fait donc l'objet de procédures juridiquement contrôlées, précédées d'analyses.

Hieruit volgt dat een raadpleging van de functionaris voor gegevensbescherming of de bevoegde toezichthoudende autoriteit of een impactanalyse geen voorafgaande vereiste kunnen zijn voor de mededeling van informatie.

Dit weerhoudt een publiek of een particulier orgaan er niet van om, indien de partijen dit wensen, een protocolakkoord te sluiten met een verwerkingsverantwoordelijke bedoeld in deze ondertitel, of om het advies van de functionaris voor gegevensbescherming of de bevoegde toezichthoudende autoriteit te vragen, of om een impactanalyse te vragen. Dit mag echter geen voorafgaande voorwaarde zijn voor de in het kader van de procedure veiligheidsmachtiging of veiligheidsverificatie wettelijk vereiste informatie-uitwisseling die er toe kan leiden dat de wettelijk bepaalde termijnen voor communicatie van deze gegevens overschreden wordt.

De tweede paragraaf van dit artikel wijkt af van artikel 23, § 1, tweede lid, voor wat betreft de verplichte vermeldingen in het protocol. Dit is om evidente redenen van discretie over de *modus operandi* van de entiteiten die verwerkingen uitvoeren, en meer bepaald de manier waarop zij informatie beschermen. Waar toepasselijk, en mogelijk, zullen de vermeldingen in het tweede paragraaf ingevuld worden. Wanneer deze vermeldingen echter niet beschikbaar zijn, of niet mogen vermeld worden omwille van de aard en afkomst van de vermelding en dit in het kader van de nationale veiligheid, moeten de desbetreffende vermeldingen niet ingevuld worden.

Afdeling 2

Doorgifte van persoonsgegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 126

Het eerste en tweede lid van dit artikel zijn een exacte reproductie van de eerste paragraaf van artikel 21 WVP. Zij hernemen het criteria van het adequate beschermingsniveau dat de niet-lidstaat van de Europese Unie moet waarborgen opdat de betrokken bedoeld in deze ondertitel persoonsgegevens mag doorgeven.

De term “internationale organisatie” wordt toegevoegd omdat een internationale organisatie eveneens de bestemmeling kan zijn van persoonsgegevens.

Het derde lid bepaalt dat het adequaat beschermingsniveau gewaarborgd kan worden door veiligheidsclausules

Il s’ensuit qu’une consultation du délégué à la protection des données ou de l’autorité de contrôle compétente ou une analyse d’impact ne peuvent pas être exigées comme préalable à la transmission des informations.

Cela n’empêche évidemment pas un organe public ou privé, si les parties le souhaitent, de conclure un protocole d’accord avec un responsable du traitement visé dans le présent sous-titre, ou de demander l’avis de son délégué à la protection des données ou de l’autorité de contrôle compétente ou de procéder à une analyse d’impact. Cela ne peut cependant pas constituer une condition préalable à l’échange d’informations légalement requis par l’habilitation de sécurité ou la procédure de vérification de la sécurité, ce qui peut entraîner le dépassement des délais légaux de communication de ces données.

Le second paragraphe du présent article déroge à l’article 23, § 1er, alinéa 2, en ce qui concerne les mentions que doit contenir le protocole. Cela s’explique pour des raisons évidentes de discrétion du *modus operandi* des entités qui exécutent le traitement et notamment de la manière dont ils protègent les informations. Le cas échéant, et éventuellement, les mentions du deuxième paragraphe seront complétées. Cependant, si ces mentions ne sont pas disponibles, ou ne peuvent être mentionnées en raison de la nature et de l’origine de la mention et ceci dans le contexte de la sécurité nationale, les mentions pertinentes ne doivent pas être complétées.

Section 2

Transfert des données vers des pays non membres de l’Union européenne ou à des organisations internationales

Art. 126

Les alinéas premier et 2 du présent article sont l’exacte reproduction du premier paragraphe de l’article 21 LVP. Ils reprennent le critère du niveau de protection adéquat que doit assurer le pays non membre de l’Union européenne pour que le responsable du traitement concerné visé dans le présent sous-titre puisse lui transférer une donnée à caractère personnel.

Le terme “organisation internationale” a été ajoutés puisqu’une organisation internationale peut également être le destinataire de données à caractère personnel.

Le troisième alinéa fixe que le niveau de protection adéquat peut être assuré par des clauses de sécurité

waarop de betrokken verwerkingsverantwoordelijke en de bestemmeling zich afstemmen. Dit lid herneemt het idee van alinea 2 van artikel 22 WVP.

Art. 127

Dit voorziet uitzonderingen op de vereiste van een adequaat beschermingsniveau:

1. na instemming van de betrokkene (kopij van artikel 22, 1°, WVP);

2. Indien de doorgifte noodzakelijk of wettelijk verplicht is voor de bescherming van de fysieke integriteit van een persoon of van een belangrijk openbaar belang (fusie van 4° en 5°, van artikel 22 WVP);

3. Indien de doorgifte noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

Zelfs indien het voor de hand ligt dat de verwerkingsverantwoordelijke de doorgifte van persoonsgegevens aan landen die niet een adequaat beschermingsniveau waarborgen, tracht te voorkomen, kan het gebeuren dat hij verplicht is in het kader van de nationale veiligheid, de strijd tegen terrorisme, de bescherming van Belgische troepen in het buitenland, …

Ter informatie, de samenwerking tussen de verwerkingsverantwoordelijken en hun buitenlandse partners wordt beheerst door bilaterale verdragen met die partnerlanden.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 128

Wat betreft de gegevensverwerking bedoeld in artikel 107, eerste lid, wordt het Vast Comité I opgericht door de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse aangeduid als bevoegde toezichthoudende autoriteit. De activiteiten bedoeld in artikel 107, eerste lid, vielen reeds voor het invoegen treden van deze wet onder de bevoegdheid van het Vast Comité I. Dit is een logische voorzetting van een reeds bestaande praktijk.

Wat betreft de bevoegde toezichthoudende autoriteit voor de verwerking bedoeld in artikel 107, tweede lid,

sur lesquelles s'accordent le responsable du traitement concerné et le destinataire. Cet alinéa reprend l'idée de l'alinéa 2 de l'article 22 LVP.

Art. 127

Ceci prévoit des exceptions à l'exigence d'un niveau de protection adéquat:

1. avec le consentement de la personne concernée (copie de l'article 22, 1°, LVP);

2. si le transfert est nécessaire ou légalement obligatoire à la sauvegarde de l'intégrité physique d'une personne ou d'un intérêt public important (fusion des 4° et 5°, de l'article 22 LVP);

3. le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

Même s'il est évident que le responsable du traitement essaie d'éviter de transférer des données à caractère personnel à des pays n'assurant pas un niveau de protection adéquat, il arrive qu'il y soit contraint dans un objectif de sécurité nationale, de lutte contre le terrorisme, de protection des troupes belges à l'étranger, …

A titre d'information, la coopération entre les responsables du traitement et leurs partenaires étrangers est régie par des accords bilatéraux avec ces pays partenaires.

CHAPITRE X

Autorité de contrôle

Art. 128

S'agissant du traitement des données visé à l'article 107, premier alinéa, le Comité permanent R, institué par la loi du 18 juillet 1991 réglementant la surveillance des services de police et de renseignement et l'Organe de coordination pour l'analyse de la menace est désigné comme l'autorité de surveillance compétente. Les activités visées à l'article 107, premier alinéa, relevaient déjà de la compétence du Comité permanent R avant l'entrée en vigueur de cette loi, ce qui est la suite logique d'une pratique déjà existante.

En ce qui concerne l'autorité de contrôle compétente pour le traitement visé à l'article 107, alinéa 2, aucune

wordt er geen toezichthoudende autoriteit aangeduid omdat de rechterlijke macht geen controle wordt opgelegd.

Art. 129

Waar nodig werkt het Vast Comité I samen met andere toezichthoudende autoriteiten met respect voor de bescherming van de bronnen, de bescherming van de persoonlijke levenssfeer van derden of de vervulling van de opdrachten van de inlichtingen- en veiligheidsdiensten zoals bepaald in de artikelen 7, 8 en 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de opdrachten bedoeld in artikel 107 en de wet van 11 december 1998.

Het Vast Comité I deelt het resultaat van zijn toezicht in algemene termen mee aan de toezichthoudende autoriteiten benoemd in de andere titels van deze wet.

Art. 130

De overheden, organen en personen bedoeld in deze ondertitel werken samen met het Vast Comité I teneinde hen alle nodige medewerking te verlenen opdat het Vast Comité zijn in deze hoofdstuk toegewezen taak naar behoren kan uitvoeren.

Art. 131

Wanneer een toezichthoudende autoriteit, benoemd in de andere titels van deze wet, kennis neemt van inbreuken op deze titel, informeert zij onverwijld het Vast Comité I over deze inbreuken.

Wanneer een toezichthoudende autoriteit, benoemd in de andere titels van deze wet, gevat wordt in een dossier dat mogelijk gevolgen heeft voor de verwerking van persoonsgegevens overlegt zij met het Vast Comité I.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden

Art. 132

Zoals uiteengezet in de inleiding, is de consultatie van persoonsgegevens verwerkt in het kader van

autorité de contrôle n'est désignée car le pouvoir judiciaire n'est pas soumis à un contrôle.

Art. 129

Le cas échéant, le comité permanent R coopère avec les autres autorités de contrôle en respectant la protection des sources, à la protection de la vie privée de tiers ou à l'accomplissement des missions des services de renseignement et de sécurité telles que définies aux articles 7, 8 et 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les missions visées à l'article 107 et la loi du 11 décembre 1998.

Le Comité permanent R communique le résultat de sa surveillance en termes généraux aux autorités de contrôle désignées dans les autres titres de la présente loi.

Art. 130

Les autorités, organes et personnes visés dans le présent sous-titre coopèrent avec le Comité permanent R afin de leur fournir toute l'assistance nécessaire pour permettre au Comité permanent de mener à bien la mission qui lui est assignée dans le présent chapitre.

Art. 131

Lorsqu'une autorité de contrôle, désignée dans les autres titres de la présente loi, prend connaissance des infractions à ce titre, elle informe sans délai le Comité permanent R de ces infractions.

Lorsqu'une autorité de contrôle, désignée dans les autres titres de la présente loi, est incluse dans un dossier pouvant avoir des conséquences sur le traitement des données à caractère personnel, elle consulte le Comité permanent R.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 132

Comme expliqué dans l'introduction, la consultation à des fins historiques, scientifiques ou statistiques des

artikel 107 door een verdere verwerkingsverantwoordelijke voor historische, wetenschappelijke en statistische doeleinden slechts mogelijk indien dit geen weerslag heeft op de opdrachten bedoeld in deze ondertitel, noch een bron of een derde die zijn medewerking verleent in gevaar brengt, en die geen weerslag heeft op een lopend opsporings- of gerechtelijk onderzoek of op relaties die België onderhoudt met vreemde Staten of internationale organisaties.

De behandeling van geclassificeerde documenten moet natuurlijk de bepalingen van de wet van 11 december 1998 respecteren. Deze specifieke reglementering is nodig aangezien een aanvraag voor consultatie van persoonsgegevens verwerkt in het kader van de wet van 11 december 1998 voor historische, wetenschappelijke en statistische doeleinden op elk moment kan gebeuren, zelfs wanneer een procedure veiligheidsmachtiging of veiligheidsverificatie nog steeds lopende is.

Het is nodig te vermijden dat een betrokken persoon die het onderwerp uitmaakt van een dergelijke procedure, onder het voorwendsel dat hij student is, kennis kan nemen van het feit of deze procedure al dan niet een gunstig resultaat zal opleveren alvorens deze officieel gecommuniceerd wordt.

Zelfs indien titel 4 van onderhavige wet niet van toepassing is op de verwerking in het kader van deze ondertitel, is het aangeraden dat de entiteiten die kennis nemen van deze persoonsgegevens er een expliciete afwijking op voorzien, dit alsook voor hun personeel.

De gegevens van het personeel van de verwerkingsverantwoordelijke in het kader van de wet van 11 december 1998 zijn beschermd om te vermijden dat de leden van deze entiteiten druk ondervinden, of zelfs bedreigingen moeten ondergaan omdat hun identiteit en hun hoedanigheid werd onthuld. Bijgevolg is het aangeraden te preciseren dat de bescherming van de gegevens van hun personeel deel uitmaakt van de opdrachten. Dit betreft eveneens bronnen en derden die hun medewerking verlenen aan de verwerkingsverantwoordelijke. De betrokken verwerkingsverantwoordelijke heeft de verplichting om ook hun gegevens te beschermen (art. 23 van de wet van 11 december 1998).

De toelating tot consultatie om moet gegeven worden door de verwerkingsverantwoordelijke, zelfs indien het gegeven niet in haar handen is gekomen, omdat deze het beste kan evalueren of een consultatie een weerslag kan vormen op één van de te beschermen belangen.

données à caractère personnel traitées en vertu de l'article 107 par un responsable du traitement ultérieur n'est possible que si elle ne porte pas atteinte aux missions visées par le présent sous-titre, ni ne met en danger une source ou un tiers qui prête son concours, et ne porte pas atteinte à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales.

Le traitement des données classifiées doit bien entendu aussi respecter les dispositions de la loi du 11 décembre 1998. Cette réglementation spécifique est nécessaire car une demande de consultation des données traitées dans le cadre de la loi du 11 décembre 1998 à des fins historiques, scientifiques ou statistiques peut avoir lieu à tout moment, alors même qu'une procédure d'habilitation de sécurité ou de vérification de sécurité est encore en cours.

Il faut éviter qu'une personne concernée, qui fait l'objet d'une telle procédure, sous prétexte d'être étudiante, puisse prendre connaissance du fait que cette procédure aboutira ou non à un résultat favorable avant sa communication officielle.

Même si le titre 4 de la présente loi n'est pas applicable au traitement dans le cadre de ce sous-titre, il est recommandé que les entités qui prennent connaissance de ces données personnelles prévoient une dérogation expresse ainsi que pour leur personnel.

Les données du personnel du responsable du traitement dans le cadre de la loi du 11 décembre 1998 sont protégées pour éviter que des membres desdits services ne subissent des pressions, voire des menaces car leur identité et qualité sont dévoilées. Par conséquent, il convient de préciser que la protection des données de leur personnel fait partie des missions visées. Il en va de même des sources et des tiers qui prêtent leur concours au responsable du traitement. Le responsable du traitement concerné a d'ailleurs l'obligation de protéger ses données (art. 23 de la loi du 11 décembre 1998).

L'autorisation de consulter doit émaner du responsable du traitement, même si la donnée n'est pas entre ses mains, car c'est lui qui est le plus à même d'évaluer si la consultation est susceptible de porter atteinte à un des intérêts à protéger.

Art. 133

Om de aandacht te vestigen van de gebruiker op het bijzondere regime toepasselijk op de latere behandeling van het gegeven, vereist dit artikel dat dit gegeven gemarkeerd wordt door de vermelding “Bescherming van persoonsgegevens – artikelen 132 tot 137 van de wet van xx/xx/2018”.

Art. 134

Omwille van evidente redenen voor de bescherming van het privéleven, moeten de gegevens geanonimiseerd worden. Indien dit het niet mogelijk maakt om het doel van de latere behandeling te bereiken, kan de verwerkingsverantwoordelijke pseudonimisering op de desbetreffende gegevens toepassen.

De filosofie van dit artikel beantwoord aan wat is voorzien in hoofdstuk II van het Koninklijk Besluit van 13 februari 2001 betreffende de uitvoering van de wet van 8 december 1992.

De term pseudonimisering werd toegevoegd als gevolg van de nieuwe Europese reglementering. Indien de anonimisering of de pseudonimisering de identificatie niet onmogelijk maakt, laat de verwerkingsverantwoordelijke slecht een consultatie toe indien er geen disproportionele weerslag is op het privéleven.

In dezelfde zin, indien de latere verwerking van gepseudonimiseerde gegevens het niet toelaat om de historische, wetenschappelijke of statistische doeleinden te bereiken, kan de betrokken verwerkingsverantwoordelijke niet-gepseudonimiseerde gegevens toelaten indien er geen disproportionele weerslag is op het privéleven.

Art. 135

Omwille van redenen van bescherming van het privéleven en de belangen bedoeld in artikel 129, kan geen enkele communicatie of publicatie van niet-geanonimiseerde en niet-gepseudonimiseerde gegevens plaatsvinden zonder toelating van de verwerkingsverantwoordelijke.

Art. 136

Dit artikel verplicht het bewaren van een register betreffende de latere verwerking door de verdere verwerkingsverantwoordelijke in het kader van deze ondertitel en andere verantwoordelijken voor de verwerking.

Art. 133

Pour attirer l’attention de l’utilisateur sur le régime particulier applicable à la donnée lors du traitement ultérieur, exige cet article que cette donnée soit marquée de la mention “Protection des données à caractère personnel – articles 132 à 137 de la loi du xx/xx/2018”.

Art. 134

Pour des raisons évidentes de protection du droit à la vie privée, les données doivent être rendues anonymes. Si cela ne permet pas d’atteindre le but du traitement ultérieur, le responsable du traitement peut effectuer la pseudonymisation sur les données concernées.

La philosophie de cet l’article correspond à ce qui était prévu dans le chapitre II de l’arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992.

Le terme pseudonymisation est ajouté suite à la nouvelle règlementation européenne. Si l’anonymisation ou la pseudonymisation ne rend pas l’identification impossible, le responsable du traitement n’autorise la consultation que si cela ne constitue pas une atteinte disproportionnée à la vie privée.

Dans le même sens, si un traitement ultérieur de données pseudonymisées ne permet pas d’atteindre les fins historiques, statistiques ou scientifiques, le responsable du traitement peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 135

Pour des raisons de protection de la vie privée et des intérêts visés à l’article 129, toute communication et toute publication des données consultées non anonymisées et non pseudonymisées ne peuvent avoir lieu qu’avec l’autorisation du responsable du traitement.

Art. 136

Cet article impose la tenue d’un journal du traitement ultérieur par le responsable du traitement dans le cadre du présent sous-titre et des autres responsables du traitement.

Dit logboek is logischerwijze geclassificeerd indien de latere verwerking betrekking heeft op geclassificeerde gegevens.

Dit logboek moet vermelden:

1. de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;

2. de doeleinden van de verdere verwerking;

3. de eventuele voorwaarden voor de verdere verwerking vastgelegd door de verwerkingsverantwoordelijke in het kader van artikel 107;

4. de eventuele ontvangers toegestaan door de verwerkingsverantwoordelijke in het kader van de artikel 107.

Art. 137

Dit artikel preciseert dat elke persoon die gegevens verwerkt voor historische, wetenschappelijke of statistische doeleinden verantwoordelijk is van deze verwerking.

Zij houdt een verbod in om geanonimiseerde, of gepseudonimiseerde persoonsgegevens om te zetten. Dit verbod is hernomen uit het artikel 6 van het Koninklijk Besluit van 13 februari 2001 houdende uitvoering van de wet van 8 december 1992.

ONDERTITEL 4

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR HET COORDINATIEORGAAN VOOR DE DREIGINGSANALYSE

ALGEMEEN DEEL

Zoals bepaald in artikel 2 van de Verordening, is deze niet van toepassing op de verwerking van persoonsgegevens in het kader van een activiteit die niet binnen het toepassingsgebied van het Europees Recht valt. Gezien de activiteiten van het OCAD niet tot de bevoegdheden van de Unie behoren (cf. art. 4 VEU), zijn de bepalingen uit de Verordening niet op hen van toepassing. De verwerking van persoonsgegevens door het OCAD werd geregeld door de wet van 8 december 1992. Deze wet voorzag in een toepassing van algemene principes en enkele uitzonderingen die voortvloeiden uit de

Ce journal est bien entendu classifié si le traitement ultérieur porte sur des données classifiées.

Ce journal doit mentionner:

1. les coordonnées du responsable du traitement initial, du responsable ultérieur et du délégué à la protection des données de ce dernier;

2. les finalités du traitement ultérieur;

3. les éventuelles conditions du traitement ultérieur fixées par le responsable du traitement dans le cadre de l'article 107;

4. les éventuels destinataires autorisés par le responsable du traitement dans le cadre de l'article 107.

Art. 137

Cet article précise que toute personne qui traite des données à des fins historiques, scientifiques ou statistiques est responsable dudit traitement.

Elle a interdiction de convertir des données anonymes ou pseudonymisées en données à caractère personnel. Cette interdiction est reprise de l'article 6 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992.

SOUS-TITRE 4

DE LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL PAR L'ORGANE DE COORDINATION POUR L'ANALYSE DE LA MENACE

PARTIE GENERALE

Comme le précise l'article 2 du Règlement, celui-ci ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union européenne. Les activités de l'OCAM n'entrant pas dans les compétences de l'Union (cf. art. 4 TUE), les dispositions du Règlement ne leur sont pas applicables. Le traitement des données à caractère personnel de l'OCAM était réglementé par la loi du 8 décembre 1992. Cette loi prévoyait une application des principes généraux et quelques exceptions en raison des spécificités

specifieke opdrachten van het OCAD. Gelet op de opheffing van de wet van 8 december 1992 door onderhavige wet, wordt een nieuw regime ingevoerd door ondertitel 4. Deze titel bepaalt aldus de toepasselijke regels voor elke verwerking van persoonsgegevens door het OCAD en zijn verwerkers in het belang van de uitoefening van de opdrachten van voornoemde diensten.

De titel volgt vier richtsnoeren:

1. overname van de bepalingen van WVP die van toepassing zijn op het OCAD.

2. naleving van de Conventie voor de bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa van 28 januari 1981 (het zogeheten Verdrag 108);

3. bekrachtiging van bepaalde verplichtingen van de verwerkingsverantwoordelijken;

4. specifieke bepalingen voor het gebruik van persoonsgegevens van het OCAD voor historische, wetenschappelijke of statistische doeleinden.

I. — **STATUS QUO IN VERGELIJKING MET DE WET VAN 8 DECEMBER 1992**

Deze ondertitel maakt dezelfde principes als de WVP toepasselijk op het OCAD en voorziet dezelfde uitzonderingen om dezelfde redenen van discretie.

II. — **NALEVING VAN DE PRINCIPES VAN HET VERDRAG 108**

Het OCAD is onderworpen aan het Verdrag 108. Ondertitel 4 houdt de rechten en verplichtingen in vastgelegd door het Verdrag 108 en voorziet geen juridische uitzonderingen dan wanneer toegelaten door het Verdrag zelf.

III. — **BEKRACHTIGING VAN BEPAALDE VERPLICHTINGEN**

In vergelijking met de verplichtingen vastgelegd door de WVP, gaat ondertitel 4 verder en voorziet deze in nieuwe verplichtingen. Aldus wordt gesteld dat het OCAD registers moeten bijhouden van zijn verwerkingsactiviteiten. Het OCAD heeft eveneens de verplichting om melding te maken aan de bevoegde toezichthoudende autoriteit van elke inbreuk op de beveiliging van persoonsgegevens die een risico voor de rechten en

des finalités de l'OCAM. La loi du 8 décembre 1992 étant abrogée par la présente loi, un nouveau régime est prévu dans le sous-titre 4. Celui-ci détermine donc de nouvelles règles applicables à tout traitement de données à caractère personnel par l'OCAM et ses sous-traitants dans l'intérêt de l'exercice des missions desdits services.

Le titre suit quatre lignes directrices:

1. reprise des mêmes dispositions que celles applicables à l'OCAM dans la LVP;

2. respect de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe du 28 janvier 1981 (dite Convention 108);

3. renforcement de certaines obligations des responsables du traitement;

4. dispositions particulières pour l'utilisation des données à caractère personnel de l'OCAM à des fins historiques, scientifiques ou statistiques.

I. — **STATU QUO PAR RAPPORT À LA LOI DU 8 DÉCEMBRE 1992**

Le présent sous-titre rend les mêmes principes de la LVP applicables à l'OCAM et prévoit les mêmes exceptions pour les mêmes raisons de discrétion.

II. — **RESPECT DES PRINCIPES DE LA CONVENTION 108**

L'OCAM est soumis à la Convention 108. Le sous-titre 4 contient tous les droits et obligations fixés dans la Convention 108 et n'y prévoit d'exceptions légales expresses que lorsque la Convention elle-même les autorise.

III. — **RENFORCEMENT DE CERTAINES OBLIGATIONS**

Par rapport aux obligations fixées par la LVP, le sous-titre 4 va plus loin et prévoit de nouvelles obligations. Ainsi, il dispose que l'OCAM doit tenir des registres de ses activités de traitement. L'OCAM a également l'obligation de notifier à l'autorité de contrôle compétente toute brèche de sécurité portant sur des données à caractère personnel et représentant un risque pour les droits et libertés des personnes physiques. Le sous-titre

vrijheden van natuurlijke personen inhoudt. De ondertitel legt aan het OCAD ook op een functionaris voor gegevensbescherming aan te duiden. Deze verplichting bestond niet in de WVP maar werd niettemin al opgelegd door het Koninklijk Besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Foreign Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling 1*bis* "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt De rol van deze functionaris voor gegevensbescherming wordt uitgebreid in de deze ondertitel.

IV. — **VERWERKING VOOR HISTORISCHE, WETENSCHAPPELIJKE EN STATISTISCHE DOELEINDEN**

Het raadplegen van persoonsgegevens van het OCAD en diens personeel voor historische, wetenschappelijke en statistische doeleinden wordt gereglementeerd. Deze raadpleging is slechts mogelijk indien zij geen weerslag heeft op de opdrachten van het OCAD en indien zij geen weerslag heeft op een lopend opsporings- of gerechtelijk onderzoek of op de relaties die België onderhoudt met andere Staten of internationale organisaties. De verwerking van geclassificeerde documenten dient natuurlijk ook de bepalingen van de wet van 11 december 1998 te respecteren.

Deze specifieke reglementering is noodzakelijk gezien een aanvraag tot verwerking van gegevens komende van het OCAD voor historische, wetenschappelijke of statistische doeleinden kan plaatsvinden op elk moment, zelfs wanneer een onderzoek van een van de ondersteunende diensten van het OCAD nog lopende is. Het is te vermijden dat een betrokkene van een dienst, onder het voorwendsel dat hij student is, kennis kan nemen van het feit dat hij het voorwerp uitmaakt van een opvolging, wat het gehele onderzoek in het gedrang zou brengen.

ARTIKELSGEWIJZE TOELICHTING

HOOFDSTUK I

Definities

Art. 138

De eerste paragraaf wijst naar de definities die gehanteerd worden in titel 2, met uitzondering van diegene die betrekking hebben op de gerechtelijke overheden of de politie en hun toezichthoudende autoriteit. Paragraaf 2 voert hieraan enkele definities toe die eigen zijn aan ondertitel 4 en die enkel relevant zijn voor het OCAD.

impose aussi à l'OCAM de désigner un délégué à la protection des données. Cette obligation qui n'existait pas dans la LVP mais est néanmoins fixée dans l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters et portant exécution de certaines dispositions de la section 1er*bis* "de la gestion des informations" du chapitre IV de la loi sur la fonction de police. Le rôle du délégué à la protection des données est renforcé dans le présent sous-titre.

IV. — **TRAITEMENT À DES FINS HISTORIQUES, SCIENTIFIQUES OU STATISTIQUES**

La consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel de l'OCAM et de leur personnel est réglementée. Elle n'est possible que si elle ne porte pas atteinte aux missions de l'OCAM et ne porte pas atteinte à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales. Le traitement des données classifiées doit bien entendu aussi respecter les dispositions de la loi du 11 décembre 1998.

Cette réglementation spécifique est nécessaire car une demande de consultation des données de l'OCAM à des fins historiques, scientifiques ou statistiques peut avoir lieu à tout moment, alors même qu'une enquête d'un des services d'appui de l'OCAM est encore en cours. Il faut éviter qu'une personne concernée d'un service, sous prétexte qu'elle est étudiante, puisse prendre connaissance du fait qu'elle fait l'objet d'un suivi, ce qui mettrait en péril toute l'enquête.

COMMENTAIRE DES ARTICLES

CHAPITRE IER

Définitions

Art. 138

Le premier paragraphe renvoie aux définitions prévues dans le titre 2, à l'exception de celles qui visent les autorités judiciaires ou de police et leur autorité de contrôle. Le paragraphe 2 ajoute quelques notions qui sont propres au sous-titre 4 et qui ne sont pertinentes que pour l'OCAM.

HOOFDSTUK II

Toepassingsgebied

Art. 139

De verwerking van persoonsgegevens door het OCAD wordt momenteel geregeld door de WVP. Deze wet sluit de toepassing van enkele artikelen uit voor deze diensten en onder andere enkele verplichtingen en rechten van betrokken personen. Gezien "nationale veiligheid" uitgesloten is van de toepassing van de Verordening, is een aparte regeling nodig voor de gegevensverwerking door het OCAD. Dit regime is geinspireerd op de huidige WVP en beantwoordt aan de standaarden van het Verdrag 108.

Het eerste lid verduidelijkt het toepassingsgebied van deze ondertitel. Dit zijn de verwerkingen die worden uitgevoerd in het kader van de wettelijke missies van het OCAD de inlichtingen- en veiligheidsdiensten. Deze missies vloeien voort uit de wet van 10 juli 2006 betreffende de analyse van de dreiging evenals uit andere bijzondere rechtsgrondslagen. Het tweede lid verduidelijkt dat de andere titels van deze wet niet van toepassing zijn op de verwerkingen door het OCAD. De ondertitel 4 omvat het geheel van bepalingen dat van toepassing is op het OCAD voor zijn verwerking van persoonsgegevens bij de uitoefening van zijn wettelijke opdrachten (rechten, verplichtingen, archivering, controle,…), de toepassing van andere titels van deze wet met uitzondering van sommige straf- en slotbepalingen is dus niet te rechtvaardigen.

HOOFDSTUK III

Algemene voorwaarden voor de verwerking

Art. 140

Dit artikel beschrijft in welke gevallen een verwerking van persoonsgegevens rechtmatig is.

Deze gevallen zijn deze zoals ze vervat waren in artikel 3, § 4, WVP. Het OCAD kan aldus persoonsgegevens verwerken indien dit nuttig is voor de uitvoering van zijn opdrachten zoals voorzien in de wet van 10 juli 2006, voor de uitvoering van een contract of voor andere verplichtingen. Een verwerking van persoonsgegevens is eveneens toegelaten wanneer dit noodzakelijk is voor de uitvoering van een opdracht van openbaar belang.

De behandeling van persoonsgegevens is eveneens steeds mogelijk met de instemming van de betrokken

CHAPITRE II

Champ d'application

Art. 139

Le traitement de données à caractère personnel par l'OCAM est actuellement réglé par la LVP. Cette loi exclut l'application de certains articles à ces services et notamment de certains droits et obligations des personnes concernées. Vu que la "sécurité nationale" est exclue du champ d'application du Règlement, une règlementation séparée est nécessaire pour le traitement des données par l'OCAM. Ce régime est inspiré de la LVP et répond aux normes de la Convention 108.

L'alinéa premier précise le champ d'application du sous-titre. Il s'agit des traitements effectués dans le cadre des missions légales de l'OCAM. Ces missions découlent de la loi du 10 juillet 2006 relative à l'analyse de la menace, ainsi que d'autres bases légales particulières. L'alinéa 2 précise que les autres titres ne s'appliquent pas aux traitements des données à caractère personnel par l'OCAM. Le sous-titre 4 couvre l'ensemble des dispositions applicables à l'OCAM dans son traitement de données à caractère personnel dans l'exercice de ses missions légales (droits, obligations, archivage, contrôle, …). L'application d'autres titres de la présente loi à l'exception de certaines dispositions pénales et finales ne se justifie donc pas.

CHAPITRE III

Conditions générales du traitement

Art. 140

Cet article décrit les cas dans lesquels le traitement de données à caractère personnel est légitime.

Ces cas sont ceux qui étaient repris à l'article 3, § 4, LVP. Ainsi, l'OCAM peut traiter des données à caractère personnel si cela est utile pour l'exercice de ses missions prévues dans la loi du 10 juillet 2006, pour l'exécution d'un contrat ou pour d'autres obligations. Un traitement de données à caractère personnel est également autorisé s'il est nécessaire pour l'exécution d'une mission d'intérêt public.

Le traitement de données à caractère personnel est également toujours possible avec l'accord de la

persoon, op voorwaarde dat de toestemming vrij en geïnformeerd is zoals de rechtspraak bepaalt.

Art. 141

Iedere verwerking van persoonsgegevens dient rechtmatig en eerlijk te geschieden met het oog op specifieke, vastgestelde doeleinden. De betrokkenen moeten kennis kunnen nemen van de regels, waarborgen en rechten in verband met de verwerking van hun persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot de verwerking kunnen uitoefenen.

De specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt dienen welbepaald, expliciet en legitiem te zijn. De persoonsgegevens dienen niet verder te worden verwerkt op een wijze die onverenigbaar is met deze doeleinden. Er wordt verduidelijkt dat verdere verwerking voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd wordt.

De persoonsgegevens dienen toereikend, ter zake dienend en niet overmatig te zijn voor de doeleinden waarvoor zij worden verwerkt.

De persoonsgegevens dienen nauwkeurig te zijn. De onjuiste persoonsgegevens dienen verbeterd of verwijderd te worden. Deze beginselen zijn overgenomen uit artikel 5 van het Verdrag 108 en artikel 4 WVP.

Wat betreft de bewaring van de gegevens, worden de modaliteiten in 164 tot 169 bepaald.

HOOFDSTUK IV

Aard van de persoonsgegevens

Art. 142

Dit artikel laat het OCAD toe om persoonsgegevens te verwerken die gevoelig zijn vanwege hun aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of geaardheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen.

personne concernée pour autant que le consentement soit libre et éclairé tel que la jurisprudence le prévoit.

Art. 141

Chaque traitement de données à caractère personnel doit être effectué licitement et loyalement, en lien avec des finalités spécifiques et déterminées. Les personnes concernées doivent pouvoir prendre connaissance des règles, garanties et droits en lien avec le traitement de leurs données à caractère personnel, ainsi que de la manière dont elles peuvent exercer leurs droits relatifs au traitement.

Les finalités spécifiques pour lesquelles les données à caractère personnel sont traitées doivent être déterminées, explicites et légitimes. Les données ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités. Il est précisé qu'un traitement ultérieur à des fins historiques, scientifiques ou statistiques n'est pas réputé incompatible.

Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

Les données à caractère personnel doivent être exactes. Les données inexactes doivent être rectifiées ou effacées. Ces principes sont repris de l'article 5 de la Convention 108 et de l'article 4 LVP.

En ce qui concerne la conservation des données, les modalités sont fixées aux articles 164 à 169.

CHAPITRE IV

Nature des données à caractère personnel

Art. 142

Cet article autorise l'OCAM à traiter des données à caractère personnel qui sont sensibles de par leur nature, notamment celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

Deze uitzondering was voor het OCAD reeds voorzien in de WVP (artikel 3, § 4). Hoewel deze verwerking in principe verboden is, voorziet het Verdrag 108 in haar artikel 9, § 2, een uitzondering op het verbod deze gegevens te verwerken in het belang van de nationale veiligheid indien dit uitdrukkelijk voorzien is in een wet, wat de bestaansreden is van dit artikel. Deze mogelijkheid om gevoelige gegevens te verwerken wordt gerechtvaardigd door het feit dat het OCAD in staat moeten zijn om elk type gegeven, zonder onderscheid, te verwerken om te kunnen anticiperen op elke bedreiging van de nationale veiligheid.

Zo kunnen bijvoorbeeld politieke, godsdienstige of levensbeschouwelijke overtuigingen belangrijke indicatoren vormen voor het inschatten van de bedreiging die een persoon kan vormen voor de nationale veiligheid, onder andere als indicator voor radicalisering. Biometrische gegevens laten dan weer een formele identificatie toe van vreemdelingen wanneer hun identiteitsdocumenten niet betrouwbaar zijn. Gegevens betreffende ras en etniciteit maken het mogelijk om lidmaatschap tot welbepaalde groeperingen te bepalen en bepaalde fenomenen te onderzoeken die een bedreiging vormen voor de nationale veiligheid.

Eender welk gegeven kan nuttig zijn op elk moment. Het OCAD moet elk type van gegeven kunnen verwerken zonder beperkingen om naar best vermogen hun opdrachten te kunnen uitvoeren, dit met naleving van het principe van proportionaliteit en met onderwerping aan een diepgaande controle.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 143

Voor de bewaring van de persoonsgegevens verwijst dit artikel naar de wet van 10 juli 2006 en de wet op het politieambt.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 144

Dit algemeen principe, met name dat elke natuurlijke persoon recht heeft op de bescherming van zijn persoonsgegevens, is overgenomen van artikel 2 WVP.

Cette possibilité pour l'OCAM de traiter ces données était déjà adoptée par la LVP (article 3, § 4). La Convention 108 autorise d'ailleurs dans son article 9, § 2, une exception à l'interdiction de traiter ces données dans l'intérêt de la sécurité nationale si elle est expressément prévue dans une loi, raison d'être de cet article. Cette possibilité de traiter des données sensibles est justifiée par le fait que pour anticiper toute menace contre la sécurité nationale, l'OCAM doit pouvoir collecter tout type de données, sans distinction.

Par exemple, les opinions politiques, les convictions religieuses ou philosophiques peuvent former des indicateurs importants pour l'évaluation de la menace qu'une personne peut former pour la sécurité nationale, par exemple un indicateur de radicalisation. Les données biométriques permettent l'identification formelle des étrangers là où leurs documents d'identité ne sont pas fiables. Les données sur la race et l'ethnie permettent de déterminer l'appartenance à certains groupes et d'étudier certains phénomènes présentant une menace pour la sécurité nationale.

N'importe quelle donnée peut être nécessaire à tout moment. L'OCAM doit pouvoir traiter tout type de données sans limitation pour pouvoir exercer au mieux leurs missions, en respectant bien entendu l'exigence de proportionnalité et en étant soumis à un contrôle approfondi.

CHAPITRE V

Conservation des données à caractère personnel

Art. 143

Pour la conservation des données à caractère personnel, cet article renvoie à la loi du 10 juillet 2006 et la loi sur la fonction de la police.

CHAPITRE VI

Droits de la personne concernée

Art. 144

Ce principe général, à savoir que toute personne physique a droit au respect de sa vie privée, est repris de l'article 2 LVP.

Art. 145

Dit artikel bevat een opsomming van de rechten van de persoon wiens gegevens verwerkt worden door het OCAD. De uitoefening van deze rechten wordt verder uitgewerkt in de artikelen 148 en 149. Het Verdrag 108 voorziet in diens artikelen 8 en 9 dat er uitzonderingen mogelijk zijn op het recht op informatie, rectificatie en vergetelheid van de betrokkene, indien de wet hierin voorziet en het om een maatregel gaat die in een democratische samenleving noodzakelijk is ten behoeve van de bescherming van de veiligheid van de staat. Deze uitzonderingen werden al vastgelegd in artikel 3, § 4, WVP.

Art. 146

Om de discretie van de onderzoeken van de ondersteunende diensten van het OCAD te vrijwaren, is de toegang van de betrokken persoon tot zijn persoonsgegevens beperkt. In overeenstemming met de rechtspraak van het Europees Hof van de Rechten van de Mens, voorziet artikel 2, § 3, van de wet van 30 november 1998 in een systeem van beperkte kennisgeving aan betrokkene.

Art. 147

Op vraag van de burger controleert de bevoegde toezichthoudende autoriteit de rechtmatigheid van de gegevensverwerking door het OCAD. Na controle deelt de toezichthoudende autoriteit aan de betrokkene mee dat de nodige verificaties werden verricht. Indien nodig gaan het OCAD over tot de verbetering of verwijdering van onjuiste of niet-pertinente gegevens. De procedure wordt verder uitgewerkt in de wet.

Art. 148

Deze bepaling stelt dat het OCAD geen besluit mag nemen met negatieve of ingrijpende rechtsgevolgen voor de betrokkene, voor zover dit gebeurt louter op grond van een geautomatiseerde verwerking die bedoeld is om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid. Dit verbod geldt niet indien dergelijke verwerking door of krachtens een wet wordt toegelaten of indien dit noodzakelijk is voor redenen van zwaarwegend openbaar belang, zoals de veiligheid van de Staat.

Wat betreft de besluiten, is het de norm dat het OCAD in principe geen besluiten nemen met directe rechtsgevolgen voor de burgers. De voornaamste rol van het

Art. 145

Cet article contient une énumération des droits de la personne dont les données sont traitées par l'OCAM. Les modalités d'exercice de ces droits sont précisées dans les articles 148 et 149. La Convention 108 prévoit en ses articles 8 et 9 combinés que des exceptions aux droits de la personne concernée à l'information, à la rectification et à l'effacement sont possibles, pour autant qu'elles soient prévues par la loi et qu'il s'agisse de mesures nécessaires dans une société démocratique à la protection de la sécurité de l'État. Ces exceptions étaient déjà établies dans l'article 3, § 4, LVP.

Art. 146

Pour assurer la discrétion des enquêtes des services d'appui de l'OCAM, l'accès par la personne concernée à ses données à caractère personnel est limité. L'article 2, § 3, de la loi du 30 novembre 1998 prévoit un système de notification limitée à l'intéressé, conformément à la jurisprudence de la Cour européenne des droits de l'homme.

Art. 147

L'autorité de contrôle compétente vérifie, à la demande de la personne concernée, la licéité du traitement des données par l'OCAM. Après contrôle, l'autorité de contrôle communique à celle-ci que les vérifications nécessaires ont été faites. Si nécessaire, l'OCAM procède à la correction ou l'effacement des données inexactes ou non pertinentes. Les modalités de la procédure sont précisées dans la loi.

Art. 148

Cette disposition prescrit que l'OCAM ne peut prendre aucune décision produisant des effets juridiques dommageables ou lourds de conséquence pour la personne concernée, sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects de sa personnalité. Cette interdiction ne s'applique pas lorsqu'un tel traitement est autorisé par ou en vertu d'une loi ou lorsqu'il est nécessaire en raison d'un intérêt public important, tel que la sécurité de l'État.

Au sujet des décisions, la règle est que l'OCAM ne prend en principe pas de décisions ayant des effets juridiques directs à l'égard des citoyens. Le rôle principal

OCAD is het informeren van de overheidsinstanties, in hoofdzaak naar aanleiding van terroristische of extremistische dreigingen uitgaande van individuen, voor zover deze dreigingen gelinkt zijn aan de opdrachten van de geïnformeerde instanties. Het zijn deze bevoegde overheidsinstanties die de nodige besluiten nemen (bijvoorbeeld de Dienst Vreemdelingenzaken).

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 149

Dit artikel bepaalt de verplichtingen van de verwerkingsverantwoordelijke van het OCAD. Hij moet waken over de juistheid van de persoonsgegevens. Hij moet ook zorgen dat voor de personen die onder hun gezag handelen, de toegang tot de gegevens beperkt blijft tot wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst. Het OCAD ziet erop toe dat personen die onder hun gezag handelen kennis hebben van de verplichtingen en voorschriften die hen door deze titel worden opgelegd.

Deze verplichtingen zijn conform de verplichtingen voor de verantwoordelijke van de verwerking vervat in artikel 16, § 2, 1°, WVP, met een kleine aanpassing om de tekst in overeenstemming te brengen met artikel 9 van de wet 10 juli 2006.

Art. 150

Het gaat over een overname van artikel 16, § 2, WVP. Voor de bescherming van de rechten van betrokkenen en om de verantwoordelijkheid en aansprakelijkheid van het OCAD en hun verwerkers te bepalen, is het noodzakelijk dat verantwoordelijkheden op duidelijke wijze worden vastgesteld wanneer een verwerking namens het OCAD wordt uitgevoerd.

De verwerkingsverantwoordelijke moet een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking. De uitvoering van een verwerking door een verwerker dient te worden geregeld door een overeenkomst die de verwerker bindt aan de verwerkingsverantwoordelijke, en

de l'OCAM est d'informer les autorités publiques, essentiellement, à propos de menaces terroristes ou extrémistes véhiculées par des individus, dès lors que ces menaces ont un lien avec les missions des autorités averties. Ce sont ces autorités publiques compétentes qui prennent les décisions qui s'imposent (par exemple l'Office des étrangers).

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 149

Le présent article détermine certaines obligations pour le responsable du traitement de l'OCAM. Il doit veiller à la justesse des données à caractère personnel. Il doit également veiller à ce que, pour les personnes agissant sous leur autorité, l'accès aux données soit limité à ce qui est utile pour l'exercice de leurs fonctions ou pour les besoins du service. L'OCAM fait également en sorte que les personnes agissant sous leur autorité aient connaissance des obligations et prescriptions qui leur sont imposées par le présent titre.

Ces obligations sont conformes à celles du responsable du traitement contenues dans l'article 16, § 2, 1°, LVP, avec une petite adaptation pour rendre le texte conforme à l'article 9 de la loi du 10 juillet 2006.

Art. 150

Il s'agit d'une reprise de l'article 16, § LVP. Pour la protection des droits des personnes concernées et pour déterminer les responsabilités de l'OCAM et celles des sous-traitants, il est nécessaire que des responsabilités soient fixées de manière claire quand un traitement est effectué au nom de l'OCAM.

Le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements. L'exécution d'un traitement par un sous-traitant doit être réglée par un accord qui lie le sous-traitant au responsable du traitement et dans lequel il est notamment fixé que le sous-traitant agit

waarin met name is bepaald dat de verwerker uitsluitend op instructie van het OCAD dient te handelen, dat hij de voorziene technische beveiligingsmaatregelen naleeft en dat hij door dezelfde verplichtingen als deze van het OCAD is gebonden.

Deze overeenkomst bepaalt ook de verantwoordelijkheden van de verwerker.

Art. 151

Dit artikel legt aan de verwerker dezelfde verplichtingen op als deze waartoe de verwerkingsverantwoordelijken zijn gehouden. Gelet op de opdrachten van het OCAD en de gevoeligheid van sommige persoonsgegevens, mag de verwerker de verwerking niet aan een andere verwerker doorgeven zonder de uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Art. 152

Dit artikel is een overname van artikel 16, § 3, WVP. Een verwerker of eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker zelf verwerkt de persoonsgegevens slechts in opdracht van de verwerkingsverantwoordelijke, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 153

Wanneer meerdere verwerkingsverantwoordelijken worden aangesteld voor éénzelfde verwerking, worden zij de gezamenlijke verwerkingsverantwoordelijken genoemd. Dit artikel beoogt de hypothese waarbij er meerdere verwerkingsverantwoordelijken voor één persoonsgegevensbank zijn, waarin verwerkingen van het OCAD vervat zijn. De verplichtingen van de verwerkingsverantwoordelijken ten aanzien van de betrokkenen en de mededeling van gegevens, zijn in het algemeen gedefinieerd door of krachtens de wet. Gezien er in dit geval meerdere verwerkingsverantwoordelijken zijn, moeten hun respectievelijke verplichtingen gepreciseerd worden. Indien dit niet voorzien is door of krachtens de wet, biedt dit artikel de mogelijkheid om de verplichtingen vast te leggen in een akkoord. Voor het gemak van de betrokkenen kan in het akkoord één contactpunt aangewezen worden voor de verschillende verwerkingsverantwoordelijken.

exclusivement sur instruction de l'OCAM, qu'il respecte les mesures de sécurité techniques prévues et qu'il est tenu aux mêmes obligations que l'OCAM.

Cet accord détermine aussi les responsabilités du sous-traitant.

Art. 151

Cet article impose au sous-traitant les mêmes obligations que celles qui incombent aux responsables de traitement. Vu les missions de l'OCAM et la sensibilité de certaines données à caractère personnel, le sous-traitant ne peut pas confier le traitement à un autre sous-traitant sans l'autorisation expresse du responsable du traitement.

Art. 152

Cet article est une reprise de l'article 16, § 3, LVP. Un sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant lui-même ne traite des données à caractère personnel que sur instruction du responsable du traitement, sauf en cas d'obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 153

Lorsque plusieurs responsables du traitement sont désignés pour un même traitement, on appelle ceux-ci responsables conjoints du traitement. Cet article vise l'hypothèse où il y a plusieurs responsables du traitement pour une banque de données à caractère personnel, dans laquelle il y a des traitements de l'OCAM. De manière générale, les obligations des responsables du traitement à l'égard des personnes concernées et de la communication des données sont définies par ou en vertu de la loi. Compte tenu qu'en l'espèce, il y a plusieurs responsables du traitement, il faut que leurs obligations respectives soient précisées. Si ce n'est pas prévu par ou en vertu de la loi, cet article permet que ces obligations respectives soient définies dans un accord. Pour la facilité des personnes concernées, l'accord peut aussi désigner un seul point de contact pour les différents responsables du traitement.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 154

Dit artikel herneemt artikel 16, § 4, WVP. Het vermeldt de passende technische en organisatorische maatregelen die de verwerkingsverantwoordelijke moet treffen. Dit artikel stelt dat er hierbij steeds een belangenafweging gemaakt wordt. Zo worden de stand van de techniek (technologische evoluties), de kosten van de toe te passen maatregelen, de aard van de te beveiligen gegevens en de mogelijke risico's mee in overweging genomen om het passende karakter van de maatregelen vast te stellen.

Om de wettelijke verplichtingen van haar ondersteunende diensten, onder meer inzake het beschermen van bronnen en de derden die hun medewerking verlenen, van de identiteit van de agenten en van de inlichtingenonderzoeken te waarborgen, is het cruciaal voor het OCAD dat de technische en organisatorische maatregelen op deze verplichtingen aansluiten. Daarnaast bepaalt artikel 6 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging dat de personeelsleden van het OCAD toegang hebben tot de ingewonnen en verwerkte persoonsgegevens, voor zover deze nuttig zijn voor hun opdracht.

Art. 155

Om het toezicht op het OCAD daadkrachtiger te maken, voert dit artikel een nieuwe verplichting in voor de verwerkingsverantwoordelijke.

Zo moet de verwerkingsverantwoordelijke zo snel mogelijk haar toezichthoudende autoriteit, op de hoogte brengen indien er een inbreuk op de beveiliging plaatsvindt die een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Er is echter geen sprake van een kennisgeving aan de betrokkene, gezien dit in het belang van de uitvoering van de opdrachten van het OCAD niet mogelijk is. Het beschermen van de nationale veiligheid laat het uitblijven van deze kennisgeving toe.

De verwerker moet elke inbreuk op de beveiliging melden aan de verwerkingsverantwoordelijke die het risico voor de rechten en vrijheden van personen zal beoordelen. Opnieuw is er hier echter geen sprake van een kennisgeving aan de betrokkene.

Section 3

Sécurité des données à caractère personnel

Art. 154

Cet article reprend l'article 16, § 4, LVP. Il mentionne les mesures techniques et organisationnelles adéquates que le responsable du traitement doit prendre. Cet article suppose toujours une mise en balance des intérêts. Ainsi, l'état de la technique (les progrès technologiques), les coûts des mesures à appliquer, la nature des données à protéger et les risques encourus doivent être pris en considération pour déterminer le caractère adéquat des dispositions à prendre.

Il est crucial pour les services d'appui de l'OCAM, que les mesures techniques et organisationnelles de ces services d'appui correspondent à leurs obligations légales en matière de, entre autre, la protection de sources, des tiers qui lui prêtent leur concours, de l'identité de ses agents et des enquêtes de renseignement. Par ailleurs, l'article 6 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace que les membres de personnel n'ont accès aux données à caractère personnel recueillies et traitées que pour autant qu'elles soient utiles à l'exécution de leur mission.

Art. 155

Cet article introduit une nouvelle obligation à charge du responsable du traitement afin de rendre plus efficace le contrôle exercé sur eux.

Le responsable du traitement doit dans les meilleurs délais mettre au courant son autorité de contrôle, d'une brèche de sécurité si elle recèle un risque élevé pour les droits et libertés de personnes physiques. Par contre, il n'est pas question d'une notification à la personne concernée, vu que ce n'est pas possible dans l'intérêt de l'exercice des missions de l'OCAM. La protection de la sécurité nationale permet l'omission de cette notification.

Le sous-traitant doit notifier toute brèche de sécurité au responsable du traitement qui évaluera le risque pour les droits et libertés des personnes. Ici non plus il n'est pas question de notification à la personne concernée.

Afdeling 4

Registers

Art. 156

Eveneens om een meer doeltreffend toezicht toe te laten, introduceert dit artikel een nieuwe verplichting voor de verwerkingsverantwoordelijke van het OCAD. Deze dienen een register bij te houden van hun gegevensbanken en van deze die hen ter beschikking worden gesteld. De keuze werd gemaakt om het bijhouden van een register van gegevensbanken op te leggen en niet van de verwerkingsactiviteiten. Deze keuze wordt verantwoord door het feit dat de gegevensbanken het resultaat van het geheel van de verwerkingsactiviteiten door het OCAD inhoudt (behalve wanneer het gegeven niet werd ingegeven of verwijderd wegens niet pertinent). Omgekeerd is het moeilijk om de verschillende verwerkingsactiviteiten van het OCAD op te sommen aangezien deze praktisch enkel gegevensverwerking doet en al zijn activiteiten verweven is.

Het register moet geclassificeerd zijn in de zin van de wet van 11 december 1998.

Dit artikel somt de informatie op die vermeld moet worden in het register. Voor de gegevensbanken van het OCAD werden dezelfde vermeldingen als die uit het artikel 30 van de Verordening hernomen, met uitzondering van de categorieën van personen en categorieën van persoonsgegevens, zonder onderscheid. Wat betreft de gegevensbanken waartoe het OCAD toegang heeft, zijn de vermeldingen gelimiteerd aangezien alle informatie vervat in deze banken zich bevinden in de registers bijgehouden door de verantwoordelijke van de verwerking van voornoemde banken. Indien het om een gegevensbank in het buitenland gaat, is het overigens mogelijk dat het OCAD niet over de precieze contactgegevens van de verwerkingsverantwoordelijke beschikt. Om deze reden is de vermelding van deze contactgegevens onderworpen aan de voorwaarde dat deze gekend zijn.

De verwerker heeft eveneens de verplichting om een geclassificeerd register met alle categorieën van verwerkingsactiviteiten, uitgevoerd voor rekening van het OCAD, bij te houden. Het register heeft hier wel betrekking op de verwerkingsactiviteiten aangezien de opdracht die werd toevertrouwd aan een verwerker steeds betrekking heeft op de een of andere gepreciseerde activiteit. Integendeel, de categorieën van personen of gegevens kunnen niet op voorhand bepaald worden vermits zij slechts gekend zullen worden op het moment van de verwerking (bijvoorbeeld een onderzoek in open bronnen, een analyse van een fenomeen op

Section 4

Registres

Art. 156

Pour permettre un contrôle plus efficace, cet article introduit une nouvelle obligation dans le chef du responsable du traitement de l'OCAM. Ceux-ci doivent tenir un registre de leurs banques de données et de celles mises à leur disposition. Il a été fait le choix d'imposer la tenue d'un registre portant sur les banques de données et non sur les activités de traitement. Ce choix est motivé par le fait que les banques de données contiennent le résultat de l'ensemble des activités de traitement de l'OCAM (sauf si la donnée n'est pas introduite ou est effacée pour cause de non pertinence). A l'inverse, il est difficile d'énumérer différentes activités de traitement de l'OCAM puisque celui-ci ne fait pratiquement que du traitement de données à caractère personnel et que tous ses activités sont indissociables.

Le registre doit être classifié au sens de la loi du 11 décembre 1998.

Cet article énumère les informations qui doivent être mentionnées dans le registre. Pour les banques de données de l'OCAM, les mêmes mentions que celles prévues à l'article 30 du Règlement sont reprises, à l'exception des catégories de personnes concernées et des catégories de données à caractère personnel. Pour les banques de données auxquelles l'OCAM a accès, les mentions sont limitées car toutes les informations portant sur ces banques se trouvent dans le registre tenu par le responsable du traitement desdites banques. Par ailleurs, s'il s'agit d'une banque de données à l'étranger, il est possible que l'OCAM ne dispose pas des coordonnées exactes du responsable du traitement. Pour cette raison, l'indication de ces coordonnées est soumise à la condition de les connaître.

Le sous-traitant a également l'obligation de tenir un registre classifié de toutes les catégories d'activités de traitement effectuées pour le compte de l'OCAM. Le registre porte ici sur les activités de traitement car la mission confiée au sous-traitant portera toujours sur l'une ou l'autre activité précise. Par contre, les catégories de personnes ou de données ne peuvent pas être déterminées à l'avance puisqu'elles ne seront connues qu'à l'issue du traitement (par exemple une recherche dans les sources ouvertes, une analyse d'un phénomène sur les média sociaux). Aucun destinataire n'est mentionné car c'est le service concerné, et non

sociale media). Geen enkele bestemmeling wordt vermeld aangezien het de betrokken dienst is, en niet de verwerker, die de verzamelde gegevens zal doorgeven.

De derde paragraaf voorziet een schriftelijke vorm, met inbegrip van elektronische vorm, voor het register.

De vierde paragraaf bepaalt dat de registers ter beschikking worden gesteld op vraag van de bevoegde toezichthoudende autoriteit. Het register van de verwerker wordt steeds ter beschikking gesteld van de verwerkingsverantwoordelijke.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 157

Dit artikel legt de aanduiding van een functionaris voor gegevensverwerking op door de verwerkingsverantwoordelijke en, in voorkomend geval de verwerker. Deze moet titularis zijn van een veiligheidsmachtiging zeer geheim want de inlichtingendiensten, ondersteunende diensten van het OCAD, kunnen classificeren tot en met dit niveau. Hij mag niet worden ontzet uit zijn functies omwille van de uitvoering van zijn opdrachten.

Zijn functie herneemt deze van de raadgever informatieveiligheid vervat in artikel 4 van het Koninklijk Besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 en wordt uitgebreid. De functionaris wordt betrokken bij alle vragen betreffende de bescherming van persoonsgegevens.

Hij oefent zijn functie in volledige onafhankelijkheid uit en moet beschikken over de nodige middelen. De Koning kan indien nodig, andere modaliteiten voor de werking vastleggen en de bevoegdheden van de functionaris uitbreiden.

le sous-traitant, qui transmettra éventuellement les renseignements collectés.

Le paragraphe 3 prévoit une forme écrite, y compris la forme électronique pour le registre.

Le paragraphe 4 dispose que les registres sont mis à la disposition de l'autorité de contrôle compétente à sa demande. Le registre du sous-traitant est en permanence mis à la disposition du responsable du traitement.

Section 5

Délégué à la protection des données

Art. 157

Cet article impose la désignation d'un délégué à la protection des données par le responsable du traitement, et le cas échéant, par le sous-traitant. Celui-ci doit être titulaire d'une habilitation de sécurité du niveau très secret car les services de renseignement, qui sont des services d'appui de l'OCAM, peuvent classifier jusqu'à ce niveau. Il ne peut être relevé de ses fonctions en raison de l'exercice de ses missions.

Sa fonction reprend celle du conseiller en sécurité de l'information visé à l'article 4 de l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique et est étendue. Le délégué doit être associé à toutes les questions relatives à la protection des données à caractère personnel.

Il exerce ses fonctions en toute indépendance et doit disposer des ressources nécessaires. Le Roi peut fixer, si nécessaire, d'autres modalités de fonctionnement et étendre les compétences du délégué.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van gegevens aan de publieke sector en de privésector

Art. 158

De uitwisseling van gegevens tussen het OCAD, en de publieke en private sector wordt geregeld in de artikelen 8, 9, 10, 11 en 12 van de wet van 10 juli 2006 en onderafdeling 7*bis* van de wet op het politieambt. Betrokken bepalingen bevatten de wettelijke modaliteiten voorde informatie-uitwisseling in dit kader.

Dit artikel bepaalt ook dat een raadpleging van de functionaris voor gegevensbescherming of de bevoegde toezichthoudende autoriteit of een impactanalyse geen voorafgaande vereiste kunnen zijn voor de mededeling van informatie. De gegevensuitwisseling met het OCAD, welke een loutere toepassing is van de artikelen 8, 9, en 10, 11 en 12 van de wet van 10 juli 2006 en onderafdeling 7*bis* van de wet op het politieambt. Als er overgegaan wordt tot een beoordeling van de belangen, dan spreekt voor zich dat de opdrachten tot nationale veiligheid waarmee het OCAD belast is van hoger belang zijn dan andere belangen, voor zover ze een collectief belang beschermen en geen individuele belangen. De uitzondering van artikel 23 van de Verordening op de impactanalyse is bovendien een toepassing van de uitzondering in artikel 35.10 van de Verordening: *"Wanneer verwerking uit hoofde van artikel 6, lid 1, onder c) of e), haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is, de specifieke verwerking of geheel van verwerkingen in kwestie daarbij wordt geregeld, en er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een gegevensbeschermingseffectbeoordeling is uitgevoerd, zijn de leden 1 tot en met 7 niet van toepassing, tenzij de lidstaten het noodzakelijk achten om voorafgaand aan de verwerkingen een dergelijke beoordeling uit te voeren.".*

Dit weerhoudt een overheidsinstantie of een particulier orgaan er logischerwijs niet van om een protocolakkoord te sluiten met het OCAD of om het advies van de functionaris voor gegevensbescherming of van de bevoegde toezichthoudende autoriteit te vragen of een impactanalyse, maar dit mag geen voorafgaande

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données avec le secteur public et le secteur privé

Art. 158

L'échange de données entre les services de renseignement et de sécurité et les secteurs public et privé est réglée aux articles 8, 9, 10, 11 et 12 de la loi du 16 juillet 2006 et la loi sur la fonction de la police. Les dispositions concernées contiennent les modalités légales de l'échange d'informations dans ce cadre.

Le présent article dispose également qu'une consultation du délégué à la protection des données ou de l'autorité de contrôle compétente ou une analyse d'impact ne peuvent pas être exigées comme préalable à la transmission des informations. Les échanges de données avec les services de renseignement étant une simple application des articles 8, 9, 10, 11 de la loi du 16 juillet 2006 et la loi sur la fonction de la police. Lorsque l'on procède à une appréciation des intérêts en présence, il va de soi que les missions de sécurité nationale dont est chargé l'OCAM constituent un intérêt supérieur à d'autres intérêts, dans la mesure où elles protègent un intérêt collectif et non des intérêts individuels. L'exception à l'article 23 du Règlement sur l'analyse d'impact est d'ailleurs une application de l'exception visée à l'article 35.10 du Règlement: *"Lorsque le traitement effectué en application de l'article 6, paragraphe 1er, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.".*

Cela n'empêche évidemment pas l'autorité publique ou l'organisme privé de conclure un protocole d'accord avec l'OCAM ou de demander l'avis de son délégué à la protection des données ou de l'autorité de contrôle compétente ou de procéder à une analyse d'impact, mais le résultat de ces consultations ne peut pas être

voorwaarde voor de informatie-uitwisseling zijn die er toe kan leiden dat de mededeling van belangrijke informatie die gericht is een zwaarwegender belang te beschermen vertraagd wordt.

Afdeling 2

Doorgifte van gegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 159

Het eerste en tweede lid van dit artikel zijn een exacte reproductie van de eerste paragraaf van artikel 21 WVP. Zij hernemen het criteria van het adequate beschermingsniveau dat de niet-lidstaat van de Europese Unie moet waarborgen opdat het OCAD persoonsgegevens mag doorgeven. Enkel de termen "internationale organisatie" wordt toegevoegd omdat een internationale organisatie eveneens de bestemmeling kan zijn van persoonsgegevens. De derde alinea bepaalt dat het adequaat beschermingsniveau gewaarborgd kan worden door veiligheidsclausules waarop het OCAD en de bestemmeling zich afstemmen. Dit lid herneemt de idee van alinea 2 van artikel 22 WVP.

Art. 160

Dit artikel voorziet uitzonderingen op de vereiste van een adequaat beschermingsniveau:

— na instemming van de betrokkene (kopij van artikel 22, 1°, WVP);

— indien de doorgifte noodzakelijk of wettelijk verplicht is voor de bescherming van de fysieke integriteit van een persoon of van een belangrijk openbaar belang (fusie van 4° en 5°, WVP);

— indien de doorgifte noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend openbaar belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 161

Overeenkomstig artikel 10 van de wet van 10 juli 2006 worden het Vast Comité van Toezicht op de inlichtingendiensten, in zijn hoedanigheid van onafhankelijke

une condition préalable à l'échange d'informations qui serait susceptible de retarder la transmission d'une information dont le besoin peut être urgent et qui vise à protéger un intérêt supérieur et collectif.

Section 2

Transfert des données vers des pays non membres de l'Union européenne ou à des organisations internationales

Art. 159

Les alinéas premier et 2 du présent article sont l'exacte reproduction du paragraphe premier de l'article 21 LVP. Ils reprennent le critère du niveau de protection adéquat que doit assurer le pays non membre de l'Union européenne pour que l'OCAM puisse lui transférer une donnée à caractère personnel. Seuls les termes "organisation internationale" ont été ajoutés puisqu'une organisation internationale peut également être le destinataire de données à caractère personnel. Le troisième alinéa fixe que le niveau de protection adéquat peut être assuré par des clauses de sécurité sur lesquelles s'accordent l'OCAM et le destinataire. Cet alinéa reprend l'idée de l'alinéa 2 de l'article 22 LVP.

Art. 160

Cet article prévoit des exceptions à l'exigence d'un niveau de protection adéquat:

— avec le consentement de la personne concernée (copie de l'article 22, 1°, LVP);

— si le transfert est nécessaire ou légalement obligatoire à la sauvegarde de l'intégrité physique d'une personne ou d'un intérêt public important (fusion des 4° et 5°, de l'article 22 LVP);

— si le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

CHAPITRE X

Autorité de contrôle

Art. 161

Conformément à l'article 10 de la loi du 10 juillet 2006, le Comité permanent R, en sa qualité d'autorité publique indépendante, et le Comité permanant de Contrôle des

publieke autoriteit, en het Vast Comité van Toezicht op de politiediensten, aangeduid als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens door het OCAD en zijn verwerkers volgens de nadere regels vastgelegd in de wet van 18 juli 1991.

In overeenstemming met artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging, wordt een instantie opgezet onder de naam "Coördinatieorgaan voor de dreigingsanalyse", hierna "OCAD" genoemd, verantwoordelijk voor de dreigingsbeoordeling overeenkomstig artikelen 3 en 4 van dezelfde wet. Dit orgaan staat onder het gezamenlijke gezag van de ministers van Justitie en van Binnenlandse Zaken. Behalve de uitzonderingen voorzien door deze wet, zijn deze ministers samen verantwoordelijk voor de organisatie en algemene administratie van het OCAD. In dit verband zijn de toezichthoudende autoriteiten van de OCAD daarom de I- en P-comités. Bovendien bepaalt artikel 10, § 4, van de wet van 10 juli 2006 dat tweemaal per jaar een evaluatieverslag van de activiteiten en de strategische doelstellingen van het OCAD wordt voorgelegd aan de Nationale Veiligheidsraad, dat het vervolgens overzendt aan het Vast Comité van Toezicht op de inlichtingendiensten en aan het Vast Comité van Toezicht op de politiediensten.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden

Art. 162

Zoals uiteengezet in de inleiding, is de raadpleging van persoonsgegevens van het OCAD of zijn personeel door een verdere verwerkingsverantwoordelijke voor historische, wetenschappelijke of statistische doeleinden slechts mogelijk indien dit geen weerslag heeft op de opdrachten van het OCAD, en indien dit geen weerslag heeft op een lopend opsporings- of gerechtelijk onderzoek of op de relaties die België onderhoudt met vreemde Staten of internationale organisaties. De behandeling van geclassificeerde documenten moet vanzelfsprekend de bepalingen van de wet van 11 december 1998 respecteren. Deze specifieke reglementering is nodig aangezien een aanvraag tot raadpleging van persoonsgegevens van het OCAD voor historische, wetenschappelijke en statistische doeleinden op elk moment kan gebeuren, zelfs wanneer een onderzoek nog steeds lopende is.

Zelfs indien titel 4 van onderhavige wet niet van toepassing is op het OCAD, is het aangeraden om er

Servcies de police, sont désignés comme autorités de protection des données chargée du contrôle du traitement des données à caractère personnel par l'OCAM et par ses sous-traitants selon les modalités fixées par la loi du 18 juillet 1991.

Suivant l'article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace est institué sous la dénomination "Organe de coordination pour l'analyse de la menace", ci-après dénommé "OCAM", un organe chargé de l'évaluation de la menace conformément aux articles 3 et 4 de la même loi. Cet organe est placé sous l'autorité conjointe des ministres de la Justice et de l'Intérieur. Hormis les exceptions prévues par la présente loi, ces ministres sont chargés ensemble de l'organisation et de l'administration générale de l'OCAM. Dans ce cadre, les autorités de contrôle de l'OCAM sont donc les Comités R et P. Par ailleurs, l'article 10, § 4, de la loi du 10 juillet 2006 stipule que deux fois par an, un rapport d'évaluation des activités et des objectifs stratégiques de l'OCAM est soumis au Conseil national de sécurité qui le transmet ensuite au Comité permanent de Contrôle des services de renseignement et au Comité permanent de Contrôle des Services de police.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 162

Comme expliqué dans l'introduction, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel de l'OCAM et de son personnel par un responsable du traitement ultérieur n'est possible que si elle ne porte pas atteinte aux missions de l'OCAM et ne porte pas atteinte à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales. Le traitement des données classifiées doit bien entendu aussi respecter les dispositions de la loi du 11 décembre 1998. Cette réglementation spécifique est nécessaire car une demande de consultation des données de l'OCAM à des fins historiques, scientifiques ou statistiques peut avoir lieu à tout moment, alors même qu'une enquête est encore en cours.

Même si le titre 4 de la présente loi n'est pas applicable à l'OCAM, il convient d'y faire une dérogation

een expliciete afwijking op te voorzien voor de andere organismen die hun gegevens verwerken alsook deze van hun personeel. Bepaalde persoonsgegevens van de diensten bevinden zich immers bij de Staatsarchieven; hun personeel wordt beheerd door andere algemene secretariaten van hun FOD/Ministerie, …

De gegevens van het personeel van het OCAD zijn beschermd om te vermijden dat de leden van deze diensten druk ondervinden, of zelfs bedreigingen moeten ondergaan omdat hun identiteit en hun hoedanigheid werd onthuld.

De toelating tot raadpleging moet gegeven worden door het OCAD, zelfs indien het gegeven niet meer in haar bezit is, omdat deze het beste kan evalueren of een raadpleging een weerslag kan hebben op één van de te beschermen belangen.

Hiertoe, wanneer de persoonsgegevens van het OCAD overgedragen zijn naar het Algemeen Rijksarchief, dan zou het kunnen dat er een vraag tot raadpleging (latere verwerking) zonder historische, statistische of wetenschappelijke doeleinden gericht wordt aan de algemeen archivist. Die mogelijkheid wordt in acht genomen om desgevallend een vergunning te bekomen buiten de reeds voorziene gevallen, eerder dan een systematische weigering.

Art. 163

Om de aandacht van de gebruiker te vestigen op het bijzondere regime toepasselijk op de verdere verwerking van het gegeven, vereist dit artikel dat dit gegeven gemarkeerd wordt met de vermelding “Bescherming van persoonsgegevens – hoofdstuk XI van titel 3 van de wet van xx/xx/2018”.

Art. 164

Omwille van evidente redenen voor de bescherming van het privéleven, moeten de gegevens anoniem worden gemaakt. Indien dit het niet mogelijk maakt om het doel van de verdere verwerking te bereiken, kan het OCAD pseudonimisering toestaan. De filosofie van dit artikel beantwoord aan wat is voorzien in hoofdstuk II van het Koninklijk Besluit van 13 februari 2001 betreffende de uitvoering van de wet van 8 december 1992. De term pseudonymisering werd toegevoegd als gevolg van de nieuwe Europese reglementering. Indien de anonimisering of de pseudonimisering de identificatie niet onmogelijk maakt, laat de inlichtingendienst slecht een consultatie toe indien er geen disproportionele weerslag is op het privéleven. In dezelfde zin, indien de

expresse pour les autres organismes qui traitent leurs données ainsi que celles de leur personnel. En effet, certaines données à caractère personnel des services se trouvent aux Archives de l’État; la gestion de leur personnel se fait par d’autres directions générales de leur SPF/Ministère, …

Les données du personnel de l’OCAM sont protégées pour éviter que des membres desdits services ne subissent des pressions, voire des menaces car leur identité et qualité sont dévoilées.

L’autorisation de consulter doit émaner de l’OCAM, même si la donnée n’est pas entre ses mains, car c’est lui qui est le plus à même d’évaluer si la consultation est susceptible de porter atteinte à un des intérêts à protéger.

A cet égard, lorsque les données à caractère personnel de l’OCAM sont transférées aux Archives générales du Royaume, il se peut qu’une demande de consultation (traitement ultérieur) sans finalités historiques, statistiques ou scientifiques soit présentée à l’archiviste général. Cette éventualité est prise en considération pour permettre d’obtenir, le cas échéant, une autorisation en dehors des cas déjà prévus, plutôt qu’un refus systématique.

Art. 163

Pour attirer l’attention de l’utilisateur sur le régime particulier applicable à la donnée lors du traitement ultérieur, exige cet article que cette donnée soit marquée de la mention “Protection des données à caractère personnel – chapitre XX du titre XX3 de la loi du xx/xx/2018”.

Art. 164

Pour des raisons évidentes de protection du droit à la vie privée, les données doivent être rendues anonymes. Si cela ne permet pas d’atteindre le but du traitement ultérieur, l’OCAM peut autoriser la pseudonymisation. La philosophie de cet l’article correspond à ce qui était prévu dans le chapitre II de l’arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992. Le terme pseudonymisation est ajouté suite à la nouvelle règlementation européenne. Si l’anonymisation ou la pseudonymisation ne rend pas l’identification impossible, le service de renseignement concerné n’autorise la consultation que si cela ne constitue pas une atteinte disproportionnée à la vie privée. Dans le même sens, si un traitement ultérieur de données pseudonymisées ne

latere verwerking van gepseudonimiseerde gegevens het niet toelaat om de historische, wetenschappelijke of statistische doeleinden te bereiken, kan het OCAD niet-gepseudonimiseerde gegevens toelaten indien er geen disproportionele weerslag is op het privéleven.

Art. 165

Omwille van redenen van bescherming van het privéleven en de belangen in de zin van artikel 164, kan geen enkele communicatie of publicatie van niet-geanonimiseerde en niet-gepseudonimiseerde gegevens plaatsvinden zonder toelating van het OCAD.

Art. 166

Dit artikel legt de verwerkingsverantwoordelijke op een logbestand betreffende de verdere verwerking te bewaren.

Het begrip logbestand dat hier gebruikt wordt beoogt het bijhouden van een lijst concreet uitgevoerde verwerkingen in het kader van latere verwerkingen. Dit begrip differentieert zich van dat in het register elders gebruikt in de kaderwet om elke verwarring te voorkomen.

Naast het logbestand dat wordt bijgehouden door de verantwoordelijke voor de verdere verwerking, moet de Algemene Rijksarchivaris een spoor bij van de raadplegingen uitgevoerd door elke verantwoordelijke voor de verdere verwerking houden.

Dit logbestand is logischerwijze geclassificeerd indien de latere verwerking betrekking heeft op geclassificeerde gegevens.

Dit logbestand helpt identificeren wie doet wat en moet vermelden:

1° de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van hun functionaris voor gegevensbescherming van de laatste;

2° de doeleinden van de verdere verwerking;

3° de gegevens die later verwerkt worden;

4° de eventuele voorwaarden voor de verdere verwerking vastgelegd door het OCAD;

5° de eventuele ontvangers toegestaan door het OCAD.

permet pas d'atteindre les fins historiques, statistiques ou scientifiques, l'OCAM peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 165

Pour des raisons de protection du droit à la vie privée et des intérêts visés à l'article 164, toute communication et toute publication des données consultées non anonymisées et non pseudonymisées ne peuvent avoir lieu qu'avec l'autorisation de l'OCAM.

Art. 166

Cet article impose la tenue d'un journal du traitement ultérieur par le responsable du traitement.

Le terme de journal, utilisé ici, vise la tenue d'une liste des traitements effectués concrètement et sur quelles données, dans le cadre des traitements ultérieurs. Ce terme se différencie de celui de registre utilisé ailleurs dans la loi-cadre pour éviter toute confusion.

A côté du journal tenu par le responsable du traitement ultérieur, l'Archiviste général du Royaume doit également garder une trace des consultations effectuées par chaque responsable du traitement ultérieur.

Ce journal est bien entendu classifié si le traitement ultérieur porte sur des données classifiées.

Ce journal permet d'identifier qui fait quoi et doit mentionner:

1° les coordonnées du responsable du traitement initial, du responsable ultérieur et du délégué à la protection des données de ce dernier;

2° les finalités du traitement ultérieur;

3° les données faisant l'objet du traitement ultérieur;

4° les éventuelles conditions du traitement ultérieur fixées par l'OCAM;

5° les éventuels destinataires autorisés par l'OCAM.

Dit logbestand laat toe de traceerbaarheid van de verdere verwerkingen en in het bijzonder de controle door de bevoegde toezichthoudende autoriteit te vergemakkelijken.

Art. 167

Dit artikel verduidelijkt dat elke persoon die gegevens verwerkt voor historische, wetenschappelijke of statistische doeleinden verantwoordelijk is voor deze verwerking. Dit houdt een verbod in om geanonimiseerde, of gepseudonimiseerde gegevens in persoonsgegevens om te omzetten. Dit verbod is overgenomen van het artikel 6 van het Koninklijk Besluit van 13 februari 2001 houdende uitvoering van de wet van 8 december 1992.

ONDERTITEL 5

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT BEPAALDE VERWERKINGEN VAN PERSOONSGEGEVENS DOOR DE PASSAGIERSINFORMATIE-EENHEID

De wet van 25 december 2016 betreffende de verwerking van passagiersgegevens zet zowel de PNR Richtlijn (Richtlijn 2016/681 van 27 april 2016 van het Europees Parlement en de Raad betreffende het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en zware criminaliteit) om als de API-Richtlijn (Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven).

In artikel 8 van voornoemde wet van 25 december 2016 staat beschreven voor welke doeleinden de passagiersgegevens kunnen verwerkt worden.

De verwerkingen ter verbetering van de grenscontroles en bestrijding van de illegale immigratie, bedoeld in artikel 8, § 2, van voornoemde wet van 25 december 2016, die een omzetting betreft van de API-Richtlijn, worden ingedeeld onder titel 1 van deze wet.

De verwerkingen in het kader van de finaliteiten opgenomen in artikel 8, § 1, 1°, 2°, 3° en 5°, van voornoemde wet van 25 december 2016 worden ingedeeld onder titel 2 aangezien dit verwerkingen betreffen van persoonsgegevens (passagiersgegevens) door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare

Ce journal permet de faciliter la traçabilité des traitements ultérieurs et notamment le contrôle par l'autorité de contrôle compétente.

Art. 167

Cet article précise que toute personne qui traite des données à des fins historiques, scientifiques ou statistiques est responsable dudit traitement. Elle a interdiction de convertir des données anonymes ou pseudonymisées en données à caractère personnel. Cette interdiction est reprise de l'article 6 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992.

SOUS-TITRE 5

DE LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DE CERTAINS TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR L'UNITE D'INFORMATION DES PASSAGERS

La loi du 25 décembre 2016 relative au traitement des données des passagers transpose la Directive PNR (Directive 2016/681 de 27 avril 2016 du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière) ainsi que la Directive API (la Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers).

L'article 8 de la loi précitée du 25 décembre 2016 décrit les finalités pour lesquelles les données des passagers peuvent être traitées.

Les traitements en vue de l'amélioration des contrôles de personnes aux frontières extérieures et en vue de lutter contre l'immigration illégale, visés à l'article 8, § 2, de la loi précitée du 25 décembre 2016, qui constitue une transposition de la Directive API, sont classés sous le titre 1er de la présente loi.

Les traitements dans le cadre des finalités visées à l'article 8, § 1er, 1°, 2°, 3° et 5°, de la loi précitée du 25 décembre 2016 sont classés sous le titre 2 puisqu'il s'agit de traitements de données à caractère personnel (données des passagers) effectués par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la

feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

De verwerkingen in het kader van de finaliteit bedoeld in artikel 8, § 1, 4°, van voornoemde wet van 25 december 2016 worden ingedeeld onder titel 3 daar dit verwerkingen betreffen van persoonsgegevens (passagiersgegevens), uitgevoerd in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten als bedoeld in artikelen 7 en 11 van de wet van 30 november 1998.

Voornoemde wet van 25 december 2016 bevat reeds verscheidene bepalingen inzake gegevensbescherming zoals het aanstellen van een functionaris voor gegevensbescherming, het voorzien van een manuele validatie of het verbod om gevoelige gegevens te verwerken. Bepaalde punten die reeds opgenomen zijn in de wet van 25 december 2016 dienen bijgevolg niet opgenomen worden in de huidige wet.

matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Les traitements dans le cadre de la finalité visée à l'article 8, § 1er, 4°, de la loi précitée du 25 décembre 2016 sont classés sous le titre 3 puisqu'il s'agit de traitements de données à caractère personnel (données des passagers) dans le cadre des missions des services de renseignement et de sécurité visés aux articles 7 et 11 de la loi du 30 novembre 1998.

La loi du 25 décembre 2016 précitée contient plusieurs dispositions concernant la protection des données telles que la désignation d'un délégué à la protection des données, la prévision d'une validation manuelle ou encore l'interdiction de traiter des données sensibles. Certains points déjà repris dans la loi du 25 décembre 2016 ne doivent par conséquent plus être repris dans la présente loi.

HOOFDSTUK I

Definities

Art. 168

De eerste paragraaf verwijst naar de relevante definities voorzien in titel 2. De Raad van State (pagina 36) merkt op dat het noodzakelijk is om de definitie van ontvanger (10°) toe te voegen vanaf het moment dat dit begrip gebruikt wordt in de ondertitel. Het artikel werd in die zin aangepast.

Paragraaf 2 voert hieraan twee definities toe die eigen zijn aan ondertitel 5 en die enkel relevant zijn voor de PIE.

Wat betreft punt 252 van het advies van de Privacycommissie, waarin zij opmerkt dat de verwerkingsverantwoordelijke met name niet aangeduid is in ondertitel 5 terwijl deze wel vermeld is in de wet van 25 december 2016, wordt opgemerkt dat de verwerkingsverantwoordelijke eveneens aangeduid is op een algemene manier voor de verwerkingen uitgevoerd door de PIE in het kader van titel 2 alsook voor de verwerkingen uitgevoerd door de autoriteiten van titel 3. Teneinde de uniformiteit tussen de titels 2 en 3 te verzekeren, is het aldus te verkiezen dat dezelfde definitie behouden wordt door verwijzing te maken naar artikel 26, 8°, van deze wet.

Anderzijds, aangezien als gevolg van punt 250 van het advies van de CBPL gespecifieerd wordt dat de

CHAPITRE IER

Définitions

Art. 168

Le premier paragraphe renvoie aux définitions pertinentes prévues dans le titre 2. Le Conseil d'État (page 36) remarque la nécessité de rajouter la définition de destinataire (10°) dès lors que cette notion est utilisée dans le sous-titre. L'article a été modifié en ce sens.

Le paragraphe 2 ajoute deux notions qui sont propres au sous-titre 5 et qui ne sont pertinentes que pour l'UIP.

Quant au point 252 de l'avis de la Commission vie privée, dans lequel elle remarque que le responsable du traitement n'est pas désigné nommément dans le sous-titre 5 alors qu'il l'est dans la loi du 25 décembre 2016, on fera remarquer que le responsable du traitement est également désigné de manière très générale pour les traitements effectués par l'UIP dans le cadre du titre 2, ainsi que pour les traitements effectués par les autres autorités du titre 3. De manière à assurer une uniformité entre les titres 2 et 3, il est donc préférable d'en garder la même définition, en faisant référence à l'article 26, 8°, de la présente loi.

D'autre part, puisqu'il est précisé dans certains articles, suite au point 250 de l'avis de la Commission

bevoegde toezichthoudende autoriteit het Vast Comité I is, wordt de verwijzing gemaakt naar artikel 72, § 2, 7°, van deze wet, dat “Het Comité I” definieert.

HOOFDSTUK II

Toepassingsgebied

Art. 169

De verwerking van persoonsgegevens door de PIE wordt momenteel geregeld door de wet van 25 december 2016. Het eerste lid verduidelijkt het toepassingsgebied van deze ondertitel. De verwerkingen in het kader van de finaliteit bedoeld in artikel 8, § 1, 4°, van wet van 25 december 2016 worden ingedeeld onder titel 3 daar dit verwerkingen betreffen van persoonsgegevens (passagiersgegevens), in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten als bedoeld in artikelen 7 en 11 van de wet van 30 november 1998.

Het tweede lid verduidelijkt dat de andere titels niet van toepassing zijn op de verwerkingen van persoonsgegevens bedoeld in het eerste lid. De ondertitel 5 omvat het geheel van bepalingen dat van toepassing is op de PIE in het kader van de verwerking van voormelde gegevens. De toepassing van andere titels van deze wet met uitzondering van sommige straf- en slotbepalingen is dus niet te rechtvaardigen.

HOOFDSTUK III

Algemene voorwaarden voor de verwerking

Art. 170

Iedere verwerking van persoonsgegevens dient rechtmatig en eerlijk te geschieden met het oog op specifieke, vastgestelde doeleinden. De betrokkenen moeten kennis kunnen nemen van de regels, waarborgen en rechten in verband met de verwerking van hun persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot de verwerking kunnen uitoefenen.

De specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt dienen welbepaald, expliciet en legitiem te zijn. De persoonsgegevens dienen niet verder te worden verwerkt op een wijze die onverenigbaar is met deze doeleinden.

vie privée, que l’autorité de contrôle compétente est le Comité permanent R, il est fait référence à l’article 72, § 2, 7°, de la présente loi qui définit “le Comité permanent R”.

CHAPITRE II

Champ d’application

Art. 169

Le traitement de données à caractère personnel par l’UIP est actuellement réglé par la loi du 25 décembre 2016. L’alinéa premier précise le champ d’application du sous-titre. Les traitements dans le cadre de la finalité visée à l’article 8, § 1er, 4°, de la loi du 25 décembre 2016 sont classés sous le titre 3 puisqu’il s’agit de traitements de données à caractère personnel (données des passagers) dans le cadre des missions des services de renseignement et de sécurité visés aux articles 7 et 11 de la loi du 30 novembre 1998.

L’alinéa 2 précise que les autres titres ne s’appliquent pas aux traitements des données à caractère personnel visés par l’alinéa premier. Le sous-titre 5 couvre l’ensemble des dispositions applicables à l’UIP dans le cadre du traitement des données précitées. L’application d’autres titres de la présente loi, à l’exception de certaines dispositions pénales et finales, ne se justifie donc pas.

CHAPITRE III

Conditions générales du traitement

Art. 170

Chaque traitement de données à caractère personnel doit être effectué licitement et loyalement, en lien avec des finalités spécifiques et déterminées. Les personnes concernées doivent pouvoir prendre connaissance des règles, garanties et droits en lien avec le traitement de leurs données à caractère personnel, ainsi que de la manière dont elles peuvent exercer leurs droits relatifs au traitement.

Les finalités spécifiques pour lesquelles les données à caractère personnel sont traitées doivent être déterminées, explicites et légitimes. Les données ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.

De persoonsgegevens dienen toereikend, ter zake dienend en niet overmatig te zijn voor de doeleinden waarvoor zij worden verwerkt.

De persoonsgegevens dienen nauwkeurig te zijn. Onjuiste persoonsgegevens dienen verbeterd of verwijderd te worden. Deze beginselen zijn overgenomen uit artikel 5 van het Verdrag 108 en artikel 4 WVP.

Wat betreft de bewaring van de gegevens, worden de modaliteiten in het volgende artikel bepaald.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 171

Voor de bewaring van de persoonsgegevens verwijst dit artikel naar de wet van 25 december 2016.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 172

Dit algemeen principe, met name dat elke natuurlijke persoon recht heeft op de bescherming van zijn persoonsgegevens, is overgenomen van artikel 2 WVP.

Art. 173

Dit artikel bevat een opsomming van de rechten van de persoon wiens gegevens verwerkt worden door de PIE. De uitoefening van deze rechten wordt verder uitgewerkt in artikel 174.

Het Verdrag 108 voorziet in diens artikelen 8 en 9 dat er uitzonderingen mogelijk zijn op het recht op informatie, rectificatie en vergetelheid van de betrokkene, voor zover de wet hierin voorziet en het om een maatregel gaat die in een democratische samenleving noodzakelijk is ten behoeve van de bescherming van de veiligheid van de staat. Deze uitzonderingen werden al vastgelegd in artikel 3, § 4, WVP.

Teneinde het vertrouwelijk karakter en de discretie van de inlichtingenopdrachten van de PIE te verzekeren, is de toegang van betrokkene een onrechtstreekse toegang uitgeoefend via het Vast Comité I die gesubrogeerd werd in de rechten van deze.

Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

Les données à caractère personnel doivent être exactes. Les données inexactes doivent être rectifiées ou effacées. Ces principes sont repris de l'article 5 de la Convention 108 et de l'article 4 LVP.

En ce qui concerne la conservation des données, les modalités sont fixées à l'article suivant.

CHAPITRE V

Conservation des données à caractère personnel

Art. 171

Pour la conservation des données à caractère personnel, cet article renvoie à la loi du 25 décembre 2016.

CHAPITRE VI

Droits de la personne concernée

Art. 172

Ce principe général, à savoir que toute personne physique a droit au respect de sa vie privée, est repris de l'article 2 LVP.

Art. 173

Cet article contient une énumération des droits de la personne dont les données sont traitées par l'UIP. Les modalités d'exercice de ces droits sont précisées à l'article 174.

La Convention 108 prévoit en ses articles 8 et 9 combinés que des exceptions aux droits de la personne concernée à l'information, à la rectification et à l'effacement sont possibles, pour autant qu'elles soient prévues par la loi et qu'il s'agisse de mesures nécessaires dans une société démocratique à la protection de la sécurité de l'État. Ces exceptions étaient déjà établies à l'article 3, § 4, LVP.

Pour assurer la nature confidentielle et la discrétion des missions de renseignement de l'UIP, l'accès de la personne concernée est un accès indirect exercé par l'intermédiaire du Comité permanent R qui est subrogé dans les droits de celle-ci.

Om te beantwoorden aan de punten 247 en 250 in het advies van de Privacycommissie werden de artikelen 173 en 174 aangepast en het oude ontwerp van artikel 176, die geen enkele meerwaarde had, werd gewist.

In feite, het binaire systeem van rechtreekse en onrechtstreekse toegang voorzien in artikel 15, § 3, van de wet van 25 december 2016 wordt afgeschaft in het kader van titel 8 van huidige wet.

Dit systeem paste niet bij het vertrouwelijk karakter van de verwerkte gegevens. Het binaire karakter van het systeem zou namelijk een passagier, in functie van de entiteit bij wie hij de toegang tot zijn gegevens zou kunnen uitoefenen, in staat hebben kunnen stellen te weten of zijn gegevens een positieve overeenstemming hadden opgeleverd of het resultaat vormden van een gerichte opzoeking en dus te weten of hij al dan niet door de bevoegde diensten werd onderzocht.

Door het afschaffen van voormeld systeem zijn de bepalingen in de wet betreffende de bescherming met betrekking tot persoonsgegevens, die een rechtstreekse of onrechtstreekse toegang voorzien in functie van de toepasselijktitel van huidige wet, van toepassing.

Art. 174

Op vraag van de burger controleert het Vast Comité I de rechtmatigheid van de gegevensverwerking door de PIE. Na controle deelt de toezichthoudende autoriteit aan de betrokkene mee dat de nodige verificaties werden verricht. Indien nodig gaat de PIE over tot de verbetering of verwijdering van onjuiste of niet-pertinente gegevens. De procedure wordt verder uitgewerkt in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

Art. 175

Dit artikel vergt geen commentaar.

Art. 176

Deze bepaling stelt dat de PIE geen besluit mag nemen met negatieve of ingrijpende rechtsgevolgen voor de betrokkene, voor zover dit gebeurt louter op grond van een geautomatiseerde verwerking die bedoeld is om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid.

Pour répondre aux points 247 et 250 de l'avis de la Commission vie privée, les articles 173 et 174 ont été adaptés et l'ancien projet d'article 176 qui ne présentait aucune plus-value a été supprimé.

En effet, le système dual d'accès direct et indirect prévu par l'article 15, § 3, de la loi du 25 décembre 2016 est abrogé dans le cadre du titre 8 de la présente loi.

Ce système ne convenait pas à la nature confidentielle des données traitées, et souffre d'une faille. Le caractère binaire de ce système aurait pu permettre à un passager de savoir, en fonction de l'entité auprès de laquelle il puisse exercer l'accès à ses données, si ses données ont fait l'objet d'une correspondance positive ou d'une recherche ponctuelle, et ainsi savoir s'il était recherché ou suivi par les services compétents.

Le système susmentionné ainsi supprimé, ce sont les dispositions présentes dans la présente loi qui s'appliquent et qui prévoient un accès direct ou indirect en fonction du titre applicable.

Art. 174

Le Comité permanent R vérifie, à la demande de la personne concernée, la licéité du traitement des données par l'UIP. Après contrôle, il communique à celle-ci que les vérifications nécessaires ont été effectuées. Si nécessaire, l'UIP procède à la correction ou l'effacement des données inexactes ou non pertinentes. Les modalités de la procédure sont précisées dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

Art 175

Cet article n'appelle pas de commentaires.

Art. 176

Cette disposition prescrit que l'UIP ne peut prendre aucune décision produisant des effets juridiques dommageables ou lourds de conséquence pour la personne concernée, sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects de sa personnalité.

Om te beantwoorden aan punt 251 van het advies van de Privacycommissie werd het tweede lid van de eerste versie van het artikel geschrapt. Deze voorzag uitzonderingen op het principe beschreven in het eerste lid, wanneer de beslissing gebaseerd is op een wet of wanneer zij noodzakelijk is voor het vrijwaren van een belangrijk algemeen belang. De PNR Richtlijn (en meer bijzondere artikel 24, § 4, van de wet van 25 december 2016) verbieden in elk geval beslissingen op basis van een geautomatiseerde verwerking van passagiersgegevens. Het tweede lid werd aldus geschrapt.

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 177

Dit artikel bepaalt de verplichtingen van de verwerkingsverantwoordelijke van de PIE. Hij moet waken over de juistheid van de persoonsgegevens. Hij moet ook zorgen dat voor de personen die onder hun gezag handelen, de toegang tot de gegevens beperkt blijft tot wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst.

De PIE ziet erop toe dat personen die onder haar gezag handelen kennis hebben van de verplichtingen en voorschriften die hen door deze titel worden opgelegd. Deze verplichtingen zijn conform de verplichtingen voor de verantwoordelijke van de verwerking vervat in artikel 16, § 2, 1°, WVP.

Art. 178

Het gaat over een overname van artikel 16, § 2, WVP. Voor de bescherming van de rechten van de betrokkenen en om de verantwoordelijkheid en aansprakelijkheid van de PIE te bepalen, is het noodzakelijk dat verantwoordelijkheden op duidelijke wijze worden vastgesteld wanneer een verwerking namens de PIE wordt uitgevoerd.

Pour répondre au point 251 de l'avis de la Commission vie privée, le deuxième alinéa de la première version de l'article a été supprimé. Il prévoyait des exceptions au principe décrit à l'alinéa premier, lorsque la décision est fondée sur une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important. La Directive PNR (et plus particulièrement l'article 24 § 4 de la loi du 25 décembre 2016) interdisent de toute façon les décisions sur base d'un traitement automatisé de données des passagers. Le deuxième alinéa a donc été supprimé.

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 177

Le présent article détermine certaines obligations pour le responsable du traitement de l'UIP. Il doit veiller à la justesse des données à caractère personnel. Il doit également veiller à ce que, pour les personnes agissant sous leur autorité, l'accès aux données soit limité à ce qui est utile pour l'exercice de leurs fonctions ou pour les besoins du service.

L'UIP fait également en sorte que les personnes agissant sous son autorité aient connaissance des obligations et prescriptions qui leur sont imposées par le présent titre. Ces obligations sont conformes à celles du responsable du traitement contenues dans l'article 16, § 2, 1°, LVP.

Art. 178

Il s'agit d'une reprise de l'article 16, § 2, LVP. Pour la protection des droits des personnes concernées et pour déterminer les responsabilités de l'UIP, il est nécessaire que des responsabilités soient fixées de manière claire quand un traitement est effectué au nom de l'UIP.

Afdeling 2

Beveiliging van persoonsgegevens

Art. 179

Dit artikel herneemt artikel 16, § 4, WVP. Het vermeldt de passende technische en organisatorische maatregelen die de verwerkingsverantwoordeljke moet treffen. Dit artikel stelt dat er hierbij steeds een belangenafweging gemaakt wordt. Zo worden de stand van de techniek (technologische evoluties), de kosten van de toe te passen maatregelen, de aard van de te beveiligen gegevens en de mogelijke risico's mee in overweging genomen om het passende karakter van de maatregelen vast te stellen.

Het is cruciaal voor de PIE dat de passagiersgegevens onderworpen zijn aan voldoende garanties om hun bescherming te verzekeren. Alzo voorzien de artikelen 14, § 2 en 17 van de wet van 25 december 2016 het afsluiten tussen de bevoegde diensten van de PIE en de PIE van een protocolakkoord dat met name het nemen van technische en organisationele maatregelen ter bescherming van de passagiersgegevens voorziet.

Art. 180

Om het toezicht op de PIE daadkrachtiger te maken, voert dit artikel een nieuwe verplichting in voor de verwerkingsverantwoordelijke. Zo moet de verwerkingsverantwoordelijke zo snel mogelijk haar toezichthoudende autoriteit, op de hoogte brengen ingeval van een inbreuk op de beveiliging indien deze een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Om te beantwoorden aan de aanbeveling van de Privacycommissie (punt 234 van haar advies) en de Raad van State (pagina 34 van diens advies) werd het ontwerp aangepast via het toevoegen van het respecteren van een termijn van 72 uur uiterlijk na de kennisname van de inbreuk op de beveiliging indien mogelijk. Er is daarentegen geen sprake van een kennisgeving aan de betrokkene, gezien dit in het belang van de uitvoering van de opdrachten van de PIE niet mogelijk is. Het beschermen van de nationale veiligheid laat het uitblijven van deze kennisgeving toe.

De te vermelden gegevens worden opgesomd in het wetsartikel.

Section 2

Sécurité des données à caractère personnel

Art. 179

Cet article reprend l'article 16, § 4, LVP. Il mentionne les mesures techniques et organisationnelles adéquates que le responsable du traitement doit prendre. Cet article suppose toujours une mise en balance des intérêts. Ainsi, l'état de la technique (les progrès technologiques), les coûts des mesures à appliquer, la nature des données à protéger et les risques encourus doivent être pris en considération pour déterminer le caractère adéquat des dispositions à prendre.

Il est crucial pour l'UIP que des les données des passagers soient soumises à des garanties suffisantes pour assurer leur protection. Ainsi, les articles 14, § 2, et 17 de la loi du 25 décembre 2016 prévoient la conclusion d'un protocole d'accord entre les services compétents de l'UIP et l'UIP, qui comprend notamment la prise de mesures techniques et organisationnelles visant à protéger les données des passagers.

Art. 180

Cet article introduit une nouvelle obligation à charge du responsable du traitement afin de rendre plus efficace le contrôle exercé sur l'UIP. Le responsable du traitement doit dans les meilleurs délais mettre au courant le comité permanent R d'une brèche de sécurité si elle recèle un risque élevé pour les droits et libertés de personnes physiques. Pour répondre à la recommandation de la Commission vie privée (point 234 de son avis) et du Conseil d'État (page 34 de son avis), le projet a été adapté pour ajouter le respect d'un délai de 72 heures au plus tard après avoir pris connaissance de la brèche de sécurité, si cela est possible. Par contre, il n'est pas question d'une notification à la personne concernée, vu que ce n'est pas possible dans l'intérêt de l'exercice des missions de l'UIP. La protection de la sécurité nationale permet l'omission de cette notification.

Le texte légal énumère les informations à communiquer.

Afdeling 3

Register

Art. 181

Eveneens om een meer doeltreffend toezicht toe te laten, introduceert dit artikel een nieuwe verplichting voor de verwerkingsverantwoordelijke van de PIE. Deze dient een register bij te houden van haar gegevensbank en van deze die hen ter beschikking worden gesteld.

Ten gevolge van punt 252 van het advies van de Privacycommissie is er geen sprake meer in het artikel van het ontwerp van "de gegevensbanken van de PIE" maar wel van de "passagiersgegevensbank" aangezien de wet van 25 december 2016 enkel als gegevensbank van de PIE de passagiersgegevensbank aanhaalt.

Dit artikel somt de informatie op die vermeld moet worden in het register. Voor de passagiergegevensbank werden dezelfde vermeldingen als die uit het artikel 30 van de Verordening hernomen, met uitzondering van de categorieën van personen en categorieën van persoonsgegevens, zonder onderscheid. Wat betreft de gegevensbanken waartoe de PIE toegang heeft, zijn de vermeldingen gelimiteerd aangezien alle informatie vervat in deze banken zich bevinden in de registers bijgehouden door de verantwoordelijke van de verwerking van voornoemde banken. Om te beantwoorden aan punt 237 van het advies werd specifiek vermeld dat de PIE, voor landen buiten de Europese unie, de gegevens van "de beheerder van de gegevensbank", indien deze gekend zijn, moet vermelden.

De derde paragraaf bepaalt dat de registers ter beschikking worden gesteld op vraag van het Vast Comité I.

HOOFDSTUK VII

Mededeling en doorgifte van persoonsgegevens

Art. 182

Het eerste en tweede lid van dit artikel zijn een exacte reproductie van de eerste paragraaf van artikel 21 WVP. Zij hernemen het criteria van het adequate beschermingsniveau dat de niet-lidstaat van de Europese Unie moet waarborgen opdat de PIE persoonsgegevens mag doorgeven. Enkel de termen "internationale organisatie" wordt toegevoegd omdat een internationale organisatie eveneens de bestemmeling kan zijn van

Section 3

Registre

Art. 181

Pour permettre un contrôle plus efficace, cet article introduit une nouvelle obligation dans le chef du responsable du traitement de l'UIP. Celle-ci doit tenir un registre de sa banque de données et de celles mises à sa disposition.

Suite au point 252 de l'avis de la Commission vie privée, il n'est plus question dans l'article en projet de "banques de données de l'UIP", mais bien de "la banque de données des passagers" puisque la loi du 25 décembre 2016 ne mentionne comme banque de données de l'UIP que cette seule banque de données des passagers.

Cet article énumère les informations qui doivent être mentionnées dans le registre. Pour la banque de données des passagers, les mêmes mentions que celles prévues à l'article 30 du Règlement sont reprises, à l'exception des catégories de personnes concernées et des catégories de données à caractère personnel. Pour les banques de données auxquelles l'UIP a accès, les mentions sont limitées car toutes les informations portant sur ces banques se trouvent dans le registre tenu par le responsable du traitement desdites banques. Pour répondre au point 237 de l'avis, il est indiqué plus précisément que l'UIP doit mentionner, pour les pays hors de l'Union européenne, les coordonnées du "service gestionnaire de la banque de données" si celles-ci sont connues.

Le paragraphe 3 dispose que les registres sont mis à la disposition du Comité permanent R à sa demande.

CHAPITRE VII

Communication et transfert de données à caractère personnel

Art. 182

Les alinéas premier et 2 du présent article sont l'exacte reproduction du premier paragraphe de l'article 21 LVP. Ils reprennent le critère du niveau de protection adéquat que doit assurer le pays non membre de l'Union européenne pour que l'UIP puisse lui transférer une donnée à caractère personnel. Seuls les termes "organisation internationale" ont été ajoutés puisqu'une organisation internationale peut également

persoonsgegevens. Het derde lid specifieert dat het adequaat beschermingsniveau gewaarborgd kan worden door veiligheidsclausules waarop de PIE en de ontvanger zich afstemmen. Dit lid herneemt de idee van lid 2 van artikel 22 WVP.

Er wordt gespecifieerd dat, teneinde te beantwoorden aan punt 253 van het advies van de Privacycommissie, de bepalingen van hoofdstuk 2 van de wet van 25 december 2016 eveneens moeten gerespecteerd worden. Voormelde wet bepaalt in feite een aantal verplichtingen die moeten gerespecteerd worden opdat het doorsturen van passagiersgegevens naar het buitenland kan uitgevoerd worden, met name het afsluiten van een protocolakkoord tussen de PIE en de instantie met wie de gegevens worden uitgewisseld.

Art. 183

Dit artikel voorziet uitzonderingen op de vereiste van een adequaat beschermingsniveau:

— na instemming van de betrokkene (kopij van artikel 22, 1°, WVP);

— indien de doorgifte noodzakelijk of wettelijk verplicht is voor de bescherming van de fysieke integriteit van een persoon of van een belangrijk openbaar belang (fusie van 4° en 5°, van artikel 22 WVP);

— Indien de doorgifte noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend openbaar belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

HOOFDSTUK VIII

Toezichthoudende autoriteit

Art. 184

Wat betreft de gegevensverwerking bedoeld in artikel 169, wordt het Vast Comité I opgericht door de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse aangeduid als bevoegde toezichthoudende autoriteit.

être le destinataire de données à caractère personnel. Le troisième alinéa précise que le niveau de protection adéquat peut être assuré par des clauses de sécurité sur lesquelles s'accordent l'UIP et le destinataire. Cet alinéa reprend l'idée de l'alinéa 2 de l'article 22 LVP.

Il est précisé, pour répondre au point 253 de l'avis de la Commission vie privée, que les dispositions du chapitre 12 de la loi du 25 décembre 2016 doivent également être respectées. En effet, la loi précitée établit un certain nombre d'obligations à respecter pour que des transferts de données des passagers vers l'étranger puissent être effectués, notamment la conclusion d'un protocole d'accord entre l'UIP et l'instance avec laquelle les données sont échangées.

Art. 183

Cet article prévoit des exceptions à l'exigence d'un niveau de protection adéquat:

— avec le consentement de la personne concernée (copie de l'article 22, 1°, LVP);

— si le transfert est nécessaire ou légalement obligatoire à la sauvegarde de l'intégrité physique d'une personne ou d'un intérêt public important (fusion des 4° et 5°, de l'article 22 LVP);

— si le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

CHAPITRE VIII

Autorité de contrôle

Art. 184

S'agissant du traitement des données visé à l'article 169, le Comité permanent R, institué par la loi du 18 juillet 1991 réglementant la surveillance des services de police et de renseignement et l'Organe de coordination pour l'analyse de la menace, est désigné comme l'autorité de contrôle compétente.

ONDERTITEL 6

BIJZONDERE BEPALINGEN

Art. 185

De bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, het Comité I, het Comité P en het Controleorgaan op de politionele informatie, in hun hoedanigheid van toezichthoudende autoriteit voor de inlichtingen- en de politiediensten, moeten toegang kunnen hebben tot alle gegevens die verwerkt worden deze laatste, met inbegrip van de gegevens die binnen de bijzondere categorieën vallen.

De eerste paragraaf beoogt dergelijke verwerking toe te laten. Om te antwoorden op de vraag van de Privacycommissie in haar punt 241, de bestuurlijke commissie valt niet onder de controle van het Comité I.

De tweede paragraaf beperkt het recht op toegang van de betrokkene voor evidente redenen van discretie. De derde paragraaf voorziet in het recht van de betrokkene om de verbetering of wissing van zijn onjuiste gegevens te vragen.

De laatste paragraaf onttrekt de vier autoriteiten bedoeld in de eerste paragraaf van de contrôle van de Gegevensbeschermingsautoriteit aangezien zij zelf toezichthoudende autoriteiten zijn. Om op het punt 240 van het advies van de Privacycommissie te antwoorden en op de opmerking van de Raad van State (pagina 37) werd de vierde paragraaf aangepast om te verduidelijken dat die enkel van toepassing is voor verwerkingen verricht in het kader van opdrachten bedoeld in de eerste paragraaf.

TITEL 4

Verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden ter uitvoering van artikel 89 paragrafen 2 en 3 van de verordening

Inleiding

De Verordening promoot de wetenschap. Overweging 113 van de Verordening stelt in dat verband dat, met betrekking tot verwerkingen *"met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden, rekening [dient] te worden gehouden met de gerechtvaardigde verwachting van de maatschappij dat er sprake is van kennisvermeerdering".*

SOUS-TITRE 6

DISPOSITIONS PARTICULIÈRES

Art. 185

La Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité, le Comité R, le Comité P et l'Organe de contrôle de l'information policière, en leur qualité d'autorité de contrôle des services de renseignement et de police, doivent pouvoir avoir accès à toutes les données traitées par ces derniers, y compris aux données tombant dans des catégories particulières.

Le premier paragraphe vise à autoriser un tel traitement. Pour répondre à la question de la Commission vie privée en son point 241, la Commission administrative ne relève pas du contrôle du Comité R.

Le second paragraphe limite le droit d'accès de la personne concernée pour des raisons évidentes de discrétion. Le troisième paragraphe prévoit le droit pour la personne concernée de demander la rectification ou la suppression de ses données inexactes.

Le dernier paragraphe soustrait les quatre autorités visées au paragraphe premier du contrôle de l'Autorité de protection des données car elles sont elles-mêmes des autorités de contrôle. Pour répondre au point 240 de l'avis de la Commission vie privée et à la remarque du Conseil d'État (page 37), le paragraphe 4 a été adapté pour préciser qu'il ne s'applique que pour les traitements effectués dans le cadre des missions visées au premier paragraphe.

TITRE 4

Traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques en exécution de l'article 89 paragraphes 2 et 3 du règlement

Introduction

Le Règlement promeut la science. Le considérant 113 du Règlement dispose à cet égard que, concernant les traitements *"à des fins de recherche scientifique ou historique ou à des fins statistiques, il y a lieu de prendre en considération les attentes légitimes de la société en matière de progrès des connaissances".*

Om een evenwicht te vinden tussen de vrijheid van het onderzoek en de bescherming van de persoonlijke levenssfeer voorziet de Verordening, inzonderheid artikel 89, in een specifieke regeling voor de verwerking van persoonsgegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Zo stelt artikel 89.1 van de Verordening dat gepaste waarborgen de rechten en vrijheden van de betrokkenen moeten waarborgen tijdens de verwerkingen met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. De artikelen 89.2 en 89.3 laten lidstaten toe om afwijkingen te voorzien op de rechten bedoeld in de artikelen 15, 16, 18 en 21 van de Verordening voor wat betreft de verwerkingen met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden en op de rechten bedoeld in de artikelen 15, 16, 18, 19, 20 en 21 voor wat betreft de verwerkingen met het oog op archivering in het algemeen belang.

Deze afwijkingen zijn onderworpen aan twee voorwaarden. Enerzijds zijn de gepaste waarborgen bedoeld in artikel 89.1 van toepassing en dient de lidstaat in zijn wetgeving de afwijkingen bedoeld in de artikelen 89.2 en 89.3 te voorzien. Vervolgens zijn ze slechts van toepassing in de gevallen dat de toepassing van de rechten voorzien in de artikelen 89.2 en 89.3 de verwezenlijking van de doeleinden van de verwerkingsverantwoordelijke onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken

Bovendien voorzien een hele reeks van artikelen van de Verordening bijzondere toepassingsmodaliteiten voor de verwerkingen met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, overeenkomstig artikel 89.1. Het betreft de artikelen 5.1.b), 5.1.e), 9.2 j), 14.5 en 17.3.d) van de Verordening.

De Verordening bepaalt aldus twee regimes voor verwerkingen met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden:

— krachtens artikel 89.1. van de Verordening: de verwerkingsverantwoordelijke moet technische en organisatorische maatregelen aannemen die gepaste waarborgen vormen wanneer hij de manoeuvreerruimte wenst te gebruiken die wordt toegestaan door de artikelen 5.1.b), 5.1.e), 9.2 j), 14.5 en 17.3.d);

— krachtens de artikelen 89.2 en 89.3 van de Verordening: de lidstaat dient in zijn wetgeving

Afin de trouver un équilibre entre la liberté de la recherche et la protection de la vie privée, le Règlement institue un régime spécifique pour le traitement des données à caractère personnel à des fins d'archivistique dans l'intérêt public, à des fins de recherche scientifique et historique ou à des fins statistiques.

Ainsi, l'article 89.1 du Règlement dispose que des garanties appropriées doivent garantir les droits et libertés des personnes concernées lors de traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistique. Les articles 89.2 et 89.3 permettent aux États membres de prévoir des dérogations respectivement aux droits visés aux articles 15, 16, 18 et 21 du Règlement pour les traitements à des fins de recherche scientifique ou historique ou à des fins statistique et aux droits visés aux articles 15, 16, 18, 19, 20 et 21 pour les traitements à des fins archivistiques dans l'intérêt public.

Ces dérogations sont conditionnées par deux aspects. D'une part, les garanties appropriées visées à l'article 89.1 s'appliquent et d'autre part l'État membre doit prévoir dans sa législation les dérogations visées aux articles 89.2 et 89.3. Ensuite, elles ne sont applicables que dans les cas où l'application des droits visées aux articles 89.2 et 89.3 risqueraient de rendre impossible ou d'entraver sérieusement les finalités du responsable du traitement et de telles dérogations sont nécessaires pour atteindre ces finalités.

En outre, toute une série d'articles du Règlement prévoient des modalités d'application particulières pour les traitements à des fins d'archivistique dans l'intérêt public, à des fins de recherche scientifique et historique ou à des fins statistiques, conformément à l'article 89.1. Il s'agit des articles 5.1.b), 5.1.e), 9.2 j), 14.5 et 17.3.d) du Règlement.

Le Règlement détermine dès lors deux régimes pour les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques:

— en vertu de l'article 89.1 du Règlement: le responsable du traitement doit adopter des mesures techniques et organisationnelles, et qui établissent des garanties appropriées lorsqu'il veut utiliser les marges de manœuvres autorisées par les articles 5.1.b), 5.1.e), 9.2 j), 14.5 et 17.3.d);

— en vertu des articles 89.2 et 89.3 du Règlement: l'État membre doit adopter dans sa législation des

afwijkingen aan te nemen, onder voorbehoud van de gepaste waarborgen bedoeld in artikel 89.1 en die de verwerkingsverantwoordelijke dient na te leven indien hij wenst af te wijken van de artikelen 15, 16, 18, 19, 20 en 21.

Uit het verschil tussen artikel 89.1 en de artikelen 89.2 en 89.3 kan men afleiden dat de Europese wetgever een zekere flexibiliteit heeft willen geven aan de verwerkingsverantwoordelijken voor wat betreft de afwijkingen van de principes en hun verplichtingen maar dat hij anderzijds gewild heeft dat de afwijkingen van de rechten van de betrokkenen gekaderd worden op een meer uniforme en voorzienbare wijze.

Titel 4 van deze wet voert dan ook de artikelen 89.2 en 89.3 van de Verordening uit door gepaste waarborgen te voorzien die moeten nageleefd worden door verwerkingsverantwoordelijken wanneer zij de rechten van de betrokkenen wensen te beperken.

Tot slot dient te worden verduidelijkt dat de verantwoordelijke voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden van mening kan zijn dat hij aan alle bepalingen van de Verordening kan beantwoorden en zich dan ook niet te willen beroepen, of slechts gedeeltelijk, van de afwijkingen voorzien in de Verordening of in huidige titel. Er zijn vier scenario's mogelijk:

— ofwel kan een verwerkingsverantwoordelijke zijn doeleinden bereiken door aan alle verplichtingen van de Verordening te beantwoorden en alle rechten van de betrokkenen na te leven; in dat geval beroept hij zich op geen enkele afwijking.

— ofwel kan een verwerkingsverantwoordelijke zijn doeleinden bereiken door aan alle verplichtingen van de Verordening te beantwoorden maar zonder te kunnen waarborgen dat alle rechten van de betrokkenen worden nageleefd; hij kan zich dus niet beroepen op de manoeuvreerruimte voorzien in de artikelen 5.1.b), 5.1.e), 9.2 j), 14.5 en 17.3.d) van de Verordening maar hij kan – voor zover hij de gepaste waarborgen voorzien in huidige titel naleeft – zich beroepen op de afwijkingen van de artikelen 15, 16, 18, 20 (en 19 en 21 indien het een verwerking met het oog op archivering in het algemeen belang betreft);

— ofwel kan een verwerkingsverantwoordelijke zijn doeleinden niet bereiken indien hij aan alle verplichtingen van de Verordening dient te beantwoorden maar kan hij daarentegen de naleving waarborgen van de rechten van de betrokkenen; hij dient dus gepaste waarborgen te voorzien die technische en organisatorische

dérogations, sous réserve des garanties appropriées visées à l'article 89.1 et que le responsable du traitement doit respecter lorsqu'il veut déroger aux articles 15, 16, 18, 19, 20 et 21.

De la différence entre l'article 89.1 et les articles 89.2 et 89.3 on peut déduire que le législateur européen souhaite donner une certaine flexibilité aux responsables du traitement en ce qui concerne les dérogations aux principes et à leurs obligations mais qu'en revanche il souhaite que les dérogations aux droits des personnes soient encadrées de manière plus uniforme et prévisible.

Dès lors, le titre 4 de la présente loi met en œuvre les articles 89.2 et 89.3 du Règlement en prévoyant des garanties appropriées que doivent respecter les responsables du traitement lorsqu'ils veulent limiter les droits des personnes concernées.

Enfin, il est à préciser que le responsable du traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques peut très bien estimer qu'il peut répondre à toutes les dispositions du Règlement et de ne pas se prévaloir, ou seulement partiellement, des dérogations prévues dans le Règlement ou dans le présent titre. Il y a quatre cas de figure possible:

— soit un responsable du traitement peut atteindre ses finalités en répondant à toutes les obligations du Règlement et en respectant tous les droits des personnes concernées, il ne peut alors se prévaloir d'aucune dérogations;

— soit un responsable du traitement peut atteindre ses finalités en répondant à toutes les obligations du Règlement mais sans pouvoir garantir de respecter tous les droits des personnes concernées, il ne peut alors pas se prévaloir des marges de manœuvre prévues aux articles 5.1.b), 5.1.e), 9.2 j), 14.5 et 17.3.d) du Règlement mais il peut – pour autant qu'il respecte les garanties appropriées prévues dans le présent titre – se prévaloir des dérogations aux articles 15, 16, 18, 20 (et 19 et 21 s'il s'agit d'une traitement à des fins archivistiques dans l'intérêt public;

— soit un responsable du traitement ne peut pas atteindre ses finalités s'il doit répondre à toutes les obligations du Règlement mais peut en revanche garantir de respecter tous les droits des personnes concernées, il doit alors prévoir des garanties appropriées qui établissent des mesures organisationnelles et techniques

maatregelen vormen om van de artikelen 5.1.b), 5.1.e), 9.2 j), 14.5 en 17.3.d) van de Verordening te kunnen afwijken maar zal niet onderworpen zijn aan de gepaste waarborgen voorzien in huidige titel;

— ofwel kan de verwerkingsverantwoordelijke zijn doeleinden slechts bereiken door af te wijken van de principes en verplichtingen en rechten van de betrokkenen; hij dient dus zowel technische en organisatorische maatregelen te voorzien als zich te onderwerpen aan de gepaste waarborgen in huidige titel.

Het spreekt voor zich dat de verplichtingen van de Verordening die niet het voorwerp kunnen uitmaken van enige afwijking van toepassing zijn. Bijvoorbeeld, de verplichting een register bij te houden is van toepassing krachtens artikel 30 van de Verordening, zelfs indien de verwerkingsverantwoordelijke geen beroep doet op de gepaste waarborgen in deze titel. Anders gezegd, indien de verwerkingsverantwoordelijke niet onder de voorwaarden van artikel 30.5 van de Verordening valt dan dient hij een register bij te houden. Ook is de verplichting een DPO te gebruiken, desgevallend, van toepassing krachtens artikel 37 van de Verordening.

Het is duidelijk dat huidige titel op geen enkele manier een bijkomende verplichting inhoudt voor de verantwoordelijken voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Integendeel, huidige titel voorziet in gepaste waarborgen die de verwerkingsverantwoordelijke die wenst af te wijken van de rechten van de betrokkenen dient ten uitvoer te brengen.

Dient te worden onderstreept, tot slot, het feit dat huidige titel in nauwe samenwerking werd uitgewerkt met vertegenwoordigers van verantwoordelijken voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Huidige regeling

Nu worden verwerkingen met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden geregeld bij het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992, die de aangelegenheid deels reglementeert (verenigbaarheid voor de verdere verwerkingen met het oog op onderzoek) maar het voorziet niet in gepaste waarborgen als tegenpartij voor de beperking van de rechten van de betrokkenen en beoogt enkel de verdere verwerking van gegevens.

pour déroger aux articles 5.1.b), 5.1.e), 9.2 j), 14.5 et 17.3.d) du Règlement mais ne devra pas se soumettre aux garanties appropriées prévues dans le présent titre;

— soit le responsable du traitement ne peut atteindre ses finalités qu'en dérogeant tant aux principes et obligations ainsi qu'aux droits des personnes, il doit alors tant prévoir des mesures techniques et organisationnelles que se soumettre aux garanties appropriées prévues dans le présent titre.

Il va de soi que les obligations du Règlement qui ne peuvent faire l'objet d'aucune dérogations s'appliquent. Par exemple, l'obligation de tenir un registre s'applique en vertu de l'article 30 du Règlement même si le responsable du traitement ne se prévaut pas des garanties appropriées prévues dans le présent chapitre. En d'autres mots, si le responsable du traitement n'entre pas dans les conditions de l'article 30.5 du Règlement, il doit tenir un registre. De même, le cas échéant, l'obligation de recourir à un DPO s'applique en vertu de l'article 37 du Règlement.

Il est bien établi que le présent titre ne représente en rien une obligation supplémentaire pour les responsables du traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques mais au contraire le présent titre dispose des garanties appropriées que le responsable du traitement qui veut déroger aux droits des personnes doit mettre en œuvre.

Il faut souligner enfin que le présent titre a été élaboré en collaboration étroite avec des représentants des responsables du traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Régime actuel

Actuellement les traitements à des fins de recherche scientifique ou historique ou à des fins statistiques sont régis par l'arrêté royal du 13 février 2001 exécutant la loi du 8 décembre 1992 qui règlemente partiellement la matière (compatibilité pour les traitements ultérieurs à des fins de recherche) mais mais il ne prévoit pas de garanties appropriées en contrepartie de la limitation des droits des personnes concernée et ne vise que les traitements de données ultérieurs.

Met betrekking tot het statistisch onderzoek stelt de wet van 4 juli 1962 betreffende de openbare statistiek daarentegen een reeks van verplichtingen en gepaste waarborgen op.

Met betrekking tot de archiefverwerkingen in het algemeen belang bestaat volgende wetgeving:

— de archiefwet van 24 juni 1955;

— de ordonnantie van 19 maart 2009 betreffende de archieven van het Brussels Hoofdstedelijk Gewest en het Waals decreet van 6 december 2001 betreffende de openbare archieven;

— het decreet van de Vlaamse Gemeenschap van 9 juli 2010 betreffende de bestuurlijk-administratieve archief-werking;

— het decreet van 12 mei 2004 betreffende de centra voor private archieven in de Franse Gemeenschap van België.

Met betrekking tot het wetenschappelijk onderzoek zijn er:

— de wet van 7 mei 2004 inzake de experimenten op personen, de Europese verordening 536/2014 betreffende klinische proeven met geneesmiddelen voor menselijk gebruik en de wet van 19 december 2008 inzake het verkrijgen en het gebruik van menselijk lichaamsmateriaal met het oog op de geneeskundige toepassing op de mens of het wetenschappelijk onderzoek, de geïnformeerde toestemming van de betrokkene voor de deelname aan het onderzoek;

— de Europese Richtlijn 2004/23 van 31 maart 2004 tot vaststelling van kwaliteits- en veiligheidsnormen voor het doneren, verkrijgen, testen, bewerken, bewaren en distribueren van menselijke weefsels en cellen, evenals de wet van 19 december 2008 inzake het verkrijgen en het gebruik van menselijk lichaamsmateriaal met het oog op de geneeskundige toepassing op de mens of het wetenschappelijk onderzoek, stelt dat de uitdrukkelijke instemming vereist is voor het secundair gebruik met wetenschappelijke doeleinden van menselijk celweefsel;

— het Raadgevend Comité voor Bio-ethiek in zijn advies 25 van 17 november 2003 heeft de anonimisering aanbevolen van de gegevens die verder worden verwerkt met het oog op onderzoek. Deze waarborg is opgenomen in deze wetdit wetsontwerp.

Concernant la recherche statistique, la loi du 4 juillet 1962 relative à la statistique établit en revanche une série d'obligations et de garanties appropriées..

Concernant les traitements archivistiques d'intérêt public, il existe les législations suivantes:

— la loi du 24 juin 1955 relative aux archives;

— l'ordonnance relative aux archives de la Région de Bruxelles capitale du 19 mars 2009 et le décret wallon du 6 décembre 2001 relatif aux archives publiques;

— le decret de la Communauté flamande relatif à l'organisation des archives administratives et de gestion du 9 juillet 2010;

— le décret relatif aux centres d'archives privées en communauté française en Belgique du 12 mai 2004.

Concernant la recherche scientifique il y a:

— la loi du 7 mai 2004 relative aux expérimentations sur la personne humaine , le règlement UE 536/2014 du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humains, et la loi du 19 décembre 2008 relative à l'obtention et à l'utilisation de matériel corporel humain destiné à des applications médicales humaines ou à des fins de recherche scientifique exigent le consentement informé de la personne concernée pour la participation à la recherche (et donc à la collecte de ses données;

— la directive européenne 2004/23 du 31 mars 2004, relatvie à l'établissement de normes de qualité et de sécurité pour le don, l'obterntion, le contrôle, la transformation, la conservation, le stockage et la distribution des tissus et cellules humains, ainsi que la loi du 19 décembre 2008 relative à l'obtention et à l'utilisiation de matériel corporel humain ou à des fins de recherche scientifique dispose que le consentement explicite est nécessaire pour le prélèvement de matériel corporel et que le consentement implicite est nécessaire pour l'usage secondaire à des fins scientifiques de matériau cellulaire humain;

— le comité consultatif bioéthique, dans son avis 25 du 17 novembre 2003, a recommandé l'anonymisation des données traitées ultérieurement à des fins de recherche.

Met betrekking tot historisch onderzoek is er geen wet.

Huidig wetsontwerp heeft geprobeerd de gepaste waarborgen te definiëren, rekening houdende met het feit dat deze adequaat moeten kunnen overeenstemmen met de sectorale waarborgen voorzien in de sectorale wetten.

Advies van de Privacycommissie

Het advies van de Privacycommissie, in de punten 258 en 259, heeft zorgvuldig een verwarring opgemerkt in het voorontwerp dat in eerste lezing werd goedgekeurd. Het voorontwerp behandelde inderdaad het artikel 89 in zijn geheel door een algemeen afwijkend regime voor te stellen en de twee types van gepaste waarborgen bedoeld enerzijds in artikel 89.1 en anderzijds de artikelen 89.2 en 89.3 onvoldoende te scheiden.

Die verwarring is nu opgeheven in artikel 186 waarin verduidelijkt wordt dat het ontwerp de artikelen 89.2 en 89.3 uitvoert.

Het advies van de Privacycommissie baseert gans haar advies op dit vertrekpunt. Door te verduidelijken dat de artikelen 89.2 en 89.3 als wettelijke grondslag van huidige titel gelden wordt beantwoord aan quasi het geheel van opmerkingen van de Privacycommissie voor deze titel.

Het advies van de Privacycommissie gaat gepaard met verschillende algemene overwegingen.

Ten eerste vermeldt de Privacycommissie, in de punten 260 tot 262, dat het belang van de Verordening bestaat in het harmoniseren eerder dan het creëren van nationale regimes. Maar het zijn de artikelen 89.2 en 89.3 zelf die de lidstaten oproepen om in hun nationale wetgeving gepaste waarborgen te voorzien. En omdat het makkelijker is voor een verwerkingsverantwoordelijke die actief is in meerdere landen om over een enkel wettelijk regime te beschikken, worden er net in deze titel gepaste waarborgen voorzien die zo dicht mogelijk aansluiten bij die van de Verordening.

Voor het overige betreffende deze overweging kan er getwijfeld worden of de door de Privacycommissie genoemde voorbeelden (inventarisatie van de mobiliteitsbehoeften van een onderneming, consumententevredenheidsenquête over de verpakking van een product) gelijkgesteld kunnen worden met verwerkingen met het oog op wetenschappelijk onderzoek of voor statistische doeleinden in de zin van artikel 89 van de Verordening en in dat opzicht uitgezonderd kunnen worden van het naleven van de rechten van de betrokkenen.

Concernant la recherche historique, il n'y a pas de loi.

Le présent projet de loi a tenté de définir des garanties appropriées, gardant à l'esprit que celles-ci doivent pouvoir s'accorder adéquatement aux garanties sectorielles prévues dans les lois sectorielles.

Avis de la Commission vie privée

L'avis de la Commission vie privée a judicieusement relevé dans ses points 258 et 259 une confusion dans l'avant-projet approuvé en première lecture. En effet, celui-ci traitait indifféremment de l'article 89, proposant un régime dérogatoire global, et ne scindait pas suffisamment les deux types de garanties appropriées visées d'une part à l'article 89.1 et d'autre part aux articles 89.2 et 89.3.

Cette confusion est à présent levée à l'article 186 qui précise que le projet exécute les articles 89.2 et 89.3.

L'avis de la Commission vie privée établit l'ensemble de son avis sur ce point de départ. En clarifiant la base légale du présent titre comme étant les articles 89.2 et 89.3 du Règlement, il est répondu à la quasi-totalité des remarques de la Commission vie privée pour ce titre.

La Commission vie privée accompagne son avis par plusieurs considérations d'ordre général.

Tout d'abord, la Commission vie privée mentionne en ses points 260 à 262 que l'intérêt du Règlement est d'harmoniser plutôt que de créer des régimes nationaux. Toutefois, ce sont les articles 89.2 et 89.3 eux-mêmes qui enjoignent aux États membres de prévoir dans leur loi des garanties appropriées. Puisqu'il est vrai qu'il est plus facile pour un responsable du traitement qui opère dans plusieurs pays d'avoir à faire à un seul régime légal, il est justement prévu dans ce titre des garanties appropriées les plus proches possibles de ce que le Règlement contient.

Pour le surplus de cette considération, on nourrit des doutes sur le fait que les exemples cités par la Commission vie privée (cartographie des besoins de mobilité d'une société, enquête de satisfaction des consommateurs sur l'emballage d'un produit) puissent être assimilés à des traitements à des fins de recherche scientifique ou à des fins statistiques au sens de l'article 89 du Règlement et puissent à ce titre être exemptés du respect des droits des personnes concernées.

In die zin citeren we overweging 113 van de Verordening stelt dat voor wat de verwerkingen betreft "*het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden dient rekening te worden gehouden met de gerechtvaardigde verwachting van de maatschappij dat er sprake is van kennisvermeerdering*.".

We citeren ook overweging 157 en volgende van de Verordening geven als voorbeeld voor wetenschappelijk onderzoek en statistiek het onderzoek naar cardiovasculaire ziekten, kanker en depressie, de bestaande langetermijncorrelaties tussen een bepaald aantal sociale omstandigheden, zoals werkloosheid en opleiding en andere levensomstandigheden, de ontwikkeling en demonstratie van technologieën, fundamenteel onderzoek, toegepast wetenschappelijk onderzoek en onderzoek gefinancierd door de privésector, het verwerven van kennis om de levenskwaliteit te verbeteren van een bepaald aantal personen en de doeltreffendheid van de sociale diensten te versterken.

Statistisch onderzoek geleid door een onderneming over de tevredenheidsgraad van de consument in verband met de verpakkingen van hun producten kan niet beschouwd worden als zijnde statistisch onderzoek dat voldoet aan de legitieme verwachtingen van de onderneming inzake kennis. Artikel 89 van de Verordening heeft niet als doel om het recht van de betrokkenen op informatie, op verzet, om vergeten te worden te beperken voor dit type verwerking, die derhalve uitgesloten zijn van het toepassingsgebied van artikel 89 van de Verordening en van deze titel.

Het advies van de Privacycommissie meent vervolgens in punt 263 dat het ontwerp als uitgangspunt blijkbaar de stelling inneemt"*dat deze verwerkingen per definitie een hoog risico met zich meebrengen. Een uitgangspunt dat zonder meer haaks staat op de realiteit en niet onderbouwd wordt in de Memorie van toelichting."*

In tegenstelling tot wat de Privacycommissie benadrukt, neemt deze titel zulk uitgangspunt niet aan. Er kan worden verondersteld dat de Privacycommissie tot dergelijke conclusie is gekomen vermits de twee algemene gepaste waarborgen voorzien in deze titel ook twee maatregelen zijn die worden voorzien in de Verordening voor risicoverwerkingen.

Vervolgens wordt het advies van de Privacycommissie niet gedeeld volgens dewelke het duidelijk is dat afwijken van de rechten van de betrokkenen geen risico inhoudt. Om redenen reeds eerder uitgelegd, met name het zo veel mogelijk harmoniseren en het vermijden van het creëren van verschillende nationale regimes werd ervoor geopteerd zich te inspireren door de maatregelen

A cet effet, on cite le considérant 113 du Règlement qui dispose que concernant les traitements "*à des fins de recherche scientifique et statistique, il y a lieu de prendre en considération les attentes légitimes de la société en matière de connaissance*.".

On cite aussi les considérants 157 et suivants du Règlement qui donnent pour exemple de recherche scientifique et statistique la recherche sur les maladies cardiovasculaires, le cancer et la dépression, les corrélations à long terme existant entre un certain nombre de conditions sociales telles que le chômage et l'éducation et d'autres conditions de vie, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé, l'acquisition de connaissance pour améliorer la qualité de vie d'un certain nombre de personnes et renforcer l'efficacité des services sociaux.

Une enquête statistique menée par une entreprise sur le degré de satisfaction des consommateurs sur ses emballages ne peut être qualifiée de recherche statistique répondant aux attentes légitimes de la société en matière de connaissance. L'article 89 du Règlement n'a pas pour objectif de limiter le droit d'information, d'opposition, à l'oubli des personnes concernées pour ce type de traitement, qui sont dès lors exclus du champ d'application de l'article 89 du Règlement et du présent titre.

L'avis de la Commission vie privée estime ensuite en son point 263 que "*le projet adopte pour point de départ l'affirmation selon laquelle ces traitements impliquent par définition un risque élevé. Un point de départ qui est purement et simplement en contradiction fragrante avec la réalité et qui n'est pas étayé dans l'exposé des motifs*".

Contrairement à ce que souligne la Commission vie privée, le présent titre n'adopte pas un tel point de départ. On suppose que la Commission vie privée est arrivée à une telle déduction car les deux garanties appropriées générales prévues dans ce titre sont également deux mesures prévues dans le Règlement pour les traitements à risque.

Ensuite, on ne partage pas l'avis de la Commission vie privée selon laquelle il est flagrant que déroger aux droits des personnes concernées ne comporte pas risque. Pour les raisons expliquées ci-avant, à savoir harmoniser tant que possible et éviter de créer des régimes nationaux différents les uns des autres, il a été choisi de s'inspirer des mesures déjà présentes dans le

reeds aanwezig in de Verordening om de gepaste waarborgen te bepalen. Het gaat hier om het ondersteunen van een bewuste kennisvermeerdering voor wat betreft de risico's jegens de betrokkenen maar die desalniettemin gekend zijn voor de verwerkingsverantwoordelijken.

Het ontwerp werd gewijzigd, geïnspireerd door het advies van de Privacycommissie door het volgende onderscheid te maken:

— de verwerkingen van niet gevoelige gegevens en gevoelige, maar gepseudonimiseerde gegevens die een vereenvoudigd systeem volgen;

— de verwerkingen van gevoelige gegevens anderzijds, die een hoger risico inhouden en waarvoor er extra passende waarborgen voorzien zijn.

In het punt 264 meent de Privacycommissie dat de noodzaak om een DPO te gebruiken te formalistisch is.

De universiteiten, zowel nederlandstalig als franstalig, hebben eveneens de schrapping van deze verplichting gevraagd tijdens de verschillende stappen van het onderzoek.

Die standpunten worden gevolgd en de raadpleging van de DPO in de verschillende stappen van het onderzoek werd geschrapt uit het ontwerp. Desalniettemin wordt de verplichting om een DPO aan te stellen voor risicoverwerkingen behouden. Er dient echter herhaald te worden dat verschillende reglementeringen inzake onderzoek, zoals bijvoorbeeld de Europese Verordening 536/214 over klinische proeven, de wet van 7 mei 2004 over klinische onderzoeken en de wet van 19 december 2008 inzake het verkrijgen en het gebruik van menselijk lichaamsmateriaal reeds voor elk onderzoek het advies van de ethische commissie opleggen en met inbegrip van de privacyaspecten.

Er is geen sprake van om hier de twee verplichtingen te doen overlappen. Zo moet de DPO kunnen coördineren met de ethische commissie, met respect voor de onafhankelijkheid van elkeen.

Daarnaast, in de gevallen voorzien in de artikelen 35 en 37 van de Verordening is de tussenkomst van een DPO reeds verplicht, onafhankelijk van dit wetsontwerp.

Het vierde en laatste algemene argument van de Privacycommissie, op punt 265, is het betreuren van de afwezigheid van een Europees regime betreffende wetenschappelijk onderzoek.

Règlement pour déterminer les garanties appropriées. Il s'agit ici de soutenir la production de connaissance de manière consciencieuse quant aux risques vis-à-vis des personnes concernées mais néanmoins déjà familières pour les responsables du traitement.

Trouvant néanmoins de l'inspiration, dans l'avis de la Commission vie privée, le projet a été modifié en distinguant:

— les traitements de données non-sensibles et sensibles mais pseudonymisées qui suivent un régime simplifié;

— les traitements de données sensibles d'autre part, qui constituent un risque plus élevé et pour lesquels davantage de garanties appropriées sont prévues.

En son point 264, la Commission vie privée estime trop formaliste la nécessité de recourir à un DPO.

Les universités, tant flamandes que francophones ont également demandé la suppression de cette obligation lors des différentes étapes de la recherche.

Ces points de vue ont été suivi et la consultation du DPO aux différentes étapes de la recherche a été supprimé du projet. Toutefois l'obligation est maintenu de recourir à un DPO pour les traitements à risque. Il est nécessaire de rappeler néanmoins que plusieurs réglementations concernant la recherche, comme par exemple le règlement européen 536/214 sur les essais cliniques, la loi du 7 mai 2004 sur les essais cliniques et la loi du 19 décembre 2008 relative à l'obtention et à l'utilisation du matériel corporel humain imposent déjà pour toute recherche, l'avis du comité d'éthique en ce compris concernant les aspects relatifs à la vie privée.

Il n'est pas question ici de se faire chevaucher ces deux obligations. Ainsi, le DPO doit pouvoir se coordonner, dans le respect de l'indépendance de chacun, avec le comité d'éthique.

En outre, dans les cas prévus aux articles 35 et 37 du Règlement, l'intervention du DPO est déjà obligatoire, indépendamment de ce projet de loi.

Le quatrième et dernier argument général de la Commission vie privée , au point 265, est de regretter l'absence d'un régime européen relatif à la recherche scientifique.

De Raad van de Vlaamse Universiteiten heeft eveneens gevraagd om een uniek Europees systeem voor onderzoek te ontwikkelen.

Zelfs als de idee verleidelijk lijkt, de huidige titel houdt geen rekening met de intereuropese verwerkingen met het oog op onderzoek want de Verordening staat dit niet toe. Er bestaat enkel de overweging 159 die vraagt om rekening te houden met artikel 179 VWEU .

De artikelen 89.2 en 89.3 van de Verordening laten aan nationale wetgevers dan ook slechts twee keuzes:

— ofwel een wetsontwerp indienen dat passende waarborgen opstelt als tegenprestatie voor de beperking van de rechten van de betrokkenen binnen het domein van onderzoek, met het risico dat de passende waarborgen een rem betekenen voor het grensoverschrijdende onderzoek;

— ofwel niets doen, waarbij dan de verwerkingen met het oog op onderzoek onderworpen zijn aan de volledige rechten van de betrokkenen, hetgeen een op zijn minst even belangrijke rem betekent voor het onderzoek.

De verwerkingsverantwoordelijken voor onderzoek die vrezen dat de passende waarborgen bepaald in dit wetsontwerp hun grensoverschrijdend onderzoek in het gedrang brengen, zijn vrij deze titel niet te volgen. In dat geval moeten ze echter de volledige rechten van de betrokken personen toepassen op hun verwerkingen zoals voorzien in artikel 89.1 van de Verordening.

Dit ontwerp, dat verre van schadelijk is voor het concurrentievermogen van onze onderzoekscentra, geeft hen een rechtszekerheid. En verre van Belgische onderzoekers te isoleren van hun Europese collega's, dankzij zijn evenwicht tussen enerzijds een verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden en anderzijds een hoog beschermingsniveau, zou het in de toekomst een mijlpaal kunnen vormen naar een Europese norm.

Le Conseil des universités flamandes a également demandé que soit développé un régime unique européen pour la recherche

Même si l'idée est séduisante, le présent titre ne prend pas en compte les traitements intereuropéens à des fins de recherche parce que le Règlement ne l'y autorise pas. Il existe uniquement le considérant 159 qui invite à tenir compte de l'article 179 TFUE.

Les articles 89.2 et 3 du Règlement ne donne dès lors que deux choix aux législateurs nationaux:

— soit déposer un projet de loi qui établisse des garanties appropriées en contrepartie de la limitation des droits de la personne concernée dans le domaine de la recherche, avec le risque que les garanties appropriées soient un frein à la recherche transfrontalière;

— soit ne rien faire, auquel cas les traitements à des fins de recherche sont soumis aux droits pleins et entiers des personnes concernées ce qui constitue un frein au moins aussi important à la recherche.

Les responsables du traitement de recherche qui craignent que les garanties appropriées déterminées dans le projet de loi ne compromettent leurs recherches transfrontalière demeurent libres de ne pas suivre le présent titre. Dans ce cas, ils devront néanmoins appliquer pleinement les droits des personnes concernées à leur traitements tel que prévu par l'article 89.1 du Règlement.

Ce projet, loin de nuire à la compétitivité de nos centres de recherches, leur donnent une sécurité juridique. Et loin d'isoler les chercheurs belges de leurs collègues européens, grâce à son équilibre entre d'une part le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques et d'autre part un haut niveau de protection, il pourrait constituer à l'avenir un jalon vers une norme européenne.

Advies van de Raad van State

De opmerkingen van de Raad van State werd opgenomen in dit wetsontwerp.

ARTIKELSGEWIJZE TOELICHTING

HOOFDSTUK I

Algemene bepalingen

Art. 186

De opmerkingen van de Privacycommissie en de Raad van State werden beantwoord door de draagwijdte van huidige titel te verduidelijken die enkel de artikelen 89.2 en 89.3 van de Verordening ten uitvoer brengen.

Art. 187

Dit artikel voorziet dat de gepaste waarborgen van huidige titel niet van toepassing kunnen zijn terwijl de verwerkingsverantwoordelijke zich toch kan beroepen op de afwijkingen van de rechten van de betrokkenen maar op voorwaarde van het gebruik van een gedragscode. Er bestaan dus twee manieren voor een verwerkingsverantwoordelijke om af te wijken van de rechten van de betrokkenen:

— ofwel volgt hij de gepaste waarborgen voorzien in huidige titel;

— ofwel verwerkt hij de persoonsgegevens in het kader van een gedragscode overeenkomstig artikel 40 van de Verordening.

Deze wet voorziet dus dat een gedragscode een geldige passende waarborg kan vormen.

Art. 188

Veel termen gebruikt in deze titel werden reeds gedefinieerd in de Verordening en, zoals de Raad van State en de Privacycommissie in herinnering brengen, is het niet aan de Belgische wetgever om die termen te herdefiniëren.

Dit artikel definieert dan ook de termen waarvoor dat niet reeds is gebeurd in de Verordening met inbegrip van de overwegingen.

In antwoord op punten 275 en 276 van het advies van de Privacycommissie schrapt het ontwerp de definitie

Avis du Conseil d'État

Les remarques du Conseil d'État ont été intégrées au projet de loi.

COMMENTAIRES DES ARTICLES

CHAPITRE I^ER

Dispositions générales

Art. 186

Il a été répondu aux remarques de la Commission vie privée et du Conseil d'État en clarifiant la portée du présent titre, qui met en œuvre uniquement les articles 89.2 et 89.3 du Règlement.

Art. 187

Cet article prévoit que les garanties appropriées du présent titre peuvent ne pas s'appliquer mais tout de même permettre au responsable du traitement de se prévaloir des dérogations aux droits des personnes mais à condition d'utiliser un code de conduite. Ainsi il y a deux manières pour un responsable du traitement de déroger aux droits des personnes concernées:

— soit il suit les garanties appropriées prévues dans le présent titre;

— soit il traite les données à caractère personnel dans le cadre d'un code de conduite conformément à l'article 40 du Règlement.

La présente loi prévoit donc que le code de conduite puisse valablement constituer une garantie appropriée.

Art. 188

Beaucoup de termes utilisés dans le présent titre sont déjà définis dans le Règlement et, comme le rappellent le Conseil d'État et la Commission vie privée, il n'appartient pas au législateur belge de redéfinir ces termes.

Alors cet article définit les termes qui ne le sont pas déjà dans le Règlement, y compris ses considérants.

En réponse aux points 275 et 276 de l'avis de la Commission vie privée, le projet supprime sa définition

van verwerkingen met het oog op archivering in het algemeen belang.

Zelfs indien de Privacycommissie kan worden bijgetreden wanneer zij zegt dat een document geen statuut van archief heeft vanaf diens overdracht naar een archiveringsorgaan, maar wel vanaf het ogenblik dat het geen functioneel nut meer heeft, moet er uit de afwezigheid van een definitie niet worden afgeleid dat het statuut van archief begint vanaf het ogenblik dat het document geschreven is: zolang het document leeft wordt het niet vrijgesteld van het toegangsrecht en het recht op rectificatie van de betrokkenen.

Archieven kunnen allerlei vormen aannemen. Naast schriftelijke documenten kan het archief ook bestaan uit foto's, filmmateriaal, interviews met de betrokkene, enz.

Tot slot geeft dit wetsontwerp geen definitie van het algemeen belang dat de verwerking met het oog op archivering verantwoordt: het gaat om een evolutief begrip dat niet in een wet kan worden gegoten en dat bovendien niet valt onder de bescherming van de persoonlijke levenssfeer.

Huidige titel definieert drie nieuwe begrippen: bekendmaking van de gegevens, verspreiding van gegevens en derde vertrouwenspersoon.

Art. 189

Met betrekking tot door de politie verrichte verwerkingen met het oog op archivering, onderzoek of statistische doeleinden onderscheidt Richtlijn twee soorten verwerkingen.

Enerzijds zijn er de verwerkingen met het oog op archivering, onderzoek of statistische doeleinden die strekken tot de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

In artikel 4.3 van de Richtlijn is daarover het volgende bepaald: "*Verwerking door dezelfde of een andere verwerkingsverantwoordelijke kan onder meer omvatten archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of gebruik voor statistische doeleinden voor de in artikel 1, lid 1, bedoelde doeleinden, mits is voorzien in passende waarborgen voor de rechten en vrijheden van de betrokke.*"

des traitement à des fins d'archivistiques d'intérêt général.

Si l'on rejoint la Commission vie privée pour dire qu'un document a un statut d'archive non pas à partir de son transfert à l'organisme d'archivage mais bien à partir du moment où le document n'a plus d'utilité fonctionnelle, il ne doit pas être déduit de l'absence de définition que le statut d'archive commence dès le moment où le document est écrit: tant que le document est vivant, il n'est pas exempté des droits d'accès et de rectification des personnes concernées.

Les archives peuvent être de différentes natures. A côté des documents écrits, les archives peuvent également être constituées de photos, de films, d'interviews des personnes concernée, etc.

Enfin, ce projet de loi ne définit pas ce qu'est l'intérêt général qui justifie le traitement à des fins d'archives: c'est une notion évolutive qui ne peut être figée dans une loi et qui, en outre, ne relève pas de la protection de la vie privée.

Le présent titre définit trois nouveaux termes: communication des données, diffusion des données et tiers de confiance.

Art. 189

Concernant les traitements à des fins d'archives, de recherche ou statistique effectués par la police, la Directive distingue deux types de traitements.

D'une part, les traitements à des fins d'archives, de recherche ou statistique effectués à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

L'article 4.3 de la Directive dispose à cet égard que: "*Le traitement des données par le même ou par un autre responsable du traitement peut comprendre 'l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, aux fins énoncées à l'article 1er, paragraphe 1er, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée'*".

Vallen onder die categorie: analysewerk in een labo, beleidsanalyse, statistische politie... Voor die verwerkingen geldt de algemene regeling van de Richtlijn, omgezet in titel 2 van deze kaderwet.

Anderzijds vallen de verwerkingen met het oog op archivering, onderzoek of statistische doeleinden voor andere doeleinden dan de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, onder het toepassingsgebied van artikel 89 van de Verordening.

In artikel 9.2 van de Richtlijn is immers het volgende bepaald: "*Wanneer aan bevoegde autoriteiten krachtens het lidstatelijke recht andere taken dan die ter verwezenlijking van de in artikel 1, lid 1, omschreven doeleinden worden toevertrouwd, is Verordening (EU) 2016/679 van toepassing op verwerking voor die doeleinden, waaronder archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden [..”]*".

Die verwerkingen hebben geen operationeel doeleinde en volgen de in deze titel vastgestelde regeling.

Voor de door de inlichtingen en veiligheidsdiensten of andere overheden bedoeld in titel 3 verrichte verwerkingen met het oog op archivering, onderzoek of statistische doeleinden geldt de regeling die in titel 3 van deze wet dit wetsontwerp is vastgesteld.

HOOFDSTUK II

Algemene waarborgen

Art. 190

Artikel 37 van de Verordening bepaalt de gevallen waarin de verwerkingsverantwoordelijke een functionaris voor gegevensbescherming aanwijst.

Niettemin voorziet het wetsontwerp in de uitbreiding van de verplichte benoeming van een functionaris voor gegevensbescherming tot alle verwerkingen met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, wanneer deze mogelijks een hoog risico kunnen doen ontstaan voor de betrokkenen. Hiermee wordt beantwoord aan punt 258 van het advies van de Privacycommissie.

Het huishoudelijk reglement van de rechtspersonen zal bepalen op welk niveau van de organisatie de functionaris voor gegevensbescherming wordt benoemd: de universiteit, de faculteit, het onderzoekscentrum.

Tombent dans cette catégorie: le travail d'analyse en laboratoire, l'analyse stratégique, la police statistique… Ces traitements suivent le régime général de la Directive, transposée dans le titre 2 de la présente loi.

D'autre part, les traitements à des fins d'archives, de recherche ou statistique effectués à des fins autres que de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, tombent dans le champ d'application de l'article 89 du Règlement.

L'article 9.2 de la Directive dispose en effet que: "*Lorsque les autorités compétentes sont chargées par le droit d'un État membre d'exécuter des missions autres que celles exécutées pour les finalités énoncées à l'article 1er, paragraphe 1er, le règlement (UE) 2016/679' s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques…*".

Ces traitements n'ont pas de finalité opérationnelle et suivent le régime établi par le présent titre.

Concernant les traitements à des fins d'archives, de recherche ou statistique effectués par les services de renseignements et de sécurité ou d'autres autorités visées au titre 3, ceux-ci suivent le régime établi par le titre 3 de ce projet de loi.

CHAPITRE II

Garanties générales

Art. 190

L'article 37 du Règlement dispose des cas dans lesquels le responsable du traitement doit désigner un délégué à la protection des données.

Le projet de loi étend néanmoins l'obligation de nommer un délégué à la protection des données à tous traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, lorsque ceux-ci sont susceptible d'engendrer un risque élevé pour les personnes concernées. Ceci répond au point 285 de l'avis de la Commission vie privée.

Le règlement interne des personnes morales déterminera à quel niveau de l'organisation le délégué à la protection des données est désigné: l'université, la faculté, le centre de recherche.

Met betrekking tot de individuele onderzoekers of kleine organisaties bepaalt artikel 37 van de Verordening dat het mogelijk is om een deeltijdse of een externe functionaris voor gegevensbescherming te hebben, en dat verscheidene verwerkingsverantwoordelijken zich kunnen groeperen om een functionaris voor gegevensbescherming te hebben.

Art. 191 tot 192

Het wetsontwerp voorziet in de uitbreiding van het verplicht bijhouden van een register tot alle verwerkingen met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Zoals hoger al aangehaald kan het feit af te wijken van de rechten van de betrokkenen op zich beschouwd worden als een risico en elke situatie waarbij wordt afgeweken moet kunnen genieten van een raadgeving, zelfs algemeen, om de verwerking tot een goede einde te brengen door de risico's die ze inhoudt te beheersen. Daarenboven te dienen als een procedureel stuk in geval van een controle, heeft het register in de eerste plaats de verdienste als hulpmiddel te dienen voor de verwerkingsverantwoordelijken om de elementen tot bescherming van de gegevens te kunnen organiseren en de oefening tot bevraging en rechtvaardiging van zijn keuze te verwezenlijken. Het gaat dus minder om een formaliteit dan om een instrument van bewustwording van het belang van gegevensbescherming.

Tot slot kan moeilijk gezegd worden dat, voor de verwerkingsverantwoordelijke die gegevensbescherming in zijn overwegingen opneemt, het invullen van enkele vakjes in een register een tijd- en energierovend werk uitmaakt. Het gaat niet meer en niet minder dan om overwegingen op papier te zetten die in ieder geval plaats moeten vinden voor de verwerkingsverantwoordelijke die zich op deze titel wil beroepen.

Om deze redenen wordt beslist de punten 286 en 287 van het advies van de Privacycommissie niet te volgen.

Op grond van verscheidene artikelen van dit wetsontwerp zijn de verwerkingsverantwoordelijken daarenboven verplicht om bijzondere vermeldingen in hun register toe te voegen.

Het huishoudelijk reglement van de rechtspersonen zal bepalen op welk niveau van de organisatie het register wordt bijgehouden: de universiteit, de faculteit, het onderzoekscentrum.

Pour les chercheurs individuels ou les petites organisations, l'article 37 du Règlement dispose qu'il est possible d'avoir un délégué à la protection des données à temps partiel, un délégué à la protection des données externe et que plusieurs responsables du traitement peuvent se grouper pour avoir un délégué à la protection des données.

Art. 191 à 192

Le projet de loi étend l'obligation de tenir un registre à tous traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Comme dit plus haut, le simple fait de déroger aux droits des personnes concernées peut être considéré comme un risque en soit et toute situation de dérogation doit pouvoir disposer d'un conseil, même générique, pour mener à bien son traitement de données en maîtrisant les risques qu'il comporte. En plus de servir de pièce procédurale en cas de contrôle, le registre a d'abord le mérite de servir d'aide aux responsables du traitement pour organiser les éléments de protection des données et de réaliser l'exercice questionnement et de justification de ses choix. Il s'agit donc moins d'une formalité que d'un outil de prise de conscience de l'importance de la protection des données.

Enfin, pour le responsable du traitement qui intègre la protection des données dans sa réflexion, on ne peut pas dire que les quelques champs à remplir dans le registre représentent un travail chronophage ou énergivore. Il s'agit ni plus ni moins de mettre sur papier des réflexions qui doivent de toute façon avoir lieu pour le responsable du traitment qui veut se prévaloir du présent titre.

Pour ces raisons, il est décidé de ne pas suivre les points 286 et 287 de l'avis de la Commission vie privée.

Différents articles de ce projet de loi contraignent en outre le responsable du traitement à ajouter des mentions particulières dans son registre.

Le règlement interne des personnes morales déterminera à quel niveau de l'organisation le registre est tenu: l'université, la faculté, le centre de recherche.

HOOFDSTUK III

Gegevensverzameling

Art. 193

Artikel 13 van de Verordening bepaalt reeds de minimuminhoud van de informatie die moet worden verstrekt aan de betrokkene wanneer de gegevens rechtstreeks bij hem worden verzameld. Aan die vermeldingen worden op grond van dit wetsontwerp nog de volgende toegevoegd: de anonimisering of eventuele pseudonimisering van de gegevens na verzameling ervan; en de redenen waarom de uitoefening van de rechten van de betrokkene de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren.

Voor het overige wordt op de punten 319 tot 324 van het advies van de Privacycommissie geantwoord door de verwijzing naar de toestemming te schrappen. We weerhouden echter dat toestemming niet een wettelijke grondslag kan zijn van de verwerking maar een gepaste waarborg die de verwerkingsverantwoordelijke kan voorzien.

Wat betreft de toestemming moet genoteerd worden dat, wanneer de verwerkingsverantwoordelijke beslist er een wettelijke grondslag van te maken hij rekening kan houden met overweging 33 van de Verordening die de ruime toestemming definieert. De doeleinde kan worden omschreven als “onderzoek tegen kanker” maar het is daarentegen niet toegelaten dat ze zo breed zou zijn als “onderzoek” of “medisch onderzoek”.

Er moet nog onderstreept worden dat andere reglementeringen een toestemming vereisen, bijvoorbeeld de Verordening 536/2014 betreffende klinische proeven of nog de Richtlijn 2004/23 betreffende menselijke weefsels en cellen. Hieruit moet echter niet worden besloten dat de vereiste toestemming in deze regelgevingen moet overeenkomen met de rehtsgrond die gebruikt wordt in het kader van het onderzoek. Ook al wordt dezelfde term gebruikt, het gaat om twee verschillende concepten die niet mogen worden verward. We verwijzen hier naar de richtlijnen “*Article 29 Working Party Guidelines on consent under Regulation 2016/679*” aangenomen op 10 april 2018. Toestemming kan een procedurele vereiste zijn afkomstig uit een andere tekst, zelfs een gepaste waarborg in de zin van artikel 89.1 van de Verordening maar zonder evenwel de rechtsgrond te zijn in de zin van de Verordening. Bijvoorbeeld, het intrekken van de toestemming door een deelnemer aan een klinische proef zal niet verplicht tot gevolg hebben dat de gegevens die reeds werden verzameld in het kader van de klinische proef moeten worden gewist.

CHAPITRE III

Collecte de données

Art. 193

L’article 13 du Règlement détermine déjà le contenu minimal de l’information à donner à la personne concernée lorsque les données sont collectées directement auprès d’elle. A ces mentions, l’article du projet de loi ajoutent les mentions suivantes: l’anonymisation ou la pseudonymisation éventuelle des données après leur collecte; et des motifs selon lesquels l’exercice des droits de la personne concernée risque de rendre impossible ou d’entraver sérieusement la réalisation des finalités spécifiques

Pour le surplus, on répond aux points 319 à 324 de l’avis de la Commission vie privée en supprimant la référence au consentement. On maintient cependant que le consentement peut ne pas être une base légale de traitement mais une garantie appropriée que le responsable du traitement peut prévoir.

A propos du consentement, il est à noter que lorsque le responsable du traitement décide d’en faire une base légale, il peut tenir compte du considérant 33 du Règlement, qui définit le consentement large. La finalité peut être de la sorte décrite comme étant “recherche contre le cancer”. Il n’est en revanche pas admissible qu’elle soit par exemple aussi large que “recherche” ou “recherche médicale”.

Il faut encore souligner que d’autres règlementations exigent un consentement, comme par exemple le Règlement 536/2014 sur les essais cliniques ou encore la Directive 2004/23 sur les tissus et cellules humaines. Pour autant, il ne faut pas en conclure que le consentement exigé dans ces règlementations doit correspondre à la base légale utilisée dans le cadre de la recherche. Bien que dénomée par le même terme, il s’agit de deux concepts différents qui ne doivent pas être confondus. On se réfère aux lignes directrices *“Article 29 Working Party Guidelines on consent under Regulation 2016/679*” adoptée le 10 avril 2018. Le consentement peut être une exigence procédurale issue d’un autre texte, voire même une garantie appropriée au sens de l’article 89.1 du Règlement, sans pour autant être une base légale au sens du Règlement. Par exemple, le retrait du consentement par un participant à un essai clinique n’aura pas obligatoirement pour conséquence l’effacement des données déjà récoltée dans le cadre de l’essai clinique.

Wat de rechtsgrond voor de verwerking van gevoelige gegevens betreft, bepaalt artikel 9.2.j van de Verordening dat gevoelige gegevens mogen worden verwerkt met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden "*op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.*".

Dit wetsontwerp voorziet in passende specifieke maatregelen voor de bescherming van de grondrechten. Zij vormt dus een rechtsgrond voor de verwerking van gevoelige gegevens met het oog op archivering, onderzoek of statistische doeleinden.

Art. 194

Er wordt geantwoord op punt 347 van het advies van de Privacycommissie door te verduidelijken in artikel 187*bis* dat huidige titel de artikelen 89.2 en 89.3 van de Verordening uitvoeren. De overeenkomst die in dit artikel wordt voorzien wordt aldus beschouwd als een gepaste waarborg.

Wanneer dezelfde verwerkingsverantwoordelijke een verdere verwerking verricht, wordt een overeenkomst afgesloten tussen de dienst, faculteit of kenniscentrum die de oorspronkelijke verwerking heeft verricht en de dienst, faculteit of kenniscentrum die de verdere verwerking verricht.

Binnen een universiteit sluit een faculteit een overeenkomst af met een andere faculteit. Binnen een administratie of gemeente sluit de archiefdienst een overeenkomst af met de andere diensten die een archief aanleggen.

Het tweede lid stelt de verantwoordelijke voor de verdere verwerking die openbaar gemaakte gegevens door de betrokken persoon of door de verwerkingsverantwoordelijke overeenkomstig artikel 6 van de verordening verzamelt vrij van de verplichting tot het afsluiten van een overeenkomst met de verantwoordelijke voor de oorspronkelijke verwerking.

Een openbare gegevensverwerking wordt gedefinieerd als een verwerking zonder beperking tot toegang, noch voor de betrokken personen, noch voor derden.

Concernant la base légale des traitements de données sensibles, l'article 9.2.j du Règlement dispose que les fins archivistiques dans l'intérêt public, de recherche scientifique ou historique ou à des fins statistiques peuvent traiter des données sensibles "*sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.*".

Ce projet de loi prévoit des mesures appropriées spécifiques pour la sauvegarde des droits fondamentaux. Elle constitue donc une base légale pour le traitement des données sensibles à des fins d'archives, de recherche ou statistiques.

Art. 194

On répond au point 347 de l'avis de la Commission vie privée en précisant à l'article 187*bis* que le présent titre exécute les articles 89.2 et 89.3 du Règlement. On considère dès lors que la convention prévue dans cet article constitue une garantie appropriée.

Lorsque le traitement ultérieur est opéré par le même responsable du traitement mais par des entités différentes, par exemple quand l'université est un seul et même responsable du traitement, une convention est passée entre le service, la faculté, le centre de recherche qui a opéré le traitement originel et celui qui opère le traitement ultérieur.

Au sein d'une université, une faculté passera une convention avec une autre faculté. Au sein d'une administration ou d'une commune, le service d'archives passera une convention avec les autres services producteur d'archives.

Le second alinéa exempte le responsable du traitement ultérieur qui collecte des données rendues publiques par la personne concernée ou par le responsable du traitement conformément à l'article 6 du Règlement, de l'obligation de passer une convention avec le responsable du traitement initial.

Un traitement public de données se définit comme un traitement sans limite d'accès ni pour les personnes concernées ni pour les tiers.

Om de openbare aard van de persoonsgegevens te bepalen, kunnen we ons ook baseren op een arrest van het Hof van Cassatie van 28 maart 2017, dat bepaalt dat onder semi openbaar belang dient verstaan te worden dat er toegangsformaliteiten kunnen bestaan, bijvoorbeeld tot een forum, maar dat er dan enerzijds een niet uitdagende fictieve identiteit gebruikt moet worden en dat er anderzijds geen controle op de juistheid van de toegangsgegevens mag gebeuren. Om deze redenen wordt beslist niet het punt 348 van het advies van de Privacycommissie te volgen.

Het tweede lid beoogt ook de vrijstelling van de verplichting inzake overeenkomst voor de verwerkingsverantwoordelijken die wettelijk verplicht zijn de gegevens voor archivering, met het oog op wetenschappelijk onderzoek of voor statistische doeleinden te verzamelen en te verwerken.

Hierbij wordt in het bijzonder gedacht aan de wet van 4 juli 1962 betreffende de openbare statistiek, die het Nationaal Instituut voor de statistiek belast met het verzamelen van gegevens teneinde statistieken op te maken betreffende de demografische, economische, sociale, ecologische en technologische toestand.

Ook wordt gedacht aan het samenwerkingsakkoord van 15 juli 2014 tussen de Federale Staat en de gemeenschappen en gewesten betreffende de nadere regels voor de werking van het Interfederaal Instituut voor de statistiek, van de raad van bestuur en de Wetenschappelijke Comités van het Instituut voor de nationale rekeningen.

Hierbij wordt nog gedacht aan de archiefwet, die het Algemeen Rijksarchief belast met het verwerven van het rijksarchief en die de overheidsdepartementen, provincies, hoven en rechtbanken verplicht om hun archief over te brengen aan het Algemeen Rijksarchief.

Ook wordt gedacht aan artikel 132 van de gemeentewet (W. 27.5 1989, B.S. 30.5 1989) in de Brusselse gemeenten die bepaalt dat: *"Het college van burgemeester en schepenen zorgt voor de bewaring van het archief.".*

In dat geval kan er geen sprake van een overeenkomst zijn, aangezien de verantwoordelijke voor de oorspronkelijke verwerking niet mag weigeren om de gegevens te verstrekken.

Teneinde de verantwoordelijke voor de verdere verwerking vrij te stellen van de verplichting tot het ondertekenen van een overeenkomst met de verantwoordelijke voor de oorspronkelijke verwerking, legt dit wetsontwerpwet twee voorwaarden op: de verantwoordelijke

Pour déterminer la nature publique de la donnée personnelle, on peut aussi s'appuyer sur un arrêt de la Cour de Cassation du 28 mars 2017, qui détermine que par intérêt semi public, il faut entendre qu'il peut y avoir des formalités d'accès, à un forum par exemple, mais qu'alors d'une part on doit recourir à une identité fictive non provocante, et d'autre part il ne doit pas y avoir de contrôle de l'exactitude des données d'accès. Pour ces raisons, il est décidé de ne pas suivre le point 348 de l'avis de la Commission vie privée.

L'alinéa 2 exempte également de l'obligation de convention les responsables du traitement qui ont l'obligation légale de collecter et de traiter les données à des fins d'archives, de recherche scientifiques ou statistiques.

On songe en particulier à la loi du 4 juillet 1962 relative à la statistique publique, qui charge l'Institut national de statistique de collecter des données afin de réaliser des statistiques sur la situation démographique, économique, sociale, écologique, technologique.

On songe également à l'accord de coopération du 15 juillet 2014 entre l'État fédéral et les Régions et Communautés concernant les modalités de fonctionnement de l'Institut interfédéral de statistique, du conseil d'administration et des Comités scientifiques de l'Institut des comptes nationaux.

On songe à la loi sur les archives, qui donne mission aux archives générales du Royaume de collecter les archives de l'État et obligation aux départements publics, provinces et cours et tribunaux de transmettre leurs archives aux Archives générales du Royaume.

On songe également à l'article 132 de la loi communale en Région bruxelloise (loi du 27.5 1989, M.B. 30.5 1989) qui dispose que: "*le collège des bourgmestre et échevins veille à la garde des archives.".*

Dans ce cas, il ne peut être question de convention car le responsable du traitement initial ne peut refuser de fournir les données.

Pour exempter le responsable du traitement ultérieur de l'obligation de signer une convention avec le responsable du traitement initial, ce projet de loi impose deux conditions: une loi particulière, un décret ou une ordonnance doit donner pour mission au responsable

voor de verdere verwerking moet op grond van een bijzondere wet, een decreet of een ordonnantie opdracht hebben gekregen om gegevens te verwerken met het oog op archivering, onderzoek of statistische doeleinden en moet het gebruik van de verzamelde gegevens voor andere doeleinden verboden zijn.

Wat het verbod op het gebruik van de gegevens voor andere doeleinden betreft, moet worden verduidelijkt dat – zoals aangehaald in overweging 158 van de Verordening – het verzamelen van de gegevens met het oog op archivering bedoeld is om ze ter beschikking te stellen van het publiek. Zij zijn dus herbruikbaar door andere verwerkingsverantwoordelijken met het oog op historisch/sociologisch onderzoek of statistische doeleinden.

Art. 195

Terwijl de artikelen 13 en 14 van de Verordening de inhoud bepalen van de informatie die moet worden verstrekt aan de betrokkene, geeft de Verordening geen nadere omschrijving van de inhoud van de informatie die door de verantwoordelijke van de verdere verwerking moet worden verstrekt aan de verantwoordelijke van de oorspronkelijke verwerking.

Het oorspronkelijke ontwerp hernam de inhoud bepaald in de artikelen 13 en 14 van de Verordening. De punten 353 en volgende van het advies van de Privacycommissie worden gevolgd en het ontwerp wordt dus op dit punt herzien. De inhoud van de overeenkomst wordt beperkt tot de contactgegevens van de verwerkingsverantwoordelijken en tot de redenen waarom de uitoefening van de rechten van de betrokkene de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren.

Art. 196

Dit artikel vergt geen commentaar.

Art. 197

Dit artikel nodigt de verwerkingsverantwoordelijke uit om de middelen te onderzoeken die hem ter beschikking staan om de doeleinden van zijn verwerking te bereiken in de zin dat de persoonsgegevens slechts worden gebruikt wanneer het strikt noodzakelijk is. In bepaalde gevallen blijkt het mogelijk om met geanonimiseerde gegevens te werken. Indien dat niet het geval is moet de verwerkingsverantwoordelijke de mogelijkheid voorzien

du traitement ultérieur de traiter des données à des fins d'archives, de recherche ou statistique et elle doit interdire l'utilisation des données collectées à d'autres fins.

Concernant l'interdiction d'utiliser les données à d'autres fins, il faut préciser que, comme le rappelle le considérant 158 du Règlement que les données collectées à des fins d'archives sont collectées afin d'être mises à la disposition du public. Elles sont donc réutilisables par d'autres responsables du traitement à des fins de recherches historiques, sociologiques ou statistiques.

Art. 195

Alors que les articles 13 et 14 du Règlement déterminent le contenu de l'information à donner à la personne concernée, le Règlement ne détermine pas le contenu de l'information à donner par le responsable du traitement ultérieur au responsable du traitement initial.

Le projet initial reprenait le contenu de l'information déterminée dans les articles 13 et 14 du Règlement. On suit partiellement les points 353 et suivants de l'avis de la Commission vie privée, le projet a été revu sur ce point et le contenu de la convention limité aux données de contact des responsables du traitement et aux motifs selon lesquels l'exercice des droits de la personne concernée risque de rendre impossible ou d'entraver sérieusement la réalisation de la finalité du traitement ultérieur.

Art. 196

Cet article n'appelle pas de commentaires.

Art. 197

Cet article invite le responsable du traitement à examiner les moyens à sa disposition pour atteindre les finalités de son traitement de manière à utiliser les données personnelles lorsqu'elles sont strictement nécessaires. Dans certains cas, il s'avère possible de travailler sur des données anonymes. Si cela n'est pas possible, le responsable du traitement doit envisager la possibilité de travailler sur des données pseudonymisées. Enfin,

om te werken met gespeudonimiseerde gegevens. Tot slot, indien dat niet mogelijk is zal de verwerkingsverantwoordelijke werken met niet-gepseudonimiseerde gegevens.

Wat betreft geanonimiseerde gegevens bestaat er een debat omtrent de vraag inzake heridentificering. Meerdere studies hebben aangetoond dat het slechts zelden, zelfs nooit, onmogelijk is een geanonimiseerd gegeven te heridentificeren. Anderen verzekeren daarentegen dat het de ideale oplossing is om gegevens te verwerken omdat ze niet meer persoonlijk zijn en dus niet meer in het toepassingsgebied van de Verordening vallen of meer algemeen van de wetten met betrekking tot de bescherming van de persoonlijke levenssfeer.

Dit wetsontwerp heeft niet de roeping om te beslissen tussen de verschillende standpunten in dit debat. De wil van de wetgever is eerder om de verwerkingsverantwoordelijke uit te nodigen om de verschillende mogelijkheden te onderzoeken die hem ter beschikking staan om zijn doeleinden te bereiken. De anonimisering moet niet beschouwd worden als een manier om zich te onttrekken aan de veiligheidsprincipes met betrekking tot de bescherming van gegevens.

Zo kan het in bepaalde gevallen mogelijk zijn om niet met geanonimiseerde gegevens te werken maar wel om anoniem te werken met gegevens. Bijvoorbeeld, wanneer een onderzoeker reeds verzamelde gegevens wil hergebruiken kan een manier zijn om zich te associëren met de oorspronkelijke verwerkingsverantwoordelijke om de gegevensverwerking te doen zonder evenwel toegang te hebben tot de gegevensbank in kwestie.

Het is niet altijd mogelijk om in het begin van het onderzoek te weten of het mogelijk is om met gepseudonimiseerde of geanonimiseerde gegevens te werken.

De onderzoeker zal vervolgens in het register de redenen verantwoorden waarom de uitoefening van de rechten van de betrokkene dreigen de verwezenlijking van het doeleinde van het onderzoek onmogelijk te maken of ernstig te bedreigen.

Artikel 89 van de Verordening bepaalt dat de passende waarborgen:

— pseudonimisering inhouden;

— de voorkeur geven aan verdere verwerkingen die de identificatie van betrokkenen niet of niet langer toelaten.

si cela n'est pas possible, le responsable du traitement travaillera sur des données non-pseudonymisées.

A propos des données anonymisées, il existe un débat autour de la question de la réidentification. De nombreuses études ont démontré qu'il n'est que très rarement, voire jamais, impossible de réidentifier une donnée rendue anonyme. D'autres, au contraire assurent que c'est la solution idéale pour traiter des données puisque celles-ci ne sont plus personnelles et ne tombent dès lors plus dans le champ d'application du Règlement ou plus généralement des lois relatives à la protection de la vie privée.

Ce projet de loi n'a pas vocation à trancher entre les différentes positions dans ce débat. La volonté du législateur est plutôt d'inviter le responsable du traitement à examiner les différentes possibilités qui s'offrent à lui pour atteindre ses finalités. L'anonymisation ne doit pas être considérée comme une manière de se soustraire aux principes de sécurité en matière de protection des données.

Ainsi, dans certains cas, il peut être possible de travailler non pas avec des données anonymisées mais bien de travailler de manière anonyme sur des données. Par exemple, lorsqu'un chercheur veut réutiliser des données déjà collectées, une manière de faire serait de s'associer avec le responsable du traitement initial pour mener à bien le traitement de données qu'il veut opérer sans pour autant avoir accès à la base de données en question.

Il n'est pas toujours possible au début de la recherche de savoir si la recherche est possible avec des données pseudonymisées ou anonymisées. Dans ce cas, le responsable du traitement explique dans son registre les motifs pour lesquels ce n'est pas possible.

Le chercheur justifiera ensuite dans le registre les motifs pour lesquels l'exercice des droits de la personne concernée risquent de rendre impossible ou d'entraver sérieusement la réalisation de la finalité de la recherche.

L'article 89 du Règlement dispose que les garanties appropriées:

— comprennent la pseudonimysation;

— privilégient les traitements ultérieurs ne permettant pas ou plus l'identification des personnes concernées.

Deze artikelen brengen die principes ten uitvoer. Die principes zijn niet van toepassing voor verwerkingen met het oog op archivering aangezien in de mate dat, om hun doeleinden te verwezenlijken, het de bedoeling is dat de archieven integraal moeten worden verworven en ter beschikking gesteld van het publiek.

De beginselen zijn ook niet van toepassing op de verwerkingen voor historische, statistische of wetenschappelijke doeleinden waarvan de verwerkingsverantwoordelijke, overeenkomstig artikel 99 van dit ontwerp, aantoont dat hij de doeleinden van de verwerking niet kan verwezenlijken met enkel beroep te doen op niet geprseudonymiseerde of niet geanonymiseerde persoonsgegevens.

De Privacycommissie meent in de punten 363 tot 367 van haar advies dat het vanzelfsprekend is dat persoonsgegevens in de mate van het mogelijke zo vroeg mogelijk gepseudonimiseerd moeten worden om in overeenstemming te zijn met de bepalingen van de Verordening.

In tegenstelling tot wat de Privacycommissie beweert is dit niet zo vanzelfsprekend en zijn de betrokken partijen niet altijd het best geplaatst om de regels inzake pseudonimisering te bepalen. De artikelen 89.2 en 89.3 van de Verordening vereisen bovendien dat de wet de regels inzake pseudonimisering bepaalt. Dit deel blijft dus behouden.

Art. 198

Dit artikel herneemt de principes uit artikel 8 van het koninklijk besluit van 13 februari 2001: wanneer een verantwoordelijke voor verwerking met het oog op onderzoek of statistische doeleinden gegevens verzamelt bij de betrokkenen, worden de gegevens geanonimiseerd of gepseudonimiseerd vóór de analyse ervan.

Vaak verzamelen de onderzoekers zelf de gegevens, verrichten zij betrouwbaarheids- en consistentietests en pseudonimiseren zij vervolgens de gegevens voorafgaandelijk aan hun kwalitatieve of kwantitatieve analyses.

In dat geval kan de onderzoeker zelf de gegevens anonimiseren of pseudonimiseren, maar vertrouwt hij vervolgens de pseudonimiseringssleutel toe aan de verwerkingsverantwoordelijke alvorens ze te analyseren.

Wanneer de onderzoeker niet zelf de gegevens verzamelt, pseudonimiseert de verwerkingsverantwoordelijke de gegevens alvorens ze mee te delen aan de onderzoeker.

Ces articles mettent en œuvre ces principes. Ces principes ne sont pas d'application pour les traitements à des fins d'archives, dans la mesure où, pour réaliser leurs finalités, elles doivent être collectées et mises à disposition du public intégralement.

Ces principes ne sont pas non plus d'application pour les traitements à des fins historiques, statistiques ou scientifiques dont le responsable du traitement démontre, conformément à l'article 99 du présent projet, qu'il ne peut réaliser la finalité du traitement qu'en ayant recours à des données à caractère personnel non pseudonymisées ou non anonymisées.

La Commission vie privée considère dans les points 363 à 367 de son avis qu'il va de soi que les données à caractère personnel doivent être pseudonymisées le plus tôt possible -dans la mesure du possible pour se conformer aux dispositions du Règlement.

Contrairement à ce qu'affirme la Commission vie privée, cela ne va pas de soi et les parties concernées ne sont pas toujours le mieux placées pour déterminer les règles de pseudonymisation. Les articles 89.2 et 89.3 du Règlement exigent en outre que la loi déterminent les règles de pseudonymisation. La section est donc maintenue.

Art. 198

Cet article reprend les principes de l'article 8 de l'arrêté royal du 13 février 2001: lorsqu'un responsable du traitement à des fins de recherche ou statistiques collecte des données auprès des personnes concernées, les données sont anonymisées ou pseudonymisées avant leur analyse.

Souvent ce sont les chercheurs eux-mêmes qui collectent les données, font des tests de fiabilité et de consistance et puis pseudonymisent les données avant leur analyses quantitatives ou qualitatives**.**

Dans ce cas, le chercheur peut anonymiser ou pseudonymiser les données lui-même mais il confie ensuite la clé de la pseudonymisation au responsable du traitement avant de les analyser.

Lorsque ce n'est pas le chercheur lui-même qui collecte les données, le responsable du traitement pseudonymise les données avant leur communication au chercheur.

Art. 199

Dit artikel herneemt het principe uit artikel 6 van het koninklijk besluit van 13 februari 2001: de gegevens mogen enkel gedepseudonimiseerd onder toezicht van de functionaris voor gegevensbescherming, desgevallend, en vanwege de noodwendigheden van het onderzoek (nazicht van de gegevens) of om een maatregel te treffen ten aanzien van de betrokkene, bijvoorbeeld een medische behandeling.

Art. 200

Dit artikel herneemt artikel 9 van het koninklijk besluit van 13 februari 2001: in het kader van een verdere verwerking door een verantwoordelijke voor verdere verwerking die verschillend is van de verantwoordelijke voor de oorspronkelijke verwerking pseudonimiseert of anonimiseert de verantwoordelijke voor de oorspronkelijke verwerking de gegevens alvorens ze mee te delen aan de verantwoordelijke voor verdere verwerking.

De kost en de betaler van de pseudonimisering of anonimisering van de gegevens wordt bepaald ofwel bij wet ofwel met onderlinge instemming tussen de oorspronkelijke en latere verwerkingsverantwoordelijke.

Hiertoe kan verwezen worden naar de wet van 4 mei 2016 inzake het hergebruik van informatie van de openbare sector waarin sommige bepalingen gaan over de verdeling van de kosten bij anonimisering.

Art. 201

Dit artikel herneemt de principes uit artikel 10 van het koninklijk besluit van 13 februari 2001: in het kader van een verdere verwerking die meerdere oorspronkelijke verwerkingen van gegevens combineert, pseudonimiseert of anonimiseert de verantwoordelijke voor de oorspronkelijke verwerking de gegevens alvorens ze mee te delen aan de verantwoordelijke voor verdere verwerking.

Niettemin zijn de verantwoordelijken voor de oorspronkelijke verwerkingen niet langer gedwongen de gegevens te laten pseudonimiseren door een derde vertrouwenspersoon.

De inschakeling van een derde vertrouwenspersoon blijkt immers duur en dreigt daardoor een rem te zetten op het onderzoek.

Art. 199

Cet article reprend le principe de l'article 6 de l'arrêté royal du 13 février 2001: les données ne peuvent être dépseudonymisées que sous le contrôle du délégué à la protection des données, le cas échéant, et pour les nécessités de la recherche (vérification des données) ou pour prendre une mesure à l'égard de la personne concernée, par exemple un traitement médical.

Art. 200

Cet article reprend l'article 9 de l'arrêté royal du 13 février 2001: lors d'un traitement ultérieur par un responsable du traitement ultérieur distinct du responsable du traitement initial, le responsable du traitement initial pseudonymise ou anonymise les données avant leur communication au responsable du traitement ultérieur.

Le coût et le payeur de la pseudonimysation ou de l'anonymisation des données est déterminé soit par la loi soit de commun accord entre les responsables du traitement initiaux et ultérieurs.

A cet égard, on peut citer la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public dont certaines dispositions traitent de la répartition des coûts en cas d'anonymisation.

Art. 201

Cet article reprend les principes de l'article 10 de l'arrêté royal du 13 février 2001: lors d'un traitement ultérieur recoupant plusieurs traitements de données initiaux, le responsable du traitement initial pseudonymise ou anonymise les données avant leur communication au responsable du traitement ultérieur.

Néanmoins, les responsables des traitements initiaux ne sont plus contraints à faire pseudonymiser les données par un tiers de confiance.

Le recours à un tiers de confiance apparait en effet coûteux et, par ce fait, risque d'être un frein à la recherche.

Een van de verantwoordelijken voor de oorspronkelijke verwerking kan zelf een pseudonimiseringssleutel aanleveren aan de overige verantwoordelijken voor de oorspronkelijke verwerkingen.

Wanneer een van de oorspronkelijke verwerkingen een verwerking van gevoelige gegevens is, is de verantwoordelijke voor de oorspronkelijke verwerking die de gegevens pseudonimiseert degene die de pseudonimiseringssleutel verstrekt aan de andere verantwoordelijken voor de oorspronkelijke verwerkingen.

Wanneer verschillende verantwoordelijken voor de initiële verwerking gevoelige gegevens verwerken, pseudonimiseert een van hen de gegevens.

Zij kunnen tevens een derde vertrouwenspersoon inschakelen voor de pseudonimisering van de gegevens.

Art. 202

Dit artikel huldigt de principes uit het koninklijk besluit van 13 februari 2001: de derde vertrouwenspersoon moet onafhankelijk zijn van de verantwoordelijken voor de verdere verwerkingen.

Art. 203

Dit artikel vergt geen commentaar.

Art. 204 en 205

In overweging 159 van de Verordening wordt verduidelijkt dat de verwerking zou moeten voldoen aan specifieke voorwaarden wat betreft het publiceren of openbaar maken van de gegevens.

De Privacycommissie brengt in herinnering dat artikel 89.1 van de Verordening geen enkele openingsclausule inhoudt voor de lidstaten en dringt op de schrapping van die artikelen aan (punt 382). Huidig ontwerp voert artikel 89.1 niet uit maar wel de artikelen 89.2 en 89.3 die een wet vereisen. De regels met betrekking tot de publicatie en verspreiding van gegevens worden beschouwd als gepaste waarborgen die noodzakelijk zijn wanneer een verwerkingsverantwoordelijke de uitoefening van de rechten van de betrokkene wenst te beperken. Dit deel blijft dus behouden.

Hoewel de verwerkingen om te archiveren of voor onderzoek of statistieken onderworpen zijn aan de opgelegde voorwaarden in deze titel, moet er rekening gehouden worden met de gevallen waar de

L'un des responsables du traitement initial peut lui-même fournir une clé de pseudonymisation aux autres responsables des traitements initiaux.

Lorsqu'un des traitements initiaux est un traitement de données sensibles, le responsable du traitement initial qui pseudonymise les données est celui qui fournit la clé de pseudonymisation aux autres responsables des traitements initiaux.

Lorsque plusieurs responsables du traitement initial traitent des données sensibles, l'un d'entre eux pseudonymise les données.

Ils peuvent également recourir à un tiers de confiance pour pseudonimyser les données.

Art. 202

Cet article reprend les principes de l'arrêté royal du 13 février 2001: le tiers de confiance doit être indépendant des responsables des traitements ultérieurs.

Art. 203

Cet article n'appelle pas de commentaires.

Art. 204 et 205

Le considérant 159 du Règlement précise que des conditions particulières devraient s'appliquer concernant la publication ou la divulgation des données.

La Commission vie privée rappelle que l'article 89.1 du Règlement ne contient aucune clause d'ouverture pour les États membres et insiste pour que ces articles soient supprimés (point 382). Le présent projet n'exécute pas l'article 89.1 mais bien les articles 89.2 et 89.3 qui requierent une loi. Il considère que des règles relatives à la publication et à la diffusion des données sont des garanties appropriées nécessaires lorsqu'un responsable du traitement souhaite limiter l'exercice des droits de la personne concernée. La section est donc maintenue.

Bien que les traitements à des fins d'archives, ou de recherche ou statistiques soient soumis aux conditions imposées dans le présent titre, il devra être tenu compte des cas où le responsable du traitement a pour mandat,

verwerkingsverantwoordelijke mandaat heeft om, in het kader van de uitoefening van zijn wettelijke taken, persoonsgegevens te verwerken met als doelstelling in het kader van de uitoefening van zijn wettelijke taken, om te archiveren, voor onderzoek of statistieken, en waarvoor er beveiligings- en vertrouwelijkheidsregels bestaan.

Bijvoorbeeld, daarenboven moeten de statistische autoriteiten bijvoorbeeld moeten bovendien het beginsel van statistische geheimhouding naleven.

Overweging 163 van de Verordening vermeldt dat "*De vertrouwelijke gegevens die statistische autoriteiten van de Unie en de lidstaten voor de productie van officiële Europese en officiële nationale statistieken verzamelen, moeten worden beschermd. Europese statistieken moeten worden ontwikkeld, geproduceerd en verspreid overeenkomstig de statistische beginselen van artikel 338, lid 2, VWEU; nationale statistieken moeten ook aan het lidstatelijke recht voldoen. […]".*

Er zal dus rekening gehouden worden met de nationale en *supra*nationale wettelijke bepalingen, van toepassing op de statistische autoriteiten inzake het verspreiden of communiceren van verwerkte gegevens voor statistische doeleinden; die ook nageleefd moeten worden om in overeenstemming te zijn met wat bepaald wordt in overweging 163 van de Verordening. Hetzelfde geldt voor de bepalingen voorzien in de wet van 4 juli 1962 betreffende de openbare statistiek, ook voor de bepalingen voorzien in de samenwerkingsovereenkomst van 15 juli 2014 betreffende de nadere regels voor de werking van het Interfederaal Instituut voor de statistiek, en voor de bepalingen opgenomen in Verordening (EG) nr. 223/2009 betreffende de Europese statistieken.

Dit wetsontwerp verbiedt de verspreiding, bijvoorbeeld, middels een schriftelijke publicatie of op het internet, van:

— niet-gepseudonimiseerde gegevens;

— gevoelige gepseudonimiseerde gegevens.

De niet-gepseudonimiseerde gegevens mogen echter worden verspreid wanneer de betrokkene zijn toestemming heeft gegeven of wanneer hij de gegevens openbaar heeft gemaakt of wanneer de gegevens nauw samenhangen met het openbare of historische karakter van de betrokkene of met de feiten waaraan hij gelinkt is.

Met betrekking tot dat laatste criterium, heeft het Hof van Justitie van de Europese Unie in zijn arrest van

dans le cadre de l'exercice de ses missions légales, de traiter des données à caractère personnel à des fins d'archives, de recherche ou statistiques, et pour lesquels il existe des règles de sécurité et de confidentialité.

Par exemple, les autorités statistiques sont soumises, au surplus, au respect du principe du secret statistique.

Le considérant 163 du Règlement mentionne que "*Les informations confidentielles que les autorités statistiques de l'Union et des États membres recueillent pour élaborer des statistiques officielles européennes et nationales devraient être protégées. Les statistiques européennes devraient être mises au point, élaborées et diffusées conformément aux principes statistiques énoncés à l'article 338, paragraphe 2, du traité sur le fonctionnement de l'Union européenne, et les statistiques nationales devraient également respecter le droit des États membres. […]*".

Il sera donc tenu compte des dispositions légales nationales et *supra*nationales, applicables aux autorités statistiques en matière de diffusion ou de communication des données traitées à des fins statistiques; lesquelles devront également être respectées pour se conformer au prescrit du considérant 163 du Règlement. Il en va ainsi des dispositions prévues dans la loi du 4 juillet 1962 relative à la statistique, de celles prévues dans l'accord de coopération du 15 juillet 2014 concernant les modalités de fonctionnement de l'Institut interfédéral de Statistique, ainsi que des dispositions reprises dans le Règlement (CE) n° 223/2009 relatif aux statistiques européennes.

Ce projet de loi interdit la diffusion, par exemple, par une publication écrite ou sur internet de:

— données non-pseudonymisées;

— données sensibles pseudonymisées.

Les données non pseudonymisées peuvent néanmoins être diffusées lorsque la personne a donné son consentement, ou lorsqu'elle a rendu les données publiques ou lorsque les données ont une relation étroite avec le caractère public ou historique de la personne concernée ou des faits auxquelles elle est liée.

Concernant ce dernier critère, la Cour de justice de l'Union européenne, dans son arrêt du 13 mai 2014

13 mei 2014 C-131/12, Google Spain SL, geoordeeld dat de rol van een persoon in het openbare leven de inmenging in het zijn privéleven van een persoon en de verspreiding van gegevens over hem: *"[Er moet] met name worden onderzocht of de betrokkene recht erop heeft dat de aan de orde zijnde informatie over hem thans niet meer met zijn naam wordt verbonden via een resultatenlijst die wordt weergegeven nadat op zijn naam is gezocht [...]. [Deze] rechten [krijgen] in beginsel voorrang [...] op het belang van dit publiek om toegang tot deze informatie te krijgen wanneer op de naam van deze persoon wordt gezocht. Dit zal echter niet het geval zijn indien de inmenging in de grondrechten van de betrokkene wegens bijzondere redenen, zoals de rol die deze persoon in het openbare leven speelt, wordt gerechtvaardigd door het overwegende belang dat het publiek erbij heeft om, door deze opneming, toegang tot de betrokken informatie te krijgen.".*

Voor wat betreft de rechten van de betrokkene, dient herhaald te worden dat de wet van 23 juni 1961 betreffende het recht tot antwoord van toepassing is op wetenschappelijke onderzoeksdoeleinden en dat de betrokkene een recht tot antwoord heeft om een zakelijk element recht te zetten of een aantasting van de eer af te weren.

Concernant la rectification d'un élément de fait, la jurisprudence souligne qu' il n'appartient à la personne concernée "*qui est prise à partie (…) d'apporter la preuve que les faits allégués sont inexacts, ce qui serait inverser la charge de la preuve"*.

Voor wat betreft de aantasting van de eer, meent de rechtspraak dat die "*le résultat d'un amalgame de faits sans doute exact mais présentés de manière tendancieuse*" (Bxl, 14 mai 1992, F-19920514-12) kan zijn.

Art. 206 en 207

Dit artikel verbiedt de verwerkingsverantwoordelijke om niet-gepseudonimiseerde gevoelige gegevens te reproduceren.

Het beoogt de invoering van de praktijk van "*safe rooms*", die de onderzoeker niet kan betreden met een fototoestel of scan en waarbij hij de documenten met niet-gecodeerde gevoelige gegevens niet kan reproduceren.

Wel mag de onderzoeker notities nemen en daarmee een gegevensbank creëren.

C-131/12, Google Spain SL, a jugé que le rôle d'une personne dans la vie publique peut justifier l'ingérence dans sa vie privée et à la diffusion de données qui la concernent: *"Il convient notamment d'examiner si la personne concernée a un droit à ce que l'information relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom (…) Ces droits prévalent (…) sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question.".*

Concernant les droits de la personne concernée, il faut rappeler que la loi du 23 juin 1961 relative au droit de réponse s'applique aux traitements à des fins de critique scientifique et que la personne concernée a un droit de réponse pour rectifier un élément de fait ou repousser une atteinte à l'honneur.

Concernant la rectification d'un élément de fait, la jurisprudence souligne qu' il n'appartient à la personne concernée "*qui est prise à partie (…) d'apporter la preuve que les faits allégués sont inexacts, ce qui serait inverser la charge de la preuve*".

Concernant l'atteinte à l'honneur, la jurisprudence considère que celle-ci peut être "le résultat d'un amalgame de faits sans doute exact mais présentés de manière tendancieuse" (Bxl, 14 mai 1992, F-19920514-12).

Art. 206 et 207

Cet article impose au responsable du traitement que les données sensibles non-pseudonymisées ne puissent être reproduites.

Il vise à instituer la pratique des "*safe room*" dans lesquelles le chercheur ne peut pénétrer avec un appareil photo, un scan et ne peut reproduire les documents sur lesquels figurent des données sensibles non-codées.

Par contre le chercheur est autorisé à prendre note et à constituer une banque de données avec ses notes.

TITEL 5

Rechtsmiddelen en vertegenwoordiging van de betrokkenen

De Verordening en de Richtlijn voorzien in een aantal rechtsmiddelen waarin in het nationale recht moet worden voorzien:

1. Artikelen 52 van de Richtlijn en 77 van de Verordening hebben betrekking op het beroep bij een toezichthoudende autoriteit. Dit zal worden geregeld in de organieke wetten waarin zij worden georganiseerd.

2. Artikelen 53 van de Richtlijn en 78 van de Verordening hebben betrekking op het beroep tegen een beslissing van de toezichthoudende autoriteit. Dit zal ook worden geregeld in de organieke wetten. Voor de Gegevensbeschermingsautoriteit bijvoorbeeld voorziet de organieke wet van 3 december 2017 in een beroep bij het Marktenhof.

3. Artikelen 56 van de Richtlijn en 82 van de Verordening hebben betrekking op de schadevergoeding. Die wordt beoogd in de artikelen 1382 en 1383 van het Burgerlijk Wetboek, die ruimschoots volstaan.

4. Artikelen 54 van de Richtlijn en 79 van de Verordening vereisen dat wordt voorzien in een doeltreffende voorziening in rechte tegen een verwerkingsverantwoordelijke of een verwerker. Dit moet specifiek door deze wetworden geregeld. Bovendien voorziet artikel 6 van de organieke wet van 3 december 2017 dat de Gegevensbeschermingsautoriteit bevoegd is om "*inbreuken op de grondbeginselen van de bescherming van de persoonsgegevens, in het kader van de wet en van de wetten die bepalingen bevatten inzake de bescherming van de verwerking van persoonsgegevens"* ter kennis te brengen van de gerechtelijke autoriteiten en, desgevallend, een rechtsvordering in te stellen teneinde deze grondbeginselen te doen naleven. Artikel 211, § 3, van deze wet voorziet dit ook.

5. Artikelen 55 van de Richtlijn en 80 van de Verordening bevatten ook modaliteiten voor de vertegenwoordiging van betrokkenen, die gedeeltelijk in deze wet worden vastgelegd.

Het gemeen recht alsook de specifieke regels zijn van toepassing. Er bestaan dus twee mogelijkheden:

— een gemeenschappelijke basis tot stand brengen met alle mogelijke rechtsmiddelen. Dit zou betekenen dat de bepalingen substantiëler moeten zijn; of

TITRE 5

Voies de recours et représentation des personnes concernées

Le Règlement et la Directive prévoient une série de recours qui doivent être prévues en droit national:

1. Les articles 52 de la Directive et 77 du Règlement concernent le recours auprès d'une autorité de contrôle. Ceci sera réglé dans les lois organiques qui les organisent.

2. Les articles 53 de la Directive et 78 du Règlement concernent le recours contre une décision de l'autorité de contrôle. Ceci sera également réglé dans les lois organiques. Pour l'Autorité de protection des données par exemple, la loi organique du 3 décembre 2017 prévoit un recours à la Cour des marchés.

3. Les articles 56 de la Directive et 82 du Règlement concernent la réparation d'un dommage. Celle-ci est visée par les articles 1382 et 1383 du Code civil, lesquels suffisent largement.

4. Les articles 54 de la Directive et 79 du Règlement exigent que soit prévu un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant. Ceci doit être prévu spécifiquement dans la présente loi. L'article 6 de la loi organique du 3 décembre 2017 prévoit en outre que l'Autorité de protection des données a le pouvoir de porter toute "*infraction aux principes fondamentaux de la protection des données à caractère personnel, dans le cadre de la loi et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel"*, à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice en vue de voir appliquer ces principes fondamentaux. L'article 211, § 3, de la présente loi le prévoit également.

5. Les articles 55 de la Directive et 80 du Règlement prévoient également des modalités pour la représentation des personnes concernées, lesquelles sont aménagées en partie dans la présente loi.

Le droit commun ainsi que des règles spécifiques s'appliquent. Il existe donc deux possibilités:

— établir un socle commun reprenant tous les recours possibles. Cela impliquerait que les dispositions soient plus substantielles; ou

— de organieke wetten van de toezichthoudende autoriteiten en het gemeen recht laten voorzien in de beoogde rechtsmiddelen.

De voorkeursoplossing hier is om enkel wat specifiek is in te voegen en naar de andere procedures van het gemeen recht te verwijzen. Deze oplossing is eenvoudiger en samenhangender, en biedt meer rechtszekerheid.

HOOFDSTUK I

Vordering tot staking

Art. 209 tot 219

In de Verordening en de Richtlijn wordt bepaald dat in het nationale recht wordt voorzien in een voorziening in rechte. Een voorziening in rechte moet dus worden georganiseerd. Het betreft een vordering tot staking en tot verkrijging van mededeling, opschorting en rectificatie van gegevens door de rechter zitting houdende zoals in kort geding.

Conform artikel 267 van VWEU, kan de voorzitter van de rechtbank van eerste aanleg ook gevat worden krachtens artikel 209 om een prejudiciële vraag te stellen aan het Hof van Justitie van de Europese Unie. In het arrest Schrems vs. Data protection Commissioner (C-362/14), heeft het Hof van Justitie geoordeeld dat het aan de nationale wetgever is om te voorzien in rechtsmiddelen die de bevoegde overheid in staat stelt de voor haar gegronde grieven te brengen voor de nationale rechtbanken zodat deze laatste, indien zij twijfelen aan de geldigheid van de handeling, een prejudiciële vraag stellen om de geldigheid van die handeling te onderzoeken (§ 65).

Deze artikelen nemen grotendeels artikel 14 WVP, die de vordering tot staking georganiseerd, over aangezien die bepaling zal worden opgeheven. Er moet evenwel goed worden opgelet voor de kruising van de strafrechtelijke, administratieve en andere procedures. Daarom wordt artikel 14 WVP overgenomen maar een specifieke bepaling voorziet dan ook erin dat het strafgerecht uitspraak doet wanneer een betwist gegeven in een strafdossier voorkomt. Het gaat niet enkel om een zaak die voor de strafrechter zou worden gebracht.

Onder de vordering tot staking moet worden begrepen de procedure volgens dewelke de voorzitter van de rechtbank van eerste aanleg, zitting houdende zoals in kort geding kennis neemt van de vorderingen betreffende:

— laisser les lois organiques des autorités de contrôle et le droit commun prévoir les recours envisagés.

La solution ici privilégiée est de n'insérer que ce qui est spécifique et renvoyer aux autres procédures de droit commun. Cette solution est plus simple et plus cohérente, et apporte plus de sécurité juridique.

CHAPITRE I^ER

Action en cessation

Art. 209 à 219

Le Règlement et la Directive prévoient qu'un recours juridictionnel soit prévu en droit national. Il s'agit donc du recours juridictionnel qui doit être organisé. Il s'agit d'une action en cessation ainsi que tendant à obtenir communication, suspension et rectification de données par le juge siégeant comme en référé.

Conformément à l'article 267 du TFUE, le président du Tribunal de première instance peut également être saisi en vertu de l'article 209 afin de poser une question préjudicielle à la Cour de Justice de l'Union européenne. Dans l'arrêt M. Schrems c. Data Protection Commissioner (C-362/14), la Cour de Justice a estimé qu'il incombait au législateur national de prévoir des voies de recours permettant à l'autorité compétente de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles doutent de la validité de l'acte, à un renvoi préjudiciel aux fins de l'examen de la validité de cet acte (§ 65).

Ces articles reprennent en grande partie l'article 14 LVP, qui organise le recours en cessation, puisque cette disposition sera abrogée. Mais il doit être fait bien attention au croisement des procédures, pénales, administratives et autres. Pour cette raison, l'article 14 LVP est repris mais une disposition spécifique prévoit dès lors que lorsqu'une donnée mise en cause se trouve dans un dossier pénal, c'est au pénal de se prononcer. Il ne s'agit pas uniquement d'une affaire qui serait portée devant le juge pénal.

Il faut entendre par action en cessation, la procédure selon laquelle le président du tribunal de première instance, siégeant comme en référé connaît de toute demande:

— tot staking van een verwerking verricht in strijd met de wettelijke en reglementaire bepalingen;

— het door of krachtens de wet, ongeacht het criminele karakter van het strafbare feit, verleende recht op mededeling van persoonsgegevens.

Hij neemt ook kennis van de vorderingen tot verbetering, tot verwijdering of tot het verbieden van de aanwending van onjuiste, onvolledige of niet ter zake dienende persoonsgegevens, waarvan de registratie, de mededeling of de bewaring verboden is en waartegen de betrokkene zich heeft verzet of die langer bewaard werden dan de toegestane duur.

In tegenstelling tot wat de Raad van State argumenteert over het artikel 209 (voriger 223) stelt het College van Procureurs-generaal: "*Artikel 223 is een belangrijk artikel dat grenzen stelt aan de bevoegheid en tussenkomst van de kort gedingrechter in strafrechtelijke procedures en is essentieel. Het kan immers niet de bedoeling zijn dat een kort gedingrechter zou beslissen gegevens die zich bijvoorbeeld in een lopende vooronderzoek in strafzaken bevinden (hetzij een opsporingsonderzoek, hetzij een gerechtelijk onderzoek) te schrappen of te rectificeren en op die manier actief in te grijpen in dat lopend onderzoek met alle gevolgen van dien voor de waarheidsvinding. Deze ontworpen bepaling is ook conform artikel 79 AVG (recht op een doeltreffende voorziening in rechte) omdat, zelfs wanneer betrokkene meent geen genoegdoening te hebben bekomen vanwege het OM (omdat het OM niet akkord gaat met de zienswijze van de betrokken of het dossier bv geseponeerd wordt zonder aan de inhoud, waarvan bepaalde aspecten door de betrokkene worden betwist, te raken), hij nadien steeds naar de burgelijke of de strafrechter kan om genoegdoening te bekomen en er dus steeds een doeltreffende voorziening in rechte aanwezig is*.".

Onder randnummers 2, 3 en 4 (pagina 43) van het advies van de Raad van State, is de basisassumpie niet correct. Het Openbaar Ministerie zal niet noodzakelijk alleen als "vervolgende partij" en/of "verweerder" optreden. Bovendien maakt de Raad van State volledig abstractie van de bijzondere grondwettelijke positie die het OM inneemt en die herhaaldelijk in meerdere arresten van het Grondwettelijk Hof is bevestigd doordat zij het publiek belang en geen private belangen nastreeft. Deze bepaling werd enkel geschreven om te vermijden dat een kort geding rechter, op vraag van één van de partijen (of zelfs de GBA) zich actief zou bemoeien met een lopend onderzoek en bv. verbeteringen zou beginnen bevelen van stukken van de strafprocedure.

— en cessation d'un traitement fait en violation des dispositions légales ou réglementaires;

— relative au droit accordé par ou en vertu de la loi indépendamment du caractère pénal de l'infraction, d'obtenir communication de données à caractère personnel.

Il connait également de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, et pour laquelle la personne concernée s'est opposée au traitement ou qui a été conservée au-delà de la période autorisée.

Au contraire de ce qu'argumente le Conseil d'État sur l'article 209 (anciennement 223), le Collège des Procureurs généraux estime dans son avis du 26 avril 2018 que: "*L'article 223 est un article important qui fixe des limites sur la compétence et l'implication du juge des référés dans la procédure pénale ce qui est essentielle. Il ne peut en effet pas être l'intention qu'un juge en référé déciderait quelles données contenues dans une enquête pénale en cours (soit à l'information, soit à l'instruction) puissent être supprimées ou rectifiées et de cette façon intervenir activement au niveau de l'enquête avec toutes ses conséquences pour aboutir à la vérité. Cette disposition est conforme également à l'article 79 du Règlement (droit à un recours efficace en droit) parce que, même si la personne concernée ne demande pas à obtenir satisfaction, (parce que le Ministère public n'est pas d'accord avec la personne concernées ou le fichier par exemple est séparé sans contenu, dont certains aspects sont contestés par la personne concernée), il va alors aux tribunaux civils ou criminels peuvent obtenir satisfaction et il y a toujours un recours effectif.*"

Sous les points 2, 3 et 4 (page 43) de l'avis du Conseil d'État, l'hypothèse de base n'est pas correcte. Le ministère public n'agira pas nécessairement uniquement en tant que "partie poursuivante" et/ou "partie adverse". En outre, le Conseil d'État méconnait entièrement la position constitutionnelle particulière que le ministère public détient, laquelle a été confirmée à plusieurs reprises dans différents arrêts de la Cour constitutionnelle parce qu'il poursuit l'intérêt public et non des intérêts privés. Cette disposition n'a été rédigée que pour éviter qu'un juge en référé, à la demande de l'une des parties (ou même de l'APD), n'intervienne activement dans une enquête en cours et que, par exemple, des rectifications de pièces de la procédure pénale soient ordonnées.

Het is eigenlijk niet meer dan een bevestiging en herhaling van wat reeds werd voorzien in de artikelen 37, § 4 en 44 van deze wet waaromtrent de Raad van State vreemd genoeg geen enkele opmerking heeft: van zodra gegevens in een lopend onderzoek zitten spelen uitsluitend de regels van de strafprocedure. De notie van "juge pénal compétent" is glashelder. Zolang een zaak enkel in opsporingsonderzoek zit moet men zich richten naar het OM. Is men niet tevreden met de beslissing van het OM dan kan men zich altijd wenden tot de burgerlijke rechter nadat de strafprocedure is afgerond, of zelfs de strafrechter gezien er nu ook inzagerechten zijn in het opsporingsonderzoek. In alle andere gevallen komt er een rechter bij kijken die het verzoek van de betrokkene kan bekijken en dit volgens de regels van de toepasselijke strafprocedure. Dat "lopend onderzoek" is inderdaad te begrijpen als "afhankelijk van de stand van de procedure".

Een nieuwe procedure in deze wet zoals de Raad van State het voorstelt heeft dus geen zin.

Met betrekking tot de regels van de bevoegde rechtbank moet hier worden afgeweken van artikel 624 van het Gerechtelijk Wetboek. Artikel 624 voorziet immers in verschillende bevoegde rechters naar keuze van de eiser, zulks met uitzondering van de gevallen waarin de wet iets anders bepaalt. Bijvoorbeeld, artikelen 627 en volgende van het Gerechtelijk Wetboek voorzien reeds in bijzondere bevoegdheidsregels. Bovendien moet hier, aangezien de materie specifiek is, worden voorzien in een aangepast stelsel in plaats van artikel 624 van het Gerechtelijk Wetboek toe te passen, welke niet toelaat om alle mogelijke scenario's die zich kunnen voordoen te behandelen. Wat de datastromen betreft, en de uitbreiding van het territoriale toepassingsgebied is het zo dat de inbreuk niet alleen een verweerder met woonplaats in België treft, maar ook een ingezeten persoon. Evenzo kan de verweerder regelmatig een rechtspersoon zijn, die een statutaire zetel in België kan hebben maar evengoed in het buitenland. De overtreding kan ook buiten het Belgische grondgebied plaatsvinden. Daarom moet van de beginselen van artikel 624 van het Gerechtelijk Wetboek worden afgeweken. De Privacycommissie oordeelt in punt 400 van haar advies dat het beter is de zaken te centraliseren: "*wat de Nederlandstalige zaken betreft voor de voorzitter van de Nederlandstalige rechtbank van eerste aanleg, wat de Franstalige zaken betreft voor de voorzitter van de Franstalige rechtbank van eerste aanleg te Brussel en wat de Duitstalige zaken betreft voor de voorzitter van de rechtbank van eerste aanleg te Eupen*.". Deze vraag verdient een lezing van de College van Procureur Generaals

Il ne s'agit en réalité que d'une confirmation et d'un rappel de ce qui était déjà prévu aux articles 37, § 4, et 44 de la présente loi sur lesquels le Conseil d'État n'a émis aucun commentaire: dès que des données existent dans le cadre d'une enquête, ce sont les règles de la procédure pénale qui s'appliquent. La notion de "juge pénal compétent" est claire. Tant qu'une affaire ne concerne que des enquêtes, il faut s'adresser au ministère public. Si l'on n'est pas satisfait de la décision du ministère public, il est toujours possible de s'adresser au tribunal civil une fois la procédure pénale achevée, ou même au juge pénal, étant donné qu'il existe désormais des droits d'accès dans l'enquête pénale. Dans tous les autres cas, il y aura un juge qui pourra examiner la demande de la personne concernée et ce, selon les règles de la procédure pénale applicable. La notion "lors d'une enquête" peut en effet être comprise comme "en fonction de l'état de la procédure".

Une nouvelle procédure telle que le propose le Conseil d'État n'a dès lors pas de sens dans la présente loi.

En ce qui concerne les règles du tribunal compétent, il y a lieu ici de déroger à l'article 624 du Code judiciaire. En effet, l'art 624 prévoit différents juges compétents au choix du demandeur, hormis les cas où la loi prévoit autre chose. Par exemple, les articles 627 et suivants du Code judiciaire prévoient déjà des règles de compétence particulières. De plus ici, la matière étant particulière il y a lieu de prévoir un système adapté et ne pas appliquer l'article 624 du Code judiciaire lequel ne permet pas de viser tous les cas de figure qui peuvent se présenter. S'agissant de flux de données, et l'extension du champ d'application territorial il se peut que la violation commise touche non pas seulement un défendeur domicilié en Belgique, mais également une personne résidente. De même le défendeur pourra régulièrement être une personne morale, celle-ci pouvant avoir un siège social sur le territoire belge mais également à l'étranger. La violation peut également avoir lieu en dehors du territoire belge. En conséquence, il est nécessaire de déroger aux principes énoncés par l'article 624 du Code judiciaire. La Commission vie privée estime dans le point 400 de son avis qu'il serait plus adéquat de centraliser les affaires *"en ce qui concerne les affaires néerlandophones devant le président du tribunal de première instance néerlandophone de Bruxelles, en ce qui concerne les affaires francophones, devant le président du tribunal de permière instance francopone de Bruxelles et en ce qui concerne les affaires germanophones, devant le président du tribunal de première instance d'Eupen.".* Cette question mériterait de faire l'objet d'une lecture par le Collège des Procureurs généraux.

Een bepaling wordt hier ingevoerd met betrekking tot de rechtsmacht van Belgische hoven en rechtbanken wanneer een element van buitenlandse nationaliteit tussenbeide komt. Ter herinnering, de Verordening is van toepassing op het grondgebied van de Europese Unie en natuurlijk op het nationale grondgebied. Maar de Verordening voorziet ook in een uitbreiding van de territoriale reikwijdte. Bovendien zijn gegevensbescherming en de stromen die daarmee gepaard gaan niet beperkt tot grenzen. Datastromen reiken verder dan nationaal en Europees grondgebied. Het is daarom noodzakelijk om in deze situaties te voorzien in een internationale privaatrechtelijke regel.

Er wordt ook voorzien in het feit dat de bevoegde toezichthoudende autoriteit zal worden geïnformeerd door kennisgeving van de beschikking die in openbare zitting wordt uitgesproken, maar ook op elke andere manier, dat een beroep tegen de beschikking werd ingediend.

Er wordt ook voorzien in het feit dat de eiser schadevergoeding kan eisen overeenkomstig het contractuele of buitencontractuele aansprakelijkheidsrecht. Het betreft hier niet, zoals de Raad van state het gesteld heeft in haar advies, om schadevergoeding te eisen volgens de hier voorziene procedure. Maar als gevolg van een beschikking van de rechter ten gronde, zal het mogelijk zijn om de artikelen 1282 en 1283 van het Burgerlijk wetboek toe te passen voor de bevoegde rechtbank.

Indien dwingende redenen de vrees doen rijzen dat bewijsmateriaal zou kunnen worden verheeld of zou kunnen verdwijnen, of dat zij ontoegankelijk zouden worden gemaakt, bijvoorbeeld wanneer de gegevens zijn opgeslagen in een derde staat waar er geen adequate gegevensbeschermingsregels zijn, gelast de voorzitter van de rechtbank van eerste aanleg elke maatregel ter voorkoming van die verheling of verdwijning.

HOOFDSTUK II

Vertegenwoordiging van betrokkenen

Art. 220

Teneinde in overeenstemming te zijn met artikel 80.1 van de Verordening en met artikel 55 van de Richtlijn wordt erin voorzien dat een orgaan, organisatie of vereniging, dat of die op geldige wijze werd opgericht volgens Belgisch recht en waarvan de statutaire doeleinden het openbare belang dienen, die actief is op het gebied van de bescherming van de rechten en vrijheden van de betrokkene in verband met de bescherming van diens persoonsgegevens en dit sedert ten minste drie

Une disposition est introduite ici en ce qui concerne la compétence des cours et tribunaux belges lorsqu'un élément d'extranéité intervient. Pour rappel, le Règlement est applicable sur le territoire de l'Union européenne et bien évidemment sur le territoire national. Mais le Règlement prévoit également une extension du champ d'application territorial. De plus, la protection des données et les flux qui l'accompagnent ne se cantonnent pas aux frontières. Les flux de données dépassent le territoire national et européen. Il y a dès lors lieu de prévoir une règle de droit international privé pour ces situations.

Il est également prévu que l'autorité de contrôle compétente soit informée par notification de l'ordonnance prononcée en audience publique mais également par tout autre moyen l'information qu'un recours contre l'ordonnance a été introduit.

Il est également prévu que le demandeur puisse réclamer des dommages et intérêts conformément à la responsabilité contractuelle ou extracontractuelle. Il ne s'agit pas ici, comme l'a stipulé le Conseil d'État dans son avis, de demander des dommages et intérêts selon la procédure prévue ici. Mais en conséquence d'une ordonnance du juge statuant sur le fond, il pourra être fait application des articles 1282 et 1283 du Code civil auprès de la juridiction compétente.

Lorsqu'il existe des motifs impérieux de craindre la dissimulation ou la disparition des éléments de preuve, ou que ceux-ci sont rendus inaccessibles, par exemple lorsque les données sont stockées dans un état tiers dans lequel il n'existe pas de règles de protection des données adéquates, le président du tribunal de première instance ordonne toute mesure de nature à éviter cette dissimulation ou cette disparition.

CHAPITRE II

Représentation des personnes concernées

Art. 220

Afin de se conformer à l'article 80.1 du Règlement et 55 de la Directive, il est prévu qu'un organisme, une organisation, ou une association valablement constituée conformément au droit belge dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel la concernant depuis au moins trois ans puisse représenter une personne

jaar, een betrokkene kan vertegenwoordigen die van oordeel is dat zijn rechten inzake bescherming van de persoonlijke levenssfeer werden geschonden en aldus namens hem kan optreden. Het betreft hier niet het recht om te pleiten.

De artikel 80.1 van de Verordening en 55 van de Richtlijn voorzien er immers in dat de betrokkene het recht heeft een orgaan, organisatie of vereniging zonder winstoogmerk dat of die op geldige wijze volgens het recht van een lidstaat van de Europese unie is opgericht, waarvan de statutaire doelstellingen het openbare belang dienen en dat of die actief is op het gebied van de bescherming van de rechten en vrijheden van de betrokkene in verband met de bescherming van diens persoonsgegevens, opdracht te geven de klacht namens hem in te dienen en namens hem de in hoofdstuk VIII van de Verordening en de Richtlijn bedoelde rechten uit te oefenen.

Er wordt besloten om dit recht te beperken tot organen, organisaties en verenigingen zonder winstoogmerk, die rechtsgeldig zijn opgericht volgens het Belgisch recht en vooral de wet van 27 juni 1921 betreffende de verenigingen zonder winstoogmerk, de stichtingen en de Europese politieke partijen en stichtingen. Deze organen, organisaties en verenigingen moeten ook rechtspersoonlijkheid hebben gedurende ten minste drie jaar en een activiteit uitoefenen op het gebied van de bescherming van de rechten en vrijheden van de betrokkenen in verband met de bescherming van de persoonsgegevens gedurende ten minste drie jaar, activiteit die is gerelateerd aan het maatschappelijk doel van openbaar belang. Een schriftelijke volmacht is vereist. Deze vereiste van kwaliteit is geïnspireerd op artikel XVII.39 van het Wetboek van economische recht, dat verwijst naar de vertegenwoordiger van een rechtsvordering tot collectief herstel, dat een bijzondere procedure is.

Hier wordt bepaald dat deze vertegenwoordiging van toepassing is op beroepen bij een toezichthoudende autoriteit, beroepen tegen een beslissing van de toezichthoudende autoriteit en voor rechtsmiddelen.

De vereiste van rechtspersoonlijkheid doet geen afbreuk aan wat nu al wettelijk mogelijk is. We kunnen hier onder meer verwijzen naar de representatieve werkgevers- en werknemersorganisaties, zoals gedefinieerd in artikel 3 van de cao-wet van 5 december 1968, die overeenkomstig artikel 4 van dezelfde wet in rechte "*mogen optreden in alle geschillen die uit de toepassing van deze wet kunnen ontstaan en ter verdediging van de rechten welke haar leden putten in de door haar gesloten overeenkomsten. Het optreden van de organisaties laat het recht van de leden onverkort om*

concernée qui estime que ses droits en matière de protection de la vie privée ont été floués, et ainsi agir en son nom. Il ne s'agit pas ici du droit de plaider.

L'articles 80.1 du Règlement et 55 de la Directive prévoient en effet que la personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre de l'Union européenne, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel la concernant, pour qu'il introduise une réclamation en son nom et exerce en son nom les droits visés au chapitre VIII du Règlement et de la Directive.

Il est fait le choix de limiter ce droit aux organismes, organisations et associations sans but lucratif valablement constituée conformément au droit belge et notamment à la loi du 27 juin 1921 sur les associations sans but lucratif, les fondations, les partis politiques européens et les fondations politiques européennes. Ces organes, organismes et associations doivent en outre avoir la personnalité juridique depuis au moins trois ans et avoir une activité dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel depuis au moins trois ans également, laquelle activité est en rapport avec son objet social d'intérêt public. Une procuration écrite est exigée. Cette exigence de qualité est inspirée de l'article XVII.39 du Code des droits économique qui vise le représentant d'une action en réparation collective, laquelle est une procédure particulière.

Il est ici prévu que cette représentation s'applique pour les recours auprès d'une autorité de contrôle, les recours contre une décision prononcée par l'autorité de contrôle et pour les recours juridictionnels.

L'exigence de personnalité juridique n'empêche pas ce qui est déjà légalement possible. On peut se référé aux organisations représentatives des travailleurs et des employeurs, tel que défini à l'article 3 de la loi du 5 décembre 1968 sur les conventions collectives de travail et les commissions paritaires, conformément à l'article 4 de la même loi, lesquelles "*peuvent ester en justice dans tous les litiges auxquels l'application de la présente loi donnerait lieu et pour la défense des droits que leurs membres puisent dans les conventions conclues par elles. Ce pouvoir des organisations ne*

zelf op te treden, zich bij een vordering aan te sluiten of in het geding tussen te komen." In het kader van een arbeidsrechtelijke verhouding zijn de privacy-aspecten immers geconcretiseerd in cao nr 68 betreffende bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats, en cao nr 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens en cao nr 89 betreffende de diefstalpreventie en de uitgangscontroles van de werknemers bij het verlaten van de onderneming of de werkplaats.

Zowel de Raad van State als de Privacycommissie stellen zich in hun respectievelijk advies de vraag waarom de wetgever geen gebruik gemaakt heeft van de mogelijkheid voorzien in artikel 80 § 2 van de Verordening. Deze bepaling voorziet in de mogelijkheid voor de listaten om een systeem tot vordering in rechte in collectief belang door een vereniging in te stellen, onafhankelijk van de opdracht van een betrokkene. De wetgever wenst deze mogelijkheid niet in het hader van huidige wet te voorzien. Een dergelijke procedure moet immers in een breder kader voorzien worden in toepassing van het gemeen recht. Het is waar dat er momenteel wel specifieke procedures bestaan die collectieve vorderingen voor de gewone hoven en rechtbanken toelaten voor specifieke belangen:

— in milieu-aangelegenheden: art. 2 van de wet van 12 januari 1993 betreffende een vorderingsrecht inzake bescherming van het leefmilieu;

— in consumentenzaken: art.113 van de wet van 6 april 2010 betreffende marktpraktijken en consumentenbescherming;

— gelijke kansen en strijd tegen xenofobie en racisme: art.32 van de wet van30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, art.30 van de wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie en art.35 van de wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie tussen vrouwen en mannen.

Het Grondwettelijk hof (arrest 133/2013) heeft bovendien geoordeeld dat een rechtspersoon die geen rechtsvordering kan instellen om een einde te maken aan een onmenselijke en vernederende behandeling in de zin van artikel 3 EVRM, omdat ze geen betrekking heeft op het bestaan van de rechtspersoonlijkheid, haar patrimoniale of morele rechten, wordt gediscrimineerd

porte pas atteinte au droit des membres d'agir personnellement, de se joindre à l'action ou d'intervenir dans l'instance". Dans le cadre d'une relation de droit du travail, les aspects relatifs à la vie privée ont été concrétisés dans la convention collective n°68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, la convention collective n °81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau, et la convention collective n°89 concernant la prévention des vols et les contrôles de sortie des travailleurs quittant l'entreprise ou le lieu de travail.

Le Conseil d'État ainsi que la Commission de la protection de la vie privée posent la question dans leur avis respectif de savoir pourquoi le législateur n'a pas usé de la possibilité prévue par l'article 80, § 2, du Règlement. Cette disposition prévoit la possibilité pour les États membres de mettre en place un système de recours en intérêt collectif par une association en dehors de tout mandat confié par une personne concernée. Le législateur ne souhaite pas prévoir une telle possibilité dans le cadre du présent projet de loi. En effet, une telle procédure a plus sa place dans un cadre plus général en application du droit commun. Il est vrai qu'il existe actuellement des procédures spécifiques permettant des actions d'intérêt collectif devant les cours et tribunaux ordinaires pour des intérêts spécifiques:

— en matière d'environnement: art. 2 de la loi du 12 janvier 1993 concernant un droit d'action en matière de protection de l'environnement;

— en matière de consommation: art. 113 de la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur;

— en matière d'égalité des chances et de lutte contre la xénophobie et le racisme: art. 32 de la loi du 30 juillet 1981 tendant à lutter contre certains actes inspirés par le racisme et la xénophobie, art. 30 de la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination et art. 35 de la loi du 10 mai 2007 tendant à lutter contre les discriminations entre les femmes et les hommes.

La Cour constitutionnelle (arrêt 133/2013) a en outre estimé qu'une personne morale qui ne peut intenter une action judiciaire aux fins de faire cesser des traitements inhumains et dégradants au sens de l'article 3 de la CEDH parce qu'elle n'a pas trait à l'existence de la personne morale, à ses biens patrimoniaux ou à ses droits moraux, est discriminée par rapport aux associations qui

ten aanzien van verenigingen die een beroep kunnen doen op de speciale wetgeving inzake gelijke kansen en de strijd tegen xenofobie en racisme.

De wetgever moet dus maatregelen nemen om deze discriminatie bij de collectieve vorderingen weg te nemen. Maar met het huidig ontwerp van wet in het bijzonder kan niet beantwoord worden aan de rechtspraak van het Grondwettelijk Hof. Dit moet geregeld worden in een meer algemeen kader dan dit van de bescherming van de gegevens. De wetgever is zich bewust van deze bestaande lacune maar een dergelijke aanpassing heeft niet zijn plaats in huidig wetsontwerp.

TITEL 6

Sancties

Er dienen sancties te worden opgelegd aan de natuurlijke personen of rechtspersonen, ongeacht of deze personen onder het publiekrecht dan wel onder het privaatrecht vallen, die inbreuk maken op deze wet. De sancties, of ze nu strafrechtelijk dan wel administratiefrechtelijk zijn, moeten doeltreffend, evenredig en afschrikkend zijn.

Artikel 83 van de Verordening voorziet in administratieve geldboeten, naast of in plaats van de in artikel 58 bedoelde maatregelen, voor de volgende bepalingen van de Verordening: 5 tot 9 – 11 tot 22 – 25 tot 39 – 41.4 – 42 tot 49 – 85 tot 91 (bijzondere verwerkingen).

De Verordening voorziet dus niet in administratieve geldboeten voor de volgende bepalingen:

— art. 10: verwerkingen van gerechtelijke gegevens;

— art. 23: uitzonderingen waarin de lidstaten kunnen voorzien;

— art 24: (algemene) verantwoordelijkheid van de verwerkingsverantwoordelijke;

— artt. 40 en 41.1 tot 41.3: gedragscodes;

— art. 50: internationale samenwerking inzake doorgiften;

— artt. 51 tot 59: toezichthoudende autoriteit;

— art. 60 tot 76: samenwerking en bijstand (toezichthoudende autoriteit/Board);

— art. 77 tot 84: beroep en sancties.

peuvent faire appel à la législation spéciale en matière d'égalité des chances et de lutte contre la xénophobie et le racisme.

Le législateur doit donc prendre des mesures afin de palier à cette discrimination en matière de recours à titre collectif. Mais le présent projet de loi particulier ne peut pas répondre à la jurisprudence de la Cour constitutionnelle. Cela doit nécessairement être réglé dans un cadre plus général que la protection des données. Le législateur est conscient de la lacune actuelle mais une telle réforme n'a pas sa place dans le présent projet de loi.

TITRE 6

Sanctions

Toute personne physique ou morale, qu'elle soit soumise au droit privé ou au droit public, qui enfreint la présente loi devrait faire l'objet de sanctions. Les sanctions, qu'elles soient pénales ou administratives, doivent être effectives, proportionnées et dissuasives.

L'article 83 du Règlement prévoit des amendes administratives, en complément ou à la place des mesures visées à l'art. 58, pour les dispositions suivantes du Règlement: 5 à 9 – 11 à 22 – 25 à 39 – 41.4 – 42 à 49 – 85 à 91 (traitements particuliers).

Le Règlement ne prévoit donc pas d'amendes administratives pour les dispositions suivantes:

— art. 10: traitements des données judiciaires;

— art. 23: exceptions que les États membres peuvent prévoir;

— art. 24: responsabilité (générale) du responsable du traitement;

— art. 40 et 41.1 à 41.3: codes de conduite;

— art. 50: coopération internationale en matière de transferts;

— art. 51 à 59: autorité de contrôle;

— art. 60 à 76: coopération et assistance (autorité de contrôle/Board);

— art. 77 à 84: recours et sanctions.

De afwezigheid van administratieve geldboeten voor die artikelen is logisch en coherent gelet op de inhoud van die artikelen.

Er kan dan ook worden besloten dat de Verordening voorziet in administratieve geldboeten voor (vrijwel) alle verplichtingen van de Verordening. De Europese wetgever is blijkbaar artikel 10 van de Verordening in de sancties vergeten. Aangezien het om een vergetelheid gaat moet een overtreding op dit artikel ook bestraft worden.

De nationale wetgever moet eventueel voorzien in aanvullende sancties voor hetgeen niet werd voorzien door de Verordening, overeenkomstig artikel 84 van de Verordening.

Er moet ook worden voorzien in sancties voor de aanvullende verplichtingen die de nationale wetgever oplegt, zoals de bepalingen voor de federale publieke sector bijvoorbeeld met betrekking tot het protocol, de DPO… .

Artikel 57 van de Richtlijn bepaalt ook dat de lidstaten de regels inzake toepasselijke sancties vaststellen, die doeltreffend, evenredig en afschrikkend moeten zijn. De gegevensverwerkingen bedoeld in titel 2 die in strijd zijn met deze wet worden eveneens onderworpen aan sancties.

Artikel 10 van het Verdrag 108 bepaalt ook dat de Partijen passende sancties vaststellen voor schendingen van de bepalingen van het nationale recht die uitvoering geven aan de fundamentele gegevensbeschermingsbeginselen van het Verdrag. Als zodanig zijn ook sancties voorzien voor de gegevensverwerkingen bedoeld in titel 3.

HOOFDSTUK I

Administratieve sancties

Art. 221

De in artikel 83 van de Verordening bepaalde geldboeten zijn maximumbedragen, wat betekent dat de toezichthoudende autoriteit in lagere bedragen kan voorzien. Voornoemde autoriteit is evenmin verplicht ze toe te passen, aangezien het om aanvullende geldelijke sancties gaat of om sancties die de klassieke administratieve sancties vervangen zoals bedoeld in artikel 58 van de Verordening.

Ter aanvulling van de boetes die voorzien worden door de Verordening, voorziet deze wet eveneens

L'absence d'amendes administratives pour ces articles est logique et cohérent en raison du contenu de ces articles.

On peut donc conclure que le Règlement prévoit des amendes administratives pour (presque) toutes les obligations prévues dans le Règlement. En effet, le législateur européen a oublié semble-t-il l'article 10 du Règlement dans les sanctions. S'agissant d'un oubli, une violation de cet article devrait également être sanctionnée.

Le législateur national a l'obligation de prévoir éventuellement des sanctions supplémentaires pour ce qui n'a pas été prévu par le Règlement, et ce en vertu de l'article 84 du Règlement.

De même il faut prévoir des sanctions pour les obligations supplémentaires que le législateur national impose, tel que les dispositions pour le secteur public fédéral, par exemple en ce qui concerne le protocole, le DPO....

L'article 57 de la Directive prévoit également que les États membres déterminent le régime des sanctions applicables, lesquelles doivent être effectives, proportionnées et dissuasives. Les traitements visés par le titre 2 faits en violation de la présente loi sont donc également soumis à sanctions.

L'article 10 de la Convention 108 prévoit également que les Parties établissent des sanctions appropriées visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans la Convention. A ce titre, des sanctions sont également prévues pour les traitements visés au titre 3.

CHAPITRE I^ER

Sanctions administratives

Art. 221

Les amendes fixées par l'article 83 du Règlement sont un montant maximum, ce qui signifie que l'autorité de contrôle peut prévoir des montants bien inférieurs. Cette dernière n'est pas non plus tenue de les appliquer, car il s'agit de sanctions pécuniaires complémentaires ou remplaçant les sanctions administratives classiques prévues à l'article 58 du Règlement.

En complément des amendes prévues par le Règlement, la présente loi prévoit également des

administratieve sancties voor specifieke bepalingen van titel 1 en titel 2. Voor de bepalingen van titel 1 betreft het de bepalingen waar de lidstaten een beoordelingsmarge gelaten is door de Verordening en voor dewelke dit wetsontwerp nieuwe verplichtingen invoert. Voor titel 2 betreft het bepalingen die identiek zijn aan deze van de Verordening, teneinde een gelijke behandeling te voorzien tussen de publieke diensten die geviseerd worden door deze verwerkingen. Het is wel te verstaan dat de administratieve sancties die worden uitgesproken door de toezichthoudende autoriteit niet van toepassing zijn op de verwerkingen door de hoven en rechtbanken alsook door het openbaar ministerie wanneer deze gebeuren bij de uitoefening van hun rechterlijke functie, gezien deze laatsten niet kunnen gecontroleerd worden door een toezichthoudende autoriteit in het kader van de Verordening en deze wet. Desalniettemin kunnen zij gecontroleerd worden door een ad-hocsysteem. Wat de andere overheden betreft die gerechtelijke gegevens verwerken, zoals de politiediensten, deze kunnen wel onderworpen worden aan de corrigerende maatregelen van de toezichthoudende autoriteiten.

Het is duidelijk dat de overheid niet uitgesloten is van de verplichtingen voorzien in de Verordening en deze wet. Er is echter voor geopteerd om geen administratieve geldboetes op te leggen aan de overheid als bedoeld in artikel 5. Zij worden echter wel onderworpen aan niet-geldelijke administratieve sancties alsook aan strafrechtelijke sancties.

Dit verschil in behandeling wordt verklaard door het feit dat het bestuur de taak heeft om het algemeen belang te dienen. Bovendien is de administratie in de meeste gevallen verplicht om persoonsgegevens te verwerken en heeft deze er geen financieel voordeel uit. Het administratief recht is een uitzonderingsrecht dat rekening houdt met de bijzondere positie van de uitvoerende macht in het rechtsverkeer. Zo kan de overheid eenzijdige beslissingen nemen en aan de burger opleggen, maar is het bestuur omgekeerd ook onderworpen aan allerlei bijzondere verplichtingen.

De regels van het publiekrecht zijn gericht op de behartiging van het algemeen belang terwijl de private rechtsregels gericht zijn op de realisatie van louter particuliere belangen. Bij het realiseren van de taken van algemeen belang moet er een ander instrumentarium worden gehanteerd dan voor de privaatrechtelijke actoren.

De grondwettelijke regels van gelijkheid en nondiscriminatie sluiten niet uit dat er een verschil is in behandeling tussen categorieën van personen, voor zover deze verschillende behandeling berust op een objectief criterium, goed gemotiveerd is en de gebruikte

sanctions administratives pour certaines dispositions du titre 1er et titre 2. Pour les dispositions du titre 1er, il s'agit des dispositions dons les États membres ont une marge d'appréciation et pour lesquelles ce projet de loi introduit de nouvelles obligations. Pour le titre 2, il s'agit des dispositions identiques à celles se retrouvant dans le Règlement, afin d'insérer une égalité de traitement entre les services publics visés par ces traitements. Il est entendu que les sanctions administratives prononcées par l'autorité de contrôle ne s'appliquent pas aux traitements effectués par les cours et tribunaux ainsi que le ministère public lorsqu'ils agissent dans l'exercice de leur fonction juridictionnelle, puisque ces derniers ne peuvent pas être contrôlés par une autorité de contrôle au sens du Règlement et de la présente loi. Néanmoins, ils peuvent être contrôlés par un système ad hoc. En ce qui concerne les autres autorités qui traitent des données judiciaires tel que les services de police, celles-ci sont concernées par les mesures correctrices des autorités de contrôle.

Il est naturellement clair que l'autorité publique n'est pas exemptée des obligations prévues par le Règlement et la présente loi. Toutefois il est choisi de ne pas faire appliquer les amendes administratives aux autorités publiques telles que définies à l'article 5. Celles-ci sont néanmoins soumises aux sanctions administratives non pécuniaires, ainsi qu'aux sanctions pénales.

Cette différence de traitement s'explique par le fait que l'administration a pour mission de servir l'intérêt public. De plus, l'administration est, dans la majorité des cas, dans l'obligation de traiter des données à caractère personnel, et n'en retire aucun bénéfice pécunier. Le droit administratif est un droit d'exception qui tient compte de la position particulière de l'exécutif dans les transactions juridiques. Par exemple, le gouvernement peut prendre des décisions unilatérales et les imposer au citoyen, mais l'administration est également soumise à diverses obligations particulières.

Les règles de droit public visent à promouvoir l'intérêt public, tandis que les règles de droit privé visent à la réalisation d'intérêts purement privés. Lors de la mise en œuvre des missions d'intérêt général, un ensemble d'instruments différents de ceuxs applicables aux acteurs de droit privé doit être utilisé.

Les règles constitutionnelles de l'égalité et de la non-discrimination n'excluent pas qu'une différence de traitement soit établie entre des catégories de personnes, pour autant que cette différence de traitement repose sur un critère objectif, raisonnablement

middelen proportioneel zijn aan het beoogde doel. In dit geval rechtvaardigt de noodzaak om de continuïteit van de openbare dienstverlening te waarborgen en de uitoefening van een taak van algemeen belang niet in gevaar te brengen, het verschil in behandeling tussen deze laatste en de verantwoordelijken van de verwerking in de privésector. Het niet toepassen van de administratieve geldboete voor de verwerkingsverantwoordelijken binnen de overheidssector is proportioneel met het beoogde doel, in de mate dat dit toelaat om de continuïteit van de openbare dienstverlening niet in gevaar te brengen, zonder alle drukkingsmiddelen te verbannen om de verantwoordelijke voor de verwerking ertoe aan te zetten om nauwgezet de regels voor gegevensbescherming na te leven. Ook als de drukkingsmiddelen niet helemaal dezelfde zijn naargelang het gaat om een verantwoordelijke voor de verwerking van de publieke sector of de privésector, blijven ze niettemin gelijkwaardig en laten toe om het doel te bereiken. In het advies van de Raad van State is bepaald dat de drukkingsmiddelen gelijkaardig moeten zijn en niet noodzakelijk identiek.

Het is geenszins de bedoeling van de wetgever om de publieke sector uit te sluiten van elk toezicht: zij blijft, desgevallend, onderworpen aan de controle van de bevoegde toezichthoudende autoriteit voor wat betreft de administratieve sancties (corrigerende maatregelen) alsook aan de rechterlijke controle en aan de strafrechtelijke sancties.

HOOFDSTUK II

Strafsancties

Art. 222

De cumulatie van strafrechtelijke, burgerrechtelijke en administratiefrechtelijke procedures kan moeilijkheden veroorzaken in geval van parallelle toepassing van deze procedures. Het “non bis in idem” beginsel moet gerespecteerd worden.

Daarom wordt de voorkeur gegeven aan de maximalisatie van de administratieve procedure. In het algemeen gelden de algemene regels van het strafrecht voor gevallen van samenloop.

Enkel voor de ernstige inbreuken wordt een strafrechtelijke sanctie voorzien. Het gaat om gedragingen die als bijzonder ernstig worden beschouwd. Deze gedragingen worden opgesomd in dit artikel. Het betreft veelal inbreuken die samenlopen met inbreuken die strafrechtelijk gekwalificeerd worden in het Strafwetboek. Voor alle overige inbreuken wordt een administratiefrechtelijke procedure voorzien bij de toezichthoudende autoriteit.

justifié et que les moyens utilisés soient proportionnés à l’objectif poursuivi. En l’occurrence, la nécessité d’assurer la continuité du service public et de ne pas mettre en péril l’exercice d’une mission d’intérêt général justifie la différence de traitement entre ces derniers et les responsables de traitement du secteur privé. La non-application de l’amende administrative pour les responsables du traitement du service public est une mesure proportionnée par rapport à l’objectif poursuivi dans la mesure où elle permet d’éviter de mettre en péril la continuité du service public sans pour autant supprimer tout moyen de pression susceptible d’amener le responsable de traitement à veiller scrupuleusement au respect des règles de protection des données. Si les moyens de pression ne sont pas exactement identiques selon que le responsable de traitement appartienne au secteur public ou au secteur privé, ils restent néanmoins équivalents et permettent d’atteindre leur objectif. Dans son avis le Conseil d’État stipule que les moyens de pression doivent être équivalents, et donc pas nécessairement identiques.

Il n’est nullement l’intention du législateur de soustraire le secteur public à tout contrôle: il reste en effet soumis, le cas échéant, à la surveillance de l’autorité de contrôle compétente en ce qui concerne les sanctions administratives (mesures correctrices), il reste soumis également au contrôle judiciaire et aux sanctions pénales.

CHAPITRE II

Sanctions pénales

Art. 222

Le cumul des procédures pénales, civiles, administratives en parallèle peut poser certaines difficultés en cas de leur application parallèle. Le principe du “non bis in idem” doit être respecté.

Pour cette raison, il est privilégié la maximisation de la procédure administrative. De manière générale, les dispositions générales du droit pénal en matière de concours d’infractions sont applicables.

Il est prévu une sanction pénale seulement pour les violations graves. Il s’agit d’actes qui sont considérés comme extrêmement grave. Ces actes sont énumérés dans le présent article. Il s’agit souvent d’infractions qui se cumulent avec des infractions qualifiées comme pénales dans le Code pénal. Pour toutes les autres infractions il est prévu une procédure administrative auprès de l’autorité de contrôle.

Met betrekking tot de Richtlijn bestaat ook de mogelijkheid voor de lidstaten om strafrechtelijke en administratiefrechtelijke sancties te voorzien. De Richtlijn verleent dus in deze ook bepaalde bevoegdheden aan de toezichthoudende autoriteit. Gezien de Richtlijn niet verduidelijkt of het om strafsancties dan wel om administratieve sancties gaat, moet in deze wet ook voorzien worden in sancties voor de inbreuken die niet onder de bevoegdheid van de toezichthoudende autoriteit vallen. Het betreft hier duidelijk een bevoegdheid van de lidstaten. In deze wil de Europese Commissie de lidstaten van de Unie aanmoedigen om de bepalingen van de Verordening zoveel mogelijk toe te passen wanneer de Richtlijn niets voorziet. Het is nodig een coherent en identiek stelsel voor beide rechtsinstrumenten in te voeren en ook hier de procedures niet te vermenigvuldigen. Er wordt dan ook voorgesteld te verwijzen naar de artikelen 58 en 83 van de Verordening met betrekking tot de administratieve sancties en geldboeten. Die sancties en de eventuele geldboeten worden uitgesproken door de bevoegde toezichthoudende autoriteit.

Wanneer een vordering wordt ingesteld voor de hoven en rechtbanken moet evenwel ook in een burgerrechtelijke sanctie of strafsanctie worden voorzien.

Daarom wordt een hoofdstuk over de sancties behouden dat voorziet in enkele strafsancties maar enkel voor de gevallen waarin de procedure voor de rechter wordt gebracht.

Om de strafsancties te versterken en ze afschrikkend te maken in het licht van de administratieve sancties worden de bedragen als dusdanig behouden, zulks op grond van artikel 2 van de wet van 26 juni 2000 betreffende de invoering van de euro in de wetgeving die betrekking heeft op aangelegenheden als bedoeld in artikel 78 van de Grondwet: de bedragen uitgedrukt in BEF worden geacht te zijn uitgedrukt in euro, zonder omrekening. Er wordt tevens op gewezen dat de bedragen sedert 1 januari 2017 worden vermenigvuldigd met 8 ingevolge artikel 1, eerste en tweede lid, van de wet van 5 maart 1952 betreffende de opdeciemen op de strafrechtelijke geldboeten, gewijzigd door artikel 59 van de wet van 25 december 2016.

De Privacycomissie verwondert zich over de bedragen van de strafrechtelijke sancties die minder zijn dan de administratiefrechtelijke geldboetes die voorzien worden in de Verordening. Nochtans zijn de bedragen van de sancties die in het wetsontwerp voorzien worden al veel hoger dan hetgeen voorzien is in de huidige privacywet. Temeer, de bedragen van de administratieve geldboetes voorzien in de Verordening betreffen een vork en zijn eveneens gebaseerd op het omzetcijfer, die een marge laat aan de toezichthoudende autoriteit die

En ce qui concerne la Directive, il existe également la possibilité pour les États membres de prévoir des sanctions administratives et pénales. La Directive attribue donc également certaines compétences à l'autorité de contrôle. Vu que la Directive ne clarifie pas s'il s'agit de sanctions pénales ou administratives il y a lieu également de prévoir dans la présente loi des sanctions pour les infractions hors compétence de l'autorité de contrôle. En effet, il s'agit là bien de la compétence des États membres de l'Union. La Commission européenne entend encourager les États membres de l'Union à appliquer les dispositions du Règlement au maximum lorsque la Directive reste muette. Il est nécessaire d'établir un système cohérent et identique pour les deux instruments juridiques et de ne pas multiplier les procédures non plus ici. Il est donc proposé de faire une référence aux articles 58 et 83 du Règlement pour ce qui concerne les sanctions et amendes administratives. Ces sanctions et les amendes éventuelles sont prononcées par l'autorité de contrôle compétente.

Toutefois, lorsqu'une action est menée devant les cours et tribunaux, une sanction civile ou pénale doit également être prévue.

Raison pour laquelle, est maintenu un chapitre sur les sanctions, qui prévoient quelques sanctions pénales mais uniquement pour les cas où la procédure est portée devant le juge.

Afin de renforcer les sanctions pénales, et les rendre dissuasives, au regard des sanctions administratives, les montants sont maintenus tels quels et ce, en vertu de l'article 2 de la loi du 26 juin 2000 relative à l'introduction de l'euro dans la législation concernant les matières visées à l'article 78 de la Constitution: les montants exprimés en BEF sont censés être exprimés en EUR sans conversion. Il est également rappelé que les montants sont, depuis le 1 janvier 2017, multipliés par 8, en vertu de l'article 1er, alinéas 1 et 2 de la loi du 5 mars 1952 relative aux décimes additionnels sur les amendes pénales, modifiée par l'article 59 de la loi du 25 décembre 2016.

La Commission vie privée s'étonne du montant des santions pénales comme étant bien inférieures au montant des amendes adminsitratives prévues par le Règlement. Or les montants prévus ici ont déjà été augmentés par rapport à la loi vie privée actuelle. De plus, les montants des amendes administratives prévues par le Règlement sont une fourchette et basés également sur le chiffre d'affaire, qui laisse une marge à l'autorité de contrôle qui sanctionnera le responsable du traitement. On peut également mentionner la jurisprudence

de sancties zal opleggen. We kunnen eveneens melding maken van de rechtspraak van het Europees Hof van de Rechten van de Mens die stelt dat, wanneer een boete die wordt opgelegd voor een overtreding excessief is, en die dus een repressief en afschrikkend karakter heeft, zij kan beschouwd worden als een strafrechtelijke sanctie (Inocencio t. Portugal, 43862/98).

De publieke overheden die uitgesloten zijn van de toepassing van administratieve geldboetes zijn wel degelijk onderworpen aan strafrechtelijke sancties. En zoals de Privacycommissie onderstreept, sluit artikel 5 van het Strafwetboek bepaalde rechtspersonen uit van hun strafrechtelijke verantwoordelijkheid, zoals de Federale Staat, de deelstaten…. Dit sluit in geen geval de strafrechtelijke verantwoordelijkheid uit van de verwerkingsverantwoordelijke. In dit geval is de orgaantheorie van toepassing.

Inderdaad, het Grondwettelijk Hof heeft, in zijn arrest 128/2002 van 10 juli 2002, vastgesteld dat: "*B.7.5. Het verschil in behandeling van rechtspersonen naargelang zij al dan niet een democratisch verkozen orgaan hebben, berust op een pertinent criterium. De publiekrechtelijke rechtspersonen opgesomd in artikel 5, vierde lid, van het Strafwetboek vertonen het bijzondere kenmerk dat zij hoofdzakelijk belast zijn met een essentiële politieke opdracht in een representatieve democratie, dat zij beschikken over democratisch verkozen vergaderingen en dat zij organen hebben die aan een politieke controle onderworpen zijn. De wetgever kon redelijkerwijze vrezen dat, indien hij die rechtspersonen strafrechtelijk aansprakelijk zou maken, een collectieve strafrechtelijke aansprakelijkheid zou worden uitgebreid tot situaties waarin ze meer nadelen dan voordelen vertoont, door onder meer klachten uit te lokken waarvan het werkelijke doel zou zijn via strafrechtelijke weg politiek strijd te voeren.*"

Zij voegt eraan toe: *"B.7.6. Daaruit volgt dat de wetgever, door bepaalde publiekrechtelijke rechtspersonen uit het werkingsgebied van artikel 5 van het Strafwetboek uit te sluiten, en door die uitsluiting te beperken tot de publiekrechtelijke rechtspersonen vermeld in het vierde lid van dat artikel, hen geen immuniteit heeft toegekend die niet verantwoord zou zijn."*

In zijn arrest nr. 31/2007 van 21 februari 2007 was het Hof van oordeel dat "*het verschil in behandeling van rechtspersonen naargelang zij al dan niet een democratisch verkozen orgaan hebben, op een pertinent criterium berust. De publiekrechtelijke rechtspersonen opgesomd in artikel 5, vierde lid, van het Strafwetboek vertonen het bijzondere kenmerk dat zij hoofdzakelijk zijn belast met een essentiële politieke opdracht in een representatieve democratie, dat zij beschikken*

de la Cour européenne des droits de l'homme qui stipule que lorsqu'une amende donnée à l'encontre d'une violation a montant excessif, et qui a dès lors un caractère répressif et dissuasif, celle-ci peut être considérée comme une sanction pénale (Inocencio c. Portugal, 43862/98).

Les autorités publiques étant exclues de l'application des amendes administratives, ces dernières sont soumises aux sanctions pénales. Comme le souligne la Commission vie privée, l'article 5 du Code pénal exclut de la responsabilité pénale certaines personnes morales telles que l'État fédéral, les entités fédérées, … Ceci n'exclut toutefois pas la responsabilité pénale du responsable de traitement. En l'occurrence, la théorie de l'organe sera d'application également.

En effet, la Cour constitutionnelle a, dans son arrêt 128/2002 du 10 juillet 2002, établit que "*B.7.5. La différence de traitement ainsi établie entre personnes morales selon qu'elles disposent d'un organe démocratiquement élu ou non repose sur un critère objectif. Les personnes morales de droit public énumérées à l'article 5, alinéa 4, du Code pénal ont la particularité d'être principalement chargées d'une mission politique essentielle dans une démocratie représentative, de disposer d'assemblées démocratiquement élues et d'organes soumis à un contrôle politique. Le législateur a pu raisonnablement redouter, s'il rendait ces personnes morales pénalement responsables, d'étendre une responsabilité pénale collective à des situations où elle comporte plus d'inconvénients que d'avantages, notamment en suscitant des plaintes dont l'objectif réel serait de mener, par la voie pénale, des combats qui doivent se traiter par la voie politique.*"

Elle ajoute ensuite: *"B.7.6. Il s'ensuit que, en excluant des personnes morales de droit public du champ d'application de l'article 5 du Code pénal et en limitant cette exclusion à celles qui sont mentionnées à l'alinéa 4 de cet article, le législateur n'a pas accordé à celles-ci une immunité qui serait injustifiée."*

Dans son arrêt n° 31/2007 du 21 février 2007, la Cour a estimé que "*la différence de traitement ainsi établie entre personnes morales selon qu'elles disposent d'un organe démocratiquement élu ou non repose sur un critère objectif. Les personnes morales de droit public énumérées à l'article 5, alinéa 4, du Code pénal ont la particularité d'être principalement chargées d'une mission politique essentielle dans une démocratie représentative, de disposer d'assemblées*

over democratisch verkozen vergaderingen en dat zij organen hebben die aan een politieke controle zijn onderworpen.".

Art. 223

Strafsancties worden voorzien in het geval van schending van de artikelen 11 et 12 van deze wet om zo de nodige discretie te verzekeren voor de uitoefening van de opdrachten van de overheden bedoeld in titel 3 door verwerkingsverantwoordellijken bedoeld in titel 1.

Art. 224

Er wordt in een sanctie voorzien voor leden van het personeel van de bevoegde toezichthoudende autoriteit of voor een door de toezichthoudende autoriteit aangewezen deskundige die de vertrouwelijkheidsverplichting heeft geschonden, zoals bepaald in de organieke wetten.

Art. 225 en 226

Voor de in titel 3 bedoelde verwerkingen worden specifieke bepalingen in deze artikelen voorzien. De verwerkingsverantwoordelijke, de verwerker en de persoon die handelt onder het gezag van de overheden bedoeld in titel 3 worden bestraft wanneer zij hun verplichtingen in het kader van hun verwerking van persoonsgegevens niet nakomen. Een voorbeeld is het niet verbeteren van gegevens, waarvan zij weten dat ze onjuist zijn, of het niet respecteren van het "need to know"-beginsel. De strafbepaling is niet van toepassing op de verwerkingsverantwoordelijke, aangezien een overheidsinstantie zonder rechtspersoonlijkheid niet strafrechtelijk veroordeeld kan worden. Ten slotte moet worden opgemerkt dat de persoon die handelt onder het gezag van de overheden bedoeld in titel 3 enkel gestraft wordt indien deze kwaadwillig of met grove nalatigheid gehandeld heeft.

De verwerker of de persoon die handelt onder het gezag van de overheden bedoeld in titel 3 wordt ook bestraft wanneer zij op onwettige wijze (niet naleven van het finaliteitsbeginsel) of op een ongeschikte wijze (niet naleven van de beginselen van noodzakelijkheid en subsidiariteit) persoonsgegevens verwerken.

Om te antwoorden op de vraagstelling van de Privacycommissie in het punt 442 van haar advies, wat betreft het personele toepassingsgebied van de punten 4° en 5°, ten opzichte van de twee eerste punten van

démocratiquement élues et d'organes soumis à un contrôle politique.".

Art. 223

Des sanctions pénales sont prévues en cas de violations des articles 11 et 12 de la présente loi assurant la nécessaire discrétion de l'exécution des missions des autorités visées au titre 3 par des responsables du traitement visés au titre 1er.

Art. 224

Une sanction est prévue à charge des membres du personnel de l'autorité de contrôle compétente ou d'un expert désigné par cette autorité de contrôle, tel que le prévoient les lois organiques, qui aurait violé l'obligation de confidentialité.

Art. 225 et 226

Pour les traitements visés au titre 3, des dispositions spécifiques sont prévues aux présents articles. Est sanctionné le responsable de traitement, le sous-traitant et la personne agissant sous l'autorité d'une autorité visée au titre 3, lorsqu'ils ne respectent pas leurs obligations dans le cadre de leur traitement de données à caractère personnel. Par exemple, ne pas rectifier des données, alors qu'ils les savent incorrectes ou ne pas respecter le principe du besoin d'en connaître (need to know). Le responsable du traitement n'est pas visé par la disposition pénale, étant donné qu'une autorité publique n'ayant pas la personnalité juridique ne peut pas être condamnée au pénal. Enfin, il est à noter que la personne agissant sous l'autorité des autorités visées au titre 3 n'est sanctionnée que si elle a agi avec une intention malveillante ou avec négligence grave.

Le sous-traitant ou la personne agissant sous l'autorité des autorités visées au titre 3, lorsqu'ils effectuent illégalement des traitements de données à caractère personnel (non-respect du principe de finalité) ou de manière inadéquate (non-respect des principes de nécessité et de proportionnalité) est également sanctionné pénalement.

Pour répondre à l'interrogation de la Commission vie privée dans le point 442 de son avis, au sujet du champ d'application personnel des 4° et 5°, points au regard des deux premiers points de la disposition, il

de bepaling, kunnen we verduidelijken dat de punten 4° en 5°, eigenlijk een ruimer toepassingsgebied hebben dan de eerste twee punten, omdat ze andere personen kunnen betreffen dan de verwerker, zoals de persoon die handelt onder het gezag van een overheid als bedoeld in titel 3 of onder het gezag van de verwerker of de gemachtigde.

Art. 227

Dit artikel is afkomstig uit artikel 42 WVPen betreft de burgerrechtelijk aansprakelijkheid van de gegevensverantwoordelijke voor de betaling van de boeten waartoe zijn aangestelde of gemachtigde is veroordeeld.

Art. 228

In het algemeen, gelden de algemene regels van het strafrecht voor gevallen van samenloop van inbreuken.

Het is nog altijd mogelijk dat verschillende procedures gestart worden voor eenzelfde inbreuk. Daarom wordt een bepaling voorzien dat het ondertekenen van een protocol toelaat tussen de bevoegde toezichthoudende autoriteit en het openbaar ministerie. In dit protocol wordt de werkwijze en de wijze van samenwerking bepaald bij overlapping van verschillende soorten procedures voor eenzelfde inbreuk. Het Grondwettelijk Hof heeft in zijn arrest 86/2015 van 11 juni 2015 immers geoordeeld dat, in de gevallen waarin er sprake is van een cumulatie tussen een strafrechtelijke sanctie en een administratieve sanctie "*de "non bis in idem" regel [moet] worden nageleefd bij de concrete toepassing van deze regels in de praktijk.*."

De modaliteiten en het model van dit protocol zullen vastgelegd worden bij koninklijk besluit in Ministerraad overlegd.

Wanneer niet geopteerd wordt voor een protocol dan worden in de wet een aantal standaardregels voorzien, zoals het Wetboek van sociaal strafrecht en zijn artikelen 68 en volgende. Wanneer een inbreuk ook strafrechtelijk kan gekwalificeerd worden beschikt de procureur des Konings over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het origineel proces-verbaal, om aan de bevoegde toezichthoudende autoriteit mee te delen dat een opsporingsonderzoek of een gerechtelijk onderzoek werd opgestart, vervolging werd ingesteld. Deze mededeling doet de mogelijkheid vervallen voor de toezichthoudende autoriteit om haar corrigerende bevoegdheden uit te oefenen. Dit is geen

peut être précisé que les points 4° et 5°, ont en effet un champ d'application personnel plus large que les deux premiers points, puisqu'ils peuvent concerner d'autres personnes que le sous-traitant, la personne agissant sous l'autorité d'une autorité visée au titre 3 ou sous l'autorité du sous-traitant ou encore que le mandataire.

Art. 227

Cet article est repris de l'article 42 LVP et concerne la responsabilité civile du responsable du traitement du paiement des amendes auxquelles son préposé ou son mandataire a été condamné.

Art. 228

De manière générale, les dispositions générales du droit pénal en matière de concours d'infractions sont applicables.

Il est toujours possible que plusieurs procédures soient introduite pour la même violation. Pour cette raison il est prévu une disposition qui permette qu'un protocole soit signé entre l'autorité de contrôle compétente et le ministère public. Dans ce protocole il est déterminé le mode de fonctionnement et de coopération lorsque les différents types de procédures pour la même infraction se chevauchent. En effet, la Cour constitutionnelle dans son arrêt 86/2015 du 11 juin 2015 a statué que "*dans les cas où il y a cumul entre uns sanction pénale, et une sanction administrative, le principe non bis in idem doit être respecté lors de l'application de ces règles dans la pratique*.".

Un arrêté royal délibéré en Conseil des ministres devra prévoir les modalités ainsi que le modèle de ce protocole.

Lorsqu'on n'opte pas pour un protocole, la loi prévoit quelques règles standard, à l'instar du Code pénal social et de ses articles 68 et suivants. Lorsqu'une violation peut aussi être qualifiée comme étant pénale, le procureur du Roi dispose d'un délai de deux mois, à compter du jour de la réception de l'original du procès-verbal, pour communiquer à l'autorité de contrôle compétente qu'une information ou une instruction a été ouverte ou que des poursuites ont été entamées. Cette communication éteint la possibilité pour l'autorité de contrôle d'exercer ses mesures correctrices. Cette situation n'est pas idéale en effet, mais n'est valable que pour les situations où aucun protocole d'accord n'a été

ideale situatie, maar ze is enkel van toepassing wanneer geen protocolakkoord werd ondertekend. De wetgever wil dan ook het afsluiten van protocolakkoorden stimuleren om dergelijke situaties te regelen.

Bij gebrek aan een mededeling binnen twee maanden, kunnen de feiten enkel nog administratiefrechtelijk worden gesanctioneerd.

Er wordt eveneens voorzien dat bepaalde artikelen niet van toepassing zijn op de publieke overheden en instellingen.

Art. 229

Dit artikel herneemt het oude artikel 43 WVP en is nodig om expliciet de toepassing te voorzien van hoofdstuk VII en artikel 85 van het Strafwetboek die de deelneming en de verzachtende omstandigheden betreffen. Er is geen onmiddellijke toepassing van de verzachtende omstandigheden op strafrechtelijke sancties, tenzij de bijzondere wet dit expliciet vermeldt.

Art. 230

Dit artikel vergt geen commentaar.

TITEL 7

Het controleorgaan op de politionele informatie

HOOFDSTUK I

Samenstelling en statuut van de leden

Art. 231

De samenstelling van het C.O.C. wordt gewijzigd en gaat van 8 naar 3 leden. De Privacycommissie vergist zich dus in zijn advies 33/2018 waar het in punt 456 *in fine* stel dat het C.O.C. in het ontwerp 6 leden zou tellen. Het zijn er 3 naar analogie met het Vast Comité I. Het lid van de Privacycommissie wordt vervangen door een magistraat van het openbaar ministerie, vermits de Privacycommissie wordt opgeheven en vervangen door een nieuw samengestelde Gegevensbeschermingsautoriteit. Daarnaast zullen twee leden van de geïntegreerde politie en één deskundige niet-jurist deel uitmaken van een nieuwe dienst onderzoeken van het Controleorgaan... De voorzitter blijft zoals voorheen een magistraat zonder nog het onderscheid te maken tussen zittende en staande

signé. Le législateur encourage dès lors l'adoption d'un tel protocole afin de régler de telles situations.

A défaut de communication du Procureur du Roi dans les deux mois, les faits ne peuvent être sanctionnés que de manière administrative.

Il est également prévu que certains articles ne s'appliquent pas aux autorités et institutions publiques.

Art. 229

Cet article est l'ancien article 43 LVP et est nécessaire afin de prévoir explicitement l'application du chapitre VII et de l'article 85 du Code pénal qui concerne la participation et les circonstances atténuantes. Il n'y a en effet pas d'application explicite des circonstances atténuantes sur les sanctions pénales, à moins que la loi particulière le stipule expressément.

Art. 230

Cet article n'appelle aucun commentaire.

TITRE 7

L'organe de contrôle de l'information policière

CHAPITRE I^ER

Composition et statut des membres

Art. 231

La composition du C.O.C. est modifiée et passe de 8 à 3 membres. La Commission vie privée se trompe donc dans l'avis 33/2018 où elle mentionne au point 456 *in fine* que le C.O.C. compterait 6 membres dans le projet. Il s'agit du 3 membres par analogie avec le Comité permanent R. Le membre de la Commission vie privée est remplacé par un magistrat du ministère public, puisqu'elle est abrogée et remplacée par la nouvelle Autorité de protection des données recomposée. Par ailleurs deux membre de la police intégrée et un expert non-juriste formeront le nouveau service d'enquête. Le président reste, comme par le passé, un magistrat sans faire encore de distinction entre la magistrature assise et debout. Les deux peuvent prétendre à la présidence, afin d'augmenter le nombre potentiel de candidats pour

magistratuur. Beiden kunnen in aanmerking komen voor het voorzitterschap, teneinde het potentieel aantal kandidaten voor de functie te verhogen. De hervorming van de samenstelling wordt verder ingegeven door de volgende motieven:

— de voorzitter: om de hogervermelde redenen wordt de mogelijkheid voorzien dat zowel een zittend als een staand magistraat zich kandidaat voor de functie kan stellen (De commissie voor bijzondere administratieve methodes –BAM). Het blijft belangrijk dat de voorzitter een magistraat is, niet enkel omdat de core-business van de opdrachten van het C.O.C. te maken heeft met de eerbiediging van grondrechten zoals het recht op privacy, maar ook en vooral omdat het C.O.C. of zijn voorzitter een aantal quasi jurisdictionele bevoegdheden heeft. In tegenstelling tot de kritiek van de Privacycommissie (cf. advies 33/2018, n° 456) is de hoedanigheid van magistraat als lid van het C.O.C. belangrijk en heeft het ook te maken met de verschillende rollen die het C.O.C. heeft. Terreinkennis is essentieel voor een toezichtsorgaan op de politiesector, reden waarom er politieambtenaren en magistraten aanwezig moeten zijn. Niet toevallig zijn bijv. zowel de voorzitter van het Comité P als het Comité I (en het OCAD) verplicht magistraat en kan worden vastgesteld dat doorheen zijn 25 jarig bestaan de meerderheid van de 5 leden van het Comité P steeds magistraat is.

— een magistraat van het openbaar ministerie: er kan niet langer een lid van de (nieuwe) GBA tegelijk ook lid zijn van het Controleorgaan zijn omdat de leden van het directiecomité van de nieuwe GBA voltijdse mandaten zijn met een eigen belangrijke verantwoordelijkheid binnen de nieuwe GBA. In de toekomst wordt een gedegen kennis van het gegevensbeschermingsrecht trouwens geëist van alle leden (zie benoemingsvoorwaarden) van het Controleorgaan en de dienst onderzoeken. De meerwaarde van een parketmagistraat voor het C.O.C. sluit ook aan bij wat hoger werd gesteld als antwoord op het advies van de Privacycommissie. Hij/zij is vertrouwd met de politiewerking en politieorganisatie, kent tegelijk als magistraat de noden en bezorgdheden van het opsporingswerk en is vertrouwd met de verwachtingen van justitie ten aanzien van de politie en omgekeerd. Voorts wordt hij als magistraat dagelijks geconfronteerd met de grondrechtenproblematiek.

— twee leden van de dienst onderzoeken komende van de geïntegreerde politie: de meerwaarde en zelfs absolute noodzaak voor een politioneel controleorgaan om ook personeelsleden van de politie in huis te hebben staat buiten kijf. De kennis van de interne structuren, werkprocessen, methoden, gewoonten en politiecultuur is primordiaal voor een toezichtsorgaan dat met

la fonction. La réforme de la composition est fondée sur les motifs suivants:

— le président: sur base du raisonnement précité, est prévue la possibilité qu'un magistrat tant assis que debout puisse se porter candidat à la fonction (La Commission des méthodes administratives particulières – MAP). Il est en tout cas primordial que le président soit un magistrat, non seulement parce que le core-business des missions du C.O.C. concerne le respect des droits fondamentaux comme le droit à la vie privée, mais aussi et surtout parce que le C.O.C. ou son président a un nombre de compétences quasi juridictionnelles. Contrairement à la critique de la Commission vie privée (cf. avis 33/2018, n° 456), la qualité de magistrat en tant que membre du C.O.C. est importante et elle est aussi liée aux différents rôles du C.O.C. La connaissance du terrain est essentielle pour un organe de contrôle du secteur policier, raison pour laquelle la présence de fonctionnaires de police et de magistrats est nécessaire. Ce n'est pas par hasard que tant le président du Comité P que celui du Comité R (et de l'OCAM) doivent obligatoirement être des magistrats et que l'on constate qu'en ses 25 ans d'existence, la majorité des 5 membres du Comité P aura toujours été composée de magistrats.

— un magistrat du ministère public: un membre de la (nouvelle) APD ne peut plus être en même temps membre de l'Organe de contrôle parce que les membres du comité de direction de la nouvelle APD sont des mandats à temps plein avec une responsabilité importante au sein de la nouvelle APD. A l'avenir, une connaissance approfondie du droit de la protection des données est d'ailleurs exigée pour tous les membres (voir conditions de nomination) de l'Organe de contrôle et du service d'enquête. La plus-value d'un magistrat du parquet pour le C.O.C. rejoint aussi ce qui a été souligné *supra*, en réponse à l'avis de la Commission vie privée. Il/Elle connaît le fonctionnement de la police et l'organisation de la police, connaît en tant que magistrat à la fois les besoins et préoccupations du travail d'enquête est familiarisé avec les attentes de la justice vis-à-vis de la police et inversement. En outre, il est en tant que magistrat quotidiennement confronté à la problématique des droits fondamentaux.

— deux membres du service d'enquête venant de la police intégrée: la plus-value et même l'absolue nécessité pour un organe de contrôle de police de disposer aussi de membres du personnel de la police est incontestable. La connaissance des structures internes, des processus de travail, méthodes, habitudes et culture policière est primordial pour un organe de contrôle qui

de voeten in de (politionele) realiteit wil staan. Ook het Grondwettelijk Hof oordeelde in die zin in zijn arrest 108/2016: "*De verwerking van persoonsgegevens in de politionele databanken is krachtens artikel 44/1 van de wet op het politieambt immers slechts mogelijk voor zover die gegevens toereikend, ter zake dienend en niet overmatig van aard zijn "in het licht van de doeleinden van bestuurlijke en van gerechtelijke politie waarvoor ze verkregen worden en waarvoor ze later verwerkt worden". Het uitoefenen van toezicht op de naleving van die bepaling veronderstelt aldus een bepaalde deskundigheid en ervaring op het vlak van de doeleinden van bestuurlijke en gerechtelijke politie die de politiediensten nastreven*" (overweging B. 120.3).

De vermindering van het aantal personeelsleden van de politie van vier leden van het Controleorgaan naar twee leden binnen de dienst onderzoeken heeft eveneens te maken met de visie van het Grondwettelijk Hof op de samenstelling van het C.O.C. onder de WVP: "*Gelet op de nagestreefde doelstelling van controle op de naleving, door de politiediensten, van de bepalingen van de bestreden wet, is het evenwel niet redelijk verantwoord dat wegens het ontbreken van bepalingen betreffende het aantal leden die afkomstig zijn van de politiediensten alsook betreffende het totale aantal leden van het Controleorgaan, de meerderheid van de leden van het Controleorgaan zou worden benoemd op grond van hun hoedanigheid van lid van de lokale of van de federale politie*" (overweging B. 120.5, 5e §).

Waar het Grondwettelijk Hof aldus een meerderheid van personeelsleden van de politie binnen het Controleorgaan als ongrondwettig beoordeelt gaat dit ontwerp verder in op die redenering en voorziet het dat het aantal personeelsleden van de politie nooit meer dan 1/3 van het totaal aantal leden (controleorgaan en dienst enquêtes samen genomen) mag bedragen, en voorziet het dat de politieambtenaren deel uitmaken van de dienst onderzoeken en niet langer van het Controleorgaan zelf onder wiens gezag zij staan Een beperking van het aantal personeelsleden van de politie des te meer nu het als DPA toezicht dient te houden op de geïntegreerde politie.

Daarnaast wil het ontwerp door een vermindering van het aantal leden budgettaire ruimte vrijmaken voor het aanwerven van meer ondersteunend personeel, wat actueel een reëel probleem is voor het C.O.C. Niet alleen is er thans een gemis op dat vlak, dat zal, gezien de nieuwe bijkomende bevoegdheden in de toekomst, alleen maar nijpender worden. Het Controleorgaan heeft absoluut nood aan één jurist en één ICT-deskundige als ondersteuning voor haar werking. Ten einde de budgettaire meerkost te beperken voorziet het ontwerp om die

veut garder les pieds sur terre dans la réalité (policière). La Cour Constitutionnelle a aussi jugé dans ce sens dans son arrêt 108/2016: *"En effet, le traitement des données à caractère personnel dans les banques de données de (la) police en vertu de l'article 44/1 de la loi sur la fonction de police est seulement possible "pour autant que ces données présentent un caractère adéquat, pertinent et non excessif au regard des finalités de police administrative et de police judiciaire pour lesquelles elles ont été obtenues et pour lesquelles elles seront traitées ultérieurement. Le contrôle du respect de cette disposition suppose donc une certaine expertise et expérience des finalités de police administrative et judiciaire que poursuivent les services de police."* (considérant B.120.3).

La diminution du nombre de membres du personnel de la police comme membre de l'organe de Contrôle de quatre à deux au sein du service d'enquête tient compte également de la vision de la Cour Constitutionnelle sur la composition du C.O.C. sous le régime de la LVP: *"Eu égard à l'objectif de contrôle du respect, par les services de police, des dispositions de la loi attaquée, il n'est toutefois pas raisonnablement justifié qu'en l'absence de dispositions relatives au nombre de membres issus des services de police et au nombre total de membres de l'Organe de contrôle, la majorité des membres de l'Organe de contrôle soient nommés, en leur qualité de membre de la police locale ou de la police fédérale"* (considérant B. 120. 5e §).

Par conséquent, où la Cour Constitutionnelle évalue une majorité de membres du personnel de la police au sein de l'Organe de contrôle comme inconstitutionnelle, ce projet va plus loin dans ce raisonnement et prévoit que le nombre de membres du personnel de la police ne peut jamais s'élever à plus d'1/3 du nombre total des membres (Organe de contrôle et service d'enquête ensemble) et prévoit qu'ils font partie du service d'enquête en non plus de l'organe de Contrôle et sont soumis a l'autorité de l'Organe de contrôle. Une limitation du nombre de membres du personnel de la police s'impose d'autant plus maintenant que le C.O.C. en tant que DPA doit assurer le contrôle de la police intégrée.

En outre, le projet veut, en diminuant le nombre de membres, dégager des moyens budgétaires pour recruter plus de personnel d'appui, ce qui est actuellement un réel problème pour le C.O.C. Non seulement il y a actuellement une lacune sur ce point, ce qui à l'avenir sera encore plus urgent compte tenu des nouvelles compétences supplémentaires. L'Organe de contrôle a absolument besoin d'un juriste et d'un expert ICT comme appui pour son fonctionnement. Afin de limiter le surcoût budgétaire le projet prévoit en conséquence

reden in een vermindering van het aantal leden. Tot slot zal die vermindering ook het beslissingsproces binnen het C.O.C. vereenvoudigen.

Voor het overige herhaalt dit artikel in grote mate het huidige artikel 36*ter*/1 WVP. De onafhankelijkheid van het C.O.C. wordt versterkt door erin te voorzien dat de leden niet van hun functie kunnen worden ontheven voor meningen die zij uiten of daden die zij stellen bij het vervullen van zijn functies. De duur van het mandaat wordt bepaald op zes jaar, éénmaal hernieuwbaar en is daarmee identiek aan het huidige artikel 36*ter*/1 WVP en identiek aan de toekomstige regeling van de mandaten van lid van het directiecomité in de nieuwe GBA.

Ook de 2e en 3e paragrafen bevatten weinig nieuwe bepalingen ten opzichte van het huidige artikel 36*ter*/1 WVP. De leden oefenen hun ambt voltijds uit zoals dat thans het geval is. In antwoord op de opmerking van de Raad van State (p. 103) met betrekking tot de taal, wordt er besloten om dezelfde taalvereisten die in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit staan, te integreren.

De 4e en 5e paragrafen voorzien de creatie van een dienst onderzoeken binnen en onder het gezag van het Controleorgaan.

Art. 232

Dit artikel behandelt in zijn eerste paragraaf de algemene benoemingsvoorwaarden voor de leden. De voorwaarden zijn identiek aan het huidig art. 36*ter*/1 § 4 WVP behalve de bijkomende benoemingsvoorwaarde die bestaat in het verbod een functie uit te oefenen in een beleidscel van een federale of regionale minister. Deze voorwaarde is overgenomen van de wet van 3 december 2017 (cf. art. 38, 5°) en is noodzakelijk om de onafhankelijkheid van het Controleorgaan te versterken gezien ook zijn bijkomende rol als toezichthoudende autoriteit.

De tweede paragraaf is nieuw en voorziet ook voor de voorzitter en de parketmagistraat een relevante ervaring van 10 jaar in het domein van de bescherming van persoonsgegevens en de politionele informatiehuishouding.

Paragraaf 3 behandelt de specifieke benoemingsvoorwaarden voor de expert als lid van het Controleorgaan. Er is voorzien dat het een licentiaat of master in de rechten moet zijn, wat niet wordt vereist van de expert binnen de dienst onderzoeken.

et aussi pour cette raison une diminution du nombre de membres. Enfin, cette diminution simplifiera aussi le processus de décision au sein du C.O.C.

Pour le surplus, cet article répète en grande partie l'actuel article 36*ter*/1 de la LVP. L'indépendance du C.O.C est renforcée en prévoyant que les membres ne peuvent être relevés de leur fonction en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent dans le cadre de l'exercice de leurs fonctions. La durée du mandat est fixée à 6 ans, renouvelable une fois et est identique à l'actuel article 36*ter*/1 LVP et identique à la future réglementation des mandats des membres du comité de direction dans la nouvelle APD.

Les paragraphes 2 et 3 contiennent peu de nouvelles dispositions par rapport à l'actuel article 36*ter*/1 LVP. Les membres exercent leur fonction à temps plein comme c'est le cas actuellement. En réponse à la remarque du Conseil d'État (p. 103) relative aux exigences linguistiques, il est décidé d'insérer les mêmes exigences linguistiques prévues dans la loi du 3 décembre 2017 relative à l'Autorité de protection des données.

Les paragraphes 4 et 5 prévoient la création d'un service d'enquête au sein et sous l'autorité de l'Organe de Contrôle.

Art. 232

Cet article traite dans son paragraphe premier des conditions générales de nomination pour les membres. Les conditions sont identiques à l'actuel article 36*ter*/1 § 4 LVP hormis la condition de nomination supplémentaire qui interdit d'exercer une fonction dans une cellule stratégique d'un ministre fédéral ou régional. Cette condition est reprise de la loi du 3 décembre 2017 (cf. art. 38, 5°) et est indispensable pour renforcer l'indépendance de l'Organe de contrôle vu aussi son rôle supplémentaire en tant qu'autorité de contrôle.

Le paragraphe 2 est nouveau et prévoit aussi pour le président et le magistrat du parquet une expérience pertinente de 5 ans dans le domaine de la protection des données à caractère personnel et de la gestion des informations policières.

Le paragraphe 3 traite des conditions spécifiques de nomination pour l'expert qui est membre de l'organe de Contrôle. Il est prévu qu'il doit être licencié ou master en droit ce qui n'est pas exigé de l'expert au sein du service d'enquête.

De vervangingsregeling van de vierde paragraaf ontbrak in de huidige WVP en voorziet dat het vervangend lid het mandaat van het te vervangen lid beëindigt. Hij/zij begint dus niet aan een nieuw mandaat. Deze regeling is identiek aan die van de leden van de Vaste Comités P en I.

Paragraaf 5, eerste lid behandelt de algemene benoemingsvoorwaarden van de leden van de dienst onderzoeken van het Controleorgaan terwijl het tweede lid de specifieke benoemingsvoorwaarden voor de personeelsleden van de politie behandelt. Ze zijn identiek aan de huidige benoemingsvoorwaarden voorzien in art. 36*ter*/1 § 5 WVP, met uitzondering van de voorziene ervaring van minimum twee jaar inzake de verwerking van politionele informatie of de bescherming van persoonsgegevens in de plaats van slechts één jaar actueel (art. 36*ter*/1 § 5, 3°, WVP). Ook die verstrakking is ingegeven door de noodzaak aan nog meer expertise binnen het C.O.C., gelet op zijn bijkomende opdrachten als DPA en door eventuele andere wetten.

Paragraaf 6 behandelt de specifieke benoemingsvoorwaarden voor de expert binnen de dienst onderzoeken die minder veeleisend zijn dan voor de expert die lid is van het Controleorgaan zelf.

Art. 233

De eerste paragraaf voorziet in de opstelling van een huishoudelijk reglement en is de overname van het huidige art. 36*ter* § 3 WVP. Het tweede lid bepaalt de rol die de Voorzitter van het C.O.C. dient te spelen en is identiek aan het actuele art. 36*ter*/1/1 WVP.

De tweede paragraaf is nieuw en bepaalt dat de leden van het Controleorgaan binnen de perken van hun bevoegdheden op directe of indirecte wijze van niemand instructies of vragen kunnen krijgen (zie de identieke bepaling onder art. 42.2 van de Richtlijn) en dat zij niet aanwezig kunnen zijn bij beslissingen over dossiers waarbij zij een persoonlijk of rechtstreeks belang hebben of waarbij hun bloed- of aanverwanten tot en met de vierde graad een persoonlijk of rechtstreeks belang hebben. Ook deze bepaling heeft als doelstelling de onafhankelijkheid en integriteit van de beslissingen van het Controleorgaan te versterken en is geïnspireerd op de overeenkomstige bepalingen van de wet van 3 december 2017 (art. 43).

De derde paragraaf voorziet dat de leden van het Controleorgaan en zijn personeelsleden niet burgerlijk aansprakelijk kunnen worden gesteld voor hun beslissingen, handelingen of gedragingen in de uitoefening van

La règle de remplacement du paragraphe 4 était manquante dans la LVP actuelle et prévoit que le membre suppléant achève le mandat du membre à remplacer. Il/elle ne commence donc pas un nouveau mandat. Ce règlement est identique à celui des membres des Comités Permanents P et R.

Le paragraphe 5, alinéa premier traite les conditions de nomination générales des membres du service d'enquêtes de l'Organe de contrôle tandis que l'alinéa 2 traite des conditions de nomination spécifiques pour les membres du personnel de la police. Elles sont identiques aux conditions de nomination actuelles prévues à l'art. 36*ter*/1 § 5 LVP, à l'exception de l'expérience prévue de minimum deux ans en matière de traitement de l'information policière ou de protection des données à caractère personnel à la place de seulement un an actuellement (art. 36*ter*/1 § 5, 3°, LVP). Ce durcissement se fonde également sur la nécessité à encore plus d'expertise au sein du C.O.C. vu ses missions supplémentaires en tant que DPA et par d'autres lois éventuelles.

Paragraphe 6 traite des conditions spécifiques de nomination pour l' expert au sein du service d'enquête qui sont moins sévères que pour l'expert comme membre de l'Organe de contrôle.

Art. 233

Le paragraphe premier prévoit la rédaction d'un règlement d'ordre intérieur et est la reprise de l'actuel art. 36*ter* § 3 LVP. Le 2e alinéa définit le rôle du président du C.O.C. et est identique à l'actuel art. 36*ter*/1/1 LVP.

Le paragraphe 2 est nouveau et stipule que les membres de l'Organe de contrôle ne peuvent recevoir de personne des instructions ou demandes d'information dans les limites de leurs compétences directement ou indirectement (voir la disposition identique sous l'art. 42.2 de la Directive) et qu'ils ne peuvent pas être présents lors de décisions portant sur des dossiers pour lesquels ils ont un intérêt personnel et direct ou pour lesquels leurs parents ou alliés jusqu'au quatrième degré ont un intérêt personnel ou direct. Cette disposition a également pour objectif de renforcer l'indépendance et l'intégrité des décisions de l'Organe de contrôle et s'inspire des dispositions correspondantes de la loi du 3 décembre 2017 (art. 43).

Le paragraphe 3 prévoit que les membres de l'Organe de contrôle et ses membres du personnel n'encourent aucune responsabilité civile en raison de leurs décisions, actes ou comportements dans l'exercice de

hun wettelijke opdrachten behalve in geval van bedrog of zware fout. Een analoge bepaling is voorzien in de wet van 3 december 2017 (art. 5, 2e lid).

De vierde paragraaf tot slot bevat de klassieke geheimhoudingsclausule die nieuw is in vergelijking met de huidige regeling maar vrij essentieel is, ook geldt voor bijvoorbeeld de leden van het Comité P of I (cf. art. 64 van de wet van 18 juli 1991 betreffende Wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse) en eveneens is voorzien voor de commissarissen in de nieuwe GBA zoals voorzien in de wet van 3 december 2017 (art. 48).

Art. 234

Dit artikel betreft het financieel en administratief statuut van de 3 leden van het Controleorgaan en de 3 leden van de dienst onderzoeken. Het beoogt te komen tot de noodzakelijke uniformiteit in verloning en statuut tussen enerzijds alle leden van het Controleorgaan onderling en anderzijds de leden van het C.O.C. met andere gelijkaardige collaterale organen van het parlement, zoals het Vast Comité P en het Vast Comité I (en binnenkort de leden van het directiecomité van de Gegevensbeschermingsautoriteit), nu hun opdrachten, taken en verantwoordelijkheden analoog zijn.

Tot slot voorziet de WVP actueel in geen enkele financiële regeling voor het lid van de Privacycommissie ondanks gedeeltelijke voorstellen in het verleden om zijn financieel statuut te regelen (zie het "*Wetsvoorstel n° DOC 54, 1943/001 van 29 juni 2016 tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, wat betreft de werking van het Controleorgaan op de politionele informatie*" (artikel 3), ingediend door de heer Brecht Vermeulen, hierna "Wetsvoorstel DOC 54, 1943/001").

De actuele statutaire situatie van de leden is dus een incoherent imbroglio, met substantieel verschillende verloningen en verloningssystemen tussen de leden onderling waaraan een einde moet gesteld worden om te komen tot een meer coherente en uniforme regeling naar analogie met andere collaterale parlementaire instellingen zoals het Comité P en I. Om die reden wordt net dezelfde statutaire en financiële regeling voorzien voor de leden van het Controleorgaan als voor de leden van beide voornoemde Vaste Comités en als voor de nieuwe Gegevensbeschermingsautoriteit. Voor de leden van de dienst onderzoeken wordt eveneens een zelfde verloning voorzien op het niveau

leurs missions légales, sauf en cas de dol ou de faute lourde. Une disposition analogue est prévue dans la loi du 3 décembre 2017 (art. 5, 2e alinéa).

Enfin le paragraphe 4 contient la clause de confidentialité classique qui est nouvelle en comparaison avec l'actuelle règlementation mais qui est vraiment essentielle, vaut aussi pour par exemple les membres du Comité P ou R (cf. art. 64 de la loi du 18 juillet 1991 relative à la loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace) et est également prévue pour les commissaires dans la nouvelle APD, comme prévu dans la loi du 3 décembre 2017 (art. 48).

Art. 234

Le présent article concerne le statut financier et administratif des 3 membres de l'Organe de contrôle et des 3 membres du service d'enquête. Cela a pour objectif de parvenir à l'indispensable uniformité de rémunération et de statut entre d'une part les membres de l'Organe de contrôle entre eux et d'autre part les membres du C.O.C avec d'autres organes collatéraux similaires du Parlement, comme le Comité Permanent P et le Comité Permanent R (et bientôt les membres du comité de direction de l'Autorité de protection des données), maintenant que leurs missions, tâches et responsabilités sont analogues.

Enfin la LVP ne prévoit actuellement aucun règlement financier pour le membre de la Commission vie privée malgré des propositions partielles dans le passé pour régler son statut financier (voir la *"proposition de loi n° Doc 54, 1943/001 du 29 juin 2016 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel, en ce qui concerne le fonctionnement de l'Organe de contrôle de l'information policière"* (article 3), introduit par Monsieur Brecht Vermeulen, ci-après "Proposition de loi Doc 54, 1943/001").

La situation statutaire actuelle des membres est donc un imbroglio incohérent, avec en substance des rémunérations et systèmes de rémunération différents entre les membres auquel il faut mettre fin pour arriver à un règlement plus cohérent et uniforme par analogie avec d'autres organes collatéraux du parlement comme le Comité P et R. C'est la raison pour laquelle exactement le même règlement statutaire et financier est prévu pour les membres de l'Organe de contrôle comme pour les membres des deux Comités Permanents précités et comme pour la nouvelle autorité de protection de données. Pour les membres du service d'enquête est également prévues un salaire identiques à savoir le barème

van een A3 baréma van de personeelsleden van de Gegevensbeschermingsautoriteit. Dat is het huidige baréma van de experten binnen het Controleorgaan.

Art. 235

Dit artikel wil een minimaal secretariaat verankeren in de wet. Zoals hoger gesteld wordt enerzijds een vermindering van het aantal leden van 8 naar 3 voorzien, maar tegelijk voorzien in de mogelijkheid één jurist en één informaticadeskundige aan te werven aan een baréma dat voldoende aantrekkelijk is om valabele kandidaten te kunnen aantrekken.

De personeelsleden staan onder het gezag van het Controleorgaan en de dagelijkse leiding van de voorzitter.

Art. 236

De artikelen 236 tot 238 geven inhoud aan afdeling 1 ("*Algemene bepalingen*") van hoofdstuk II ("*De opdrachten*") van het ontwerp.

Dit artikel behandelt in het algemeen de opdrachten waarmee het Controleorgaan is belast en verwijst naar de opsomming onder de punten 1° tot en met 3°, van artikel 71. Het betreft alle opdrachten als politionele DPA in de zin van de Richtlijn en van het huidig ontwerp tot omzetting van voormelde Richtlijn.

De tweede paragraaf komt tegemoet aan een vergetelheid van de wetgever in 2014. Er werd toen niet expliciet aan het Controleorgaan een adviesbevoegdheid gegeven hoewel in de praktijk de actoren in het werkveld het Controleorgaan regelmatig advies vragen over aangelegenheden die verband houden met politionele informatiehuishouding.

De bepaling is overgenomen uit het artikel 5 van het *Wetsvoorstel n° DOC 54, 1943/001* dat evenzeer deze lacune wou opvullen onder de volgende motivering: "*Het is wenselijk om voor het Controleorgaan in een adviesbevoegdheid te voorzien voor wat betreft iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer, zoals onder meer bepaald in afdeling 1bis van de wet op het politieambt. Het Controleorgaan kan de regering of de wetgevende kamers advies geven in deze materies. De Commissie voor de bescherming van de persoonlijke levenssfeer stelt dit reeds voor in haar advies 47/2013, randnummer 152. Zoals de Commissie eveneens stelt in haar advies 30/2015, bevinden zich immers in het Controleorgaan de specialisten in het politionele informatiebeheer, en*

A3 du statut des agents de l'autorité de protection de données. C'est le barème existant des experts au sein de l'Organe de Contrôle.

Art. 235

Le présent article veut intégrer dans la loi un secrétariat minimum. Comme précisé précédemment est prévu d'une part une diminution du nombre de membres de 8 à 3, mais est en même temps prévu la possibilité de recruter un juriste et un expert en informatique à un barème qui est suffisamment attrayant pour pouvoir attirer des candidats valables.

Les membres du personnel sont placés sous l'autorité de l'Organe de contrôle et sous la direction journalière du Président.

Art. 236

Les articles 236 à 238 donnent du contenu à la section 1 *("Dispositions générales")* du chapitre II *("Les missions")* du projet.

Le présent article traite en général des missions dont l'Organe de contrôle est chargé et fait référence à l'énumération sous les points 1° à 3°, de l'article 71. Cela concerne toutes les missions en tant que DPA policière au sens de la Directive et de l'actuelle projet de transposition de la Directive précitée.

Le paragraphe 2 répond à un oubli du législateur en 2014. On n'avait alors pas donné explicitement de compétence d'avis à l'Organe de contrôle bien que dans la pratique les acteurs de terrain demandent régulièrement des avis à l'Organe de contrôle sur des matières ayant trait à la gestion de l'information policière.

Cette disposition est repris de l'article 5 de la *proposition de loi n° DOC 54, 1943/001* qui voulait remplir cette lacune sous la motivation suivante: "*Il serait souhaitable de conférer à l'Organe de contrôle une compétence d'avis concernant toute matière ayant trait à la gestion de l'information policière, comme le prévoit notamment la section 1re bis de la loi sur la fonction de police. L'Organe de contrôle peut remettre un avis au gouvernement ou aux chambres législatives dans ces matières. C'est ce que propose déjà la Commission de la protection de la vie privée dans son avis 47/2013, point 152. Comme le précise également la Commission dans son avis 30/2015, l'Organe de contrôle compte en son sein les spécialistes en gestion de l'information policière et l'aspect "vie privée" au sein de l'Organe de*

wordt het aspect persoonlijke levenssfeer binnen het Controleorgaan specifiek opgevolgd door het lid van de Commissie en de 2 leden-experten".

De adviesbevoegdheid is overigens ook voorgeschreven door art. 46.1.c) van de Richtlijn.

De derde paragraaf geeft een opsomming van zijn huidige politionele controleopdrachten zoals die ook zijn voorzien waren in artikel 36*ter*/9 WVP maar is iets ruimer en volledieger in zijn opsomming. Het C.O.C. zal inderdaad niet alleen de rechtstreekse toegang en rechtstreekse bevraging van de ANG controleren, maar meer algemeen elke mededeling van persoonsgegevens en informatie uit een eender welke politionele gegevensbank.

Art. 237

Dit artikel is een herneming van artikel 36*ter*/8 WVP waar het aangeeft op wiens verzoek het C.O.C. kan optreden, naast het eigen ambtshalve optreden. Bijkomend werd hier voorzien in een verzoekrecht voor de minister die de materie betreffende privacy in zijn bevoegdheden heeft. Dit is logisch gezien de uitbreiding van de bevoegdheden van het C.O.C. als gemeenrechtelijke DPA en DPA voor de politiesector.

Art. 238

Dit artikel is een quasi woordelijke herneming van artikel 36*ter*/13 WVP.

Art. 239

De eerste paragraaf is een parafraseren van het artikel 36*ter*/10 § 1 WVP met dien verstande dat het vervolledigd werd door er ook in te voorzien dat de controle naar de conformiteit van de inhoud van de politionele gegevensbanken en de verwerkingsprocedures met de wettelijke bepalingen, niet alleen slaat op de ANG, maar ook op de basisgegevensbanken, de bijzondere gegevensbanken en de technische gegevensbanken.

De tweede paragraaf herneemt en vervolledigt de actuele tweede paragraaf van artikel 36*ter*/10 WVP door ook de bijzondere gegevensbanken en de technische gegevensbanken te viseren in de daar voorziene controleopdrachten.

De derde paragraaf, 1e en 2e lid hernemen de actuele 1e en 2e leden van de derde paragraaf van artikel 36*ter*/10 WVP, wat eveneens het geval is voor het

contrôle fait l'objet d'un suivi spécifique par le membre de la Commission et les deux membres-experts".

La compétence d'avis est d'ailleurs aussi prescrite par l'article 46.1c) de la Directive.

Le paragraphe 3 énumère ses missions de contrôle de police actuelles comme celles-ci étaient aussi prévues à l'article 36*ter*/9 LVP mais est un peu plus large et plus complet dans son énumération. En effet, le C.O.C. ne contrôlera pas seulement l'accès direct et l'interrogation directe de la BNG mais plus généralement toute communication de données à caractère personnel et d'informations à partir de n'importe quelle banque de données policière.

Art. 237

Cet article est une reprise de l'article 36*ter*/8 LVP où il indique à la requête de qui le C.O.C. peut intervenir, en complément de l'intervention d'office. De plus, il est aussi prévu un droit de demande pour le ministre qui a la matière de la vie privée dans ses compétences. C'est logique vu l'extension des compétences du C.O.C. en tant que DPA de droit commun et DPA pour le secteur de la police.

Art. 238

Cet article est une reprise quasi littérale de l'article 36*ter*/13 LVP.

Art. 239

Le paragraphe premier est une paraphrase de l'article 36*ter*/10 § 1er LVP étant entendu qu'il a été complété en y prévoyant que le contrôle de la conformité du contenu des banques de données policières et des procédures de traitement avec les dispositions légales porte non seulement sur la BNG mais aussi sur les banques de données de base, les banques de données particulières et les banques de données techniques.

Le paragraphe 2 reprend et complète l'actuel paragraphe 2 de l'article 36*ter*/10 LVP en visant aussi les banques de données particulières et les banques de données techniques dans les missions de contrôles qui y sont prévues.

Le paragraphe 3, premier et 2e alinéa reprend les actuels premier et 2e alinéa du paragraphe 3 de l'article 36*ter*/10 LVP, ce qui est également le cas pour le dernier

laatste lid met betrekking tot de toegang tot het centraal register van de bijzondere gegevensbanken.

Art. 240

Dit artikel somt alle opdrachten van het Controleorgaan als DPA voor de operationele gegevensverwerkingen van de politiediensten op. Zij weerspiegelen de opdrachten van de toezichthoudende autoriteit die voorzien werden in de Richtlijn.

Het gaat om:

1° een algemene voorlichtingsopdracht van het brede publiek (zie ook art. 46.1.b) van de Richtlijn). Dit is een opdracht die het actuele Controleorgaan ook thans reeds vervult met onder meer een eigen website (*www.controleorgaan.eu);*

2° een algemene voorlichtingsopdracht voor de verwerkingsverantwoordelijken en de betrokkenen (zie ook art. 46.1.d) van de Richtlijn). Ook dit is een opdracht die het actuele Controleorgaan reeds waarneemt. Zo is er bijvoorbeeld reeds enige tijd regelmatig overleg met de politiediensten omtrent de toekomstige verplichtingen van de Richtlijn en beantwoordt het Controleorgaan regelmatig privacy-gerelateerde vragen van de politiediensten;

3° een informatieverplichting ten voordele van elke betrokkene zowel omtrent de Verordening als de Richtlijn, alsmede een samenwerkingsverplichting met toezichthoudende autoriteiten van andere lidstaten (zie ook art. 46.1.e) van de Richtlijn). Ook deze verplichting kan uiteraard reeds op vandaag door het Controleorgaan waargenomen worden zij het dat het actueel toch vooral de politiediensten zelf zijn die de weg naar het Controleorgaan vinden veeleer dan de betrokkene/burger. Door evenwel van het Controleorgaan een volwaardige toezichthoudende autoriteit te maken en haar ook toe te laten de klachten te behandelen (zie hieronder onder 4°), wat tot op heden steeds tot de bevoegdheid van de Privacycommissie heeft behoord, zal zij ten volle ook die rol kunnen spelen. Wat de samenwerking met andere toezichthoudende autoriteiten betreft kan melding gemaakt worden van het feit dat ook op heden reeds een lid van het C.O.C. deelneemt aan de zgn. “Schengen-evaluaties” samen met de Privacycommissie;

4° de klachtenbehandeling (zie ook art. 46.1.f) van de Richtlijn).

Gezien het COC eveneens de DPA is voor de persoonsgegevensverwerkingen in het kader van de

alinéa relatif à l’accès au registre central des banques de données particulières.

Art. 240

Cet article énumère toutes les missions de l’Organe de contrôle en tant que DPA pour les traitements des données opérationnels des services de police. Elles mettent en évidence les missions de l’autorité de contrôle qui sont prévues dans la Directive.

Il s’agit:

1° d’une mission d’information générale du grand public (voir aussi art. 46.1.b) de la Directive). C’est une mission que l’actuel Organe de contrôle remplit aussi déjà actuellement, entre autres, via son site internet (*www.organedecontrole.eu);*

2° une mission d’information générale pour les responsables du traitement et les personnes concernées (voir aussi art. 46.1d) de la Directive). C’est aussi une mission que l’actuel Organe de contrôle assure déjà. Ainsi, l’Organe de contrôle entretient déjà depuis un certain temps une concertation régulière avec les services de police relative aux futures obligations de la Directive et l’Organe de contrôle répond régulièrement à des questions des services de police liées à la vie privée;

3° une obligation d’information à toute personne concernée tant concernant le Règlement que la Directive, ainsi qu’une obligation de collaboration avec les autorités de contrôle d’autres États membres (voir aussi art.46.1.e) de la Directive). Evidemment il va de soi que cette obligation peut aussi déjà aujourd’hui être assurée par l’Organe de contrôle, bien qu’actuellement ce sont aussi surtout les services de police eux-mêmes qui trouvent le chemin de l’Organe de contrôle plutôt que la personne concernée/citoyen. Toutefois, en faisant de l’Organe de contrôle une autorité de contrôle à part entière et en lui permettant aussi de traiter les plaintes (voir ci-dessous (*infra*) le point 4°), ce qui jusqu’à présent relève toujours de la compétence de la Commissie vie privée, il pourra aussi jouer pleinement ce rôle. En ce qui concerne la collaboration avec d’autres autorités de contrôle, il peut être fait état qu’aussi à présent un membre du C.O.C. participe déjà aux dites “évaluations Schengen” ensemble avec la Commission vie privée;

4° le traitement des plaintes (voir aussi art. 46.1.f) de la Directive).

Le C.O.C étant également la DPA pour les traitements de données à caractère personnel effectués

Verordening, moeten ook de bevoegdheden die worden toegekend door de Verordening worden voorzien, zoals de Privacy Commissie opmerkt in haar advies in paragraaf 456. In dit opzicht werden enkele opdrachten toegevoegd, met name:

Verplichte opstelling van een lijst van verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling vereist is;

Bevorderen, adviseren en goekeuren van gedragscodes;

Bevorderen van certificeringsmechanismen;

Opstellen en bekendmaken van criteria voor de accreditatie van toezichtsorganen op gedragscodes;

Toetsing van afgegeven certificeringen.

Art. 241

Dit artikel voorziet erin dat het Controleorgaan één van haar leden kan afvaardigen binnen comités of groepen waaraan het als toezichtsautoriteit in de politiesector verplicht deelneemt of verkiest aan deel te nemen en is mede geïnspireerd op het artikel 52, § 2, van de de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit.

Art. 242

Dit artikel voorziet dat het Controleorgaan een breed openbaar onderzoek of een brede openbare raadpleging of tot een meer gericht onderzoek of een meer gerichte raadpleging van de vertegenwoordigers van de sector politie kan overgaan.

Art. 243

Dit artikel omschrijft de internationale verplichtingen die het Controleorgaan in haar domein dient na te komen en is mede geïnspireerd op de artikelen 55 en 56 van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Het vloeit ook voort uit de artikelen 40 en 50 van de Richtlijn.

Bovendien wil de wetgever het Controleorgaan de middelen geven om internationale samenwerkingen tot stand te brengen teneinde haar taken uit te voeren, inzonderheid door te voorzien in gemeenschappelijke kennis via deskundigheidspools en door informatie uit

conformément au Règlement, il y a lieu de prévoir les compétences attribuées par le Règlement, ainsi que l'a signalé la Commission vie privée dans son avis au point 456. A cet effet, plusieurs missions sont ainsi ajoutées, telles que:

Établir la liste des traitements pour lesquels une analyse d'impact relative à la protection des données est requise;

Favoriser, recommander et approuver des codes de conduite;

Favoriser des mécanismes de certification;

Etablir et publier des critères pour l'accréditation d'organes de contrôle en matière de codes de conduite;

Vérifier des certifications délivrées.

Art. 241

Cet article prévoit que l'Organe de contrôle peut détacher un de ses membres dans des comités ou groupes auxquels en tant qu'autorité de contrôle dans le secteur de la police il participe obligatoirement ou choisit d'y participer et est également inspiré de l'article 52, § 2, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

Art. 242

Cet article prévoit que l'Organe de contrôle peut procéder à une large enquête publique ou une large consultation publique ou une enquête ou une consultation plus ciblées des représentants du secteur policier.

Art. 243

Cet article définit les obligations internationales que l'Organe de contrôle doit respecter dans son domaine et est également inspiré des articles 55 et 56 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données. Cela découle aussi des articles 40 et 50 de la Directive.

En outre, le législateur entend donner à l'Organe de Contrôle les moyens de créer des collaborations internationales afin de remplir ses missions, notamment en créant une connaissance commune via des pôles d'expertises et en échangeant de l'information, ou

te wisselen of nog, door middelen te delen om gemeenschappelijke doelstellingen te bereiken.

Net zoals dat op nationaal niveau mogelijk is, wordt ook op internationaal niveau het Controleorgaan gemachtigd bepaalde van haar leden of personeelsleden aan te wijzen als vertegenwoordigers bij internationale autoriteiten.

Art. 244

Heel wat bepalingen zijn de woordelijke overname van de bestaande bevoegdheden zoals opgenomen in de WVP. Er zijn echter ook een aantal nieuwe of bijkomende bevoegdheden voorzien die noodzakelijk zijn gebleken zowel voor zijn reguliere werking als Controleorgaan op de politie zoals het dat sinds oktober 2015 uitoefent, als voor de toekomstige bevoegdheid als DPA voor de politiesector. Een aantal bepalingen zijn overgenomen uit het *Wetsvoorstel n° DOC 54, 1943/001* waaromtrent het Controleorgaan op vraag van de voorzitter van de Commissie Binnenlandse Zaken van de Kamer het "*Advies wetgeving nr. 01/2016 van 15 september 2016*" uitbracht. In dat advies werd onder meer gesteld dat "*om de goede werking van het C.O.C. te verzekeren het immers van meet af aan duidelijk* (was) *dat de eerste reparatiewet van 23 augustus 2015 niet zou volstaan en dat derhalve een tweede reparatiewet noodzakelijk is. Deze aanpassingen betreffen een verdere verduidelijking van de statutaire bepaling rond verloning en een aantal operationele bepalingen*" (randnummer 2). Die eerste reparatiewet betrof inderdaad de "*Wet van 23 augustus 2015 tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, wat het Controleorgaan op de politionele informatie betreft*", die voornamelijk een eerste reeks statutaire problemen en onduidelijkheden heeft opgelost, maar die een aantal andere onopgelost heeft gelaten die dat tot op de dag van vandaag zijn gebleven. Het zijn deze die het *Wetsvoorstel n° DOC 54, 1943/001* (minstens gedeeltelijk) heeft willen aanpakken. De behandeling ervan werd in de Commissie Binnenlandse Zaken nadien niet meer verder gezet, mede in het licht van de nakende hervorming van de Privacycommissie en dus ook van het Controleorgaan. Huidig ontwerp is de gelegenheid om enkele ervan terug op te pikken.

Er moet ook op gewezen worden dat art. 47.1 van de Richtlijn voorschrijft dat "*Elke lidstaat voorziet erin bij wet dat elke toezichthoudende autoriteit effectieve onderzoeksbevoegdheden heeft. Die bevoegdheden omvatten ten minste de bevoegdheid om van de verwerkingsverantwoordelijke en de verwerker toegang*

encore en partageant des ressources pour atteindre des objectifs communs.

Comme au niveau national, l'Organe de contrôle est habilité au niveau internationale à désigner certains de ses membres ou membres du personnel en tant que représentants auprès d'autorités internationales.

Art. 244

De nombreuses dispositions sont la reproduction in extenso des compétences existantes telles que reprises dans LVP. Cependant est aussi prévu un nombre de compétences nouvelles ou supplémentaires qui se sont avérées nécessaires tant pour son fonctionnement régulier en tant qu'Organe de contrôle de la police comme il l'exerce depuis octobre 2015, que pour sa future compétence en tant que DPApour le secteur de la police. Un nombre de dispositions sont reprises de la *Proposition de loi n° DOC 51, 1943/001* où l'Organe de contrôle, à la demande du président de la Commission Intérieur de la Chambre, a rendu *"l'avis législation n° 01/2016 du 15 septembre 2016"*. Cet avis énonçait notamment que *"afin d'assurer le bon fonctionnement de l'Organe de contrôle, il est toutefois apparu d'emblée clairement que la loi de réparation du 23 août 2015 ne suffirait pas et qu'il en faudrait par conséquent une seconde. Ces modifications visent à clarifier la disposition statutaire relative à la rémunération ainsi que plusieurs dispositions organisationnelles"* (considérant – point 2). Cette première loi de réparation concernait en effet la *"Loi du 23 août 2015 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en ce qui concerne l'Organe de contrôle de l'information policière"*, qui a principalement résolu une première série de problèmes statutaires ainsi que des ambiguïtés mais qui a laissé en suspens plusieurs autres qui le sont encore aujourd'hui. Ce sont ces problèmes spécifiques que la *proposition de loi n° DOC 54, 1943/001* a voulu (du moins en partie) résoudre. Leur traitement n'a ensuite pas été poursuivi dans la commission Intérieur, notamment à la lumière de la réforme imminente de la Commission vie privée et donc aussi de l'Organe de contrôle. Le projet actuel est l'occasion d'en reprendre certains.

Il faut aussi noter que l'art. 47.1 de la Directive prévoit que *"Chaque état membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui d'obtenir du responsable du traitement ou du sous-traitant accès à toutes les données à caractère*

te verkrijgen tot alle persoonsgegevens die worden verwerkt en tot alle informatie die noodzakelijk is voor de uitvoering van haar taken".

De eerste paragraaf van dit artikel is de gedeeltelijke overname van het artikel 36*ter*/11 WVP zodat het onbeperkt recht op toegang ook slaat op gegevensbanken die door de Belgische politiediensten worden gevoed. Deze verduidelijking werd ook al voorgesteld in het art. 8 van het *Wetsvoorstel n° DOC 54, 1943/001.* Het onbeperkt toegangsrecht voorzien in het 2e lid is de overname van art. 36*ter*/11 WVP.

De tweede paragraaf voorziet voor het Controleorgaan en haar leden de bevoegdheid in de lokalen alle voorwerpen, documenten en gegevens van een informaticasysteem die nuttig zijn voor hun onderzoek in beslag nemen, behalve indien ze betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek. Dit is nieuw en een noodzakelijke bevoegdheid voor elke toezichtautoriteit en was ook voorzien in het *Wetsvoorstel n° DOC 54, 1943/001*, meer bepaald het ontworpen art. 8, 3°. De beslagbevoegdheid is uitgesloten wanneer het beslag betrekking heeft op een lopend vooronderzoek in strafzaken. Ook in de wet van 3 december 2017 wordt een gelijkaardige bevoegdheid voor de inspectiedienst voorzien in het artikel 66 § 1, 5°, tot en met ten 8°, en de artikelen 89 en 90. Tegen de beslagbevoegdheid kan de politiechef zich wel verzetten waarna de zaak wordt voorgelegd aan de Voorzitter van het Controleorgaan die als magistraat het ook gewoon is dergelijk beslissingen te nemen en belangenafwegingen te maken. Ook deze tussenkomst van de Voorzitter was voorzien in voormeld *Wetsvoorstel n° DOC 54, 1943/001* (art. 8) en was op zijn beurt geïnspireerd op een gelijkaardige bevoegdheid voor de Voorzitter van de Comités P en I (cf. art. 24 § 2, 4e lid, art. 27, art. 48 § 2, 4e lid en art. 51 van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse).

De paragrafen 3 en 4 voorzien de vaststellingsbevoegdheid van de leden, de mogelijkheid de openbare macht te vorderen en het opleggen van dwingende antwoordtermijnen. Deze bevoegdheden zijn enerzijds reeds gedeeltelijk voorzien in art. 36*ter*/11 WVP en anderzijds overgenomen van het *Wetsvoorstel n° DOC 54, 1943/001* (art. 8).

Het uitoefenen van het toezichtstaken door het Controleorgaan kan de toegang noodzaken tot bepaalde gegevens van het Rijksregister. Het betreft in het bijzonder: de naam en voornamen, de geboorteplaats en -datum, het geslacht, de nationaliteit, de hoofdverblijfplaats, de plaats en datum van het overlijden, de samenstelling van het gezin en tenslotte de akten en beslissingen

personnel qui sont traitées et à toutes les informations nécessaires à l'exercice de ses missions".

Le paragraphe premier du présent article est repris partiellement de l'article 36*ter*/11 LVP de sorte que le droit illimité d'accès concerne également les banques de données qui sont alimentées par les services de police belges. Cette clarification a aussi déjà été proposée à l'art. 8 de la *Proposition de loi n° DOC 54, 1943/001.* Le droit d'accès illimité prévu au 2e alinéa est repris de l'art. 36*ter*/11 LVP.

Le paragraphe 2 prévoit pour l'Organe de contrôle et ses membres la compétence de confisquer dans les locaux tous les objets, documents et données d'un système informatique utiles pour leur enquête, sauf s'ils concernent une information ou instruction judiciaire en cours. Ceci est nouveau et c'est une compétence nécessaire pour toute autorité de contrôle et c'était aussi prévu dans la *Proposition de loi n° DOC 54, 1943/001,* plus particulièrement l'art. 8, 3°, en projet. La compétence en matière de saisie est exclue lorsque la saisie concerne une information ou instruction judiciaire en cours en matière pénale. Dans la loi du 3 décembre 2017 est également prévue une compétence similaire pour le service inspection visé à l'article 66 § 1er, 5° et 8°, inclus et les articles 89 et 90. Le chef de la police peut s'opposer à la compétence en matière de saisie, à la suite de quoi l'affaire est présentée au Président de l'Organe de contrôle qui, en tant que magistrat, est habitué à prendre pareilles décisions et à trancher. Cette intervention du Président était également prévue dans la *Proposition de loi n° DOC 54, 1943/001* précitée (art. 8) et était à son tour inspirée d'une compétence similaire pour le Président des Comités P et R (cf. art. 24 § 2, 4e alinéa, art. 27, art. 48 § 2, 4e alinéa et art. 51 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace).

Les paragraphes 3 et 4 prévoient la compétence de constatation des membres, la possibilité de requérir la force publique et l'imposition de délais de réponse obligatoires. Ces compétences sont d'une part partiellement prévues à l'art. 36*ter*/11 LVP et d'autre part reprises de la *Proposition de loi n° DOC 5554, 1943/001* (art. 8).

L'exercice des tâches de contrôle par l'Organe de contrôle peut nécessiter l'accès à certaines données du registre national. Il s'agit en particulier: des nom et prénoms, des lieu et date de naissance, du sexe, de la nationalité, de la résidence principale, des lieu et date de décès, de la composition de ménage et, enfin, des actes et décisions relatifs à la capacité juridique. Par

betreffende de rechtsbekwaamheid. Met deze bepaling verleent de wetgever aan het Controleorgaan de toegang tot deze gegevens alsook de mogelijkheid om het rijksregisternummer te gebruiken. Dit wordt bepaald in de vijfde paragraaf.

Art. 245

Dit artikel voorziet de bevoegdheid tot verhoren, de mogelijkheid voor de leden van de politiediensten om verklaringen af te leggen betreffende feiten gedekt door het beroepsgeheim en de verplichting te spreken ten aanzien van het Controleorgaan, behoudens indien de feiten betrekking hebben op een lopend vooronderzoek in strafzaken. Opnieuw wordt aan de Voorzitter van het Controleorgaan een beslissingsbevoegdheid gegeven wanneer de politieambtenaar/lid van het administratief en logistiek kader meent de geheimen te moeten bewaren omdat een persoon door de bekendmaking ervan fysiek gevaar zou kunnen lopen. Daarnaast is er de mogelijkheid voor het C.O.C. om de leden van de politiediensten te dagvaarden en hun de eed op te dragen en tot slot een regeling voor het opstellen van processen-verbaal gepaard gaande met strafsancties voor de weigering om te getuigen.

Ook deze bevoegdheden zijn voorzien in het voormeld *Wetsvoorstel n° DOC 54, 1943/001* (art. 9) en zijn volledig geïnspireerd en/of overgenomen van de artikelen 24 tot en met 27*bis* van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse voor wat het Vast Comité P betreft.

Art. 246

Dit artikel voorziet de verplichting voor alle diensten van de Staat, met inbegrip van de parketten en de griffies van de hoven en van alle rechtscolleges, de provincies, de gemeenten, de verenigingen waartoe zij behoren, de overheidsinstellingen die ervan afhangen, aan het Controleorgaan, op haar verzoek, alle inlichtingen te geven die laatstgenoemde nuttig achten voor het toezicht op de naleving van de wetgeving waarmee zij belast zijn, alsmede gelijk welke informatiedragers ter inzage voor te leggen en kopieën ervan te verstrekken onder gelijk welke vorm. Indien deze inlichtingen deel uitmaken van een lopend strafrechtelijk vooronderzoek is de goedkeuring nodig van het bevoegde openbaar ministerie.

Deze bepaling werd overgenomen uit de wet van 3 december 2017 (art. 68) en is ook terug te vinden in tal van andere wetgevingen (bijv. art. 44/11/9 § 4 WPA,

cette disposition, le législateur octroie à l'Organe de contrôle accès à ces données ainsi que la possibilité d'utiliser le numéro de registre national. Ceci est mentionné dans le paragraphe 5.

Art. 245

Cet article prévoit la compétence d'audition, la possibilité pour les membres des services de police de faire des déclarations concernant des faits couverts par le secret professionnel et l'obligation de s'exprimer face à l'Organe de contrôle sauf si les faits concernent une enquête pénale en cours. A nouveau, une compétence de décision est donnée au Président de l'Organe de contrôle lorsque le fonctionnaire de police/membre du cadre administratif et logistique pense devoir garder les secrets dont il est dépositaire parce que par sa publication une personne pourrait être physiquement en danger. Ensuite, il est possible pour le C.O.C. de citer les membres des services de police et de déférer le serment et enfin un règlement pour la rédaction des procès-verbaux accompagnés de sanctions pénales en cas de refus de témoigner.

Ces compétences sont également prévues dans la *Proposition de loi n° DOC 54, 1943/001* précité (art. 9) et sont entièrement inspirées et/ou reprises des articles 24 à 27*bis* inclus de la Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace pour ce qui concerne le Comité Permanent P.

Art. 246

Cet article prévoit l'obligation pour tous les services de l'État, y compris les parquets et les greffes des cours et de toutes les juridictions, les provinces, les communes, les associations dont elles font partie, les institutions publiques qui en dépendent de fournir à l'Organe de contrôle, à sa demande, tous renseignements que ces derniers estiment utiles au contrôle du respect des législations dont ils sont chargés, ainsi que de leur produire, pour en prendre connaissance, tous supports d'information et de leur en fournir des copies sous quelque forme que ce soit. Si ces informations font partie d'une instruction pénale en cours, l'autorisation du ministère public compétent est requise.

Cette disposition est reprise de la loi du 3 décembre 2017 (art. 68) et ainsi que dans bon nombre d'autres législations (par exemple art. 44/11/9 § 4 LFP, art. 14 de

art. 14 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, enz …).

Artt 247 en 248

De beide artikelen zijn de omzetting van de corrigerende bevoegdheden waarover de toezichthoudende autoriteit dient te beschikken zoals voorzien door artikel 47.2 van de Richtlijn. Dit werd terecht opgemerkt door de Privacycommissie in haar advies 33/2018 (cf. n° 456, p. 122 *in fine*) waarbij de analogie werd nagestreefd met artikel 270 (cf. artikel 51/3 van de wet van 18 juli 1991).

Art. 249

Dit artikel somt enkele statutaire bevoegdheden op die reeds lang bij het Controleorgaan zitten en zijn de overname van artikel 36*ter*/12 WVP.

Art. 250

Artikel 52.4 van de Verordening en artikel 42.4 van de Richtlijn voorzien erin dat de autoriteiten van elke lidstaat "*over de [...] technische en financiële middelen moeten beschikken*". Artikel 52.6 van de Verordening en art. 42.6 van de Richtlijn voorzien er verder in dat elke lidstaat financieel toezicht uitoefent of laat uitoefenen zonder dat daarbij de onafhankelijkheid van de gegevensbeschermingsautoriteit in het gedrang komt.

Dit artikel van deze wet voorziet erin dat het Controleorgaan een jaarbegroting krijgt die wordt uitgetrokken als dotatie op de algemene begroting van het Rijk.

De begroting moet worden goedgekeurd door de Kamer van volksvertegenwoordigers en de uitvoering van de begroting kan worden gecontroleerd door de Kamer van volksvertegenwoordigers, bijgestaan door het Rekenhof. Om de werkzaamheden van goedkeuring en toezicht op de uitvoering van de begroting door de Kamer van volksvertegenwoordigers te vergemakkelijken, voegt het Controleorgaan aan haar voorstel van jaarbegroting een strategisch plan toe.

la Loi organique du 30 novembres 1998 des services de renseignement et de sécurité, etc).

Art. 247 et 248

Les deux articles représentent la transposition des compétences correctrices que l'autorité de contrôle doit avoir sur base de l'article 47.2 de la Directive. Cette remarque a été soulevé à juste titre par la Commission vie privée dans son avis 33/2018 (cf. n° 456, p. 122 *in fine*) qui visait l'analogie avec l'article 270 (cf. l'article 51/3 de la loi du 18 juillet 1991).

Art. 249

Cet article énumère quelques compétences statutaires qui sont depuis longtemps à l'Organe de contrôle et sont la reprise de l'article 36*ter*/12 LVP.

Art. 250

L'article 52.4 du Règlement et l'article 42.4 de la Directive disposent que les autorités de chaque État membre doivent disposer des "*ressources (…) techniques et financières*". L'article 52.6 du Règlement et l'article 42.6 de la Directive disposent en outre que chaque État membre effectue ou fasse effectuer un contrôle financier qui ne menace pas l'indépendance de l'autorité de protection des données.

Cet article de la présente loi prévoit que l'Organe de contrôle reçoit un budget annuel inscrit à titre de dotation au budget général de l'État.

Le budget doit être approuvé par la Chambre des représentants et l'exécution du budget peut être contrôlé par la Chambre de représentants, assistée par la Cour des comptes. Afin de faciliter le travail d'approbation et de contrôle d'exécution du budget par la Chambre des représentants, l'Organe de contrôle joint à sa proposition de budget annuel un plan stratégique.

TITEL 8

Slotbepalingen

Art. 251

De bescherming van de persoonsgegevens is een transversale materie geregeld in deze wet, maar kan ook geregeld worden in sectorale bepalingen voor een efficiente en bijzondere bescherming eigen aan elke situatie. Het kan dus gebeuren dat er wetten genomen worden die tegelijk van toepassing zijn op dezelfde verwerking van persoonsgegevens zonder echter verenigbaar te zijn. Zo een situatie kan negatieve gevolgen hebben en we moeten duidelijk zijn over welke wetgeving van toepassing is. Daarom is het opportuun in deze wet te voorzien in een regel betreffende wetsconflicten. De voorgestelde regel bepaalt dat in geval dat verschillende wetgevingen tegelijkertijd van toepassing zijn, en in geval van conflict tussen deze wetgevingen, de regels van deze wet primeren. Hoewel men kon hebben bepaald dat de regel die van toepassing is in geval van conflict, de meest strikte regel is (de meest strikte beschermingsregel, aangezien dit de persoonlijke levenssfeer betreft), werd geopteerd voor een duidelijke keuze, om te voorkomen dat er nieuwe vragen rijzen. Immers, in haar adviezen nr. 42/2013 en 01/2015 stelt de Privacycommissie dat de bepaling dat de meest strikte regeling wordt toegepast het niet mogelijk maakt duidelijk te zien welke wetgeving de meest strikte regels zou bevatten.

Art. 252

Er wordt tevens voorzien in een algemene delegatiebepaling aan de Koning teneinde deze wet uit te voeren.

HOOFDSTUK I

Wijzigingsbepalingen

Art. 253

Het eerste lid is een generieke bepaling die het mogelijk maakt om de verwijzing naar de WVP in alle huidige reglementeringen die ernaar verwijzen, te wijzigen.

Het tweede lid geeft aan de Koning een delegatie om in de wetten of andere reglementering elke verwijzing naar artikelen van de WVP te veranderen teneinde ze aan te kunnen passen aan bepalingen van de huidige wet of van de Verordening die ermee overeenkomen. Het betreft enkel een bevoegdheid tot legistiek-technische aanpassing.

TITRE 8

Dispositions finales

Art. 251

La protection des données à caractère personnel est une matière transversale réglée dans la présente loi mais qui également être réglée dans des dispositions sectorielles pour une protection efficace et particulière propre à chaque situation. Il peut donc advenir que des législations soient prises, lesquelles s'appliquent simultanément au même traitement de données à caractère personnel sans toutefois être compatibles. Une telle situation pourrait engendrer des effets pervers et il y a lieu d'être clair quant à savoir quelle législation sera d'application. C'est pourquoi il est opportun de prévoir dans la présente loi une règle de conflit de lois. La règle proposée prévoit qu'au cas où différentes législations s'appliquent de manière simultanée et qu'en cas de conflit entre celles-ci, les règles de la présente loi prévalent. Si l'on pouvait être tenté de prévoir que la règle applicable en cas de conflit soit la règle la plus stricte (règle de la protection la plus stricte, étant donné que l'on touche à la vie privée), il a été opté pour un choix clair, afin d'éviter de susciter de nouvelles questions. En effet, dans ses avis n° 42/2013 et 01/2015, la Commission vie privée affirme que prévoir l'application du régime le plus strict ne permet pas de voir clairement quelle législation comporterait les règles plus strictes.

Art. 252

Il est également prévu une disposition générale de délégation au Roi aux fins d'exécuter la présente loi.

CHAPITRE I^ER

Dispositions modificatives

Art. 253

L'alinéa premier est une disposition générique qui permet de modifier la référence à la LVP dans toute la réglementation actuelle qui y fait référence.

L'alinéa 2 donne une délégation au Roi pour modifier dans les lois ou autres réglementations toute référence à des articles de la LVP afin de les pouvoir adapter à des dispositions correspondantes dans la présente loi ou dans le Règlement. Il s'agit uniquement d'un pouvoir d'adaption légistique-technique.

Art. 254

De Verordening, net zoals de Richtlijn, laten de lidstaten toe om meerdere toezichthoudende autoriteiten op te richten. In dat geval dient de lidstaat de toezichthoudende autoriteit te benoemen die zal zetelen in het Europees comité voor gegevensbescherming waarin de toezichthoudende autoriteiten van elke lidstaat van de Europese Unie verzameld zijn. Er wordt voor gekozen om de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 te benoemen. Een samenwerkingsakkoord tussen de verschillende toezichthoudende autoriteiten zal de samenwerkings- en vertegenwoordigingskwesties moeten regelen voor de gevallen waarin binnen het Comité zaken worden besproken die tot de bevoegdheid behoren van een andere toezichthoudende autoriteit dan de GBA.

Art. 255 en 256

De artikelen 263 en 264 betreffen enkel technische correcties.

Art. 257

Dit artikel omschrijft wat men moet verstaan onder “gegevensbeschermingswet” en “gegevensbeschermingsautoriteit”.

Art. 258

De uitoefening van taak van gegevensbeschermingsautoriteit verreist een aantal vaardigheden zodat het opportuun is om de toegangsvoorwaarden aan te passen.

Art. 259

Dit is een vervollediging om een juiste verwijzing tot stand te brengen.

Art. 260

Artikel 268 past artikel 31 in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse aan om deze conform te maken aan de wijziging van de opdrachten van de Veiligheid van de Staat.

Art. 254

Le Règlement, tout comme la Directive, permettent aux États membres de mettre en place plusieurs autorités de protection des données. Dans un tel cas, l’État membre doit désigner quelle sera l’autorité de contrôle qui siègera au sein du Comité européen de la protection des données qui réunit les autorités de protection des données de chaque État membre de l’Union européenne. Il est opté de désigner l’Autorité de protection des données visée dans la loi du 3 décembre 2017. Un protocole de coopération entre les différentes autorités de contrôle devra régler les questions de coopération et représentation pour les cas où les matières discutées au sein du Comité relevent de la compétence particulière d’une autre autorité de contrôle que l’APD.

Art. 255 et 256

Les articles 263 et 264 ne portent que sur des corrections techniques.

Art. 257

Cet article définit ce que l’on entend par “la loi protection des données” et “une autorité de protection des données”.

Art. 258

L’exécution de la fonction d’autorité de protection des données demande un certain nombre de compétences, dès lors il est opportun d’adapter les conditions d’accès.

Art. 259

Ceci est un ajout afin d’effectuer une référence correcte.

Art. 260

L’article 268 adapte l’article 31 dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l’Organe de coordination pour l’analyse de la menace pour le rendre conforme à la modification des missions de la Sûreté de l’État.

Art. 261

Dit artikel voorziet dat het Comité I ook kan handelen op vraag van een andere gegevensbeschermingsautoriteit.

Dit sluit onderzoeken over de verwerking van persoongegevens uit van het toepassingsgebied van het tweede lid dat voorziet in een verplichting in hoofde van het hoofd van het Comité I om de Kamer van volksvertegenwoordigers meteen te informeren als het uit eigen initiatief optreedt. Dit wordt gerechtvaardigd door het feit dat er in elk geval een verplichting bestaat om een rapport voor de Kamer van volksvertegenwoordiger op te maken over ieder onderzoek in uitvoering van artikel 33 van de wet van 18 juli 1991.

Art. 262

Via dit artikel wordt een onderzoeksbevoegdheid aan het Vast Comité I toegekend inzake de verwerking van persoonsgegevens.

Art. 263

Via dit artikel wordt een bevoegdheid aan het Vast Comité I toegekend met betrekking tot verzoeken inzake de verwerking van persoonsgegevens.

Om te verhinderen dat misbruik wordt gemaakt aan de hand van een verzoek om na te gaan of een inlichtingendienst al dan niet een onderzoek over hem heeft lopen, wordt enkel aan de indiener gemeld dat men het onderzoek met betrekking tot de bescherming van de persoonsgegevens gevoerd heeft.

Art. 264

Dit artikel legt een jaarlijkse verslagplicht op in het kader van het toezicht op de verwerkingen van persoonsgegevens ten opzichte van de Kamer van volksvertegenwoordigers.

Art. 265

Dit artikel voert een technische correctie door.

Art. 261

Cet article prévoit que le Comité R peut également agir à la demande d'une autre autorité de protection des données.

Il exclut les enquêtes portant sur les traitements de données à caractère personnel du champ d'application de l'alinéa 2 qui prévoit une obligation dans le chef du Comité R d'informer aussitôt la Chambre des représentants lorsqu'il agit d'initiative. Cela se justifie par le fait qu'il a de toute façon l'obligation de faire un rapport à la Chambre des représentants relatif à chaque enquête en application de l'article 33 de la loi du 18 juillet 1991.

Art. 262

Par cet article une compétence d'enquête est octroyée au Comité permanent R concernant le traitement des données à caractère personnel.

Art. 263

Par cet article une compétence est octroyée au Comité permanent R pour les requêtes sur le traitement des données à caractère personnel.

Afin d'éviter l'abus par le biais d'une requête et de vérifier si une enquête est en cours ou non par un service de renseignement, le requérant ne sera informé que sur le fait qu'une enquête sur la protection des dossiers a été réalisée.

Art. 264

Cet article impose une obligation de rapportage annuel dans le cadre des traitements des données à caractère personnel vis-à-vis de la Chambre des représentants.

Art. 265

Cet article apporte une correction technique.

Art. 266 en 267

Door de invoering van extra bevoegdheden aan het Comité I moet ook de bevoegdheid van de Dienst Enquêtes aangepast worden.

Art. 268

Dit artikel is een vervollediging om een juiste verwijzing tot stand te brengen.

Art. 269

Artikel 46 van de wet van 18 juli 1991 voorziet een verplichting voor een lid van de Dienst Enquête om de bevoegde Procureur des Konings te informeren als hij kennis krijgt van een misdaad of wanbedrijf.

Dit artikel heeft tot doel om het toepassinggebied van deze verplichting van wanbedrijven en misdaden voor dewelke de agenten vrijsgeteld zijn van straf in toepassing van artikel 13/1 van de wet van 30 november 1998 houdende regelening van de inlinchtignediensten.

De inbreuken voorzien in de artikelen 226 en 227 van deze wet zijn eveneens uitgesloten omdat het aan het Comité I toekomt, en niet aan de Dienst Enquêtes, om te beslissien om het dossier aan het parket over te maken in toepassing van het artikel 51/3 van de wet van 18 juli 1991.

Art. 270

Dit artikel betreft de oprichting van een nieuwe afdeling in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse om de leesbaarheid te verhogen.

Art. 271

Dit artikel voegt vier artikelen in in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse om de procedure in te stellen om de functie van gegevensbeschermingsautoriteit uit te oefenen.

Art. 266 et 267

En insérant des compétences complémentaires pour le Comité R, la compétence du Service d'Enquêtes doit être adaptée.

Art. 268

Cet article est un ajout afin d'effectuer une référence correcte.

Art. 269

L'article 46 de la loi du 18 juillet 1991 prévoit l'obligation pour un membre du Service d'Enquête d'informer sur le champ le Procureur du Roi s'il prend connaissance d'un crime ou d'un délit.

Cet article a pour but d'exclure du champ de cette obligation les délits et crimes pour lesquels les agents ont été exemptés de peine en application de l'article 13/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les infractions prévues aux articles 226 et 227 de la présente loi sont également exclues car il appartient au Comité R, et non à son Service d'Enquête, de décider de transmettre le dossier au Parquet en application de l'article 51/3 de la loi du 18 juillet 1991.

Art. 270

Cet article concerne la création d'un nouveau chapitre dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace afin d'augmenter la lisibilité.

Art. 271

Cet article insère quatre articles dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace pour introduire une procédure pour exercer la fonction d'autorité de protection des données.

Art. 272

Dit artikel omvat een aanpassing die wordt ingeschreven in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit ingevolge het advies van de Privacycommissie (punt 456). Enkel de Gegevensbeschermingsautoriteit zal als toezichthoudende autoriteit bevoegd zijn het uitoefenen van de controlebevoegdheden in kader van de Verordening, tenzij een wet anders bepaalt.

Art. 273

Als antwoord op het advies van de Privacycommissie (punt 408) wordt een bepaling toegevoegd die bepaalt dat het directiecomité van de Gegevensbeschermingsautoriteit bevoegd is om de beslissing te nemen om in rechte op te treden.

Art. 274

Aangezien België ervoor opteert om te werken met meerdere toezichthoudende autoriteiten kunnen er zich gevallen voordoen waarbij klachten, adviezen of aanbevelingen moeten behandeld worden die raken aan de bevoegdheden van meerdere toezichthoudende autoriteiten. In een landschap van overlappende bevoegdheden is het des te meer van belang dat er waarborgen bestaan voor een coherente en consequente toepassing van de toepasselijke privacyregels. Dit is in de eerste plaats in het belang van de burger, opdat die zich niet tot meerdere instellingen zou hoeven te richten, maar evenzeer voor de overheidsinstanties en de privésector opdat zij zouden kunnen rekenen op duidelijke en eenvormige beslissingen en adviezen. Bovendien moeten we rekening houden met de inwerkingtreding van het onestopshop systeem of het coherentiemechanisme op Europees niveau waarbij de transnationale behandeling van een dossier een duidelijk en gecoördineerd aanspreekpunt voor Europa kan vereisen. Hetzelfde geldt voor de toepassing van de bepalingen in de Verordening en de Richtlijn inzake wederzijdse bijstand en gezamenlijke werkzaamheden tussen nationale toezichthoudende autoriteiten.

Daarom wordt in de wet van 3 december 2017 tot oprichting van de gegevensbeschermingsautoriteit, in het deel over de nationale samenwerking, een artikel 54/1 ingevoegd dat de verplichting tot samenwerking bij gedeelde bevoegdheden verankert.

Bovendien wordt bij wet bepaald dat de Gegevensbeschermingsautoriteit als één-loket zal optreden voor de gezamenlijke behandeling van klachten, adviezen en

Art. 272

Cet article contient une clarification qui doit être inscrit dans la loi du 3/12/2017 portant création de l'Autorité de protection des données suite à l'avis de la Commission vie privée (point 456). Seule l'Autorité de protection des données sera compétente en tant qu'autorité de contrôle pour effectuer les compétences de contrôle dans le cadre du Règlement, à moins qu'une loi en dispose autrement.

Art. 273

En réponse à l'avis de la Commission vie privée (point 408) il est inséré une disposition qui précise que le comité de direction de l'Autorité de protection des données est compétent pour prendre la décision d'agir en droit.

Art. 274

Étant donné que la Belgique a choisi de travailler avec plusieurs autorités de contrôle, il peut y avoir des situations où des plaintes, des avis ou des recommandations sont traitées et qui ont un impact sur les pouvoirs de plusieurs autorités de contrôle. Dans un paysage de compétences qui se chevauchent, il est d'autant plus important de prévoir des garanties pour une application cohérente et conséquente des principes en matière de protection des données. Il en va, en premier lieu, de l'intérêt des citoyens, de sorte que ces derniers ne doivent pas s'adresser à plusieurs institutions, mais c'est également dans l'intérêt des autorités publiques et du secteur privé afin qu'ils puissent compter sur des décisions ou des avis clairs et uniformes. De plus, nous devons tenir compte de l'introduction du système de guichet unique ("one stop shop") ou le mécanisme de contrôle de la cohérence au niveau européen, dans lequel un traitement transnational d'un dossier peut nécessiter un point de contact pour l'Europe clair et coordonné. Il en va de même pour l'application des dispositions du Règlement et de la directive sur l'assistance mutuelle et la coopération entre les autorités de contrôle nationales.

En conséquence, il est inséré un article 54/1 dans la section sur la coopération nationale de la loi du 3 décembre 2017 instituant l'Autorité de protection des données, lequel établit l'obligation de coopérer lorsqu'il s'agit de compétences partagées.

En outre, la loi stipule que l'Autorité de protection des données agira comme un guichet unique pour le traitement conjoint des plaintes, avis et recommandations

aanbevelingen wanneer er sprake is van overlappende bevoegdheden. De Gegevensbeschermingsautoriteit treedt daarbij niet alleen op als ingangspoort, voor zover de klacht of vraag tot advies rechtstreeks aan de Gegevensbeschermingsautoriteit wordt gesteld, maar ook als enige uitgangspoort in de communicatie naar de klager of aanvrager toe. Dit neemt uiteraard niet weg dat de klager of aanvrager zich tot eender welke toezichthoudende autoriteit mag richten. Doch, de verdere communicatie met de klager of aanvrager zal gebeuren door de Gegevensbeschermingsautoriteit.

De modaliteiten van deze samenwerking dienen te worden vastgelegd in een samenwerkingsprotocol.

HOOFDSTUK II

Opheffings bepalingen

Art. 275

De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, gewijzigd bij de wet van 11 december 1998, het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het koninklijk besluit van 17 december 2003 tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van bepaalde sectorale comités opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer, worden opgeheven.

In het laatste lid wordt het systeem van rechtstreekse en onrechtstreekse toegang voor de betrokkenen tot hun gegevens voorzien in artikel 15 van de PNR-wet afgeschaft. Dit systeem paste niet bij het vertrouwelijk karakter van de verwerkte gegevens. Het binaire karakter van het systeem zou namelijk een passagier, in functie van de entiteit bij wie hij de toegang tot zijn gegevens zou kunnen uitoefenen, in staat hebben kunnen stellen te weten of zijn gegevens een positieve overeenstemming hadden opgeleverd of het resultaat vormden van een gerichte opzoeking en dus te weten of hij al dan niet door de bevoegde diensten werd onderzocht. Door het afschaffen van voormeld systeem zijn de bepalingen in de wet betreffende de bescherming met betrekking tot persoonsgegevens, die een rechtstreekse of onrechtstreekse toegang voorzien in functie van de toepasselijke Titel van huidige wet, van toepassing. Deze laat eveneens toe om te beantwoorden aan punt

lorsqu'il y a chevauchement des pouvoirs. L'Autorité de protection des données agit non seulement comme porte d'entrée, dans la mesure où la plainte ou la demande d'avis est adressée directement à l'Autorité de protection des données, mais aussi comme seul point de sortie dans la communication au plaignant ou au demandeur. Bien entendu, cela ne change rien au fait que le plaignant ou demandeur peut s'adresser à une autre autorité de contrôle. Cependant, d'autres communications avec le plaignant ou demandeur seront effectuées par l'Autorité de protection des données.

Les modalités de cette coopération doivent être définies dans un protocole de coopération.

CHAPITRE II

Dispositions abrogatoires

Art. 275

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, modifiée par la loi du 11 décembre 1998, l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et l'arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée sont abrogés.

Dans le dernier alinéa le système d'accès direct et indirect des personnes concernées à leurs données prévu par l'article 15 de la loi PNR est supprimé. En effet, ce système ne convenait pas à la nature confidentielle des données traitées, et souffre d'une faille. Le caractère binaire de ce système aurait pu permettre à un passager de savoir, en fonction de l'entité auprès de laquelle il aurait pu exercer l'accès à ses données, si celles-ci ont fait l'objet d'une correspondance positive ou d'une recherche ponctuelle, et ainsi savoir s'il était recherché ou suivi par les services compétents. Le système susmentionné ainsi supprimé, ce sont les dispositions présentes dans la loi relative à la protection à l'égard des données à caractère personnel qui s'appliquent et qui prévoient un accès direct ou indirect en fonction du Titre de la présente loi qui s'applique. Cela permet également de répondre au point 247 de l'avis de la Commission vie privée qui s'interroge sur

247 van het advies van de Privacycommissie, die zich afvraagt of zulk systeem conform is met de bepalingen van huidige wet.

HOOFDSTUK III

Inwerkingtreding en overgangsbepalingen

Art. 276

De omzettingstermijn van de Richtlijn verstrijkt op 6 mei 2018 terwijl de Verordening van directe toepassing is vanaf 25 mei 2018. Gelet op deze termijnen en de directe toepassing van de Verordening is het absoluut noodzakelijk dat de wet in werking treedt op een datum zo dicht mogelijk bij 25 mei met het risico dat sommige bepalingen van toepassing zouden zijn en andere, daarbij aansluitende bepalingen, nog niet, hetgeen schadelijk zou zijn voor de juridische zekerheid. Om deze reden wordt ervoor gekozen om deze wet in werking te laten treden dop de dag van publicatie in het *Belgisch Staatsblad*.

Het tweede lid voorziet in een afwijkende bepaling voor het aannemen van de protocollen bedoeld in artikel 20. Immers, de toepassing van dit artikel vanaf de inwerkingtreding van deze wet zou betekenen dat overheidsdiensten die nog niet over een protocol zouden beschikken voor nieuwe verwerkingen die plaatsvinden onmiddellijk na de inwerkingtreding, deze wet zouden schenden. Teneinde de overheidsdiensten toe te laten een protocol aan te nemen voor deze nieuwe verwerkingen wordt in een redelijke termijn voorzien om zich in orde te stellen.

Art. 277

Met deze bepaling wordt voorzien dat de gegevensverwerkingen die vóór de inwerkingtreding van dit wetsontwerp en vóór de toepassing van de Verordening zijn uitgevoerd, geldig blijven en niet in twijfel worden getrokken. Er is dus geen terugwerkende kracht. Het is evenwel vereist dat alle nieuwe gegevensverwerkingen in overeenstemming worden gebracht met de nieuwe regelgeving.

Art. 278

De Verordening en de Richtlijn bepalen dat internationale overeenkomsten die vóór 25 mei 2016 of 6 mei 2016 zijn gesloten, worden gehandhaafd totdat ze worden gewijzigd, vervangen of ingetrokken.

la conformité d'un tel système avec les dispositions de la présente loi.

CHAPITRE III

Entrée en vigueur et dispositions transitoires

Art. 276

Le délai de transposition de la Directive est fixé au 6 mai 2018 tandis que le Règlement est applicable directement dès le 25 mai 2018. Vu ces délais, et l'application directe du Règlement, il est impératif que la loi entre en vigueur à une date la plus proche possible du 25 mai au risque de voir certaines dispositions applicables et d'autres dispositions liées non encore applicables, ce qui nuit à la sécurité juridique. Pour cette raison il est choisi de faire entrer en vigueur la présente loi le jour de sa publication au *Moniteur belge*.

L'alinéa 2 prévoit une disposition dérogatoire pour l'adoption des protocoles visés dans l'article 20. En effet, l'application de cet article dès l'entrée en vigueur de la présente loi impliquerait que les administrations publiques qui ne disposeraient pas de protocole pour de nouveaux traitements réalisés directement après l'entrée en vigueur, seraient en violation de la présente loi. Afin de permettre aux administrations publiques d'adopter le protocole pour ces nouveaux traitements, il est prévu un délai raisonable pour se mettre en conformité.

Art. 277

Il est prévu avec cette disposition que les traitements effectués avant l'entrée en vigueur de ce projet de loi et avant l'application du Règlement restent valables et ne sont pas remis en cause. Il n'y a donc pas d'effet rétroactif. Toutefois il est bien entendu requis que tous les nouveaux traitements soient mis en conformité avec la nouvelle règlementation.

Art. 278

Le Règlement et la Directive prévoient que les accords internationaux qui auraient été conclus respectivement avant le 25 mai 2016 ou le 6 mai 2016, sont maintenus jusqu'à ce que ceux-ci soient modifiés,

Vanaf deze data moeten alle internationale overeenkomsten voldoen aan de nieuwe regelgeving inzake gegevensbescherming.

Art. 279

Op grond van artikel 63 van de Richtlijn kan een lidstaat uitzonderlijk bepalen dat de geautomatiseerde verwerkingssystemen die zijn opgezet vóór 6 mei 2016, en voor zover dat buitensporige inspanningen vereist, uiterlijk op 6 mei 2023 met artikel 25, eerste paragraaf, in overeenstemming moeten worden gebracht, niet later dan 6 mei 2023. Wat de politiediensten en de rechterlijke orde echter betreft, wordt gewerkt aan de modernisering van het informaticasysteem. Aanzienlijke inspanningen zullen worden gedaan om ervoor te zorgen dat deze vereiste voor logbestanden als bedoeld in artikel 25 van de Richtlijn en omgezet in artikel 56 van deze wet vanaf 2023 van kracht kan zijn.

Art. 280

Dit artikel bevat de overgangsbepaling voor de leden van het Controleorgaan die benoemd werden onder gelding van de WVP voor een mandaat van zes jaar. De leden die, op het moment van de inwerkingtreding van deze wet, nog steeds lid zijn van het Controleorgaan zullen dus hun mandaat van rechtswege verder zetten, zodat alle nieuwe mandaten van het Controleorgaan (zowel lid van het Controleorgaan als lid van de dienst onderzoeken), met toepassing van de bepalingen van deze wet, slechts op 1 september 2021 zullen open vallen. Het is verkieselijk dat alle mandaten worden hernieuwd op 1 september 2021 ongeacht de datum waarop de huidige leden hun mandaat hebben aangevangen.

Bijkomend zijn ook de statutaire bepalingen voorzien in de artikelen 246 en 247 van deze wet onmiddellijk van toepassing vanaf de inwerkingtreding van deze wet teneinde (1) de noodzakelijk rechtszekerheid voor de leden van het Controleorgaan en de leden van de dienst onderzoeken te creëren op dat moment, (2) gezien het nieuwe en veel uitgebreidere takenpakket met de bijgaande verantwoordelijkheid dat hen wacht, (3) de noodzaak aan continuïteit voor de huidige leden die nog maar twee jaar van hun mandaat hebben voleindigd en de doelstelling de net opgebouwde expertise niet verloren te laten gaan en (4) om een einde te maken aan de huidige statutaire onzekerheid, ongelijkheid en verscheidenheid binnen het Controleorgaan zodat het een efficiënte doorstart kan nemen. De paragrafen 2, 3 en 4 bevatten de concrete overgang van de actuele

remplacés ou révoqués. A partir de ces dates, tous les accords internationaux doivent se conformer à la nouvelle réglementation en matière de protection des données.

Art. 279

L'article 63 de la Directive permet qu'un État membre puisse prévoir que, à titre exceptionnel, lorsque cela exige des efforts disproportionnés, les systèmes de traitement automatisé installés avant le 6 mai 2016 soient mis en conformité avec l'article 25, paragraphe premier, au plus tard le 6 mai 2023. Pour les services de police et l'ordre judiciaire, le système informatique est en cours de modernisation. Des efforts substantiels vont être mis en œuvre afin que cette obligation des fichiers de journalisations prévue à l'article 25 de la Directive transposé à l'article 56 dans la présente loi puisse être effective dès 2023.

Art. 280

Cet article contient la disposition transitoire pour les membres de l'Organe de contrôle qui sont nommés sous la LVP pour un mandat de 6 ans. Les membres qui, au moment de l'entrée en vigueur de cette loi, sont encore toujours membre de l'Organe de contrôle poursuivront donc leur mandat de plein droit, de sorte que tous les nouveaux mandats de l'Organe de contrôle (tant membre le membre de l'Organe de contrôle que membre du service d'enquête), par application des dispositions de cette loi s'ouvriront seulement le 1 septembre 2021. Il est préférable que tous les mandats soient renouvelés le 1 septembre 2021 quelle que soit la date à laquelle les membres actuels ont débuté leur mandat.

Les dispositions statutaires prévues aux articles 246 et 247 de la présente loi sont également immédiatement d'application dès l'entrée en vigueur de cette loi afin de (1) créer la sécurité juridique nécessaire pour les membres de l'Organe de contrôle et les membres du service d'enquête à ce moment, (2) vu les tâches nouvelles et supplémentaires avec la responsabilité y afférente qui les attend, (3) le besoin de continuité pour les membres actuels qui n'ont encore presté que 2 ans de leur mandat et l'objectif de ne pas perdre l'expertise juste créée et (4) mettre fin à l'insécurité statutaire actuelle, inégalité et diversité au sein de l'Organe de contrôle de sorte qu'il puisse repartir du bon pied. Les paragraphes 2, 3 et 4 concernent le transfert concret des membres actuelles de l'Organe de contrôle vers, soit le nouvelle Organe de contrôle, soit le service

leden van het controleorgaan naar hetzij het nieuwe Controleorgaan, hetzij de dienst onderzoeken binnen het nieuwe controleorgaan. Zowel de leden van het Controleorgaan zelf, als de leden van de dienst onderzoeken voldoen daarmee reeds ten volle aan alle algemene en specifieke benoemingsvoorwaarden voorzien door deze wet voor respectievelijk het Controleorgaan zelf dan wel zijn dienst onderzoeken.

Met de vijfde paragraaf wordt een einde gemaakt aan de onduidelijkheid nopens de verloning van het lid van de Commissie voor de bescherming van de persoonlijke levenssfeer en tegelijk wordt voor de overgangsperiode tot 1 september 2021 de mogelijkheid verder gezet om de functie deeltijds uit te oefenen zoals dat voorzien was in art. 36*ter*/2 WVP. Niets belet dat lid evenwel de keuze te maken voor een voltijds ambtsuitoefening. Blijft voormeld lid echter kiezen voor een deeltijds betrekking tot 2021 dan wordt ook het actuele gebrek aan regeling rond de verloning geregeld. Er wordt voorzien in 1/5 van het loon van een voltijds lid wat min of meer overeenkomt met de huidige inzet van voormeld lid in het Controleorgaan.

De minister van Sociale Zaken en Volksgezondheid,

Maggie DE BLOCK

De minister van Justitie,

Koen GEENS

De vice-eersteminister bevoegd voor Binnenlandse Zaken,

Jan JAMBON

De minister van Defensie,

Steven VANDEPUT

De staatssecretaris voor Privacy,

Philippe DE BACKER

d'enquête au sein du nouvelle Organe de contrôle. Tant les membres du nouvelle Organe de contrôle que les membres du service d'enquête répondent déjà maintenant pleinement au conditions générales et spécifiques de nomination prévues dans la présente loi respectivement pour l'Organe de contrôle que pour son service d'enquête.

Dans le cinquième paragraphe il est mis fin au manque de clarté relatif à la rémunération du membre de la Commission vie privée et pour la période de transition jusqu'au 1 septembre 2021, il peut continuer à exercer la fonction à temps partiel comme prévu à l'art. 36*ter*/2 LVP. Rien n'empêche le membre de choisir également d'exercer la fonction à temps plein. Cependant, si le membre précité choisit un emploi à temps partiel jusqu'en 2021, alors l'actuelle absence de règlement concernant sa rémunération est réglée. Est prévu 1/5 du salaire d'un membre à temps plein, ce qui correspond plus ou moins à l'investissement actuel du membre précité dans l'Organe de contrôle.

La ministre des Affaires sociales et de la Santé publique,

Maggie DE BLOCK

Le ministre de la Justice,

Koen GEENS

Le vice-premier ministre chargé de l'Intérieur,

Jan JAMBON

De minister van Defensie,

Steven VANDEPUT

Le secrétaire d'État à la Protection de la vie privée,

Philippe DE BACKER

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

VOORAFGAANDE TITEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Deze wet is van toepassing op elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op elke niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

De Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG, hierna "de Verordening", geldt ook voor de verwerking van persoonsgegevens bedoeld in de artikelen 2.2.a) en 2.2.b) van de Verordening.

De Verordening is niet van toepassing op de verwerkingen bedoeld in de titels 2 en 3 van deze wet.

In afwijking van het tweede lid en onverminderd artikel 107 is deze wet niet van toepassing op:

1. de aanwending van de krijgsmacht, en

2. de paraatstelling met het oog op de aanwending van de krijgsmacht.

Art. 3

Het vrije verkeer van persoonsgegevens in de Europese Unie en op het Belgische grondgebied wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.

In het bijzonder kan de uitwisseling van persoonsgegevens tussen de verwerkingsverantwoordelijken, de bevoegde overheden, de diensten, organen en de ontvangers die zich in de titels 1 tot 3 van deze wet bevinden et die binnen het kader van de doelstellingen bedoeld in artikel 23.1.a) tot h), van de Verordening werken niet worden beperkt noch verboden omwille van dergelijke redenen, onverminderd de bevoegdheden van de bevoegde toezichthoudende autoriteit.

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

TITRE PRELIMINAIRE

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

La présente loi s'applique à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après "le Règlement" s'applique également au traitement de données à caractère personnel visés aux articles 2.2.a) et 2.2.b) du Règlement.

Le Règlement ne s'applique pas aux traitements visés aux titres 2 et 3 de la présente loi.

Par dérogation à l'alinéa 2, et sans préjudice de l'article 107, la présente loi n'est pas applicable à:

1. la mise en œuvre des forces armées, et

2. la mise en condition des forces armées en vue de leur mise en œuvre.

Art. 3

La libre circulation des données à caractère personnel au sein de l'Union européenne et sur le territoire belge n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

En particulier, le partage des données à caractère personnel entre les responsables du traitement, les autorités compétentes, les services, organes et les destinataires, qui se situent dans les titres 1 à 3 de la présente loi et qui travaillent dans le cadre des finalités visées à l'article 23.1.a) à h), du Règlement ne peut être ni limité ni interdit pour de tels motifs, sans préjudice des compétences de l'autorité de contrôle compétente.

Art. 4

§ 1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker op het Belgische grondgebied, ongeacht of de verwerking al dan niet op het Belgische grondgebied plaatsvindt.

§ 2. Deze wet is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich op het Belgische grondgebied bevinden, door een niet in de Europese Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:

a) het aanbieden van goederen of diensten aan deze betrokkenen op het Belgische grondgebied, ongeacht of een betaling door de betrokkenen is vereist; of

b) het monitoren van het gedrag van deze personen, voor zover dit gedrag op het Belgische grondgebied plaatsvindt.

§ 3. Deze wet is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet op het Belgische grondgebied is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het Belgische recht van toepassing is.

Art. 5

Onverminderd de definities bepaald in deze wet, zijn de definities van de Verordening van toepassing.

TITEL 1

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

HOOFDSTUK I

Algemene bepalingen

Art. 6

Met uitzondering van de verwerkingen bedoeld in de titels 2 en 3, en onverminderd bijzondere bepalingen, geeft deze titel uitvoering aan de Verordening.

HOOFDSTUK II

Beginselen van verwerking

Art. 7

Met betrekking tot een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, is de verwerking van de persoonsgegevens van een kind rechtmatig indien

Art. 4

§ 1er. La présente loi s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire belge, que le traitement ait lieu ou non sur le territoire belge.

§ 2. La présente loi s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire belge par un responsable du traitement ou un sous-traitant qui n'est pas établi sur le territoire de l'Union européenne, lorsque les activités de traitement sont liées:

a) à l'offre de biens ou de services à ces personnes concernées sur le territoire belge, qu'un paiement soit exigé ou non desdites personnes; ou

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu sur le territoire belge.

§ 3. La présente loi s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi sur le territoire belge mais dans un lieu où le droit belge s'applique en vertu du droit international public.

Art. 5

Sans préjudice des définitions prévues dans la présente loi, les définitions prévues dans le Règlement s'appliquent.

TITRE 1ER

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel

CHAPITRE IER

Dispositions générales

Art. 6

A l'exception des traitements visés aux titres 2 et 3, et sous réserve de dispositions particulières, le présent titre exécute le Règlement.

CHAPITRE II

Principes de traitement

Art. 7

En ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatif aux enfants est licite lorsque le

de toestemming verleend wordt door kinderen van 13 jaar of ouder.

Wanneer deze verwerking betrekking heeft op de persoonsgegevens van een kind jonger dan 13 jaar, is die slechts rechtmatig indien de toestemming wordt verleend door de wettelijke vertegenwoordiger van dit kind.

Art. 8

In uitvoering van artikel 9.2.g) van de Verordening, worden de hieronder vermelde verwerkingen beschouwd als noodzakelijke verwerkingen om redenen van zwaarwegend algemeen belang:

1. de verwerking door verenigingen met rechtspersoonlijkheid of instellingen van openbaar nut die als hoofddoel de verdediging van de rechten van de mens en van de fundamentele vrijheden hebben, verricht voor de verwezenlijking van dat doel, op voorwaarde dat voor de verwerking een machtiging is verleend door de Koning bij een in Ministerraad overlegd besluit, na advies van de bevoegde toezichthoudende autoriteit. De Koning kan nadere regels bepalen voor die verwerking;

2. de verwerking beheerd door de stichting van openbaar nut "Stichting voor Vermiste en Seksueel Uitgebuite Kinderen" voor de ontvangst, de overzending aan de gerechtelijke overheid en de opvolging van gegevens betreffende personen die ervan verdacht worden in een bepaald dossier van vermissing of seksuele uitbuiting, een misdaad of wanbedrijf te hebben begaan;

3. de verwerking van persoonsgegevens die het seksuele leven betreffen, verricht door een vereniging met rechtspersoonlijkheid of door een instelling van openbaar nut met als statutair hoofddoel de evaluatie, de begeleiding en de behandeling van personen van wie het seksueel gedrag gekwalificeerd kan worden als een misdrijf en die voor de verwezenlijking van dat doel door de bevoegde overheid worden erkend en gesubsidieerd. Voor dergelijke verwerkingen, waarvan de bedoeling moet bestaan in de evaluatie, begeleiding en behandeling van de in deze paragraaf bedoelde personen en de verwerking uitsluitend persoonsgegevens betreft die, wanneer ze het seksueel leven betreffen, enkel betrekking hebben op laatstgenoemde personen, moet door de Koning bij een in een Ministerraad overlegd besluit, na advies van de bevoegde toezichthoudende autoriteit, een bijzondere, individuele machtiging worden verleend.

Het in eerste lid, 3°, bedoelde besluit verduidelijkt de duur van de machtiging, de nadere regels voor de gegevensverwerking, de nadere regels voor de controle van de gemachtigde vereniging of instelling door de bevoegde overheid en de wijze waarop door deze overheid aan de bevoegde toezichthoudende autoriteit verslag moet worden uitgebracht over de verwerking van persoonsgegevens in het kader van de verleende machtiging.

Behoudens bijzondere wettelijke bepalingen is de verwerking van genetische en biometrische gegevens door deze

consentement a été donné par des enfants âgés de 13 ans ou plus.

Lorsque ce traitement porte sur des données à caractère personnel de l'enfant âgé de moins de 13 ans, il n'est licite que si le consentement est donné par le représentant légal de cet enfant.

Art. 8

En exécution de l'article 9.2.g) du Règlement, les traitements ci-après sont considérés comme traitements nécessaires pour des motifs d'intérêt public important:

1. le traitement effectué par des associations dotées de la personnalité juridique ou par des établissements d'utilité publique qui ont pour objet social principal la défense et la promotion des droits de l'homme et des libertés fondamentales, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par le Roi, par arrêté délibéré en Conseil des ministres, après avis de l'autorité de contrôle compétente. Le Roi peut prévoir des modalités de ce traitement;

2. le traitement géré par la fondation d'utilité publique "Fondation pour Enfants Disparus et Sexuellement Exploités" pour la réception, la transmission à l'autorité judiciaire et le suivi de données concernant des personnes qui sont suspectées dans un dossier déterminé de disparition ou d'exploitation sexuelle, d'avoir commis un crime ou un délit;

3. le traitement de données à caractère personnel concernant la vie sexuelle, effectué par une association dotée de la personnalité juridique ou par un établissement d'utilité publique, qui a pour objet statutaire principal l'évaluation, la guidance et le traitement des personnes dont le comportement sexuel peut être qualifié d'infraction, et qui est agréé et subventionné par l'autorité compétente en vue de la réalisation de ce but. Ces traitements, qui doivent être destinés à l'évaluation, la guidance et le traitement des personnes visées dans le présent paragraphe et qui ne peuvent porter que sur des données à caractère personnel qui, pour autant qu'elles sont relatives à la vie sexuelle, concernent les personnes visées dans le présent paragraphe, sont soumis à une autorisation spéciale individuelle accordée par le Roi, dans un arrêté royal délibéré en Conseil des ministres, après avis de l'autorité de contrôle compétente.

L'arrêté visé à l'alinéa premier, 3°, précise la durée de validité de l'autorisation, les modalités du traitement des données, les modalités de contrôle de l'association ou de l'établissement par l'autorité compétente et la façon dont cette autorité informera l'autorité de contrôle compétente sur le traitement de données à caractère personnel effectué dans le cadre de l'autorisation accordée.

Sauf dispositions légales particulières, le traitement de données génétiques et biométriques aux fins d'identifier une

verenigingen, instellingen en stichtingen, met als doel het op een unieke wijze identificeren van een fysieke persoon, verboden.

Art. 9

§ 1. In uitvoering van artikel 10 van de Verordening wordt de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen uitgevoerd:

1. door natuurlijke personen of door privaatrechtelijke of publiekrechtelijke rechtspersonen voor zover dat noodzakelijk is voor het beheer van hun eigen geschillen; of

2. door advocaten of andere juridische raadgevers in zoverre de verdediging van de belangen van hun cliënten dit vereist; of

3. door andere personen, indien de verwerking noodzakelijk is voor de verwezenlijking van doeleinden die door of krachtens een wet, een decreet, een ordonnantie of de Europese regelgeving zijn vastgesteld; of

4. voor zover de verwerking noodzakelijk is voor wetenschappelijk onderzoek en verricht wordt onder de voorwaarden voorzien in titel 4 van deze wet; of

5. door de stichting van openbaar nut "Stichting voor Vermiste en Seksueel Uitgebuite Kinderen".

§ 2. De verwerkingsverantwoordelijke, en in voorkomend geval, de verwerker stelt een lijst op van de categorieën van personen die de persoonsgegevens kunnen raadplegen, met een beschrijving van hun hoedanigheid ten opzichte van de verwerking van de beoogde gegevens. Deze lijst wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit.

De verwerkingsverantwoordelijke, en in voorkomend geval, de verwerker zorgt dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling, ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.

HOOFDSTUK III

Rechten van de betrokkene

Art. 10

Onder de voorwaarden vastgelegd in artikel 11, zijn artikel 12 tot 22 en 34 van de Verordening niet van toepassing voor de verwerkingsverantwoordelijke of verwerker voor de verwerkingen van persoonsgegevens in het kader:

§ 1. van de preventie en detectie van strafbare feiten, evenals onderzoeken en vervolgingen of de uitvoering van strafrechtelijke sancties, met inbegrip van de bescherming tegen bedreigingen van de openbare veiligheid en de preventie van

personne physique de manière unique par ces associations, établissements et fondations est interdit.

Art. 9

§ 1er. En exécution de l'article 10 du Règlement, le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions pénales ou aux mesures de sûreté connexes est effectué:

1. par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige; ou

2. par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige; ou

3. par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret, d'une ordonnance ou du droit de l'Union européenne; ou

4. pour les nécessités de la recherche scientifique, dans le respect des conditions prévues au titre 4 de la présente loi; ou

5. par la fondation d'utilité publique "Fondation pour Enfants Disparus et Sexuellement Exploités".

§ 2. Le responsable du traitement et, le cas échéant, le sous-traitant établit une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l'autorité de contrôle compétente.

Le responsable du traitement et, le cas échéant, le sous-traitant veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

CHAPITRE III

Droits de la personne concernée

Art. 10

Dans les conditions fixées à l'article 11, les articles 12 à 22 et 34 du Règlement ne s'appliquent pas au responsable du traitement ou au sous-traitant pour les traitements de données à caractère personnel dans le cadre:

§ 1er. de la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles

zulke bedreigingen, uitgezonderd de bevoegde overheden in de zin van titel 2 van deze wet, en de inlichtingen- en veiligheidsdiensten in de zin van titel 3 van deze wet;

§ 2. van de bescherming van belangrijke doelstellingen voor algemeen openbaar belang zoals het economisch of financieel belang, met inbegrip van het monetair, budgettair en fiscaal domein, van de volksgezondheid en de sociale zekerheid;

§ 3. van een controle-, inspectie of regelgevingsopdracht verbonden, zelfs occasioneel, aan de uitoefening van het openbaar gezag, in de gevallen beoogd in punt a), e) en g), van artikel 23.1 van de Verordening.

Art. 11

De in artikel 10 bedoelde beperking mag alleen worden verstrekt onder de volgende waarborgen:

§ 1. Zonder afbreuk te doen aan de toepassing van bijzondere wettelijke bepalingen, is de beperking van de rechten en verplichtingen van toepassing op de verwerkingen beheerd door de verwerkingsverantwoordelijken of verwerkers bedoeld in artikel 10 tijdens de periode waarbinnen de betrokkene deel uitmaakt van een controle, onderzoek, strafrechtelijke vervolging, hierop voorbereidende handelingen of procedures in het kader van de uitoefening van wettelijke opdrachten, voor zover de toepassing ervan de behoeften van de controle, het onderzoek, de strafrechtelijke vervolging, de voorbereidende handelingen of de procedures zou schaden en zolang vereist ter bescherming van de belangrijke doelstellingen van algemeen openbaar belang, zoals bedoeld in artikel 10, 2°.

De verantwoordelijke voor de verwerking of verwerker, zoals bedoeld in artikel 10, informeert de betrokken personen over de toepassing van dit artikel, hetzij dit het doel van de beperking kan schaden.

De in artikel 10 bedoelde verwerkingsverantwoordelijke of verwerker moet zijn beleid om de rechten en plichten, vermeld in datzelfde artikel 10 te beperken, rechtvaardigen op verzoek van de Gegevensbeschermingsautoriteit.

§ 2. De verantwoordelijke voor de verwerking of verwerker, bedoeld in artikel 10 houdt een logboek bij van alle aanvragen tot uitoefening van de rechten, bedoeld in de artikelen 12 tot 22 en 34 van de Verordening, evenals de rechtvaardiging in geval van weigering. Dit logboek wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit.

§ 3. Na het afsluiten van de controle, het onderzoek, de strafrechtelijke vervolging of de procedure in het kader van wettelijke opdrachten, worden de rechten vermeld in artikel 10 hersteld.

Hetzelfde geldt wanneer de bescherming van de belangrijke doelstellingen van algemeen openbaar belang niet langer vereist is evenals na de afsluiting van de voorbereidende

menaces, à l'exception des autorités compétentes au sens du titre 2 de la présente loi, et des services de renseignement et de sécurité au sens du titre 3 de la présente loi;

§ 2. de la protection d'objectifs importants d'intérêt public général tel que l'intérêt économique ou financier, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;

§ 3. d'une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g), de l'article 23.1 du Règlement.

Art. 11

La limitation visée à l'article 10 ne peut se faire que dans les conditions suivantes:

§ 1er. Sans préjudice de l'application de dispositions légales particulières, la limitation aux droits et obligations s'applique aux traitements gérés par les responsables du traitement ou sous-traitants visés à l'article 10 soit pendant la période durant laquelle la personne concernée fait l'objet d'un contrôle, d'une enquête, d'une poursuite pénale, d'actes préparatoires à ceux-ci ou de procédures dans le cadre de l'exécution de missions légales, dans la mesure où cette application nuirait aux besoins du contrôle, de l'enquête, de la poursuite pénale, des actes préparatoires ou des procédures, soit aussi longtemps que la protection d'objectifs importants d'intérêt public général visé à l'article 10, 2°, l'exige.

Le responsable du traitement ou sous-traitant visé à l'article 10 informe les personnes concernées de l'application du présent article à moins que cela ne puisse nuire à la finalité de la limitation.

Le responsable du traitement ou sous-traitant visé à l'article 10, doit justifier sa politique de limitations des droits et obligations mentionnés dans ce même article 10, à la demande de l'Autorité de protection des données.

§ 2. Le responsable du traitement ou sous-traitant visé à l'article 10 tient un journal des demandes d'exercice des droits visés aux articles 12 à 22 et 34 du Règlement, ainsi que la justification en cas de refus. Ce journal est tenu à la disposition de l'autorité de contrôle compétente.

§ 3. Après la clôture du contrôle, de l'enquête, de la poursuite pénale ou de la procédure dans le cadre de l'exécution de missions légales, les droits mentionnés à l'article 10 sont rétablis.

Il en est de même lorsque la protection d'objectifs importants d'intérêt public général ne l'exige plus ainsi qu'après la clôture des actes préparatoires lorsque ceux-ci n'ont pas

handelingen als ze niet geleid hebben tot een controle, een onderzoek, een strafrechtelijke vervolging of een procedure in het kader van wettelijke opdrachten.

§ 4. In het kader van de toepassing van dit artikel, streeft de verantwoordelijke voor de verwerking of de verwerker, zoals bedoeld in artikel 10, naar een juist evenwicht tussen de finaliteiten van de verwerking, als bedoeld in artikel 10 en de risico's voor de rechten en vrijheden van de betrokkenen. Hij weet de toepassing van regels en principes van de Verordening op zijn werkprocessen aan te tonen. Hij neemt met name de nodige maatregelen om misbruik en onrechtmatige toegang tot en overdracht van persoonsgegevens te voorkomen, met name de gepaste technische en organisatorische maatregelen, zoals bedoeld in artikel 32 van de Verordening.

§ 5. Als de betrokkene onder de omstandigheden vermeld in dit artikel een verzoek indient op basis van de artikelen 15 tot 22 van de Verordening, behandelt de functionaris voor gegevensbescherming van de in artikel 10 bedoelde verwerkingsverantwoordelijken of verwerkers het verzoek. Die deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht en over de mogelijkheid om klacht in te dienen bij de Gegevensbeschermingsautoriteit en een beroep in rechte in te stellen.

Art. 12

In toepassing van artikel 23 van de Verordening, geniet de betrokkene met betrekking tot de verwerking van zijn persoonsgegevens die rechtstreeks of onrechtstreeks afkomstig zijn van andere overheden bedoeld in artikel 3 van deze wet, niet van de rechten bedoeld in de artikelen 12 tot 22 en 34 van de Verordening en ook niet van het recht op transparantie van de verwerking bedoeld in artikel 5 van de Verordening betreffende deze gegevens, met betrekking tot:

— de instanties en personen bedoeld in artikel 19 van de wet van 30 november 1998 naar wie deze gegevens werden overgebracht door de inlichtingen- en veiligheidsdiensten;

— tot de instanties en personen bedoeld in artikel 10 van de wet van 10 juli 2006 betreffende de analyse van de dreiging en in artikel 44/11/3*ter*, §§ 2 en 3 en artikel 44/11/3*quater* van de wet op het politieambt, en die onder het toepassingsgebied van titel 1 vallen, en aan wie deze gegevens werden overgemaakt.

In toepassing van artikel 23 van de Verordening zijn de verplichtingen bedoeld in artikelen 12 tot 22 en 34 van de Verordening niet van toepassing op instanties en personen die in het bezit zijn van deze gegevens.

De verwerkingsverantwoordelijke bedoeld in deze titel die in het bezit is van zulke gegevens deelt deze niet mee aan de betrokkene tenzij:

1. de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

abouti à un contrôle, une enquête, de la poursuite pénale ou de la procédure dans le cadre de l'exécution de missions légales.

§ 4. Dans le cadre de l'application du présent article, le responsable du traitement ou sous-traitant visé à l'article 10 vise à trouver un juste équilibre entre les finalités du traitement visées à l'article 10 et les risques pour les droits et libertés des personnes concernées. Il sait démontrer l'application des règles et principes du Règlement à ses processus de travail. Il adopte notamment les mesures nécessaires destinées à garantir la prévention des abus ainsi que de l'accès et du transfert illicites des données à caractère personnel, notamment les mesures techniques et organisationnelles appropriées visées à l'article 32 du Règlement.

§ 5. Lorsque la personne concernée présente une demande en vertu des articles 15 à 22 du Règlement dans les conditions prévues au présent article le délégué à la protection des données du responsable du traitement ou sous-traitant visée à l'article 10 traite la demande. Celui-ci informe la personne concernée que les vérifications nécessaires ont été effectuées et de la possibilité d'introduire une plainte auprès de l'Autorité de protection des données et de former un recours juridictionnel.

Art. 12

En application de l'article 23 du Règlement, la personne concernée par le traitement de ses données à caractère personnel, émanant directement ou indirectement des autres autorités visées au titre 3 de la présente loi, ne bénéfice pas des droits visés aux articles 12 à 22 et 34 du Règlement, ainsi que du droit à la transparence du traitement visée à l'article 5 du Règlement, concernant ces données, à l'égard:

— des autorités et personnes visées à l'article 19 de la loi du 30 novembre 1998 auxquelles ces données ont été transmises par les services de renseignement et de sécurité;

— des autorités et personnes visées à l'article 10 de la loi du 10 juillet 2006 relative à l'analyse de la menace ainsi que celles mentionnées à l'article 44/11/3 ter §§ 2 et 3 et à l'article 44/11/3 quater de la loi sur la fonction de police, et qui ressortent du titre 1er, et auxquelles ces données ont été transmises.

En application de l'article 23 du Règlement, les obligations visées aux articles 12 à 22 et 34 du Règlement ne s'appliquent pas aux autorités et personnes en possession de ces données.

Le responsable du traitement visé dans le présent titre qui est en possession de telles données ne les communique pas à la personne concernée à moins que:

1. la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que

2. de betrokken overheid bedoeld in lid 1 hem dit toestaat

De verwerkingsverantwoordelijke of de bevoegde overheid deelt niet mee dat hij in het bezit is van gegevens die van overheden bedoeld in titel 3 afkomstig zijn.

De beperkingen bedoeld in het eerste lid hebben eveneens betrekking op het logbestand van de verwerkingen van een overheid bedoeld in titel 3 van deze wet in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel waartoe de de overheid rechtstreeks toegang heeft.

§ 2. Wanneer een beroep aanhangig wordt gemaakt bij de bevoegde toezichthoudende autoriteit waarbij de verwerkingsverantwoordelijke zich beroept op de toepassing van dit artikel, wendt deze eerste zich tot het Vast Comité I opdat het de nodige verificaties bij de betrokken autoriteit bedoeld in titel 3 verricht.

De bevoegde toezichthoudende autoriteit brengt de betrokkene enkel op de hoogte van de resultaten van de verificatie, die geen betrekking hebben op persoonsgegevens die van een autoriteit bedoeld in titel 3 afkomstig zijn, die ze wettelijk gehouden is mee te delen.

Indien het beroep enkel betrekking heeft op persoonsgegevens afkomstig van een autoriteit bedoeld in titel 3, antwoordt de toezichthoudende autoriteit dat de nodige verificaties werden verricht.]

Art. 13

In toepassing van artikel 23 van de Verordening, is een verwerkingsverantwoordelijke die persoonsgegevens meedeelt aan een overheid bedoeld in titel 3 van deze wet niet onderworpen aan de artikelen 13.1.e, 14.1.e en 15.1.c van de Verordening en aan artikel 23, 6°, van deze wet en mag de betrokkene niet van deze overdracht op de hoogte brengen.

Algemene informatie over de samenwerking tussen de autoriteiten bedoeld in titel 3 en de bevoegde autoriteiten als bedoeld in artikel 31, 7°, valt niet onder het eerste lid.

Art. 14

Wanneer een overheid bedoeld in titel 3 van deze wet over een rechtstreekse toegang of over een rechtstreekse bevraging van een gegevensbank van de openbare of private sector beschikt, worden zijn verwerkingen van persoonsgegevens in deze gegevensbank beschermd door technische, organisatorische en persoonlijke beveiligingsmaatregelen zodat alleen de volgende actoren toegang kunnen hebben tot de inhoud van deze verwerkingen om hun wettelijke toezichtsopdrachten uit te voeren:

1. de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke van de gegevensbank of de persoon die hij daartoe machtigt;

2. l'autorité visée à l'alinéa 1er concernée ne l'y autorise.

Le responsable du traitement ou l'autorité compétente ne fait aucune mention qu'il est en possession de données émanant des autorités visées au titre 3.

Les limitations visées à l'alinéa premier portent également sur la journalisation des traitements d'une autorité visée au titre 3 de la présente loi dans les banques de données des responsables du traitement visés par le présent titre auxquelles l'autorité a directement accès.

§ 2. Lorsque l'autorité de contrôle compétente est saisie d'un recours où le responsable du traitement fait état de l'application du présent article, celle-ci s'adresse au Comité permanent R pour qu'il fasse les vérifications nécessaires auprès de l'autorité visée au titre 3.

L'autorité de contrôle compétente n'informe la personne concernée que des résultats de la vérification portant sur les données à caractère personnel n'émanant pas des autorités visées au titre 3 qu'elle est légalement tenue de communiquer.

Si le recours ne porte que sur des données à caractère personnel émanant d'une autorité visée au titre 3, l'autorité de contrôle répond que les vérifications nécessaires ont été effectuées.

Art. 13

En application de l'article 23 du Règlement, un responsable du traitement qui communique des données à caractère personnel à une autorité visée au titre 3 de la présente loi n'est pas soumis aux articles 13.1.e, 14.1.e. et 15.1.c. du Règlement et à l'article 23, 6°, de la présente loi et ne peut informer la personne concernée de cette transmission.

Les informations générales sur la collaboration entre les autorités visées au titre 3 et les autorités compétentes visées à l'article 31, 7°, ne sont pas visées par l'alinéa premier.

Art. 14

Lorsqu'une autorité visée au titre 3 de la présente loi dispose d'un accès direct ou d'une interrogation directe à une banque de données du secteur public ou du secteur privé, ses traitements de données à caractère personnel dans cette banque de données sont protégés par des mesures de sécurité techniques, organisationnelles et personnelles de sorte que seuls les acteurs suivants puissent accéder au contenu de ces traitements pour assurer leurs missions légales de contrôle:

1. le délégué à la protection des données du responsable du traitement de la banque de donnée ou la personne qu'il délègue à cet effet;

2. de functionaris voor gegevensbescherming van de overheid bedoeld in titel 3;

3. de verwerkingsverantwoordelijke van de gegevensbank of de persoon die hij daartoe machtigt;

4. de verwerkingsverantwoordelijke van de overheid bedoeld in titel 3, in voorkomend geval;

5. elke andere persoon bepaald in een protocol tussen de verwerkingsverantwoordelijken.

Deze beveiligingsmaatregelen zijn bedoeld om de wettelijke verplichtingen met betrekking tot de bescherming van bronnen, de bescherming van de identiteit van de agenten en de discretie van de onderzoeken van de overheden beodel in titel 3 te beschermen.

Deze verwerkingen mogen enkel toegankelijk zijn voor andere doeleinden die verband houden met het toezicht en slechts op basis van een protocolakkoord tussen de betrokken verwerkingsverantwoordelijken.

Het controlesysteem wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

De betrokken overheid bedoeld in titel 3 kan afwijken van het eerste lid wanneer hij van oordeel is dat de toepassing op een bepaalde gegevensbank niet relevant is.

Art. 15

Overeenkomstig artikel 23.1 van de Verordening kan de betrokkene wiens persoonsgegevens aanvankelijk door de politiediensten bedoeld in titel 2 verwerkt worden, de in de artikelen 12 tot 22 en 34 van de Verordening bedoelde rechten betreffende die gegevens en het recht op transparantie van de verwerking bedoeld in artikel 5 van de Verordening niet inroepen ten aanzien van de ontvangers voorzien in de artikelen 44/1, §§ 3 en 4 alsook in de artikelen 44/11/7 tot 44/11/11 van de wet op het politieambt aan wie de politiediensten die gegevens bezorgd hebben.

Onverminderd bijzondere wetten zijn de verplichtingen bedoeld in dezelfde artikelen overeenkomstig artikel 23.1 van de Verordening niet van toepassing op de ontvangers vermeld in het eerste lid.

De beperkingen bedoeld in de leden 1 en 2 hebben eveneens betrekking op de logbestanden van de verwerkingen door een politiedienst bedoeld in titel 2 van deze wet, in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel.

Deze uitzonderingen op de rechten en verplichtingen zijn slechts van toepassing op de gegevens die aanvankelijk door de politiediensten verwerkt worden voor de doeleinden bedoeld in artikel 32 van deze wet.

De in het eerste lid vermelde ontvangers moeten in de gepaste waarborgen voorzien voor de rechten en vrijheden

2. le délégué à la protection des données de l'autorité visée au titre 3;

3. le responsable du traitement de la banque de données ou la personne qu'il délègue à cet effet;

4. le responsable du traitement de l'autorité visée au titre 3, le cas échéant;

5. toute autre personne précisée dans un protocole entre les responsables du traitement.

Ces mesures de sécurité visent à protéger les obligations légales portant sur la protection des sources, la protection de l'identité de leurs agents et la discrétion des enquêtes des autorités visées au titre 3.

Ces traitements ne peuvent être accessibles pour d'autres finalités que celles liées au contrôle que sur la base d'un protocole d'accord entre les responsables du traitement concernés.

Le système de contrôle est mis à la disposition de l'autorité de contrôle compétente.

L'autorité visée au titre 3 concernée peut déroger à l'alinéa premier lorsqu'elle estime que son application à une banque de données déterminée n'est pas pertinente.

Art. 15

En application de l'article 23.1 du Règlement, la personne concernée par le traitement de ses données à caractère personnel, initialement traitées par les services de police visés au titre 2, ne peut opposer les droits visés aux articles 12 à 22 et 34 du Règlement, ainsi que le droit à la transparence du traitement visée à l'article 5 du Règlement, concernant ces données, à l'égard des destinataires prévus dans les articles 44/1, §§ 3 et 4 ainsi qu'aux articles 44/11/7 à 44/11/11 de la loi sur la fonction de police auxquelles ces données ont été transmises par les services de police.

Sans préjudice de lois particulières, en application de l'article 23.1 du Règlement, les obligations visées aux mêmes articles ne s'appliquent pas aux destinataires mentionnés à l'alinéa premier.

Les limitations visées aux l'alinéas 1 et 2 portent également sur la journalisation des traitements effectués par un service de police visé au titre 2 de la présente loi dans les banques de données des responsables du traitement visés par le présent titre.

Ces exceptions aux droits et obligations ne valent que pour les données traitées initialement, par les services de police, pour les finalités visées à l'article 32 de la présente loi.

Les destinataires mentionnés à l'alinéa premier sont tenus de prévoir les garanties appropriées pour les droits

van de betrokkenen zoals bedoeld in artikel 23.2 van de Verordening.

Elk verzoek dat betrekking heeft op de uitoefening van de in de artikelen 12 tot 22 van de Verordening vastgelegde rechten betreffende in het lid 4 bedoelde gegevens en dat aan een ontvanger wordt gericht, wordt zo snel mogelijk en in elk geval binnen een maand na de ontvangst van het verzoek aan de bevoegde toezichthoudende autoriteit bezorgd.

Art. 16

Overeenkomstig artikel 23.1 van de Verordening kan de betrokkene wiens persoonsgegevens aanvankelijk door de gerechtelijke overheden bedoeld in titel 2 verwerkt worden, de in de artikelen 12 tot 22 en 34 van de Verordening bedoelde rechten betreffende die gegevens en het recht op transparantie van de verwerking bedoeld in artikel 5 van de Verordening niet inroepen ten aanzien van de ontvangers aan wie de gerechtelijke overheden die gegevens bezorgd hebben, tenzij:

1. de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2. de betrokken gerechtelijke overheden hem dit toestaat.

Onverminderd bijzondere wetten zijn de verplichtingen bedoeld in dezelfde artikelen overeenkomstig artikel 23.1 van de Verordening niet van toepassing op de ontvangers vermeld in het eerste lid.

De beperkingen bedoeld in de leden 1 en 2 hebben eveneens betrekking op de logbestanden van de verwerkingen door de gerechtelijke overheden bedoeld in titel 2 van deze wet, in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel.

Deze uitzonderingen op de rechten en verplichtingen zijn slechts van toepassing op de gegevens die aanvankelijk door de gerechtelijke overheden verwerkt worden voor de doeleinden bedoeld in artikel 32 van deze wet.

De in het eerste lid vermelde ontvangers moeten in de gepaste waarborgen voorzien voor de rechten en vrijheden van de betrokkenen zoals bedoeld in artikel 23.2 van de Verordening.

Elk verzoek dat betrekking heeft op de uitoefening van de in de artikelen 12 tot 22 van de Verordening vastgelegde rechten betreffende in het lid 4 bedoelde gegevens en dat aan een ontvanger wordt gericht, wordt zo snel mogelijk en in elk geval binnen een maand na de ontvangst van het verzoek aan de bevoegde toezichthoudende autoriteit bezorgd.

Art. 17

Wanneer de persoonsgegevens in een rechterlijke beslissing of een gerechtelijk dossier zijn opgenomen of in het kader van strafrechtelijke onderzoeken en procedures worden verwerkt, worden de in de artikelen 12 tot 22 en 34 van de

et libertés des personnes concernées, telles que visées à l'article 23.2 du Règlement.

Toute demande portant sur l'exercice des droits visés aux articles 12 à 22 du Règlement, concernant des données visées à l'alinéa 4, adressée à un destinataire est transmise dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, à l'autorité de contrôle compétente.

Art. 16

En application de l'article 23.1 du Règlement, la personne concernée par le traitement de ses données à caractère personnel, initialement traitées par les autorités judiciaires visées au titre 2 ne peut opposer les droits visés aux articles 12 à 22 et 34 du Règlement, ainsi que le droit à la transparence du traitement visée à l'article 5 du Règlement, concernant ces données, à l'égard des destinataires auxquelles ces données ont été transmises par les autorités judiciaires, à moins que :

1. la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que

2. les autorités judiciaires concernées ne l'y autorise.

Sans préjudice de lois particulières, en application de l'article 23.1 du Règlement, les obligations visées aux mêmes articles ne s'appliquent pas aux destinataires mentionnés à l'alinéa premier.

Les limitations visées aux alinéas 1 et 2 portent également sur la journalisation des traitements effectués par les autorités judiciaires visées au titre 2 de la présente loi dans les banques de données des responsables du traitement visés par le présent titre.

Ces exceptions aux droits et obligations ne valent que pour les données traitées initialement, par les autorités judiciaires, pour les finalités visées à l'article 32 de la présente loi.

Les destinataires mentionnés à l'alinéa premier sont tenus de prévoir les garanties appropriées pour les droits et libertés des personnes concernées, telles que visées à l'article 23.2 du Règlement.

Toute demande portant sur l'exercice des droits visés aux articles 12 à 22 du Règlement, concernant des données visées au paragraphe 4, adressée à un destinataire est transmise dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, à l'autorité de contrôle compétente.

Art. 17

Lorsque les données à caractère personnel figurent dans une décision judiciaire ou un dossier judiciaire, ou font l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale, les droits visés aux articles 12 à 22 et 34 du

Verordening bedoelde rechten uitgeoefend overeenkomstig het Gerechtelijk wetboek en het wetboek van Strafvordering.

Art. 18

§ 1. In toepassing van artikel 23 van de Verordening, geniet de persoon die betrokken is bij een gemeenschappelijke behandeling van zijn persoonsgegevens, rechtstreeks of onrechtstreeks afkomstig van ten minste één bevoegde autoriteit van titel 2 of ten minste één dienst, één autoriteit of één orgaan bedoeld in titel 3, voor wat zijn gegevens bij de verantwoordelijke of verantwoordelijken voor de verwerking betreft, niet van de in de artikelen 12 tot 22 en 34 van de Verordening genoemde rechten, en ook niet van het recht op transparantie van de verwerking bedoeld in artikel 5 van de Verordening.

§ 2. Krachtens artikel 23 van de Verordening zijn de in de artikelen 12 tot 22 en 34 van de Verordening bedoelde verplichtingen niet van toepassing op de autoriteiten, personen of verantwoordelijken voor de verwerking, die over de in het eerste lid bedoelde gegevens beschikken.

§ 3.De verwerkingsverantwoordelijke bedoeld in deze titel die in het bezit is van de gegevens bedoeld in het eerste lid deelt deze niet mee aan de betrokkene tenzij:

1. de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2. de verantwoordelijke of verantwoordelijken voor de gemeenschappelijke verwerking hem dit toestaat.

§ 4. De verantwoordelijke of verantwoordelijken voor de gemeenschappelijke verwerking doen geen enkele melding aan de betrokkene dat hij in het bezit is van gegevens die afkomstig zijn van de gemeenschappelijke verwerking.

§ 5. De beperkingen bedoeld in het eerste lid hebben eveneens betrekking op de dagdagelijkse verwerking van de gemeenschappelijke verwerking.

§ 6. Wanneer een beroep aanhangig wordt gemaakt bij de bevoegde toezichthoudende autoriteit waarbij de verantwoordelijke of verantwoordelijken voor de verwerking zich beroepen op de toepassing van dit artikel, wendt deze zich tot andere toezichthoudende autoriteiten die bevoegd zijn voor gemeenschappelijke verwerking, opdat zij de nodige verificaties kunnen verrichten bij de verantwoordelijken voor de gemeenschappelijke verwerking. De toezichthoudende autoriteit antwoordt alleen dat de nodige verificaties zijn verricht.

Règlement sont exercés conformément au Code judiciaire et au Code d'instruction criminelle.

Art. 18

§ 1er. En application de l'article 23 du Règlement, la personne concernée par un traitement commun de ses données à caractère personnel, émanant directement ou indirectement d'au moins une autorité compétente du titre 2 ou d'au moins un service, une autorité ou un organe du titre 3 ne bénéfice pas des droits visés aux articles 12 à 22 et 34 du Règlement, ainsi que du droit à la transparence du traitement visée à l'article 5 du Règlement, à l'égard de ses données auprès du ou des responsables du traitement commun.

§ 2. En application de l'article 23 du Règlement, les obligations visées aux articles 12 à 22 et 34 du Règlement ne s'appliquent pas aux autorités, personnes ou responsables du traitement en possession des données visées à l'alinéa premier.

§ 3. Le responsable du traitement visé dans le présent titre qui est en possession de données visées à l'alinéa premier ne les communique pas à la personne concernée à moins que:

1. la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que

2. le ou les responsables du traitement commun ne l'y autorise.

§ 4. Le ou les responsables du traitement commun ne font aucune mention à la personne concernée qu'il est en possession de données émanant du traitement commun.

§ 5. Les limitations visées à l'alinéa premier portent également sur la journalisation des traitements dans le traitement commun.

§ 6. Lorsque l'autorité de contrôle compétente est saisie d'un recours où le ou les responsables du traitement font état de l'application du présent article, celle-ci s'adresse aux autres autorités de contrôle compétentes pour le traitement commun, pour qu'elles fassent les vérifications nécessaires auprès du ou des responsables du traitement commun. L'autorité de contrôle répond uniquement que les vérifications nécessaires ont été effectuées.

HOOFDSTUK IV

Verwerkingsverantwoordelijke en verwerker

Afdeling 1

Algemene bepalingen

Art. 19

De verwerkingsverantwoordelijke die een verzoek ontvangt om een recht bedoeld in de artikelen 15 tot 22 van de Verordening uit te oefenen, bezorgt de verzoeker onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek een gedagtekend ontvangstbewijs.

Art. 20

In uitvoering van artikel 43 van de Verordening worden de certificeringsorganen geaccrediteerd, op basis van de norm EN-ISO/IEC 17065 en de aanvullende eisen die door de bevoegde toezichthoudende autoriteit zijn vastgesteld, door de nationale accreditatie-instantie die is aangewezen in overeenstemming met Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad.

Afdeling 2

Publieke sector

Art. 21

Voor de toepassing van deze afdeling wordt onder "overheidsinstantie"en "openbaar orgaan" de openbare instelling of privaatrechtelijke instelling of publiekrechtelijke instelling verstaan die een openbare dienst verleent.

Tenzij er specifiek van afgeweken wordt, is deze afdeling van toepassing op de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

Art. 22

§ 1. In uitvoering van artikel 6.2 van de Verordening kan een federale overheidsinstantie of een federaal openbaar orgaan beslissen de persoonsgegevens verwerkt op basis van artikel 6.1.c) en e), van de Verordening door te geven aan enig andere overheidsinstantie, openbaar of privé orgaan aan de hand van een protocol dat tot stand komt tussen de initiële gegevensverwerker en de verdere gegevensverwerker.

Dit protocol kan in het bijzonder voorzien in:

1. de identificatie van de federale overheidsinstantie of federaal openbaar orgaan die de persoonsgegevens doorgeeft alsook die van de ontvanger;

CHAPITRE IV

Responsable du traitement et sous-traitant

Section 1re

Dispositions générales

Art. 19

Le responsable du traitement qui reçoit une demande d'exercer un droit visé aux articles 15 à 22 du Règlement délivre dans les meilleurs délais et, en tout état de cause dans un délai d'un mois à compter de la réception de la demande, un accusé de réception daté à l'auteur de la demande.

Art. 20

En exécution de l'article 43 du Règlement, les organismes de certification sont accrédités conformément à la norme EN-ISO/IEC 17065 et aux exigences supplémentaires établies par l'autorité de contrôle par l'organisme national d'accréditation désigné conformément au Règlement (CE) no 765/2008 du Parlement européen et du Conseil.

Section 2

Secteur public

Art. 21

Pour l'application de la présente section, on entend par "autorité publique" et "organisme publics" l'institution publique, ou l'institution de droit privé ou de droit public qui fournit un service public.

Sauf si il y est expressément dérogé, la présente section est applicable aux services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police structuré organisé à deux niveaux.

Art. 22

§ 1er. En exécution de l'article 6.2 du Règlement, une autorité publique fédérale ou un organisme public fédéral qui transmet des données à caractère personnel sur la base de l'article 6.1.c) et e), du Règlement à toute autre autorité publique, organisation publique ou privée, peut formaliser cette transmission par un protocole entre le responsable du traitement initial et le responsable du traitement ultérieur.

Ce protocole peut prévoir notamment:

1. l'identification de l'autorité publique fédérale ou organisme public fédéral qui transfère les données à caractère personnel et celle du destinataire;

2. de identificatie van de verwerkingsverantwoordelijke;

3. de contactgegevens van de functionarissen voor gegevensbescherming;

4. de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5. de categorieën van meegedeelde persoonsgegevens;

6. de categorieën van ontvangers;

7. de wettelijke grondslag;

8. de modaliteiten inzake gehanteerde communicatie;

9. de gepaste beveiligingsmaatregelen ter bescherming van de persoonsgegevens;

10. het voorafgaand akkoord van de administratie die houder is van de gegevens bij de inschakeling van een verwerker door de ontvanger;

11. de beperkingen met betrekking tot de rechten van de betrokkene;

12. de modaliteiten inzake de rechten van de betrokkene bij de ontvanger;

13. de modaliteiten inzake tenuitvoerlegging en evaluatie door de functionaris voor gegevensbescherming;

14. de periodiciteit van de doorgifte;

15. de duur van het protocol;

16. de sancties die van toepassing zijn in geval van niet naleving van het protocol onverminderd titel 4.

§ 2. Het protocol wordt afgesloten na de respectievelijke adviezen van de functionaris voor gegevensbescherming van de federale overheidsinstantie of federaal openbaar orgaan die houder is van de persoonsgegevens en van de ontvanger.

Art. 23

§ 1. Overeenkomstig artikel 30 van de Verordening staat elke federale overheidsinstantie of federaal openbaar orgaan in voor het uitwerken en het bijhouden van een register van de verwerking van persoonsgegevens.

§ 2. Het register bevat de volgende elementen:

1. de naam en de contactgegevens van de verwerkingsverantwoordelijke of de verwerker, en van zijn gedelegeerde of vertegenwoordiger;

2. de naam en de contactgegevens van de functionaris voor gegevensbescherming;

2. l'identification du responsable du traitement;

3. les coordonnées des délégués à la protection des données concernés;

4. les finalités pour lesquelles les données à caractère personnel sont transférées;

5. les catégories de données à caractère personnel communiquées;

6. les catégories de destinataire;

7. la base légale;

8. les modalités de communication utilisé;

9. les mesures de sécurité propres à assurer la protection des données à caractère personnel;

10. l'accord préalable de l'administration détentrice des données lors du recours à un sous-traitant par le destinataire;

11. les restrictions aux droits de la personne concernée;

12. les modalités des droits de la personne concernées auprès du destinataire;

13. les modalités de mise en œuvre et d'évaluation par le délégué à la protection des données;

14. la périodicité du transfert;

15. la durée du protocole;

16. des sanctions applicables en cas de non respect du protocole, sans préjudice du titre 4.

§ 2. Le protocole est adopté après les avis respectifs du délégué à la protection des données de l'autorité publique fédérale ou organisme public fédéral détendeur des données à caractère personnel et du destinataire.

Art. 23

§ 1er. Conformément à l'article 30 du Règlement, toute autorité publique fédérale ou organisme public fédéral doit établir et maintenir à jour un registre des traitements de données à caractère personnel.

§ 2. Le registre contient les éléments suivants:

1. le nom et les coordonnées du responsable du traitement ou sous-traitant, de son délégué ou représentant;

2. le nom et les coordonnées du délégué à la protection des données;

3. de verwerkingsdoeleinden;

4. de categorieën van betrokkenen;

5. de categorieën van persoonsgegevens;

6. de categorieën van ontvangers;

7. de doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in voorkomend geval, de documenten die het bestaan van passende waarborgen aantonen;

8. de beoogde termijnen voor het wissen van de verschillende gegevenscategorieën;

9. een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 32.1 van de Verordening;

10. het gebruik van profilering;

11. de rechtsgrondslag;

12. de categorie van externe bronnen;

13. het protocol bedoeld in artikel 22, het advies van de functionaris voor gegevensbescherming en de motivering bedoeld in artikel 26.

§ 3. Onverminderd het besluit bedoeld in artikel 57, § 3, wordt de functionaris voor gegevensbescherming betrokken bij de uitwerking en het bijhouden van het register door de federale overheidsinstanties of federale openbare organen.

§ 4. Het register, dat bij de Gegevensbeschermingsautoriteit wordt bijgehouden, wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

§ 5. In afwijking van paragraaf 4 wordt het register van de politiediensten in de zin van artikel 3 van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten beheerd binnen de politie. Het wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Art. 24

§ 1. Het register bedoeld in artikel 23 wordt op een geinformatiseerde manier beheerd. De modaliteiten van het beheer en, voor wat betreft de politiediensten de integratie van de elementen afkomstig van het register door deze laatste opgesteld, worden door de Koning bepaald.

§ 2. Onverminderd het besluit bedoeld in artikel 57, § 3, bepaalt de Koning, bij een in Ministerraad overlegd besluit en na advies van de bevoegde toezichthoudende autoriteit, de modaliteiten en het geheel of gedeeltelijk publieke karakter van het register.

3. les finalités du traitement;

4. les catégories de personnes concernées;

5. les catégories de données à caractère personnel;

6. les catégories de destinataires;

7. les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, le cas échéant, les documents attestant de l'existence de garanties appropriées;

8. les délais prévus pour l'effacement des différentes catégories de données;

9. une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32.1 du Règlement;

10. le recours au profilage;

11. la base juridique;

12. la catégorie de sources externes;

13. le protocole visé à l'article 22, l'avis du délégué à la protection des données et la motivation visés à l'article 26.

§ 3. Sans préjudice de l'arrêté visé à l'article 57, § 3, le délégué à la protection des données est associé à l'élaboration et au maintien du registre par les autorités publiques fédérales ou organismes publics fédéraux.

§ 4. Le registre, tenu auprès de l'Autorité de protection des données, est mis à la disposition de l'autorité de contrôle compétente.

§ 5. Par dérogation au paragraphe 4, le registre des services de police au sens de l'article 3 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, est géré au sein de la police. Il est mis à la disposition de l'autorité de contrôle compétente.

Art. 24

§ 1er. Le registre visé à l'article 23 fait l'objet d'une gestion informatisée. Les modalités de la gestion et, en ce qui concerne les services de police, l'intégration des éléments provenant du registre établi par ceux-ci sont déterminées par le Roi.

§ 2. Sans préjudice de l'arrêté visé à l'article 57, § 3, le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis de l'autorité de contrôle compétente, les modalités et le caractère public, en tout ou en partie du registre.

Art. 25

§ 1. In uitvoering van artikel 37.4 van de Verordening wijst een particulier orgaan dat persoonsgegevens verwerkt voor rekening van een federale overheidsinstantie of federaal openbaar orgaan, of waaraan een federale overheidsinstantie of federaal openbaar orgaan persoonsgegevens doorgeeft, een functionaris voor gegevensbescherming aan.

§ 2. Naast de gevallen bedoeld in de eerste paragraaf en in artikel 37 van de Verordening, kan de wet de aanwijzing van een functionaris voor gegevensbescherming verplichten.

Art. 26

De federale overheidsinstantie of het federaal openbaar orgaan vraagt voorafgaand aan de verwerking het advies van de functionaris voor gegevensbescherming.

Wanneer de federale overheidsinstantie of het federaal openbaar orgaan doorgaat met de uitvoering van deze verwerking afwijkend van het advies gegeven door de functionaris voor gegevensbescherming, dan moet hij zijn beslissing motiveren.

De motivering moet de redenen aangeven voor het niet volgen van het advies of de aanbevelingen.

Art. 27

Op federaal niveau kan er een “expertengroep van de verwerkingsverantwoordelijken” opgericht worden die samengesteld is uit vertegenwoordigers van de federale overheidsinstanties en de federale openbare organen die dat wensen. De expertengroep kan bijgestaan worden door externe experten.

De expertengroep, bedoeld in het eerste lid, treedt op als overlegplatform in het kader van de ontwikkeling van het~~het~~ gegevensbeschermingsbeleid binnen de federale overheidsinstanties en de federale openbare instellingen overeenkomstig deze wet.

Deze expertengroep doet geen afbreuk aan de verplichtingen van elke federale overheidsinstantie en elk federaal openbaar orgaan als verantwoordelijke voor de verwerking of als verwerker.

Deze expertengroep kan zich op geen enkele wijze in de plaats stellen van de toezichthoudende autoriteiten waarnaar wordt verwezen in deze wet.

De Koning kan, bij een in Ministerraad overlegd besluit, de organisatorische en operationele modaliteiten van deze expertengroep bepalen.

Art. 25

§ 1er. En exécution de l’article 37.4 du Règlement, un organisme privé qui traite des données à caractère personnel pour le compte d’une autorité publique fédérale ou d’un organisme public fédéral ou à qui une autorité publique fédérale ou un organisme public fédéral a transféré des données à caractère personnel désignent un délégué à la protection des données.

§ 2. Outre les cas visés au paragraphe premier et à l’article 37 du Règlement, la loi peut exiger de désigner un délégué à la protection des données.

Art. 26

Préalablement au traitement, l’autorité publique fédérale ou l’organisme public fédéral demande l’avis du délégué à la protection des données.

Lorsque l’autorité publique fédérale ou l’organisme public fédéral poursuit la mise en œuvre de ce traitement en dérogation à l’avis donné par le délégué à la protection des données, il doit motiver sa décision.

La motivation doit indiquer les raisons du non-suivi de l’avis ou des recommandations.

Art. 27

Il peut être créé au niveau fédéral un “groupe d’experts des responsables de traitements” composé de représentants des autorités publiques fédérales et des organismes publics fédéraux qui le souhaitent. Le groupe d’experts peut se faire assister par des experts externes.

Le groupe d’experts visé à l’alinéa premier agit en tant que plateforme de concertation dans le cadre du développement de la politique relative à la protection des données au sein des autorités publiques fédérales et les organismes publics fédéraux conformément à la présente loi.

Ce groupe d’experts ne peut porter atteinte aux obligations de toute autorité publique fédérale et de tout organisme public fédéral en tant que responsable du traitement ou sous-traitant.

Ce groupe d’experts ne peut d’aucune manière se substituer aux autorités de contrôle dont il est fait référence dans la présente loi.

Le Roi peut, par arrêté délibéré en Conseil des ministres, déterminer les modalités d’organisation et de fonctionnement de ce groupe d’experts.

Art. 28

§ 1. De effectbeoordeling, bedoeld in artikel 35 van de Verordening, wordt onderworpen aan het advies van de functionaris voor gegevensbescherming.

§ 2. In uitvoering van artikel 35.10 van de Verordening moet een specifieke gegevensbeschermingseffectbeoordeling worden verricht vóór de verwerkingsactiviteit, ook al werd reeds een algemene gegevensbeschermingseffectbeoordeling uitgevoerd in het kader van de vaststelling van de rechtsgrond.

HOOFDSTUK V

Verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen

Art. 29

§ 1. Onder verwerking van persoonsgegevens voor journalistieke doeleinden wordt verstaan een verwerking die voornamelijk gericht is op het verzamelen, opstellen, voortbrengen of verspreiden van informatie van algemeen belang, met behulp van media, ten bate van het publiek.

§ 2. De artikelen 9 en 10 van de Verordening zijn niet van toepassing op verwerkingen van persoonsgegevens voor uitsluitend journalistieke, academische, artistieke of literaire doeleinden wanneer de verwerking betrekking heeft op persoonsgegevens die kennelijk publiek zijn gemaakt door de betrokkene of die in nauw verband staan met het publieke karakter van de betrokkene of van het feit waarin die persoon betrokken is.

§ 3. Artikel 11.2 van de Verordening is niet van toepassing op verwerkingen van de persoonsgegevens uitgevoerd enkel voor journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen wanneer de toepassing ervan tot één of meer van de volgende gevolgen zou leiden:

— door de toepassing wordt de verzameling van gegevens in het gevaar gebracht;

— door de toepassing wordt een voorgenomen publicatie in het gedrang gebracht;

— in verband met de verwerkingen voor journalistieke doeleinden, zou de toepassing aanwijzingen verschaffen over de bronnen van informatie.

§ 4. Artikelen 13 en 14 van de Verordening zijn niet van toepassing op verwerkingen van persoonsgegevens voor uitsluitend journalistieke, academische, artistieke of literaire doeleinden wanneer de toepassing ervan tot een of meer van de volgende gevolgen zou leiden:

— door de toepassing wordt de verzameling van gegevens in het gedrang gebracht;

Art. 28

§ 1er. L'analyse d'impact visée à l'article 35 du Règlement est soumise à l'avis du délégué à la protection des données.

§ 2. En exécution de l'article 35.10 du Règlement, une analyse d'impact spécifique de protection des données doit être effectuée avant l'activité de traitement, même si une analyse d'impact générale relative à la protection des données a déjà été réalisée dans le cadre de l'adoption de la base juridique.

CHAPITRE V

Traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire

Art. 29

§ 1er. On entend par traitement de données à caractère personnel aux fins de journalisme un traitement ayant comme finalité u la collecte, la rédaction, la production ou la diffusion d'informations d'intérêt général, par le biais de média, au profit du public.

§ 2. Les articles 9 et 10 du Règlement ne s'appliquent pas aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou sur des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée.

§ 3. L'article 11.2 du Règlement ne s'applique pas aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire lorsque son application aurait une ou plusieurs des conséquences suivantes:

— son application compromettrait la collecte des données;

— son application compromettrait une publication en projet;

— concernant les traitements aux fins journalistiques, son application fournirait des indications sur les sources d'information.

§ 4. Les articles 13 et 14 du Règlement ne s'appliquent pas aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire lorsque son application aurait une ou plusieurs des conséquences suivantes:

— son application compromettrait la collecte des données;

— door de toepassing wordt een voorgenomen publicatie in het gedrang gebracht;

— in verband met de verwerkingen voor journalistieke doeleinden, zou de toepassing aanwijzingen verschaffen over de bronnen van informatie.

§ 5. Artikel 15.1 van de Verordening is niet van toepassing op verwerkingen van persoonsgegevens voor uitsluitend journalistieke, academische, artistieke of literaire doeleinden wanneer de toepassing ervan tot een of meer van de volgende gevolgen zou leiden:

— door de toepassing wordt de verzameling van gegevens in het gedrang gebracht;

— door de toepassing wordt een voorgenomen publicatie in het gedrang gebracht;

— in verband met de verwerkingen voor journalistieke doeleinden, zou de toepassing aanwijzingen verschaffen over de journalistieke bronnen.

§ 6. Artikel 16 van de Verordening is niet van toepassing op verwerkingen van persoonsgegevens voor uitsluitend journalistieke, academische, artistieke of literaire doeleinden wanneer door de toepassing een voorgenomen publicatie in het gedrang wordt gebracht inzoverre de betrokkene beschikt over het recht om, na de publicatie, aanvullende verklaringen af te leggen en een soortgelijke publiciteit daarbij wordt verzekerd door de verwerkingsverantwoordelijke en de verwerker, tenzij de aanvullende verklaring beledigend zou zijn of in strijd met de wetten en de goede zeden.

§ 7. Artikel 18 van de Verordening is niet van toepassing op de verwerkingen voor journalistieke, academische, artistieke of literraire doeleinden wanneer door de toepassing een voorgenomen publicatie in het gedrang wordt gebracht.

§ 8. Artikel 21.1 van de Verordening is niet van toepassing op de verwerkingen voor journalistieke doeleinden.

§ 9. Artikelen 30.4, 31, 33 en 36 van de Verordening zijn niet van toepassing op de verwerkingen voor journalistieke, academische, artistieke of literaire doeleinden wanneer door de toepassing een voorgenomen publicatie in het gedrang wordt gebracht of wanneer de toepassing ervan een controlemaatregel voorafgaandelijk aan de publicatie van een artikel zou uitmaken.

§ 10. Artikelen 44 tot 50 van de Verordening zijn niet van toepassing op doorgiften van persoonsgegevens voor uitsluitend journalistieke, academische, artistieke of literaire doeleinden aan derde landen of internationale organisaties in de mate dat het nodig is om het recht op privacy te verzoenen met de regels betreffende de vrijheid van meningsuiting.

§ 11. Artikel 58 van de Verordening is niet van toepassing op verwerkingen van persoonsgegevens voor uitsluitend journalistieke, academische, artistieke of literaire doeleinden wanneer de toepassing aanwijzingen zou verschaffen over de

— son application compromettrait une publication en projet;

— concernant les traitements aux fins journalistiques, son application fournirait des indications sur les sources d'information.

§ 5. L'article 15.1 du Règlement ne s'applique pas aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire lorsque son application aurait une ou plusieurs des conséquences suivantes:

— son application compromettrait la collecte des données;

— son application copromettrait une publication en projet;

— concernant les traitements à des fins journalistiques, son application fournirait des indications sur les sources journalistiques.

§ 6. L'article 16 du Règlement ne s'applique pas aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire lorsque son application compromettrait une publication en projet pour autant que la personne concernée dispose, après publication, du droit de faire des déclarations complémentaires et qu'une publicité similaire y soit assurée par le responsable du traitement et le sous-traitant sauf dans la mesure où la déclaration complémentaire est injurieuse ou contraire aux lois et aux bonnes mœurs.

§ 7. L'article 18 du Règlement ne s'applique pas aux traitements à des fins de journalisme, académique, artistique ou littéraire lorsque son application compromettrait une publication en projet.

§ 8. L'article 21.1 du Règlement ne s'applique pas aux traitements à des fins de journalisme.

§ 9**.** Les articles 30.4, 31, 33 et 36 du Règlement ne s'appliquent pas aux traitements à des fins de journalisme, académique, artistique ou littéraire dans la mesure où son application compromettrait une publication en projet ou constituerait une mesure de contrôle préalable à la pubication d'un article.

§ 10. Les articles 44 à 50 du Règlement ne s'appliquent pas aux transferts de données à caractère personnel effectués aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire vers des pays tiers ou à des organisations internationales dans la mesure il est nécessaire pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

§ 11. L'article 58 du Règlement ne s'applique pas aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression universitaire, artistique ou littéraire lorsque son application fournirait des indications

bronnen van informatie of wanneer de toepassing ervan een controlemaatregel voorfafgaandelijk aan de publicatie van een artikel zou uitmaken.

TITEL 2

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid

HOOFDSTUK I

Algemene bepalingen

Art. 30

Deze titel voorziet in de omzetting van de richtlijn 2016/680/EU van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Art. 31

Voor de toepassing van deze titel wordt verstaan onder:

1. “persoonsgegevens”: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon – “de betrokkene”; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatiemiddel zoals een naam, een identificatienummer, locatiegegevens, een online identificatiemiddel of van èèn of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

2. “verwerking”: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, bekendmaking door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

sur les sources d’information ou constituerait une mesure de contrôle préalable à la publication d’un article.

TITRE 2

De la protection des personnes physiques à l’égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière ou d’exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces

CHAPITRE IER

Dispositions générales

Art. 30

Le présent titre transpose la directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière ou d’exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Art. 31

Pour l’application du présent titre, on entend par:

1. “données à caractère personnel”: toute information se rapportant à une personne physique identifiée ou identifiable, ci-après dénommée “personne concernée”; est réputée “identifiable” une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu’un nom, un numéro d’identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

2. “traitement”: toute opération ou tout ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l’enregistrement, l’organisation, la structuration, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l’interconnexion, la limitation, l’effacement ou la destruction.

3. “verwerkingsbeperking”: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken.

4. “profilering”: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling aspecten betreffende zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

5. “pseudonimisering”: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om te waarborgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

6. “bestand”: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

7. “bevoegde overheden”:

a) de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus;

b) de gerechtelijke overheden, te verstaan als de gemeenrechtelijke hoven en rechtbanken en het openbaar ministerie;

c) de Dienst Enquêtes van het Vast Comité van Toezicht op de politiediensten in het kader van zijn gerechtelijke opdrachten zoals bedoeld in artikel 16, 3e lid van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

d) de Algemene Inspectie van de federale politie en van de lokale politie zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten;

e) De Algemene administratie van de douane en accijnzen, in het kader van haar taak inzake opsporing, vaststelling en vervolging van de misdrijven die onder haar bevoegdheid vallen zoals bepaald in de Algemene Wet inzake douane en accijnzen van 18 juli 1977, en desgevallend in de Wet van 22 april 2003 houdende toekenning van de hoedanigheid van officier van gerechtelijke politie aan bepaalde ambtenaren van de administratie der douane en accijnzen.

f) de Passagiersinformatie-eenheid zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens;

3. “limitation du traitement”: le marquage de données à caractère personnel conservées en vue de limiter leur traitement futur.

4. “profilage”: toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

5. “pseudonymisation”: le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

6. “fichier”: tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

7. “autorités compétentes”:

a) les services de police au sens de l’article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

b) les autorités judiciaires, entendues comme les cours et tribunaux du droit commun et le ministère public;

c) le service d’enquêtes du Comité permanent de contrôle des services de police dans le cadre de ses missions judiciaires telles que prévues à l’article 16, alinéa 3, de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l’Organe de coordination pour l’analyse de la menace;

d) l’Inspection générale de la police fédérale et de la police locale, tel que visé à l’article 2 de la loi du 15 mai 2007 sur l’Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police;

e) l’Administration générale des douanes et accises, dans le cadre de sa mission relative à la recherche, la constatation et la poursuite des infractions déterminée par la Loi générale du 18 juillet 1977 sur les douanes et accises et, le cas échéant, par la Loi du 22 avril 2003 octroyant la qualité d’officier de police judiciaire à certains agents de l’Administration des douanes et accises.

f) l’Unité d’information des passagers, telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers;

g) de Cel voor financiële informatieverwerking bedoeld in artikel 76 van de wet van 18 septembre 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten.

8. “verwerkingsverantwoordelijke”: de bevoegde overheid die, alleen of samen met andere, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer de doeleinden van en de middelen voor die verwerking door of krachtens een wet, een decreet of een ordonnantie zijn bepaald, is de verwerkingsverantwoordelijke de entiteit die door of krachtens de wet, het decreet of de ordonnantie als de verwerkingsverantwoordelijke wordt aangewezen.

9. “verwerker”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat namens de verwerkingsverantwoordelijke of een andere verwerker persoonsgegevens verwerkt.

10. “ontvanger”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie ofwaaraan de persoonsgegevens worden bekendgemaakt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig de wet, het decreet of de ordonnantie, gelden echter niet als ontvangers; de verwerking van die persoonsgegevens door deze overheidsinstanties voldoet aan de toepasselijke regels inzake gegevensbescherming overeenkomstig de doeleinden van de verwerking.

11. “inbreuk op de beveiliging”: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

12. “genetische gegevens”: persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.

13. “biometrische gegevens”: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

14. “gezondheidsgegevens”: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, met inbegrip van de gegevens over verleende gezondheidsdiensten, waarmee informatie over zijn gezondheidstoestand wordt gegeven.

15. “toezichthoudende autoriteit”: de onafhankelijke overheidsinstantie die bij wet belast is met het toezicht op de

g) la Cellule de traitement des informations financières visée à l’article 76 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l’utilisation des espèces.

8. “responsable du traitement”: l’autorité compétente qui, seule ou conjointement avec d’autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens de ce traitement sont déterminés par la loi, le décret ou l’ordonnance , le responsable du traitement est l’entité désignée comme responsable du traitement par ou en vertu de cette loi, ce décret ou cette ordonnance.

9. “sous-traitant”: la personne physique ou morale, l’autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ou d’un autre sous-traitant.

10. “destinataire”: la personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu’il s’agisse ou non d’un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d’une mission d’enquête particulière conformément à la loi, au décret ou à l’ordonnance, ne sont pas considérées comme des destinataires; le traitement de ces données par ces autorités publiques est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

11. “brèche de sécurité”: une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l’altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d’une autre manière, ou l’accès non autorisé à de telles données.

12. “données génétiques”: les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d’une personne physique qui donnent des informations uniques sur la physiologie ou l’état de santé de cette personne physique et qui résultent, notamment, d’une analyse d’un échantillon biologique de la personne physique en question.

13. “données biométriques”: les données à caractère personnel résultant d’un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d’une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

14. “données concernant la santé”: les données à caractère personnel relatives à la santé physique ou mentale d’une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l’état de santé de cette personne.

15. “autorité de contrôle”: l’autorité publique indépendante chargée par la loi de surveiller l’application du présent titre,

toepassing van deze titel, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met verwerking te beschermen en het vrije verkeer van persoonsgegevens binnen de Europese Unie te vergemakkelijken.

16. "internationale organisatie": een organisatie en de daaronder vallende internationaal publiekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.

17. "internationale overeenkomst": een van kracht zijnde bilaterale of multilaterale internationale overeenkomst tussen lidstaten van de Europese Unie en derde landen op het gebied van justitiële samenwerking en/of politiële samenwerking.

Art. 32

Deze titel is van toepassing op de verwerkingen van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

HOOFDSTUK II

Beginselen van verwerking

Art. 33

De persoonsgegevens moeten:

a) rechtmatig en eerlijk worden verwerkt;

b) voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt;

c) toereikend, ter zake dienend en niet bovenmatig zijn in verhouding tot de doeleinden waarvoor zij worden verwerkt;

d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren;

e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt;

f) met gebruikmaking van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union européenne.

16. "organisation internationale": une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.

17. "accord international": tout accord international bilatéral ou multilatéral en vigueur entre les États membres de l'Union européenne et des pays tiers dans les domaines de la coopération judiciaire et/ou de la coopération policière.

Art. 32

Le présent titre s'applique aux traitements de données à caractère personnel effectués par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

CHAPITRE II

Principes de traitement

Art. 33

Les données à caractère personnel doivent être:

a) traitées de manière licite et loyale;

b) collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités;

c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées;

d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées;

f) traitées avec des mesures techniques et organisationnelles adéquates de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Art. 34

§ 1. Verdere verwerking door dezelfde of een andere verwerkingsverantwoordelijke voor een doeleinde vermeld in artikel 32, ander dan dat waarvoor de persoonsgegevens werden verzameld, is toegelaten voor zover:

a) de verwerkingsverantwoordelijke overeenkomstig de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst gemachtigd is deze persoonsgegevens voor een dergelijk doeleinde te verwerken; en

b) de verwerking noodzakelijk is en in verhouding staat overeenkomstig de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst.

§ 2. De persoonsgegevens kunnen niet verder verwerkt worden door dezelfde of een andere verwerkingsverantwoordelijke voor een ander doeleinde dan dat waarvoor de persoonsgegevens werden verzameld, indien dat doeleinde niet ondergebracht kan worden onder de doeleinden vermeld in artikel 27, tenzij deze verdere verwerking is toegestaan overeenkomstig de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst.

§ 3. Wanneer de wet, het decreet, de ordonnantie, de Europese regelgeving of een internationale overeenkomst specifieke voorwaarden oplegt voor de verwerking, stelt de bevoegde overheid die de gegevens doorzendt, de ontvanger van die persoonsgegevens in kennis van de voorwaarden en de verplichting om die na te leven.

§ 4. De bevoegde overheden die de gegevens doorzenden aan de ontvangers in de andere lidstaten van de Europese Unie, mogen geen bijkomende specifieke voorwaarden doen gelden dan degene die gelden voor de nationale gegevensdoorgifte.

§ 5. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van dit artikel en kan de naleving ervan aantonen.

Art. 35

De maximale bewaartermijn van de gegevens wordt bepaald in de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst dat de basis vormt voor de betrokken bewaring. Na afloop van die termijn worden de gegevens gewist.

In afwijking van het eerste lid, kan de wet, het decreet, de ordonnantie, de Europese regelgeving, of de internationale overeenkomst voorzien dat na afloop van een eerste bewaartermijn een analyse moet worden uitgevoerd op basis van verschillende noodzakelijkheids- en proportionaliteitscriteria om te bepalen of het nodig is dat de gegevens bewaard blijven, en in voorkomend geval, de nieuwe bewaartermijn.

In dat geval voorziet de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst een maximale bewaartermijn.

Art. 34

§ 1er. Le traitement ultérieur, par le même ou par un autre responsable du traitement, pour l'une des finalités énoncées à l'article 32, autre que celles pour lesquelles les données ont été collectées, est autorisé aux conditions suivantes:

a) le responsable du traitement est autorisé à traiter ces données à caractère personnel pour une telle finalité conformément à la loi, au décret ou à l'ordonnance, au droit de l'Union européene et à la convention internationale; et

b) le traitement est nécessaire et proportionné conformément, à la loi, au décret ou à l'ordonnance au droit de l'Union européene et à la convention internationale.

§ 2. Les données à caractère personnel ne peuvent pas être traitées par le même ou un autre responsable du traitement à d'autres fins que celles pour lesquelles les données à caractère personnel ont été collectées, et non comprises dans les finalités énoncées à l'article 32, à moins que cette finalité ne soit permise conformément à la loi, le décret, l'ordonnance, le droit de l'Union européenne et à la convention internationale.

§ 3. Lorsque la loi, le décret, l'ordonnance, le droit de l'Union européene ou une convention internationale, soumet le traitement à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter.

§ 4. Les autorités compétentes qui transmettent les données aux destinataires dans les autres États membres de l'Union européenne ne peuvent faire appliquer des conditions spécifiques supplémentaires de celles applicables aux transferts nationaux.

§ 5. Le responsable du traitement est responsable du respect du présent article et est en mesure de le démontrer.

Art. 35

La durée maximale de conservation des données est déterminée dans la loi, le décret, l'ordonnance, le droit de l'Union européenne ou la convention internationale qui est à la base de la conservation concernée. A l'échéance de cette durée, les données sont effacées.

Par dérogation à l'alinéa premier , la loi, le décret ou l'ordonnance, le droit de l'Union européenne, la convention internationale peut prévoir qu'à l'échéance d'un premier délai de conservation, une analyse soit effectuée sur base de différents critères de nécessité et de proportionnalité afin de déterminer si la conservation des données doit être maintenue et, le cas échéant, le nouveau délai de conservation.

Dans ce cas, la loi, le décret ou l'ordonnance, le droit de l'Union européenne, ou la convention internationale prévoit un délai maximum de conservation.

Art. 36

De verwerkingsverantwoordelijke maakt in voorkomend geval en voor zover mogelijk een duidelijk onderscheid tussen persoonsgegevens betreffende verschillende categorieën van betrokkenen, zoals:

a) personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;

b) personen die voor een strafbaar feit zijn veroordeeld;

c) slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit;

d) andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld in a) en b).

Art. 37

§ 1. Persoonsgegevens die op feiten zijn gebaseerd, worden voor zover mogelijk onderscheiden van persoonsgegevens die op een persoonlijk oordeel zijn gebaseerd.

§ 2. De bevoegde overheden nemen alle redelijke maatregelen om ervoor te zorgen dat persoonsgegevens die onjuist, onvolledig of niet meer actueel zijn, niet worden doorgezonden of beschikbaar worden gesteld. Daartoe controleert iedere bevoegde overheid, voor zover mogelijk, de kwaliteit van de persoonsgegevens voordat de gegevens worden doorgezonden of beschikbaar worden gesteld.

Voor zover mogelijk wordt bij de doorzending van persoonsgegevens te allen tijde de noodzakelijke aanvullende informatie worden toegevoegd aan de hand waarvan de ontvangende bevoegde overheid de mate van juistheid, volledigheid en betrouwbaarheid van persoonsgegevens kan beoordelen, alsmede de mate waarin ze actueel zijn.

§ 3. Indien blijkt dat onjuiste persoonsgegevens zijn doorgezonden, of dat de persoonsgegevens op onrechtmatige wijze zijn doorgezonden, wordt de ontvanger daarvan onverwijld in kennis gesteld. In dat geval worden de persoonsgegevens gerectificeerd of gewist, of wordt de verwerking beperkt overeenkomstig artikel 44.

Art. 36

Le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que:

a) les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale;

b) les personnes reconnues coupables d'une infraction pénale;

c) les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale;

d) les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux points a) et b).

Art. 37

§ 1er. Les données à caractère personnel fondées sur des faits sont dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles.

§ 2. Les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour ne soient pas transmises ou mises à disposition. À cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition.

Dans la mesure du possible, lors de toute transmission de données à caractère personnel, sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à caractère personnel, et de leur niveau de mise à jour.

§ 3. S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 44.

Art. 38

§ 1. De verwerking is rechtmatig indien:

a) ze noodzakelijk is voor de uitvoering van een opdracht uitgevoerd door een overheid bevoegd voor de in artikel 32, bedoelde doeleinden, en

b) ze gebaseerd is op een wettelijke of reglementaire verplichting.

§ 2. De wettelijke verplichting verduidelijkt ten minste de categorieën van persoonsgegevens die verwerkt moeten worden en de doeleinden van de verwerking.

Art. 39

§ 1. Verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid of gegevens over seksueel gedrag of seksuele gerichtheid van een natuurlijke persoon zijn slechts toegelaten wanneer de verwerking strikt noodzakelijk is en geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene, en enkel in een van de volgende gevallen:

a) wanneer de verwerking door de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst is toegestaan;

b) wanneer de verwerking noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een andere fysieke persoon;

c) wanneer de verwerking betrekking heeft op gegevens die kennelijk openbaar zijn gemaakt door de betrokkene.

§ 2. De passende waarborgen zoals bedoeld in de eerste paragraaf moeten ten minste voorzien dat de bevoegde overheid of de verwerkingsverantwoordelijke een lijst van de categorieën van personen die de persoonsgegevens kunnen raadplegen opstelt, met een beschrijving van hun hoedanigheid ten opzichte van de verwerking van de beoogde gegevens. Deze lijst wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit.

De bevoegde overheid waak erover dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.

Art. 40

§ 1. Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten, met inbegrip van profilering, die voor

Art. 38

§ 1er. Le traitement est licite si:

a) il est nécessaire à l'exécution d'une mission effectuée par l'autorité compétente pour les finalités énoncées à l'article 32, et

b) s'il est fondé sur une obligation légale ou réglementaire.

§ 2. L'obligation légale précise au moins, les catégories de données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement.

Art. 39

§ 1er. Le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, n'est autorisé qu'en cas de stricte nécessité et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement dans l'un des cas suivants:

a) lorsque le traitement est autorisé par la loi, le décret, l'ordonnance, le droit de l'Union européenne ou la convention internationale;

b) lorsque le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne physique;

c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

§ 2. Les garanties nécessaires visées au paragraphe premier doivent au moins prévoir que l'autorité compétente ou le responsable de traitement établisse une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l'autorité de contrôle compétente.

L'autorité compétente veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Art. 40

§ 1er. Toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des

de betrokkene nadelige rechtsgevolgen hebben of hem in aanmerkelijke mate treffen, zijn toegestaan als een wet, een decreet, een ordonnantie, de Europese regelgeving of een internationale overeenkomst voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkene, met inbegrip van ten minste het recht op menselijke interventie van de verwerkingsverantwoordelijke.

§ 2. Profilering die leidt tot discriminatie van natuurlijke personen op grond van de in artikel 39 bedoelde bijzondere categorieën van persoonsgegevens, is verboden.

HOOFDSTUK III

Rechten van de betrokkene

Art. 41

§ 1. De verwerkingsverantwoordelijke neemt passende maatregelen om de in artikel 42 bedoelde informatie te verstrekken en mededelingen te doen bedoeld in de artikelen 40, 43 tot 46 en artikel 64 in een beknopte, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. De informatie wordt schriftelijk of met andere middelen, met inbegrip van elektronische middelen, verstrekt.

§ 2. De verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene waarop de artikelen 40 en 43 tot 46 betrekking hebben.

§ 3. De verwerkingsverantwoordelijke of de toezichthoudende autoriteit, in het geval bedoeld in artikel 45, informeert de betrokkene schriftelijk, zonder onnodige vertraging met betrekking tot het gevolg dat werd gegeven aan zijn verzoek.

§ 4. Eenieder heeft het recht om kosteloos de informatie bedoeld in artikel 42, te verkrijgen en de maatregelen bedoeld in de artikelen 40, 43 tot 46 en 64, te laten nemen. Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de verwerkingsverantwoordelijke ofwel:

a) een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het nemen van de gevraagde maatregelen gepaard gaan; ofwel

b) weigeren gevolg te geven aan het verzoek.

Het is aan de verwerkingsverantwoordelijke om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

§ 5. Wanneer de verwerkingsverantwoordelijke redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het in artikel 43 of 44 bedoelde verzoek indient, kan hij om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est autorisé si une loi, un décret, une ordonnance, le droit de l'Union européenne ou une convention internationale fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement.

§ 2. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 39 est interdit.

CHAPITRE III

Droits de la personne concernée

Art. 41

§ 1er. Le responsable du traitement prend des mesures appropriées pour fournir toute information visée à l'article 42 ainsi que pour procéder à toute communication au titre des articles 40, 43 à 46 et de l'article 64 d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par écrit ou par d'autres moyens y compris, par voie électronique.

§ 2. Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée par les articles 40 et 43 à 46.

§ 3. Le responsable du traitement, ou l'autorité de contrôle dans le cas visé à l'article 45, informe par écrit, dans les meilleurs délais, la personne concernée des suites données à sa demande.

§ 4**.** Toute personne a le droit d'obtenir sans frais les informations visées à l'article 42 ainsi que toute mesure au titre des articles 40, 43 à 46 et 64. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut:

a) exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées; ou

b) refuser de donner suite à la demande.

Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

§ 5. Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée à l'article 43 ou 44, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

Art. 42

§ 1. Teneinde de betrokkene de mogelijkheid te bieden zijn recht op informatie uit te oefenen, stelt de verwerkingsverantwoordelijke de betrokkene de volgende informatie ter beschikking:

a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke;

b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;

c) de doeleinden van de verwerking;

d) het bestaan van het recht om klacht in te dienen bij de toezichthoudende autoriteit, en de contactgegevens van voornoemde autoriteit;

e) het bestaan van het recht de verwerkingsverantwoordelijke te verzoeken om toegang tot en rectificatie of wissing van hem betreffende persoonsgegevens, en beperking van de verwerking van hem betreffende persoonsgegevens;

f) de rechtsgrond van de verwerking;

g) de termijn gedurende welke de persoonsgegevens zullen worden bewaard, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

h) in voorkomend geval, de categorieën van ontvangers van de persoonsgegevens;

i) indien noodzakelijk, bijkomende informatie, in het bijzonder wanneer de persoonsgegevens zonder medeweten van de betrokkene worden verzameld.

§ 2. De in de eerste paragraaf bedoelde informatie kan bij wet worden uitgesteld of beperkt dan wel achterwege worden gelaten, voor zover een dergelijke maatregel in een democratische samenleving, met naar behoren inachtneming van de fundamentele rechten en de legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

a) belemmering van strafrechtelijke of andere gereglementeerde onderzoeken, opsporingen of procedures te voorkomen;

b) nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

c) de openbare veiligheid te beschermen;

d) de nationale veiligheid te beschermen;

e) de rechten en vrijheden van anderen te beschermen.

§ 3. De wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst kan bepalen

Art. 42

§ 1er. Afin de permettre à la personne concernée d'exercer son droit à l'information, le responsable du traitement met à la disposition de la personne concernée les informations suivantes:

a) l'identité et les coordonnées du responsable du traitement;

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement;

d) le droit d'introduire une plainte auprès de l'autorité de contrôle et les coordonnées de ladite autorité;

e) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel le concernant;

f) la base juridique du traitement;

g) la durée de conservation des données à caractère personnel ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée;

h) le cas échéant, les catégories de destinataires des données à caractère personnel;

i) si besoin est, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.

§ 2. L'information visée au paragraphe premier, peut être retardée, limitée ou exclue par la loi dès lors qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour:

a) éviter de gêner des enquêtes, des recherches, des procédures pénales ou autres procédures réglementées;

b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

c) protéger la sécurité publique;

d) protéger la sécurité nationale;

e) protéger les droits et libertés d'autrui.

§ 3. La loi, le décret, l'ordonnance, le droit de l'Union européenne ou la convention internationale peut déterminer des

welke verwerkingscategorieën geheel of gedeeltelijk onder één van de punten opgesomd in paragraaf 2 kunnen vallen.

§ 4. De rechten geviseerd in dit hoofdstuk voor wat betreft de gegevensverwerking van de hoven en rechtbanken van het gemeen recht en het openbaar ministerie worden uitsluitend uitgeoefend binnen de grenzen en in het kader van de regels en modaliteiten verduidelijkt in het Gerechtelijk Wetboek, het wetboek van Strafvordering en de bijzondere wetten.

Art. 43

§ 1. Teneinde de betrokkene de mogelijkheid te bieden zijn recht op verzoek tot toegang tot zijn persoonsgegevens uit te oefenen, stelt de verwerkingsverantwoordelijke de betrokkene de volgende informatie ter beschikking:

a) de bevestiging dat de hem betreffende persoonsgegevens al dan niet worden verwerkt en toegang tot die persoonsgegevens;

b) de doeleinden en de rechtsgrond van de verwerking;

c) de betreffende categorieën van persoonsgegevens;

d) de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn bekendgemaakt;

e) de bewaartermijn, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

f) dat hij het recht heeft van de verwerkingsverantwoordelijke de rectificatie of wissing van hem betreffende persoonsgegevens of beperking van verwerking van hem betreffende persoonsgegevens te vragen;

g) dat hij het recht heeft klacht in te dienen bij de toezichthoudende autoriteit, en de contactgegevens van deze autoriteit;

h) de persoonsgegevens die worden verwerkt, en alle beschikbare informatie over de oorsprong van die gegevens.

§ 2. De wet, het decreet of de ordonnantie kan het inzagerecht van de betrokkene geheel of gedeeltelijk beperken, voor zover en zolang die volledige of gedeeltelijke beperking in een democratische samenleving, met inachtneming van de grondrechten en legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

a) belemmering van strafrechtelijke of andere gereglementeerde onderzoeken, opsporingen of procedures te voorkomen;

b) nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

catégories de traitements susceptibles de relever, dans leur intégralité ou en partie, d'un quelconque des points énumérés au paragraphe 2.

§ 4. Les droits visés dans ce chapitre pour ce qui concernent les traitements de données des cours et tribunaux du droit commun et le ministère public sont exercés exclusivement dans les limites et dans le cadre des règles et des modalités précisées dans le Code judiciaire, le Code d'instruction criminelle et les lois particulières.

Art. 43

§ 1er. Afin de permettre à la personne concernée de demander l'accès à ses données personnelles, le responsable du traitement met à la disposition de la personne concernée, les informations suivantes:

a) la confirmation que des données la concernant sont ou ne sont pas traitées ainsi que l'accès à ces données;

b) les finalités du traitement ainsi que sa base juridique;

c) les catégories de données à caractère personnel concernées;

d) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées;

e) la durée de conservation ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée;

f) l'existence du droit de demander au responsable du traitement, la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement des données à caractère personnel relatives à la personne concernée;

g) le droit d'introduire une plainte auprès de l'autorité de contrôle et les coordonnées de cette autorité;

h) la communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source.

§ 2. La loi, le décret ou l'ordonnance peut limiter entièrement ou partiellement, le droit d'accès de la personne concernée, dès lors et aussi longtemps qu'une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour:

a) éviter de gêner des enquêtes, des recherches, des procédures pénales ou autres procédures réglementées;

b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

c) de openbare veiligheid te beschermen;

d) de nationale veiligheid te beschermen;

e) de rechten en vrijheden van anderen te beschermen.

§ 3. In de in de paragrafen 2 en 3 bedoelde gevallen schrijft de wet, het decreet of de ordonnantie voor dat de verwerkingsverantwoordelijke de betrokkene zonder onnodige vertraging schriftelijk in kennis moet stellen van een eventuele weigering of beperking van de inzage en van de redenen voor die weigering of beperking. Die informatie kan achterwege worden gelaten wanneer de verstrekking daarvan een van de doeleinden van paragraaf 2 zou ondermijnen. De wet, het decreet of de ordonnantie schrijft voor dat de verwerkingsverantwoordelijke de betrokkene moet inlichten over de mogelijkheid om klacht in te dienen bij de bevoegde toezichthoudende instantie of om een beroep in te stellen bij de rechter.

§ 4. De wet, het decreet of de ordonnantie bepaalt dat de verwerkingsverantwoordelijke de feitelijke of juridische redenen die aan het besluit ten grondslag liggen, documenteert. Die informatie wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Art. 44

§ 1. De betrokkene heeft het recht om zonder onnodige vertraging van de verwerkingsverantwoordelijke de rectificatie en eventueel de aanvulling te verkrijgen van hem betreffende onjuiste persoonsgegevens.

§ 2. De verwerkingsverantwoordelijke wist de persoonsgegevens zonder onnodige vertraging wanneer de verwerking indruist tegen de bepalingen goedgekeurd krachtens artikelen 33, 34, 38 of 39 of wanneer de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting waaraan de verwerkingsverantwoordelijke gehouden is.

§ 3. In plaats van tot wissing over te gaan, mag de verwerkingsverantwoordelijke de verwerking beperken wanneer:

a) de juistheid van de persoonsgegevens door de betrokkene wordt betwist en niet kan worden geverifieerd of de gegevens al dan niet juist zijn; of

b) de persoonsgegevens als bewijsmateriaal moeten worden bewaard.

Wanneer de verwerking op grond van punt a) van het eerste lid wordt beperkt, informeert de verwerkingsverantwoordelijke de betrokkene alvorens de verwerkingsbeperking op te heffen.

§ 4. De verwerkingsverantwoordelijke stelt de betrokkene schriftelijk in kennis van een eventuele weigering tot rectificatie of wissing van persoonsgegevens of verwerkingsbeperking, en van de redenen voor die weigering. De hierboven bedoelde informatie kan bij wet, decreet of ordonnantie, worden beperkt, voor zover een dergelijke verwerkingsbeperking in een democratische samenleving, met inachtneming van de

c) protéger la sécurité publique;

d) protéger la sécurité nationale;

e) protéger les droits et libertés d'autrui.

§ 3. Dans les cas visés aux paragraphes 2 et 3, la loi, le décret ou l'ordonnance prévoit que le responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au paragraphe 2. La loi, le décret ou l'ordonnance prévoit que le responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel.

§ 4. La loi, le décret ou l'ordonnance prévoit que le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition de l'autorité de contrôle compétente.

Art. 44

§ 1er. La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification, et éventuellement la complétude, des données à caractère personnel la concernant qui sont inexactes.

§ 2. Le responsable du traitement efface dans les meilleurs délais les données à caractère personnel lorsque le traitement constitue une violation des dispositions adoptées en vertu des articles 33, 34, 38 ou 39 ou lorsque les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

§ 3. Au lieu de procéder à l'effacement, le responsable du traitement peut limiter le traitement lorsque:

a) l'exactitude des données à caractère personnel est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non; ou

b) les données à caractère personnel doivent être conservées à des fins probatoires.

Lorsque le traitement est limité en vertu du premier alinéa, point a), le responsable du traitement informe la personne concernée avant de lever la limitation du traitement.

§ 4. Le responsable du traitement informe la personne concernée par écrit de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus. L'information visée ci-dessus, peut être limitée par la loi, le décret, ou l'ordonnance, dès lors qu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant

grondrechten en legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

a) belemmering van strafrechtelijke of andere gereglementeerde onderzoeken, opsporingen of procedures te voorkomen;

b) nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

c) de openbare veiligheid te beschermen;

d) de nationale veiligheid te beschermen;

e) de rechten en vrijheden van anderen te beschermen.

De verwerkingsverantwoordelijke licht de betrokkene in over de mogelijkheid om klacht in te dienen bij de bevoegde toezichthoudende autoriteit of om beroep in rechte in te stellen.

§ 5. De verwerkingsverantwoordelijke deelt de rectificatie van de onjuiste persoonsgegevens mee aan de overheid van wie de onjuiste persoonsgegevens afkomstig zijn.

§ 6. In geval van rectificatie, wissing of verwerkingsbeperking bedoeld in paragrafen 1, 2 en 3, stelt de verwerkingsverantwoordelijke de ontvangers daarvan in kennis, en rectificeren of wissen de ontvangers de persoonsgegevens of beperken ze de onder hun bevoegdheid vallende verwerking van persoonsgegevens.

Art. 45

De verwerkingsverantwoordelijke die een verzoek ontvangt om een recht uit te oefenen bedoeld in de artikelen 41 tot 44 van deze titel, bezorgt de verzoeker onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek een gedagtekende ontvangstbevestiging.

Art. 46

§ 1. In de in artikel 42, § 2, artikel 43, § 4, artikel 44, § 4, en artikel 64, § 1, bedoelde gevallen, kan de wet, het decreet of de ordonnantie, voorzien dat de rechten van de betrokkene via de bevoegde toezichthoudende autoriteit worden uitgeoefend, met respect voor de de principes van noozakelijkheid en proportionaliteit in een democratische samenleving.

§ 2. In het geval bedoeld in de eerste paragraaf stelt de verwerkingsverantwoordelijke de betrokkene ervan in kennis dat hij zijn rechten via de bevoegde toezichthoudende autoriteit uitoefent.

§ 3. In het geval bedoeld in de eerste paragraaf, dient de betrokkene het verzoek om zijn rechten uit te oefenen in bij de bevoegde toezichthoudende autoriteit.

dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour:

a) éviter de gêner des enquêtes, des recherches, des procédures pénales ou autres procédures réglementées;

b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

c) protéger la sécurité publique;

d) protéger la sécurité nationale;

e) protéger les droits et libertés d'autrui.

Le responsable du traitement informe la personne concernée des possibilités d'introduire une plainte auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel.

§ 5. Le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité dont proviennent les données à caractère personnel inexactes.

§ 6. En cas de rectification, effacement ou de limitation de traitement tel que visés aux paragraphes 1, 2 et 3, le responsable du traitement adresse une notification aux destinataires afin que ceux-ci rectifient ou effacent les données à caractère personnel ou limitent le traitement des données à caractère personnel sous leur responsabilité.

Art. 45

Le responsable du traitement qui reçoit une demande d'exercer un droit visé aux articles 41 à 44 du présent titre délivre dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande un accusé de réception daté à l'auteur de la demande.

Art. 46

§ 1er. Dans les cas visés à l'article 42, § 2, à l'article 43, § 4, à l'article 44, § 4, et à l'article 64, § 1er, la loi, le décret ou l'ordonnance, peut prévoir que les droits de la personne concernée sont exercés par l'intermédiaire de l'autorité de contrôle compétente, dans le respect des principes de nécessité et de proportionnalité dans une société démocratique.

§ 2. Dans le cas visé au paragraphe premier, le responsable du traitement informe la personne concernée qu'elle exerce ses droits par l'intermédiaire de l'autorité de contrôle compétente.

§ 3. Dans le cas visé au paragraphe premier, la demande d'exercer ses droits est introduite par la personne concernée auprès de l'autorité de contrôle compétente.

§ 4. Voor wat betreft de politiediensten, in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus, worden de rechten van de betrokkene, bedoeld in dit hoofdstuk uitgeoefend door de bevoegde toezichthoudende autoriteit.

Deze deelt uitsluitend aan de betrokkene mede dat de nodige verificaties werden verricht.

In afwijking van lid 2 kan de bevoegde toezichthoudende autoriteit aan de betrokkene bepaalde contextuele informatie verstrekken.

De bevoegde ministers voor de politie bepalen bij richtlijn, na advies van de bevoegde toezichthoudende autoriteit, de categorieën van contextuele informatie die door de bevoegde toezichthoudende autoriteit aan de betrokkene kunnen worden medegedeeld.

§ 5. Voor wat betreft de gegevensverwerkingen van de douanediensten bedoeld in artikel 31, 7°, e), en de Cel voor financiële informatieverwerking bedoeld in artikel 31, 7°, g), worden de rechten van de betrokkene zoals bedoeld in dit hoofdstuk uitgeoefend door de bevoegde toezichthoudende autoriteit.

Deze deelt uitsluitend aan de betrokkene mede dat de nodige verificaties werden verricht.

In afwijking van lid 2 kan de bevoegde toezichthoudend autoriteit aan de betrokkene bepaalde contextuele informatie verstrekken.

De bevoegde ministers bepalen bij richtlijn, nadat eerder door de bevoegde toezichthoudende autoriteit een advies is uitgebracht, de categorieën van contextuele informatie die via de bevoegde toezichthoudende autoriteit aan de betrokkene kunnen worden meede gedeeld.

Art. 47

Wanneer de persoonsgegevens in een rechterlijke beslissing of een gerechtelijk dossier zijn opgenomen of in het kader van strafrechtelijke onderzoeken en procedures worden verwerkt, worden de in de artikelen 42, 43, § 1 en 44 bedoelde rechten uitgeoefend overeenkomstig het Gerechtelijk wetboek en het wetboek van Strafvordering.

Art. 48

De betrokkene geniet met betrekking tot de verwerking van zijn persoonsgegevens die rechtstreeks of onrechtstreeks afkomstig zijn van overheden bedoeld in titel 3 van deze wet, niet van de rechten bedoeld in de artikelen 41 tot 47 en 64 betreffende deze gegevens met betrekking tot de verwerkingsverantwoordelijken en de bevoegde overheden bedoeld in deze titel naar wie deze gegevens werden overgebracht.

§ 4. Pour ce qui concerne les services de police, au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant la police intégrée, structurée à deux niveaux, les droits des personnes concernées visées au présent chapitre sont exercés via l'autorité de contrôle compétente.

Celle-ci communique uniquement à la personne concernée qu'il a été procédé aux vérifications nécessaires.

Par dérogation à l'alinéa 2, l'autorité de contrôle compétente peut communiquer à la personne concernée certaines informations contextuelles.

Les ministres compétents pour la police déterminent par directive, après avis de l'autorité de contrôle compétente, les catégories d'informations contextuelles qui peuvent être communiquées à la personne concernée, par l'autorité de contrôle compétente.

§ 5. Pour ce qui concerne les traitements des services de douanes visés à l'article 31, 7°, e), et la Cellule de traitement des informations financières visée à l'article 31, 7°, g), les droits des personnes concernées visés au présent chapitre sont exercés via l'autorité de contrôle compétente.

Celle-ci communique uniquement à la personne concernée qu'il a été procédé aux vérifications nécessaires.

Par dérogation à l'alinéa 2, l'autorité de contrôle compétente peut communiquer à la personne concernée certaines informations contextuelles.

Les ministres compétents déterminent par directive, ayant préalablement fait l'objet d'un avis de l'autorité de contrôle compétente, les catégories d'informations contextuelles qui peuvent être communiquées à la personne concernée, via l'autorité de contrôle compétente.

Art. 47

Lorsque les données à caractère personnel figurent dans une décision judiciaire ou un dossier judiciaire, ou faisant l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale, les droits visés aux articles 42, 43, § 1er, et 44 sont exercés conformément au Code judiciaire et au Code d'instruction criminelle.

Art. 48

La personne concernée par le traitement de ses données à caractère personnel, émanant directement ou indirectement des autorités visées au titre 3 de la présente loi ne bénéfice pas des droits visés aux articles 41 à 47 et 64 concernant ces données à l'égard des responsables du traitement et des autorités compétentes visées dans le présent titre auxquelles ces données ont été transmises.

De verplichtingen bedoeld in de artikelen 41 tot 47 en 64 zijn niet van toepassing op de verwerkingsverantwoordelijken of op de bevoegde overheden die in het bezit zijn van deze gegevens.

De verwerkingsverantwoordelijke of de bevoegde overheid bedoeld in deze titel die in het bezit is van zulke gegevens deelt deze niet mee aan de betrokkene tenzij:

1. de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2. de betrokken overheid bedoeld in titel 3 hem dit toestaat.

De verwerkingsverantwoordelijke of de bevoegde overheid deelt niet mee dat hij of zij in het bezit is van gegevens die van overheden bedoeld in titel 3 afkomstig zijn.

De beperkingen bedoeld in het eerste lid hebben eveneens betrekking op het logbestand van de verwerkingen van een overheid bedoeld in titel 3 van deze wet in de gegevensbanken van de verwerkingsverantwoordelijken en van de bevoegde overheden bedoeld in deze titel waartoe de overheid bedoeld in titel 3 rechtstreeks toegang heeft.

Art. 49

Een verwerkingsverantwoordelijke of een bevoegde overheid bedoeld in deze titel die persoonsgegevens meedeelt aan een overheid bedoeld in titel 3 van deze wet is niet onderworpen aan de artikelen 42, § 1, h), en 43, § 1, d), en mag de betrokkene niet van deze overdracht op de hoogte brengen.

De algemene informatie over de samenwerking tussen de overheden bedoeld in titel 3 en de bevoegde overheden bedoeld in artikel 31,7° worden niet beoogd door deze bepaling.

Art. 50

Wanneer een overheid bedoeld in titel 3 van deze wet over een rechtstreekse toegang of over een rechtstreekse bevraging van een gegevensbank van de openbare of private sector beschikt, worden zijn verwerkingen van persoonsgegevens in deze gegevensbank beschermd door technische, organisatorische en persoonlijke beveiligingsmaatregelen zodat alleen de volgende actoren toegang kunnen hebben tot de inhoud van deze verwerkingen om hun wettelijke toezichtsopdrachten uit te voeren:

a) de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke van de gegevensbank of de persoon die hij daartoe machtigt;

b) de functionaris voor gegevensbescherming van de overheid bedoeld in titel 3;

c) de verwerkingsverantwoordelijke van de gegevensbank of de persoon die hij daartoe machtigt;

Les obligations visées aux articles 41 à 47 et 64 ne s'appliquent pas aux responsables du traitement ou aux autorités compétentes en possession de ces données.

Le responsable du traitement ou l'autorité compétente visé dans le présent titre qui est en possession de telles données ne les communique pas à la personne concernée à moins que:

1. la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que

2. l'autorité visée au titre 3 concernée ne l'y autorise.

Le responsable du traitement ou l'autorité compétente ne fait aucune mention qu'il ou elle est en possession de données émanant des autorités visées au titre 3.

Les limitations visées à l'alinéa premier porte également sur la journalisation des traitements d'une autorité visée dans le titre 3 de la présente loi dans les banques de données des responsables du traitement et des autorités compétentes visés par le présent titre, auxquelles l'autorité visée au titre 3 a directement accès.

Art. 49

Un responsable du traitement ou une autorité compétente visés dans le présent titre qui communique des données à caractère personnel à une autorité visée au titre 3 de la présente loi, n'est pas soumis aux articles 42, § 1er, h), et 43, § 1er, d), et ne peut informer la personne concernée de cette transmission.

Les informations générales sur la collaboration entre les autorités visées au titre 3 et les autorités compétentes visées à l'article 31, 7°, ne sont pas visées par cette disposition.

Art. 50

Lorsqu'une autorité visée au titre 3 de la présente loi dispose d'un accès direct ou d'une interrogation directe à une banque de données du secteur public, ses traitements de données à caractère personnel dans cette banque de données sont protégés par des mesures de sécurité techniques, organisationnelles et personnelles de sorte que seuls les acteurs suivants puissent accéder au contenu de ces traitements pour assurer leurs missions légales de contrôle:

a) le délégué à la protection des données du responsable du traitement de la banque de donnée ou la personne qu'il délègue à cet effet;

b) le délégué à la protection des données de l'autorité visée au titre 3;

c) le responsable du traitement de la banque de données ou la personne qu'il délègue à cet effet;

d) de verwerkingsverantwoordelijke van de overheid bedoeld in titel 3;

e) elke andere persoon bepaald in een protocol tussen de verwerkingsverantwoordelijken.

Deze beveiligingsmaatregelen zijn bedoeld om de wettelijke verplichtingen met betrekking tot de bescherming van bronnen, de bescherming van de identiteit van de agenten en de discretie van de onderzoeken van de overheden bedoeld in titel 3 te beschermen.

Deze verwerkingen mogen enkel toegankelijk zijn voor andere doeleinden die verband houden met het toezicht en slechts op basis van een protocolakkoord tussen de betrokken verwerkingsverantwoordelijken.

Het controlesysteem wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

De betrokken overheid bedoeld in titel 3 kan afwijken van het eerste lid wanneer hij van oordeel is dat de toepassing op een bepaalde gegevensbank niet relevant is.

Art. 51

§ 1. De persoon die betrokken is bij een gemeenschappelijke behandeling van zijn persoonsgegevens, rechtstreeks of onrechtstreeks afkomstig van ten minste één bevoegde autoriteit van titel 2 of ten minste één autoriteit, één dienst of orgaan bedoeld in titel 3, voor wat zijn gegevens bij de verantwoordelijken voor de verwerking betreft, geniet niet van de in de artikelen 41 tot 47 et 64 genoemde rechten, waarnaar wordt verwezen.

§ 2. De in de artikelen 41 tot 47 en 64 bedoelde verplichtingen zijn niet van toepassing op de autoriteiten, personen of verantwoordelijken voor de verwerking, die over de in de eerste paragraaf bedoelde gegevens beschikken.

§ 3. De verwerkingsverantwoordelijke bedoeld in deze titel die in het bezit is van zulke gegevens bedoeld in de eerste paragraaf, deelt deze niet mee aan de betrokkene tenzij:

1. de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2. de verantwoordelijke of verantwoordelijken voor de gemeenschappelijke verwerking hem dit toestaat.

§ 4. De verantwoordelijke of verantwoordelijken voor de gemeenschappelijke verwerking doen geen enkele melding aan de betrokkene dat hij in het bezit is van gegevens die afkomstig zijn van de gemeenschappelijke verwerking.

§ 5. De beperkingen bedoeld in de eerste paragraaf hebben eveneens betrekking op de dagdagelijkse verwerking van de gemeenschappelijke verwerking.

d) le responsable du traitement de l'autorité visée au titre 3;

e) toute autre personne précisée dans un protocole entre les responsables du traitement.

Ces mesures de sécurité visent à protéger les obligations légales portant sur la protection des sources, la protection de l'identité de leurs agents et la discrétion de leurs enquêtes des autorités visées au titre 3.

Ces traitements ne peuvent être accessibles pour d'autres finalités que celles liées au contrôle que sur la base d'un protocole d'accord entre les responsables du traitement concernés.

Le système de contrôle est mis à la disposition de l'autorité de contrôle compétente.

L'autorité visée au titre 3 concernée peut déroger à l'alinéa premier lorsqu'il estime que son application à une banque de données déterminée n'est pas pertinente.

Art. 51

§ 1er . La personne concernée par un traitement commun de ses données à caractère personnel, émanant directement ou indirectement d'au moins une autorité compétente du titre 2 ou d'au moins une autorité, un service ou organe du titre 3 ne bénéfice pas des droits visés aux articles 41 à 47 et 64, à l'égard de ses données auprès du ou des responsables du traitement commun.

§ 2. Les obligations visées aux articles 41 à 47 et 64 ne s'appliquent pas aux autorités, personnes ou responsables du traitement en possession des données visées au paragraphe premier.

§ 3. Le responsable du traitement visé dans le présent titre qui est en possession de données visées au paragraphe premier ne les communique pas à la personne concernée à moins que:

1. la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que

2. le ou les responsables du traitement commun ne l'y autorise.

§ 4. Le ou les responsables du traitement commun ne font aucune mention à la personne concernée qu'il est en possession de données émanant du traitement commun.

§ 5. Les limitations visées au paragraphe premier portent également sur la journalisation des traitements dans le traitement commun.

§ 6. Wanneer een beroep aanhangig wordt gemaakt bij de bevoegde toezichthoudende autoriteit waarbij de verantwoordelijke of verantwoordelijken voor de verwerking zich beroepen op de toepassing van dit artikel, wendt deze zich tot andere toezichthoudende autoriteiten die bevoegd zijn voor gemeenschappelijke verwerking, opdat zij de nodige verificaties kunnen verrichten bij de verantwoordelijken voor de gemeenschappelijke verwerking. De toezichthoudende autoriteit antwoordt alleen dat de nodige verificaties zijn verricht.

HOOFDSTUK IV

Verwerkingsverantwoordelijke en verwerker

Afdeling 1

Organisatorische en technische maatregelen

Art. 52

Rekening houdend met de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen. Deze maatregelen mogen de invoering van een passend beleid inzake gegevensbescherming omvatten.

De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerking in overeenstemming met de wet wordt uitgevoerd.

Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

Art. 53

§ 1. Rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, dienen de technische en organisatorische maatregelen, bedoeld in artikel 52, om de gegevensbeschermingsbeginselen op een doeltreffende manier door te voeren en de nodige waarborgen in de verwerking in te bouwen ter bescherming van de rechten van de betrokkenen, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf.

§ 2. De technische en organisatorische maatregelen bedoeld in artikel 52 waarborgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. In het bijzonder, waarborgen deze maatregelen dat persoonsgegevens in beginsel niet zonder menselijke interventie voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

§ 6. Lorsque l'autorité de contrôle compétente est saisie d'un recours où le ou les responsables du traitement font état de l'application du présent article, celle-ci s'adresse aux autres autorités de contrôle compétentes pour le traitement commun, pour qu'elles fassent les vérifications nécessaires auprès du ou des responsables du traitement commun. L'autorité de contrôle répond uniquement que les vérifications nécessaires ont été effectuées.

CHAPITRE IV

Responsable du traitement et sous-traitant

Section 1re

Mesures organisationnelles et techniques

Art. 52

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées. Ces mesures peuvent comprendre la mise en œuvre de politiques appropriées en matière de protection des données.

Le responsable du traitement doit être en mesure de démontrer que le traitement est effectué conformément à la loi.

Ces mesures sont réexaminées et actualisées si nécessaire.

Art. 53

§ 1er. Compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, les mesures techniques et organisationnelles visées à l'article 52, sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires afin de protéger les droits de la personne concernée, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même.

§ 2. Les mesures techniques et organisationnelles appropriées visées à l'article 52 garantissent que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne concernée.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 54

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken.

Een onderlinge regeling stelt op transparante wijze de respectieve verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en om de in de artikelen 42 en 43 bedoelde informatie te verstrekken, tenzij hun respectieve verantwoordelijkheden zijn vastgesteld bij de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst.

In de onderlinge regeling kan één enkel contactpunt voor de betrokkenen worden aangewezen.

Afdeling 3

Verwerker

Art. 55

§ 1. Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verwerkingsverantwoordelijke een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de verwerking.

§ 2. De verwerker neemt een andere verwerker in dienst met voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke.

In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

§ 3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het type persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.

Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:

a) uitsluitend volgens de instructies van de verwerkingsverantwoordelijke handelt;

Section 2

Responsables conjoints du traitement

Art. 54

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Un accord définit de manière transparente les obligations respectives des responsables conjoints de traitement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et la communication des informations visées aux articles 42 et 43, sauf si, leurs obligations respectives sont définies par la loi, le décret, l'ordonnance, le droit de l'Union européenne ou la convention internationale.

Un seul point de contact pour les personnes concernées peut être désigné dans l'accord.

Section 3

Sous-traitant

Art. 55

§ 1er. Lorsque le traitement est confié à un sous-traitant, le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements.

§ 2. Le sous-traitant recrute un autre sous-traitant avec l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement.

Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

§ 3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique qui lie le sous-traitant à l'égard du responsable du traitement, et définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant:

a) n'agit que sur instruction du responsable du traitement;

b) ervoor zorgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verplicht geheimhouding in acht te nemen of door een passende wettelijke verplichting van geheimhouding gebonden zijn;

c) de verwerkingsverantwoordelijke met passende middelen bijstaat om de naleving van de bepalingen betreffende de rechten van de betrokkene te verzekeren;

d) na afloop van de gegevensverwerkingsdiensten, alle persoonsgegevens wist of die terugbezorgt aan de verwerkingsverantwoordelijke, en bestaande kopieën verwijdert, tenzij de bewaring van de persoonsgegevens verplicht is bij de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst;

e) aan de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de naleving van dit artikel aan te tonen;

f) aan de in de paragrafen 2 en 3 bedoelde voorwaarden voor indienstneming van een andere verwerker voldoet.

§ 4. De in paragraaf 3 bedoelde overeenkomst of andere rechtshandeling is gesteld in schriftelijke vorm, daaronder begrepen in elektronische vorm.

§ 5. Indien een verwerker in strijd met deze titel de doeleinden en middelen van de verwerking bepaalt, wordt die verwerker met betrekking tot deze verwerking als de verwerkingsverantwoordelijke beschouwd.

Art. 56

De verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt die uitsluitend in opdracht van de verwerkingsverantwoordelijke, of krachtens de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst.

Afdeling 4

Verplichtingen

Art. 57

Elke verwerkingsverantwoordelijke en verwerker houdt een register bij van de categorieën van verwerkingsactiviteiten die onder hun verantwoordelijkheid worden verricht. Dat register bevat de volgende elementen:

a) de naam en de contactgegevens van de verwerkingsverantwoordelijke of de verwerker, en van zijn gedelegeerde of vertegenwoordiger;

b) de naam en de contactgegevens van de functionaris voor gegevensbescherming;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;

c) aide le responsable du traitement, par tout moyen approprié, à veiller au respect des dispositions relatives aux droits de la personne concernée;

d) supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation des services de traitement des données, et détruit les copies existantes, à moins que la loi, le décret, l'ordonnance, le droit de l'Union européenne ou la convention internationale n'exige la conservation des données à caractère personnel;

e) met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect du présent article;

f) respecte les conditions visées aux paragraphes 2 et 3 pour recruter un autre sous-traitant.

§ 4. Le contrat ou l'autre acte juridique visé au paragraphe 3 revêt la forme écrite, y compris la forme électronique.

§ 5. Si, en violation du présent titre, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme le responsable du traitement pour ce qui concerne ce traitement.

Art. 56

Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut traiter ces données, que sur instruction du responsable du traitement, ou en vertu de la loi, du décret, de l'ordonnance, du droit de l'Union européenne ou de la convention internationale.

Section 4

Obligations

Art. 57

Chaque responsable du traitement et sous-traitant tient un registre des catégories d'activités de traitement effectuées sous sa responsabilité. Ce registre contient les éléments suivants:

a) le nom et les coordonnées du responsable du traitement ou sous-traitant, de son délégué ou représentant;

b) le nom et les coordonnées du délégué à la protection des données;

c) de verwerkingsdoeleinden;

d) de categorieën van betrokkenen;

e) de categorieën van persoonsgegevens;

f) de categorieën van ontvangers;

g) de doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in voorkomend geval, de documenten inzake de passende waarborgen;

h) de beoogde termijnen voor het wissen van de verschillende gegevenscategorieën;

i) een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 53 van deze wet;

j) het gebruik van profilering;

k) de rechtsgrondslag;

l) de categorie van externe bronnen;

m) het protocol bedoeld in artikel 22 evenals het advies van de functionaris voor gegevensbescherming en de motivering bedoeld in artikel 26.

§ 3. De Koning bepaalt, bij een in Ministerraad overlegd besluit en na advies van de bevoegde toezichthoudende autoriteit, voor elke bevoegde overheid de modaliteiten en het geheel of gedeeltelijk publieke karakter van het register bepalen.

§ 4. De functionaris voor gegevensbescherming wordt betrokken bij de uitwerking en het bijhouden van het register.

§ 5. Het register wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

§ 6. Het registermodel wordt door de Koning bepaald.

Art. 58

§ 1. De logbestanden van tenminste de volgende verwerkingen worden bijgehouden in systemen voor geautomatiseerde verwerking: verzameling, wijziging, raadpleging, bekendmaking, met inbegrip van de doorgiften, en wissing.

De logbestanden van raadpleging en bekendmaking maken het mogelijk om het volgende te achterhalen:

— de redenen, de datum en het tijdstip van die handelingen;

— de categorieën van personen die persoonsgegevens hebben geraadpleegd, en indien mogelijk, de identiteit van de persoon die persoonsgegevens heeft geraadpleegd;

c) les finalités du traitement;

d) les catégories de personnes concernées;

e) les catégories de données à caractère personnel;

f) les catégories de destinataires;

g) les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, le cas échéant, les documents attestant de l'existence de garanties appropriées;

h) les délais prévus pour l'effacement des différentes catégories de données;

i) une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 53 de la présente loi;

j) le recours au profilage;

k) la base juridique;

l) la catégorie de sources externes;

m) le protocole visé à l'article 22 ainsi que l'avis du délégué à la protection des données et la motivation visés à l'article 26.

§ 3. Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis de l'autorité de contrôle compétente, déterminer pour chaque autorité compétente, les modalités et le caractère public, en tout ou en partie du registre.

§ 4. Le délégué à la protection des données est associé à l'élaboration et au maintien du registre.

§ 5. Le registre est mis à la disposition de l'autorité de contrôle compétente.

§ 6. Le modèle de registre est déterminé par le Roi.

Art. 58

§ 1er. Les fichiers de journalisation sont établis dans des systèmes de traitement automatisé au moins pour les opérations de traitement suivantes: la collecte, la modification, la consultation, la communication, y compris les transferts et l'effacement.

Les fichiers de journalisation des opérations de consultation et de communication permettent d'établir:

— le motif, la date et l'heure de celles-ci;

— les catégories de personnes qui ont consulté les données à caractère personnel, et si possible, l'identification de la personne qui a consulté ces données;

— de systemen die deze persoonsgegevens bekendgemaakt hebben;

— en de categorieën van personen die persoonsgegevens ontvangen, en indien mogelijk, de identiteit van de ontvangers van die persoonsgegevens.

De Koning kan, bij een in de Ministerraad overlegd besluit en na advies van de bevoegde toezichthoudende autoriteit, andere soorten van verwerking bepalen waarvoor logbestanden moeten worden opgesteld.

§ 2. De logbestanden worden uitsluitend gebruikt om te controleren of de verwerking rechtmatig is, voor interne controles, ter waarborging van de integriteit en de beveiliging van de persoonsgegevens en voor doeleinden bedoeld in artikel 31.

§ 3. De verwerkingsverantwoordelijke en de verwerker stellen de logbestanden desgevraagd ter beschikking van de bevoegde toezichthoudende autoriteit.

Art. 59

De verwerkingsverantwoordelijke en de verwerker werken desgevraagd samen met de bevoegde toezichthoudende autoriteit bij het vervullen van haar taken.

Art. 60

§ 1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert, verricht de verwerkingsverantwoordelijke vóór de verwerking een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

§ 2. De in de eerste paragraaf bedoelde beoordeling bevat ten minste een algemene beschrijving van de beoogde verwerkingen, een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen, de beoogde maatregelen ter beperking van de risico's, de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te beschermen en aan te tonen dat aan deze titel is voldaan, met inachtneming van de rechten en legitieme belangen van de betrokkenen en de andere belanghebbenden.

Art. 61

§ 1. De verwerkingsverantwoordelijke of zijn verwerker raadpleegt de bevoegde toezichthoudende autoriteit van de verwerkingsverantwoordelijke voordat de verwerking van persoonsgegevens in een nieuw bestand wordt opgenomen:

a) indien uit een gegevensbeschermingseffectbeoordeling als bedoeld in artikel 60 blijkt dat de verwerking een hoog

— les systèmes qui ont communiqué ces données;

— et les catégories de destinataires des données à caractère personnel, et si possible, l'identité des destinataires de ces données.

Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres après avis de l'autorité de contrôle compétente, d'autres types de traitements pour lesquels les fichiers de journalisation sont établis.

§ 2. Les fichiers de journalisation sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins visées à l'article 31.

§ 3. Le responsable du traitement et le sous-traitant mettent les journaux à la disposition de l'autorité de contrôle compétente, sur demande.

Art. 59

Le responsable du traitement et le sous-traitant coopèrent avec l'autorité de contrôle compétente, à la demande de celle-ci, dans l'exécution de ses missions.

Art. 60

§ 1er. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

§ 2. L'analyse visée au paragraphe premier contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent titre, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes intéressées.

Art. 61

§ 1er. Le responsable du traitement ou son sous-traitant consulte l'autorité de contrôle compétente du responsable du traitement préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer:

a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 60, indique que

risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken; of

b) indien de aard van de verwerking, in het bijzonder wanneer wordt gebruikgemaakt van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt; of

c) bij het opstellen van een wet, een decreet of een ordonnantie, of een daarop gebaseerde reglementaire maatregel in verband met de verwerking.

§ 2. De bevoegde toezichthoudende autoriteit kan een lijst opstellen van de verwerkingen waarvoor overeenkomstig paragraaf 1 een voorafgaande raadpleging moet plaatsvinden.

§ 3. De verwerkingsverantwoordelijke verstrekt de bevoegde toezichthoudende autoriteit de gegevensbeschermingseffectbeoordeling krachtens artikel 60 en, desgevraagd, alle andere informatie op grond waarvan de bevoegde toezichthoudende autoriteit de conformiteit van de verwerking en met name de risico's voor de bescherming van de persoonsgegevens van de betrokkene en de betrokken waarborgen kan beoordelen.

§ 4. Wanneer de bevoegde toezichthoudende autoriteit van oordeel is dat de in de eerste paragraaf van dit artikel bedoelde voorgenomen verwerking indruist tegen deze titel, met name wanneer de verwerkingsverantwoordelijke het risico onvoldoende heeft onderkend of beperkt, geeft ze binnen de zes weken na ontvangst van het verzoek om niet bindend raadpleging schriftelijk advies aan de verwerkingsverantwoordelijke en in voorkomend geval aan de verwerker, en kan ze al haar bij de wet verleende bevoegdheden uitoefenen. Die termijn kan, naargelang de complexiteit van de voorgenomen verwerking, met een maand worden verlengd. De bevoegde toezichthoudende autoriteit stelt de verwerkingsverantwoordelijke en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van een eventuele verlenging, samen met de redenen voor de vertraging.

Art. 62

§ 1. De verwerkingsverantwoordelijke en de verwerker nemen passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, met name met betrekking tot de verwerking van persoonsgegevens bedoeld in artikel 39 van deze wet en rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, om een op het risico afgestemd beveiligingsniveau te waarborgen.

§ 2. Ten aanzien van de geautomatiseerde verwerking neemt de verwerkingsverantwoordelijke of de verwerker, na beoordeling van het risico, maatregelen om:

le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; ou

b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées; ou

c) dans le cadre de l'élaboration d'une loi, d'un décret ou d'une ordonnance, ou d'une mesure réglementaire fondée sur une telle loi, décret, ordonnance, qui se rapporte au traitement.

§ 2. L'autorité de contrôle compétente peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable conformément au paragraphe 1er.

§ 3. Le responsable du traitement fournit à l'autorité de contrôle compétente l'analyse d'impact relative à la protection des données en vertu de l'article 60 et, sur demande, toute autre information afin de permettre à l'autorité de contrôle compétente d'apprécier la conformité du traitement et, en particulier, les risques pour la protection des données à caractère personnel de la personne concernée et les garanties qui s'y rapportent.

§ 4. Lorsque l'autorité de contrôle compétente est d'avis que le traitement prévu, visé au paragraphe premier du présent article, constituerait une violation des dispositions adoptées en vertu du présent titre, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle compétente fournit par écrit, dans un délai maximum de six semaines à compter de la réception de la demande de consultation, un avis écrit non contraignant au responsable du traitement, et le cas échéant au sous-traitant, et elle peut faire usage des pouvoirs qui lui sont conférés par la loi. Ce délai peut être prolongé d'un mois, en fonction de la complexité du traitement prévu. L'autorité de contrôle compétente informe le responsable du traitement et, le cas échéant, le sous-traitant de toute prorogation dans un délai d'un mois à compter de la réception de la demande de consultation, ainsi que des motifs du retard.

Art. 62

§ 1er. Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des données à caractère personnel, visées à l'article 39 de la présente loi, et compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque.

§ 2. En ce qui concerne le traitement automatisé, le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à:

a) te verhinderen dat onbevoegden toegang krijgen tot de verwerkingsapparatuur;

b) te verhinderen dat onbevoegden de gegevensdragers kunnen lezen, kopiëren, wijzigen of verwijderen;

c) te verhinderen dat onbevoegden persoonsgegevens invoeren of opgeslagen persoonsgegevens inzien, wijzigen of verwijderen;

d) te verhinderen dat onbevoegden geautomatiseerde verwerkingssystemen gebruiken met behulp van datatransmissieapparatuur;

e) ervoor te zorgen dat personen die bevoegd zijn om een geautomatiseerd verwerkingssysteem te gebruiken, uitsluitend toegang hebben tot de persoonsgegevens waarop hun toegangsbevoegdheid betrekking heeft;

f) ervoor te zorgen dat kan worden nagegaan en vastgesteld aan welke organen persoonsgegevens zijn of kunnen worden doorgezonden of beschikbaar gesteld met behulp van datatransmissieapparatuur;

g) ervoor te zorgen dat later kan worden nagegaan en vastgesteld welke persoonsgegevens wanneer en door wie in geautomatiseerde verwerkingssystemen zijn ingevoerd;

h) te verhinderen dat onbevoegden persoonsgegevens kunnen lezen, kopiëren, wijzigen of verwijderen bij de doorgifte van persoonsgegevens of het vervoer van gegevensdragers;

i) ervoor te zorgen dat de geïnstalleerde systemen in geval van storing opnieuw kunnen worden ingezet;

j) ervoor te zorgen dat de functies van het systeem werken, dat eventuele functionele storingen worden gesignaleerd en dat de bewaarde persoonsgegevens niet kunnen worden beschadigd door het verkeerd functioneren van het systeem.

Art. 63

§ 1. De verwerkingsverantwoordelijke meldt de inbreuk op de beveiliging zonder onnodige vertraging en indien mogelijk niet meer dan 72 uur nadat hij er kennis van heeft genomen aan de bevoegde toezichthoudende autoriteit. Die verplichte kennisgeving is niet van toepassing wanneer het waarschijnlijk is dat de inbreuk op de beveiliging geen risico voor de rechten en vrijheden van personen met zich brengt.

Wanneer de kennisgeving aan de bevoegde toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat ze vergezeld van een motivering voor de vertraging.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke zonder onnodige vertraging en uiterlijk binnen 72 uur zodra hij kennis heeft genomen van een inbreuk op de beveiliging.

a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement;

b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée;

c) empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que la consultation, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées;

d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données;

e) garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation;

f) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données;

g) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites;

h) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée;

i) garantir que les systèmes installés puissent être rétablis en cas d'interruption;

j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système.

Art. 63

§ 1er. Le responsable du traitement notifie la brèche de sécurité, à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, dans un délai de 72 heures après en avoir pris connaissance. Cette obligation de notification n'est pas applicable lorsqu'il est raisonnable de croire que la brèche de sécurité en question n'engendre pas de risque pour les droits et les libertés d'une personne physique.

Lorsque la notification à l'autorité de contrôle compétente n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais et au plus tard dans les 72 heures après en avoir pris connaissance.

§ 3. In de in de eerste paragraaf bedoelde melding wordt het volgende omschreven of meegedeeld:

a) de aard van de inbreuk op de beveiliging, onder vermelding van, indien mogelijk de categorieën van betrokkenen en gegevensbestanden in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensbestanden in kwestie;

b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

c) de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, met inbegrip, in voorkomend geval maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

§ 4. Indien en voor zover het niet mogelijk is alle informatie gelijktijdig te verstrekken, kan de informatie zonder onnodige verdere vertraging in stappen worden verstrekt.

§ 5. Wanneer de inbreuk op de beveiliging betrekking heeft op persoonsgegevens die zijn doorgezonden door of aan de verwerkingsverantwoordelijke van een andere lidstaat van de Europese Unie, wordt de in paragraaf 3 bedoelde informatie zonder onnodige vertraging aan de verwerkingsverantwoordelijke van die lidstaat meegedeeld.

§ 6. De verwerkingsverantwoordelijke documenteert alle in de eerste paragraaf bedoelde inbreuken op de beveiliging, met inbegrip van de feiten, de gevolgen ervan en de genomen corrigerende maatregelen. Die documentatie moet de bevoegde toezichthoudende autoriteit ertoe in staat stellen de naleving van dit artikel te controleren.

Art. 64

§ 1. Wanneer de inbreuk op de beveiliging waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk op de beveiliging onverwijld mee.

§ 2. De in de eerste paragraaf van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, van de aard van de inbreuk op de beveiliging en ten minste de in artikel 63, paragraaf 3, b), c) en d), bedoelde gegevens en maatregelen.

§ 3. De in de eerste paragraaf bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

a) de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen

§ 3. La notification visée au paragraphe premier contient notamment:

a) la description de la nature de la brèche de sécurité y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) la description des conséquences probables de la brèche de sécurité;

d) la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

§ 4. Si et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

§ 5. Lorsque la brèche de sécurité porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre État membre de l'Union européenne ou à celui-ci, les informations visées au paragraphe 3 sont communiquées au responsable du traitement de cet État membre dans les meilleurs délais.

§ 6. Le responsable du traitement documente toute brèche de sécurité visée au paragraphe premier, en indiquant les faits, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle compétente de vérifier le respect du présent article.

Art. 64

§ 1er. Lorsqu'une brèche de sécurité est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la brèche de sécurité à caractère personnel à la personne concernée dans les meilleurs délais.

§ 2. La communication à la personne concernée visée au paragraphe premier du présent article décrit, la nature de la brèche de sécurité et contient au moins les informations et mesures visées à l'article 63, paragraphe 3, points b), c) et d).

§ 3. La communication à la personne concernée visée au paragraphe premier n'est pas nécessaire si l'une des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées

genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk op de beveiliging betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

b) de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in paragraaf 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er daarvan een openbare mededeling of een soortgelijke maatregel waarbij de betrokkenen even doeltreffend worden geïnformeerd.

§ 4. Indien de verwerkingsverantwoordelijke de inbreuk op de beveiliging nog niet aan de betrokkene heeft gemeld, kan de bevoegde toezichthoudende autoriteit, na beraad over de kans dat de inbreuk op de beveiliging een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in paragraaf 3 bedoelde voorwaarden is voldaan.

§ 5. De in de eerste paragraaf van dit artikel bedoelde mededeling aan de betrokkene kan worden uitgesteld, beperkt of achterwege worden gelaten onder de voorwaarden en om de redenen bedoeld in artikel 42, paragraaf 2.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 65

§ 1. De verwerkingsverantwoordelijke wijst een of meerdere functionarissen voor gegevensbescherming aan.

§ 2. De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 67 bedoelde taken te vervullen.

§ 3. Het is mogelijk om voor verschillende bevoegde overheden of verwerkingsverantwoordelijken, rekening houdend met hun organisatiestructuur en omvang, één functionaris voor gegevensbescherming aan te wijzen.

§ 4. De verwerkingsverantwoordelijke maakt de contactgegevens van de functionaris voor gegevensbescherming openbaar en deelt die mee aan de bevoegde toezichthoudende autoriteit.

§ 5. De nadere regels voor de werking, de aanwijzing en vereiste competenties worden door de Koning bepaald.

en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite brèche de sécurité;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1er n'est plus susceptible de se matérialiser;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

§ 4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la brèche de sécurité la concernant, l'autorité de contrôle compétente peut, après avoir examiné si cette brèche de sécurité est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

§ 5. La communication à la personne concernée visée au paragraphe mier du présent article peut être retardée, limitée ou omise, sous réserve des conditions et pour les motifs visés à l'article 42, paragraphe 2.

Section 5

Délégué à la protection des données

Art. 65

§ 1er. Le responsable du traitement désigne un ou plusieurs délégués à la protection des données.

§ 2. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à exercer les missions visées à l'article 67.

§ 3. Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes ou responsables du traitement, compte tenu de leur structure organisationnelle et de leur taille.

§ 4. Le responsable du traitement publie les coordonnées du délégué à la protection des données et les communique à l'autorité de contrôle compétente.

§ 5. Les modalités de fonctionnement, de désignation ainsi que les compétences requises sont définies par le Roi.

Art. 66

§ 1. De verwerkingsverantwoordelijke ziet erop toe dat de functionaris voor gegevensbescherming tijdig en naar behoren bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden, wordt betrokken.

§ 2. De verwerkingsverantwoordelijke stelt de functionaris voor gegevensbescherming de benodigde middelen ter beschikking voor het vervullen van die taken en verschaft hem toegang tot de persoonsgegevens en de verwerkingen, en biedt hem de mogelijkheid zijn deskundigheid op peil te houden.

§ 3. De verwerkingsverantwoordelijke ziet erop toe dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken. De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke.

§ 4. Behalve bij toepassing van artikel 46 kunnen de betrokkenen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten.

§ 5. De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.

§ 6. De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

Art. 67

De functionaris voor gegevensbescherming vervult in het bijzonder de volgende taken:

a) de verwerkingsverantwoordelijke en de werknemers die de verwerking verrichten informeren en adviseren over hun verplichtingen met betrekking tot de bescherming van de persoonsgegevens;

b) toezien op de naleving van de regelgeving en de interne regels van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, de bewustmaking en de opleiding van het bij de verwerking betrokken personeel en de betreffende audits;

c) desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 60;

d) met de bevoegde toezichthoudende autoriteit samenwerken;

Art. 66

§ 1er. Le responsable du traitement veille à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

§ 2. Le responsable du traitement fournit au délégué à la protection des données les ressources nécessaires pour exercer ses missions ainsi que l'accès aux données à caractère personnel et aux traitements, et lui permet d'entretenir ses connaissances spécialisées.

§ 3. Le responsable du traitement veille à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement.

§ 4. Sauf application de l'article 46, les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits qui leur sont conférés.

§ 5. Le délégué à la protection des données est soumis au secret ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.

§ 6. Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement veille à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts.

Art. 67

Les missions du délégué à la protection des données sont notamment les suivantes:

a) informer et conseiller le responsable du traitement et les employés qui procèdent au traitement sur les obligations qui leur incombent en matière de protection des données;

b) contrôler le respect de la réglementation et des règles internes du responsable du traitement en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant à des opérations de traitement, et les audits s'y rapportant;

c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 60;

d) coopérer avec l'autorité de contrôle compétente;

e) optreden als contactpunt voor de bevoegde toezichthoudende autoriteit inzake met de verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 61 bedoelde voorafgaande raadpleging, en, in voorkomend geval, overleg plegen over enige andere aangelegenheid.

HOOFDSTUK V

Doorgiften van persoonsgegevens aan derde landen of internationale organisaties

Art. 68

§ 1. Onverminderd de bepalingen van deze titel, mogen de bevoegde overheden persoonsgegevens slechts doorgeven aan landen buiten de Europese unie of aan een internationale organisatie, eventueel met het oog op verdere doorgifte aan een ander land buiten de Europese unie of een andere internationale organisatie, indien aan de volgende voorwaarden is voldaan:

a) de doorgifte is noodzakelijk met het oog op de doeleinden van artikel 31;

b) de persoonsgegevens worden doorgegeven aan een verwerkingsverantwoordelijke in een land buiten de Europese unie of in een internationale organisatie die een bevoegde overheid is voor de in artikel 31, bedoelde doeleinden;

c) ingeval persoonsgegevens worden doorgezonden of beschikbaar gesteld vanuit een andere lidstaat van de Europese Unie, heeft die lidstaat overeenkomstig zijn nationale recht zijn voorafgaande toestemming gegeven voor de doorgifte;

d) de Europese Commissie heeft een adequaatheidsbesluit zoals bedoeld in artikel 60 vastgesteld, of, indien een dergelijk besluit er niet is, zijn er krachtens artikel 61 passende waarborgen geboden of gelden er afwijkingen voor specifieke situaties uit hoofde van artikel 71;

e) in het geval van een verdere doorgifte aan een ander land buiten de Europese unie of een andere internationale organisatie, heeft de verwerkingsverantwoordelijke, toestemming voor de verdere doorgifte gegeven, na alle relevante factoren naar behoren in aanmerking te hebben genomen, met inbegrip van de ernst van het strafbare feit, het doel waarvoor de persoonsgegevens oorspronkelijk waren doorgegeven en het niveau van persoonsgegevensbescherming in het derde land of de internationale organisatie waaraan de persoonsgegevens verder worden doorgegeven.

§ 2. De doorgifte zonder de voorafgaande toestemming vanwege een andere lidstaat van de Europese Unie zoals bedoeld in punt c) van de eerste paragraaf is slechts toegelaten indien deze doorgifte van persoonsgegevens noodzakelijk is met het oog op de voorkoming van een acute en ernstige bedreiging van de openbare veiligheid van een lidstaat of een derde land of voor de fundamentele belangen van een lidstaat van de Europese Unie, en voorafgaande toestemming

e) faire office de point de contact pour l'autorité de contrôle compétente sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 61, et mener des consultations, le cas échéant, sur tout autre sujet.

CHAPITRE V

Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

Art. 68

§ 1er. Sans préjudice des dispositions du présent titre, un transfert, par des autorités compétentes, de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale, y compris des transferts ultérieurs vers un autre pays non membre à l'Union européenne ou à une autre organisation internationale, n'a lieu, que lorsque les conditions ci-après sont respectées:

a) le transfert est nécessaire aux fins énoncées à l'article 31;

b) les données à caractère personnel sont transférées à un responsable du traitement dans un pays non membre de l'Union européenne ou à une organisation internationale qui est une autorité compétente aux fins visées à l'article 31;

c) en cas de transfert ou de mise à disposition de données à caractère personnel provenant d'un autre État membre de l'Union européenne, celui-ci a préalablement autorisé ce transfert conformément à son droit national;

d) la Commission européenne a adopté une décision d'adéquation tel que visé à l'article 60, ou, en l'absence d'une telle décision, des garanties appropriées ont été prévues ou existent en application de l'article 61 ou, des dérogations pour des situations particulières s'appliquent en vertu de l'article 71;

e) en cas de transfert ultérieur vers un autre pays non membre de l'Union européenne ou à une autre organisation internationale, le responsable du traitement qui a reçu les données autorise le transfert ultérieur, après avoir dûment pris en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, la finalité pour laquelle les données à caractère personnel ont été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données à caractère personnel sont transférées ultérieurement.

§ 2. Les transferts effectués sans l'autorisation préalable d'un autre État membre de l'Union européenne prévue au paragraphe premier, point c), sont autorisés uniquement lorsque le transfert de données à caractère personnel est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre de l'Union européenne et si l'autorisation préalable ne peut

niet tijdig kan worden verkregen. De voor het geven van voorafgaande toestemming verantwoordelijke overheid wordt onverwijld in kennis gesteld.

Art. 69

Een doorgifte van persoonsgegevens aan een land buiten de Europese unie of een internationale organisatie kan slechts plaatsvinden wanneer de Europese Commissie bij adequaatheidsbesluit bepaald heeft dat het land, een gebied of één of meerdere nader bepaalde sectoren in dat land, of de internationale organisatie in kwestie een passend beschermingsniveau waarborgt. Voor een dergelijke doorgifte is geen specifieke toestemming nodig.

Art. 70

§ 1. Bij gebreke van een adequaatheidsbesluit zoals bedoeld in artikel 69, of wanneer dat is opgeheven, gewijzigd of opgeschort, kan een doorgifte van persoonsgegevens aan een land buiten de Europese unie of een internationale organisatie slechts plaatsvinden wanneer:

a) in een juridisch bindend instrument wordt voorzien in passende waarborgen voor de bescherming van persoonsgegevens; of

b) de verwerkingsverantwoordelijke alle omstandigheden in verband met de doorgifte van persoonsgegevens heeft beoordeeld en heeft geconcludeerd dat er passende waarborgen bestaan voor de bescherming van persoonsgegevens.

§ 2. De verwerkingsverantwoordelijke informeert de bevoegde toezichthoudende autoriteit over de categorieën van doorgiften uit hoofde van de eerste paragraaf, punt b).

§ 3. De doorgifte gebaseerd op de eerste paragraaf, punt b) wordt gedocumenteerd en bevat:

— de datum en tijd van doorgifte;

— informatie over de ontvangende bevoegde autoriteit;

— de reden voor de doorgifte en de doorgegeven persoonsgegevens zelf.

De documentatie wordt desgevraagd ter beschikking van de bevoegde toezichthoudende autoriteit gesteld.

Art. 71

§ 1. Bij gebreke van een adequaatheidsbesluit zoals bedoeld in artikel 69, of van passende waarborgen zoals bedoeld in artikel 70, is een doorgifte of een categorie van doorgiften van persoonsgegevens aan een land buiten de Europese unie of een internationale organisatie slechts toegelaten indien de doorgifte noodzakelijk is:

pas être obtenue en temps utile. L'autorité à laquelle il revient d'accorder l'autorisation préalable est informée sans retard.

Art. 69

Un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale peut avoir lieu lorsque la Commission européenne a constaté par voie de décision d'adéquation que le pays, un territoire ou un ou plusieurs secteurs déterminés dans ce pays, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

Art. 70

§ 1er. En l'absence de décision d'adéquation, visée à l'article 69, ou lorsque celle-ci est abrogée, modifiée ou suspendue, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale peut avoir lieu lorsque:

a) des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant; ou

b) le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.

§ 2. Le responsable du traitement informe l'autorité de contrôle compétente des catégories de transferts relevant du paragraphe premier, point b).

§ 3. Le transfert effectué en vertu du paragraphe premier, point b), est documenté et, comporte:

— la date et l'heure du transfert;

— des informations sur l'autorité compétente destinataire;

— la justification du transfert et les données à caractère personnel transférées.

La documentation est mise à la disposition de l'autorité de contrôle compétente sur demande.

Art. 71

§ 1er. En l'absence de décision d'adéquation visée à l'article 69 ou de garanties appropriées visées à l'article 70, un transfert ou une catégorie de transferts de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale ne peut avoir lieu qu'à condition que le transfert soit nécessaire:

a) om de vitale belangen van de betrokkene of van een andere persoon te beschermen;

b) om de legitieme belangen van de betrokkene te beschermen wanneer de wet daarin voorziet;

c) om een onmiddellijke en ernstige bedreiging van de openbare veiligheid te voorkomen;

d) in uitzonderlijke gevallen met het oog op de doeleinden van artikel 31;

e) in uitzonderlijke gevallen met het oog op het instellen, uitoefenen of verdedigen van rechtsvorderingen in verband met de doeleinden van artikel 31.

§ 2. Persoonsgegevens worden niet doorgegeven indien de bevoegde autoriteit die de doorgifte verricht, meent dat de grondrechten en fundamentele vrijheden van de betrokkene zwaarder wegen dan het algemeen belang van de doorgifte bedoeld in de eerste paragraaf, punten d) en e).

§ 3. De doorgifte bedoeld in de eerste paragraaf, punt b), wordt gedocumenteerd en bevat:

— de datum en tijd van doorgifte;

— de informatie over de ontvangende bevoegde autoriteit;

— de reden voor de doorgifte en de doorgegeven persoonsgegevens zelf.

De documentatie wordt desgevraagd ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Art. 72

§ 1. In afwijking van artikel 68, eerste paragraaf, punt b), en onverminderd de internationale overeenkomsten en bepalingen van deze titel, mogen de bevoegde autoriteiten persoonsgegevens, in bepaalde specifieke gevallen, persoonsgegevens rechtstreeks doorgeven aan ontvangers in landen buiten de Europese unie die geen autoriteit zijn bevoegd voor de doeleinden in artikel 31, voor zover aan alle onderstaande voorwaarden is voldaan:

a) de doorgifte is strikt noodzakelijk voor de uitvoering van de opdrachten van de bevoegde autoriteit die de doorgifte doet;

b) de bevoegde autoriteit die de gegevens doorgeeft, stelt vast dat er geen fundamentele rechten en vrijheden van de betrokkene voorrang hebben op het algemeen belang waarvoor de overdracht in het betreffende geval vereist is;

c) de bevoegde autoriteit die de doorgifte doet, meent dat de doorgifte aan een bevoegde autoriteit binnen het desbetreffende land ondoeltreffend of ongeschikt is, met name omdat de doorgifte niet tijdig kan worden bewerkstelligd;

a) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne;

b) à la sauvegarde des intérêts légitimes de la personne concernée lorsque la loi le prévoit;

c) pour prévenir une menace grave et immédiate pour la sécurité publique;

d) dans des cas particuliers, aux fins énoncées à l'article 31;

e) dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les fins énoncées à l'article 31.

§ 2. Les données à caractère personnel ne sont pas transférées si l'autorité compétente qui transfère les données estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert visé au paragraphe premier, points d) et e).

§ 3. Le transfert visé au paragraphe premier, point b), est documenté et indique:

— la date et l'heure du transfert;

— les informations sur l'autorité compétente destinataire;

— la justification du transfert et les données à caractère personnel transférées.

La documentation est mise à la disposition de l'autorité de contrôle compétente, sur demande.

Art. 72

§ 1er. Par dérogation à l'article 68, paragraphe premier, point b), et sans préjudice de tout accord international et des dispositions du présent titre, les autorités compétentes peuvent, dans certains cas particuliers, transférer des données à caractère personnel directement aux destinataires qui ne sont pas des autorités compétentes pour les finalités visées à l'article 31, établis dans des pays non membre de l'Union européenne, uniquement lorsque toutes les conditions ci-après sont remplies:

a) le transfert est strictement nécessaire à l'exécution de la mission de l'autorité compétente qui transfère les données;

b) l'autorité compétente qui transfère les données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas en question;

c) l'autorité compétente qui transfère les données estime que le transfert à une autorité compétente, dans le pays concerné est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun;

d) de bevoegde autoriteit in het desbetreffende land wordt zonder onnodige vertraging op de hoogte gebracht, tenzij dat ondoeltreffend of ongeschikt is;

e) de bevoegde autoriteit die de doorgifte doet, licht de ontvanger in over het nader bepaalde doel of de nader bepaalde doeleinden waarvoor de persoonsgegevens bij uitsluiting door laatstgenoemde mogen worden verwerkt, op voorwaarde dat een dergelijke verwerking noodzakelijk is.

§ 2. De bevoegde autoriteit die de doorgifte doet, stelt de toezichthoudende autoriteit in kennis van doorgiften die gebeuren in het kader van dit artikel.

§ 3. Wanneer een doorgifte is gebaseerd op de eerste paragraaf, wordt die gedocumenteerd.

HOOFDSTUK VI

Onafhankelijke toezichthoudende autoriteiten

Art. 73

§ 1. Bij de Kamer van volksvertegenwoordigers wordt een onafhankelijke toezichthoudende autoriteit op de politionele informatie opgericht, Controleorgaan op de politionele informatie genoemd.

Zij is de rechtsopvolger van het Controleorgaan op de politionele informatie bedoeld in artikel 44/6, § 1, van de wet van 5 augustus 1992 op het politieambt.

Zij is ten aanzien van de bevoegde overheden bedoeld in artikel 31, 7°, a), c), d), f), belast, met:

1. het toezicht op de toepassing van de huidige titel II, zoals voorzien door artikel 31, 15°, en op de bepalingen van titel I, hoofdstuk IV, afdeling 2 in de mate dat zij van toepassing zijn op de politiediensten in de zin van artikel 2,2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus;

2. de uitoefening van de competenties, taken en bevoegdheden voorzien in artikel 4, § 2, laatste alinea van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit;

3. de controle van de verwerking van de informatie en de persoonsgegevens bedoeld in artikel 44/1 tot en met 44/11/13 van de wet van 5 augustus 1992 op het politieambt, met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2;

4. elke andere opdracht haar door of krachtens andere wetten verleend.

§ 2. De zetel van het Controleorgaan op de politionele informatie is gevestigd in het administratief arrondissement Brussel-Hoofdstad.

d) l'autorité compétente dans le pays concerné est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié;

e) l'autorité compétente qui transfère les données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel ne doivent faire l'objet d'un traitement que par cette dernière, à condition qu'un tel traitement soit nécessaire.

§ 2. L'autorité compétente qui transfère les données informe l'autorité de contrôle des transferts relevant du présent article.

§ 3. Lorsqu'un transfert est effectué sur la base du paragraphe premier, ce transfert est documenté.

CHAPITRE VI

Autorités de contrôle indépendantes

Art. 73

§ 1er. Il est créé auprès de la Chambre des représentants une autorité de contrôle indépendante de l'information policière, dénommé Organe de contrôle de l'information policière.

Elle succède à l'organe de contrôle de l'information policière visé à l'article 44/6, § 1er, de la loi du 5 août 1992 sur la fonction de police.

Elle est, vis-à-vis des autorités compétentes visées à l'article 31, 7°, a), c), d), f), chargée de:

1. surveiller l'application du présent titre II, comme prévu à l'article 31, 15°, et les disposition du titre I, chapitre IV, section 2, dans la mesure ou ils sont applicables aux services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police structuré organisé à deux niveaux;

2. exercer les compétences, missions et pouvoirs visés à l'article 4, § 2, dernier alinéa de la loi du 3 decembre 2017 portant création de l'Autorité de protection des données;

3. contrôler le traitement des informations et des données à caractère personnel visées à l'article 44/1 jusqu'au 44/11/13 de la loi du 5 août 1992 sur la fonction de police y compris celles incluses dans les banques de données visées à l'article 44/2;

4. toute autre mission organisée par ou en vertu d'autres lois.

§ 2. Le siège de l'Organe de contrôle de l'information policière est établi dans l'arrondissement administratif de Bruxelles-Capitale.

Bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden overeenkomstig deze wet en andere wetten treedt het Controleorgaan op de politionele informatie volledig onafhankelijk op.

§ 3. Haar samenstelling, het statuut van haar leden, haar opdrachten, haar bevoegdheden evenals haar financiering worden geregeld in titel 7.

Dans l'exercice de ses missions et des pouvoirs dont elle est investie conformément à la présente loi, l'Organe de contrôle de l'information policière agit en toute indépendance.

§ 3. Sa composition, le statut de ses membres, ses missions, ses compétences ainsi que son financement sont réglés dans le titre 7.

TITEL 3

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door andere overheden dan die bedoeld in titels 1 en 2

ONDERTITEL 1

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

HOOFDSTUK I

Definities

Art. 74

§ 1. De definities bedoeld in de artikelen 31, 1° tot 6°, 9°, 11° tot 14°, en 16° tot 17°, zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder:

1. "de inlichtingen- en veiligheidsdiensten": de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2. "de verwerkingsverantwoordelijke": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

3. "de wet van 30 november 1998": de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

4. "de wet van 18 juli 1991": de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

5. "de wet van 11 december 1998": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

6. "toezichthoudende autoriteit": de onafhankelijke overheidsinstantie die bij de wet belast is met het toezicht op de

TITRE 3

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par d'autres autorités que celles visées aux titres 1 et 2

SOUS-TITRE 1ER

DE LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL PAR LES SERVICES DE RENSEIGNEMENT ET DE SECURITE

CHAPITRE IER

Définitions

Art. 74

§ 1er. Les définitions visées à l'article 31, 1° à 6°, 9°, 11° à 14°, et 16° à 17°, sont applicables au présent sous-titre.

§ 2. Pour l'application du présent sous-titre, on entend par:

1. "les services de renseignement et de sécurité": la Sûreté de l'État et le Service Général du Renseignement et de la Sécurité visés dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2. "le responsable du traitement": la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement;

3. "la loi du 30 novembre 1998": la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

4. "la loi du 18 juillet 1991": la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace;

5. "la loi du 11 décembre 1998": la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

6. "autorité de contrôle": l'autorité publique indépendante chargée par la loi de surveiller l'application du présent

toepassing van deze ondertitel, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met verwerking te beschermen.

HOOFDSTUK II

Toepassingsgebied

Art. 75

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten en hun verwerkers, uitgevoerd in het kader van de opdrachten van deze diensten als bedoeld in artikelen 7 en 11 van de wet van 30 november 1998 en door of krachtens bijzondere wetten.

Titels 1, 2, 4, 5 en 7 van deze wet zijn niet van toepassing op de verwerkingen bedoeld in het eerste lid. Enkel de artikelen 239 en 240 van titel 6 zijn van toepassing.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 76

Persoonsgegevens mogen slechts verwerkt worden in één van de volgende gevallen:

a) wanneer de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend;

b) wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;

c) wanneer de verwerking nuttig is om een verplichting na te komen waaraan de inlichtingen en veiligheidsdienst is onderworpen door of krachtens een wet;

d) wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verwerkingsverantwoordelijke of aan de overheidsinstantie aan wie de persoonsgegevens worden verstrekt.

Art. 77

Persoonsgegevens dienen:

1. eerlijk en rechtmatig te worden verwerkt;

2. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de toepasselijke

sous-titre, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement.

CHAPITRE II

Champ d'application

Art. 75

Le présent sous-titre s'applique à tout traitement de données à caractère personnel par les services de renseignement et de sécurité et leurs sous-traitants effectués dans le cadre des missions desdits services visés aux articles 7 et 11 de la loi du 30 novembre 1998 ainsi que par ou en vertu de lois particulières.

Les titres 1, 2, 4, 5 et 7 de la présente loi ne s'appliquent pas aux traitements visés à l'alinéa premier. Dans le titre 6, seuls les articles 239 et 240 sont d'application.

CHAPITRE III

Conditions générales du traitement

Art. 76

Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants:

a) lorsque la personne concernée a indubitablement donné son consentement;

b) lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) lorsqu'il est utile au respect d'une obligation à laquelle le service de renseignement et de sécurité concerné est soumis par ou en vertu d'une loi;

d) lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou une autorité publique à laquelle les données à caractère personnel sont communiquées.

Art. 77

Les données à caractère personnel doivent être:

1. traitées loyalement et licitement;

2. collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et

wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden. Onder de voorwaarden vastgesteld door de artikelen 101 tot en met 106 wordt verdere verwerking van de gegevens voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd;

3. toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4. nauwkeurig te zijn en, zo nodig, te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren.

HOOFDSTUK IV

Aard van de persoonsgegevens

Art. 78

De inlichtingen- en veiligheidsdiensten verwerken, voor het belang van de uitoefening van hun opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of de seksuele geaardheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 79

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de modaliteiten bepaald in het kader van artikel 21 van de wet van 30 november 1998.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 80

Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.

réglementaires applicables. Un traitement ultérieur à des fins historiques, scientifiques ou statistiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par les articles 101 à 106;

3. adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4. exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

CHAPITRE IV

Nature des données à caractère personnel

Art. 78

Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité traitent des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

CHAPITRE V

Conservation des données à caractère personnel

Art. 79

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées dans le cadre de l'article 21 de la loi du 30 novembre 1998.

CHAPITRE VI

Droits de la personne concernée

Art. 80

Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 81

De betrokkene heeft het recht te vragen:

1. om toegang tot zijn persoonsgegevens overeenkomstig artikel 82;

2. om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen overeenkomstig artikel 83;

3. om de verificatie bij de bevoegde toezichthoudende autoriteit van de naleving van de bepalingen van deze ondertitel overeenkomstig artikel 83.

Art. 82

Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van de opdrachten van de inlichtingen- en veiligheidsdiensten te waarborgen, is de toegang van de betrokkene tot zijn persoonsgegevens beperkt tot de toegang bedoeld in artikel 2, § 3, van de wet van 30 november 1998 en tot de toegangen die expliciet voorzien zijn bij wet.

Art. 83

Voor de uitoefening van zijn rechten, bedoeld in artikel 81, 2° en 3°, richt de betrokkene, die zijn identiteit bewijst, zich kosteloos tot de bevoegde toezichthoudende autoriteit.

Deze voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht.

De nadere regels voor de uitoefening van dit beroep zijn bepaald in de wet.

Art. 84

Een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn, mag niet louter worden genomen op grond van een geautomatiseerde persoonsgegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.

Het in het eerste lid vastgestelde verbod geldt niet indien het besluit zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet of wanneer het noodzakelijk is vanwege een zwaarwegend openbaar belang.

Art. 81

La personne concernée a le droit de demander:

1. l'accès à ses données à caractère personnel conformément à l'article 82;

2. la rectification ou la suppression de ses données à caractère personnel inexactes conformément à l'article 83;

3. la vérification auprès de l'autorité de contrôle compétente du respect des dispositions du présent sous-titre conformément à l'article 83.

Art. 82

Afin de garantir la confidentialité et l'efficacité de l'exécution des missions des services de renseignement et de sécurité, l'accès par la personne concernée à ses données à caractère personnel est limité à celui visé à l'article 2, § 3, de la loi du 30 novembre 1998 et à ceux prévus expressément par une loi.

Art. 83

Pour l'exercice de ses droits visés à l'article 81, 2° et 3°, la personne concernée justifiant de son identité s'adresse, sans frais, à l'autorité de contrôle compétente.

Celle-ci effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Les modalités d'exercice de ce recours sont déterminées par la loi.

Art. 84

Une décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

L'interdiction prévue à l'alinéa premier ne s'applique pas lorsque la décision est fondée sur une disposition prévue par ou en vertu d'une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important.

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 85

De verwerkingsverantwoordelijke moet:

1. er nauwlettend over waken dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2. ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot hetgeen wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst;

3. alle personen die onder zijn gezag handelen, kennisgeven van de bepalingen van deze ondertitel en van alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer die bij het verwerken van persoonsgegevens gelden.

Art. 86

Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verwerkingsverantwoordelijke:

1. een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking;

2. toezien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen;

3. de aansprakelijkheid van de verwerker vaststellen in de overeenkomst;

4. met de verwerker overeenkomen dat de verwerker slechts handelt in opdracht van de verwerkingsverantwoordelijke en dat de verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke in toepassing van deze ondertitel is gehouden;

5. in een geschrift of op een elektronische drager de elementen van de overeenkomst met betrekking tot de bescherming van de persoonsgegevens en de eisen met betrekking tot de maatregelen bedoeld in 3° en 4°, vaststellen.

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 85

Le responsable du traitement doit:

1. faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2. veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins du service;

3. informer les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 86

Lorsque le traitement est confié à un sous-traitant, le responsable du traitement doit:

1. choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements;

2. veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles;

3. fixer dans le contrat la responsabilité du sous-traitant;

4. convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et qu'il est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du présent sous-titre;

5. consigner par écrit ou sur un support électronique les éléments du contrat relatifs à la protection des données à caractère personnel et les exigences relatives aux mesures visées aux 3° et 4°.

Art. 87

De verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke is gehouden.

Hij mag de verwerking van persoonsgegevens, die hij verwerkt, niet toevertrouwen aan een andere verwerker, behoudens uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Art. 88

Eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verwerkingsverantwoordelijke verwerken, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 89

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken.

Een onderlinge regeling bepaalt de respectievelijke verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken, met name met betrekking tot de uitoefening van de rechten van de betrokkene en de mededeling van persoonsgegevens, tenzij hun respectievelijke verantwoordelijkheden zijn vastgesteld door of krachtens een wet.

In de onderlinge regeling kan één contactpunt voor betrokkenen worden aangewezen.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 90

Om de veiligheid van de persoonsgegevens te waarborgen, treffen de verwerkingsverantwoordelijke, alsmede de verwerker, de passende technische en organisatorische maatregelen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen verzekeren een passend beveiligingsniveau, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen persoonsgegevens en de potentiële risico's.

Art. 87

Le sous-traitant est soumis aux mêmes obligations que celles qui incombent au responsable du traitement.

Il ne peut pas confier le traitement de données à caractère personnel qu'il sous-traite à un autre sous-traitant, sauf autorisation expresse du responsable du traitement.

Art. 88

Toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 89

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Un accord définit les obligations respectives des responsables conjoints de traitement, notamment en ce qui concerne l'exercice des droits de la personne concernée et la communication des données à caractère personnel, sauf si leurs obligations respectives sont définies par ou en vertu d'une loi.

Un seul point de contact pour les personnes concernées peut être désigné dans l'accord.

Section 3

Sécurité des données à caractère personnel

Art. 90

Le responsable du traitement ainsi que le sous-traitant prennent les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures assurent un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels.

Art. 91

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk zo snel mogelijk aan de bevoegde toezichthoudende autoriteit.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke zo snel mogelijk van elke inbreuk op de beveiliging.

§ 3. In de in paragrafen 1 en 2 bedoelde melding wordt het volgende omschreven of meegedeeld:

a) de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en persoonsgegevensbestanden in kwestie;

b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

c) de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

d) de maatregelen die de verwerkingsverantwoordelijke, of de verwerker heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder in voorkomend geval maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Afdeling 4

Registers

Art. 92

§ 1. De verwerkingsverantwoordelijke houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van de gegevensbanken van de inlichtingen- en veiligheidsdiensten en deze die aan hem ter beschikking worden gesteld.

Dit register bevat de volgende gegevens:

1° voor de gegevensbanken van de inlichtingen- en veiligheidsdiensten:

a) de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden;

c) de categorieën van voornaamste ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

d) indien mogelijk, de beoogde termijnen voor het verwijderen van de persoonsgegevens;

Art. 91

§ 1er. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie à l'autorité de contrôle compétente dans les meilleurs délais.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais.

§ 3. La notification visée aux paragraphes 1 et 2 doit, à tout le moins:

a) décrire la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la brèche de sécurité;

d) décrire les mesures prises ou que le responsable du traitement ou le sous-traitant propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Section 4

Registres

Art. 92

§ 1er. Le responsable du traitement tient un registre, classifié au sens de la loi du 11 décembre 1998, des banques de données des services de renseignement et de sécurité et de celles mises à leur disposition.

Ce registre comporte les informations suivantes:

1° pour les banques de données des services de renseignement et de sécurité:

a) les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) les catégories de destinataires auxquels des données à caractère personnel peuvent être communiquées;

d) dans la mesure du possible, les délais prévus pour l'effacement des données à caractère personnel;

e) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 90.

2° voor gegevensbanken die aan de inlichtingen- en veiligheidsdiensten ter beschikking gesteld worden:

a) indien mogelijk, de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de gezamenlijke verwerkingsverantwoordelijken en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden van de inlichtingen- en veiligheidsdiensten.

§ 2. Elke verwerker houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.

Dit register bevat de volgende elementen:

a) de contactgegevens van de verwerker en van de verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, in voorkomend geval, van de functionaris voor gegevensbescherming;

b) de categorieën van verwerkingen die voor rekening van de verwerkingsverantwoordelijke zijn uitgevoerd;

c) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 90.

§ 3. De in de paragrafen 1 en 2 bedoelde registers zijn in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 4. De verwerkingsverantwoordelijke stelt het register ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

De verwerker stelt het register ter beschikking van de verwerkingsverantwoordelijke en stelt het eveneens ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 93

§ 1. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker, wijzen een functionaris voor gegevensbescherming aan. Deze beslissing wordt meegedeeld aan de bevoegde toezichthoudende autoriteit.

De functionaris voor gegevensbescherming is titularis van een veiligheidsmachtiging “zeer geheim”, in de zin van de wet van 11 december 1998.

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l’article 90.

2° pour les banques de données mises à la disposition des services de renseignement et de sécurité:

a) si possible, les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement par le service de renseignement et de sécurité.

§ 2. Chaque sous-traitant tient un registre, classifié au sens de la loi du 11 décembre 1998, de toutes les catégories d’activités de traitement effectuées pour le compte d’un responsable du traitement.

Ce registre comprend les éléments suivants:

a) les coordonnées du sous-traitant et du responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les coordonnées du délégué à la protection des données;

b) les catégories de traitements effectués pour le compte du responsable du traitement;

c) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l’article 90.

§ 3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

§ 4. Le responsable du traitement met le registre à la disposition de l’autorité de contrôle compétente à sa demande.

Le sous-traitant met le registre à la disposition du responsable du traitement ainsi qu’à la disposition de l’autorité de contrôle compétente à sa demande.

Section 5

Délégué à la protection des données

Art. 93

§ 1er. Le responsable du traitement et, le cas échéant, le sous-traitant désignent un délégué à la protection des données. Cette décision est communiquée à l’autorité de contrôle compétente.

Le délégué à la protection des données est titulaire d’une habilitation de sécurité de niveau très secret, au sens de la loi du 11 décembre 1998.

De functionaris voor gegevensbescherming kan niet van zijn functie ontheven of gestraft worden omwille van de uitvoering van zijn opdrachten.

Hij is, op een onafhankelijke wijze, belast met de volgende taken:

— toezien op de naleving van deze ondertitel voor elke verwerking van persoonsgegevens;

— adviseren over alle nuttige maatregelen teneinde de veiligheid van de opgeslagen gegevens te verzekeren;

— de verwerkingsverantwoordelijke, en in voorkomend geval de verwerker, het diensthoofd en de personeelsleden van de betrokken dienst die de verwerking verrichten informeren en adviseren over hun verplichtingen op grond van deze ondertitel;

— adviezen of aanbevelingen verstrekken aan de verwerkingsverantwoordelijke, en in voorkomend geval aan de verwerker of het diensthoofd;

— het uitvoeren van de andere opdrachten die hem door de verwerkingsverantwoordelijke, en in voorkomend geval de verwerker of het diensthoofd toevertrouwd zijn.

De functionaris voor gegevensbescherming is de contactpersoon voor de bevoegde toezichthoudende autoriteit met betrekking tot de toepassing van deze ondertitel.

§ 2. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker ziet erop toe dat hun functionaris voor gegevensbescherming tijdig en naar behoren wordt betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden.

§ 3. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker ziet erop toe dat de functionaris voor gegevensbescherming de benodigde middelen ter beschikking heeft voor het vervullen van zijn taken.

De functionaris voor gegevensbescherming kan worden bijgestaan door één of meerdere medewerkers.

§ 4. In voorkomend geval worden nadere regels voor de werking, de aanwijzing en de vereiste bevoegdheden door de Koning bepaald.

Le délégué à la protection des données ne peut pas être relevé de ses fonctions ou sanctionné en raison de l'exercice de ses missions.

Il est chargé de manière indépendante:

— de veiller au respect du présent sous-titre lors de tout traitement de données à caractère personnel;

— de conseiller toutes mesures utiles afin d'assurer la sécurité des données enregistrées;

— d'informer et conseiller le responsable du traitement, et le cas échéant le sous-traitant, le dirigeant et le personnel du service concerné procédant au traitement sur les obligations qui leur incombent en vertu du présent sous-titre;

— de fournir des avis ou des recommandations au responsable du traitement, et le cas échéant au sous-traitant, et au dirigeant du service;

— d'exécuter d'autres missions qui lui sont confiées par le responsable du traitement, le cas échéant le sous-traitant ou le dirigeant du service.

Le délégué à la protection des données est le point de contact avec l'autorité de contrôle compétente pour l'application du présent sous-titre.

§ 2. Le responsable du traitement et, le cas échéant le sous-traitant, veille à ce que son délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

§ 3. Le responsable du traitement et, le cas échéant le sous-traitant veille à ce que son délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

§ 4. Le cas échéant, les modalités de fonctionnement, de désignation ainsi que les compétences requises peuvent être définies par le Roi.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van persoonsgegevens aan de publieke sector en de private sector

Art. 94

In afwijking van de artikelen 22, 26, 28, 60 en 61 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen een inlichtingen- en veiligheidsdienst en enig openbaar of privé orgaan, in het belang van de uitvoering van de opdrachten van de inlichtingen- en veiligheidsdiensten.

Deze mededeling vindt plaats in overeenstemming met de artikelen 14, 16 en 19 van de wet van 30 november 1998.

Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 22, § 1, derde lid, het volgende:

1. de identificatie van de inlichtingen- en veiligheidsdienst en het openbaar of particulier orgaan die de persoonsgegevens uitwisselen;

2. de identificatie van de verwerkingsverantwoordelijken;

3. de contactgegevens van de functionarissen voor gegevensbescherming;

4. de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5. de wettelijke grondslag;

6. de beperkingen met betrekking tot de rechten van de betrokkene.

Afdeling 2

Doorgifte van persoonsgegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 95

Persoonsgegevens mogen slechts worden doorgegeven aan een land dat geen lid is van de Europese Unie of een internationale organisatie, indien dat land of die organisatie een passend beschermingsniveau en de naleving van de andere bepalingen van deze ondertitel waarborgt.

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données à caractère personnel avec le secteur public et le secteur privé

Art. 94

Par dérogation aux articles 22, 26, 28, 60 et 61 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme préalable à la communication de données à caractère personnel entre un service de renseignement et de sécurité et tout organisme public ou privé dans l'intérêt de l'exercice des missions des services de renseignement et de sécurité.

Cette communication se déroule conformément aux articles 14, 16 et 19 de la loi du 30 novembre 1998.

Par dérogation à l'article 22, § 1er, alinéa 3, lorsque les parties décident de conclure un protocole, celui-ci porte notamment sur:

1. l'identification du service de renseignement et de sécurité et de l'organisme public ou privé qui échangent les données à caractère personnel;

2. l'identification des responsables du traitement;

3. les coordonnées des délégués à la protection des données concernés;

4. les finalités pour lesquelles les données à caractère personnel sont transférées;

5. la base légale;

6. les restrictions aux droits de la personne concernée.

Section 2

Transfert des données à caractère personnel vers des pays non membres de l'Union européenne ou à des organisations internationales

Art. 95

Le transfert de données à caractère personnel vers un pays non membres de l'Union européenne ou vers une organisation internationale ne peut avoir lieu que si le pays ou l'organisation en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions du présent sous-titre.

De vraag of het beschermingsniveau passend is, wordt beoordeeld met inachtneming van alle omstandigheden die betrekking hebben op de doorgifte van persoonsgegevens of op een categorie van doorgiften van persoonsgegevens; in het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen of organisaties worden nageleefd.

Het passende beschermingsniveau kan verzekerd worden door veiligheidsclausules tussen de verwerkingsverantwoordelijke en de ontvanger van de persoonsgegevens.

Art. 96

In afwijking van artikel 95 mag een doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie, hetwelke geen waarborgen biedt voor een passend beschermingsniveau, slechts plaatsvinden wanneer:

1. de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven; of

2. de doorgifte verplicht is in het kader van de internationale betrekkingen; of

3. de doorgifte noodzakelijk is ter vrijwaring van het vitaal belang van de personen; of

4. de doorgifte noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend openbaar belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 97

In afwijking van het bepaalde in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, is het Vast Comité I, in zijn hoedanigheid van onafhankelijke publieke autoriteit, aangeduid als gegevensbeschermingsautoriteit belast met de controle van de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten en hun verwerkers volgens de nadere regels vastgelegd in de wet van 18 juli 1991.

Hij waakt over de toepassing van deze ondertitel ter bescherming van de fundamentele rechten en vrijheden van de natuurlijke personen met betrekking tot deze verwerking.

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données à caractère personnel ou à une catégorie de transferts de données à caractère personnel; il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays ou l'organisation en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

Le niveau de protection adéquat peut être assuré par des clauses de sécurité entre le responsable du traitement et le destinataire des données à caractère personnel.

Art. 96

Par dérogation à l'article 95, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale n'assurant pas un niveau de protection adéquat, peut être effectué lorsque:

1. la personne concernée a indubitablement donné son consentement au transfert envisagé; ou

2. le transfert est obligatoire dans le cadre de des relations internationales; ou

3. le transfert est nécessaire à la sauvegarde de l'intérêt vital des personnes; ou

4. le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

CHAPITRE X

Autorité de contrôle

Art. 97

Par dérogation à la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, le Comité permanent R, en sa qualité d'autorité publique indépendante, est désigné comme autorité de protection des données chargée du contrôle du traitement des données à caractère personnel par les services de renseignement et de sécurité et par leurs sous-traitants selon les modalités fixées par la loi du 18 juillet 1991.

Il surveille l'application du présent sous-titre afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard dudit traitement.

Art. 98

Het Vast Comité I werkt, indien nodig, samen met de andere belgische toezichthoudende autoriteiten, zonder dat dit afbreuk doet aan de fysieke integriteit van personen, of aan de opdrachten van de inlichtingen- en veiligheidsdiensten en de wet van 11 december 1998.

In het kader van de uitoefening van het toezicht bedoeld in artikel 97, deelt het Vast Comité I in algemene termen het resultaat hiervan mee aan de andere bevoegde toezichthoudende autoriteiten . Deze maken deze resultaten niet aan de betrokkene over.

Art. 99

De inlichtingen- en veiligheidsdiensten en hun verwerkers werken samen met het Vast Comité I.

Art. 100

Een toezichthoudende autoriteit informeert het Vast Comité I over inbreuken op de reglementering inzake de verwerking van persoonsgegevens van de inlichtingen- en veiligheidsdiensten zodra zij er kennis van neemt.

Elke toezichthoudende autoriteit overlegt met het Vast Comité I wanneer zij gevat wordt in een dossier dat mogelijk gevolgen heeft voor de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden

Art. 101

In afwijking van titel 4, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens van de inlichtingen- en veiligheidsdiensten en van hun personeel toegestaan door de betrokken inlichtingen- en veiligheidsdienst indien dit geen afbreuk doet aan zijn opdrachten, aan zijn verplichtingen bedoeld in de artikelen 13, derde lid en 13/4, tweede lid van de wet van 30 november 1998, aan een lopend opsporings- of gerechtelijk onderzoek, of aan de betrekkingen die België met vreemde staten of internationale organisaties onderhoudt en overeenkomstig de wet van 11 december 1998.

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens van de inlichtingen- en veiligheidsdiensten en van hun personeel voor overige doelen dan die bedoeld in het eerste lid wordt geweigerd, behalve met uitdrukkelijke toestemming van de betrokken inlichtingen- en veiligheidsdienst die de voorwaarden van deze verwerking bepaalt.

Art. 98

Le Comité permanent R coopère, le cas échéant, avec les autres autorités de contrôle belges, sans que cela ne porte atteinte à l'intégrité physique d'une personne, ou aux missions des services de renseignement et de sécurité et de la loi du 11 décembre 1998.

Dans le cadre de l'exercice du contrôle visé à l'article 97, le Comité permanent R communique le résultat de celui-ci en termes généraux aux autres autorités de contrôle compétentes. Celles-ci ne tranmettent pas ces résultats à la personne concernée.

Art. 99

Les services de renseignement et de sécurité et leurs sous-traitants coopèrent avec le Comité permanent R.

Art. 100

Lorsqu'elle en prend connaissance, une autorité de contrôle informe le Comité permanent R des violations de la règlementation relative aux traitements de données à caractère personnel des services de renseignement et de sécurité.

Toute autorité de contrôle saisie d'un dossier susceptible d'avoir une répercussion sur le traitement de données à caractère personnel par les services de renseignement et de sécurité se concerte avec le Comité permanent R.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 101

Par dérogation au titre 4, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel des services de renseignement et de sécurité et de leur personnel par un responsable du traitement ultérieur est autorisée par le service de renseignement et de sécurité concerné si cela ne porte pas atteinte à ses missions, à ses obligations visées aux articles 13, alinéa 3 et 13/4, alinéa 2 de la loi du 30 novembre 1998, à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales et conformément à la loi du 11 décembre 1998.

Toute demande adressée aux Archives de l'État de traitement ultérieur de données à caractère personnel des services de renseignement et de sécurité et de leur personnel à d'autres fins que celles visées à l'alinéa premier est refusée, sauf autorisation expresse du service de renseignement et de sécurité concerné qui fixe les conditions dudit traitement.

Art. 102

Vóór hun raadpleging bedoeld in artikel 101 moeten de persoonsgegevens voorzien worden van de vermelding “Bescherming van persoonsgegevens – artikelen 101 tot 106 van de wet van xx/xx/2018”.

Art. 103

De persoonsgegevens bedoeld in artikel 101 worden voorafgaand aan hun raadpleging geanonimiseerd.

Indien een verdere verwerking van anonieme gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan de inlichtingen- en veiligheidsdienst de raadpleging van gepseudonimiseerde gegevens toestaan.

Indien de anonimisering of pseudonimisering de identificatie van de gegevens niet onmogelijk maakt, weigert de inlichtingen- en veiligheidsdienst de raadpleging indien dit een onevenredige afbreuk doet aan het privéleven.

Indien een verdere verwerking van gepseudonimiseerde gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan de inlichtingen- en veiligheidsdienst de raadpleging van niet-gepseudonimiseerde gegevens toestaan indien dit geen onevenredige afbreuk doet aan het privéleven.

Art. 104

In afwijking van titel 4, is een mededeling of publicatie van niet-geanonimiseerde of niet-gepseudonimiseerde persoonsgegevens bedoeld in artikel 101, geraadpleegd door de verdere verwerkingsverantwoordelijke, enkel mogelijk met het akkoord van de betrokken inlichtingen- en veiligheidsdienst en onder de voorwaarden die hij vastlegt.

Art. 105

De verdere verwerkingsverantwoordelijke van persoonsgegevens bedoeld in artikel 101 houdt een logboek van zijn verdere verwerkingsactiviteiten voor historische, wetenschappelijke of statistische doeleinden bij.

Dit logboek is geclassificeerd in de zin van de wet van 11 december 1998 indien de verwerking betrekking heeft op geclassificeerde gegevens.

Dit logboek bevat de volgende informatie:

1. de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming van deze laatste;

2. de doeleinden van de verdere verwerking;

Art. 102

Avant leur consultation visée à l’article 101, les données à caractère personnel doivent être marquées de la mention “Protection des données à caractère personnel – articles 101 à 106 de la loi du xx/xx/2018”.

Art. 103

Les données à caractère personnel visées à l’article 101 sont rendues anonymes préalablement à leur consultation.

Si un traitement ultérieur de données anonymes ne permet pas d’atteindre les fins historiques, scientifiques ou statistiques, le service de renseignement et de sécurité peut autoriser la consultation de données pseudonymisées.

Si l’anonymisation ou la pseudonymisation ne rend pas l’identification des données impossible, le service de renseignement et de sécurité refuse la consultation si cela constitue une atteinte disproportionnée à la vie privée.

Si un traitement ultérieur de données pseudonymisées ne permet pas d’atteindre les fins historiques, scientifiques ou statistiques, le service de renseignement et de sécurité peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 104

Par dérogation au titre 4, une communication ou publication des données à caractère personnel visées à l’article 101 non anonymisées ou non pseudonymisées, consultées par le responsable du traitement ultérieur n’est possible qu’avec l’accord du service de renseignement et de sécurité concerné et sous les conditions que celui-ci aura fixées.

Art. 105

Le responsable du traitement ultérieur des données à caractère personnel visées à l’article 101 tient un journal de ses activités de traitement ultérieur à des fins historiques, scientifiques ou statistiques.

Ce journal est classifié au sens de la loi du 11 décembre 1998 si le traitement porte sur des données classifiées.

Ce journal comporte les informations suivantes:

1. les coordonnées du responsable du traitement initial, du responsable du traitement ultérieur et du délégué à la protection des données de ce dernier;

2. les finalités du traitement ultérieur;

3. de gegevens die het voorwerp uitmaken van de verdere verwerking;

4. de eventuele voorwaarden voor de verdere verwerking vastgelegd door de betrokken inlichtingen- en veiligheidsdienst;

5. de eventuele ontvangers toegestaan door de betrokken inlichtingen- en veiligheidsdienst.

Art. 106

Elke overheidsinstantie of elke natuurlijke of rechtspersoon die persoonsgegevens bedoeld in artikel 101 verwerkt om historische, wetenschappelijke of statistische doeleinden is de verantwoordelijke van deze verwerking.

Hij mag geen handelingen verrichten die zijn gericht op de omzetting van anonieme of gepseudonimiseerde gegevens in persoonsgegevens.

ONDERTITEL 2

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR DE KRIJSMACHT

Art. 107

In afwijking van artikel 2, tweede lid, is bij de aanwending van de krijgsmacht, en de paraatstelling met het oog op de aanwending van de krijgsmacht, is het volgende regime van toepassing:

1. de Krijgsmacht verwerkt, voor zover noodzakelijk voor het belang van de uitoefening van hun opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of de seksuele geaardheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen;

2. de persoonsgegevens mogen slechts verwerkt worden wanneer de verwerking nuttig is voor de aanwending of de paraatstelling met het oog op de aanwending van de krijgsmacht;

3. de persoonsgegevens dienen toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4. de persoonsgegevens dienen nauwkeurig te zijn en, zo nodig, te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor

3. les données faisant l'objet du traitement ultérieur;

4. les éventuelles conditions du traitement ultérieur fixées par le service de renseignement et de sécurité concerné;

5. les éventuels destinataires autorisés par le service de renseignement et de sécurité concerné.

Art. 106

Toute autorité publique ou toute personne physique ou morale qui traite des données à caractère personnel visées à l'article 101 à des fins historiques, scientifiques ou statistiques est responsable dudit traitement.

Elle n'entreprendra aucune action pour convertir des données anonymes ou pseudonymisées en données à caractère personnel.

SOUS-TITRE 2

LA PROTECTION DES PERSONNES PHYSIQUES CONCERNANT LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL PAR LES FORCES ARMEES

Art. 107

Par dérogation à l'article 2, alinéa 2, le régime suivant est d'application lors de la mise en œuvre des forces armées et de la mise en condition en vue de la mise en œuvre des forces armées:

1. pour autant que cela soit nécessaire dans l'exercice de leurs missions, les forces armées traitent des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes;

2. les données à caractère personnel ne peuvent être traitées que lorsque le traitement est utile pour la mise en œuvre des forces armées ou la mise en condition des forces armées;

3. les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4. les données à caractère personnels doivent être exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités

zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren.

5. de persoonsgegevens mogen doorgegeven worden aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie indien die doorgifte noodzakelijk is voor operationele redenen;

6. met uitzondering van de definities vervat in artikel 31 en van de artikelen 2, 33, 77, 80, 84 tot en met 91 zijn de bepalingen van de andere titels niet van toepassing;

7. met betrekking tot de verwerking van persoonsgegevens worden de volgende rechten slechts beperkt indien dit een noodzakelijke en evenredige maatregel vormt voor de aanwending van de krijgsmacht of paraatstelling met het oog op aanwending van de krijgsmacht:

— het recht kennis te nemen van het bestaan van een geautomatiseerd bestand van persoonsgegevens, de voornaamste doeleinden hiervan, alsmede de identiteit en de gewone verblijfplaats of de hoofdvestiging van de houder van het bestand;

— het recht om in voorkomend geval die gegevens te doen verbeteren of uitwissen, indien deze zijn verwerkt in strijd met de wet;

— het recht over een rechtsmiddel te beschikken, indien geen gevolg wordt gegeven aan een verzoek om uitsluitsel of, al naargelang het geval, mededeling, verbetering of uitwisseling van persoonsgegevens.

8. in de mate dat deze de aanwending en de paraatstelling van de Krijgsmacht niet in het gedrang mag brengen zijn de verwerkingen van persoonsgegevens onderworpen aan het toezicht van de bevoegde toezichthoudende autoriteit.

ONDERTITEL 3

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS IN HET KADER VAN DE WET VAN 11 DECEMBER 1998 BETREFFENDE DE CLASSIFICATIE EN DE VEILIGHEIDSMACHTIGINGEN, VEILIGHEIDSATTESTEN EN VEILIGHEIDSADVIEZEN.

HOOFDSTUK I

Definities

Art. 108

§ 1. De definities bedoeld in artikel 31, 1° tot 6°, 9°, 11° tot 14°, en 16° tot 17°, zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder:

1. “de Verordening”: Verordening (EU) 2016/679 van Het Europees Parlement en de Raad van 27 april 2016 betreffende

pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

5. les données à caractère personnel peuvent être transmises vers un pays non membres de l’Union Européenne ou vers une organisation internationale dans le cas où ce transfert est nécessaire pour des raisons opérationnelles;

6. à l’exception des définitions dans l’article 31 et les articles 2, 33, 77, 80, 84 à 91 , les dispositions des autres titres ne sont pas d’application;

7. concernant le traitement des données à caractère personnel, les droits suivants sont limités lorsqu’il s’agit d’une mesure nécessaire et proportionnelle pour la mise en œuvre des forces armées, ou la mise en condition des forces armées en vue de leur mise en œuvre:

— le droit de prendre connaissance de l’existence d’un fichier de données automatisée à caractère personnel, de ses principaux objectifs ainsi que de l’identité et de la résidence habituelle ou de l’établissement principal du titulaire du fichier;

— le droit de faire corriger ou d’effacer ces données si nécessaire, si celles-ci ont été traitées en violation de la loi;

— le droit de disposer de voies de recours en l’absence de réponse à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d’échange de données à caractère personnel.

8. dans la mesure où ceci ne peut pas mettre en péril la mise en œuvre et la mise en condition des forces armées, le traitement des données à caractère personnelle est soumis à l’autorité de contrôle.

SOUS-TITRE 3

DE LA PROTECTION DES PERSONNES PHYSIQUES A L’EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL DANS LE CADRE DE LA LOI DU 11 DECEMBRE 1998 RELATIVE À LA CLASSIFICATION ET AUX HABILITATIONS, ATTESTATIONS ET AVIS DE SÉCURITÉ

CHAPITRE I^ER

Définitions

Art. 108

§ 1^er. Les définitions visées à l’article 31, 1° à 6°, 9°, 11° à 14°, et 16° à 17°, sont applicables au présent sous-titre.

§ 2. Pour l’application du présent sous-titre, on entend par:

1. “le Règlement”: le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la

de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;

2. "de wet van 11 december 1998": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

3. "de wet van 11 december 1998 tot oprichting van een beroepsorgaan": de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

4. "beroepsorgaan": het beroepsorgaan bedoeld in artikel 3 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan;

5. "de verwerkingsverantwoordelijke": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

6. "toezichthoudende autoriteit": de onafhankelijke overheidsinstantie die bij de wet belast is met het toezicht op de toepassing van deze ondertitel, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met verwerking te beschermen.

HOOFDSTUK II

Toepassingsgebied

Art. 109

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens in het kader van veiligheidsmachtigingen, attesten en adviezen bedoeld in de wet van 11 december 1998 door:

1° de veiligheidsoverheid bedoeld in artikel 15, eerste lid, van de wet van 11 december 1998;

2° elke overheidslid van de overheid bedoeld in 1°;

3° de overheden bedoeld in artikelen 15, tweede lid en 22*ter* van de wet van 11 december 1998;

4° de veiligheidsofficieren bedoeld in artikel 13, 1°, van de wet van 11 december 1998;

5° de verwerkers van overheden en personen bedoeld in 1°tot 4°.

Deze ondertitel is ook van toepassing op elke verwerking van persoonsgegevens door het beroepsorgaan in het kader van de beroepsprocedures bedoeld in de wet van 11 december 1998 tot oprichting van het beroepsorgaan.

protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

2. 2° "la loi du 11 décembre 1998": la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

3. "la loi du 11 décembre 1998 portant création d'un organe de recours": Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité;

4. "l'organe de recours": l'organe de recours visé à l'article 3 de la loi du 11 décembre 1998 portant création d'un organe de recours;

5. "le responsable du traitement": la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles;

6. "autorité de contrôle": l'autorité publique indépendante chargée par la loi de surveiller l'application du présent sous-titre, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement.

CHAPITRE II

Champ d'application

Art. 109

Le présent sous-titre s'applique à tout traitement de données à caractère personnel dans le cadre des habilitations de sécurité, attestations et avis de sécurité visés dans la loi du 11 décembre 1998 par:

1° l'autorité de sécurité visée à l'article 15, alinéa 1er, de la loi du 11 décembre 1998;

2° chaque autorité membre de l'autorité visée au 1°;

3° les autorités visées aux articles 15, alinéa 2, et 22*ter* de la loi du 11 décembre 1998;

4° les officiers de sécurité visés à l'article 13, 1°, de la loi du 11 décembre 1998 ;

5° les sous-traitants des autorités et personnes visées aux 1° à 4°.

Le présent sous-titre s'applique également à chaque traitement de données à caractère personnel par l'organe de recours dans le cadre des recours visés dans la loi du 11 décembre 1998 portant création d'un organe de recours.

Met uitzondering van deze ondertitel en artikelen 239 en 240, zijn de titels 1 tot 7 van deze wet niet van toepassing op de verwerkingen bedoeld in het eerste en tweede lid.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 110

Persoonsgegevens mogen slechts verwerkt worden in één van de volgende gevallen:

1. wanneer de betrokkene daarvoor ondubbelzinnig zijn toestemming verleend;

2. wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;

3. wanneer de verwerking noodzakelijk is om een verplichting na te komen waaraan de verwerkingsverantwoordelijke is onderworpen door of krachtens een wet;

4. wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verwerkingsverantwoordelijke of aan de derde aan wie de persoonsgegevens worden verstrekt.

Art. 111

Persoonsgegevens moeten:

1. worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig en behoorlijk is;

2. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden. Onder de voorwaarden vastgesteld door de artikelen 134 tot en met 139 wordt verdere verwerking van de gegevens voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd;

3. toereikend, ter zake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4. nauwkeurig te zijn en, zo nodig, te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren.

A l'exception du présent sous-titre, et les articles 239 et 240, les titres 1 à 7 de la présente loi ne s'appliquent pas aux traitements visés aux alinéas premier et 2.

CHAPITRE III

Conditions générales du traitement

Art. 110

Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants:

1. lorsque la personne concernée a indubitablement donné son consentement;

2. lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

3. lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi;

4. lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou une autorité publique à laquelle les données à caractère personnel sont communiquées.

Art. 111

Les données à caractère personnel doivent être:

1. traitées d'une manière qui est loyal et légitime à l'égard de la personne concernée;

2. collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et réglementaires applicables. Un traitement ultérieur à des fins historiques, scientifiques ou statistiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par les articles 134 à 139;

3. adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4. exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

HOOFDSTUK IV

Aard van de persoonsgegevens

Art. 112

Overheden, organen en personen bedoeld in artikel 109 verwerken, in het belang van de uitoefening van haar opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of de seksuele geaardheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 113

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen werden en volgens de modaliteiten bepaald in artikel 25 van de wet van 11 december 1998.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 114

Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.

Art. 115

De betrokkene heeft het recht te vragen overeenkomstig artikel 116:

1. om toegang tot zijn persoonsgegevens;

2. om zijn onjuiste persoonsgegevens te laten verbeteren of;

3. de verificatie bij de bevoegde toezichthoudende autoriteit van de naleving van de bepalingen van deze ondertitel;

Art. 116

§ 1. Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van de verwerking te waarborgen, is de toegang

CHAPITRE IV

Nature des données à caractère personnel

Art. 112

Dans l'intérêt de l'exercice de leurs missions, les autorités, l'organe de recours et les personnes visés à l'article 109 traitent des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

CHAPITRE V

Conservation des données à caractère personnel

Art. 113

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées à l'article 25 de la loi du 11 décembre 1998.

CHAPITRE VI

Droits de la personne concernée

Art. 114

Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 115

La personne concernée a le droit de demander conformément à l'article 116:

1. l'accès à ses données à caractère personnel;

2. la rectification ou la suppression de ses données à caractère personnel inexactes;

3. la vérification auprès de l'autorité de contrôle compétente du respect des dispositions du présent sous- titre.

Art. 116

§ 1er. Afin de garantir la confidentialité et l'efficacité de l'exécution des traitements, l'accès de la personne concernée

van de betrokkene tot zijn persoonsgegevens verwerkt in het kader van artikel 109, eerste lid, beperkt tot de informatie die de betrokkene aanlevert.

Voor de uitoefening van zijn rechten bedoeld in artikel 115, 2° en 3°, ten aanzien van de verwerking bedoeld in artikel 109, eerste lid, richt de betrokkene, die zijn identiteit bewijst, zich kosteloos tot de bevoegde toezichthoudende autoriteit. Deze voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht.

§ 2. De toegang van de betrokkene tot zijn persoonsgegevens verwerkt door het beroepsorgaan verloopt conform het artikel 6 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan.

Voor de uitoefening van zijn rechten bedoeld in artikel 115, 2°, en ten aanzien van de verwerking bedoeld in artikel 109, tweede lid, richt de betrokkene zich tot het beroepsorgaan conform de modaliteiten bepaald door of krachtens de wet van 11 december 1998 tot oprichting van een beroepsorgaan.

Art. 117

Een besluit waaraan voor een persoon negatieve rechtsgevolgen verbonden zijn, mag niet louter worden genomen op grond van een geautomatiseerde persoonsgegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.

Het in het eerste lid vastgestelde verbod geldt niet indien het besluit zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet of wanneer het noodzakelijk is vanwege een zwaarwegend openbaar belang.

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 118

De verwerkingsverantwoordelijke moet:

1. er nauwlettend over waken dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet ter zake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2. ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot hetgeen wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst;

à ses données à caractère personnel traités par les autorités et personnes visées à l'article 109, alinéa premier, est limité à l'information que la personne concernée leur fournit.

Pour l'exercice de ses droits visés à l'article 115, 2° en 3°, à l'égard du traitement visé à l'article 109, alinéa premier, la personne concernée justifiant de son identité s'adresse, sans frais, à l'autorité de contrôle compétente. Celle-ci effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

§ 2. L'accès par la personne concernée à ses données à caractère personnel traitées par l'organe de recours s'effectue conformément à l'article 6 de la loi du 11 décembre 1998 portant création d'un organe de recours.

Pour l'exercice de ses droits visés à l'article 115, 2°, à l'égard du traitement visé à l'article 109, l'alinéa 2, la personne concernée s'adresse à l'organe de recours conformément aux modalités fixées par ou en vertu la loi du 11 décembre 1998 portant création d'un organe de recours.

Art. 117

Une décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

L'interdiction prévue à l'alinéa premier ne s'applique pas lorsque la décision est fondée sur une disposition prévue par ou en vertu d'une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important.

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 118

Le responsable du traitement doit:

1. faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2. veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins du service;

3. alle personen die onder zijn gezag handelen, kennisgeven van de bepalingen van deze ondertitel en van alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer die bij het verwerken van persoonsgegevens gelden.

Art. 119

Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verwerkingsverantwoordelijke:

1. een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking;

2. toezien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen;

3. de aansprakelijkheid van de verwerker vaststellen in de overeenkomst;

4. met de verwerker overeenkomen dat de verwerker slechts handelt in opdracht van de verwerkingsverantwoordelijke en dat de verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke in toepassing van deze ondertitel is gehouden.

Art. 120

De verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke is gehouden.

Hij mag de verwerking van persoonsgegevens, die hij verwerkt, niet toevertrouwen aan een andere verwerker, behoudens uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Art. 121

Eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verwerkingsverantwoordelijke verwerken, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 122

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken.

3. informer les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 119

Lorsque le traitement est confié à un sous-traitant, le responsable du traitement doit:

1. choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements;

2. veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles;

3. fixer dans le contrat la responsabilité du sous-traitant;

4. convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et qu'il est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du présent sous-titre.

Art. 120

Le sous-traitant est soumis aux mêmes obligations que celles qui incombent au responsable du traitement.

Il ne peut pas confier le traitement de données à caractère personnel qu'il sous-traite à un autre sous-traitant, sauf autorisation expresse du responsable du traitement.

Art. 121

Toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 122

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Een onderlinge regeling bepaalt de respectievelijke verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken, met name met betrekking tot de uitoefening van de rechten van de betrokkene en de mededeling van persoonsgegevens, tenzij hun respectievelijke verantwoordelijkheden zijn vastgesteld door of krachtens een wet.

In de onderlinge regeling kan één contactpunt voor betrokkenen worden aangewezen.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 123

Om de veiligheid van de persoonsgegevens te waarborgen, treffen de verwerkingsverantwoordelijke, alsmede de verwerker, de passende technische en organisatorische maatregelen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen verzekeren een passend beveiligingsniveau, rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen persoonsgegevens en de potentiële risico's.

Art. 124

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk zo snel mogelijk aan de bevoegde toezichthoudende autoriteit.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke zo snel mogelijk van elke inbreuk op de beveiliging.

§ 3. In de in paragraaf 1 en 2 bedoelde melding wordt het volgende omschreven of meegedeeld:

1. de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en persoonsgegevensbestanden in kwestie;

2. de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

3. de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4. de maatregelen die verwerkingsverantwoordelijke, of de verwerker heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder in voorkomend geval maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Un accord définit les obligations respectives des responsables conjoints de traitement, notamment en ce qui concerne l'exercice des droits de la personne concernée et la communication des données à caractère personnel, sauf si leurs obligations respectives sont définies par ou en vertu d'une loi.

Un seul point de contact pour les personnes concernées peut être désigné dans l'accord.

Section 3

Sécurité des données à caractère personnel

Art. 123

Le responsable du traitement ainsi que le sous-traitant prennent les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures assurent un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels.

Art. 124

§ 1er. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie à l'autorité de contrôle compétente dans les meilleurs délais.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais.

§ 3. La notification visée aux paragraphes 1er et 2 doit, à tout le moins, décrire ou communiquer:

1. la nature de la brèche de sécurité y compris et, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2. le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3. les conséquences probables de la brèche de sécurité;

4. les mesures prises ou que le responsable du traitement ou le sous-traitant propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Afdeling 4

Registers

Art. 125

§ 1. De verwerkingsverantwoordelijke, en desgevallend zijn verwerker, houdt een register bij van de verwerkingsactiviteiten van persoonsgegevens.

Dit register bevat, indien toepasselijk en mogelijk, de volgende gegevens voor wat betreft de activiteitent van de verwerking:

1. de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

2. de verwerkingsdoeleinden;

3. de categorieën van betrokkenen;

4. de categorieën van persoonsgegevens;

5. de categorieën van voornaamste ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

6. de doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in voorkomend geval, de documenten inzake de passende waarborgen;

7. de beoogde termijnen voor het verwijderen van de persoonsgegevens;

8. het gebruik van profilering;

9. de rechtsgrondslag;

10. een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 123.

§ 2. De in de eerste paragraaf bedoelde registers zijn in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 3. De verwerkingsverantwoordelijke stelt het register ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

De verwerker stelt het register ter beschikking van de verwerkingsverantwoordelijke en stelt het eveneens ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

Section 4

Registres

Art. 125

§ 1er. Le responsable du traitement, et le cas échéant son sous-traitant, tient un registre d'activités de traitement des données à caractère personnel.

Ce registre comporte, le cas échéant et si possible, les informations suivantes en ce qui concerne les activités de traitement:

1. les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

2. les finalités du traitement;

3. les catégories des personnes concernées;

4. les catégories des données personnelles;

5. les catégories de destinataires principaux auxquels des données à caractère personnel peuvent être communiquées;

6. les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, le cas échéant, les documents attestant de l'existence de garanties appropriées;

7. les délais prévus pour l'effacement des données à caractère personnel;

8. le recours au profilage;

9. la base juridique;

10. une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 123.

§ 2. Le registre visé au paragraphe premier se présente sous une forme écrite y compris la forme électronique.

§ 3. Le responsable du traitement met le registre à la disposition de l'autorité de contrôle compétente à sa demande.

Le sous-traitant met le registre à la disposition du responsable du traitement ainsi qu'à la disposition de l'autorité de contrôle compétente à sa demande.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 126

§ 1. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker, wijzen een functionaris voor gegevensbescherming aan. Deze beslissing wordt meegedeeld aan de bevoegde toezichthoudende autoriteit.

De functionaris voor gegevensbescherming is titularis van een veiligheidsmachtiging "zeer geheim", in de zin van de wet van 11 december 1998.

De functionaris voor gegevensbescherming kan niet van zijn functie ontheven of gestraft worden omwille van de uitvoering van zijn opdrachten.

Hij is, op een onafhankelijke wijze, belast met de volgende taken:

1. toezien op de naleving van deze ondertitel voor elke verwerking van persoonsgegevens;

2. adviseren over alle nuttige maatregelen met het oog op het verzekeren van de beveiliging van de opgeslagen persoonsgegevens;

3. de verwerkingsverantwoordelijke, en in voorkomend geval de verwerker, en hun personeelsleden die de verwerking verrichten informeren en adviseren over hun verplichtingen op grond van de huidige ondertitel;

4. adviezen of aanbevelingen verstrekken aan de verwerkingsverantwoordelijke, en in voorkomend geval aan de verwerker;

5. het uitvoeren van de andere opdrachten die hem door de verwerkingsverantwoordelijke, en in voorkomend geval de verwerker toevertrouwd zijn.

De functionaris voor gegevensbescherming is de contactpersoon voor de bevoegde toezichthoudende autoriteit met betrekking tot de toepassing van deze ondertitel.

§ 2. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker ziet erop toe dat hun functionaris voor gegevensbescherming tijdig en naar behoren wordt betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden.

§ 3. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker ziet erop toe dat de functionaris voor gegevensbescherming de benodigde middelen ter beschikking heeft voor het vervullen van zijn taken.

De functionaris voor gegevensbescherming kan worden bijgestaan door één of meerdere medewerkers.

Section 5

Délégué à la protection des données

Art. 126

§ 1er. Le responsable du traitement et, le cas échéant, le sous-traitant désignent un délégué à la protection des données. Cette décision est communiquée à l'autorité de contrôle compétente.

Le délégué à la protection des données est titulaire d'une habilitation de sécurité de niveau très secret, au sens de la loi du 11 décembre 1998.

Le délégué à la protection des données ne peut pas être relevé de ses fonctions ou sanctionné en raison de l'exercice de ses missions.

Il est chargé de manière indépendante:

1. de veiller au respect du présent sous-titre lors de tout traitement de données à caractère personnel;

2. de conseiller toutes mesures utiles afin d'assurer la sécurité des données enregistrées;

3. d'informer et conseiller le responsable du traitement, et le cas échéant le sous-traitant, et leur personnel procédant au traitement des obligations qui leur incombent en vertu du présent sous-titre;

4. de fournir des avis ou des recommandations au responsable du traitement, et le cas échéant au sous-traitant;

5. d'exécuter d'autres missions qui lui sont confiées par le responsable du traitement, le cas échéant le sous-traitant.

Le délégué à la protection des données est le point de contact avec l'autorité de contrôle compétente pour l'application du présent sous-titre.

§ 2. Le responsable du traitement et, le cas échéant le sous-traitant, veille à ce que son délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

§ 3. Le responsable du traitement et, le cas échéant le sous-traitant veille à ce que son délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

§ 4. In voorkomend geval worden nadere regels voor de werking, de aanwijzing en de vereiste bevoegdheden door de Koning bepaald.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van persoonsgegevens aan de publieke sector en de private sector

Art. 127

§ 1. In afwijking van de artikelen 22, 26, 28, 60 en 61 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen de overheid, het beroepsorgaan of de persoon bedoeld in artikel 109 en enig openbaar of privé orgaan.

Deze mededeling vindt plaats in overeenstemming met de wet van 11 december 1998.

§ 2. Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 22, § 1, derde lid, het volgende:

1. de identificatie van de federale overheidsinstantie of federaal openbaar orgaan die de persoonsgegevens doorgeeft;

2. de identificatie van de verwerkingsverantwoordelijke;

3. de contactgegevens van de functionarissen voor gegevensbescherming;

4. de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5. de wettelijke grondslag;

6. de modaliteiten inzake gehanteerde communicatie;

7. de beperkingen met betrekking tot de rechten van de betrokkene;

8. de periodiciteit van de doorgifte;

9. de duur van het protocol.

§ 4. Le cas échéant, les modalités de fonctionnement, de désignation ainsi que les compétences requises peuvent être définies par le Roi.

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données à caractère personnel avec le secteur public et le secteur privé

Art. 127

§ 1er. Par dérogation aux articles 22, 26, 28, 60 et 61 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme préalable à la communication de données à caractère personnel entre l'autorité, l'organe de recours ou la personne visé à l'article 109 et tout organisme public ou privé.

Cette communication se déroule conformément à la loi du 11 décembre 1998.

§ 2. Par dérogation à l'article 22, § 1er, alinéa 3, de la présente loi, lorsque les parties décident de conclure un protocole, celui-ci porte notamment sur:

1. l'identification du service public fédéral ou de l'organisme public fédéral qui échange les données à caractère personnel;

2. l'identification des responsables du traitement;

3. les coordonnées des délégués à la protection des données concernés;

4. les finalités pour lesquelles les données à caractère personnel sont transférées;

5. la base légale;

6. les modalités de communication utilisées;

7. les restrictions aux droits de la personne concernée;

8. la périodicité du transfert;

9. la durée du protocole.

Afdeling 2

Doorgifte van persoonsgegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 128

Persoonsgegevens mogen slechts worden doorgegeven aan een land dat geen lid is van de Europese Unie of een internationale organisatie, indien dat land of die organisatie een passend beschermingsniveau en de naleving van de andere bepalingen van deze ondertitel waarborgt.

De vraag of het beschermingsniveau passend is, wordt beoordeeld met inachtneming van alle omstandigheden die betrekking hebben op de doorgifte van persoonsgegevens of op een categorie persoonsgegevensdoorgiften; in het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen of organisaties worden nageleefd.

Het passende beschermingsniveau kan verzekerd worden door veiligheidsclausules tussen de verwerkingsverantwoordelijke en de ontvanger van de persoonsgegevens.

Art. 129

In afwijking van artikel 128 mag een doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie, dewelke geen waarborgen biedt voor een passend beschermingsniveau, slechts plaatsvinden wanneer:

1. de betrokkene heeft zijn ondubbelzinnige toestemming gegeven voor de beoogde doorgifte; of

2. de doorgifte is verplicht in het kader van de internationale betrekkingen; of

3. de doorgifte is noodzakelijk ter vrijwaring van het vitaal belang van de personen; of

4. de doorgifte is noodzakelijk of wettelijk verplicht vanwege een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 130

§ 1. In afwijking van het bepaalde in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, is het

Section 2

Transfert des données à caractère personnel vers des pays non membres de l'Union européenne ou à des organisations internationales

Art. 128

Le transfert de données à caractère personnel vers un pays non membres de l'Union européenne ou vers une organisation internationale ne peut avoir lieu que si le pays ou l'organisation en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions du présent sous-titre.

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données à caractère personnel ou à une catégorie de transferts de données à caractère personnel; il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays ou l'organisation en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

Le niveau de protection adéquat peut être assuré par des clauses de sécurité entre le responsable du traitement et le destinataire des données à caractère personnel.

Art. 129

Par dérogation à l'article 128, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale n'assurant pas un niveau de protection adéquat, peut être effectué lorsque:

1. la personne concernée a indubitablement donné son consentement au transfert envisagé ou

2. le transfert est obligatoire dans le cadre de des relations internationales; ou

3. le transfert est nécessaire à la sauvegarde de l'intérêt vital des personnes; ou

4. le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

CHAPITRE X

Autorité de contrôle

Art. 130

§ 1er. Par dérogation à la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, le Comité

Vast Comité I, in zijn hoedanigheid van onafhankelijke publieke autoriteit, aangeduid als toezichthoudende autoriteit belast met de controle van de verwerking van persoonsgegevens uitgevoerd door de overheden en personen bedoeld in artikel 109, eerste lid.

Hij waakt over de toepassing van deze ondertitel ter bescherming van de fundamentele rechten en vrijheden van de natuurlijke personen met betrekking tot deze verwerking.

§ 2. In zijn hoedanigheid van rechterlijke instantie is het beroepsorgaan niet onderworpen aan de controle door een toezichthoudende autoriteit voor de bescherming van persoonsgegevens.

Art. 131

Het Vast Comité I werkt, inzake de wet van 11 december 1998, indien nodig, samen met de andere Belgische toezichthoudende autoriteiten, zonder dat dit afbreuk doet aan de belangen bedoeld in artikel 5 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan.

In het kader van de uitoefening van het toezicht bedoeld in artikel 130, deelt het Vast Comité I in algemene termen het resultaat hiervan mee aan de andere bevoegde toezichthoudende autoriteiten.

Art. 132

De overheden en personen bedoeld in artikel 109, eerste lid werken samen met het Vast Comité I.

Art. 133

Een toezichthoudende autoriteit informeert het Vast Comité I over inbreuken op de reglementering inzake de verwerking van persoonsgegevens in het kader van artikel 109 zodra zij er kennis van neemt.

Elke toezichthoudende autoriteit overlegt met het Vast Comité I wanneer zij gevat wordt in een dossier dat mogelijk gevolgen heeft voor de verwerking van persoonsgegevens in het kader van artikel 109.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden

Art. 134

In afwijking van titel 4, is de raadpleging voor historische, wetenschappelijke of statistische doeleinden van persoonsgegevens van overheden, het beroepsorgaan of personen bedoeld in artikel 109 en hun personeel door een verdere verwerkingsverantwoordelijke toegestaan indien dit geen

permanent R, en sa qualité d'autorité publique indépendante, est désigné comme autorité de protection des données chargée du contrôle du traitement des données à caractère personnel effectué par les autorités et personnes visées à l'article 109, alinéa premier.

Il surveille l'application du présent sous-titre afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard dudit traitement.

§ 2. En sa qualité d'autorité juridictionnelle, l'organe de recours n'est pas soumis au contrôle d'une autorité de protection des données à caractère personnel.

Art. 131

Dans le respect de la loi du 11 décembre 1998 le Comité permanent R coopère, le cas échéant, avec les autres autorités de contrôle belges, sans que cela ne porte atteinte aux intérêts visés à l'article 5 de la loi du 11 décembre 1998 portant création d'un organe de recours.

Dans le cadre de l'exercice du contrôle visé à l'article 130, le Comité permanent R communique le résultat de celui-ci en termes généraux aux autres autorités de contrôle compétentes.

Art. 132

Les autorités et personnes visés à l'article 109, alinéa premier, coopèrent avec le Comité permanent R.

Art. 133

Lorsqu'elle en prend connaissance, une autorité de contrôle informe le Comité permanent R des violations de la règlementation relative aux traitements de données à caractère personnel dans le cadre de l'article 109.

Toute autorité de contrôle saisie d'un dossier susceptible d'avoir une répercussion sur le traitement de données à caractère personnel dans le cadre de l'article 109 se concerte avec le Comité Permanent R.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 134

Par dérogation au titre 4, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel des autorités, organe de recours ou personnes visés à l'article 109 et de leur personnel par un responsable du traitement ultérieur est autorisée si cela ne porte pas atteinte

afbreuk doet aan de belangen bedoeld in artikel 12, eerste lid, van de wet van 11 december 1998.

Art. 135

Vóór de raadpleging bedoeld in artikel 134 moeten de persoonsgegevens voorzien worden van de vermelding "Bescherming van persoonsgegevens – artikelen 134 tot 139 van de wet van xx/xx/2018".

Art. 136

De persoonsgegevens bedoeld in artikel 134 worden voorafgaand aan hun raadpleging geanonimiseerd.

Indien een verdere verwerking van anonieme gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan de verwerkingsverantwoordelijke in het kader van artikel 109 de raadpleging van gepseudonimiseerde gegevens toestaan

Indien de anonimisering of pseudonimisering de identificatie van de gegevens niet onmogelijk maakt, weigert de verwerkingsverantwoordelijke in het kader van artikel 109 de raadpleging indien dit een onevenredige afbreuk doet aan het privéleven.

Indien een verdere verwerking van gepseudonimiseerde gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan de verwerkingsverantwoordelijke in het kader van artikel 109 de raadpleging van niet-gepseudonimiseerde gegevens toestaan indien dit geen onevenredige afbreuk doet aan het privéleven.

Art. 137

In afwijking van titel 4, is een mededeling of publicatie van niet-geanonimiseerde of niet-gepseudonimiseerde persoonsgegevens bedoeld in artikel 134, die werden geraadpleegd door de verdere verwerkingsverantwoordelijke, enkel mogelijk met het akkoord van de verwerkingsverantwoordelijke in het kader van artikel 109 en onder de voorwaarden die hij vastlegt.

Art. 138

De verdere verwerkingsverantwoordelijke van persoonsgegevens bedoeld in artikel 134 houdt een logboek van zijn verdere verwerkingsactiviteiten voor historische, wetenschappelijke of statistische doeleinden bij.

Dit logboek is geclassificeerd in de zin van de wet van 11 december 1998 indien de verwerking betrekking heeft op geclassificeerde gegevens.

Dit logboek bevat de volgende informatie:

aux intérêts visés par l'article 12, alinéa premier, de la loi du 11 décembre 1998.

Art. 135

Avant leur consultation visée à l'article 134, les données à caractère personnel doivent être marquées de la mention "Protection des données à caractère personnel – articles 134 à 139 de la loi du xx/xx/2018".

Art. 136

Les données à caractère personnel visées à l'article 134 sont rendues anonymes préalablement à leur consultation.

Si un traitement ultérieur de données anonymes ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, le responsable du traitement, dans le cadre de l'article 109, peut autoriser la consultation de données pseudonymisées.

Si l'anonymisation ou la pseudonymisation ne rend pas l'identification des données impossible, le responsable du traitement, dans le cadre de l'article 109, refuse la consultation si cela constitue une atteinte disproportionnée à la vie privée.

Si un traitement ultérieur de données pseudonymisées ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, le responsable du traitement, dans le cadre de l'article 109, peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 137

Par dérogation au titre 4, une communication ou publication des données à caractère personnel visées à l'article 134 non anonymisées ou non pseudonymisées, consultées par le responsable du traitement ultérieur n'est possible qu'avec l'accord du responsable du traitement dans le cadre de l'article 109 concerné et sous les conditions que celui-ci aura fixées.

Art. 138

Le responsable du traitement ultérieur des données à caractère personnel visées à l'article 134 tient un journal de ses activités de traitement ultérieur à des fins historiques, scientifiques ou statistiques.

Ce journal est classifié au sens de la loi du 11 décembre 1998 si le traitement porte sur des données classifiées.

Ce journal comporte les informations suivantes:

1. de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming van deze laatste;

2. de doeleinden van de verdere verwerking;

3. de eventuele voorwaarden voor de verdere verwerking vastgelegd door de verwerkingsverantwoordelijke in het kader van artikel 109;

4. de eventuele ontvangers toegestaan door de verwerkingsverantwoordelijke in het kader van artikel 109.

Art. 139

Elke overheidsinstantie of elke natuurlijke of rechtspersoon die persoonsgegevens bedoeld in artikel 134 verwerkt om historische, wetenschappelijke of statistische doeleinden is de verantwoordelijke van deze verwerking.

Hij mag geen handelingen verrichten die zijn gericht op de omzetting van anonieme of gepseudonimiseerde gegevens in persoonsgegevens.

ONDERTITEL 4

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR HET COORDINATIEORGAAN VOOR DE DREIGINGSANALYSE

HOOFDSTUK I

Definities

Art. 140

§ 1. De definities bedoeld in de artikelen 31, 1° tot 6°, 9°, 11° tot 14°, en 16° tot 17°, zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder:

1. “het OCAD”: Coördinatieorgaan voor de dreigingsanalyse bedoeld in de wet van 10 juli 2006 betreffende de analyse van de dreiging.

2. “de verwerkingsverantwoordelijke”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

3. “de wet van 18 juli 1991”: de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

1. les coordonnées du responsable du traitement initial, du responsable du traitement ultérieur et du délégué à la protection des données de ce dernier;

2. les finalités du traitement ultérieur;

3. les éventuelles conditions du traitement ultérieur fixées par le responsable du traitement dans le cadre de l’article 109;

4. les éventuels destinataires autorisés par le responsable du traitement dans le cadre de l’article 109.

Art. 139

Toute autorité publique ou toute personne physique ou morale qui traite des données à caractère personnel visées à l’article 134 à des fins historiques, scientifiques ou statistiques est responsable dudit traitement.

Elle n’entreprendra aucune action pour convertir des données anonymes ou pseudonymisées en données à caractère personnel.

SOUS-TITRE 4

DE LA PROTECTION DES PERSONNES PHYSIQUES A L’EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL PAR L’ORGANE DE COORDINATION POUR L’ANALYSE DE LA MENACE

CHAPITRE I[ER]

Définitions

Art. 140

§ 1[er]. Les définitions visées à l’article 31, 1° à 6°, 9°, 11° à 14°, et 16° à 17°, sont applicables au présent sous-titre.

§ 2. Pour l’application du présent sousitre, on entend par:

1. “l’OCAM”: Organe de coordination pour l’analyse de la menace visé dans la loi du 10 juillet 2006 relative à l’analyse de la menace.

2. “le responsable du traitement”: la personne physique ou morale, l’autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement;

3. “la loi du 18 juillet 1991”: la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l’Organe de coordination pour l’analyse de la menace;

4. “de wet van 11 december 1998”: de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

5. “toezichthoudende autoriteit”: de onafhankelijke overheidsinstantie die bij de wet belast is met het toezicht op de toepassing van deze ondertitel, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met verwerking te beschermen;

6. “de wet van 10 juli 2006”: de wet van 10 juli 2006 betreffende de analyse van de dreiging;

7. “het informatiesysteem van het OCAD”: het informatiesysteem bedoeld in artikel 9 van de wet van 10 juli 2006.

HOOFDSTUK II

Toepassingsgebied

Art. 141

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door het OCAD en zijn verwerkers, uitgevoerd in het kader van de opdrachten van deze als bedoeld in de wet van 10 juli 2006, en door of krachtens bijzondere wetten.

Titels 1, 2, 4, 5 en 7 van deze wet zijn niet van toepassing op de verwerkingen bedoeld in het eerste lid. Enkel de artikelen 239 en 240 van titel 6 zijn van toepassing.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 142

Persoonsgegevens mogen slechts verwerkt worden in één van de volgende gevallen:

a) wanneer de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend;

b) wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;

c) wanneer de verwerking nuttig is om een verplichting na te komen waaraan het OCAD is onderworpen door of krachtens een wet;

d) wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verwerkingsverantwoordelijke of aan de overheidsinstantie aan wie de persoonsgegevens worden verstrekt.

4. “la loi du 11 décembre 1998”: la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

5. “autorité de contrôle”: l’autorité publique indépendante chargée par la loi de surveiller l’application du présent sous-titre, afin de protéger les libertés et droits fondamentaux des personnes physiques à l’égard du traitement;

6. “la loi du 10 juillet 2006”: la loi du 10 juillet 2006 relative à l’analyse de la menace;

7. “le système d’informations de l’OCAM”: le système d’informations visé dans l’article 9 de la loi du 10 juillet 2006.

CHAPITRE II

Champ d’application

Art. 141

Le présent sous-titre s’applique à tout traitement de données à caractère personnel par l’OCAM, et ses sous-traitants effectués dans le cadre des missions de celle-ci visée dans la loi du 16 juillet 2006, ainsi que par ou en vertu de lois particulières.

Les titres 1, 2, 4, 5, et 7 de la présente loi ne s’appliquent pas aux traitements visés à l’alinéa premier. Dans le titre 6, seuls les articles 239 et 240 sont d’application.

CHAPITRE III

Conditions générales du traitement

Art. 142

Le traitement de données à caractère personnel ne peut être effectué que dans l’un des cas suivants:

a) lorsque la personne concernée a indubitablement donné son consentement;

b) lorsqu’il est nécessaire à l’exécution d’un contrat auquel la personne concernée est partie ou à l’exécution de mesures précontractuelles prises à la demande de celle-ci;

c) lorsqu’il est utile au respect d’une obligation à laquelle l’OCAM est soumis par ou en vertu d’une loi;

d) lorsqu’il est nécessaire à l’exécution d’une mission d’intérêt public ou relevant de l’exercice de l’autorité publique, dont est investi le responsable du traitement ou une autorité publique à laquelle les données à caractère personnel sont communiquées.

Art. 143

Persoonsgegevens dienen:

1. eerlijk en rechtmatig te worden verwerkt;

2. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden. Onder de voorwaarden vastgesteld door de artikelen 164 tot en met 169 wordt verdere verwerking van de gegevens voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd;

3. toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4. nauwkeurig te zijn en, zo nodig, te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren.

HOOFDSTUK IV

Aard van de persoonsgegevens

Art. 144

Het OCAD verwerkt, voor zover noodzakelijk voor het belang van de uitoefening van zijn opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of de seksuele geaardheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 145

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de modaliteiten bepaald in artikel 9 van de wet van 10 juli 2006 voor wat het informatiesysteem van het OCAD betreft en artikel 44/11/3*bis* van de wet van 5 augustus 1992 op het politieambt voor wat betreft de gemeenschappelijke gegevensbanken waarvan het OCAD de operationele beheerder is.

Art. 143

Les données à caractère personnel doivent être:

1. traitées loyalement et licitement;

2. collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et réglementaires applicables. Un traitement ultérieur à des fins historiques, scientifiques ou statistiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par les articles 164 à 169;

3. adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4. exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

CHAPITRE IV

Nature des données à caractère personnel

Art. 144

Dans la mesure nécessaire à l'intérêt de l'exercice de ses missions, l'OCAM traite des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

CHAPITRE V

Conservation des données à caractère personnel

Art. 145

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées dans l'article 9 de la loi du 16 juillet 2006 en ce qui concerne le système d'informations de l'OCAM et l'article 44/11/3*bis* de la loi de 5 août 1992 sur la fonction de police en ce qui concerne les banques de données communes dont l'OCAM est le gestionnaire opérationnel.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 146

Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.

Art. 147

De betrokkene heeft het recht te vragen:

1. om toegang tot zijn persoonsgegevens verwerkt overeenkomstig artikel 148;

2. om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen overeenkomstig artikel 149;

3. om de verificatie bij de bevoegde toezichthoudende autoriteit van de naleving van de bepalingen van deze ondertitel overeenkomstig artikel 149.

Art. 148

Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van de opdrachten van het OCAD te waarborgen, is de toegang van de betrokkene tot zijn persoonsgegevens beperkt als het waarschijnlijk niet schadelijk tot is artikel 6 van de wet van 11 april 1994 betreffende de openbaarheid van bestuur.

Art. 149

Voor de uitoefening van zijn rechten, bedoeld in artikel 147, 2° en 3°, richt de betrokkene, die zijn identiteit bewijst, zich kosteloos tot de bevoegde toezichthoudende autoriteit.

Deze voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht.

De nadere regels voor de uitoefening van dit beroep zijn bepaald in de wet.

Art. 150

Een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn, mag niet louter worden genomen op grond van een geautomatiseerde persoonsgegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.

Het in het eerste lid vastgestelde verbod geldt niet indien het besluit zijn grondslag vindt in een bepaling voorgeschreven

CHAPITRE VI

Droits de la personne concernée

Art. 146

Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 147

La personne concernée a le droit de demander:

1. l'accès à ses données à caractère personnel conformément à l'article 148;

2. la rectification ou la suppression de ses données à caractère personnel inexactes conformément à l'article 149;

3. la vérification auprès de l'autorité de contrôle compétente du respect des dispositions du présent sous-titre conformément à l'article 149.

Art. 148

Afin de garantir la confidentialité et l'efficacité de l'exécution des missions de l'OCAM, l'accès par la personne concernée à ses données à caractère personnel est autorisé s'il n'est pas susceptible de porter atteinte à l'article 6 de la loi du 11 avril 1994 relative à la publicité de l'administration.

Art. 149

Pour l'exercice de ses droits visés à l'article 147, 2° et 3°, la personne concernée justifiant de son identité s'adresse, sans frais, à l'autorité de contrôle compétente.

Celle-ci effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Les modalités d'exercice de ce recours sont déterminées par la loi.

Art. 150

Une décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

L'interdiction prévue à l'alinéa premier ne s'applique pas lorsque la décision est fondée sur une disposition prévue

door of krachtens een wet of wanneer het noodzakelijk is vanwege een zwaarwegend openbaar belang.

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 151

De verwerkingsverantwoordelijke moet:

1. er nauwlettend over waken dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2. ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot hetgeen wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst;

3. alle personen die onder zijn gezag handelen, kennisgeven van de bepalingen van deze ondertitel en van alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer die bij het verwerken van persoonsgegevens gelden.

Art. 152

Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verwerkingsverantwoordelijke:

1. een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking;

2. toezien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen;

3. de aansprakelijkheid van de verwerker vaststellen in de overeenkomst;

4. met de verwerker overeenkomen dat de verwerker slechts handelt in opdracht van de verwerkingsverantwoordelijke en dat de verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke in toepassing van deze ondertitel is gehouden;

5. in een geschrift of op een elektronische drager de elementen van de overeenkomst met betrekking tot de bescherming van de persoonsgegevens en de eisen met betrekking tot de maatregelen bedoeld in 3° en 4°, vaststellen.

par ou en vertu d'une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important.

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 151

Le responsable du traitement doit:

1. faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2. veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins du service;

3. informer les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 152

Lorsque le traitement est confié à un sous-traitant, le responsable du traitement doit:

1. choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements;

2. veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles;

3. fixer dans le contrat la responsabilité du sous-traitant;

4. convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et qu'il est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du présent sous-titre;

5. consigner par écrit ou sur un support électronique les éléments du contrat relatifs à la protection des données à caractère personnel et les exigences relatives aux mesures visées aux 3° et 4°.

Art. 153

De verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke is gehouden.

Hij mag de verwerking van persoonsgegevens, die hij verwerkt, niet toevertrouwen aan een andere verwerker, behoudens uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Art. 154

Eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verwerkingsverantwoordelijke verwerken, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 155

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken.

Een onderlinge regeling bepaalt de respectievelijke verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken, met name met betrekking tot de uitoefening van de rechten van de betrokkene en de mededeling van persoonsgegevens, tenzij hun respectievelijke verantwoordelijkheden zijn vastgesteld door of krachtens een wet.

In de onderlinge regeling kan één contactpunt voor betrokkenen worden aangewezen.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 156

Om de veiligheid van de persoonsgegevens te waarborgen, treffen de verwerkingsverantwoordelijke, alsmede de verwerker, de passende technische en organisatorische maatregelen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen verzekeren een passend beveiligingsniveau, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen persoonsgegevens en de potentiële risico's.

Art. 153

Le sous-traitant est soumis aux mêmes obligations que celles qui incombent au responsable du traitement.

Il ne peut pas confier le traitement de données à caractère personnel qu'il sous-traite à un autre sous-traitant, sauf autorisation expresse du responsable du traitement.

Art. 154

Toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 155

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Un accord définit les obligations respectives des responsables conjoints de traitement, notamment en ce qui concerne l'exercice des droits de la personne concernée et la communication des données à caractère personnel, sauf si leurs obligations respectives sont définies par ou en vertu d'une loi.

Un seul point de contact pour les personnes concernées peut être désigné dans l'accord.

Section 3

Sécurité des données à caractère personnel

Art. 156

Le responsable du traitement ainsi que le sous-traitant prennent les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures assurent un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels.

Art. 157

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk zo snel mogelijk aan de bevoegde toezichthoudende autoriteit.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke zo snel mogelijk van elke inbreuk op de beveiliging.

§ 3. In de in paragrafen 1 en 2 bedoelde melding wordt het volgende omschreven of meegedeeld:

a) de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en persoonsgegevensbestanden in kwestie;

b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

c) de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

d) de maatregelen die de verwerkingsverantwoordelijke, of de verwerker heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder in voorkomend geval maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Afdeling 4

Registers

Art. 158

§ 1. De verwerkingsverantwoordelijke houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van de gegevensbanken van het OCAD en deze die aan hem ter beschikking worden gesteld.

Dit register bevat de volgende gegevens:

1° Voor de gegevensbanken van het OCAD:

a) de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden;

c) de categorieën van voornaamste ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

d) indien mogelijk, de beoogde termijnen voor het verwijderen van de persoonsgegevens;

Art. 157

§ 1er. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie à l'autorité de contrôle compétente dans les meilleurs délais.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais.

§ 3. La notification visée aux paragraphes 1 et 2 doit, à tout le moins:

a) décrire la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la brèche de sécurité;

d) décrire les mesures prises ou que le responsable du traitement ou le sous-traitant propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Section 4

Registres

Art. 158

§ 1er. Le responsable du traitement tient un registre, classifié au sens de la loi du 11 décembre 1998, des banques de données de l'OCAM et de celles mises à sa disposition.

Ce registre comporte les informations suivantes:

1° pour les banques de données de l'OCAM:

a) les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) les catégories de destinataires auxquels des données à caractère personnel peuvent être communiquées;

d) dans la mesure du possible, les délais prévus pour l'effacement des données à caractère personnel;

e) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 156.

2° Voor gegevensbanken die aan het OCAD ter beschikking gesteld worden:

a) indien mogelijk, de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de gezamenlijke verwerkingsverantwoordelijken en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden van het OCAD.

§ 2. Elke verwerker houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.

Dit register bevat de volgende elementen:

a) de contactgegevens van de verwerker en van de verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, in voorkomend geval, van de functionaris voor gegevensbescherming;

b) de categorieën van verwerkingen die voor rekening van de verwerkingsverantwoordelijke zijn uitgevoerd;

c) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 156.

§ 3. De in de paragrafen 1 en 2 bedoelde registers zijn in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 4. De verwerkingsverantwoordelijke stelt het register ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

De verwerker stelt het register ter beschikking van de verwerkingsverantwoordelijke en stelt het eveneens ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 159

§ 1. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker, wijzen een functionaris voor gegevensbescherming aan. Deze beslissing wordt meegedeeld aan de bevoegde toezichthoudende autoriteit.

De functionaris voor gegevensbescherming is titularis van een veiligheidsmachtiging “zeer geheim”, in de zin van de wet van 11 december 1998.

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l’article 156.

2° pour les banques de données mises à la disposition de l’OCAM:

a) si possible, les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement par l’OCAM.

§ 2. Chaque sous-traitant tient un registre, classifié au sens de la loi du 11 décembre 1998, de toutes les catégories d’activités de traitement effectuées pour le compte d’un responsable du traitement.

Ce registre comprend les éléments suivants:

a) les coordonnées du sous-traitant et du responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les coordonnées du délégué à la protection des données;

b) les catégories de traitements effectués pour le compte du responsable du traitement;

c) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l’article 156.

§ 3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

§ 4. Le responsable du traitement met le registre à la disposition de l’autorité de contrôle compétente à sa demande.

Le sous-traitant met le registre à la disposition du responsable du traitement ainsi qu’à la disposition de l’autorité de contrôle compétente à sa demande.

Section 5

Délégué à la protection des données

Art. 159

§ 1er. Le responsable du traitement et, le cas échéant, le sous-traitant désignent un délégué à la protection des données. Cette décision est communiquée à l’autorité de contrôle compétente.

Le délégué à la protection des données est titulaire d’une habilitation de sécurité de niveau très secret, au sens de la loi du 11 décembre 1998.

De functionaris voor gegevensbescherming kan niet van zijn functie ontheven of gestraft worden omwille van de uitvoering van zijn opdrachten.

Hij is, op een onafhankelijke wijze, belast met de volgende taken:

— toezien op de naleving van deze ondertitel voor elke verwerking van persoonsgegevens;

— adviseren over alle nuttige maatregelen teneinde de veiligheid van de opgeslagen gegevens te verzekeren;

— de verwerkingsverantwoordelijke, en in voorkomend geval de verwerker, het diensthoofd en de personeelsleden van de betrokken dienst die de verwerking verrichten informeren en adviseren over hun verplichtingen op grond van deze ondertitel;

— adviezen of aanbevelingen verstrekken aan de verwerkingsverantwoordelijke, en in voorkomend geval aan de verwerker of het diensthoofd;

— het uitvoeren van de andere opdrachten die hem door de verwerkingsverantwoordelijke, en in voorkomend geval de verwerker of het diensthoofd toevertrouwd zijn.

De functionaris voor gegevensbescherming is de contactpersoon voor de bevoegde toezichthoudende autoriteit met betrekking tot de toepassing van deze ondertitel.

§ 2. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker ziet erop toe dat hun functionaris voor gegevensbescherming tijdig en naar behoren wordt betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden.

§ 3. De verwerkingsverantwoordelijke, en in voorkomend geval de verwerker ziet erop toe dat de functionaris voor gegevensbescherming de benodigde middelen ter beschikking heeft voor het vervullen van zijn taken.

De functionaris voor gegevensbescherming kan worden bijgestaan door één of meerdere medewerkers.

§ 4. In voorkomend geval worden nadere regels voor de werking, de aanwijzing en de vereiste bevoegdheden door de Koning bepaald.

Le délégué à la protection des données ne peut pas être relevé de ses fonctions ou sanctionné en raison de l'exercice de ses missions.

Il est chargé de manière indépendante:

— de veiller au respect du présent sous-titre lors de tout traitement de données à caractère personnel;

— de conseiller toutes mesures utiles afin d'assurer la sécurité des données enregistrées;

— d'informer et conseiller le responsable du traitement, et le cas échéant le sous-traitant, le dirigeant et le personnel du service concerné procédant au traitement sur les obligations qui leur incombent en vertu du présent sous-titre;

— de fournir des avis ou des recommandations au responsable du traitement, et le cas échéant au sous-traitant, et au dirigeant du service;

— d'exécuter d'autres missions qui lui sont confiées par le responsable du traitement, le cas échéant le sous-traitant ou le dirigeant du service.

Le délégué à la protection des données est le point de contact avec l'autorité de contrôle compétente pour l'application du présent sous-titre.

§ 2. Le responsable du traitement et, le cas échéant le sous-traitant, veille à ce que son délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

§ 3. Le responsable du traitement et, le cas échéant le sous-traitant veille à ce que son délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

§ 4. Le cas échéant, les modalités de fonctionnement, de désignation ainsi que les compétences requises peuvent être définies par le Roi.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van persoonsgegevens aan de publieke sector en de private sector

Art. 160

In afwijking van de artikelen 22, 26, 28, 60 en 61 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen het OCADen enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten van het OCAD.

Deze mededeling vindt plaats in overeenstemming met de artikelen 8, 9, 10, 11 en 12 van de wet van 10 juli 2006 en onderafdeling 7*bis* van de wet van 5 augustus 1992 op het politieambt.

Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 21, § 1, derde lid, het volgende:

1. de identificatie van het OCAD en het openbaar of particulier orgaan die de persoonsgegevens uitwisselen;

2. de identificatie van de verwerkingsverantwoordelijken;

3. de contactgegevens van de functionarissen voor gegevensbescherming;

4. de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5. de wettelijke grondslag;

6. de beperkingen met betrekking tot de rechten van de betrokkene.

Afdeling 2

Doorgifte van persoonsgegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 161

Persoonsgegevens mogen slechts worden doorgegeven aan een land dat geen lid is van de Europese Unie of een internationale organisatie, indien dat land of die organisatie

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données à caractère personnel avec le secteur public et le secteur privé

Art. 160

Par dérogation aux articles 22, 26, 28, 60 et 61 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme préalable à la communication de données à caractère personnel entre l'OCAM et tout organisme public ou privé dans l'intérêt de l'exercice des missions de l'OCAM.

Cette communication se déroule conformément aux articles 8, 9, 10, 11 et 12 de la loi du 10 juillet 2006 et à la sous-section 7*bis* de la loi du 5 août 1992 sur la fonction de la police.

Par dérogation à l'article 21, § 1er, alinéa 3, lorsque les parties décident de conclure un protocole, celui-ci porte notamment sur:

1. l'identification de l'OCAM et de l'organisme public ou privé qui échangent les données à caractère personnel;

2. l'identification des responsables du traitement;

3. les coordonnées des délégués à la protection des données concernés;

4. les finalités pour lesquelles les données à caractère personnel sont transférées;

5. la base légale;

6. les restrictions aux droits de la personne concernée.

Section 2

Transfert des données à caractère personnel vers des pays non membres de l'Union européenne ou à des organisations internationales

Art. 161

Le transfert de données à caractère personnel vers un pays non membres de l'Union européenne ou vers une organisation internationale ne peut avoir lieu que si le pays

een passend beschermingsniveau en de naleving van de andere bepalingen van deze ondertitel waarborgt.

De vraag of het beschermingsniveau passend is, wordt beoordeeld met inachtneming van alle omstandigheden die betrekking hebben op de doorgifte van persoonsgegevens of op een categorie van doorgiften van persoonsgegevens; in het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen of organisaties worden nageleefd.

Het passende beschermingsniveau kan verzekerd worden door veiligheidsclausules tussen de verwerkingsverantwoordelijke en de ontvanger van de persoonsgegevens.

Art. 162

In afwijking van artikel 161 mag een doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie, hetwelke geen waarborgen biedt voor een passend beschermingsniveau, slechts plaatsvinden wanneer:

1. de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven; of

2. de doorgifte verplicht is in het kader van de internationale betrekkingen; of

3. de doorgifte noodzakelijk is ter vrijwaring van het vitaal belang van de personen; of

4. de doorgifte noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend openbaar belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 163

Overeenkomstig artikel 10 van de wet van 10 juli 2006 worden het Vast Comité van Toezicht op de inlichtingendiensten, in zijn hoedanigheid van onafhankelijke publieke autoriteit, en het Vast Comité van Toezicht op de politiediensten, aangeduid als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens door het OCAD en zijn verwerkers volgens de nadere regels vastgelegd in de wet van 18 juli 1991.

ou l'organisation en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions du présent sous-titre.

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données à caractère personnel ou à une catégorie de transferts de données à caractère personnel; il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays ou l'organisation en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

Le niveau de protection adéquat peut être assuré par des clauses de sécurité entre le responsable du traitement et le destinataire des données à caractère personnel.

Art. 162

Par dérogation à l'article 161, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale n'assurant pas un niveau de protection adéquat, peut être effectué lorsque:

1. la personne concernée a indubitablement donné son consentement au transfert envisagé; ou

2. le transfert est obligatoire dans le cadre de des relations internationales; ou

3. le transfert est nécessaire à la sauvegarde de l'intérêt vital des personnes; ou

4. le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

CHAPITRE X

Autorité de contrôle

Art. 163

Conformément à l'article 10 de la loi du 10 juillet 2006, le Comité permanent R, en sa qualité d'autorité publique indépendante, et le Comité permanent de Contrôle des Services de police, sont désignés comme autorités de protection des données chargée du contrôle du traitement des données à caractère personnel par l'OCAM et par ses sous-traitants selon les modalités fixées par la loi du 18 juillet 1991.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden

Art. 164

In afwijking van titel 4, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens van het OCAD en van hun personeel toegestaan door het OCAD indien dit geen afbreuk doet aan zijn opdrachten bedoeld in de wet van 10 juli 2006, aan een lopend opsporings- of gerechtelijk onderzoek, of aan de betrekkingen die België met vreemde staten of internationale organisaties onderhoudt en overeenkomstig de wet van 10 juli 2006.

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens van het OCAD en van hun personeel voor overige doelen dan die bedoeld in het eerste lid wordt geweigerd, behalve met uitdrukkelijke toestemming van het OCAD die de voorwaarden van deze verwerking bepaalt.

Art. 165

Vóór hun raadpleging bedoeld in artikel 164 moeten de persoonsgegevens voorzien worden van de vermelding “Bescherming van persoonsgegevens – hoofdstuk XX van titel XX van de wet van xx/xx/2018”.

Art. 166

De persoonsgegevens bedoeld in artikel 164 worden voorafgaand aan hun raadpleging geanonimiseerd.

Indien een verdere verwerking van anonieme gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan het OCAD de raadpleging van gepseudonimiseerde gegevens toestaan.

Indien de anonimisering of pseudonimisering de identificatie van de gegevens niet onmogelijk maakt, weigert het OCAD de raadpleging indien dit een onevenredige afbreuk doet aan het privéleven.

Indien een verdere verwerking van gepseudonimiseerde gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan het OCADde raadpleging van niet-gepseudonimiseerde gegevens toestaan indien dit geen onevenredige afbreuk doet aan het privéleven.

Art. 167

In afwijking van titel 4, is een mededeling of publicatie van niet-geanonimiseerde of niet-gepseudonimiseerde persoonsgegevens bedoeld in artikel 164, geraadpleegd door de verdere verwerkingsverantwoordelijke, enkel mogelijk met het akkoord van het OCAD en onder de voorwaarden die het vastlegt.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 164

Par dérogation au titre 4, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel de l’OCAM et de leur personnel par un responsable du traitement ultérieur est autorisée par l’OCAM si cela ne porte pas atteinte à ses missions visés dans la loi du 10 juillet 2006, à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales et conformément à la loi du 10 juillet 2006.

Toute demande adressée aux Archives de l’État de traitement ultérieur de données à carcatère personnel de l’OCAM et de son personnel à d’autres fins que celles visées à l’alinéa premier est refusée, sauf autorisation expresse de l’OCAM qui fixe les conditions dudit traitement.

Art. 165

Avant leur consultation visée à l’article 164, les données à caractère personnel doivent être marquées de la mention “Protection des données à caractère personnel – chapitre XX du titre XX de la loi du xx/xx/2018”.

Art. 166

Les données à caractère personnel visées à l’article 164 sont rendues anonymes préalablement à leur consultation.

Si un traitement ultérieur de données anonymes ne permet pas d’atteindre les fins historiques, scientifiques ou statistiques, l’OCAM peut autoriser la consultation de données pseudonymisées.

Si l’anonymisation ou la pseudonymisation ne rend pas l’identification des données impossible, l’OCAM refuse la consultation si cela constitue une atteinte disproportionnée à la vie privée.

Si un traitement ultérieur de données pseudonymisées ne permet pas d’atteindre les fins historiques, scientifiques ou statistiques, l’OCAM peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 167

Par dérogation au titre 4, une communication ou publication des données à caractère personnel visées à l’article 164 non anonymisées ou non pseudonymisées, consultées par le responsable du traitement ultérieur n’est possible qu’avec l’accord de l’OCAM et sous les conditions que celui-ci aura fixées.

Art. 168

De verdere verwerkingsverantwoordelijke van persoonsgegevens bedoeld in artikel 164 houdt een logboek van zijn verdere verwerkingsactiviteiten voor historische, wetenschappelijke of statistische doeleinden bij.

Dit logboek is geclassificeerd in de zin van de wet van 11 december 1998 indien de verwerking betrekking heeft op geclassificeerde gegevens.

Dit logboek bevat de volgende informatie:

1. de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming van deze laatste;

2. de doeleinden van de verdere verwerking;

3. de gegevens die het voorwerp uitmaken van de verdere verwerking;

4. de eventuele voorwaarden voor de verdere verwerking vastgelegd door het OCAD;

5. de eventuele ontvangers toegestaan door het OCAD.

Art. 169

Elke overheidsinstantie of elke natuurlijke of rechtspersoon die persoonsgegevens bedoeld in artikel 164 verwerkt om historische, wetenschappelijke of statistische doeleinden is de verantwoordelijke van deze verwerking.

Hij mag geen handelingen verrichten die zijn gericht op de omzetting van anonieme of gepseudonimiseerde gegevens in persoonsgegevens.

ONDERTITEL 5

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT BEPAALDE VERWERKINGEN VAN PERSOONSGEGEVENS DOOR DE PASSAGIERSINFORMATIE-EENHEID

HOOFDSTUK I

Definities

Art. 170

§ 1. De definities bedoeld in artikelen 31, 1° tot 3°, 8° en 11°, en in artikel 74, 6°, zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder:

1. “de wet van 25 december 2016”: de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens;

Art. 168

Le responsable du traitement ultérieur des données à caractère personnel visées à l’article 164 tient un journal de ses activités de traitement ultérieur à des fins historiques, scientifiques ou statistiques.

Ce journal est classifié au sens de la loi du 11 décembre 1998 si le traitement porte sur des données classifiées.

Ce journal comporte les informations suivantes:

1. les coordonnées du responsable du traitement initial, du responsable du traitement ultérieur et du délégué à la protection des données de ce dernier;

2. les finalités du traitement ultérieur;

3. les données faisant l’objet du traitement ultérieur;

4. les éventuelles conditions du traitement ultérieur fixées par l’OCAM;

5. les éventuels destinataires autorisés par l’OCAM.

Art. 169

Toute autorité publique ou toute personne physique ou morale qui traite des données à caractère personnel visées à l’article 164 à des fins historiques, scientifiques ou statistiques est responsable dudit traitement.

Elle n’entreprendra aucune action pour convertir des données anonymes ou pseudonymisées en données à caractère personnel.

SOUS-TITRE 5

DE LA PROTECTION DES PERSONNES PHYSIQUES A L’EGARD DE CERTAINS TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR L’UNITE D’INFORMATION DES PASSAGERS

CHAPITRE I^ER

Définitions

Art. 170

§ 1^er. Les définitions visées à l’article 31, 1° à 3°, 8° et 11°, et à l’article 74, 6°, sont applicables au présent sous-titre.

§ 2. Pour l’application du présent sous-titre, on entend par:

1. “la loi du 25 décembre 2016”: la loi du 25 décembre 2016 relative au traitement des données des passagers;

2. “de PIE”: de Passagiersinformatie-eenheid bedoeld in hoofdstuk 7 van de wet van 25 december 2016.

HOOFDSTUK II

Toepassingsgebied

Art. 171

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door de PIE in het kader van de finaliteiten bedoeld in artikel 8, § 1, 4°, van de wet van 25 december 2016.

Titels 1, 2, 4, 5 en 7 van deze wet zijn niet van toepassing op de verwerkingen bedoeld in het eerste lid. Enkel de artikelen 239 en 240 van titel 6 zijn van toepassing.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 172

Persoonsgegevens dienen:

1. eerlijk en rechtmatig te worden verwerkt;

2. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden;

3. toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4. nauwkeurig te zijn en, zo nodig, te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren.

HOOFDSTUK IV

Bewaring van persoonsgegevens

Art. 173

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de modaliteiten bepaald in het kader van hoofdstuk 9 van de wet van 25 december 2016.

2. “l’UIP”: l’Unité d’information des passagers visée au chapitre 7 de la loi du 25 décembre 2016.

CHAPITRE II

Champ d’application

Art. 171

Le présent sous-titre s’applique à tout traitement de données à caractère personnel par l’UIP effectué dans le cadre des finalités visées à l’article 8, § 1er, 4°, de la loi du 25 décembre 2016.

Les titres 1, 2, 4, 5 et 7 de la présente loi ne s’appliquent pas aux traitements visés à l’alinéa premier. Dans le titre 6, seuls les articles 239 et 240 sont d’application.

CHAPITRE III

Conditions générales du traitement

Art. 172

Les données à caractère personnel doivent être:

1. traitées loyalement et licitement;

2. collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et réglementaires applicables;

3. adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4. exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

CHAPITRE IV

Conservation des données à caractère personnel

Art. 173

Les données à caractère personnel sont conservées pendant une durée n’excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées dans le cadre du chapitre 9 de la loi du 25 décembre 2016.

HOOFDSTUK V

Rechten van de betrokkene

Art. 174

Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.

Art. 175

De betrokkene heeft het recht te vragen:

1. om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen overeenkomstig artikel 177;

2. om de verificatie bij de bevoegde toezichthoudende autoriteit van de naleving van de bepalingen van deze ondertitel overeenkomstig artikel 177.

Art. 176

Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van de verwerkingen zoals hierboven bedoeld, is de toegang van de betrokkene tot zijn persoonsgegevens beperkt tot de toegang die expliciet voorzien is bij wet.

Art. 177

Voor de uitoefening van zijn rechten, bedoeld in artikel 175, 2° en 3°, richt de betrokkene, die zijn identiteit bewijst, zich kosteloos tot de bevoegde toezichthoudende autoriteit.

Deze voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht.

De nadere regels voor de uitoefening van dit beroep zijn bepaald in de wet.

Art. 178

Een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn, mag niet louter worden genomen op grond van een geautomatiseerde persoonsgegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.

Het in het eerste lid vastgestelde verbod geldt niet indien het besluit zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet of wanneer het noodzakelijk is vanwege een zwaarwegend openbaar belang.

CHAPITRE V

Droits de la personne concernée

Art. 174

Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 175

La personne concernée a le droit de demander:

1. la rectification ou la suppression de ses données à caractère personnel inexactes conformément à l'article 177;

2. la vérification auprès de l'autorité de contrôle compétente du respect des dispositions du présent sous-titre conformément à l'article 177.

Art. 176

Afin de garantir la confidentialité et l'efficacité de l'exécution des traitements visés ci-dessus, l'accès par la personne concernée à ses données à caractère personnel est limité à celui prévu expressément par une loi.

Art. 177

Pour l'exercice de ses droits visés à l'article 175, 2° et 3°, la personne concernée justifiant de son identité s'adresse, sans frais, à l'autorité de contrôle compétente.

Celle-ci effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Les modalités d'exercice de ce recours sont déterminées par la loi.

Art. 178

Une décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

L'interdiction prévue à l'alinéa premier ne s'applique pas lorsque la décision est fondée sur une disposition prévue par ou en vertu d'une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important.

HOOFDSTUK VI

Verplichtingen van de verwerkingsverantwoordelijke

Afdeling 1

Algemene verplichtingen

Art. 179

De verwerkingsverantwoordelijke moet:

1. er nauwlettend over waken dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2. ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot hetgeen wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst;

3. alle personen die onder zijn gezag handelen, kennisgeven van de bepalingen van deze ondertitel en van alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer die bij het verwerken van persoonsgegevens gelden.

Art. 180

Eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verwerkingsverantwoordelijke verwerken, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Beveiliging van persoonsgegevens

Art. 181

Om de veiligheid van de persoonsgegevens te waarborgen, treft de verwerkingsverantwoordelijke de passende technische en organisatorische maatregelen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen verzekeren een passend beveiligingsniveau, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen persoonsgegevens en de potentiële risico's.

CHAPITRE VI

Obligations du responsable du traitement

Section 1re

Obligations générales

Art. 179

Le responsable du traitement doit:

1. faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2. veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins du service;

3. informer les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 180

Toute personne agissant sous l'autorité du responsable du traitement qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi.

Section 2

Sécurité des données à caractère personnel

Art. 181

Le responsable du traitement prend les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures assurent un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels.

Art. 182

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk zo snel mogelijk aan de bevoegde toezichthoudende autoriteit.

§ 2. In de in paragraaf 1 bedoelde melding wordt het volgende omschreven of meegedeeld:

a) de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en persoonsgegevensbestanden in kwestie;

b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

c) de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder in voorkomend geval maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Afdeling 3

Register

Art. 183

§ 1. De verwerkingsverantwoordelijke houdt een register bij van de gegevensbanken van de PIE en deze die aan haar ter beschikking worden gesteld.

Dit register bevat de volgende gegevens:

1° Voor de gegevensbanken van de PIE:

a) de contactgegevens van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden;

c) de categorieën van voornaamste ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

d) indien mogelijk, de beoogde termijnen voor het verwijderen van de persoonsgegevens;

e) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 181.

2° Voor gegevensbanken die aan de PIE ter beschikking gesteld worden:

Art. 182

§ 1er. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie à l'autorité de contrôle compétente dans les meilleurs délais.

§ 2. La notification visée au paragraphe 1er doit, à tout le moins:

a) décrire la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la brèche de sécurité;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Section 3

Registre

Art. 183

§ 1er. Le responsable du traitement tient un registre des banques de données de l'UIP et de celles mises à sa disposition.

Ce registre comporte les informations suivantes:

1° pour les banques de données de l'UIP:

a) les coordonnées du responsable du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) les catégories de destinataires auxquels des données à caractère personnel peuvent être communiquées;

d) dans la mesure du possible, les délais prévus pour l'effacement des données à caractère personnel;

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 181.

2° pour les banques de données mises à la disposition de l'UIP:

a) indien mogelijk, de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de gezamenlijke verwerkingsverantwoordelijken en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden van de PIE.

§ 2. De in de eerste paragraaf bedoelde register is in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 3. De verwerkingsverantwoordelijke stelt het register ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

HOOFDSTUK VII

Mededeling en doorgifte van persoonsgegevens

Art. 184

Persoonsgegevens mogen slechts worden doorgegeven aan een land dat geen lid is van de Europese Unie of een internationale organisatie, indien dat land of die organisatie een passend beschermingsniveau en de naleving van de andere bepalingen van deze ondertitel waarborgt.

De vraag of het beschermingsniveau passend is, wordt beoordeeld met inachtneming van alle omstandigheden die betrekking hebben op de doorgifte van persoonsgegevens of op een categorie van doorgiften van persoonsgegevens; in het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen of organisaties worden nageleefd.

Het passende beschermingsniveau kan verzekerd worden door veiligheidsclausules tussen de verwerkingsverantwoordelijke en de ontvanger van de persoonsgegevens.

Art. 185

In afwijking van artikel 184 mag een doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie, hetwelke geen waarborgen biedt voor een passend beschermingsniveau, slechts plaatsvinden wanneer:

1. de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven; of

2. de doorgifte verplicht is in het kader van de internationale betrekkingen; of

3. de doorgifte noodzakelijk is ter vrijwaring van het vitaal belang van de personen; of

a) si possible, les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement par l'UIP.

§ 2. Le registre visé au paragraphe premier se présente sous une forme écrite y compris la forme électronique.

§ 3. Le responsable du traitement met le registre à la disposition de l'autorité de contrôle compétente à sa demande.

CHAPITRE VII

Communication et transfert de données à caractère personnel

Art. 184

Le transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale ne peut avoir lieu que si le pays ou l'organisation en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions du présent sous-titre.

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données à caractère personnel ou à une catégorie de transferts de données à caractère personnel; il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays ou l'organisation en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

Le niveau de protection adéquat peut être assuré par des clauses de sécurité entre le responsable du traitement et le destinataire des données à caractère personnel.

Art. 185

Par dérogation à l'article 184, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale n'assurant pas un niveau de protection adéquat, peut être effectué lorsque:

1. la personne concernée a indubitablement donné son consentement au transfert envisagé; ou

2. le transfert est obligatoire dans le cadre de des relations internationales; ou

3. le transfert est nécessaire à la sauvegarde de l'intérêt vital des personnes; ou

4. de doorgifte noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend openbaar belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

HOOFDSTUK VIII

Toezichthoudende autoriteit

Art. 186

De verwerkingen van persoonsgegevens zoals bedoeld in deze ondertitel zijn onderworpen aan het toezicht van de toezichthoudende autoriteit bedoeld in artikel 97.

ONDERTITEL 6

BIJZONDERE BEPALINGEN

Art. 187

§ 1. De volgende publieke overheden verwerken, voor zover noodzakelijk voor de uitoefening van hun opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of de seksuele geaardheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen:

1. de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2. het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van haar opdrachten bedoeld in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en in bijzondere wetten;

3. het Vast Comité van Toezicht op de politiediensten in het kader van haar opdrachten bedoeld in artikel 1, 2° en 3°, en hoofdstuk IV van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

4. Het Controleorgaan op de politionele informatie in het kader van haar opdrachten bedoeld in artikel 73 § 1.

§ 2. Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van de opdrachten hierboven bedoeld, te verzekeren, is de toegang van de betrokkene tot zijn persoonsgegevens beperkt tot wat voorzien is in de bijzondere wetten.

4. le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

CHAPITRE VIII

Autorité de contrôle

Art. 186

Les traitements de données à caractère personnel tels que visés dans ce sous-titre sont soumis au contrôle de l'autorité de contrôle visée à l'article 97.

SOUS-TITRE 6

DISPOSITIONS PARTICULIÈRES

Art. 187

§ 1er. Dans la mesure nécessaire à l'exercice de leurs missions, les autorités publiques suivantes traitent des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes:

1. la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité dans le cadre de ses missions visées dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2. le Comité permanent R dans le cadre de ses missions visées dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et dans des lois particulières;

3. le Comité permanent P dans le cadre de ses missions visées dans l'article 1er, 2° et 3°, et le chapitre IV de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

4. L' Organe de contrôle de l'information policière dans le cadre de ses missions visées dans l'article 73 § 1er.

§ 2. Afin de garantir la confidentialité et l'efficacité de l'exécution des missions visées ci-dessus, l'accès par la personne concernée à ses données à caractère personnel est limité à celui qui est prévu dans les lois particulières.

§ 3. De betrokkene heeft het recht te vragen om zijn onjuiste persoonsgegevens, verwerkt door de in de eerste paragraaf vermelde overheden, te laten verbeteren of verwijderen.

§ 4. De verwerkingen van persoonsgegevens door de overheden bedoeld in het eerste lid is niet onderworpen aan het toezicht van de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit.

TITEL 4

Verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden

HOOFDSTUK I

Algemene bepalingen

Art. 188

Voor de toepassing van deze titel wordt verstaan onder:

1° "verwerking met het oog op archivering": verwerking van persoonsgegevens met het oog op archivering in het algemeen belang;

2° "archivering in het algemeen belang": statische archieven, gesorteerd omwille van hun permanente waarde en bewaard voor onbepaalde duur teneinde ze toegankelijk te maken in het algemeen belang;

3° "verwerking met het oog op onderzoek": verwerking van persoonsgegevens met het oog op wetenschappelijk of historisch onderzoek;

4° "verwerking met het oog op statistische doeleinden": verwerking van persoonsgegevens met het oog op statistische doeleinden;

5° "verwerkingsverantwoordelijke": verantwoordelijke voor de verwerking met het oog op archivering of onderzoek of statistische doeleinden;

6° "register van de verwerkingsactiviteiten": het register van verwerkingsactiviteit zoals bepaald in artikel 30 van de Verordening;

7° "functionaris voor gegevensbescherming": de functionaris voor gegevensbescherming zoals bepaald in artikel 37 van de Verordening;

8° "gepseudonimiseerde gegevens": gepseudonimiseerde gegevens in de zin van artikel 4.5 van de Verordening;

9° "derde vertrouwenspersoon": de natuurlijke persoon of rechtspersoon, de feitelijke vereniging of de

§ 3. La personne concernée a le droit de demander la rectification ou la suppression de ses données à caractère personnel inexactes traitées par les autorités visées au paragraphe premier.

§ 4. Le traitement de données à caractère personnel par les autorités visées au premier ne est pas soumis au contrôle de l'Autorité de protection des données visée dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

TITRE 4

Traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

CHAPITRE I^ER

Dispositions générales

Art. 188

Pour l'application du présent titre, on entend par:

1° "traitements à des fins d'archives": traitement de données à caractère personnel à des fins archivistiques dans l'intérêt public;

2° "archives d'intérêt public": archives statiques, triées pour leur valeur permanente et conservée pour une durée illimitée afin d'être rendue publique dans l'intérêt public général;

3° "traitement à des fins de recherche": traitement de données à caractère personnel à des fins de recherche scientifique ou historique;

4° "traitement à des fins statistiques": traitement de données à caractère personnel à des fins statistiques;

5° "responsable du traitement": responsable du traitement à des fins d'archive ou de recherche ou statistiques;

6° "registre des activités de traitement": le registre d'activité de traitement déterminé à l'article 30 du Règlement;

7° "délégué à la protection des données": le délégué à la protection des données déterminé à l'article 37 du Règlement;

8° "données pseudonymisées" : données pseudonymisées au sens de l'article 4.5 du Règlement ;

9° "tiers de confiance": la personne physique ou morale, l'association de fait ou l'administration publique autre que

overheidsadministratie, niet zijnde de verantwoordelijke voor de verwerking met het oog op archivering of onderzoek of statistische doeleinden, die de gegevens pseudonimiseert;

10° “mededeling van gegevens”: mededeling van gegevens aan geïdentificeerde derde;

11°”verspreiding van gegevens”: bekendmaking van de gegevens, zonder identificatie van de derde;

12°”toestemming”: toestemming in de zin van artikel 4, 11°, en van overweging 33 van de Verordening.

Art. 189

Dit hoofdstuk bepaalt de passende waarborgen die vereist zijn op grond van artikel 89 van de Verordening.

Art. 190

Dit hoofdstuk is van toepassing op de verwerking met het oog op archivering of onderzoek of statistische doeleinden, met uitzondering van de verwerkingen verricht door de diensten bedoeld in titel 3 van deze wet.

HOOFDSTUK II

Algemene waarborgen

Art. 191

De verwerkingsverantwoordelijke wijst een functionaris voor gegevensbescherming aan.

Art. 192

§ 1. De verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten bij.

§ 2. In het kader van een verdere verwerking van verdere persoonsgegevens maakt de verwerkingsverantwoordelijke de naam van de verwerkingsverantwoordelijke, de naam en de contactgegevens van de functionaris voor gegevensbescherming en het doel van de verwerking openbaar.

HOOFDSTUK III

Minimale gegevensverwerking

Art. 193

De verantwoordelijke voor de verwerking met het oog op onderzoek of statistische doeleinden gebruikt bij voorkeur anonieme gegevens.

le responsable du traitement à des fins d’archive ou de recherche ou statistique**,** qui pseudonymise les données;

10° “communication des données”**:** communication des données à des tiers identifiés.

11° “diffusion des données”: publication des données, sans identification des tiers;

12° “consentement”: consentement au sens de l’article 4, 11°, et du considérant 33 du Règlement.

Art. 189

Le présent chapitre détermine les garanties appropriées requises par l’article 89 du Règlement.

Art. 190

Le présent chapitre s’applique au traitement à des fins d’archives ou de recherche ou statistiques, à l’exception des traitements effectués par les services visés dans le titre 3 de la présente loi.

CHAPITRE II

Garanties générales

Art. 191

Le responsable du traitement désigne un délégué à la protection des données.

Art. 192

§ 1er. Le responsable du traitement tient un registre des activités de traitement.

§ 2. Lors d’un traitement ultérieur de données à caractère personnel, le responsable du traitement ultérieur rend public le nom du responsable du traitement, le nom et les coordonnées du délégué à la protection des données et la finalité du traitement.

CHAPITRE III

Minimisation des données

Art. 193

Le responsable du traitement à des fins de recherche ou statistiques utilise de préférence des données anonymes.

Indien het niet mogelijk is om met een verwerking van anonieme gegevens het onderzoeksdoel of statistische doel te bereiken, gebruikt hij bij voorkeur gepseudonimiseerde gegevens.

Indien het niet mogelijk is om met een verwerking van gepseudonimiseerde gegevens het onderzoeksdoel of het statistische doel te bereiken, gebruikt hij niet-gepseudonimiseerde gegevens.

Art. 194

Eerder dan de gegevens te verzamelen bij de betrokkene hanteert de verwerkingsverantwoordelijke met het oog op onderzoek of statistische doeleinden bij voorkeur de verdere verwerking.

Wanneer het niet mogelijk is om met een verdere verwerking het onderzoeksdoel of het statistische doel te bereiken, gaat hij over tot een nieuwe verzameling van gegevens bij de betrokkenen.

Art. 195

Voorafgaand aan de verzameling moet de verantwoordelijke voor de verwerking met het oog op onderzoek of statistische doeleinden:

1° het gebruik van de al dan niet gepseudonimiseerde gegevens verantwoorden;

2° de toevlucht tot een nieuwe gegevensverzameling verantwoorden;

3° het advies van de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke vragen.

De verantwoordingen en het advies bedoeld in het eerste lid, en de verantwoording van de verwerkingsverantwoordelijke wanneer hij het advies van de functionaris voor gegevensbescherming niet volgt worden bij het register van de verwerkingsactiviteiten gevoegd.

Art. 196

Voorafgaand aan de verzameling verantwoordt de verantwoordelijke voor de verwerking met het oog op archivering het algemeen belang van de bewaarde archieven.

De verantwoording wordt bij het register van de verwerkingsactiviteiten gevoegd.

Lorsqu'un traitement de données anonymes ne permet pas d'atteindre la finalité de la recherche ou statistiques, il utilise de préférence des données pseudonymisées.

Lorsqu'un traitement de données pseudonymisées ne permet pas d'atteindre la finalité de recherche ou statistique, il utilise des données non-pseudonymisées.

Art. 194

Plutôt que de collecter des données auprès de la personne concernée, le responsable du traitement à des fins de recherche ou statistiques utilise de préférence des traitements ultérieurs.

Lorsqu'un traitement ultérieur ne permet pas d'atteindre la finalité de la recherche ou de statistiques, il procède à une nouvelle collecte de données auprès des personnes concernées.

Art. 195

Préalablement à la collecte, le responsable du traitement à des fins de recherche ou statistiques:

1° justifie l'utilisation des données pseudonymisées ou non;

2° justifie le recours à une nouvelle collecte de données;

3° demande l'avis du délégué à la protection des données du responsable du traitement.

Les justifications et l'avis visés au premier alinéa, ainsi que la justification du responsable du traitement lorsqu'il ne suit pas l'avis du délégué à la protection des données sont annexés au registre des activités de traitement.

Art. 196

Préalablement à la collecte, le responsable du traitement à des fins d'archives justifie l'intérêt public des archives conservées.

La justification est annexée au registre des activités de traitement.

HOOFDSTUK IV

Gegevensverzameling

Afdeling 1

Gegevensverzameling bij de betrokkene

Art. 197

De verwerkingsverantwoordelijke die niet-gevoelige gegevens verzamelt bij de betrokkene stelt hem hiervan op de hoogte.

De verwerkingsverantwoordelijke die gevoelige gegevens verzamelt bij de betrokkene, stelt hem hiervan op de hoogte en verkrijgt zijn toestemming, behalve indien:

1. de gegevens door de betrokkene zelf openbaar zijn gemaakt; of

2. de verzameling door een wet of een openbaar belang verplicht is geworden; of

3. de verzameling wordt verricht in het vitaal belang van de betrokkene.

In dat geval stelt de verwerkingsverantwoordelijke die de gevoelige gegevens verzamelt bij de betrokkene hem daarvan op de hoogte.

Art. 198

Onverminderd artikel 13 van de Verordening stipuleert de kennisgeving de bijkomende volgende elementen:

— het algemene belang van de verzamelde gegevens, voor de verwerkingen met het oog op archivering;

— de anonimisering of eventuele pseudonimisering van de gegevens na verzameling ervan, voor de verwerking met het oog op onderzoek of statistische doeleinden;

— de beperkingen inzake de verspreiding en de mededeling van de gegevens;

— de beperkingen van de rechten van de betrokkene;

— de nadere regels inzake de uitoefening van de rechten van de betrokkene.

Art. 199

De kennisgeving wordt voor advies voorgelegd aan de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke.

CHAPITRE IV

Collecte de données

Section 1re

Collecte de données auprès de la personne concernée

Art. 197

Le responsable du traitement qui collecte des données non-sensibles auprès de la personne concernée, en informe celle-ci.

Le responsable du traitement qui collecte des données sensibles auprès de la personne concernée, en informe celle-ci et recueille son consentement, sauf si:

1. les données collectées ont été rendues publiques par la personne concernée; ou

2. si la collecte est rendue obligatoire par une loi ou l'intérêt public; ou

3. si la collecte est faite dans l'intérêt vital de la personne concernée.

Dans ces cas, le responsable du traitement qui collecte des données sensibles auprès de la personne concernée, en informe celle-ci.

Art. 198

Sans préjudice de l'article 13 du Règlement, l'information stipule les éléments supplémentaires suivants:

— l'intérêt public des données collectées, en ce qui concerne les traitements à des fins d'archives;

— l'anonymisation ou la pseudonymisation éventuelle des données après leur collecte, en ce qui concerne les traitements à des fins de recherche ou statistiques;

— les limitations à la diffusion et à la communication des données;

— les restrictions aux droits de la personne concernée;

— les modalités d'exercice des droits de la personne concernée.

Art. 199

L'information est soumise pour avis au délégué à la protection des données du responsable du traitement.

Art. 200

De kennisgeving betreffende de gegevensverzameling, het advies van de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke en de verantwoording van de verwerkingsverantwoordelijke wanneer hij het advies van de functionaris voor gegevensbescherming niet volgt, worden bij het register van de verwerkingsactiviteiten gevoegd.

Art. 201

§ 1. De artikelen 15 en 16 van de Verordening zijn niet van toepassing op verwerkingen met het oog op archivering, onderzoek of statistische doeleinden wanneer:

a) de verwerkingsverantwoordelijke motiveert dat de uitoefening van die rechten de verwezenlijking van die archiverings-, onderzoeks- of statistische doeleinden onmogelijk dreigt te maken of ernstig te belemmeren. De verantwoording, het advies van de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke en de verantwoording van de verwerkingsverantwoordelijke wanneer hij het advies van de functionaris voor gegevensbescherming niet volgt, worden bij het register van de verwerkingsactiviteiten gevoegd; of

b) de Europese regelgeving, een wet, decreet of ordonnantie:

— de verwerkingsverantwoordelijke een mandaat geeft om gegevens te verwerken met het oog op archivering, onderzoek of statische doeleinden, en

— regels inzake veiligheid en vertrouwelijkheid oplegt aan de personen die werken onder de verantwoordelijkheid of voor rekening van de verwerkingsverantwoordelijke, en

— het hergebruik van de gegevens voor andere doeleinden verbiedt.

§ 2. De artikelen 17, 18 en 21 van de Verordening zijn niet van toepassing op verwerkingen met het oog op onderzoek of statistische doeleinden die vervat zijn in de kennisgeving opgelegd in artikel 14 van de Verordening.

§ 3. De artikelen 17, 18, 20 en 21 van de Verordening zijn niet van toepassing op verwerkingen met het oog op archivering die vervat zijn in de kennisgeving betreffende de gegevensverzameling, opgelegd in artikel 14 van de Verordening.

Afdeling 2

Gegevensverzameling via verdere verwerking van gegevens

Art. 202

De verantwoordelijke voor de verdere verwerking die gegevens verzamelt sluit een overeenkomst met de verantwoordelijke voor de oorspronkelijke verwerking af.

Art. 200

L'information sur la collecte de données, l'avis du délégué à la protection des données du responsable du traitement, et la justification du responsable du traitement lorsqu'il ne suit pas l'avis du délégué à la protection des données sont annexés au registre des activités de traitement.

Art. 201

§ 1er. Les articles 15 et 16 du Règlement ne s'appliquent pas aux traitements à des fins d'archives, de recherche ou statistiques lorsque:

a) le responsable du traitement justifie que l'exercice de ces droits risquent de rendre impossible ou entravent sérieusement la réalisation de ces finalités d'archives, de recherche ou statistiques. La justification, l'avis du délégué à la protection des données du responsable du traitement et la justification du responsable du traitement lorsqu'il ne suit pas l'avis du délégué à la protection des données sont annexés au registre des activités de traitement; ou

b) le droit de l'Union européenne, une loi, un décret ou une ordonnance:

— donne pour mandat au responsable du traitement de traiter des données à des fins d'archives, de recherche ou statistique, et

— impose des règles de sécurité et de confidentialité aux personnes travaillant sous la responsabilité ou pour le compte du responsable du traitement, et

— interdit la réutilisation des données à d'autres fins.

§ 2. Les articles 17, 18 et 21 du Règlement ne s'appliquent pas aux traitements à des fins de recherche ou statistique qui font l'objet de l'information imposée à l'article 14 du Règlement.

§ 3. Les articles 17, 18, 20 et 21 du Règlement ne s'appliquent pas aux traitements à des fins d'archives qui font l'objet de l'information sur la collecte de données imposée à l'article 14 du Règlement.

Section 2

Collecte de données par traitement ultérieur de données

Art. 202

Le responsable du traitement ultérieur qui collecte des données signe une convention avec le responsable du traitement initial.

Art. 203

De verantwoordelijke voor de verdere verwerking die gegevens verzamelt via verdere verwerking is vrijgesteld van de verplichting tot het afsluiten van een overeenkomst met de verantwoordelijke voor de oorspronkelijke verwerking wanneer de oorspronkelijke verwerking een openbare verwerking van gegevens inhoudt.

Art. 204

De verantwoordelijke voor verdere verwerking die gegevens verzamelt via verdere verwerking van gegevens is vrijgesteld van de verplichting tot het afsluiten van een overeenkomst met de verantwoordelijke voor de oorspronkelijke verwerking wanneer de Europese regelgeving, een wet, decreet of ordonnantie:

— mandaat geeft aan de verwerkingsverantwoordelijke om persoonsgegevens te verwerken met het oog op archivering, onderzoek of statistische doeleinden; en

— regels inzake veiligheid en vertrouwelijkheid oplegt aan de verantwoordelijke voor de verdere verwerking en aan de personen die werken onder zijn gezag of voor zijn rekening werken; en

— het hergebruik van de verzamelde gegevens voor andere doeleinden verbiedt.

In dat geval verstrekt de verantwoordelijke voor de verdere verwerking aan de verantwoordelijke de oorspronkelijke verwerking een kennisgeving betreffende de gegevensverzameling.

Art. 205

De overeenkomst bedoeld in artikel 202 of de kennisgeving bedoeld in artikel 204 stipuleert de volgende elementen:

a) in geval van overeenkomst betreft, de contactgegevens van de verantwoordelijke voor de oorspronkelijke verwerking en van de verantwoordelijke voor de verdere verwerking;

b) wat de kennisgeving betreffende de gegevensverzameling betreft, de categorieën van verantwoordelijken voor de oorspronkelijke verwerkingen en de contactgegevens van de verantwoordelijke voor de verdere verwerking;

c) de contactgegevens van de functionaris voor gegevensbescherming van de verantwoordelijke voor de oorspronkelijke verwerking, indien hij er een heeft, en van de verantwoordelijke voor de verdere verwerking;

d) het doel van de oorspronkelijke verwerking;

e) het doel van de verdere verwerking;

f) voor verwerkingen met het oog op archivering: het algemeen belang van de verzamelde gegevens;

Art. 203

Le responsable du traitement ultérieur qui collecte des données par traitement ultérieur est exempté de l'obligation de passer une convention avec le responsable du traitement initial lorsque le traitement initial est un traitement public de données.

Art. 204

Le responsable du traitement ultérieur qui collecte des données par traitement ultérieur de données est exempté de l'obligation de passer une convention avec le responsable du traitement initial lorsque le droit de l'Union européenne, une loi, un décret ou une ordonnance:

— donne pour mandat au responsable du traitement de traiter des données à caractère personnel à des fins d'archive, de recherche ou statistiques; et

— impose des règles de sécurité et de confidentialité au responsable du traitement ultérieur et aux personnes travaillant sous son autorité ou pour son compte; et

— interdit la réutilisation des données collectées à d'autres fins.

Dans ce cas, le responsable du traitement ultérieur fournit au responsable du traitement initial une information sur la collecte de données.

Art. 205

La convention visée à l'article 202 ou l'information visée à l'article 204 stipule les éléments suivants:

a) en cas de convention: les coordonnées du responsable du traitement initial et du responsable du traitement ultérieur;

b) pour l'information sur la collecte des données, les catégories de responsables des traitements initiaux et les coordonnées du responsable du traitement ultérieur;

c) les coordonnées du délégué à la protection des données du responsable du traitement initial, s'il en a un, et de celui du responsable du traitement ultérieur;

d) la finalité du traitement initial;

e) la finalité du traitement ultérieur;

f) pour les traitements à des fins d'archives, l'intérêt public des données collectées;

g) voor verwerkingen met het oog op onderzoek of statistische doeleinden, het nut van de gegevens van de oorspronkelijke verwerking voor de verdere verwerking met het oog op onderzoek of statistische doeleinden;

h) de categorieën van verzamelde gegevens;

i) voor verwerkingen met het oog op onderzoek of statistische doeleinden: de anonimisering of eventuele pseudonimisering van de gegevens na verzameling ervan;

j) voor de verwerking met het oog op onderzoek of statistische doeleinden, de toelichting bij de toevlucht tot al dan niet gepseudonimiseerde gegevens;

k) de nadere regels inzake gegevensverzameling;

l) in geval van overeenkomst, het voorafgaand akkoord van de verantwoordelijke voor de oorspronkelijke verwerking bij de inschakeling van een verwerker door de verantwoordelijke voor de verdere verwerking;

m) in geval van overeenkomst: het voorafgaand akkoord van de verantwoordelijke voor de oorspronkelijke verwerking voor een nieuwe verdere verwerking;

n) de nadere regels inzake het recht op toegang van de betrokkene tot de verdere verwerking, wanneer de gegevens niet gepseudonimiseerd zijn;

o) het feit dat de schending van de bepalingen van de overeenkomst de nietigheid van rechtswege ervan meebrengt.

Art. 206

De overeenkomst of de kennisgeving betreffende de gegevensverzameling wordt voor advies voorgelegd aan de functionaris voor gegevensbescherming van de verantwoordelijke voor de oorspronkelijke verwerking, indien hij er een heeft, en aan die van de verantwoordelijke voor de verdere verwerking.

Art. 207

De overeenkomst of de kennisgeving betreffende de gegevensverzameling, het advies van de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke en de verantwoording van de verantwoordelijke voor de verwerking wanneer hij het advies van de functionaris voor gegevensbescherming niet volgt, worden bij het register van de verwerkingsactiviteiten gevoegd.

Art. 208

De artikelen 14, 15 en 16 van de Verordening zijn niet van toepassing op verdere verwerkingen met het oog op archivering, onderzoek of statistische doeleinden wanneer:

a) de verantwoordelijke voor de verdere verwerking motiveert dat de uitoefening van die rechten de verwezenlijking

g) pour les traitements de recherche ou statistique, l'utilité des données du traitement initial pour le traitement ultérieur à des fins de recherche ou statistique;

h) les catégories de données collectées;

i) pour les traitements à des fins de recherche ou statistique, l'anonymisation ou la pseudonymisation éventuelle des données après leur collecte;

j) pour les traitements à des fins de recherche ou statistique, l'explication du recours à des données pseudonymisées ou non;

k) les modalités de collecte des données;

l) en cas de convention, l'accord préalable du responsable du traitement initial lors du recours à un sous-traitant par le responsable du traitement ultérieur;

m) en cas de convention, l'accord préalable du responsable du traitement initial pour un nouveau traitement ultérieur;

n) les modalités de droit d'accès de la personne concernée au traitement ultérieur, lorsque les données sont non-pseudonymisées;

o) le fait que la violation des dispositions de la convention entraine sa nullité de plein droit.

Art. 206

La convention ou l'information sur la collecte de données est soumise pour avis au délégué à la protection des données du responsable du traitement initial, s'il en a un, et à celui du responsable du traitement ultérieur.

Art. 207

La convention ou l''information sur la collecte de données, l'avis du délégué à la protection des données du responsable du traitement, et la justification du responsable du traitement lorsqu'il ne suit pas l'avis du délégué à la protection des données sont annexés au registre des activités de traitement.

Art. 208

Les articles 14, 15 et 16 du Règlement ne s'appliquent pas aux traitements ultérieur à des fins d'archives, de recherche ou statistiques lorsque:

a) le responsable du traitement ultérieur justifie que l'exercice de ces droits risquent de rendre impossible ou entravent

van die archiverings-, onderzoeks- of statistische doeleinden onmogelijk dreigt te maken of ernstig te belemmeren. De verantwoording, het advies van de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke en de verantwoording van de verwerkingsverantwoordelijke wanneer hij het advies van de functionaris voor gegevensbescherming niet volgt, worden bij het register van de verwerkingsactiviteiten gevoegd; of

b) de Europese regelgeving, een wet, decreet of ordonnantie:

— de verwerkingsverantwoordelijke een mandaat geeft om gegevens te verwerken met het oog op archivering, onderzoek of statische doeleinden, en

— regels inzake veiligheid en vertrouwelijkheid oplegt aan de personen die werken voor rekening van de verwerkingsverantwoordelijke, en

— het hergebruik van de gegevens voor andere doeleinden verbiedt.

Art. 209

§ 1. De artikelen 17, 18 en 21 van de Verordening zijn niet van toepassing op verdere verwerkingen met het oog op onderzoek of statistische doeleinden, en waarvoor de kennisgeving betreffende de gegevensverzameling, opgelegd bij artikel 204, geldt.

§ 2. De artikelen 17, 18, 20 en 21 van de Verordening zijn niet van toepassing op verdere verwerkingen met het oog op archivering waarvoor de kennisgeving betreffende de gegevensverzameling, opgelegd bij artikel 204, geldt.

Afdeling 3

Anonimisering of pseudonimisering van de gegevens verwerkt met het oog op onderzoek of statistische doeleinden

Art. 210

In het kader van een verwerking van gegevens met het oog op onderzoek of statistische doeleinden, gebaseerd op een gegevensverzameling bij de betrokkene, gaat de verwerkingsverantwoordelijke over tot de anonimisering of pseudonimisering van de gegevens na de verzameling ervan.

Art. 211

In het kader van een verwerking van gegevens met het oog op onderzoek of statistische doeleinden door een verantwoordelijke voor een latere verwerking die dezelfde is als de verantwoordelijke voor de oorspronkelijke verwerking anonimiseert of pseudonimiseert de verwerkingsverantwoordelijke de gegevens voorafgaandelijk aan de verdere verwerking ervan.

sérieusement la réalisation de ces finalités d'archives, de recherche ou statistiques. La justification, l'avis du délégué à la protection des données du responsable du traitement et la justification du responsable du traitement lorsqu'il ne suit pas l'avis du délégué à la protection des données sont annexés au registre des activités de traitement; ou

b) le droit de l'Union européenne, une loi, un décret ou une ordonnance:

— donne pour mandat au responsable du traitement de traiter des données à des fins d'archives, de recherche ou statistique, et

— impose des règles de sécurité et de confidentialité aux personnes travaillant pour le compte du responsable du traitement, et

— interdit la réutilisation des données à d'autres fins.

Art. 209

§ 1er. Les articles 17, 18 et 21 du Règlement ne s'appliquent pas aux traitements ultérieur à des fins de recherche ou statistique et qui font l'objet de l'information sur la collecte de données imposée à l'article 204.

§ 2. Les articles 17, 18, 20 et 21 du Règlement ne s'appliquent pas aux traitements à des fins d'archives qui font l'objet de l'information sur la collecte de données imposée à l'article 204.

Section 3

Anonymisation ou pseudonymisation des données traitées à des fins de recherche ou statistiques

Art. 210

Lors d'un traitement de données à des fins de recherche ou statistiques basé sur une collecte de données auprès de la personne concernée, le responsable du traitement anonymise ou pseudonymise les données après leur collecte.

Art. 211

Lors d'un traitement ultérieur de données à des fins de recherche ou statistique par un responsable du traitement ultérieur identique au responsable du traitement initial, le responsable du traitement anonymise ou pseudonymise les données préalablement à leur traitement ultérieur.

Art. 212

De verwerkingsverantwoordelijke mag de gegevens slechts depseudonimiseren indien dat noodzakelijk is voor het onderzoek of de statistische doeleinden, en na advies van de functionaris voor gegevensbescherming.

Art. 213

Onverminderd bijzondere bepalingen, in het kader van een verdere verwerking van gegevens met het oog op onderzoek of statistische doeleinden door een verwerkingsverantwoordelijke die verschillend is van de verantwoordelijke voor de oorspronkelijke verwerking, pseudonimiseert of anonimiseert de verantwoordelijke voor de oorspronkelijke verwerking de gegevens voorafgaandelijk aan de mededeling ervan.

De verantwoordelijke voor de verdere verwerking heeft geen toegang tot de sleutels van de pseudonimisering.

Art. 214

§ 1. Onverminderd bijzondere bepalingen, in het kader van een latere verwerking van gegevens met het oog op onderzoek of statistische doeleinden waarbij meerdere intitiële verwerkingen worden gekoppeld, laten de verantwoordelijken voor de initiële verwerkingen vóór de mededeling van de gegevens, de gegevens ofwel door een verantwoordelijke voor de initiële verwerking ofwel door een derde vertrouwenspersoon anonimiseren of pseudonimiseren.

§ 2. Onverminderd bijzondere bepalingen, in het kader van een verdere verwerking van gepseudonimiseerde gegevens met het oog op onderzoek of statistische doeleinden die verschillende oorspronkelijke verwerkingen, waarvan tenminste één van gevoelige gegevens, aan elkaar koppelt, laten de verantwoordelijken voor de oorspronkelijke verwerkingen voorafgaandelijk aan de mededeling van de gegevens, de gegevens anonimiseren of pseudonimiseren door de verantwoordelijke voor de oorspronkelijke verwerking van gevoelige gegevens ofwel door een derde vertrouwenspersoon.

Enkel de verantwoordelijke voor de oorspronkelijke verwerking die de gegevens heeft gepseudonimiseerd of de derde vertrouwenspersoon heeft toegang tot de pseudonimiseringssleutels.

Art. 215

De derde vertrouwenspersoon mag geen belangenconflict hebben met de verantwoordelijke voor de verdere verwerking.

De derde vertrouwenspersoon is verwerker van de oorspronkelijke verwerkingsverantwoordelijken.

Art. 212

Le responsable du traitement ne peut dépseudonymiser les données que pour les nécessités de la recherche ou des fins statistiques et après avis du délégué à la protection des données.

Art. 213

Sauf dispositions particulières, lors d'un traitement ultérieur de données à des fins de recherche ou statistique par un responsable du traitement distinct du responsable du traitement initial, le responsable du traitement initial anonymise ou pseudonymise les données préalablement à leur communication.

Le responsable du traitement ultérieur n'a pas accès aux clés de la pseudonymisation.

Art. 214

§ 1er. Sauf dispositions particulières, lors d'un traitement ultérieur de données à des fins de recherche ou statistiques couplant plusieurs traitement initiaux, les responsables des traitements initiaux font, préalablement à la communication des données, anonymiser ou pseudonymiser les données soit par l'un des responsable du traitement initial soit par un tiers de confiance.

§ 2. Sauf dispositions particulières, lors d'un traitement ultérieur de données à des fins de recherche ou statistiques couplant plusieurs traitements initiaux dont l'un au moins de données sensibles, les responsables des traitements initiaux font, préalablement à la communication des données, anonymiser ou pseudonymiser les données soit par le responsable du traitement originel de données sensibles soit par un tiers de confiance.

Seul le responsable du traitement originel qui a pseudonymisé les données ou le tiers de confiance a accès aux clés de pseudonymisation.

Art. 215

Le tiers de confiance ne peut avoir de conflit d'intérêt avec le responsable du traitement ultérieur.

Le tiers de confiance est le sous-traitant des responsables des traitements initiaux.

Art. 216

De functionaris voor gegevensbescherming controleert het gebruik van de pseudonimiseringssleutels.

Art. 217

De artikelen 14, 15, 16, 18 en 21 van de Verordening zijn niet van toepassing op verwerkingen met het oog op onderzoek of statistische doeleinden wanneer de gegevens geanonimiseerd of gepseudonimiseerd zijn.

Afdeling 4

Verspreiding van gegevens verwerkt met het oog op archivering, onderzoek of statistische doeleinden

Art. 218

Onverminderd de Europese regelgeving, bijzondere wetten, ordonnanties en decreten die strengere voorwaarden opleggen voor de verspreiding van de gegevens die verwerkt zijn met het oog op archivering, onderzoek of statistische doeleinden, verspreidt de verwerkingsverantwoordelijke geen niet-gepseudonimiseerde gegevens, tenzij:

a) de betrokkene zijn toestemming heeft verleend; of

b) de gegevens door de betrokkene zelf openbaar zijn gemaakt; of

c) de gegevens nauw samenhangen met het openbare of historische karakter van de betrokkene; of

d) de gegevens nauw samenhangen met het openbare of historische karakter van feiten waarbij de betrokkene betrokken was.

Art. 219

Onverminderd de Europese regelgeving, bijzondere wetten, ordonnanties en decreten die strengere voorwaarden opleggen voor de verspreiding van de gegevens die verwerkt zijn met het oog op archivering, onderzoek of statistische doeleinden, mag de verwerkingsverantwoordelijke gepseudonimiseerde niet-gevoelige gegevens verspreiden.

Afdeling 5

Mededeling van de gegevens verwerkt met het oog op archivering, onderzoek of statistische doeleinden

Art. 220

Onverminderd de Europese regelgeving, bijzondere wetten, ordonnanties en decreten die strengere voorwaarden opleggen voor de mededeling, ziet de verwerkingsverantwoordelijke

Art. 216

Le délégué à la protection des données contrôle l'utilisation des clés de pseudonymisation.

Art. 217

Les articles 14, 15, 16, 18 et 21 du Règlement ne s'appliquent pas aux traitements à des fins de recherche ou statistiques lorsque les données sont anonymisées ou pseudonymisées.

Section 4

Diffusion des données traitées à des fins d'archives, de recherche ou statistiques

Art. 218

Sans préjudice du droit de l'Union européenne, des lois particulières, ordonnances et décrets prévoyant des conditions plus strictes de diffusion pour la diffusion des données traitées à des fins d'archives, de recherche et de statistiques le responsable du traitement ne diffuse pas les données non-pseudonymisées sauf lorsque:

a) la personne concernée a donné son consentement; ou

b) les données ont été rendues publiques par la personne concernée elle-même; ou

c) les données ont une relation étroite avec le caractère public ou historique de la personne concernée; ou

d) les données ont une relation étroite avec le caractère public ou historique de faits dans lesquelles la personne concernée a été impliquée.

Art. 219

Sans préjudice du droit de l'Union européenne, des lois particulières, ordonnances et décrets prévoyant des conditions plus strictes pour la diffusion des données traitées à des fins d'archives, de recherche et de statistiques, le responsable du traitement peut diffuser des données pseudonymisées non-sensibles.

Section 5

Communication des données traitées à des fins d'archives, de recherche ou statistiques

Art. 220

Sans préjudice du droit de l'Union européenne, des lois particulières, ordonnances et décrets prévoyant des conditions plus strictes pour la communication, le responsable du

erop toe dat de meegedeelde niet-gepseudonimiseerde gegevens niet gereproduceerd worden wanneer:

a) het om gevoelige gegevens gaat; of

b) de overeenkomst tussen de verantwoordelijke voor de oorspronkelijke verwerking en de verantwoordelijke voor de verdere verwerking zulks verbiedt; of

c) die reproductie de veiligheid van de betrokkene in het gedrang kan brengen.

Art. 221

De verplichting bedoeld in artikel 220 is niet van toepassing indien:

a) de betrokkene zijn toestemming heeft verleend; of

b) de gegevens door de betrokkene zelf openbaar zijn gemaakt; of

c) de gegevens nauw samenhangen met het openbare of historische karakter van de betrokkene; of

d) de gegevens nauw samenhangen met het openbare of historische karakter van feiten waarbij de betrokkene betrokken was.

TITEL 5

Rechtsmiddelen en vertegenwoordiging van de betrokkenen

HOOFDSTUK I

Vordering tot staking

Artikel 222

Onverminderd andere mogelijkheden tot rechterlijk, administratief of buitengerechtelijk beroep, stelt de voorzitter van de rechtbank van eerste aanleg, zitting houdende zoals in kort geding, het bestaan vast van een verwerking en beveelt er de staking van indien die een inbreuk uitmaakt op een wettelijke en reglementaire bepaling betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens.

Artikel 223

Vanaf het moment dat de gegevens waarnaar wordt verwezen in de behandeling bedoeld in artikel 222, worden verwerkt in de loop van een opsporingsonderzoek, van een gerechtelijk onderzoek, een strafrechtelijke procedure voor de bodemrechter of een procedure voor de uitvoering van een strafrechtelijk vonnis, behoort de beslissing over de rectificatie, schrapping, beperking van de behandeling, het

traitement veille à ce que les données communiquées non-pseudonymisées ne soient pas reproduites lorsque :

a) elles sont sensibles; ou

b) la convention entre le responsable du traitement initial et le responsable du traitement ultérieur, l'interdit; ou

c) cette reproduction risque de nuire à la sécurité de la personne concernée.

Art. 221

L'obligation visée à l'article 220 n'est pas applicable si:

a) la personne concernée a donné son consentement; ou

b) les données ont été rendues publiques par la personne concernée elle-même; ou

c) les données ont une relation étroite avec le caractère public ou historique de la personne concernée; ou

d) les données ont une relation étroite avec le caractère public ou historique de faits dans lesquelles la personne concernée a été impliquée.

TITRE 5

Voies de recours et représentation des personnes concernées

CHAPITRE IER

Recours en cessation

Article 222

Sans préjudice de tout autre recours juridictionnel, administratif ou extrajudiciaire, le président du tribunal de première instance, siégeant comme en référé, constate l'existence et ordonne la cessation d'un traitement, constituant une violation aux dispositions légales ou réglementaires concernant la protection des personnes physiques à l'égard du traitement de leur données à caractère personnel.

Article 223

A partir du moment où les données faisant l'objet du traitement visé par l'article 222 font l'objet d'un traitement lors d'une information, d'une instruction, d'une procédure pénale devant le juge de fond ou d'une procédure d'exécution d'une peine pénale, la décision concernant la rectification, la suppression, la limitation du traitement, l'interdiction d'utiliser, ou l'effacement de données à caractère personnel appartient

verbod op gebruik of verwijdering van persoonsgegevens echter uitsluitend, volgens de fase van de procedure, tot het openbaar ministerie of de bevoegde strafrechter.

Art. 224

§ 1. De vordering tot staking wordt ingediend bij verzoekschrift op tegenspraak, overeenkomstig de artikelen 1034*ter* tot 1034*sexies* van het Gerechtelijk wetboek.

§ 2. In afwijking van artikel 624 van het Gerechtelijk wetboek kan de vordering naar keuze van de eiser worden gebracht voor de voorzitter van de rechtbank van eerste aanleg van:

1. de woonplaats of verblijfplaats van de eiser, indien de eiser of minstens één van de eisers de betrokkene is;

2. de woonplaats, verblijfplaats, zetel of plaats van vestiging van de verweerders of één van de verweerders;

3. de plaats of één van de plaatsen waar een deel of het geheel van de verwerking gebeurt.

Indien de verweerder geen woonplaats, verblijfplaats, zetel of plaats van vestiging in België heeft, wordt de vordering gebracht voor de voorzitter van de rechtbank van eerste aanleg te Brussel.

§ 3. De vordering gegrond op artikel 222 wordt ingesteld door:

1. de betrokkene;

2. de voorzitter van de bevoegde toezichthoudende autoriteit.

Art. 225

Behoudens de toepassing van andersluidende bepalingen in internationale verdragen die in België van kracht zijn of in het recht van de Europese Unie, en onverminderd hun internationale rechtsmacht op grond van de bepalingen van het Wetboek van internationaal privaatrecht, hebben de Belgische hoven en rechtbanken in elk geval internationale rechtsmacht voor de in artikel 222 van deze wet bedoelde vorderingen tegen:

1. een verwerkingsverantwoordelijke of een verwerker die op Belgische grondgebied gevestigd is of een vestiging heeft, wat betreft de verwerking van persoonsgegevens in het kader van de activiteiten van die vestiging, ongeacht de plaats waar de verwerking plaatsvindt;

2. een verwerkingsverantwoordelijke of verwerker die niet op Belgische grondgebied gevestigd is of een vestiging heeft, wat betreft verwerkingen die gevolgen hebben voor of geheel of gedeeltelijk gericht zijn op betrokkenen die zich op het Belgische grondgebied bevinden.

toutefois exclusivement, suivant la phase de la procédure, au ministère public ou au juge pénal compétent.

Art. 224

§ 1er. Le recours en cessation est introduit par requête contradictoire conformément aux articles 1034*ter* à 1034*sexies* du Code judiciaire.

§ 2. Par dérogation à l'article 624 du Code judiciaire, le recours peut être porté, au choix du demandeur, devant le président du tribunal de première instance:

1. du domicile ou de la résidence du demandeur, si le demandeur, ou au moins un des demandeurs, est la personne concernée;

2. du domicile ou de la résidence, du siège social ou le lieu d'établissement du défendeur ou d'un des défendeurs;

3. du lieu ou d'un des lieux où une partie ou la totalité du traitement a été accompli.

Lorsque le défendeur n'a ni domicile, ni résidence, ni siège social ou lieu d'établissement en Belgique, le recours peut être porté devant le président du Tribunal de première instance de Bruxelles.

§ 3. Le recours fondé sur l'article 222 est formé à la demande:

1. de la personne concernée;

2. du président de l'autorité de contrôle compétente.

Art. 225

Sous réserve de l'application de dispositions contraires dans les traités internationaux en vigueur en Belgique ou dans le droit de l'Union européenne, et sans préjudice de leur compétence internationale en vertu des dispositions du Code de droit international privé, les cours et tribunaux belges ont la compétence internationale pour les affaires portées en vertu de l'article 222 de la présente loi contre:

1. un responsable du traitement ou un sous-traitant situé sur le territoire belge ou ayant un établissement, en ce qui concerne le traitement de données à caractère personnel en rapport avec les activités de cet établissement, quel que soit le lieu du traitement;

2. un responsable du traitement ou un sous-traitant qui n'est pas établi ou n'a pas un établissement sur le territoire belge, en ce qui concerne un traitement ayant des conséquences pour ou visant en tout ou en partie des personnes concernées résidant sur le territoire belge.

Art. 226

§ 1. De beschikking wordt in openbare rechtszitting uitgesproken.

§ 2. De beschikking wordt ter kennis gebracht aan de bevoegde toezichthoudende autoriteit binnen acht dagen.

§ 3. Bovendien is de griffier van de rechtbank waar een beroep is ingesteld tegen de in het eerste paragraaf bedoelde beschikking verplicht om de bevoegde toezichthoudende autoriteit onverwijld in te lichten.

Art. 227

De voorzitter van de rechtbank van eerste aanleg kan een termijn toestaan om aan de inbreuk een einde te maken, wanneer de aard van de inbreuk dit nodig maakt. Hij kan de opheffing van het stakingsbevel toestaan wanneer een einde werd gemaakt aan de inbreuk.

Art. 228

§ 1. De voorzitter van de rechtbank van eerste aanleg kan toestaan dat zijn beslissing of de samenvatting die hij opstelt, wordt aangeplakt tijdens de door hem bepaalde termijn, zowel buiten als binnen de betrokken inrichtingen, en kan op de wijze die hij gepast acht bevelen dat zijn beschikking of de samenvatting ervan in kranten of op enige andere wijze wordt bekendgemaakt, dit alles op kosten van de in het ongelijk gestelde partij.

§ 2. De in de eerste paragraaf vermelde maatregelen van openbaarmaking mogen evenwel slechts toegestaan worden indien zij er toe kunnen bijdragen dat de gewraakte daad of de uitwerking ervan ophouden.

§ 3. Wanneer overeenkomstig de eerste paragraaf een publicatiemaatregel werd toegekend, stelt de voorzitter van de rechtbank van eerste aanleg het bedrag vast dat moet betaald worden aan de partij die de maatregel heeft uitgevoerd in het geval dat deze maatregel in beroep hervormd wordt.

Art. 229

In het kader van een in artikel 222 bedoelde vordering kan de eiser een schadevergoeding vorderen overeenkomstig het contractuele of buitencontractuele aansprakelijkheidsrecht.

Art. 230

Indien onjuiste, onvolledige of niet ter zake dienende persoonsgegevens of persoonsgegevens waarvan de bewaring verboden is, aan derden zijn medegedeeld, of indien een mededeling van persoonsgegevens heeft plaatsgehad na verloop van de tijd waarin de verwerking van die persoonsgegevens toegelaten is, kan de voorzitter van de rechtbank van eerste aanleg gelasten dat de verwerkingsverantwoordelijke,

Art. 226

§ 1er. L'ordonnance est prononcée en audience publique.

§ 2. L'ordonnance est notifiée à l'autorité de contrôle compétente dans les huit jours.

§ 3. En outre, le greffier de la juridiction devant laquelle un recours est introduit contre l'ordonnance visée au paragraphe premier est tenu d'en informer sans délai l'autorité de contrôle compétente.

Art. 227

Le président du tribunal de première instance peut accorder un délai pour mettre fin à la violation, lorsque la nature de la violation le nécessite. Il peut accorder la levée de la cessation lorsqu'il a été mis fin à la violation.

Art. 228

§ 1er. Le président du tribunal de première instance peut autoriser l'affichage de sa décision ou du résumé qu'il en rédige, pendant le délai qu'il détermine, aussi bien à l'extérieur qu'à l'intérieur des établissements concernés et ordonner, selon la manière qu'il jugera appropriée, la publication de son ordonnance ou de son résumé par la voie de journaux ou de toute autre manière, le tout aux frais de la partie qui succombe.

§ 2. Les mesures de publicité mentionnées au paragraphe premier ne peuvent toutefois être autorisées que si elles sont de nature à contribuer à la cessation de l'acte incriminé ou de ses effets.

§ 3. Lorsque qu'une mesure de publicité a été accordée conformément au paragraphe premier, le président du tribunal de première instance fixe le montant à payer à la partie qui a exécuté la mesure dans le cas où cette mesure est réformée en appel.

Art. 229

Dans le cadre d'un recours visé à l'article 222, le demandeur peut réclamer la réparation de son dommage conformément à la responsabilité contractuelle ou extracontractuelle.

Art. 230

Lorsque des données à caractère personnel inexactes, incomplètes ou non pertinentes, ou des données à caractère personnel dont la conservation est interdite, ont été communiquées à des tiers, ou lorsque une communication de données à caractère personnel a eu lieu après l'expiration de la période durant laquelle la conservation de ces données était autorisée, le président du tribunal de première instance peut

de verwerker, de ontvanger of hun gedelegeerde aan die derden kennis geeft van de beperking van de verwerking of de verbetering of verwijdering van die persoonsgegevens.

Art. 231

Indien dwingende redenen bestaan om te vrezen dat bewijselementen die kunnen worden aangevoerd ter ondersteuning van een vordering voorzien in dit hoofdstuk worden verheeld, verdwijnen of ontoegankelijk worden gemaakt, gelast de voorzitter van de rechtbank van eerste aanleg op eenzijdig verzoekschrift, ondertekend en ingediend door de partij of haar advocaat, elke maatregel ter voorkoming van die verheling verdwijning of ontoegankelijkheid.

Art. 232

De bepalingen van dit hoofdstuk houden geen beperking in van de bevoegdheid van de rechtbank van eerste aanleg en van de voorzitter van de rechtbank van eerste aanleg zetelend in kort geding.

HOOFDSTUK II

Vertegenwoordiging van betrokkenen

Art. 233

§ 1. De betrokkene heeft het recht om een orgaan, een organisatie, of een vereniging zonder winstoogmerk de opdracht te geven een klacht namens hem in te dienen en namens hem de administratieve of gerechtelijke beroepen uit te oefenen, hetzij aan de bevoegde toezichthoudende autoriteit, hetzij aan de rechterlijke macht als bepaald in de bijzondere wetten en het Wetboek van Strafvordering.

§ 2. Bij de geschillen voorzien in de eerste paragraaf, moet een orgaan, een organisatie of een vereniging zonder winstoogmerk:

— op geldige wijze zijn opgericht in overeenstemming met de Belgische wetgeving;

— rechtspersoonlijkheid bezitten;

— statutaire doelstellingen van openbaar belang hebben;

— actief zijn op het gebied van de bescherming van de rechten en vrijheden van de betrokkenen in verband met de bescherming van de persoonsgegevens en dit sedert ten minste drie jaar.

§ 3. Het orgaan, de organisatie of vereniging zonder winstoogmerk newijst door de voorlegging van haar activiteitenverslagen of van enig ander stuk, dat zijn activiteit minstens drie jaar effectief is geweest, dat het overeenstemt met haar

ordonner au responsable du traitement, au sous-traitant, au destinataire ou son délégué d'informer ces tiers de la limitation du traitement, de la rectification ou de la suppression de ces données à caractère personnel.

Art. 231

Lorsqu'il existe des motifs sérieux de craindre la dissimulation, la disparition ou l'inaccessibilité des éléments de preuve qui peuvent être invoqués à l'appui d'une action prévue au présent chapitre, le président du tribunal de première instance, saisi par voie de requête unilatérale, signée et présentée par la partie ou son avocat, ordonne toute mesure de nature à éviter cette dissimulation, disparition ou inaccessibilité.

Art. 232

Les dispositions du présent chapitre ne limitent pas la compétence du tribunal de première instance et du président du tribunal de première instance siégeant en référé.

CHAPITRE II

Représentation des personnes concernées

Art. 233

§ 1er. La personne concernée a le droit de mandater un organe, une organisation ou une association à but non lucratif, pour qu'il introduise une réclamation en son nom et exerce en son nom les recours administratifs ou juridictionnels soit auprès de l'autorité de contrôle compétente soit auprès de l'ordre judiciaire tels que prévus par les lois particulières et le Code de procédure pénale.

§ 2. Dans les litiges prévus au paragraphe premier, un organe, une organisation ou une association sans but lucratif doit nécessairement:

— être valablement constituée conformément au droit belge;

— avoir la personnalité juridique;

— avoirdes objectifs statutaires d'intérêt public;

— être actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel depuis au moins trois ans.

§ 3. L'organe, l'organisation ou l'association sans but lucratif fournit la preuve, par la présentation de ses rapports d'activités ou de toute autre pièce, que son activité est effective depuis au moins trois ans, qu'elle corresponde à son objet

maatschappelijk doel en dat deze activiteit betrekking heeft op de bescherming van de persoonsgegevens.

TITEL 6

Sancties

HOOFDSTUK I

Administratieve sancties

Art. 234

§ 1. De corrigerende bevoegdheden van de toezichthoudende autoriteit krachtens artikel 58.2 van de Verordening zijn tevens van toepassing op de artikelen 7, 8, 9, 19, 23, 25, 26, 28 en 29 van titel 1, op de artikelen 33 tot 72 van titel 2 en op titel 4 van deze wet.

§ 2. Het artikel 83 van de Verordening is niet van toepassing op de overheidsinstanties en openbare organen.

HOOFDSTUK II

Strafsancties

Art. 235

De verwerkingsverantwoordelijke of de verwerker, zijn vertegenwoordiger in België, zijn aangestelde of gemachtigde, de bevoegde overheid, zoals bedoeld in titels 1 en 2, wordt gestraft met een geldboete van tweehonderdvijftig euro tot vijftienduizend euro wanneer:

a) de persoonsgegevens verwerkt worden zonder wettelijke basis in overeenstemming met artikel 6 van de Verordening en de artikelen 34, § 1 en 38, § 1, van deze wet, inbegrepen de voorwaarden voor de toestemming en verdere verwerking;

b) de persoonsgegevens verwerkt worden in overtreding van de voorwaarden opgelegd door artikel 5 van de Verordening en artikel 33 van deze wet, met enstige nalatigheid of kwaadwillig;

c) de verwerking waartegen ingevolge artikel 21.1 van de Verordening bezwaar is gemaakt, wordt gehandhaafd zonder dwingende wettige redenen;

d) de doorgifte van persoonsgegevens aan een ontvanger in een derde land of een internationale organisatie, gebeurt in overtreding van de waarborgen, voorwaarden of uitzonderingen voorzien in de artikelen 44 tot 49 van de Verordening of de artikelen 68 tot 72 van deze wet met ernstige nalatigheid of kwaadwillig;

social et que cette activité est en relation avec la protection des données à caractère personnel.

TITRE 6

Sanctions

CHAPITRE I^ER

Sanctions administratives

Art. 234

§ 1er. Les compétences correctrices de l'autorité de contrôle en vertu de l'article 58.2 du Règlement s'appliquent également aux articles 7, 8, 9, 19, 23, 25, 26, 28 et 29 du titre 1er, aux articles 33 à 72 du titre 2 et au titre 4 de la présente loi.

§ 2. L'article 83 du Règlement ne s'applique pas aux autorités publiques et organismes publics.

CHAPITRE II

Sanctions pénales

Art. 235

Le responsable du traitement ou le sous-traitant, son représentant en Belgique, son préposé ou mandataire, l'autorité compétente, visés aux titres 1 et 2, est puni d'une amende de deux cent cinquante euros à quinze mille euros lorsque:

a) les données à caractère personnel sont traitées sans base juridique conformément à l'article 6 du Règlement et aux articles 34, § 1er, et 38, § 1er, de la présente loi, y compris les conditions relatives au consentement et aux traitements ultérieurs;

b) les données à caractère personnel sont traitées en violation des conditions imposées par l'article 5 du Règlement et à l'article 33 de la présente loi par négligence grave ou avec intention malveillante;

c) le traitement ayant fait l'objet d'une objection conformément à l'article 21.1 du Règlement est maintenu sans raisons juridiques impérieuses;

d) le transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, effectué en violation des garanties, conditions ou exceptions prévues dans les articles 44 à 49 du Règlement ou des articles 68 à 72 de la présente loi par négligence grave ou avec intention malveillante;

e) de door de toezichthoudende autoriteit vastgestelde corrigerende maatregel voor de definitieve beperking van stromen in overeenstemming met artikel 58.2.f) van de Verordening niet wordt gerespecteerd;

f) de wettelijke verificatie- en controle-opdrachten van de bevoegde toezichthoudende overheid, haar leden of deskundigen werden belemmerd;

g) de weerspannigheid ten aanzien van de leden van de bevoegde autoriteit wordt bestraft overeenkomstig artikelen 269 tot 274 van het Strafwetboek;

h) de certificering als bedoeld in artikel 42 van de Verordening wordt geclaimd of certificeringen voor de gegevensbescherming worden openbaar gebruikt, ook al zijn die certificeringen, zegels of markeringen nog niet afgegeven door een geaccrediteerde entiteit of worden ze gebruikt na de geldigheid van de certificering, zegel of merk is verlopen;

i) de certificering als bedoeld in artikel 42 van de Verordening is verkregen op basis van valse documenten of onjuiste documenten;

j) taken worden uitgevoerd als een certificeringsorgaan, ook al is deze niet geaccrediteerd door de bevoegde nationale accreditatie-instantie;

k) het certificeringsorgaan niet voldoet aan de beginselen en taken waaraan het onderworpen is, zoals bepaald in de artikelen 42 en 43 van de Verordening;

l) de taken van het in artikel 41 van de Verordening bedoelde orgaan worden uitgevoerd zonder accreditatie van de bevoegde toezichthoudende autoriteit;

m) het geaccrediteerde orgaan bedoeld in artikel 41 van de Verordening niet de passende maatregelen heeft genomen in geval van een inbreuk op de gedragscode zoals bedoeld in artikel 41.4 van de Verordening.

Art. 236

Met een geldboete van vijfhonderd euro tot dertigduizend euro wordt de verwerkingsverantwoordelijke bedoeld in titel 1, de verwerker of de persoon die handelt onder hun gezag gestraft die:

1° de betrokkene, als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, heeft ingelicht over het bestaan van een persoonsgegeven dat hem aangaat dat afkomstig is van een overheid bedoeld in de titel 3 van deze wet in overtreding van artikel 12, terwijl hij de oorsprong van het gegeven kende en hij zich niet bevond in één van de gevallen bedoeld in 1° en 2°, van het vermelde artikel;

2° de betrokkene, als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, heeft ingelicht dat een overheid bedoeld in titel 3 de ontvanger is van één van zijn persoonsgegevens in overtreding van artikel 13.

e) la mesure correctrice adoptée par l'autorité de contrôle visant la limitation définitive des flux conformément à l'article 58.2.f) du Règlement n'est pas respectée;

f) il a été fait obstacle aux missions légales de vérification et de contrôle de l'autorité de contrôle compétente, ses membres ou ses experts;

g) la rébellion à l'encontre des membres de l'autorité de contrôle, puni conformément aux articles 269 à 274 du Code pénal;

h) la certification visée à l'article 42 du Règlement est revendiquée ou des sceaux de certification en matière de protection des données sont utilisées publiquement alors que ces certifications, labels ou marques n'ont pas été délivrés par une entité accréditée ou ceux-ci sont utilisés après que la validité de la certification, du sceau ou de la marque a expiré;

i) la certification visée à l'article 42 du Règlement a été obtenue sur la base de faux documents ou documents erronés;

j) des tâches sont exécutées en tant qu'organisme de certification alors que celui-ci n'a pas été accrédité par l'organisme national d'accréditation compétent;

k) l'organisme de certification ne se conforme pas aux principes et aux tâches auxquels il est soumis tel que prévu aux articles 42 et 43 du Règlement;

l) les tâches de l'organisme visée à l'article 41 du Règlement sont exécutées sans agrément par l'autorité de contrôle compétente;

m) l'organisme agréé visé à l'article 41 du Règlement n'a pas pris les mesures appropriées en cas de violation du code de conduite tel que visé à l'article 41.4 du Règlement.

Art. 236

Est puni d'une amende de cinq cents euros à trente mille euros, le responsable du traitement visé au titre 1er, le sous-traitant ou la personne agissant sous leur autorité qui:

1° a, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, informé la personne concernée de l'existence d'une donnée à caractère personnel la concernant émanant d'une autorité visée au titre 3 de la présente loi en violation de l'article 12, alors qu'il connaissait l'origine de la donnée et qu'il ne se trouvait pas dans un des cas visés au 1° ou 2°, dudit article;

2° a, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, informé la personne concernée qu'une autorité visée au titre 3 est destinataire d'une de ses données à caractère personnel en violation de l'article 13.

Art. 237

Met een geldboete van twee honderd tot tien duizend euro wordt gestraft elk lid of elk personeelslid van de bevoegde toezichthoudende autoriteit of elke deskundige die de verplichting tot vertrouwelijkheid waartoe hij is gehouden heeft geschonden.

Art. 238

Bij veroordeling wegens een misdrijf omschreven in de artikelen 236 of 237, kan de rechtbank bevelen dat het vonnis in zijn geheel of bij uittreksel wordt opgenomen in een of meerdere dagbladen op de wijze die zij bepaalt, zulks op kosten van de veroordeelde.

Art. 239

§ 1. Met een geldboete van honderd euro tot tienduizend euro wordt gestraft de verwerker die één van de verplichtingen van vertrouwelijkheid en beveiliging, bedoeld in de artikelen 85 tot 88, 118 tot 121, 151 tot 154 tot 179 à 180 niet heeft nageleefd.

§ 2. De persoon die handelt onder het gezag van de overheid bedoeld in titel 3 of van diens verwerker, die als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, één van de verplichtingen van vertrouwelijkheid en beveiligheid, bedoeld in de artikelen 85 tot 88, 118 tot 121, 151 tot 154 tot 179 à 180 niet heeft nageleefd, wordt gestraft met een geldboete van honderd euro tot tienduizend euro.

Art. 240

Met een geldboete van honderd euro tot twintigduizend euro wordt gestraft:

1° de verwerker, de persoon die handelt onder het gezag van de overheid bedoeld in titel 3 of van de verwerker of de aangestelde die de persoonsgegevens verwerkt buiten de gevallen bedoeld in artikelen 76, 110, 142 et 172;

2° de verwerker of de aangestelde die persoonsgegevens verwerkt met overtreding van de voorwaarden voor de verwerking opgelegd door artikelen 77, 111, 143 en 172 en de persoon die handelt onder het gezag van de overheid bedoeld in titel 3 of van diens verwerker, die als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, gegevens verwerkt met overtreding van de voorwaarden opgelegd door artikel 77, 111, 143 en 172;

3° hij die, om een persoon te dwingen hem zijn instemming te geven met de verwerking van de hem betreffende persoonsgegevens, jegens die persoon gebruik maakt van feitelijkheden, geweld, bedreigingen, giften of beloften;

4° hij die persoonsgegevens doorgeeft, doet of laat doorgeven, als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, naar een land dat geen lid is van de Europese

Art. 237

Est puni d'une amende de deux cents euros à dix mille euros, tout membre ou tout membre du personnel de l'autorité de contrôle compétente ou tout expert qui a violé l'obligation de confidentialité à laquelle il est astreint.

Art. 238

En condamnant du chef d'infraction aux articles 236 ou 237, le tribunal peut ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'il détermine, aux frais du condamné.

Art. 239

§ 1er. Est puni d'une amende de cent euros à dix mille euros, le sous-traitant qui n'a pas respecté une des obligations de confidentialité et de sécurité visées aux articles 85 à 88, 118 à 121, 151 à 154 et 179 à 180.

§ 2. Est puni d'une amende de cent euros à dix mille euros, la personne agissant sous l'autorité d'une autorité visée au titre 3 ou de son sous-traitant qui, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, n'a pas respecté une des obligations de confidentialité et de sécurité visées aux articles 85 à 88, 118 à 121, 151 à 154 et 179 à 180.

Art. 240

Est puni d'une amende de cent euros à vingt mille euros:

1° le sous-traitant, la personne agissant sous l'autorité de l'autorité visée au titre 3 ou du sous-traitant ou le mandataire qui traite des données à caractère personnel en dehors des cas prévus aux articles 76, 110, 142 et 172;

2° le sous-traitant ou le mandataire qui traite des données à caractère personnel en infraction aux conditions imposées par les articles 77, 111, 143 et 172 et la personne agissant sous l'autorité d'une autorité visée au titre 3 ou du sous-traitant qui, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, traite des données à caractère personnel en infraction aux conditions imposées par les articles 77, 111, 143 et 172;

3° quiconque, pour contraindre une personne à lui donner son autorisation au traitement de données à caractère personnel la concernant, a usé à son égard de voies de fait, de violence ou menaces, de dons ou de promesses;

4° quiconque a transféré, fait ou laissé transférer, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, des données à caractère personnel

Unie of een internationale organisatie zonder dat is voldaan aan de vereisten opgelegd door artikelen 95, 96, 128, 129, 161, 162, 184 en 185;

5° elke persoon die toegang heeft tot persoonsgegevens bedoeld in artikelen 101, 134 en 164 voor historische, wetenschappelijke of statistische doeleinden, die deze gegevens verwerkt in overtreding van met inbreuk op artikelen 104, 137, 167 of 106, 139, 169.

Art. 241

Onverminderd bijzondere wettelijke bepalingen, is de verwerkingsverantwoordelijke, de verwerker, of zijn vertegenwoordiger in België burgerrechtelijk aansprakelijk voor de betaling van de boeten waartoe zijn aangestelde of gemachtigde is veroordeeld.

Art. 242

§ 1. Met betrekking tot de in artikelen 235 en 236 bedoelde inbreuken kunnen de bevoegde toezichthoudende autoriteit en het College van procureurs-generaal een protocol afsluiten voor de werkafspraken tussen de toezichthoudende autoriteit en het openbaar ministerie in dossiers die betrekking hebben op feiten waarvoor de wetgeving zowel in de mogelijkheid van een administratieve geldboete als in de mogelijkheid van een strafsanctie voorziet.

De Koning legt, bij een in Ministerraad overlegd besluit, de nadere modaliteiten en het model vast van dit protocolakkoord.

Dit protocolakkoord leeft alle wettelijke bepalingen na die met name betrekking hebben op de procedures voorzien voor de overtreders en kan de rechten van de overtreders niet schenden.

Het protocolakkoord wordt in het *Belgisch Staatsblad* en op de internetsite van de bevoegde toezichthoudende autoriteit bekendgemaakt.

§ 2. Bij gebrek aan een protocolakkoord en voor de inbreuken bedoeld in artikelen 235 en 236 beschikt de procureur des Konings over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het origineel proces-verbaal, om aan de bevoegde toezichthoudende autoriteit mee te delen dat een opsporingsonderzoek of een gerechtelijk onderzoek werd opgestart of vervolging werd ingesteld. Deze mededeling doet de mogelijkheid vervallen voor de toezichthoudende autoriteit om haar corrigerende bevoegdheden uit te oefenen.

De bevoegde toezichthoudende autoriteit kan geen sanctie opleggen vóór het verstrijken van deze termijn. Bij gebrek aan een mededeling binnen twee maanden, kunnen de feiten enkel nog administratiefrechtelijk worden bestraft.

vers un pays non membre de l'Union européenne ou vers une organisation internationale sans qu'il ait été satisfait aux exigences prévues aux articles95, 96, 128, 129, 161, 162, 184 et 185;

5° toute personne qui a accès à des données à caractère personnel visées aux articles 101, 134 et 164 à des fins historiques, scientifiques ou statistiques qui traite ces données en violation des articles 104, 137, 167 ou 106, 139, 169.

Art. 241

Sans préjudice de toute disposition légale particulière, le responsable du traitement, le sous-traitant, ou son représentant en Belgique est civilement responsable du paiement des amendes auxquelles son préposé ou mandataire a été condamné.

Art. 242

§ 1er. En ce qui concerne les infractions visées aux articles 235 et 236, l'autorité de contrôle compétente et le Collège des Procureurs généraux peuvent conclure un protocole régissant les accords de travail entre l'autorité de contrôle et le ministère public dans des dossiers portant sur des faits pour lesquels la législation prévoit aussi bien la possibilité d'une amende administrative que la possibilité d'une sanction pénale.

Le Roi fixe les modalités et le modèle de ce protocole par arrêté délibéré en Conseil des ministres.

Ce protocole d'accord respecte l'ensemble des dispositions légales concernant notamment les procédures prévues pour les contrevenants et ne peut déroger aux droits de ceux-ci.

Le protocole d'accord est publié au *Moniteur belge* et sur le site internet de l'autorité de contrôle compétente.

§ 2. A défaut de protocole d'accord et pour les infractions visées aux articles 235 et 236 le procureur du Roi dispose d'un délai de deux mois, à compter du jour de la réception de l'original du procès-verbal, pour communiquer à l'autorité de contrôle compétente qu'une information ou une instruction a été ouverte ou que des poursuites ont été entamées. Cette communication éteint la possibilité pour l'autorité de contrôle d'exercer ses mesures correctrices.

L'autorité de contrôle compétente ne peut infliger une sanction avant l'échéance de ce délai. A défaut de communication du Procureur du Roi dans les deux mois, les faits ne peuvent être sanctionnés que de manière administrative.

TITEL 7

Het controleorgaan op de politionele informatie

HOOFDSTUK I

Samenstelling en statuut van de leden en van de dienst onderzoeken

Art. 243

§ 1. Het Controleorgaan op de politionele informatie, hierna aangeduid als "Controleorgaan" is samengesteld uit drie werkende leden, waaronder een voorzitter, die hun functies voltijds uitoefenen. De toezichthoudende autoriteit is naast de Voorzitter, die een magistraat moet zijn, samengesteld uit een magistraat van het openbaar ministerieen een expert.

Behoudens één van de leden die functioneel tweetalig dient te zijn, bestaat het Controleorgaan uit een gelijk aantal Nederlandstalige en Franstalige leden. Zij worden allen benoemd door de Kamer van volksvertegenwoordigers, die hen ook kan afzetten wanneer de in artikel 244 bepaalde voorwaarden in hun hoofde niet meer vervuld zijn of wegens ernstige redenen. Zij kunnen evenwel niet van hun mandaat worden ontheven voor meningen die zij uiten of daden die zij stellen bij het vervullen van zijn functies.

§ 2. De leden van het Controleorgaan worden op grond van hun competentie, hun ervaring, hun onafhankelijkheid en hun moreel gezag door de Kamer van volksvertegenwoordigers voor een termijn van zes jaar, éénmaal hernieuwbaar, aangesteld.

Deze termijn begint te lopen vanaf hun eedaflegging. Na afloop van deze termijn, blijven de leden hun functie uitoefenen tot de eedaflegging van hun opvolger.

De leden mogen geen bij verkiezing verleend openbaar mandaat uitoefenen. Zij mogen geen openbare of particuliere betrekking of activiteit uitoefenen die de onafhankelijkheid of de waardigheid van het ambt in gevaar zou kunnen brengen of die onverenigbaar is met hun taken.

§ 3. Alvorens hun ambt te aanvaarden, leggen de leden van het Controleorgaan in handen van de Voorzitter van de Kamer van volksvertegenwoordigers de bij artikel 2 van het decreet van 30 juli 1831 voorgeschreven eed af.

§ 4. Het Controleorgaan is daarnaast samengesteld uit een Dienst Onderzoeken, hierna genoemd "de Dienst Onderzoeken", die bestaat uit drie werkende leden die hun functies voltijds uitoefenen, waaronder twee leden van de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus, en een expert.

De dienst onderzoeken hangt exclusief af van het Controleorgaan. Het Controleorgaan oefent het gezag uit

TITRE 7

L'organe de contrôle de l'information policière

CHAPITRE I^ER

Composition et statut des membres et du service d'enquête

Art. 243

§ 1^er. L'Organe de contrôle de l'information policière, ci-après dénommé "Organe de contrôle", se compose de trois membres effectifs dont un président, lesquels exercent leurs fonctions à temps plein. Outre le président qui doit être un magistrat, l'Autorité de contrôle se compose d'un magistrat du ministère public, et d' un expert.

Un des membres qui doit être fonctionellement bilingue exclu, l'organe de contrôle comprend autant de personnes d'expression française que de personnes d'expression néerlandaise parmi ses membres. Tous sont nommés par la Chambre des représentants qui ne peut les démettre de leurs fonctions que si les conditions prévues à l'article 244 ne sont plus rencontrées ou pour motifs graves. Ils ne peuvent être relevés de leurs fonctions en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent pour remplir leurs fonctions.

§ 2. Les membres de L'Organe de contrôle sont nommés, sur base de leur compétence, de leur expérience, de leur indépendance et de leur autorité morale par la Chambre des représentants pour un terme de six ans renouvelable une fois.

Ce délai prend cours à partir de la prestation de serment. A l'issue de ce terme, les membres continuent à exercer leurs fonctions jusqu'à la prestation de serment de leur successeur.

Les membres ne peuvent occuper aucun mandat public conféré par élection. Ils ne peuvent exercer d'emploi ou d'activité public(que) ou privé(e) qui pourrait mettre en péril l'indépendance ou la dignité de la fonction ou qui est incompatible avec leur fonction.

§ 3. Avant d'entrer en fonction, les membres de L'Organe de contrôle prêtent, entre les mains du président de la Chambre des représentants, le serment prescrit par l'article 2 du décret du 30 juillet 1831.

§ 4. L'Organe de contrôle est, en outre, composé d'un service enquête ci-après dénommé "service d'enquête", lequel est composé de trois membres effectifs lesquels exercent leurs fonctions à temps plein, dont deux membres des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, et d'un expert.

Le service d'enqûete relève de l'autorité exclusive de l'Organe de Contrôle. L'Organe de controle exerce son

over de Dienst Onderzoeken, vertrouwt hem opdrachten toe en ontvangt een verslag over alle opdrachten die worden uitgevoerd.

§ 5. De leden van de Dienst Onderzoeken worden benoemd door het Controleorgaan die hen ook kan afzetten wanneer de in artikel 152 bepaalde voorwaarden in hun hoofde niet meer vervuld zijn of wegens ernstige redenen. De leden van de Dienst Onderzoeken worden voor een mandaat met een vernieuwbare termijn van zes jaar benoemd.

§ 6. Alvorens hun ambt te aanvaarden, leggen de leden van de dienst onderzoeken in handen van de Voorzitter van het Controleorgaan de bij artikel 2 van het decreet van 30 juli 1831 voorgeschreven eed af.

Art. 244

§ 1. Op het ogenblik van hun benoeming moeten de leden van de toezichthoudende autoriteit de volgende algemene voorwaarden vervullen:

1. Belg zijn;

2. genieten van de burgerlijke en politieke rechten;

3. van onberispelijk gedrag zijn;

4. het bewijs leveren van hun deskundigheid in het domein van de bescherming van persoonsgegevens en van de politionele informatiehuishouding;

5. houder zijn van een veiligheidsmachtiging van het niveau “zeer geheim” verleend overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

6. geen functie uitoefenen in een beleidscel van een federale of regionale minister.

§ 2. Op het ogenblik van hun benoeming moeten de Voorzitter en de magistraat van het openbaar ministerie aan de volgende specifieke voorwaarden voldoen: een relevante ervaring of deskundigheid hebben van minstens tien jaar in het domein van de bescherming van persoonsgegevens en de politionele informatiehuishouding;

§ 3. Op het ogenblik van zijn benoeming moet het lid-expert aan de volgende specifieke voorwaarden voldoen:

1° tien jaar ervaring hebben als deskundige in het domein van de bescherming van persoonsgegevens en de politionele informatiehuishouding;

2° houder zijn van een diploma licenciaat of master in de rechten dat toegang verleent tot de betrekkingen van niveau A in de Rijksbesturen;

autorité sur le service d’enquête, lui confie des missions et reçoit des rapports sur toutes les missions qui sont effectuées.

§ 5. Les membres du service d’enquête de l’Organe de contrôle sont nommés par l’Organe de contrôle, lesquel peuvent également les démettre de leurs fonctions que si les conditions prévues à l’article 152 ne sont plus rencontrées ou pour motifs graves. Les membres de l’Organe de contrôle sont nommés, sur base de leurs compétences, par l’Organe de contrôle pour un mandat renouvelable de six ans.

§ 6. Avant d’entrer en fonction, les membres du service d’enquête prêtent, entre les mains du président de l’Organe de contrôle, le serment prescrit par l’article 2 du décret du 30 juillet 1831.

Art. 244

§ 1er. Au moment de leur nomination, les membres de l’autorité de contrôle doivent remplir les conditions suivantes:

1. être belge;

2. jouir des droits civils et politiques;

3. être de conduite irréprochable;

4. justifier d’une expertise en matière de protection des données à caractère personnel et en matière de gestion de l’information policière;

5. être titulaire d’une habilitation de sécurité du niveau “très secret” octroyée en vertu de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

6. ne pas exercer une fonction dans une cellule stratégique ministérielle fédérale ou régionale.

§ 2. Au moment de leur nomination, le président et le magistrat du ministère public remplissent en outre les conditions spécifiques suivantes: justifier d’une expérience pertinente ou d’une expertise d’au moins dix ans en tant qu’expert en matière de protection des données à caractère personnel et de gestion de l’information policière;

§ 3. Au moment de sa nomination, l’expert remplit, en outre, les conditions spécifiques suivantes:

1° justifier d’une expérience de dix ans en tant qu’expert en matière de protection des données à caractère personnel et de gestion de l’information policière;

2° être titulaire d’un diplôme de licencié ou de master en droit donnant accès aux emplois de niveau A dans les administrations de l’État.

§ 4. Ingeval een mandaat van lid van het Controleorgaan om welke reden ook openvalt, wordt overgegaan tot de vervanging ervan voor de nog resterende duur van het mandaat.

§ 5. Op het ogenblik van hun benoeming moeten de leden van de dienst onderzoeken de volgende algemene voorwaarden vervullen:

1° Belg zijn;

2°genieten van de burgerlijke en politieke rechten;

3° van onberispelijk gedrag zijn;

4° het bewijs leveren van hun deskundigheid in het domein van de bescherming van persoonsgegevens en van de politionele informatiehuishouding;

5° houder zijn van een veiligheidsmachtiging van het niveau “zeer geheim” verleend overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

6° geen functie uitoefenen in een beleidscel van een federale of regionale minister.

Op het ogenblik van hun benoeming moeten daarenboven, voor de personeelsleden van de politiediensten die lid zijn van de dienst onderzoeken, de volgende specifieke voorwaarden zijn vervuld:

1° ten minste tien jaar dienstanciënniteit hebben en ten minste bekleed zijn met de graad van commissaris van politie of van niveau A zijn indien het een personeelslid betreft van het administratief en logistiek kader;

2° geen eindevaluatie “onvoldoende” hebben gekregen tijdens de vijf jaar voorafgaand aan de indiening van de kandidaatstelling, noch een niet uitgewiste zware tuchtstraf hebben opgelopen;

3° een ervaring van minimum twee jaar bezitten inzake de verwerking van politionele informatie of de bescherming van persoonsgegevens.

§ 6. Op het ogenblik van hun benoeming moet de expert van de dienst onderzoeken bovendien aan de volgende specifieke voorwaarden voldoen:

1. vijf jaar ervaring hebben als deskundige in het domein van de bescherming van persoonsgegevens en de politionele informatiehuishouding;

2. houder zijn van een diploma licenciaat of master dat toegang verleent tot de betrekkingen van niveau A in de Rijksbesturen.

§ 4. En cas de vacance d’un mandat de membre de L’Organe de contrôle, et ce, quelle qu’en soit la cause, il est procédé à son remplacement pour la durée du mandat restant à courir.

§ 5. Au moment de leur nomination, les membres du service d’enquête remplissent les conditions suivantes:

1° être belge;

2° jouir des droits civils et politiques;

3° être de conduite irréprochable;

4° justifier d’une expertise en matière de protection des données à caractère personnel et en matière de gestion de l’information policière;

5° être titulaire d’une habilitation de sécurité du niveau “très secret” octroyée en vertu de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

6° ne pas exercer une fonction dans une cellule stratégique ministérielle fédérale ou régionale.

Au moment de leur nomination, les membres du personnel des services de police, qui sont membres du service d’enquête, remplissent, en outre, les conditions spécifiques suivantes:

1° compter au moins dix ans d’ancienneté de service et être au moins revêtu du grade de commissaire de police ou de niveau A lorsqu’ il s’agit d’un membre du personnel du cadre administratif et logistique;

2° ne pas avoir fait l’objet d’une évaluation finale qualifiée “insuffisante” au cours des cinq années qui ont précédées l’introduction de la candidature, ni avoir encouru une sanction disciplinaire lourde non effacée;

3° justifier d’une expérience d’au moins deux ans en matière de traitement de l’information policière ou de protection des données à caractère personnel.

§ 6. Au moment de leur nomination, les experts doivent en outre remplir les conditions spécifiques suivantes:

1. justifier d’une expérience de cinq ans en tant qu’expert en matière de protection des données à caractère personnel et de gestion de l’information policière;

2. être titulaire d’un diplôme de licencié ou master donnant accès aux emplois de niveau A dans les administrations de l’État.

Art. 245

§ 1. Het Controleorgaan stelt zijn huishoudelijk reglement op en kan zijn interne organisatie bepalen. Het huishoudelijk reglement wordt goedgekeurd door de Kamer van volksvertegenwoordigers.

De voorzitter leidt, met inachtneming van de collegialiteit, de vergaderingen van het Controleorgaan en zorgt voor het dagelijks beheer van de werkzaamheden. Hij ziet toe op de goede werking van het Controleorgaan , op de goede uitvoering van de taken ervan, alsook op de toepassing van het huishoudelijk reglement. Het voormelde huishoudelijk reglement bepaalt welk lid de taken van de voorzitter overneemt, wanneer hij afwezig of verhinderd is.

§ 2. De leden van het Controleorgaan krijgen noch vragen binnen de perken van hun bevoegdheden op directe of indirecte wijze van niemand instructies. Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarbij zij een persoonlijk of rechtstreeks belang hebben of waarbij hun bloed- of aanverwanten tot en met de vierde graad een persoonlijk of rechtstreeks belang hebben.

§ 3. De leden van het Controleorgaan en haar personeelsleden zijn niet burgerlijk aansprakelijk voor hun beslissingen, handelingen of gedragingen in de uitoefening van de wettelijke opdrachten van de toezichthoudende autoriteit behalve in geval van bedrog of zware fout.

§ 4. De leden van het Controleorgaan zijn, onverminderd hun wettelijk opdrachten en bevoegdheden, tijdens en na de uitoefening van hun respectieve mandaat, tot geheimhouding verplicht ten aanzien van de feiten, handelingen of inlichtingen waarvan zij uit hoofde van hun functie kennis hebben gehad. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Art. 246

§ 1. De leden van het Controleorgaan genieten hetzelfde statuut als de raadsheren van het Rekenhof. De wedderegeling van de raadsheren van het Rekenhof, vervat in de wet van 21 maart 1964 betreffende de wedden van de leden van het Rekenhof, zoals gewijzigd bij de wetten van 14 maart 1975 en 5 augustus 1992, is van toepassing op de leden van de toezichthoudende autoriteit. Hun reeds verworven geldelijke anciënniteit wordt in aanmerking genomen en zij hebben ook recht op de tussentijdse verhogingen in dit barema.

De leden van de dienst onderzoeken genieten een wedde zoals bepaald in barema A3 van het statuut van de ambtenaren van de Gegevensbeschermingsautoriteit opgericht door de wet van 3 december 2017 houdende oprichting van de gegevensbeschermingsautoriteit. Hun reeds verworven geldelijke anciënniteit wordt in aanmerking genomen en zij hebben ook recht op de tussentijdse verhogingen in dit barema. Zij genieten alle geldelijke voordelen die voorzien zijn in het statuut van de ambtenaren en in de organieke teksten, van de Gegevensbeschermingsautoriteit.

Art. 245

§ 1er. L'Organe de contrôle élabore son règlement d'ordre intérieur et peut définir sa propre organisation. Le règlement d'ordre intérieur est soumis à l'approbation de la Chambre des représentants.

Le président assure, dans le respect de la collégialité, la direction des réunions de L'Organe de contrôle et la gestion journalière des activités. Il veille au bon fonctionnement de l'Organe de contrôle, à la bonne exécution de ses missions ainsi qu'à l'application du règlement d'ordre intérieur. Le règlement d'ordre intérieur précité détermine quel membre assume les tâches du président en cas d'absence ou d'empêchement de ce dernier.

§ 2. Les membres de l'Organe de contrôle ne reçoivent ni cherchent dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne. Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au quatrième degré ont un intérêt personnel ou direct.

§ 3. Les membres de l'Organe de contrôle et les membres de son personnel n'encourent aucune responsabilité civile en raison de leurs décisions, actes ou comportements dans l'exercice des missions légales de l'autorité de contrôle sauf en cas de dol ou de faute lourde.

§ 4. Les membres de l'Organe de contrôle sont tenus, durant et après l'exercice de leur mandat et contrat respectifs, de garder le secret à égard des faits, actes ou renseignements dont ils ont eu connaissance en raison de leurs fonctions. Toute violation du secret professionnel est punie conformément à l'article 458 du Code pénal.

Art. 246

§ 1er. Les membres de l'Organe de contrôle jouissent d'un statut identique à celui des conseillers de la Cour des comptes. Les règles régissant le statut pécuniaire des conseillers de la Cour des comptes, contenues dans la loi du 21 mars 1964 relative aux traitements des membres de la Cour des comptes, telle qu'elle a été modifiée par les lois des 14 mars 1975 et 5 août 1992, sont applicables aux membres de l'autorité de contrôle. Leur ancienneté pécuniaire déjà acquise est prise en considération et ils ont également droit aux augmentations intercalaires dans ce barème.

Les membres du service d'enquête de l'Organe de contrôle bénéficient d'un traitement tel que défini dans le barème A3 du statut des agents de l'autorité de protection de données crée par la loi du 3 décembre 2017 tenant la création de l'Autorité de protection de données. Leur ancienneté pécuniaire déjà acquise est prise en considération et ils ont également droit aux augmentations intercalaires dans ce barème. Tous les avantages pécuniaires du statut des agents de l'autorité de protection de données s'appliquent à eux.

De leden van het Controleorgaan en de leden van de dienst onderzoeken genieten de pensioenregeling die van toepassing is op de ambtenaren van het algemeen bestuur. Deze pensioenen zijn ten laste van de Staatskas. Het mandaat van de leden van het Controleorgaan en van de leden van de dienst onderzoeken wordt inzake pensioenen gelijkgesteld met een vaste benoeming.

§ 2. De leden van de dienst onderzoeken die lid zijn van de politiediensten kunnen na de beëindiging van hun mandaat in de toezichthoudende autoriteit terugkeren naar hun korps van oorsprong in het statuut dat zij hadden op het moment van hun benoeming in de toezichthoudende autoriteit. Zij behouden niettemin tijdens hun mandaat , in de dienst of het bestuur waaruit zij afkomstig zijn, hun rechten op bevordering en op weddeverhoging. Het personeelslid van de politiediensten dat lid is van de dienst onderzoeken en dat voor een betrekking in de politiediensten geschikt wordt bevonden, heeft voorrang op alle andere kandidaten met betrekking tot de toewijzing van de betrekking, zelfs indien deze laatsten over een voorrang beschikken krachtens de wet. Deze voorrang geldt gedurende het laatste jaar van de zes jaren in dienst van de toezichthoudende autoriteit.

Onder dezelfde voorwaarden wordt een voorrangstermijn van twee jaar toegekend bij de aanvang van het tiende jaar dat men in dienst is bij het Controleorgaan.

§ 3. Aan het lid van het Controleorgaan die magistraat in de rechterlijke orde, ambtenaar van het openbaar ambt of lid van de politiediensten is wordt een verlof voor opdracht van algemeen belang verleend voor de duur van het mandaat. Zij behouden, tijdens hun mandaat in het Controleorgaan of de dienst onderzoeken, in de dienst of het bestuur waaruit zij afkomstig zijn hun rechten op bevordering en op weddeverhoging.

Art. 247

§ 1. Het Controleorgaan beschikt over een secretariaat bestaande uit een directie-assistent, een jurist en een informaticus. Deze personeelsleden genieten de hiernavolgende wedde zoals voorzien in het statuut van de ambtenaren van het federaal openbaar ambt:

— Directie-assistent: barema A1

— Jurist: barema A3

— Informaticus: barema A3

Zij worden aangeworven door het Controleorgaan die daarvoor een beroep kan doen op een deskundige in human resources.

§ 2. Het secretariaat en zijn personeelsleden staan onder het gezag van de leden van het Controleorgaan en de dagelijkse leiding van de voorzitter van de toezichthoudende autoriteit.

Les membres de l'Organe de contrôle et les membres du service d'enquête bénéficient du régime de pension applicable aux fonctionnaires de l'administration générale. Ces pensions sont à charge du Trésor public. Le mandat des membres de l'Organe de contrôle et du service enquête sont assimilés, en matière de pensions, à une nomination à titre définitif.

§ 2. Les membres du service d'enquête qui sont membres des services de police peuvent, après la fin de leur mandat, réintégrer leur corps de police d'origine, dans le statut qu'ils avaient au moment de leur nomination à l'autorité de contrôle. Ils conservent néanmoins pendant leur mandat, dans le service ou dans l'administration dont ils sont originaires, leurs droits à la promotion et aux augmentations de traitement. Le membre du personnel des services de police, membre du service d'enquête, candidat pour une fonction au sein des services de police et reconnu apte pour celle-ci, bénéficie de la priorité sur tous les autres candidats à cette fonction, même si ces derniers disposent d'une priorité accordée en vertu de la loi. Cette priorité vaut pendant la dernière année des six années prestées au sein de l'autorité de contrôle.

Une période de priorité de deux années est accordée sous les mêmes conditions à partir du début de la dixième année prestée au sein de l'Organe de contrôle.

§ 3. Un congé pour mission d'intérêt général est octroyé au magistrat de l'ordre judiciaire, au fonctionnaire de la fonction publique ou membre des services de police pour la durée de leur mandat. Ils conservent, pendant leur mandat à l'Organe de contrôle ou le service d'enquête, dans le service ou dans l'administration dont ils sont originaires, leurs droits à la promotion et aux augmentations de traitement.

Art. 247

§ 1er. L'Organe de contrôle dispose d'un secrétariat composé d'un assistant de direction, un juriste et un informaticien. Ces membres du personnel jouissent du traitement prévu dans le statut des fonctionnaires de la fonction publique fédérale, soit:

— Assistant de direction: barème A1

— Juriste: barème A3

— Informaticien: barème A3

Ils sont recrutés par l'Organede contrôle qui peut se faire assister par un expert en ressources humaines.

§ 2. Le secrétariat et les membres du personnel sont placés sous l'autorité exclusive des membres de l'Organe de contrôle et sont au quotidien sous la direction du président de l'autorité de contrôle.

HOOFDSTUK II

De opdrachten

Art. 248

§ 1. Het Controleorgaan is belast met de opdrachten voorzien in artikel 73, § 1, 1°-4°.

§ 2. Het Controleorgaan dient van advies, hetzij uit eigen beweging, hetzij op verzoek van de regering of van de Kamer van volksvertegenwoordigers, van een bestuurlijke of gerechtelijke overheid dan wel een politiedienst, omtrent iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer, zoals onder meer bepaald in afdeling 1*bis* van hoofdstuk 4 van de Wet van 5 augustus 1992 op het politieambt.

Het Controleorgaan brengt advies uit binnen zestig dagen nadat alle daartoe noodzakelijke gegevens aan de toezichthoudende autoriteit zijn medegedeeld. De adviezen van de toezichthoudende autoriteit zijn met redenen omkleed. De toezichthoudende autoriteit deelt zijn advies aan de betrokken overheid mede.

In de gevallen waar het advies van het Controleorgaanvereist is krachtens een bepaling van deze wet, wordt de termijn bedoeld in het derde lid in speciaal gemotiveerde dringende gevallen verminderd tot ten minste vijftien dagen.

§ 3. In het kader van de opdracht voorzien in artikel 73, § 1, 3°, is het Controleorgaan in het bijzonder belast met de naleving van de regels inzake de mededeling van de informatie en persoonsgegevens uit de politionele gegevensbanken, de rechtstreekse toegang tot de A.N.G. en de technische gegevensbanken en de rechtstreekse bevraging ervan, alsook van de naleving van de in artikel 44/7, derde lid, van de wet van 5 augustus 1992 op het politieambt bedoelde verplichting, voor alle leden van de politiediensten, tot voeding van deze gegevensbank.

Art. 249

Het Controleorgaan treedt ambtshalve op, op verzoek van de Gegevensbeschermingsautoriteit bedoeld in artikel 2, 1°, van de Wet van 3 december 2017 tot tot oprichting van de Gegevensbeschermingsautoriteit, van de gerechtelijke of bestuurlijke overheden, van de minister van Justitie, van de minister van Binnenlandse Zaken, van de minister die de privacy in zijn bevoegdheden heeft of van de Kamer van volksvertegenwoordigers.

Wanneer het Controleorgaan ambtshalve optreedt, brengt het de Kamer van volksvertegenwoordigers daarvan dadelijk op de hoogte.

Wanneer de controle heeft plaatsgevonden binnen een lokale politie, informeert het Controleorgaan daar de burgemeester of het politiecollege van en zendt hem zijn verslag.

CHAPITRE II

Les missions

Art. 248

§ 1er. L'Organe de contrôle est chargé des missions prévues au article 73, § 1er, 1-4°.

§ 2. L'Organe de contrôle émet soit d'initiative soit sur demande du gouvernement ou de la Chambre des représentants, d'une autorité administrative ou judiciaire ou d'un service de police, des avis sur toute question relative à la gestion de l'information policière, comme prévu notamment dans la section 1*bis* du chapitre 4 de la loi du 5 août 1992 sur la fonction de police.

L'Organe de contrôle émet ses avis soixante jours après la communication de toutes les données nécessaires à cet effet. Les avis de l'Autorité de contrôle sont motivés. L'Autorité de contrôle communique son avis à l'autorité concernée.

Dans les cas où l'avis de l'Organe de contrôle est requis par une disposition de la présente loi, le délai visé à l'alinéa 3 est réduit à quinze jours minimum dans des cas d'urgence spécialement motivés.

§ 3. Dans le cadre de la mission prévue à l'article 73, § 1er, 3°, l'Organe de contrôle est particulièrement chargé du respect de la communication des informations et données à caractère personnel de banques de données policières, de l'accès direct à la BNG et les banques de données techniques et sa consultation directe, et également du respect de l'obligation prévue dans l'article 44/7, troisième partie, de la loi sur la fonction police, pour tous les membres de services de police, d'alimenter cette banque de données.

Art. 249

L'Organe de contrôle agit d'initiative, à la demande de l'Autorité de protection des données visée à l'article 2, 1°, de la Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, des autorités judiciaires ou administratives, du ministre de la Justice ou du ministre de l'Intérieur, du ministre responsable pour la protection de la vie privée ou de la Chambre des représentants.

Lorsque l'Organe de contrôle agit d'initiative, il en informe immédiatement la Chambre des représentants.

Lorsque le contrôle a eu lieu au sein d'un corps de la police locale, l'Organe de contrôle en informe le bourgmestre ou le collège de police et lui adresse son rapport.

Wanneer de controle informatie en gegevens betreft die verband houden met de uitoefening van opdrachten van gerechtelijke politie, wordt het verslag dat dienaangaande door het Controleorgaan wordt opgesteld, ook aan de bevoegde magistraat van het openbaar ministerie toegezonden.

Art. 250

Het Controleorgaan doet verslag aan de Kamer van volksvertegenwoordigers in de volgende gevallen:

1. jaarlijks, door een algemeen activiteitenverslag dat, indien nodig, algemene conclusies en voorstellen bevat en dat de periode betreft gaande van 1 januari tot 31 december van het voorgaande jaar. Dat verslag wordt uiterlijk op 1 juni overgezonden aan de voorzitter van de Kamer van volksvertegenwoordigers alsmede aan de bevoegde ministers bedoeld in artikel 249, eerste lid;

2. telkens wanneer het dit nuttig acht of op verzoek van de Kamer van volksvertegenwoordigers, door een tussentijds activiteitenverslag met betrekking tot een welbepaald onderzoeksdossier dat, indien nodig, algemene conclusies en voorstellen kan bevatten. Dat verslag wordt overgezonden aan de voorzitter van de Kamer van volksvertegenwoordigers alsmede aan de bevoegde ministers bedoeld in artikel 249, eerste lid;

3. wanneer door de Kamer van volksvertegenwoordigers een verzoek werd geuit om op te treden;

4. wanneer het vaststelt dat, bij het verstrijken van een termijn die het redelijk acht, geen gevolg werd gegeven aan zijn besluiten of dat de genomen maatregelen niet passend of ontoereikend zijn. Die termijn mag niet minder dan zestig dagen bedragen.

Art. 251

§ 1. Het Controleorgaan gaat door middel van onderzoek naar de werking na of de inhoud van de A.N.G., de basisgegevensbanken, de bijzondere gegevensbanken en de technische gegevensbanken en de procedure voor de verwerking van de daarin bewaarde gegevens en informatie overeenkomen met het bepaalde in de artikelen 44/1 tot en met 44/11/13 van de wet van 5 augustus 1992 op het politieambt en met hun uitvoeringsmaatregelen.

§ 2. Het Controleorgaan controleert in het bijzonder de regelmatigheid van de volgende verwerkingen in de algemene nationale gegevensbank, de basisgegevensbanken, de bijzondere gegevensbanken en de technische gegevensbanken:

1. de evaluatie van de gegevens en informatie;

2. de registratie van de verzamelde gegevens en informatie;

3. de validatie van de gegevens en informatie door de daartoe bevoegde organen;

Lorsque le contrôle concerne des informations et des données à caractère personnel concernant l'exécution des missions de police judiciaire, le rapport y relatif qui est établi par l'Organe de contrôle est également transmis selon le cas au magistrat du ministère public compétent.

Art. 250

L'Organe de contrôle fait rapport à la Chambre des représentants dans les cas suivants:

1. annuellement, par un rapport général d'activités qui comprend, le cas échéant, des conclusions et des propositions d'ordre général et qui couvre la période allant du 1er janvier au 31 décembre de l'année précédente. Ce rapport est transmis au plus tard le 1er juin au président de la Chambre des représentants ainsi qu'aux ministres compétents visés à l'article 249, alinea premier;

2. chaque fois qu'il l'estime utile ou à la demande de la Chambre des représentants, par un rapport d'activités intermédiaire, qui peut comprendre, le cas échéant, des conclusions et des propositions d'ordre général relatives à un dossier d'enquête déterminé. Ce rapport est transmis au président de la Chambre des représentants ainsi qu'aux ministres compétents visés à l'article 249, alinea premier;

3. lorsque la Chambre des représentants lui a confié une mission;

4. lorsqu'au terme d'un délai qu'il estime raisonnable, il constate qu'aucune suite n'a été réservée à ses conclusions, ou que les mesures prises sont inappropriées ou insuffisantes. Ce délai ne peut être inférieur à soixante jours.

Art. 251

§ 1er. L'Organe de contrôle veille, par le biais d'enquêtes de fonctionnement, à ce que le contenu de la B.N.G., les banques de données de base, les banques de données particulières et les banques de données techniques et la procédure de traitement des données et informations qui y sont conservées, soient conformes aux règles prescrites par les articles 44/1 à 44/11/13 de la loi du 5 août 1992 sur la fonction de police et à leurs mesures d'exécution.

§ 2. L'Organe de contrôle vérifie en particulier la régularité des opérations de traitement suivantes au sein de la banque de données générale, les banques de données de base, les banques de données particulières et les banques de données techniques:

1. l'évaluation des données et informations;

2. l'enregistrement des données et informations collectées;

3. la validation des données et informations par les organes compétents à cet effet;

4. de vatting van de geregistreerde gegevens en informatie op grond van de concrete aard of van de betrouwbaarheid ervan;

5. de uitwissing en de archivering van de gegevens en informatie nadat de termijn voor bewaring ervan is verstreken.

§ 3. Het Controleorgaan controleert in het bijzonder de werkelijke aard van de volgende, door de bevoegde politieoverheden voorgeschreven functiemogelijkheden en verwerkingen:

1. de relaties tussen de categorieën van gegevens en informatie geregistreerd op het tijdstip waarop zij zijn gevat;

2. de ontvangst van de gegevens en informatie door de autoriteiten en diensten die krachtens de wet tot raadpleging gemachtigd zijn;

3. de mededeling van de gegevens en de informatie aan de wettelijk gemachtigde autoriteiten en diensten;

4. de verbinding met andere systemen voor informatieverwerking;

5. de bijzondere regels houdende vatting van de gegevens en de informatie op grond van hun adequaat, pertinent en niet overmatig karakter en de concrete betrouwbaarheid ervan.

Het Controleorgaan gaat door middel van onderzoek naar de werking na of de inhoud van de bijzondere gegevensbanken en de procedure houdende verwerking van de daarin geregistreerde en bewaarde gegevens en informatie overeenkomen met het bepaalde in de artikelen 44/1 tot 44/5 en 44/11/3 van de wet van 5 augustus 1992 op het politieambt en met hun uitvoeringsmaatregelen.

Het Controleorgaan gaat in het bijzonder na of de voorwaarden inzake de rechtstreekse toegang tot en de mededeling van de informatie en gegevens van de bijzondere gegevensbanken bepaald in het in artikel 44/11/3, § 5, van de wet van 5 augustus 1992 op het politieambt bedoelde centraal register van de bijzondere gegevensbanken nageleefd worden.

Art. 252

Het Controleorgaan:

1. maakt het brede publiek beter bekend met en verschaft meer inzicht in de risico's, de regels, de waarborgen en de rechten in verband met verwerking van persoonsgegevens door de diensten voorzien in artikel 31, 7°, a), c), d), f);

2. maakt de verwerkingsverantwoordelijken en de verwerkers beter bekend met hun wettelijke verplichtingen in verband met de verwerking van persoonsgegevens;

3. verstrekt desgevraagd informatie aan iedere betrokkene over de uitoefening van zijn rechten uit hoofde van deze wet en, in voorkomend geval, werkt daartoe samen met de toezichthoudende autoriteiten in andere lidstaten. Een verzoek

4. la saisie des données et informations enregistrées en fonction du caractère concret ou de la fiabilité de celles-ci;

5. l'effacement et l'archivage des données et informations à l'échéance de leur délai de conservation.

§ 3. L'Organe de contrôle vérifie en particulier le caractère effectif des fonctionnalités et opérations de traitement suivantes, prescrites par les autorités de police compétentes:

1. les relations entre les catégories de données et informations enregistrées au moment de leur saisie;

2. la réception des données et informations par les autorités et services légalement habilités à les consulter;

3. la communication des données et informations vers les autorités et services légalement habilités;

4. la connexion avec d'autres systèmes de traitement de l'information;

5. les règles particulières de saisie des données et informations en fonction de leur caractères adéquat, pertinent et non excessif et de la fiabilité de celles-ci.

L'Organe de contrôle veille, par le biais d'enquêtes de fonctionnement, à ce que le contenu et la procédure de traitement des données et informations enregistrées et conservées au sein des banques de données particulières soient conformes aux règles prescrites par les articles 44/1 à 44/5 et 44/11/3 de la loi du 5 août 1992 sur la fonction de police et à leurs mesures d'exécution.

L'Organe de contrôle veille, en particulier, à ce que les conditions d'accès direct aux banques de données particulières et de communication des informations et données des banques de données particulières, qui sont précisées dans le répertoire central des banques de données particulières visé à l'article 44/11/3, § 5, de la loi du 5 août 1992 sur la fonction de police, soient respectées.

Art. 252

L'Organe de contrôle:

1. favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement des données à caractère personnel effectueés par les services prévus à l'article 31, 7°, a), c), d), f);

2. encourage la sensibilisation des responsables du traitement et des sous-traitants aux obligations légales à l'égard des traitements de données à caractère personnel;

3. fournit, sur demande, à toute personne concernée, des informations sur l'exercice de ses droits découlant la présente loi, et, le cas échéant, coopère à cette fin avec les autorités de contrôle d'autres États membres. La demande d'une

van een andere toezichthoudende autoriteit wordt zonder onnodige vertraging en in ieder geval binnen één maand na de ontvangst ervan beantwoord;

4. behandelt klachten, onderzoekt de inhoud van de klacht in de mate waarin dat nodig is en stelt de klager binnen een redelijke termijn in kennis van de vooruitgang en het resultaat van het onderzoek, met name indien verder onderzoek of coördinatie met een andere toezichthoudende autoriteit nodig is. Het Controleorgaan kan besluiten geen gevolg te geven aan een klacht of een aangifte die kennelijk niet gegrond is.

Art. 253

Het Controleorgaan kan aan één of meer van haar leden, leden van de dienst enquêtes of haar personeel de bevoegdheid opdragen om de toezichthoudende autoriteit te vertegenwoordigen binnen comités of groepen waaraan het als gegevensbeschermingsautoriteit in de politiesector verplicht deelneemt of kiest aan deel te nemen.

Art. 254

Het Controleorgaan kan overgaan tot een breed openbaar onderzoek of een brede openbare raadpleging of tot een meer gericht onderzoek of een meer gerichte raadpleging van de vertegenwoordigers van de sector politie.

Art. 255

§ 1. Het Controleorgaan dient de internationale verplichtingen uit te voeren die voortvloeien uit de taken en bevoegdheden die deze wet haar toebedeelt. Deze verplichtingen kunnen de samenwerking inhouden van het Controleorgaan met enige instantie of andere gegevensbeschermingsautoriteit van een andere staat door gebruik te maken van de bevoegdheden die haar zijn toegekend krachtens de van toepassing zijnde wetgeving.

Deze samenwerking kan onder meer betrekking hebben op:

1. de invoering van deskundigheidspools;

2. de uitwisseling van informatie;

3. de wederzijdse bijstand in het kader van controlemaatregelen;

4. het delen van personele en financiële middelen;

De samenwerking kan, inter alia, aan de hand van samenwerkingsakkoorden worden geconcretiseerd.

§ 2. Het Controleorgaan is gemachtigd om in dit verband bepaalde van haar leden, leden van de dienst enquêtes of personeelsleden aan te wijzen als vertegenwoordigers bij internationale autoriteiten.

autre autorité de contrôle reçoit réponse le plus vite possible et en tout cas dans les trente jours après la réception de la demande;

4. traite des réclamations, enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire. L'organe de Contrôle peut décider de ne pas donner suite à une plainte ou à une réclamation qui est manifestement non fondée.

Art. 253

L'Organe de contrôle peut déléguer à un ou plusieurs de ses membres, membres du service d'enquête ou son personnel le pouvoir de représenter l'Autorité de contrôle au sein de comités ou groupes auxquels elle est tenue ou choisit de participer en tant que Autorité de protection des données dans le secteur police.

Art. 254

L'Organe de contrôle peut procéder à une enquête ou à une large consultation publique ou à une enquête ou consultation plus ciblée des représentants du secteur police.

Art. 255

§ 1er. L'Organe de contrôle exécute les obligations internationales liées aux tâches et compétences attribuées par la présente loi. Ces obligations peuvent consister dans la collaboration de l'Organe de contrôle avec toute instance ou autre autorité de protection des données d'un autre État en faisant usage des pouvoirs qui lui sont conférés soit en vertu de la législation en vigueur.

Cette collaboration peut, inter alia, porter sur:

1. la création de pôles d'expertise;

2. l'échange d'informations;

3. l'assistance mutuelle dans le cadre de mesures de contrôle;

4. le partage de ressources humaines et financières.

La collaboration peut se concrétiser, inter alia, par le biais d'accords de coopération.

§ 2. L'Organe de contrôle est habilité à désigner à cet égard certains de ses membres, membres du service d'enquête ou membres du personnel en tant que représentants auprès d'autorités internationales.

HOOFDSTUK III

Bevoegdheden van het Controleorgaan, van haar leden en van de leden van de dienst onderzoeken

Art. 256

§ 1. Het Controleorgaan, zijn leden of de leden van de dienst onderzoeken hebben een onbeperkt recht op toegang tot alle informatie en gegevens verwerkt door de diensten voorzien in artikel 26, 7°, a), c), d), f), en in het bijzonder de politiediensten overeenkomstig artikel 44/1 tot en met 44/11/13 van de wet van 5 augustus 1992 op het politieambt, hierin begrepen deze die bewaard worden in de A.N.G., in de basisgegevensbanken, in de bijzondere gegevensbanken, in de technische gegevensbanken en in de internationale gegevensbanken die door de Belgische politiediensten worden gevoed.

De politiediensten zenden uit eigen beweging aan het Controleorgaan reglementen en interne richtlijnen over, betreffende de verwerking van persoonsgegevens en de politionele informatie die zij noodzakelijk achten voor het vervullen van hun opdracht. Het Controleorgaan en de dienst onderzoeken zijn ertoe gerechtigd alle teksten die zij noodzakelijk achten voor het vervullen van hun opdracht te laten overleggen.

Het Controleorgaan, zijn leden of de leden van de dienst onderzoeken kunnen een onderzoek ter plaatse doen. Te dien einde, beschikken zij over een onbeperkt recht op toegang tot de lokalen waarin en gedurende de tijd dat de in het eerste lid bedoelde informatie en gegevens verwerkt worden.

§ 2. Zij kunnen in deze plaatsen alle voorwerpen, documenten en gegevens van een informaticasysteem die nuttig zijn voor hun onderzoek in beslag nemen, behalve indien ze betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek.

Indien de korpschef of zijn plaatsvervanger van oordeel is dat door het beslag een persoon fysiek gevaar kan lopen, wordt de kwestie voorgelegd aan de voorzitter van het Controleorgaan of de magistraat die hem vervangt die uitspraak doet. De in beslag genomen voorwerpen en documenten worden vermeld in een daartoe speciaal bij te houden register.

§ 3. De leden van het Controleorgaan en de dienst onderzoeken doen, waar ook, alle nuttige vaststellingen.

Het Controleorgaan of zijn leden kunnen, voor het uitoefenen van haar opdrachten, de bijstand vorderen van de openbare macht.

§ 4. Het Controleorgaan, zijn leden of de leden van de dienst onderzoeken kunnen dwingende antwoordtermijnen opleggen aan de leden van de federale of van de lokale politie, waaraan ze vragen richten in de uitvoering van hun opdrachten.

CHAPITRE III

Compétences de l'Organe de contrôle, ses membres et des membres du service d'enquête

Art. 256

§ 1er. L'Organe de contrôle, ses membres et les membres du service d'enquête ont un accès illimité à toutes informations ou données traitées par les services visés par l'article 31, 7°, a), c), d), f), et en particulier, les services de police conformément aux articles 44/1 jusqu'au 44/11/13 de la loi du 5 août 1992 sur la fonction de police, en ce compris celles contenues dans la B.N.G., dans les banques de données de base, dans les banques de données particulières, les banques de données techniques et dans les bases de données internationales alimentées par les services de police belges.

Les services de police transmettent d'initiative à l'Organe de contrôle les règlements et les directives internes relatifs au traitement des données à caractère personnel et de l'information policière nécessaires à l'accomplissement de ses missions. L'Organe de contrôle et le service d'enquête ont le droit de se faire communiquer tous les textes qu'ils estiment nécessaires à l'accomplissement de leur mission.

L'Organe de contrôle, ses membres et les membres du service d'enquête peuvent effectuer des enquêtes sur place. A cette fin, les membres de l'Autorité de contrôle ont un droit d'accès illimité aux locaux dans lesquels et pendant le temps où les informations et données visées à l'alinéa premier sont traitées.

§ 2. Ils peuvent saisir dans ces lieux tous les objets, documents et données d'un système informatique utiles pour leur enquête, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours.

Si le chef de corps ou son remplaçant estime que la saisie risque de faire courir un danger physique à une personne, la question est soumise au président de l'Organe de contrôle ou le magistrat qui le remplace qui statue. Les objets et documents saisis sont mentionnés dans un registre spécial tenu à cet effet.

§ 3. Les membres de l'Organe de contrôle et les membres du service d'enquête font, en tout lieu, les constatations qui s'imposent.

L'Organe de contrôle ou ses membres peuvent, dans l'exercice de leurs missions, requérir l'assistance de la force publique.

§ 4. L'Organe de contrôle, ses membres et les membres du service d'enquête peuvent imposer des délais de réponse contraignants aux membres de la police fédérale ou de la police locale auxquels ils adressent des questions dans l'exécution de leurs missions.

§ 5. Het Controleorgaan heeft, voor de uitoefening van het toezicht dat door deze wet wordt georganiseerd, toegang tot de gegevens van art. 3, eerste lid, 1° tot 6°, 9°, 9°/1 en tweede lid, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.

Met het oog op de uitoefening van dit toezicht mag zij gebruikmaken van het rijksregisternummer.

Art. 257

§ 1. Onverminderd de wettelijke bepalingen betreffende de onschendbaarheid en het voorrecht van rechtsmacht, kunnen de leden van het Controleorgaan en van de dienst onderzoeken elke persoon van wie zij het verhoor noodzakelijk achten, uitnodigen om hem te horen. De leden of gewezen leden van de politiediensten zijn gehouden gevolg te geven aan elke schriftelijke oproeping.

De leden of gewezen leden van de politiediensten mogen verklaringen afleggen over feiten die worden gedekt door het beroepsgeheim.

§ 2. De voorzitter van het Controleorgaan de leden of gewezen leden van de politiediensten dagvaarden door tussenkomst van een gerechtsdeurwaarder. Deze leden of gewezen leden moeten getuigen na de eed te hebben afgelegd die is bepaald in artikel 934, tweede lid, van het Gerechtelijk Wetboek.

De leden of gewezen leden van de politiediensten zijn verplicht geheimen waarvan zij kennis dragen, aan het Controleorgaan bekend te maken, behalve indien ze betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek.

Als het lid of gewezen lid van de politiedienst van oordeel is dat hij het geheim waarvan hij kennis draagt, moet bewaren omdat een persoon door de bekendmaking ervan fysiek gevaar zou kunnen lopen, wordt de kwestie voorgelegd aan de voorzitter van het Controleorgaan of de magistraat die hem vervangt, die uitspraak doet.

§ 3. Het Controleorgaan kan de medewerking van deskundigen en tolken vorderen. Zij leggen de eed af volgens de formule als gebruikt voor het Hof van Assisen. De hen verschuldigde vergoedingen worden uitgekeerd overeenkomstig het tarief van de gerechtskosten in strafzaken.

§ 4. Artikel 9 van de wet van 3 mei 1880 op het parlementair onderzoek is van toepassing op de leden of gewezen leden van de politiediensten die als getuige worden gehoord of gedagvaard door het Controleorgaan en op de deskundigen en tolken die worden gevorderd.

De processen-verbaal die de inbreuken begaan voor het Controleorgaan vaststellen, worden opgesteld door een lid van de toezichthoudende autoriteit of een lid van de dienst onderzoeken en worden overgezonden aan de procureur des Konings in wiens ambtsgebied ze zijn begaan.

§ 5. L'Organe de contrôle a accès, pour l'exercice du contrôle organisé par la présente loi, aux données de l'art. 3, premier alinéa, 1° à 6°, 9°, 9°/1 et second alinéa de la loi du 8 aout 1983 instituant un registre national des personnes physiques.

En vue de l'exercice de ce contrôle, elle peut utiliser le numéro de registre national.

Art. 257

§ 1er. Sans préjudice des dispositions légales relatives aux immunités et aux privilèges de juridiction, les membres de l'Organe de contrôle et les membres du service d'enquête peuvent inviter, afin de l'entendre, toute personne dont ils estiment l'audition nécessaire. Les membres ou anciens membres des services de police sont tenus de donner suite à toute convocation écrite.

Les membres ou anciens membres des services de police peuvent déposer sur des faits couverts par le secret professionnel.

§ 2. Le président de l'Organe de contrôle peut faire citer des membres ou anciens membres des services de police par huissier de justice. Les membres ou anciens membres des services de police sont tenus de déposer après avoir prêté le serment prévu à l'article 934, alinéa 2 du Code judiciaire.

Les membres ou anciens membres des services de police sont tenus de révéler à l'Organe de contrôle les secrets dont ils sont dépositaires, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours.

Si le membre ou l'ancien membre du service de police estime devoir garder le secret dont il est dépositaire parce que sa révélation risquerait de faire courir un danger physique à une personne, la question est soumise au président de l'Organe de contrôle ou le magistrat qui le remplace qui statue.

§ 3. L'Orane de contrôle peut requérir la collaboration d'interprètes et d'experts. Ils prêtent serment d'après la formule utilisée devant la Cour d'Assises. Les indemnités qui leurs sont dues sont réglées conformément au tarif des frais en matières pénales.

§ 4. L'article 9 de la loi du 3 mai 1880 sur les enquêtes parlementaires est d'application aux membres ou anciens membres des services de police qui sont entendus ou cités par l'Organe de contrôle à titre de témoins et aux experts et interprètes qui sont requis.

Les procès-verbaux constatant les infractions commises devant l'Organe de contrôle sont établis par un membre de l'Autorité de contrôle ou un membre du service d'enquête et sont transmis au procureur du Roi dans le ressort duquel elles sont commises.

De leden of gewezen leden van de politiediensten die weigeren te getuigen voor het Controleorgaan en de deskundigen en de tolken die weigeren hun medewerking te verlenen, worden gestraft met een gevangenisstraf van één maand tot twee jaar en een geldboete van 100 tot 1 000 euro of met één van die straffen alleen.

Art. 258

Onverminderd artikel 44/1 van de wet van 5 augustus 1992 op het politieambt, zijn alle diensten van de Staat, met inbegrip van de parketten en de griffies van de hoven en van alle rechtscolleges, de provincies, de gemeenten, de verenigingen waartoe zij behoren, de overheidsinstellingen die ervan afhangen, gehouden aan het Controleorgaan, haar leden of de leden van de dienst onderzoeken, op haar of hun verzoek, alle inlichtingen te geven die laatstgenoemden nuttig acht voor het toezicht op de naleving van de wetgeving waarmee zij belast zijn, alsmede gelijk welke informatiedragers ter inzage over te leggen en kopieën ervan te verstrekken onder gelijk welke vorm.

Indien deze inlichtingen deel uitmaken van een lopend opsporings- of gerechtelijk onderzoek worden ze slechts mits voorafgaande goedkeuring van het bevoegde openbaar ministerie verstrekt.

Art. 259

§ 1. Uiterlijk één maand na ontvangst van het verzoek brengt het Controleorgaan ten behoeve van de bevoegde overheid, een omstandig advies uit over de aanwijzing, de bevordering, de benoeming of de mutatie van de personeelseden van de politiediensten belast met het beheer van de A.N.G.

§ 2. Binnen de maand na ontvangst van het verzoek brengt Het Controleorgaan ten behoeve van de bevoegde minister, een omstandig advies uit over de wenselijkheid van een tuchtrechtelijke procedure ten aanzien van het hoofd van de dienst die de A.N.G. beheert, of ten aanzien van zijn adjunct.

HOOFDSTUK IV

Financiering

Art. 260

Voor de werking van het Controleorgaan wordt een dotatie uitgetrokken op de algemene uitgavenbegroting van het Rijk.

Het Controleorgaan stelt jaarlijks een ontwerp van begroting op voor zijn werking. Bijgestaan door het Rekenhof, onderzoekt de Kamer van volksvertegenwoordigers de gedetailleerde begrotingsvoorstellen van de toezichthoudende autoriteit, keurt ze goed en controleert de uitvoering van zijn begroting, onderzoekt en keurt daarenboven de gedetailleerde rekeningen goed.

Les membres ou anciens membres des services de police qui refusent de témoigner devant l'Organe de contrôle et les experts et interprètes qui refusent leur collaboration sont punis d'un emprisonnement de un mois à deux ans et une amende de 100 euros à 1 000 euros ou une de ces peines.

Art. 258

Sans préjudice de l'article 44/1 de la loi du 5 août 1992 sur la fonction de police, tous les services de l'État, y compris les parquets et les greffes des cours et de toutes les juridictions, des provinces, des communes, des associations dont elles font partie, des institutions publiques qui en dépendent, sont tenus, vis-à-vis de l'Organe de contrôle, ses membres ou les membres du service d'enquête et à leur demande, de leur fournir tous les renseignements que ces derniers estiment utiles au contrôle du respect de la législation dont ils sont chargés, ainsi que de leur produire, pour en prendre connaissance, tous les supports d'information et de leur en fournir des copies sous n'importe quelle forme.

Si ces renseignements font partie d'une enquête judiciaire en cours, ils ne seront transmis que moyennant l'autorisation préalable du ministère public compétent.

Art. 259

§ 1er. L'Organe de contrôle émet, à l'adresse de l'autorité compétente, dans les deux semaines de la réception de la demande, un avis circonstancié sur la désignation, la promotion, la nomination ou la mutation des membres du personnel des services de police chargés de la gestion de la B.N.G.

§ 2. L'Organe de contrôle émet, à l'adresse du ministre compétent, dans les deux semaines à dater de la réception de la demande, un avis circonstancié sur l'opportunité d'entamer une procédure disciplinaire à l'égard du chef du service gérant la B.N.G. ou de l'adjoint de celui-ci.

CHAPITRE IV

Financement

Art. 260

Une dotation est inscrite au budget général des dépenses de l'État pour financer le fonctionnement de l'Organe de contrôle.

L'Organe de contrôle établit annuellement un projet de budget pour son fonctionnement. Assistée par la Cour des comptes, la Chambre des représentants examine les propositions budgétaires détaillées de l'Autorité de contrôle, elle les approuve et contrôle l'exécution de son budget, elle examine et approuve en outre les comptes détaillés.

Het Controleorgaan voegt bij haar jaarlijks begrotingsvoorstel een strategisch plan.

Het Controleorgaan hanteert voor zijn begroting en rekeningen een schema dat vergelijkbaar is met het schema van de begroting en rekeningen van de Kamer van volksvertegenwoordigers.

TITEL 8

SLOTBEPALINGEN

Art. 261

In geval van verwerking van persoonsgegevens voor meerdere doeleinden, door eenzelfde verwerkingsverantwoordelijke of verwerker, of bedoeld in verschillende regelgevingen, zijn deze verschillende regelgevingen tegelijkertijd van toepassing. In geval van conflict tussen sommige van hun bepalingen, worden de regels van deze wet toegepast.

HOOFDSTUK I

Wijzigingsbepalingen

Art. 262

De bestaande wetten, koninklijke besluiten en elke andere reglementering die verwijzen naar de opgeheven bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, worden geacht te verwijzen naar deze wet.

Art. 263

In de artikelen 3, 31 en 35 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, worden de woorden “Algemene Dienst Inlichtingen en Veiligheid” vervangen door de woorden “Algemene Dienst Inlichting en Veiligheid”.

Art. 264

In de Franse tekst van het opschrift van Hoofdstuk III en de afdelingen 1 en 2 van hetzelfde hoofdstuk, in het opschrift van Hoofdstuk IV evenals in de artikelen 2, 3, 2°, 28, 33, 38, 39, 40, 48, 53 en 65 van dezelfde wet worden de woorden “services de renseignements” vervangen door de woorden “services de renseignement”.

In de Franse tekst van de artikelen 28, 40, 41, 48, 50, 61 en 67 worden de woorden “*service de renseignements*” vervangen door de woorden “*service de renseignement*”.

L’Organe de contrôle joint à sa proposition de budget annuel un plan stratégique.

Pour son budget et ses comptes, l’Organe de contrôle utilise un schéma budgétaire et des comptes comparable à celui qui est utilisé par la Chambre des représentants.

TITRE 8

DISPOSITIONS FINALES

Art. 261

En cas de traitement de données à caractère personnel pour plusieurs finalités par un même responsable du traitement ou sous-traitant, ou visées par différentes législations, ces différentes législations s’appliquent de manière simultanée. En cas de conflit entre certaines de leurs dispositions, les règles de la présente loi sont appliquées.

CHAPITRE I^ER

Dispositions modificatives

Art. 262

Les lois, les arrêtés royaux et toute autre règlementation existants qui font référence aux dispositions abrogées de la loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel sont présumées faire référence à la présente loi.

Art. 263

Aux articles 3, 31 et 35 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l’Organe de coordination pour l’analyse de la menace, les mots “Service général du renseignement et de la sécurité” sont remplacés par les mots “Service Général du Renseignement et de la Sécurité”.

Art. 264

Dans l’intitulé du Chapitre III et des sections 1 et 2 de ce même chapitre, dans l’intitulé du Chapitre IV ainsi qu’aux articles 2, 3, 2°, 28, 33, 38, 39, 40, 48, 53 et 65 de la même loi, les mots “services de renseignements” sont remplacés par les mots “services de renseignement”.

Aux articles 28, 40, 41, 48, 50, 61 et 67, les mots “service de renseignements” sont remplacés par les mots “service de renseignement”.

In de Franse tekst van de artikelen 41 en 44 worden de woorden "*des services de police ou de renseignements*" vervangen door de woorden "*des services de police ou de renseignement*".

In de Franse tekst van het artikel 44 worden de woorden "*d'un service de police ou de renseignements*" vervangen door de woorden "*d'un service de police ou de renseignement*".

In het artikel 53 van de Franse tekst worden de woorden "*des missions de renseignements*" vervangen door de woorden "*des missions de renseignement*".

Art. 265

In artikel 3 van dezelfde wet, worden een 7°, en een 8°, ingevoegd, luidende:

"7° "de gegevensbeschermingswet": de wet van xx/xx/2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

8° "een gegevensbeschermingsautoriteit": een autoriteit die toezicht houdt op verwerkingen van persoonsgegevens."

Art. 266

In artikel 28 van dezelfde wet, derde lid, 5°, worden de volgende wijzigingen aangebracht:

1. de woorden "de inlichtingen," worden ingevoegd tussen de woorden "domein van" en "het strafrecht";

2. de woorden "het recht van de bescherming van persoonsgegevens" worden ingevoegd tussen de woorden "het publiek recht," en de woorden "of technieken inzake management".

In hetzelfde artikel wordt het vierde lid aangevuld met de woorden ", noch van een andere gegevensbeschermingsautoriteit, noch van de de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten".

Art. 267

Artikel 29, eerste lid, 8°, van dezelfde wet wordt aangevuld met de woorden ", veiligheidsattesten en veiligheidsadviezen".

Art. 268

In artikel 31 van dezelfde wet worden de woorden ", alsook voor de organisatie en het bestuur van de Veiligheid van de Staat wanneer die organisatie en dat bestuur een

Aux articles 41 et 44, les mots "des services de police ou de renseignements" sont remplacés par les mots "des services de police ou de renseignement".

A l'article 44, les mots "d'un service de police ou de renseignements" sont remplacés par les mots "d'un service de police ou de renseignement".

A l'article 53, les mots "des missions de renseignements" sont remplacés par les mots "des missions de renseignement".

Art. 265

A l'article 3 de la même loi, sont insérés un 7° et un 8° rédigés comme suit:

"7° "la loi protection des données": la loi du xx/xx/2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel;

8° "une autorité de protection des données": une autorité de contrôle des traitements de données à caractère personnel."

Art. 266

Dans l'article 28 de la même loi, alinéa 3, 5°, les modifications suivantes sont apportées:

1. mots "du renseignement," sont insérés entre les mots "le domaine" et les mots "du droit pénal";

2. les mots "du droit de la protection des données à caractère personnel," sont insérés entre les mots "du droit public," et les mots "ou de techniques de gestion".

Dans ce même article, l'alinéa 4 est complété par les mots ", ni d'une autre autorité de protection des données, ni de la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité".

Art. 267

A l'article 29 de la même loi, le 8° est complété par les mots ", attestations et avis de sécurité".

Art. 268

A l'article 31 de la même loi, les mots ", ainsi que l'organisation et l'administration de la Sûreté de l'État lorsque celles-ci ont une influence directe sur l'exécution des missions de

rechtstreekse invloed hebben op de uitvoering van de opdrachten inzake de handhaving van de openbare orde en de persoonsbescherming" opgeheven.

Art. 269

In artikel 32, eerste lid van dezelfde wet, wordt het woord "of" vervangen door",".

Het eerste lid van hetzelfde artikel wordt aangevuld met de woorden "of op vraag van een andere gegevensbeschermingsautoriteit".

In het tweede lid van hetzelfde artikel worden de woorden "in het kader van de activiteiten en methodes bedoeld in artikel 33, eerste lid" ingevoegd tussen de woorden "beweging optreedt" en ", brengt het".

Art. 270

In artikel 33 van dezelfde wet wordt tussen het eerste en het tweede lid een lid ingevoegd, luidende:

"Het Vast Comité I onderzoekt eveneens de verwerkingen van persoonsgegevens door de inlichtingendiensten en hun verwerkers."

In het vierde lid, dat het vijfde lid wordt, van hetzelfde artikel worden de volgende wijzigingen aangebracht:

1. het woord "of" wordt vervangen door ",";

2. de woorden "of de verwerkingen van persoonsgegevens" worden ingevoegd tussen de woorden "de werkwijzen" en de woorden" die de".

In het zevende lid, dat het achtste lid wordt, van hetzelfde artikel worden de woorden "Het Vast Comité I mag enkel"vervangen door de woorden "Behalve als de wet zijn advies oplegt, mag het Vast Comité I enkel".

Art. 271

In artikel 34 van dezelfde wet wordt tussen het eerste en het tweede lid een lid ingevoegd, luidende:

"Het Vast Comité I behandelt eveneens de verzoeken met betrekking tot de verwerkingen van persoonsgegevens door de inlichtingendiensten en hun verwerkers."

In het derde lid, dat het vierde lid wordt, van hetzelfde artikel, worden de volgende wijzigingen aangebracht:

1. het woord "of" wordt vervangen door ",";

2. de woorden "of een verzoek" worden ingevoegd tussen de woorden "een aangifte" en de woorden "die kennelijk".

maintien de l'ordre public et de protection des personnes" sont supprimés.

Art. 269

A l'article 32, alinéa premier de la même loi, le mot "ou" est remplacé par ",".

L'alinéa premier de ce même article est complété par les mots "ou à la demande d'une autre autorité de protection des données".

A l'alinéa 2 de ce même article, les mots "dans le cadre des activités et méthodes visées à l'article 33, alinéa 1er" sont insérés entre les mots "d'initiative" et les mots ", il en informe".

Art. 270

Dans l'article 33 de la même loi, il est inséré après le premier alinéa un nouvel alinéa rédigé comme suit:

"Le Comité permanent R enquête également sur les traitements de données à caractère personnel par les services de renseignement et leurs sous-traitants."

A l'alinéa 5 (ancien alinéa 4) de ce même article, les modifications suivantes sont apportées:

1. le mot "ou" est remplacé par ",";

2. les mots "ou les traitements des données à caractère personnel" sont insérés entre les mots "les méthodes" et les mots "qui seraient".

A l'alinéa 7, qui devient l'alinéa 8, de ce même article, les mots "Le Comité permanent R peut seulement" sont remplacés par "Sauf si la loi impose son avis, le Comité permanent R peut seulement" sont insérés au début de l'alinéa.

Art. 271

Dans l'article 34 de la même loi, il est inséré après le premier alinéa un nouvel alinéa rédigé comme suit:

"Le Comité permanent R traite également des requêtes en matière de traitements des données à caractère personnel par les services de renseignement et leurs sous-traitants."

A l'alinéa 4 (ancien alinéa 3) du même article, les modifications suivantes sont apportées:

1. les mots "ou à" sont remplacés par ",";

2. les mots "ou une requête" sont insérés entre le mot "dénonciation" et les mots "manifestement".

In het vierde lid, dat het vijfde lid wordt, van hetzelfde artikel worden de volgende wijzigingen aangebracht:

1. het woord “of” wordt vervangen door “,”;

2. de woorden “of een verzoek” worden ingevoegd tussen de woorden “klacht, aangifte” en de woorden “en om het”;

3. de woorden “of het verzoek” worden ingevoegd tussen de woorden “die de klacht” en de woorden “heeft ingediend”.

Het vijfde lid, dat het zesde lid wordt, wordt aangevuld met de woorden:

“behalve voor onderzoeken met betrekking tot de verwerking van persoonsgegevens door de inlichtingendiensten en hun verwerkers, waar het Vast Comité I enkel antwoordt dat de nodige verificaties werden verricht”.

Art. 272

Artikel 35 van dezelfde wet wordt aangevuld met een paragraaf 3, luidende:

“§ 3. Het Vast Comité I brengt jaarlijks verslag uit bij de Kamer van volksvertegenwoordigers omtrent de gegeven adviezen in zijn hoedanigheid van gegevensbeschermingsautoriteit, omtrent de onderzoeken die werden uitgevoerd en de maatregelen die werden genomen in dezelfde hoedanigheid alsook omtrent haar samenwerking met de andere gegevensbeschermingsautoriteiten.

Een kopij van dit verslag wordt eveneens gericht aan de bevoegde ministers, alsook aan de Veiligheid van de Staat en aan de Algemene Dienst Inlichting en Veiligheid, die over de mogelijkheid beschikken om het Vast Comité I attent te maken op hun bemerkingen.”

Art. 273

In artikel 38, tweede lid, van dezelfde wet wordt het woord “Vast” ingevoegd tussen de woorden “het” en het woord “Comité”.

Art. 274

In artikel 40, tweede lid, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1. de woorden “de klachten en aangiften” worden vervangen door de woorden “de klachten, aangiften en verzoeken”;

2. in de Franse tekst de woorden “*ce d’appui*” worden opgeheven;

3. de woorden “of handelingen” worden vervangen door de woorden “, handelingen of verwerkingen van persoonsgegevens”.

A l’alinéa 5 (ancien alinéa 4) du même article, les modifications suivantes sont apportées:

1. les mots “ou à” sont remplacés par “,”;

2. les mots “ou une requête” sont insérés entre le mot “dénonciation” et les mots “et de clôturer”;

3. le mot “ou” est remplacé par “,” et les mots “ou introduit la requête” complètent l’alinéa.

L’alinéa 6 (ancien alinéa 5) du même article est complété par les mots:

“, sauf en matière d’enquêtes portant sur le traitement des données à caractère personnel par les services de renseignement et leurs sous-traitants où le Comité permanent R répond uniquement que les vérifications nécessaires ont été effectuées”.

Art. 272

L’article 35 de la même loi est complété par un paragraphe 3 rédigé comme suit:

“§ 3. Le Comité permanent R fait rapport annuellement à la Chambre des représentants sur les avis rendus en sa qualité d’autorité de protection des données, sur les enquêtes effectuées et mesures prises en cette même qualité ainsi que sur sa collaboration avec les autres autorités de protection des données.

Copie de ce rapport est également adressé aux ministres compétents, ainsi qu’à la Sûreté de l’État et au Service Général du Renseignement et de la Sécurité, qui ont la faculté d’attirer l’attention du Comité permanent R sur leurs observations.”

Art. 273

A l’article 38 alinéa 2 de la même loi, le mot “permanent” est inséré entre les mots “le Comité” et le mot “R”.

Art. 274

Dans l’article 40, alinéa 2, de la même loi, les modifications suivantes sont apportées:

1. les mots “les plaintes et dénonciations” sont remplacés par les mots” les plaintes, dénonciations et requêtes”;

2. les mots “ce d’appui” sont supprimés;

3. les mots “ou des actions” sont remplacés par les mots “, des actions ou des traitements de données à caractère personnel”.

Art. 275

In artikel 44 van dezelfde wet, wordt het eerste lid aangevuld met de woorden:

"of in het verwerken van persoonsgegevens of in de informatieveiligheid."

Art. 276

Het tweede lid van artikel 45 van dezelfde wet wordt aangevuld met de woorden ", veiligheidsattesten en veiligheidsadviezen".

Art. 277

In artikel 46 van dezelfde wet worden de woorden "buiten de gevallen bepaald in artikel 13/1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en die bepaald in de artikelen 239 en 240 van de gegevensbeschermingswet" ingevoegd tussen de woorden "een wanbedrijf" en de woorden ", maakt hij".

Dit artikel wordt aangevuld met een lid, luidende:

"Wanneer een lid van de Dienst Enquêtes I kennis heeft van een wanbedrijf zoals bedoeld in de artikelen 239 en 240 van de gegevensbeschermingswet, informeert hij zo snel mogelijk het Vast Comité I hierover. Deze laatste verzekert de opvolging volgens de nadere regels bepaald in artikel 54 van deze wet."

Art. 278

In hoofdstuk III van dezelfde wet, wordt een afdeling 4 ingevoegd, die de artikelen 51/1 tot 51/4 bevat, luidende: "Afdeling 4. Bevoegdheden van het Vast Comité I als gegevensbeschermingsautoriteit".

Art. 279

In de nieuwe afdeling van hoofdstuk III van dezelfde wet, worden de artikelen 51/1 tot 51/4 ingevoegd, luidende:

"Art. 51/1. In zijn hoedanigheid van gegevensbeschermingsautoriteit voor de gegevens verwerkt door de inlichtingendiensten en hun verwerkers aangewezen door artikel 97 van de gegevensbeschermingswet, treedt het Vast Comité I ofwel op uit eigen beweging, ofwel op verzoek van een andere gegevensbeschermingsautoriteit, ofwel op verzoek van elke betrokkene.

Art. 51/2. Om ontvankelijk te zijn, moet het verzoek geschreven, gedateerd, ondertekend en gemotiveerd zijn en de identiteit van de betrokkene rechtvaardigen.

Art. 51/3. Het Vast Comité I beslist over de opvolging die het aan het dossier geeft en heeft de bevoegdheid om:

Art. 275

A l'article 44 de la même loi, l'alinéa premier est complété par les mots:

"dans le traitement des données à caractère personnel ou dans la sécurité de l'information."

Art. 276

L'alinéa 2 de l'article 45 de la même loi est complété par les mots ", attestations et avis de sécurité".

Art. 277

A l'article 46 de la même loi, les mots "en dehors des cas prévus à l'article 13/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et de ceux visés aux articles 239 et 240 de la loi protection des données" sont insérés entre les mots "d'un délit" et les mots ", il en dresse".

Ce même article est complété par un aliéna rédigé comme suit:

"Lorsqu'un membre du Service d'enquêtes R a connaissance d'un délit visé aux articles 239 et 240 de la loi protection des données, il en informe le Comité permanent R dans les meilleurs délais. Celui-ci assure le suivi selon les modalités fixées à l'article 54 de la présente loi."

Art. 278

Dans le chapitre III de la même loi, est insérée une section 4, comprenant les articles 51/1 à 51/4, intitulée: "Section 4. Pouvoirs du Comité permanent R en tant qu'autorité de protection des données".

Art. 279

Dans la nouvelle section 4 du chapitre III de la même loi, sont insérés les articles 51/1 à 51/4 rédigés comme suit:

"Art. 51/1. En sa qualité d'autorité de protection des données traitées par les services de renseignement et leurs sous-traitants désignée par l'article 97 de la loi protection des données, le Comité permanent R agit soit d'initiative, soit à la demande d'une autre autorité de protection de données, soit à la requête de toute personne concernée.

Art. 51/2. Pour être recevable, la requête doit être écrite, datée, signée, motivée et justifier de l'identité de la personne concernée.

Art. 51/3. Le Comité permanent R décide du suivi qu'il donne au dossier et a le pouvoir de:

1. te besluiten dat de verwerking is uitgevoerd in overeenstemming met de bepalingen van de reglementering inzake de verwerking van persoonsgegevens;

2. de betrokken inlichtingendienst of diens verwerker te waarschuwen dat een voorgenomen verwerking van persoonsgegevens de reglementering inzake de verwerking van persoonsgegevens kan schenden;

3. de betrokken inlichtingendienst of diens verwerker te berispen wanneer een verwerking geresulteerd heeft in een schending van een bepaling van de reglementering inzake de verwerking van persoonsgegevens;

4. de betrokken inlichtingendienst of diens verwerker te gelasten om een verwerking in overeenstemming te brengen met de bepalingen van de reglementering inzake de verwerking van persoonsgegevens, in voorkomend geval, op een nader bepaalde manier en binnen een nader bepaalde termijn;

5. een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, op te leggen;

6. het rectificeren of wissen van persoonsgegevens te gelasten;

7. het dossier over te maken aan de procureur des Konings van Brussel, die het informeert van het gevolg dat aan het dossier gegeven wordt.

Art. 51/4. Het Vast Comité I informeert de betrokken inlichtingendienst van de uitgevoerde onderzoeken naar de verwerking van persoonsgegevens van diens verwerkers en hun resultaten.

Wanneer het er kennis van neemt, informeert het Vast Comité I eveneens de betrokken inlichtingendienst van de schendingen van de reglementering inzake de verwerking van persoonsgegevens door andere verwerkingsverantwoordelijken."

Art. 280

In artikel 4, § 2, laatste alinea van de wet van 3 december 2017 tot oprichting van de gegevensbeschermingsautoriteit, worden de volgende woorden ingevoegd na de woorden "gestructureerd op twee niveaus":

"en de Dienst Enquêtes van het Vast Comité van toezicht op de politiediensten zoals bedoeld in artikel 16 van de wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse van 18 juli 1991 en de Algemene Inspectie van de federale politie en van de lokale politie zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten."

1. conclure que le traitement est effectué en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel;

2. avertir le service de renseignement concerné ou son sous-traitant du fait qu'un traitement envisagé de données à caractère personnel est susceptible de violer la règlementation relative aux traitements des données à caractère personnel;

3. rappeler à l'ordre le service de renseignement concerné ou son sous-traitant lorsqu'un traitement a entraîné une violation d'une disposition de la règlementation relative aux traitements des données à caractère personnel;

4. ordonner au service de renseignement concerné ou à son sous-traitant de mettre un traitement en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel, le cas échéant, de manière spécifique et dans un délai déterminé;

5. imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;

6. ordonner la rectification ou l'effacement de données à caractère personnel;

7. transmettre le dossier au parquet du procureur du Roi de Bruxelles, qui l'informe des suites données au dossier.

Art. 51/4. Le Comité permanent R informe le service de renseignement concerné des enquêtes effectuées sur le traitement de données à caractère personnel par ses sous-traitants et de leurs résultats.

Lorsqu'il en prend connaissance, le Comité permanent R informe également le service de renseignement concerné des violations de la règlementation relative aux traitements de ses données à caractère personnel par d'autres responsables du traitement."

Art. 280

Dans l'article 4, § 2, dernier alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, les mots suivants sont insérés après les mots "structuré à deux niveaux":

"et le service d'enquête du Comité permanent des services de police, tel que visé à l'article 16 de la loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace du 18 juillet 1991 et l'Inspection générale de la police fédérale et de la police locale, tel que visé à l'article 2 de la loi du 15 mai 2007 sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police."

Art. 281

In dezelfde wet wordt een artikel 54/1 ingevoegd, luidende:

"Art. 54/1. § 1. Met het oog op de consequente toepassing van de nationale, Europese en internationale regelgeving inzake de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens werken de Gegevensbeschermingsautoriteit en de bevoegde toezichthoudende autoriteiten waarnaar wordt verwezen in de titels 2 en 3 van de wet van XXX betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens nauw samen, voor wat betreft de behandeling van klachten, adviezen en aanbevelingen die raken aan de bevoegdheden van twee of meerdere toezichthoudende autoriteiten.

Onafgezien van bijzondere wetten dient de gezamenlijke behandeling van klachten, adviezen en aanbevelingen te gebeuren aan de hand van het "één loket principe" dat zal worden waargenomen door de Gegevensbeschermingsautoriteit.

§ 2. Teneinde de in de eerste paragraaf beoogde samenwerking te verwezenlijken sluiten de toezichthoudende autoriteiten een samenwerkingsprotocol af."

HOOFDSTUK II

Opheffingsbepalingen

Art. 282

De wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens, gewijzigd bij de wet van 11 december 1998, wordt opgeheven.

Het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens wordt opgeheven.

Het koninklijk besluit van 17 december 2003 tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van bepaalde sectorale comités opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer wordt opgeheven.

HOOFDSTUK III

Inwerkingtreding en overgangsbepalingen

Art. 283

Deze wet treedt in werking op 25 mei 2018, met uitzondering van titel 2 en de artikelen …, die op 6 mei 2018 in werking treden.

Art. 281

Il est inséré dans la même loi un article 54/1 rédigé comme suit:

"Art. 54/1. § 1er. En vue de l'application cohérente des réglementations nationales, européennes et internationales relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, l'Autorité de protection des données et les autorités de contrôle compétentes visées aux titres 2 et 3 de la loi du XXX relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel, collaborent ensemble, en ce qui concerne le traitement des plaintes, les conseils et les recommandations qui affectent les pouvoirs de deux ou plusieurs autorités de contrôle.

Nonobstant les lois particulières, le traitement conjoint des plaintes, des conseils et des recommandations doit se faire sur la base du "principe du guichet unique" qui sera assumé par l'Autorité de protection des données.

§ 2. Afin de réaliser la coopération visée au premier paragraphe, les autorités de contrôle concluent un protocole de coopération."

CHAPITRE II

Dispositions abrogatoires

Art. 282

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, modifiée par la loi du 11 décembre 1998, est abrogée.

L'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel est abrogé.

L'arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée est abrogé.

CHAPITRE III

Entrée en vigueur et dispositions transitoires

Art. 283

La présente loi entre en vigueur le 25 mai 2018, à l'exception du titre 2, et des articles … qui entrent en vigueur le 6 mai 2018.

Art. 284

De wettelijke verplichtingen zoals vastgelegd in de Verordening en in deze wet doen geen afbreuk aan de rechtsgeldigheid van de handelingen die de verwerkingsverantwoordelijke of de verwerker heeft verricht vóór de inwerkingtreding van voormelde verplichtingen.

Art. 285

De internationale overeenkomsten betreffende de doorgifte van persoonsgegevens aan derde landen of internationale organisaties die zijn gesloten vóór 6 mei 2016 en die in overeenstemming zijn met de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens en het vóór die datum van toepassing zijnde Unierecht, blijven van kracht totdat zij worden gewijzigd, vervangen of herroepen.

Art. 286

In afwijking van artikel 283, worden de geautomatiseerde verwerkingssystemen zoals bedoeld in artikel 46 die vóór 6 mei 2016 door de bevoegde autoriteiten bedoeld in titel 2 van deze wet werden opgezet, uiterlijk op 6 mei 2023 in overeenstemming gebracht met artikel 58, eerste paragraaf.

Art. 287

§ 1. In afwijking van artikel 283, blijven de leden van het Controleorgaan die de eed hebben afgelegd, daadwerkelijk in functie zijn op het moment van de inwerkingtreding van deze wet en die benoemd werden overeenkomstig artikel 36*ter*/1 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals ingevoegd bij artikel 42 van de wet van 18 maart 2014 betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering, van rechtswege aangesteld overeenkomstig de paragrafen 2, 3 en 4 als lid van het Controleorgaan of als lid van de dienst onderzoeken in de zin van deze Wet tot op het einde van hun sedert 1 september 2015 lopende mandaat van zes jaar. Zij worden vanaf de inwerkingtreding van deze wet, van rechtswege onderworpen aan de artikelen 283 en 284 van deze wet.

§ 2. De huidige leden worden van rechtswege aangesteld als lid van het controleorgaan of van de dienst onderzoeken overeenkomstig de nieuwe benoemingsvereisten zoals voorzien door deze wet en overeenkomstig de paragrafen 3 en 4.

§ 3. De Voorzitter van het Controleorgaan blijft van rechtswege aangesteld als voorzitter van het Controleorgaan in de zin van deze wet. Het lid van de Commissie voor de bescherming van de persoonlijke levenssfeer wordt van rechtswege aangesteld als het lid van het Controleorgaan afkomstig uit

Art. 284

Les obligations légales telles que prévues dans le Règlement et la présente loi ne portent pas préjudice à la légalité des traitements de données à caractère personnel réalisés par le responsable du traitement ou le sous-traitant avant l'entrée en vigueur desdites obligations.

Art. 285

Les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales conclus avant le 6 mai 2016 et qui respectent la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le droit de l'Union tel qu'il est applicable avant cette date restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.

Art. 286

Par dérogation à l'article 283, les systèmes de traitement automatisé tels que visés à l'article 46 installés avant le 6 mai 2016 par les autorités compétentes visées au titre 2 de la présente loi sont mis en conformité avec l'article 58, paragraphe premier, au plus tard le 6 mai 2023.

Art. 287

§ 1er. Par dérogation à l'article 283, les membres de l'Organe de contrôle qui ont prêté serment, qui sont effectivement en fonction au moment d'entrée en vigueur de cette loi et qui ont été nommés conformément à l'article 36*ter*/1 de la loi du 8 décembre 1992 de la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, comme introduit par l'article 42 de la loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, restent de par la loi désignés conformément aux paragraphes 2, 3 et 4 comme membres de l'Organe de contrôle ou comme membre du service d'enquête dans le sens de cette loi jusqu'à la fin de leur mandat de six ans courant depuis le 1 septembre 2015. Au moment de l'entrée en vigueur de cette loi, ils sont soumis d'office aux articles 283 et 284 de cette loi.

§ 2. Les membres actuels sont désignés de par la loi comme membre de l'Organe de Contrôle ou du service d'enquêtes en fonction des nouvelles exigences de nomination établies dans la présente loi et conformément au paragraph 3 et 4.

§ 3. Le président de l'Organe de Contrôle reste de par la loi désigné comme président de l'Organe de Contrôle au sens de la présente loi. Le membre de la Commission de la protection de la vie privée est désigné de par la loi comme membre de l'Organe de Contrôle venant du ministère public au sens de

het openbaar ministerie in de zin van deze wet en de huidige nederlandstalige expert-jurist wordt van rechtswege in de hoedanigheid van expert in de zin van deze wet aangesteld als lid van het Controleorgaan.

§ 4. De drie huidige andere leden, waarvan twee afkomstig uit de politiediensten en één franstalige expert niet-jurist worden van rechtswege aangesteld als lid van de dienst onderzoeken in de zin van deze wet in hun respectievelijke hoedanigheid van lid van de politiediensten en van expert.

§ 5. In afwijking van artikel 243, § 1, kan het lid van het Controleorgaan, dat benoemd werd in zijn hoedanigheid van lid van de Commissie voor de bescherming van de persoonlijke levenssfeer, opgeheven door artikel 114 van de wet van 3 december 2017 tot oprichting van de gegevensbeschermingsautoriteit, vanaf de inwerkingtreding van deze wet tot het einde van zijn sedert 1 september 2015 lopende mandaat, zijn functie hetzij voltijds, hetzij deeltijds blijven uitoefenen. Bij een deeltijdse uitoefening van de functie geniet hij van een wedde gelijk aan 20 % van de wedde voorzien voor de andere leden zoals vermeld in artikel 283.

la présente loi et l'actuelle expert juriste Néérlandophone est désigné de par la loi dans la capacité d'expert au sens de la présente loi comme membre de l'Organe de Contrôle.

§ 4. Les trois autres membres actuels, dont deux issues des services de police et un expert non juriste Francophone sont de par la loi désigné comme membre du service d'enquête au sens de la présente loi dans leurs capacité respective de membre des services de police et expert.

§ 5. Par dérogation à l'article 243, § 1er, le membre de l'Organe de contrôle qui a été nommé en sa qualité de membre de la Commission de la protection de la vie privée, abrogé par l'article 114 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données peut, à partir de l'entrée en vigueur de cette loi jusqu'à la fin de son mandat qui court depuis le 1er septembre 2015, continuer à excercer la fonction soit à temps plein soit à temps partiel. Lorsqu'il exerce sa fonction à temps partiel, il bénéficie d'un traitement correspondant à 20 % du traitement fixé pour les autres membres par l'article 283.

RIA formulier - v2 - oct. 2014

Regelgevingsimpactanalyse

RiA-AiR

:: Vul het formulier bij voorkeur online in ria-air.fed.be
:: Contacteer de helpdesk indien nodig ria-air@premier.fed.be
:: Raadpleeg de handleiding, de FAQ, enz. www.vereenvoudiging.be

Beschrijvende fiche

Auteur .a.

Bevoegd regeringslid	Philippe de Backer_
Contactpersoon beleidscel (Naam, E-mail, Tel. Nr.)	Veerle Van Crombrugge; veerle.vancrombrugge@debacker.fed.be; 0476 55 86 02_ _ _
Overheidsdienst	FOD Justitie_
Contactpersoon overheidsdienst (Naam, E-mail, Tel. Nr.)	Ketsia Malengreaux, ketsia.malengreaux@just.fgov.be, 02 542 74 61_ _ _

Ontwerp .b.

Titel van het ontwerp van regelgeving	Voorontwerp van wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens_ _
Korte beschrijving van het ontwerp van regelgeving met vermelding van de oorsprong (verdrag, richtlijn, samenwerkingsakkoord, actualiteit, …), de beoogde doelen van uitvoering.	Dit voorontwerp van wet viseert de tenuitvoerlegging van de open clausules van de Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, evenals de omzetting van de Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. In feite is de Verordening nr 2016/679 onmiddellijk van toepassing op de verwerkingen van persoonsgegevens. Deze Verordening bevat een aantal bepalingen waar een zekere handelingsmarge is verleend aan de lidstaten, wat meebrengt dat een aantal bepalingen moeten genomen worden in het interne recht. De Richtlijn 2016/680 moet volledig worden omgezet in intern recht en betreft een gelimiteerd toepassingsgebied m.n. de sectoren van politie en justitie voor hun opdrachten van preventie, vaststelling van strafrechtelijke inbreuken, onderzoeken en vervolgingen van strafbare feiten of de tenuitvoerlegging van straffen.
Impactanalyses reeds uitgevoerd	☐ Ja ☒ Nee — Indien ja, gelieve een kopie bij te voegen of de referentie van het document te vermelden: _ _

Raadpleging over het ontwerp van regelgeving .c.

Verplichte, facultatieve of informele raadplegingen:	Verplichte consultatie van de Commissie ter bescherming van de Persoonlijke Levenssfeer, facultatieve consultatie van het college van procureurs generaal, Vereniging van Vlaamse Steden en Gemeenten, Union des Villes et Communes de Wallonie, Association Ville et Communes de Bruxelles.Orde van Advocaten (OVB)

Bronnen gebruikt om de impactanalyse uit te voeren .d.

Statistieken, referentiedocumenten, organisaties en contactpersonen:	_/ _

Datum van beëindiging van de impactanalyse .e.

29 januari 2018_

RIA formulier - v2 - oct. 2014

Welke impact heeft het ontwerp van regelgeving op deze 21 thema's?

>

Een ontwerp van regelgeving zal meestal slechts impact hebben op enkele thema's.

Een niet-exhaustieve lijst van trefwoorden is gegeven om de inschatting van elk thema te vergemakkelijken.

Indien er een **positieve en/of negatieve impact** is, leg deze uit (gebruik indien nodig trefwoorden) en vermeld welke maatregelen worden genomen om de eventuele negatieve effecten te verlichten/te compenseren.

Voor de thema's 3, 10, 11 en 21, worden meer gedetailleerde vragen gesteld.

Raadpleeg de handleiding of contacteer de helpdesk ria-air@premier.fed.be indien u vragen heeft.

Kansarmoedebestrijding .1.

Menswaardig minimuminkomen, toegang tot kwaliteitsvolle diensten, schuldenoverlast, risico op armoede of sociale uitsluiting (ook bij minderjarigen), ongeletterdheid, digitale kloof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Gelijke Kansen en sociale cohesie .2.

Non-discriminatie, gelijke behandeling, toegang tot goederen en diensten, toegang tot informatie, tot onderwijs en tot opleiding, loonkloof, effectiviteit van burgerlijke, politieke en sociale rechten (in het bijzonder voor kwetsbare bevolkingsgroepen, kinderen, ouderen, personen met een handicap en minderheden).

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Gelijkheid van vrouwen en mannen .3.

Toegang van vrouwen en mannen tot bestaansmiddelen: inkomen, werk, verantwoordelijkheden, gezondheid/zorg/welzijn, veiligheid, opleiding/kennis/vorming, mobiliteit, tijd, vrije tijd, etc.

Uitoefening door vrouwen en mannen van hun fundamentele rechten: burgerlijke, sociale en politieke rechten.

1. Op welke personen heeft het ontwerp (rechtstreeks of onrechtstreeks) een impact en wat is de naar geslacht uitgesplitste samenstelling van deze groep(en) van personen?

   Indien geen enkele persoon betrokken is, leg uit waarom.

   Alle personen van wie de persoonsgegevens verwerkt worden zijn geviseerd door het hervormingsontwerp. Geen verschil gelinkt aan het geslacht. De rechten worden gegarandeerd voor alle betrokken personen_ _

↓ Indien er personen betrokken zijn, beantwoord dan vraag 2.

2. Identificeer de eventuele verschillen in de respectieve situatie van vrouwen en mannen binnen de materie waarop het ontwerp van regelgeving betrekking heeft.

   _ _

↓ Indien er verschillen zijn, beantwoord dan vragen 3 en 4.

3. Beperken bepaalde van deze verschillen de toegang tot bestaansmiddelen of de uitoefening van fundamentele rechten van vrouwen of mannen (problematische verschillen)? [J/N] > Leg uit

   _ _

4. Identificeer de positieve en negatieve impact van het ontwerp op de gelijkheid van vrouwen en mannen, rekening houdend met de voorgaande antwoorden?

   _ _

↓ Indien er een negatieve impact is, beantwoord dan vraag 5.

5. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

   _ _

Gezondheid .4.

Toegang tot kwaliteitsvolle gezondheidszorg, efficiëntie van het zorgaanbod, levensverwachting in goede gezondheid, behandelingen van chronische ziekten (bloedvatenziekten, kankers, diabetes en chronische ademhalingsziekten), gezondheidsdeterminanten (sociaaleconomisch niveau, voeding, verontreiniging), levenskwaliteit.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Werkgelegenheid .5.

Toegang tot de arbeidsmarkt, kwaliteitsvolle banen, werkloosheid, zwartwerk, arbeids- en ontslagomstandigheden, loopbaan, arbeidstijd, welzijn op het werk, arbeidsongevallen, beroepsziekten, evenwicht privé- en beroepsleven, gepaste verloning, mogelijkheid tot beroepsopleiding, collectieve arbeidsverhoudingen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Consumptie- en productiepatronen .6.

Prijsstabiliteit of -voorzienbaarheid, inlichting en bescherming van de consumenten, doeltreffend gebruik van hulpbronnen, evaluatie en integratie van (sociale- en milieu-) externaliteiten gedurende de hele levenscyclus van de producten en diensten, beheerpatronen van organisaties.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Economische ontwikkeling .7.

Oprichting van bedrijven, productie van goederen en diensten, arbeidsproductiviteit en productiviteit van hulpbronnen/grondstoffen, competitiviteitsfactoren, toegang tot de markt en tot het beroep, markttransparantie, toegang tot overheidsopdrachten, internationale handels- en financiële relaties, balans import/export, ondergrondse economie, bevoorradingszekerheid van zowel energiebronnen als minerale en organische hulpbronnen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Investeringen .8.

Investeringen in fysiek (machines, voertuigen, infrastructuren), technologisch, intellectueel (software, onderzoek en ontwikkeling) en menselijk kapitaal, nettoinvesteringscijfer in procent van het bbp.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Onderzoek en ontwikkeling .9.

Mogelijkheden betreffende onderzoek en ontwikkeling, innovatie door de invoering en de verspreiding van nieuwe productiemethodes, nieuwe ondernemingspraktijken of nieuwe producten en diensten, onderzoeks- en ontwikkelingsuitgaven.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Kmo's .10.

Impact op de ontwikkeling van de kmo's.

1. Welke ondernemingen zijn rechtstreeks of onrechtstreeks betrokken?
   Beschrijf de sector(en), het aantal ondernemingen, het % kmo's (< 50 werknemers), waaronder het % micro-ondernemingen (< 10 werknemers).
   Indien geen enkele onderneming betrokken is, leg uit waarom.

   Alle betrokken sectoren. Elk bedrijf is betrokken bij de bescherming van de persoonsgegevens_ _

↓ Indien er kmo's betrokken zijn, beantwoord dan vraag 2.

2. Identificeer de positieve en negatieve impact van het ontwerp op de kmo's.
   N.B. De impact op de administratieve lasten moet bij thema 11 gedetailleerd worden.

   De Gegevensbeschermingsautoriteit heeft onder meer de opdracht om de verantwoordelijken voor de verwerking van persoonsgegevens te begeleiden bij deze verwerkingen zodat ze handelen conform de Verordening (impact positief). In het geval de verantwoordelijke voor de verwerking niet handelt conform de Verordening is aan de toezichthoudende autoriteit een sanctiebevoegdheid verleend, onder andere voor het opleggen van administratieve boetes (impact negatief)

↓ Indien er een negatieve impact is, beantwoord dan vragen 3 tot 5.

3. Is deze impact verhoudingsgewijs zwaarder voor de kmo's dan voor de grote ondernemingen? [J/N] > Leg uit

   Dit hangt af van het beleid dat gevoerd wordt door de Gegevensbeschermingsautoriteit, die trouwens een onafhankelijke instantie is. Niettemin, bij het opleggen van corrigerende maatregelen of sancties kan de Gegevensbeschermingsautoriteit rekening houden met de specifieke situatie van de KMO's._ _

4. Staat deze impact in verhouding tot het beoogde doel? [J/N] > Leg uit

   Ja, de bescherming van fundamentele rechten_ _

5. Welke maatregelen worden genomen om deze negatieve impact te verlichten / te compenseren?

   Dit hangt ook af van het gevoerde beleid door de Gegevensbeschermingsautoriteit, die trouwens een onafhankelijke instantie is. Niettemin, bij de uitoefening van de controletaken voorziet de Verordening 2016/679 in de mogelijkheid voor de Gegevensbeschermingsautoriteit om rekening te houden met de specificiteit van de KMO's. (bijvoorbeeld de overweging 132: De toezichthoudende autoriteiten dienen bij voorlichtingsactiviteiten voor het publiek specifieke maatregelen te nemen voor de verwerkingsverantwoordelijken en de verwerkers, waaronder kleine, middelgrote en micro-ondernemingen, alsmede natuurlijke personen, met name in het onderwijs"

Administratieve lasten .11.

Verlaging van de formaliteiten en administratieve verplichtingen die direct of indirect verbonden zijn met de uitvoering, de naleving en/of de instandhouding van een recht, een verbod of een verplichting.

↓ Indien burgers (zie thema 3) en/of ondernemingen (zie thema 10) betrokken zijn, beantwoord dan volgende vragen.

1. Identificeer, per betrokken doelgroep, de nodige formaliteiten en verplichtingen voor de toepassing van de regelgeving.
   Indien er geen enkele formaliteiten of verplichtingen zijn, leg uit waarom.

   a. Verplichting in bepaalde gevallen (verhoogd risico ten opzichte van een betrokken persoon) om een impactanalyse te maken op het val van gegevensbescherming, en eventueel een voorafgaand advies te vragen aan de controle autoriteit.*

   b. Schrapping van de aangifteplicht en vervangen door het bijhouden van een register. Voor de publieke sector wordt hiervoor een tool ter beschikking gesteld**

↓ Indien er formaliteiten en/of verplichtingen zijn in de huidige* regelgeving, beantwoord dan vragen 2a tot 4a.

↓ Indien er formaliteiten en/of verplichtingen zijn in het ontwerp van regelgeving**, beantwoord dan vragen 2b tot 4b.

2. Welke documenten en informatie moet elke betrokken doelgroep verschaffen?

   a. Bepalen van welke verwerkingen, nieuwe verwerking, wettelijke basis en welke

   b. Screening en en analyse van de categorieën van verwerking: finaliteiten, wettelijke basis, categorieën van gegevens, categorieën van ontvangers, algemeen

technische en organisatorische maatregelen genomen zijn om de risico's te beperken_ _*	technische en organisationele maatregelen, coördinaten van de onderaannemers**

3. Hoe worden deze documenten en informatie, per betrokken doelgroep, ingezameld?

   a. Screening, analyse b. Screening, analyse

4. Welke is de periodiciteit van de formaliteiten en verplichtingen, per betrokken doelgroep?

   a. Bij elke nieuwe gegevensverwerking b. Bij elke nieuwe gegevensverwerking

5. Welke maatregelen worden genomen om de eventuele negatieve impact te verlichten / te compenseren?

   De controle autoriteit kan een lijst van verwerkingen bepalen die noodzakelijk een impactanalyse moeten ondergaan of een lijst van verwerkingen die geen impactanalyse noodzaken. Binnen de WP29, die de 29 controle-autoriteiten verenigt, worden Richtlijnen uitgewerkt.

Energie .12.

Energiemix (koolstofarm, hernieuwbaar, fossiel), gebruik van biomassa (hout, biobrandstoffen), energie-efficiëntie, energieverbruik van de industrie, de dienstensector, de transportsector en de huishoudens, bevoorradingszekerheid, toegang tot energiediensten en -goederen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Mobiliteit .13.

Transportvolume (aantal afgelegde kilometers en aantal voertuigen), aanbod van gemeenschappelijk personenvervoer, aanbod van wegen, sporen en zee- en binnenvaart voor goederenvervoer, verdeling van de vervoerswijzen (modal shift), veiligheid, verkeersdichtheid.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Voeding .14.

Toegang tot veilige voeding (kwaliteitscontrole), gezonde en voedzame voeding, verspilling, eerlijke handel.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Klimaatverandering .15.

Uitstoot van broeikasgassen, aanpassingsvermogen aan de gevolgen van de klimaatverandering, veerkracht, energie overgang, hernieuwbare energiebronnen, rationeel energiegebruik, energie-efficiëntie, energieprestaties van gebouwen, winnen van koolstof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Natuurlijke hulpbronnen .16.

Efficiënt beheer van de hulpbronnen, recyclage, hergebruik, waterkwaliteit en -consumptie (oppervlakte- en grondwater, zeeën en oceanen), bodemkwaliteit en -gebruik (verontreiniging, organisch stofgehalte, erosie, drooglegging, overstromingen, verdichting, fragmentatie), ontbossing.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Buiten- en binnenlucht .17.

Luchtkwaliteit (met inbegrip van de binnenlucht), uitstoot van verontreinigende stoffen (chemische of biologische agentia: methaan, koolwaterstoffen, oplosmiddelen, SOX, NOX, NH3), fijn stof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Biodiversiteit .18.

Graad van biodiversiteit, stand van de ecosystemen (herstelling, behoud, valorisatie, beschermde zones), verandering en fragmentatie van de habitatten, biotechnologieën, uitvindingsoctrooien in het domein van de biologie, gebruik van genetische hulpbronnen, diensten die de ecosystemen leveren (water- en luchtzuivering, enz.), gedomesticeerde of gecultiveerde soorten, invasieve uitheemse soorten, bedreigde soorten.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Hinder .19.

Geluids-, geur- of visuele hinder, trillingen, ioniserende, niet-ioniserende en elektromagnetische stralingen, lichtoverlast.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Overheid .20.

Democratische werking van de organen voor overleg en beraadslaging, dienstverlening aan gebruikers, klachten, beroep, protestbewegingen, wijze van uitvoering, overheidsinvesteringen.

☒ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☐ Geen impact

Controle door de bevoegde toezichthoudende autoriteiten op de naleving door de publieke sector van de privacy-wetgeving. De nieuw opgerichte Gegevensbeschermingsautoriteit adviseert de overheidsdiensten over de concrete persoonsgegevensverwerkingen maar ook over de wetontwerpen en uitvoeringsbesluiten met een impact op de bescherming van persoonsgegevens.

Beleidscoherentie ten gunste van ontwikkeling .21.

Inachtneming van de onbedoelde neveneffecten van de Belgische beleidsmaatregelen op de belangen van de ontwikkelingslanden.

1. Identificeer de eventuele rechtstreekse of onrechtstreekse impact van het ontwerp op de ontwikkelingslanden op het vlak van:

   - o voedselveiligheid
   - o gezondheid en toegang tot geneesmiddelen
   - o waardig werk
   - o lokale en internationale handel
   - o inkomens en mobilisering van lokale middelen (taxatie)
   - o mobiliteit van personen
   - o leefmilieu en klimaatverandering (mechanismen voor schone ontwikkeling)
   - o vrede en veiligheid

   Indien er geen enkelen ontwikkelingsland betrokken is, leg uit waarom.

   Er is geen grote impact op de ontwikkelingslanden. De persoonsgegevensstromen naar de ontwikkelingslanden zullen een minimale bescherming moeten respecteren. De overeenkomsten voor justitiële en politionele samenwerking moeten in de toekomst ook rekening houden met de nieuwe reglementering

↓ Indien er een positieve en/of negatieve impact is, beantwoord dan vraag 2.

2. Verduidelijk de impact per regionale groepen of economische categorieën (eventueel landen oplijsten). Zie bijlage

_ _

↓ Indien er een negatieve impact is, beantwoord dan vraag 3.

3. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

_ _

Formulaire AIR - v2 – oct. 2014

Analyse d'impact de la réglementation

RiA-AiR

:: Remplissez de préférence le formulaire en ligne ria-air.fed.be
:: Contactez le Helpdesk si nécessaire ria-air@premier.fed.be
:: Consultez le manuel, les FAQ, etc. www.simplification.be

Fiche signalétique

Auteur .a.

Membre du Gouvernement compétent	Philippe De Backer_
Contact cellule stratégique (nom, email, tél.)	Veerle Van Crombrugge, Veerle.Vancrombrugge@Debacker.fed.be, 0476 55 86 02
Administration compétente	SPF Justice
Contact administration (nom, email, tél.)	Ketsia Malengreaux, ketsia.malengreaux@just.fgov.be, 02 542 74 61

Projet .b.

Titre du projet de réglementation	Avant-projet de loi relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel	
Description succincte du projet de réglementation en mentionnant l'origine réglementaire (traités, directive, accord de coopération, actualité, ...), les objectifs poursuivis et la mise en œuvre.	**L'avant-projet de loi que je vous présente pour avis vise à mettre en œuvre le règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46 / CE (annexe 5), ainsi que transposer la directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.En effet, le règlement (CE) n ° 2016/679 prévoit un régime directement applicable pour l'ensemble des traitements de données à caractère personnel. Ce règlement contient toutefois des dispositions dans lesquelles une certaine marge de manœuvre est accordée aux Etats membres. Il en résulte que certaines dispositions doivent être prises en droit interne. Pour ce qui concerne la directive 2016/680, celle-ci doit être transposée en droit interne et concerne un champ d'application plus limité qui sont les secteurs de la police et justice pour leurs missions de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Mais un régime entier est prévu ici.**	
Analyses d'impact déjà réalisées	☐ Oui ☒ Non	Si oui, veuillez joindre une copie ou indiquer la référence du document : _ _

Consultations sur le projet de réglementation .c.

Consultations obligatoires, facultatives ou informelles :	Consultation obligatoire de la Commission de la protection de la vie privée, consultation facultative de l'Ordre des avocats (FR-NL), consultation du Collège des procureurs généraux,

Sources utilisées pour effectuer l'analyse d'impact .d.

Statistiques, documents de référence, organisations et personnes de référence :	/

Date de finalisation de l'analyse d'impact .e.

29 janvier 2018

Quel est l'impact du projet de réglementation sur ces 21 thèmes ?

>

Un projet de réglementation aura généralement des impacts sur un nombre limité de thèmes.

Une liste non-exhaustive de mots-clés est présentée pour faciliter l'appréciation de chaque thème.

S'il y a des **impacts positifs et / ou négatifs, expliquez-les** (sur base des mots-clés si nécessaire) et indiquez les mesures prises pour alléger / compenser les éventuels impacts négatifs.

Pour les thèmes 3, 10, 11 et 21, des questions plus approfondies sont posées.

Consultez le manuel ou contactez le helpdesk ria-air@premier.fed.be pour toute question.

Lutte contre la pauvreté .1.

Revenu minimum conforme à la dignité humaine, accès à des services de qualité, surendettement, risque de pauvreté ou d'exclusion sociale (y compris chez les mineurs), illettrisme, fracture numérique.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Égalité des chances et cohésion sociale .2.

Non-discrimination, égalité de traitement, accès aux biens et services, accès à l'information, à l'éducation et à la formation, écart de revenu, effectivité des droits civils, politiques et sociaux (en particulier pour les populations fragilisées, les enfants, les personnes âgées, les personnes handicapées et les minorités).

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Égalité entre les femmes et les hommes .3.

Accès des femmes et des hommes aux ressources : revenus, travail, responsabilités, santé/soins/bien-être, sécurité, éducation/savoir/formation, mobilité, temps, loisirs, etc.

Exercice des droits fondamentaux par les femmes et les hommes : droits civils, sociaux et politiques.

1. Quelles personnes sont directement et indirectement concernées par le projet et quelle est la composition sexuée de ce(s) groupe(s) de personnes ?

   Si aucune personne n'est concernée, expliquez pourquoi.

   Toute personne dont les données à caratère personnel sont traitées sont visées par le projet de réforme. Il n'y a pas de différence liée au sexe. Les droits sont garantis pour toute personne concernée.

↓ Si des personnes sont concernées, répondez à la question 2.

2. Identifiez les éventuelles différences entre la situation respective des femmes et des hommes dans la matière relative au projet de réglementation.

↓ S'il existe des différences, répondez aux questions 3 et 4.

3. Certaines de ces différences limitent-elles l'accès aux ressources ou l'exercice des droits fondamentaux des femmes ou des hommes (différences problématiques) ? [O/N] > expliquez

   _ _

4. Compte tenu des réponses aux questions précédentes, identifiez les impacts positifs et négatifs du projet sur l'égalité des femmes et les hommes ?

↓ S'il y a des impacts négatifs, répondez à la question 5.

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

   _ _

Santé .4.

Accès aux soins de santé de qualité, efficacité de l'offre de soins, espérance de vie en bonne santé, traitements des maladies chroniques (maladies cardiovasculaires, cancers, diabètes et maladies respiratoires chroniques), déterminants de la santé (niveau socio-économique, alimentation, pollution), qualité de la vie.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Emploi .5.

Accès au marché de l'emploi, emplois de qualité, chômage, travail au noir, conditions de travail et de licenciement, carrière, temps de travail, bien-être au travail, accidents de travail, maladies professionnelles, équilibre vie privée - vie professionnelle, rémunération convenable, possibilités de formation professionnelle, relations collectives de travail.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Modes de consommation et production .6.

Stabilité/prévisibilité des prix, information et protection du consommateur, utilisation efficace des ressources, évaluation et intégration des externalités (environnementales et sociales) tout au long du cycle de vie des produits et services, modes de gestion des organisations.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Développement économique .7.

Création d'entreprises, production de biens et de services, productivité du travail et des ressources/matières premières, facteurs de compétitivité, accès au marché et à la profession, transparence du marché, accès aux marchés publics, relations commerciales et financières internationales, balance des importations/exportations, économie souterraine, sécurité d'approvisionnement des ressources énergétiques, minérales et organiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Investissements .8.

Investissements en capital physique (machines, véhicules, infrastructures), technologique, intellectuel (logiciel, recherche et développement) et humain, niveau d'investissement net en pourcentage du PIB.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Recherche et développement .9.

Opportunités de recherche et développement, innovation par l'introduction et la diffusion de nouveaux modes de production, de nouvelles pratiques d'entreprises ou de nouveaux produits et services, dépenses de recherche et de développement.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

PME .10.

Impact sur le développement des PME.

1. Quelles entreprises sont directement et indirectement concernées par le projet ?
   Détaillez le(s) secteur(s), le nombre d'entreprises, le % de PME (< 50 travailleurs) dont le % de micro-entreprise (< 10 travailleurs).
   Si aucune entreprise n'est concernée, expliquez pourquoi.

   Tous les secteurs sont concernés. Toute entreprise est concernée par la protection des données à caractère personnelle

↓ Si des PME sont concernées, répondez à la question 2.

2. Identifiez les impacts positifs et négatifs du projet sur les PME.
   N.B. les impacts sur les charges administratives doivent être détaillés au thème 11

   L'Autorité de protection des données a entre autres la mission d'accompagner les responsables du traitement de données à caractère personnel dans ce traitement pour qu'ils procèdent conformément à la réglementation (impact positif). Dans le cas où les responsables du traitement ne procèdent pas conformément à la réglementation l'Autorité de protection des données est dotée du pouvoir de sanction, entre autres en imposant des amendes administratives (impact négatif).

↓ S'il y a un impact négatif, répondez aux questions 3 à 5.

3. Ces impacts sont-ils proportionnellement plus lourds sur les PME que sur les grandes entreprises ? [O/N] > expliquez

   Cela dépend de la politique menée par l'Autorité de protection des données qui est d'ailleurs une autorité totalement indépendante. Néanmoins, dans l'imposition de mesures ou de sanctions l'Autorité de protection des données pourra prendre en compte la situation spécifique des PME.

4. Ces impacts sont-ils proportionnels à l'objectif poursuivi ? [O/N] > expliquez

   Oui, la protection de droits fondamentaux.

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

   Cela dépend de la politique menée par l'Autorité de protection des données qui est d'ailleurs une autorité totalement indépendante. Néanmoins, dans l'exercice de ses tâches de contrôle le Règlement 2016/679 prévoit dans la possibilité que l'Autorité de protection des données prenne en compte la situation spécifique des PME. (Par exemple le considérant 132 : « Les activités de sensibilisation organisées par les autorités de contrôle à l'intention du public devraient comprendre des mesures spécifiques destinées aux responsables du traitement et aux sous-traitants, y compris les micro, petites et moyennes entreprises, ainsi qu'aux personnes physiques, notamment dans le cadre éducatif ».)

Charges administratives .11.

Réduction des formalités et des obligations administratives liées directement ou indirectement à l'exécution, au respect et/ou au maintien d'un droit, d'une interdiction ou d'une obligation.

↓ Si des citoyens (cf. thème 3) et/ou des entreprises (cf. thème 10) sont concernés, répondez aux questions suivantes.

1. Identifiez, par groupe concerné, les formalités et les obligations nécessaires à l'application de la réglementation.
   S'il n'y a aucune formalité ou obligation, expliquez pourquoi.

   a. Obligation dans certains cas (risques élevées à l'encontre de la personne concernée) d'établir une analyse d'impact en matière de protection des données, et éventuellement une consultation préalable de l'autorité de contrôle

   b. Suppression de l'obligation de déclaration remplacée par la tenue d'un registre. Pour le secteur public fédéral un outil est disponible

↓ S'il y a des formalités et des obligations dans la réglementation actuelle*, répondez aux questions 2a à 4a.

↓ S'il y a des formalités et des obligations dans la réglementation en projet**, répondez aux questions 2b à 4b.

2. Quels documents et informations chaque groupe concerné doit-il fournir ?

   a. Déterminer quels traitements, nouveaux traitement, base légale et quels mesures techniques et organisationnelles sont prises pour

   b. Screening et Analyse les catégories de traitement : finalités, base légale, catégories de données, catégories de destinataires, mesures techniques et organisationnelles générales, coordonnées des sous-

limiter les risques traitants, …

3. Comment s'effectue la récolte des informations et des documents, par groupe concerné ?

   a. Screening, analyse b. Screening, analyse

4. Quelles est la périodicité des formalités et des obligations, par groupe concerné ?

   a. À chaque nouveau type de traitement b. A chaque nouveau type de traitement

5. Quelles mesures sont prises pour alléger / compenser les éventuels impacts négatifs ?

   L'autorité de contrôle peut déterminer une liste des traitements qui doivent nécessairement faire l'objet d'une analyse d'impact, une liste des traitements qui ne nécessitent pas une telle analyse. Des directives sont élaborées par le groupe 29 qui réunit les 29 autorités de contrôle de l'Union européenne.

Énergie .12.

Mix énergétique (bas carbone, renouvelable, fossile), utilisation de la biomasse (bois, biocarburants), efficacité énergétique, consommation d'énergie de l'industrie, des services, des transports et des ménages, sécurité d'approvisionnement, accès aux biens et services énergétiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

– –

Mobilité .13.

Volume de transport (nombre de kilomètres parcourus et nombre de véhicules), offre de transports collectifs, offre routière, ferroviaire, maritime et fluviale pour les transports de marchandises, répartitions des modes de transport (modal shift), sécurité, densité du trafic.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

– –

Alimentation .14.

Accès à une alimentation sûre (contrôle de qualité), alimentation saine et à haute valeur nutritionnelle, gaspillages, commerce équitable.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

– –

Changements climatiques .15.

Émissions de gaz à effet de serre, capacité d'adaptation aux effets des changements climatiques, résilience, transition énergétique, sources d'énergies renouvelables, utilisation rationnelle de l'énergie, efficacité énergétique, performance énergétique des bâtiments, piégeage du carbone.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

– –

Ressources naturelles .16.

Gestion efficiente des ressources, recyclage, réutilisation, qualité et consommation de l'eau (eaux de surface et souterraines, mers et océans), qualité et utilisation du sol (pollution, teneur en matières organiques, érosion, assèchement, inondations, densification, fragmentation), déforestation.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

– –

Air intérieur et extérieur .17.

Qualité de l'air (y compris l'air intérieur), émissions de polluants (agents chimiques ou biologiques : méthane, hydrocarbures, solvants, SOx, NOx, NH3), particules fines.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Biodiversité .18.

Niveaux de la diversité biologique, état des écosystèmes (restauration, conservation, valorisation, zones protégées) , altération et fragmentation des habitats, biotechnologies, brevets d'invention sur la matière biologique, utilisation des ressources génétiques, services rendus par les écosystèmes (purification de l'eau et de l'air, …), espèces domestiquées ou cultivées, espèces exotiques envahissantes, espèces menacées.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Nuisances .19.

Nuisances sonores, visuelles ou olfactives, vibrations, rayonnements ionisants, non ionisants et électromagnétiques, nuisances lumineuses.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Autorités publiques .20.

Fonctionnement démocratique des organes de concertation et consultation, services publics aux usagers, plaintes, recours, contestations, mesures d'exécution, investissements publics.

☒ Impact positif ☐ Impact négatif ↓ Expliquez. ☐ Pas d'impact

Contrôle par l'autorité de contrôle compétente du respect par le secteur public de la réglementation vie privée. L'Autorité de protection des données nouvellement créée conseille les autorités publiques concernant des traitements de données à caractère personnel concrets mais également concernant des projets de loi qui ont un impact sur la protection des données à carcatère personnel.

Cohérence des politiques en faveur du développement .21.

Prise en considération des impacts involontaires des mesures politiques belges sur les intérêts des pays en développement.

1. Identifiez les éventuels impacts directs et indirects du projet sur les pays en développement dans les domaines suivants :

   - o sécurité alimentaire
   - o santé et accès aux médicaments
   - o travail décent
   - o commerce local et international
   - o revenus et mobilisations de ressources domestiques (taxation)
   - o mobilité des personnes
   - o environnement et changements climatiques (mécanismes de développement propre)
   - o paix et sécurité

   Expliquez si aucun pays en développement n'est concerné.

   Il n'y pas d'impact majeur sur les pays en développement. Les flux de données à caractère personnel vers les pays en développement devront respecter une protection minimale en la matière. Les conventions de coopération judiciaire et policière devront dans le futur tenir compte de la nouvelle réglementation

↓ S'il y a des impacts positifs et/ou négatifs, répondez à la question 2.

2. Précisez les impacts par groupement régional ou économique (lister éventuellement les pays). Cf. manuel

↓ S'il y a des impacts négatifs, répondez à la question 3.

3. Quelles mesures sont prises pour les alléger / compenser les impacts négatifs ?

_ _

ADVIES VAN DE RAAD VAN STATE NR. 63.192/2 VAN 19 APRIL 2018

Op 20 maart 2018 is de Raad van State, afdeling Wetgeving, door de Staatssecretaris voor Bestrijding van de sociale fraude, Privacy en Noordzee, toegevoegd aan de minister van Sociale Zaken en Volksgezondheid verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet "betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens".

Het voorontwerp is door de tweede kamer onderzocht op 19 april 2018. De kamer was samengesteld uit Pierre Vandernoot, kamervoorzitter, Luc Detroux en Wanda Vogel, staatsraden, Sébastien Van Drooghenbroeck en Jacques Englebert, assessoren, en Béatrice Drapier, griffier.

Het verslag is uitgebracht door Pauline Lagasse, auditeur. Élise Degrave, die als expert opgeroepen is op grond van artikel 82 van de wetten "op de Raad van State", gecoördineerde op 12 januari 1973, heeft eveneens verslag uitgebracht.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre Vandernoot en Wanda Vogel.

Het advies, waarvan de tekst hierna volgt, is gegeven op 19 april 2018.

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten "op de Raad van State", gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,[1‡] de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

VOORAFGAANDE OPMERKINGEN

1. Voor de afdeling Wetgeving van de Raad van State, die verzocht is om binnen een termijn van dertig dagen advies uit te brengen, is het niet mogelijk geweest bij de adviesaanvrager een verlenging van die termijn aan te vragen, hoewel een dergelijke verlenging in principe onontbeerlijk was wegens de grote omvang en de belangrijkheid van het voorontwerp waarop dit advies betrekking heeft.

Dat dit voor haar niet mogelijk geweest is, komt door het feit dat richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 "betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op

[1] ‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere normen verstaan.

AVIS DU CONSEIL D'ÉTAT N° 63.192/2 DU 19 AVRIL 2018

Le 20 mars 2018, le Conseil d'État, section de législation, a été invité par le Secrétaire d'État à la Lutte contre la fraude sociale, à la Protection de la vie privée et à la Mer du Nord, adjoint à la ministre des Affaires sociales et de la Santé publique à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi "relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel".

L'avant-projet a été examiné par la deuxième chambre le 19 avril 2018. La chambre était composée de Pierre Vandernoot, président de chambre, Luc Detroux et Wanda Vogel, conseillers d'État, Sébastien Van Drooghenbroeck et Jacques Englebert, assesseurs, et Béatrice Drapier, greffier.

Le rapport a été présenté par Pauline Lagasse, auditeur. Élise Degrave, appelée en qualité d'expert sur la base de l'article 82 des lois "sur le Conseil d'État", coordonnées le 12 janvier 1973, a également présenté un rapport.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre Vandernoot et Wanda Vogel.

L'avis, dont le texte suit, a été donné le 19 avril 2018.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois "sur le Conseil d'État", coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet[1‡], à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

OBSERVATIONS PRÉALABLES

1. La section de législation du Conseil d'État, saisie d'une demande d'avis fixant le délai d'examen à trente jours, n'a pas été en mesure de solliciter du demandeur d'avis une prolongation de ce délai, ce qui aurait été indispensable en raison de l'importance quantitative et qualitative de l'avant-projet faisant l'objet du présent avis.

Cette impossibilité résulte de ce qu'en vertu de l'article 63, paragraphe 1er, de la directive (UE) n° 2016/680 du Parlement européen et du Conseil du 27 avril 2016 "relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des

[1] ‡ S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad", welke richtlijn omgezet wordt bij titel 2 van het voorontwerp, een artikel 63, lid 1, bevat krachtens welke bepaling de ontworpen wet in principe uiterlijk op 6 mei 2018 vastgesteld en bekendgemaakt dient te worden, maar vooral door het feit dat in artikel 99, lid 2, eerste alinea, van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 "betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)" (hierna te noemen: "de AVG"), bepaald wordt dat deze verordening "met ingang van 25 mei 2018" toepasselijk is, waarbij het gaat om een rechtstreekse toepasselijkheid waardoor er geen omzettings- maar uitvoeringsmaatregels moeten worden genomen, die vastgesteld moeten worden zonder dat daaraan terugwerkende kracht wordt verleend, zodat de ontworpen wet, zoals bepaald wordt in artikel 283 van het voorontwerp (behalve wat titel 2 van het voorontwerp betreft), in werking treedt op diezelfde datum, namelijk op 25 mei 2018. Er wordt zelfs vastgesteld dat, wat inzonderheid titel 2 van het voorontwerp betreft, in datzelfde artikel 283 van het voorontwerp bepaald wordt dat het op 6 mei 2018 in werking treedt.

Binnen die zeer korte termijn heeft de afdeling Wetgeving geen exhaustief onderzoek van het voorontwerp kunnen uitvoeren, in het bijzonder uit het oogpunt van de verenigbaarheid ervan met het recht op eerbiediging van het privéleven, de AVG en richtlijn 2016/680.

Wanneer in dit advies opmerkingen gemaakt worden, betekent dat evenmin dat het mogelijk geweest is om rekening te houden met alle juridische aspecten van de vraagstukken die zijn opgeworpen. Dit geldt heel in het bijzonder, maar niet alleen, voor het onderzoek van de belangrijke vraag of de beperkingen die bij het voorontwerp aangebracht worden op het stuk van de verplichtingen en de rechten als bedoeld in de artikelen 12 tot en met 22, in artikel 34 en in artikel 5 van de AVG, wel aanvaardbaar zijn in het licht van de specifieke voorwaarden gesteld in artikel 23 van diezelfde verordening en van de vraag of de regeling werkbaar is, die vervat is in artikel 2, eerste en tweede lid, van het voorontwerp, waaruit volgt dat titel 1 van de ontworpen wet en de AVG van toepassing zullen zijn op de verwerkingen van persoonsgegevens die niet binnen het toepassingsgebied van de titels 1 tot 4 van het voorontwerp vallen. Zo ook, nog steeds bij wijze van voorbeeld, zou een onderzoek gewijd moeten worden aan artikel 4 van het voorontwerp, waarin de criteria inzake territoriale binding staan op basis waarvan de ontworpen wet al dan niet van toepassing dient te worden geacht, maar is het om de *supra* uiteengezette redenen niet mogelijk geweest een dergelijk onderzoek te verrichten.

Ook het feit dat in bepaalde opmerkingen verwezen wordt naar opmerkingen die de Commissie voor de bescherming van de persoonlijke levenssfeer gemaakt heeft in het belangrijke advies nr. 33/2018 dat ze op 11 april 2018 heeft uitgebracht, wil

fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil", transposée par le titre 2 de l'avant-projet, la loi en projet doit être adoptée et publiée pour le 6 mai 2018 en principe mais surtout qu'en vertu de l'article 99, paragraphe 2, alinéa 1er, du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 "relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)" (ci-après: "le RGPD"), ce règlement est "applicable à partir du 25 mai 2018", cette applicabilité étant directe et nécessitant non pas des mesures de transposition mais des mesures d'exécution qu'il est indispensable d'adopter sans rétroactivité en manière telle que, comme le prévoit l'article 283 de l'avant-projet (sauf pour le titre 2 de l'avant-projet), il entre en vigueur à cette même date du 25 mai 2018. Il est même constaté que, s'agissant notamment du titre 2 de l'avant-projet, son entrée en vigueur est fixée par le même article 283 de l'avant-projet au 6 mai 2018.

Dans ce très bref délai, la section de législation n'a pu se livrer à un examen exhaustif de l'avant-projet, au regard spécialement de sa compatibilité avec le droit au respect de la vie privée, le RGPD et la directive n° 2016/680.

De même, lorsque des observations sont formulées, elles ne signifient pas que tous les aspects juridiques des questions posées aient pu être pris en compte. Ceci concerne tout particulièrement, mais pas exclusivement, l'examen de l'importante question de l'admissibilité, au regard des conditions précises qui sont énoncées par l'article 23 du RGPD, des limitations apportées par l'avant-projet, aux obligations et aux droits prévus aux articles 12 à 22, 34 et 5 du même règlement et de la praticabilité du mécanisme prévu par l'article 2, alinéas 1er et 2, de l'avant-projet, dont il résulte que le titre 1er de celui-ci et le RGPD seront d'application aux traitements de données à caractère personnel ne tombant pas dans le champ d'application des titres 1 à 4 de l'avant-projet. De même, toujours à titre exemplatif, l'article 4 de l'avant-projet, qui énonce les facteurs de rattachement territoriaux commandant l'application de la loi en projet, mériterait une analyse, qu'il n'a pas été possible de mener pour les motifs exposés ci-avant.

Dans le même ordre d'idées, le fait que certaines observations se réfèrent à celles formulées par la Commission de la protection de la vie privée dans son substantiel avis n° 33/2018 du 11 avril 2018 ne signifie pas que l'absence de référence à

niet zeggen dat het niet-verwijzen naar andere opmerkingen van dat advies zou betekenen dat de afdeling Wetgeving het met die opmerkingen niet eens zou zijn.

Onder deze punten van voorbehoud wordt dit advies gegeven, waarbij de afdeling Wetgeving alleen kan betreuren dat, hoewel de AVG en richtlijn 2016/680 op 4 mei 2016 in *het Publicatieblad van de Europese Unie* bekendgemaakt zijn, zij niet over meer tijd heeft kunnen beschikken voor het uitbrengen van haar advies over dit voorontwerp, dat nochtans van fundamenteel belang is voor de werkzaamheid van het recht op eerbiediging van het privéleven, dat gewaarborgd wordt bij onder andere artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens.[2]

2. Het onderzoek door de afdeling Wetgeving is bovendien bepaald niet vergemakkelijkt door het feit dat het voorontwerp wat de vorm betreft, niet in orde is.

Het voorontwerp bevat nog vele fouten, inzonderheid wat de overeenstemming tussen de Nederlandse en de Franse tekst betreft en in de interne verwijzingen, die duidelijk niet systematisch herzien zijn bij het opstellen van de opeenvolgende versies van het voorontwerp.

Ook aan de regels van de wetgevingstechniek wordt vaak voorbijgegaan.

Ten slotte is de artikelsgewijze bespreking al even onvolmaakt, waarbij aan een aantal bepalingen zelfs in het geheel geen bespreking gewijd wordt.

De afdeling Wetgeving heeft niet over de nodige tijd beschikt en is dus niet in staat geweest de vinger te leggen op alle vormelijke onvolmaaktheden van het voorontwerp, die de bevattelijkheid ervan in het gedrang brengen. Bij wijze van voorbeeld wordt in de slotopmerkingen van dit advies op een aantal van die onvolmaaktheden gewezen. De steller van het voorontwerp dient de gehele tekst nauwkeurig na te zien voordat hij die bij de Kamer van volksvertegenwoordigers indient.

ALGEMENE OPMERKINGEN

A. Het recht op eerbiediging van het privéleven

1. Zoals het Grondwettelijk Hof recent nog opgemerkt heeft[3] in verband met het recht op eerbiediging van het privéleven dat gewaarborgd wordt door artikel 22 van de Grondwet, gelezen in samenhang met artikel 8 van het Europees Verdrag voor de rechten van de mens, artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten en de artikelen 7 en

[2] In haar advies van 11 april 2018 verklaart de Commissie voor de bescherming van de persoonlijke levenssfeer eveneens dat zij "betreurt (…) dat zij binnen een uiterst korte termijn haar advies moet geven over een tekst van dergelijke omvang die toch van enorm belang is voor de omkadering van persoonsgegevens" (punt 6) (wanneer verderop in dit advies sprake is van het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, is dat het advies waarnaar verwezen wordt).

[3] GwH 14 juli 2016, nr. 108/2016, B.7 tot B.13; 15 maart 2018, nr. 29/2018, B.9 tot B.15.

d'autres observations de cet avis exprimerait nécessairement un désaccord sur celles-ci.

C'est sous ces réserves que le présent avis est donné, la section de législation ne pouvant que regretter qu'alors que le RGPD et la directive n° 2016/680 ont été publiés au *Journal officiel de l'Union européenne* le 4 mai 2016, elle n'ait pu disposer de davantage de temps pour donner son avis sur cet avant-projet, pourtant fondamental au regard de l'effectivité du droit au respect de la vie privée garanti notamment par l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme[2].

2. L'examen par la section de législation n'a en outre pas été facilité par le caractère formellement inabouti de l'avant-projet.

Celui-ci comporte encore de nombreuses erreurs, notamment quant à la concordance entre le texte français et le texte néerlandais, ainsi que dans les renvois internes, qui visiblement n'ont pas été systématiquement revus lors de l'élaboration des versions successives de l'avant-projet.

Les règles de légistique formelle sont également souvent méconnues.

Enfin, le commentaire des articles est tout autant déficient, certaines dispositions en étant totalement dépourvues.

La section de législation n'a pas disposé du temps nécessaire et n'a donc pu relever toutes les imperfections formelles de l'avant-projet, qui nuisent à sa bonne compréhension. À titre illustratif, certaines de ces imperfections sont relevées en observations finales du présent avis. Il appartiendra à son auteur de revoir entièrement et scrupuleusement celui-ci avant de le déposer devant la Chambre des représentants.

OBSERVATIONS GÉNÉRALES

A. Le droit au respect de la vie privée

1. Comme l'a encore récemment rappelé la Cour constitutionnelle[3], s'agissant du droit au respect de la vie privée garanti par l'article 22 de la Constitution, combiné avec l'article 8 de la Convention européenne des droits de l'homme, l'article 17 du Pacte international relatif aux droits civils et politiques et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union

[2] Dans son avis du 11 avril 2018, la Commission de la protection de la vie privée dit aussi "regrette[r] de devoir donner son avis sur un texte d'une telle ampleur et importance pour l'encadrement des données à caractère personnel dans un délai extrêmement court" (§ 6) (lorsque, dans la suite du présent avis, il est question de celui de la Commission de la protection de la vie privée, ce sera à cet avis qu'il sera renvoyé).

[3] C.C., 14 juillet 2016, n° 108/2016, B.7 à B.13; 15 mars 2018, n° 29/2018, B.9 à B.15.

8 van het Handvest van de grondrechten van de Europese Unie, is de draagwijdte van artikel 8 EVRM analoog aan die van de voormelde grondwettelijke bepaling, zodat de waarborgen die deze beide bepalingen bieden een onlosmakelijk geheel vormen.

De artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie hebben, wat de verwerking van persoonsgegevens in het kader van de uitvoering van het Unierecht betreft, een draagwijdte die analoog is aan die van artikel 8 van het Europees Verdrag voor de rechten van de mens en aan die van artikel 22 van de Grondwet. Hetzelfde geldt voor artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten.

Het recht op eerbiediging van het privéleven, zoals gewaarborgd in de voormelde grondwets- en verdragsbepalingen, heeft voornamelijk tot doel de personen te beschermen tegen inmengingen in hun privéleven. Dat recht heeft een ruime draagwijdte en omvat onder meer de bescherming van persoonsgegevens en van persoonlijke informatie.

In dat verband en wat de toepassingsgebieden buiten de Europese Unie betreft, wordt in Verdrag nr. 108 van de Raad van Europa van 28 januari 1981 “tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens”, dat bindend is voor de Belgische Staat, eveneens bepaald dat de Belgische Staat een reeks minimale waarborgen moet bieden.

2.1. Dat recht is evenwel niet absoluut. Het sluit overheidsinmenging in het recht op eerbiediging van het privéleven niet uit, maar het is vereist dat zij toegestaan wordt door een voldoende precieze wettelijke bepaling, dat zij beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving en dat zij evenredig is met de daarmee nagestreefde wettige doelstelling. Die bepalingen houden voor de overheid bovendien de positieve verplichting in om maatregelen te nemen die een daadwerkelijke eerbiediging van het privéleven verzekeren, zelfs in de sfeer van de onderlinge verhoudingen tussen individuen.

2.2. Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. Een delegatie aan een andere macht is evenwel niet in strijd met het wettelijkheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever vastgesteld zijn.

2.3. Naast het formele wettelijkheidsvereiste legt artikel 22 van de Grondwet eveneens de verplichting op dat de inmenging in het recht op eerbiediging van het privéleven in duidelijke en voldoende nauwkeurige bewoordingen wordt

européenne, la portée de l’article 8 de la Convention est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un ensemble indissociable.

Les articles 7 et 8 de la Charte des droits fondamentaux de l’Union européenne ont, en ce qui concerne le traitement des données à caractère personnel dans le cadre de la mise en œuvre du droit de l’Union, une portée analogue à celle de l’article 8 de la Convention européenne des droits de l’homme et de l’article 22 de la Constitution. Il en va de même de l’article 17 du Pacte international relatif aux droits civils et politiques.

Le droit au respect de la vie privée, tel qu’il est garanti par les dispositions constitutionnelles et conventionnelles précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée. Ce droit a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles.

À cet égard et en ce qui concerne les domaines d’application en dehors de l’Union européenne, la Convention n° 108 du Conseil de l’Europe “pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel”, qui lie l’État belge, impose également une série de garanties minimales à l’État belge.

2.1. Ce droit n’est cependant pas absolu. Il n’exclut pas toute ingérence d’une autorité publique dans l’exercice du droit au respect de la vie privée mais il est requis qu’elle soit prévue par une disposition législative suffisamment précise, qu’elle réponde à un besoin social impérieux dans une société démocratique et qu’elle soit proportionnée à l’objectif légitime qu’elle poursuit. Ces dispositions engendrent de surcroît l’obligation positive, pour l’autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, même dans la sphère des relations entre les individus.

2.2. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l’article 22 de la Constitution garantit à tout citoyen qu’aucune ingérence dans l’exercice de ce droit ne peut avoir lieu qu’en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Une délégation à un autre pouvoir n’est toutefois pas contraire au principe de légalité, pour autant que l’habilitation soit définie de manière suffisamment précise et porte sur l’exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

2.3. Outre l’exigence de légalité formelle, l’article 22 de la Constitution impose également que l’ingérence dans l’exercice du droit au respect de la vie privée soit définie en des termes clairs et suffisamment précis qui permettent

geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging in het recht op eerbiediging van het privéleven toestaat.

Evenzo houdt het vereiste van voorzienbaarheid waaraan de wet moet voldoen om in overeenstemming te worden bevonden met artikel 8 van het Europees Verdrag voor de rechten van de mens, in dat de formulering ervan voldoende precies is zodat eenieder – desnoods met gepast advies – in de gegeven omstandigheden in redelijke mate de gevolgen van een bepaalde handeling kan voorzien. De wetgeving moet eenieder een voldoende indicatie geven over de omstandigheden waarin en de voorwaarden waaronder de overheden gebruik mogen maken van maatregelen die raken aan de rechten gewaarborgd door het Verdrag. Meer in het bijzonder wanneer het optreden van de overheid een geheim karakter vertoont, dient de wet voldoende waarborgen te bieden tegen willekeurige inmengingen in het recht op eerbiediging van het privéleven, namelijk door de beoordelingsbevoegdheid van de betrokken overheden op voldoende duidelijke wijze af te bakenen, enerzijds, en door te voorzien in procedures die een effectief toezicht toelaten, anderzijds.

Uit artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 22 van de Grondwet volgt aldus dat voldoende precies moet worden bepaald in welke omstandigheden een verwerking van persoonsgegevens is toegelaten. De vereiste graad van precisie van de betrokken wetgeving – die niet in elke hypothese kan voorzien – is, volgens het Europees Hof voor de Rechten van de Mens, onder meer afhankelijk van het domein dat wordt gereguleerd en van het aantal en de hoedanigheid van de personen tot wie de wet gericht is. Zo heeft het Europees Hof voor de Rechten van de Mens geoordeeld dat het vereiste van voorzienbaarheid in domeinen die te maken hebben met de nationale veiligheid, niet dezelfde draagwijdte kan hebben als in andere domeinen.[4]

2.4. Overheidsinmenging in het recht op eerbiediging van het privéleven dient niet alleen te steunen op een voldoende precieze wettelijke bepaling, ze dient daarenboven op een redelijke verantwoording te berusten en evenredig te zijn met de doelstellingen die nagestreefd worden door de wetgever, die ter zake over een appreciatiemarge beschikt. Die appreciatiemarge is evenwel niet onbegrensd: opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft gevonden tussen alle rechten en belangen die in het geding zijn.

Wat de evenredigheid betreft, houden het Europees Ho voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie rekening met het al dan niet aanwezig zijn van materiële en procedurele waarborgen in de betrokken regeling. Bij de beoordeling van de evenredigheid van maatregelen met betrekking tot de verwerking van persoonsgegevens, dient aldus rekening te worden gehouden met, onder meer, het geautomatiseerde karakter ervan, de gebruikte technieken, de accuraatheid, de pertinentie en het al dan niet buitensporige karakter van de gegevens die worden verwerkt, het al dan niet voorhanden zijn van maatregelen die de duur

[4] EHRM 26 maart 1987, *Leander* t. Zweden, § 51; 4 juli 2006, *Lupsa* t. Roemenië, § 33.

d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

De même, l'exigence de prévisibilité à laquelle la loi doit satisfaire pour être jugée conforme à l'article 8 de la Convention européenne des droits de l'homme implique que sa formulation soit assez précise pour que chacun puisse – en s'entourant au besoin de conseils éclairés – prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé. La législation doit donner à chacun une indication suffisante sur les circonstances dans lesquelles et à quelles conditions elle habilite la puissance publique à recourir à des mesures affectant les droits protégés par la Convention. Plus particulièrement, lorsque l'intervention de l'autorité présente un caractère secret, la loi doit offrir des garanties suffisantes contre les ingérences arbitraires dans l'exercice du droit au respect de la vie privée, en délimitant le pouvoir d'appréciation des autorités concernées avec une netteté suffisante, d'une part, et en prévoyant des procédures qui permettent un contrôle effectif, d'autre part.

Il découle dès lors de l'article 8 de la Convention et de l'article 22 de la Constitution qu'il doit être prévu de manière suffisamment précise dans quelles circonstances un traitement de données à caractère personnel est autorisé. Le niveau requis de précision de la législation concernée – laquelle ne peut du reste parer à toute éventualité – dépend notamment, selon la Cour européenne des droits de l'homme, du domaine qu'elle est censée couvrir et du nombre et de la qualité de ses destinataires. Ainsi, cette Cour a jugé que l'exigence de prévisibilité dans des domaines liés à la sécurité nationale ne pouvait avoir la même portée que dans d'autres domaines[4].

2.4. Une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise mais aussi reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur, qui dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée: pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause.

En ce qui concerne la proportionnalité, la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne tiennent compte de l'existence ou non, dans la réglementation visée, des garanties matérielles et procédurales. Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence

[4] Cour eur. D.H., arrêt *Leander c. Suède*, 26 mars 1987, § 51; arrêt *Lupsa c. Roumanie*, 4 juillet 2006, § 33.

van de bewaring van de gegevens beperken, het al dan niet voorhanden zijn van een systeem van onafhankelijk toezicht dat toelaat na te gaan of de bewaring van de gegevens nog langer is vereist, het al dan niet voorhanden zijn van afdoende controlerechten en rechtsmiddelen voor de betrokkenen, het al dan niet voorhanden zijn van waarborgen ter voorkoming van stigmatisering van de personen van wie de gegevens worden verwerkt, het onderscheidend karakter van de regeling en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik en misbruik van de verwerkte persoonsgegevens door de overheidsdiensten.

3. *In casu* houdt het recht op eerbiediging van het privéleven verband met de kern zelf van het voorontwerp dat aan de afdeling Wetgeving voorgelegd is. Het voorontwerp is dan ook onderzocht in het licht van de beginselen waaraan zonet herinnerd is.

B. Het juridisch statuut van de toezichthoudende autoriteiten

1.1. Artikel 4 van de wet van 3 december 2017 "tot oprichting van de Gegevensbeschermingsautoriteit" heeft tot doel te bepalen welke instanties naar Belgisch recht in principe de toezichthoudende autoriteiten voor de verwerking van persoonsgegevens zijn.

In principe is die instantie de "Gegevensbeschermingsautoriteit", die naar luid van artikel 3, eerste lid, van die wet bij de Kamer van volksvertegenwoordigers opgericht wordt en die krachtens het tweede lid van die bepaling de opvolger is van de Commissie voor de bescherming van de persoonlijke levenssfeer. De "Gegevensbeschermingsautoriteit" wordt bij artikel 2, 1°, van die wet gedefinieerd als "de Toezichthoudende autoriteit voor de verwerking van persoonsgegevens".

In artikel 4, § 2, eerste lid, van dezelfde wet wordt bepaald dat "[h]et toezicht dat door deze wet (…) georganiseerd [wordt] (…) geen betrekking [heeft] op de verwerkingen door de hoven en rechtbanken alsook door het openbaar ministerie bij de uitoefening van hun gerechtelijke taken", terwijl de Koning krachtens het tweede lid van dat artikel 4, § 2, "andere autoriteiten [kan] aanduiden voor zover zij persoonsgegevens verwerken in het kader van hun gerechtelijke taken".

Wat de politiediensten betreft, voorziet artikel 4, § 2, derde lid, van dezelfde wet in een afwijkende regeling: "[de] competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de [AVG] worden uitgeoefend door het Controleorgaan op de politionele informatie bedoeld in artikel 44/6, § 1, van de wet van 5 augustus 1992 op het politieambt". Bij artikel 280 van het voorliggend voorontwerp wordt die bepaling van de wet van 3 december 2017 aldus aangevuld en, volgens de bespreking van artikel 2018, "verduidelijkt" dat de uitoefening van het toezicht eveneens aan dat orgaan toevertrouwd wordt wat betreft "de Dienst Enquêtes van het Vast Comité van toezicht op de politiediensten zoals bedoeld in artikel 16 van de wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse van 18 juli 1991 en de Algemene

d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées, du caractère distinctif de la réglementation et de la présence ou de l'absence de garanties visant à éviter l'usage inapproprié et abusif, par les services publics, des données à caractère personnel traitées.

3. En l'espèce, le droit au respect de la vie privée est au cœur de l'avant-projet soumis à la section de législation. C'est donc au regard des principes qui viennent d'être rappelés que l'avant-projet a été examiné.

B. Le régime juridique des autorités de contrôle

1.1. L'article 4 de la loi du 3 décembre 2017 "portant création de l'Autorité de protection des données" a pour objet de déterminer, en principe, quelles sont, en droit belge, les autorités de contrôle des traitements de données à caractère personnel.

Il s'agit, en règle, de l'"Autorité de protection des données" instituée par l'article 3, alinéa 1er, de cette loi auprès de la Chambre des représentants, qui, en vertu de l'alinéa 2 cette disposition, succède à la Commission de la protection de la vie privée. Elle est définie par l'article 2, 1°, de cette loi comme étant "l'Autorité de contrôle des traitements de données à caractère personnel".

L'article 4, § 2, alinéa 1er, de la même loi dispose que "[l]e contrôle organisé par [cette] loi ne porte pas sur les traitements effectués par les cours et tribunaux ainsi que le ministère public dans l'exercice de leur fonction juridictionnelle", le Roi pouvant, en vertu de l'alinéa 2 de cet article 4, § 2, "désigner d'autres autorités pour autant qu'elles traitent des données à caractère personnel dans l'exercice de leur fonction juridictionnelle".

Quant aux services de police, l'article 4, § 2, alinéa 3, de la même loi prévoit un régime dérogatoire: "les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le [RGPD] sont exercés par l'Organe de contrôle de l'information policière visé à l'article 44/6, § 1er, de la loi du 5 août 1992 sur la fonction de police". L'article 280 de l'avant-projet à l'examen complète et "clarifie", selon son commentaire, cette dernière disposition pour confier également à cet Organe le contrôle du "service d'enquête du Comité permanent des services de police, tel que visé à l'article 16 de la loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace du 18 juillet 1991 et [de] l'Inspection générale de la police fédérale et de la police locale, tel que visé à l'article 2 de la loi du 15 mai 2007 sur l'Inspection générale et portant des

Inspectie van de federale politie en van de lokale politie zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten".

Daaruit volgt dat de "Gegevensbeschermingsautoriteit", die opgericht wordt bij artikel 3, eerste lid, van de wet van 3 december 2017, beschouwd dient te worden als de "toezichthoudende autoriteit" in de zin van het voorliggend voorontwerp, tenzij een wet in een afwijkende regeling voorziet.

1.2. Het begrip "bevoegde toezichthoudende autoriteit", dat in vele bepalingen van titel 1 van het voorontwerp gehanteerd wordt, dient in die zin begrepen te worden.

Strikt wettelijk gezien is die methode niet verkeerd.

Wat de politiediensten, de Dienst Enquêtes van het Vast Comité van toezicht op de politiediensten en de Algemene Inspectie van de federale politie en van de lokale politie betreft, zou de ontworpen wet, zonder nadere precisering op dat punt, eveneens in samenhang met artikel 4, § 2, derde lid, van de wet van 3 december 2017 gelezen kunnen worden, wat voldoende grond zou opleveren om ervan uit te gaan dat die diensten en instellingen onder het toezicht van het Controleorgaan op de politionele informatie vallen.

In titel 2 van het voorontwerp wordt evenwel een andere methode gevolgd.

Immers, in die titel 2:

— wordt, in artikel 31, 15°, de volgende definitie voorgesteld van het begrip "toezichthoudende autoriteit": "de onafhankelijke overheidsinstantie die bij wet belast is met het toezicht op de toepassing van deze titel, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met verwerking te beschermen en het vrije verkeer van persoonsgegevens binnen de Europese Unie te vergemakkelijken";

— wordt, bij artikel 73, § 1, "een onafhankelijke toezichthoudende autoriteit op de politionele informatie opgericht, [die] Controleorgaan op de politionele informatie genoemd [wordt]" en in verband waarmee in paragraaf 3 van hetzelfde artikel bepaald wordt dat de "samenstelling [ervan], het statuut van [zijn] leden, [zijn] opdrachten, [zijn] bevoegdheden evenals [de] financiering [ervan] (…) geregeld [worden] in titel 7";

— worden, in artikel 73, § 1, derde lid, de algemene bevoegdheden van dat orgaan ten aanzien van de politiediensten, de Dienst Enquêtes van het Vast Comité van toezicht op de politiediensten, de Algemene Inspectie van de federale politie en van de lokale politie en de Passagiersinformatie-eenheid opgesomd door te verwijzen naar onder andere artikel 31, 15°, van het voorontwerp, de bepalingen van titel 1, hoofdstuk 4, afdeling 2, die van toepassing zijn op de politiediensten, artikel 4, § 2, van de wet van 3 december 2017 en artikel 44/6 van de wet op het politieambt, waarbij de mogelijkheid opengelaten wordt dat "door of krachtens andere wetten" aan dat orgaan enige "andere opdracht" verleend zou worden.

dispositions diverses relatives au statut de certains membres des services de police".

Il en résulte que, sauf si une loi prévoit un régime dérogatoire, c'est l'"Autorité de protection des données" instituée par l'article 3, alinéa 1er, de la loi du 3 décembre 2017 qui doit être considérée comme étant "l'autorité de contrôle" au sens de l'avant-projet à l'examen.

1.2. C'est en ce sens qu'il faut comprendre la notion d'"autorité de contrôle compétente" au sein de nombreuses dispositions du titre 1er de l'avant-projet.

En droit strict, cette méthode n'est pas incorrecte.

S'agissant des services de police, du service d'enquête du Comité permanent des services de police et de l'Inspection générale de la police fédérale et de la police locale, la loi en projet, sans autre précision sur ce point, pourrait également être lue en combinaison avec l'article 4, § 2, alinéa 3, de la loi du 3 décembre 2017, ce qui suffirait à soumettre ces services et institutions au contrôle de l'Organe de contrôle de l'information policière.

La méthode suivie par le titre 2 de l'avant-projet est toutefois différente.

En effet, ce titre 2:

— propose à l'article 31, 15°, une définition de la notion d'"autorité de contrôle" comme étant "l'autorité publique indépendante chargée par la loi de surveiller l'application du présent titre, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union européenne";

— crée à l'article 73, § 1er, "une autorité de contrôle indépendante de l'information policière, dénommé Organe de contrôle de l'information policière", dont, selon le paragraphe 3 de la même disposition, "[l]a composition, le statut de ses membres, ses missions, ses compétences ainsi que son financement sont réglés dans le titre 7";

— énumère à l'article 73, § 1er, aliéna 3, les attributions générales de cet Organe à l'égard des services de police, du service d'enquête du Comité permanent de contrôle des services de police, de l'Inspection générale de la police fédérale et de la police locale et de l'Unité d'information des passagers, par référence notamment à l'article 31, 15°, de l'avant-projet, des dispositions du titre 1er, chapitre 4, section 2, applicables aux services de police, à l'article 4, § 2, de la loi du 3 décembre 2017 et à l'article 44/6 de la loi sur la fonction de police, tout en réservant la possibilité, "par ou en vertu d'autres lois", de lui assigner "toute autre mission".

In aansluiting op dat artikel 73, wordt in het voorontwerp een titel 7 gewijd aan het Controleorgaan op de politionele informatie, waarbij voorzien wordt in een regeling inzake de samenstelling van dat orgaan, het statuut van zijn leden en van zijn Dienst Onderzoeken, zijn opdrachten, zijn bevoegdheden en die van zijn leden en van de leden van zijn Dienst Onderzoeken, alsook inzake de financiering van dat orgaan.

Deze methode heeft de verdienste dat ze voorziet in duidelijke regelgeving betreffende een aangelegenheid, het toezicht op de verwerking van persoonsgegevens, die van essentieel belang is voor de werkzaamheid van het recht op eerbiediging van het privéleven, in het bijzonder wanneer de betrokkenen geen rechtstreekse toegang hebben tot de gegevens die op hen betrekking hebben.

Deze methode leidt er evenwel toe dat in twee onderscheiden wetten, namelijk de wet van 3 december 2017 en de ontworpen wet, een dispositief met een identiek doel voorkomt, namelijk het aanwijzen van de toezichtsautoriteit voor de politiediensten, de Dienst Enquêtes van het Vast Comité van toezicht op de politiediensten en de Algemene Inspectie van de federale politie en van de lokale politie.

Artikel 4, § 2, derde lid, van de wet van 3 december 2017 zou dan ook opgeheven moeten worden, aangezien die bepaling overbodig wordt gelet op de voormelde bepalingen van het voorontwerp die aan het Controleorgaan op de politionele informatie gewijd zijn.[5]

Daarbij zou artikel 4 van die wet aldus herzien moeten worden dat een algemeen voorbehoud gemaakt wordt voor de gevallen waarin bijzondere wetten dispositieven zouden bevatten waarbij andere toezichthoudende autoriteiten voor de verwerking van persoonsgegevens opgericht zouden worden. De Gegevensbeschermingsautoriteit die bij artikel 3 van die wet opgericht wordt, geldt daarbij zoals dat het geval is voor de meeste bepalingen van titel 1 van het voorliggende ontwerp als de gemeenrechtelijke autoriteit ter zake.

1.3. Die manier van werken zou ook dienstig zijn bij de methode die gebruikt wordt voor titel 3 van het voorontwerp, die gewijd is aan de verwerking van persoonsgegevens door andere overheden dan die bedoeld in de titels 1 en 2 van het voorontwerp, namelijk de inlichtingen- en veiligheidsdiensten (ondertitel 1), de krijgsmacht (ondertitel 2), de overheden die vallen onder de wet van 11 december 1998 “betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen” (ondertitel 3), het Coördinatieorgaan voor de dreigingsanalyse (ondertitel 4) en de Passagiersinformatie-eenheid (ondertitel 5).

Voor die overheden bestaat er geen regeling die vergelijkbaar is met die welke vervat is in artikel 4, § 2, derde lid, van de wet van 3 december 2017.

Voor de inlichtingen- en veiligheidsdiensten, voor de overheden die onder de wet van 11 december 1998 vallen

[5] In dat geval zou artikel 280 van het voorontwerp weggelaten moeten worden, mede gelet op artikel 73, § 1, derde lid (inleidende zin), van het voorontwerp, gelezen in samenhang met artikel 31, § 1, 7°, b), c) en d), van het voorontwerp.

En écho à cet article 73, l’avant-projet consacre un titre 7 à l’Organe de contrôle de l’information policière, qui règle la composition et le statut de ses membres et de son service d’enquête, ses missions, ses compétences et celles de ses membres et des membres de son service d’enquête, ainsi que son financement.

Cette méthode présente le mérite de la clarté normative sur une question, le contrôle du traitement des données à caractère personnel, essentielle à l’effectivité du droit au respect de la vie privée, spécialement lorsque les intéressés n’ont pas un accès direct aux données qui les concernent.

Elle aboutit toutefois à faire figurer dans deux lois différentes, celle du 3 décembre 2017 et celle en projet, un dispositif à objet identique, à savoir celui de l’identification de l’autorité de contrôle pour les services de police, le service d’enquête du Comité permanent de contrôle des services de police et l’Inspection générale de la police fédérale et de la police locale.

Il conviendrait donc d’abroger l’article 4, § 2, alinéa 3, de la loi du 3 décembre 2017, devenu inutile en raison des dispositions énoncées ci-dessus de l’avant-projet consacrées à l’Organe de contrôle de l’information policière[5].

Il faudrait alors revoir l’article 4 de cette loi pour réserver de manière générale les cas où des lois particulières contiennent des dispositifs créant d’autres autorités de contrôle des traitements de données à caractère personnel, l’Autorité de protection des données créée par l’article 3 de cette loi ayant pour vocation, comme pour la plupart des dispositions du titre 1er de l’avant-projet à l’examen, d’apparaître comme étant l’autorité de droit commun en la matière.

1.3. Pareille manière de procéder donnerait tout son sens à la méthode utilisée pour le titre 3 de l’avant-projet, consacré au traitement des données à caractère personnel par d’autres autorités que celles visées aux titres 1 et 2 de l’avant-projet, à savoir les services de renseignement et de sécurité (sous-titre 1), les forces armées (sous-titre 2), les autorités concernées par la loi du 11 décembre 1998 “relative à la classification et aux habilitations, attestations et avis de sécurité” (sous-titre 3), l’Organe de coordination pour l’analyse de la menace (sous-titre 4) et l’Unité d’information des passagers (sous-titre 5).

Il n’y a pas, pour ces autorités, de dispositif comparable à celui énoncé par l’article 4, § 2, alinéa 3, de la loi du 3 décembre 2017.

Pour les services de renseignement et de sécurité, les autorités concernées par la loi du 11 décembre 1998 et l’Unité

[5] En ce cas, compte tenu également de l’article 73, § 1er, alinéa 3 (phrase introductive), de l’avant-projet, lu en combinaison avec l’article 31, § 1er, 7°, b), c) et d), de celui-ci, l’article 280 de l’avant-projet doit être omis.

en voor de Passagiersinformatie-eenheid, wordt het Vast Comité I aangewezen als toezichthoudende autoriteit.[6] Voor de krijgsmacht gaat het om het Controleorgaan op de politionele informatie.[7] Voor het Coördinatieorgaan voor de dreigingsanalyse en zijn verwerkers worden het Vast Comité I en het Vast Comité van Toezicht op de politiediensten bij het voorontwerp als toezichthoudende autoriteiten aangewezen.[8]

De wet van 3 december 2017 en de ontworpen wet zouden beter op elkaar afgestemd zijn indien het voorbehoud dat in opmerking 1.2, *in fine*, gemaakt wordt in de eerstgenoemde van beide wetten opgenomen zou zijn.

1.4. Hoe dan ook mogen in een definitie in principe geen regelgevende elementen opgenomen worden of vermeldingen aangaande de bestaansreden van een dispositief.

Er zou dan ook voor gezorgd moeten worden dat in artikel 31, 15°, de woorden "teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met verwerking te beschermen en het vrije verkeer van persoonsgegevens binnen de Europese Unie te vergemakkelijken" vervallen en dat in de artikelen 74, § 2, 6°, 108, § 2, 6°, en 140, § 2, 5°, de woorden "teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met verwerking te beschermen" vervallen.

De vraag rijst zelfs of die definities en de verwijzingen daarnaar in de artikelen 107, 6°, en 170, § 1, wel nut hebben, temeer daar in die bepalingen verwezen wordt naar "de wet" zonder meer. Die definities nemen niet weg dat een wetgeving opgesteld dient te worden die voldoende duidelijk is opdat in elke situatie uitgemaakt kan worden welke de bevoegde toezichthoudende overheid is op basis van een transparante afstemming tussen de bevoegdheden van de Gegevensbeschermingsautoriteit die bij de wet van 3 december 2017 opgericht wordt en de overige toezichthoudende autoriteiten.

1.5. Het voorontwerp dient in het licht van deze opmerkingen aldus herzien te worden dat een wetgeving tot stand komt die, overeenkomstig de vereisten die gelden voor het begrip "wet" in de zin van artikel 8, lid 2, van het Europees Verdrag voor de rechten van de mens, voor de rechtssubjecten duidelijk genoeg en voorzienbaar is.

In de memorie van toelichting moet hoe dan ook uitleg verstrekt worden over de gevolgde methode en het zou goed zijn als daarbij, volgens de huidige stand van het recht, per categorie instellingen en diensten waarop het voorontwerp

6 Voor de inlichtingen- en veiligheidsdiensten, zie de artikelen 74, § 2, 6°, en 97; voor de overheden die onder de wet van 11 december 1998 vallen, zie de artikelen 108, § 2, 6°, en 130; voor de Passagiersinformatie-eenheid, zie de artikelen 170, § 1 (in samenhang gelezen met artikel 74, § 2, 6°), en186 (in samenhang gelezen met artikel 97).

7 De artikelen 73 (vermelding, in de inleidende zin van paragraaf 1, derde lid, van artikel 31, § 1, 7°, c)) en 107, 6°, (in samenhang gelezen met artikel 31, 15°).

8 Artikelen 140, § 2, 5°, en 163.

d'information des passagers, c'est le Comité permanent R qui est désigné comme autorité de contrôle[6]. Pour les forces armées, il s'agit de l'Organe de contrôle de l'information policière[7]. Pour l'Organe de coordination de l'analyse de la menace et ses sous-traitants, l'avant-projet désigne le Comité permanent R et le Comité permanent de contrôle des services de police[8].

L'articulation entre la loi du 3 décembre 2017 et celle en projet serait mieux assurée si la réserve évoquée à la fin de l'observation n° 1.2 était insérée dans la première de ces lois.

1.4. En tout état de cause, une définition ne doit en principe pas contenir des éléments à caractère normatif ou des indications quant à la raison d'être d'un dispositif.

Il conviendrait donc, à l'article 31, 15°, d'omettre les mots "afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union européenne" et, aux articles 74, § 2, 6°, 108, § 2, 6°, et 140, § 2, 5°, d'omettre les mots "afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement".

La question se pose même de l'utilité de ces définitions et des références qui y sont faites par les articles 107, 6°, et 170, § 1er, et ce d'autant plus que ces dispositions se réfèrent à "la loi" sans autre précision. Elles ne peuvent remplacer l'élaboration d'une législation suffisamment claire quant à la possibilité, pour chaque cas de figure, d'identifier l'autorité de contrôle compétente sur la base d'une articulation transparente entre les compétences de l'Autorité de protection des données instituée par la loi du 3 décembre 2017 et les autres autorités de contrôle.

1.5. L'avant-projet sera revu à la lumière de ces observations de manière à mettre en place une législation qui, conformément aux exigences liées à la notion de "loi" au sens de l'article 8, § 2, de la Convention européenne des droits de l'homme, soit suffisamment claire et prévisible pour les sujets de droit.

L'exposé des motifs s'expliquera en tout état de cause sur la méthode suivie et gagnerait à lister, en l'état actuel du droit, par catégories d'institutions et de services concernés par l'avant-projet, quelles sont les autorités de contrôle

6 Pour les services de renseignement et de sécurité, voir les articles 74, § 2, 6°, et 97; pour les autorités concernées par la loi du 11 décembre 1998, voir les articles 108, § 2, 6°, et 130; pour l'Unité d'information des passagers, voir les articles 170, § 1er (lu en combinaison avec l'article 74, § 2, 6°), et186 (lu en combinaison avec l'article 97).

7 Articles 73 (mention, dans la phrase liminaire du paragraphe 1er, alinéa 3, de l'article 31, § 1er, 7°, c)) et 107, 6°, (lu en combinaison avec l'article 31, 15°).

8 Articles 140, § 2, 5°, et 163.

betrekking heeft, opgelijst zou worden welke de bevoegde toezichthoudende autoriteiten zijn, telkens met vermelding van de thans relevante of ontworpen wettelijke of reglementaire bepalingen.

2. Artikel 51, lid 3, van de AVG luidt als volgt:

"Wanneer er in een lidstaat meer dan één toezichthoudende autoriteit is gevestigd, wijst die lidstaat de toezichthoudende autoriteit aan die [deze] autoriteiten in het [Europees] Comité [voor gegevensbescherming] moet vertegenwoordigen en stelt hij de procedure vast om ervoor te zorgen dat de andere autoriteiten de regels in verband met het in artikel 63 bedoelde coherentiemechanisme naleven."

Zoals *supra* uiteengezet is, blijkt *in casu* uit het voorontwerp (zie meer in het bijzonder artikel 280 van het voorontwerp) en uit de wet van 3 december 2017 (zie meer in het bijzonder artikel 4, § 2, van die wet) dat verscheidene autoriteiten de rol van toezichthoudende autoriteit in de zin van hoofdstuk VI van de AVG zullen vervullen.

Zo ook wordt in artikel 41, lid 4, van richtlijn 2016/680/EU bepaald dat

"[w]anneer er in een lidstaat meer dan één toezichthoudende autoriteit (…) opgericht [wordt], (…) die lidstaat de toezichthoudende autoriteit aan[wijst] die deze autoriteiten in het in artikel 51 bedoelde [Europees] Comité [voor gegevensbescherming] vertegenwoordigt".

In casu blijkt uit het voorontwerp dat verscheidene autoriteiten de rol van toezichthoudende autoriteit in de zin van hoofdstuk VI van de richtlijn zullen uitoefenen.

De aanwijzing van de toezichthoudende autoriteit die de andere autoriteiten bij het Europees Comité voor gegevensbescherming moet vertegenwoordigen, moet met een samenwerkingsakkoord worden geregeld. Wat dat betreft, wordt verwezen naar advies 61.267/2/AV, op 27 juni 2017 gegeven over een voorontwerp dat heeft geleid tot de wet van 3 december 2017 "tot oprichting van de Gegevensbesc hermingsautoriteit".[9]

BIJZONDERE OPMERKINGEN

VOORAFGAANDE TITEL

Artikel 2

Doordat in het tweede en het derde lid wordt gesteld dat de verordening "geldt" of "niet van toepassing" is, wekt de tekst de indruk dat een nationale wetgever de werkingssfeer van een tekst van afgeleid Europees recht kan verruimen of inperken, wat ten aanzien van de respectieve autonomie van de Europese rechtsorde en de nationale rechtsorden niet aanvaardbaar is.

[9] Algemene opmerkingen, afdeling I, II, C, *Parl.St.* Kamer 2017-18, nr. 2648/001, 121.

compétentes en indiquant chaque fois les dispositions législatives, voire réglementaires, actuellement pertinentes ou en projet.

2. Conformément à l'article 51, paragraphe 3, du RGPD,

"Lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité [européen de la protection des données] et définit le mécanisme permettant de s'assurer du respect, par les autres autorités, des règles relatives au mécanisme de contrôle et de la cohérence visé à l'article 63".

En l'espèce, ainsi qu'il vient d'être exposé, il résulte de l'avant-projet (voir plus particulièrement son article 280) et de la loi du 3 décembre 2017 (voir plus particulièrement son article 4, § 2) que plusieurs autorités exerceront le rôle d'autorité de contrôle au sens du chapitre VI du RGPD.

De même, l'article 41, paragraphe 4, de la directive n° 2016/680/UE prévoit que,

"lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité [européen de la protection des données] visé à l'article 51".

En l'espèce, il résulte de l'avant-projet que plusieurs autorités exerceront le rôle d'autorité de contrôle au sens du chapitre VI de la directive.

La désignation de l'autorité de contrôle qui représentera les autres autorités auprès du Comité européen de la protection des données doit être réglée par un accord de coopération. Il est renvoyé sur ce point à l'avis n° 61.267/2/AG donné le 27 juin 2017 sur l'avant-projet devenu la loi du 3 décembre 2017 "portant création de l'Autorité de protection des données"[9].

OBSERVATIONS PARTICULIÈRES

TITRE PRÉLIMINAIRE

Article 2

En indiquant aux alinéas 2 et 3 que le règlement "s'applique" ou ne "s'applique pas", le texte laisse à penser qu'un législateur national peut étendre ou restreindre le champ d'application d'un dispositif de droit européen dérivé, ce qui n'est pas admissible au regard de l'autonomie respective de l'ordre juridique européen et des ordres juridiques nationaux.

[9] Observations générales, section I, II, C, *Doc. parl.*, Chambre, 2017-2018, n° 2648/001, p. 121.

Het staat de nationale wetgever evenwel vrij de verordening door middel van een verwijzing toepasselijk te verklaren. Hij moet er evenwel op toezien dat de bepalingen die niet bedoeld zijn om in het interne recht te worden toegepast, zoals de artikelen 61 en 62 van de AVG, niet toepasselijk worden verklaard.

Artikel 3

Artikel 3 moet worden herzien zodat het niet kan worden geïnterpreteerd als zou het situaties regelen die zich voordoen buiten het grondgebied waarvoor de Belgische Staat bevoegd is, wat met name blijkt uit de woorden “in de Europese Unie”.

Artikel 5

De AVG is, gelet op haar werkingssfeer, rechtstreeks toepasselijk ten aanzien van titel 1 van de ontworpen wet en vormt een hogere norm die de Belgische Staat moet naleven. Wat die titel 1 betreft, kan dus niet worden bepaald dat de definities van de AVG “[o]nverminderd de definities bepaald in deze wet” van toepassing zijn.

TITEL 1

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

Artikel 6

Aangezien artikel 2, derde lid, van het voorontwerp bepaalt dat “[d]e [AVG] (…) niet van toepassing [is] op de verwerkingen bedoeld in de titels 2 en 3 van deze wet”, en aangezien artikel 6, volgens wat in het artikel zelf staat, enkel op titel 1 van het voorontwerp betrekking heeft, hoeft niet te worden gepreciseerd dat titel 1 uitvoering geeft aan de AVG “met uitzondering van de verwerkingen bedoeld in de titels 2 en 3”.

Aan de AVG wordt trouwens niet alleen door titel 1 maar ook door de titels 4 tot 8 van het voorontwerp uitvoering verleend; ook in die laatstgenoemde titels zou dus moeten worden vermeld dat ze met name de AVG ten uitvoer leggen.

Artikel 7

De steller van het voorontwerp wordt erop gewezen dat, gelet op de criteria inzake territoriale binding vermeld in artikel 4, de bepaling niet van toepassing zal zijn op de verwerking van persoonsgegevens van kinderen door verwerkingsverantwoordelijken die in andere lidstaten van de Europese Unie gevestigd zijn.

Artikel 8

1. Artikel 8 wordt aangenomen op basis van artikel 9, lid 2, g), van de AVG, waarin wordt bepaald dat het verbod op de verwerking van de gevoelige gegevens die in lid 1 van die

Il est en revanche loisible au législateur national de déclarer le règlement applicable par référence. Il prendra toutefois soin de ne pas rendre applicable les dispositions telles que les articles 61 et 62 du RGPD, qui n’ont pas vocation à s’appliquer en droit interne.

Article 3

L’article 3 doit être revu de manière à éviter qu’il soit lu comme réglant des situations sortant du cadre territorial pour lequel l’État belge est compétent, ce qui ressort notamment des mots “au sein de l’Union européenne”.

Article 5

Compte tenu de son champ d’application, le RGPD est directement applicable à l’égard du titre 1er de la loi en projet et constitue une norme supérieure dont le respect s’impose à l’État belge. En ce qui concerne ce titre 1er, il ne peut dès lors pas être prévu que les définitions du RGPD s’appliquent “sans préjudice des définitions prévues dans la présente loi”.

TITRE 1ER

De la protection des personnes physiques a l’égard du traitement des données à caractère personnel

Article 6

Dès lors que l’article 2, alinéa 3, de l’avant-projet prévoit que “le [RGPD] ne s’applique pas aux traitements visés aux titres 2 et 3 de la présente loi” et que l’article 6 ne concerne, selon son énoncé même, que le titre 1er de l’avant-projet, il n’est pas nécessaire de préciser que c’est “à l’exception des traitements visés aux titres 2 et 3” que le titre 1er exécute le RGPD.

Par ailleurs, celui-ci est exécuté non seulement par le titre 1er de l’avant-projet mais également par ses titres 4 à 8, lesquels devraient donc également préciser qu’ils exécutent notamment le RGPD.

Article 7

L’attention de l’auteur de l’avant-projet est attirée sur le fait que, compte tenu des critères de rattachement territoriaux de l’article 4, la disposition ne sera pas applicable aux traitements de données à caractère personnel d’enfants par des responsables de traitement établis dans d’autres États membres de l’Union européenne.

Article 8

1. L’article 8 est adopté sur la base de l’article 9, paragraphe 2, g), du RGPD, qui prévoit que l’interdiction du traitement des données sensibles mentionnées au

laatstgenoemde bepaling worden vermeld, niet geldt indien de volgende voorwaarde is vervuld:

"g) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene".

Overeenkomstig die bepaling moet de lidstaat die zich op die bepaling wil beroepen, voorzien in "passende en specifieke maatregelen (…) ter bescherming van de grondrechten en de fundamentele belangen" van de betrokkenen.

Dergelijke garanties zijn bijzonder belangrijk wanneer het gaat om een afwijking van het principiële verbod op de verwerking van gevoelige persoonsgegevens.

Wat betreft de verenigingen of instellingen ter verdediging van de rechten van de mens en van de fundamentele vrijheden, wordt momenteel in waarborgen voorzien bij artikel 6, § 2, k), van de wet van 8 december 1992 "tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van de persoonsgegevens", dat een specifieke machtiging bij een koninklijk besluit vereist, dat is vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Wat betreft de verenigingen en instellingen ter evaluatie, begeleiding en behandeling van personen van wie het seksuele gedrag gekwalificeerd kan worden als een misdrijf, wordt momenteel in waarborgen voorzien bij artikel 6, § 3, van de wet van 8 december 1992. Die bepaling schrijft voor dat (1) een individuele machtiging wordt verleend bij een koninklijk besluit dat is vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, (2) in de machtiging de duur van de machtiging, de nadere regels voor de controle door de bevoegde overheid en de wijze waarop deze over de verwerking wordt geïnformeerd worden gepreciseerd, (3) de verwerking beperkt wordt tot de persoonsgegevens betreffende het seksuele leven.

Wat betreft de "Stichting voor vermiste en seksueel uitgebuite kinderen" wordt momenteel in dergelijke waarborgen voorzien bij artikel 3, § 6, van de wet van 8 december 1992. Die bepaling schrijft het volgende voor:

— er moet een specifieke machtiging worden verleend bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, waarin de duur en de voorwaarden van de machtiging worden gepreciseerd;

— de personeelsleden en degenen die voor het Centrum persoonsgegevens verwerken zijn gebonden door het beroepsgeheim, waarvan de niet-inachtneming wordt bestraft bij artikel 458 van het Strafwetboek;

paragraphe 1er de cette dernière disposition ne s'applique pas si la condition suivante est remplie:

"g) le traitement est nécessaire pour des motifs d'intérêt public importants, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée".

Conformément à cette disposition, l'État membre qui entend s'autoriser de cette disposition doit prévoir des "mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts" des personnes concernées.

S'agissant d'une dérogation à l'interdiction de principe du traitement des données à caractère personnel sensibles, de telles garanties revêtent une importance toute particulière.

En ce qui concerne les associations ou les établissements de défense et de promotion des droits de l'homme et des libertés fondamentales, les garanties sont actuellement prévues par l'article 6, § 2, k), de la loi du 8 décembre 1992 "relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel", qui impose une autorisation spécifique accordée par un arrêté royal délibéré en Conseil des ministres et pris après avis de la Commission de la protection de la vie privée.

En ce qui concerne les associations et établissements d'évaluation, de guidance et de traitement des personnes dont le comportement sexuel peut être qualifié d'infraction, des garanties sont actuellement prévues par l'article 6, § 3, de la loi du 8 décembre 1992. Cette disposition impose (1) une autorisation individuelle accordée par un arrêté royal délibéré en Conseil des ministres et pris après avis de la Commission de la protection de la vie privée; (2) l'autorisation doit préciser la durée de l'autorisation, les modalités de contrôle par l'autorité compétente et la façon dont celle-ci sera informée des traitements; (3) la limitation du traitement aux données à caractère personnel concernant la vie sexuelle.

En ce qui concerne la "Fondation pour Enfants Disparus et Sexuellement Exploités", de telles garanties sont actuellement prévues par l'article 3, § 6, de la loi du 8 décembre 1992. Cette disposition impose:

— une autorisation spécifique accordée par un arrêté royal délibéré en Conseil des ministres et pris après avis de la Commission de la protection de la vie privée, cette autorisation devant préciser la durée et les conditions de l'autorisation;

— la soumission des membres du personnel et ceux qui traitent des données à caractère personnel pour le Centre à une obligation de secret professionnel sanctionnée par l'article 458 du Code pénal;

— het is verboden om een bestand bij te houden betreffende personen die ervan verdacht worden een misdaad of wanbedrijf te hebben begaan of van veroordeelde personen;

— het is verboden om telefoongesprekken op te nemen tenzij de oproeper hierover geïnformeerd wordt en voor zover hij zich daartegen niet heeft verzet.

Het voorontwerp neemt echter geen enkele van die waarborgen over.

Bovendien worden de waarborgen waarin artikel 25, 1° tot 3°, van het besluit van 13 februari 2001 voorziet,[10] enkel door artikel 9, § 2, van het voorontwerp overgenomen.

De steller van het voorontwerp moet kunnen aantonen dat het in het licht van het nagestreefde doel noodzakelijk is die waarborgen achterwege te laten. Zo niet moet het dispositief worden herzien zodat het de passende en specifieke maatregelen voorschrijft die artikel 9, lid 2, g), van de AVG vereist, of moet het worden aangevuld met een machtiging van de Koning in die zin.

2. Volgens artikel 8, 3°, vormt een "reden van zwaarwegend algemeen belang" in de zin van artikel 9, lid 2, g), van de AVG:

"de verwerking van persoonsgegevens die het seksuele leven betreffen, verricht door een vereniging met rechtspersoonlijkheid of door een instelling van openbaar nut met als statutair hoofddoel de evaluatie, de begeleiding en de behandeling van personen van wie het seksueel gedrag gekwalificeerd kan worden als een misdrijf en die voor de verwezenlijking van dat doel door de bevoegde overheid worden erkend en gesubsidieerd (…)".

Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer heeft opgemerkt, staat artikel 9, lid 2, h), van de AVG de verwerking van gevoelige persoonsgegevens echter toe wanneer:

"de verwerking (…) noodzakelijk [is] voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten,

[10] "Art. 25. Bij de verwerking van persoonsgegevens bedoeld in de artikelen 6 tot 8 van de wet, moet de verantwoordelijke voor de verwerking bovendien de volgende maatregelen nemen:
1° hij of, in voorkomend geval, de verwerker moet de categorieën van personen die de persoonsgegevens kunnen raadplegen, aanwijzen waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig moet worden omschreven;
2° hij of, in voorkomend geval, de verwerker moet de lijst van de aldus aangewezen categorieën van personen ter beschikking houden van de Commissie;
3° hij moet ervoor zorgen dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken gegevens in acht te nemen;
(…).".

— l'interdiction de tenir un fichier de personnes suspectées d'avoir commis un crime ou un délit ou de personnes condamnées;

— l'interdiction de procéder à l'enregistrement de conversations téléphoniques à moins que l'appelant en ait été informé et dans la mesure où il ne s'y est pas opposé.

Plus aucune de ces garanties n'est cependant reproduite par l'avant-projet.

En outre, les garanties prévues par l'article 25, 1° à 3°, de l'arrêté du 13 février 2001 [10] ne sont reprises que par l'article 9, § 2, de l'avant-projet.

L'auteur de celui-ci doit être en mesure de justifier la nécessité de supprimer ces garanties au regard de l'objectif poursuivi. À défaut, le dispositif sera revu afin de prévoir les mesures appropriées et spécifiques requises par l'article 9, paragraphe 2, g), du RGPD, ou complété par une habilitation permettant au Roi d'agir en ce sens.

2. L'article 8, 3°, prévoit que constitue un "motif d'intérêt public important" au sens de l'article 9, paragraphe 2, g), du RGPD

"le traitement de données à caractère personnel concernant la vie sexuelle, effectuée par une association dotée de la personnalité juridique ou par un établissement d'utilité publique, qui a pour objet statutaire principal l'évaluation, la guidance et le traitement des personnes dont le comportement sexuel peut être qualifié d'infraction, et qui est agréé et subventionné par l'autorité compétente en vue de la réalisation de ce but […]".

Or, comme le relève la Commission de la protection de la vie privée, l'article 9, paragraphe 2, h), du RGPD autorise le traitement des données à caractère personnel sensibles lorsque

"le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État

[10] "Art. 25. Lors du traitement de données à caractère personnel visées aux articles 6 à 8 de la loi, le responsable du traitement doit prendre les mesures supplémentaires suivantes:
1° les catégories de personnes, ayant accès aux données à caractère personnel, doivent être désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;
2° la liste des catégories des personnes ainsi désignées doit être tenue à la disposition de la Commission par le responsable du traitement ou, le cas échéant, par le sous-traitant;
3° il doit veiller à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées;
[…]".

op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen".

Daar de verwerking waarin artikel 8, 3°, voorziet, wordt vermeld in de uitzondering bepaald bij artikel 9, lid 2, h), van de AVG, moet naar die laatstgenoemde onderverdeling in plaats van naar artikel 9, lid 2, g), van de AVG worden verwezen.

Indien, zoals wordt toegestaan bij artikel 9, lid 4, van de AVG, de steller van het voorontwerp extra voorwaarden wenst te bepalen voor dat soort verwerking en aan de Koning een machtiging in die zin wenst te verlenen, moet hij daartoe een passende rechtsgrond vaststellen in een afzonderlijke bepaling.

3. Geen enkele ontworpen bepaling geeft uitvoering aan de mogelijkheid, waarin artikel 9, lid 2, i), van de AVG voorziet, om om "redenen van algemeen belang op het gebied van de volksgezondheid" af te wijken van de algemene regel inzake de verwerking van gevoelige persoonsgegevens op voorwaarde dat "passende en specifieke maatregelen [worden genomen] ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim".

De steller van het voorontwerp moet nagaan of het dispositief wat dat betreft niet moet worden aangevuld.

4. In de wet van 27 juni 1921 "betreffende de verenigingen zonder winstoogmerk, de stichtingen en de Europese politieke partijen en stichtingen" is het begrip "instelling van openbaar nut" vervangen door het begrip "stichting". Artikel 8 moet dan ook in die zin worden herzien.

Artikel 9

1. In de bespreking van artikel 9, § 2, staat het volgende:

"De personen, of de stichting bedoeld in § 1 kunnen niet beschikken over een rechtstreekse toegang of het bekomen van uittreksels van het systeem van de gegevensverwerking in verband met de strafrechtelijke veroordelingen en inbreuken of van de daaraan verbonden veiligheidsmaatregelen. Diezelfde beginselen gelden in het kader van het wetenschappelijk onderzoek".

Een dergelijke onrechtstreekse toegang tot de verwerkte gegevens zou ervoor kunnen zorgen dat de inmenging waarin is voorzien, evenredig is.

Dat principe van onrechtstreekse toegang staat echter niet in het dispositief.

Het dispositief dient dus in dat opzicht te worden aangevuld.

2. De steller van het voorontwerp moet ten aanzien van het grondwettelijke beginsel van gelijkheid en non-discriminatie kunnen motiveren waarom artikel 9, § 1, 4°, enkel melding maakt van "wetenschappelijk onderzoek" en niet van alle verwerkingen die onder titel 4 vallen (onverminderd de hieronder gemaakte opmerkingen in verband met die titel). Zo niet

membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3".

Dès lors que le traitement prévu par l'article 8, 3°, est visé par l'exception prévue à l'article 9, paragraphe 2, h), du RGPD, c'est à cette dernière subdivision qu'il faut se rattacher, et non à l'article 9, paragraphe 2, g), du RGPD.

Si, comme l'y autorise l'article 9, paragraphe 4, du RGPD, l'auteur de l'avant-projet souhaite prévoir des conditions supplémentaires afin d'encadrer ce type de traitement et donner une habilitation au Roi en ce sens, il doit adopter un fondement légal approprié à cette fin dans une disposition distincte.

3. Aucune des dispositions en projet ne met en œuvre la possibilité de dérogations relatives au traitement de données à caractère personnel sensibles pour "des motifs d'intérêt public dans le domaine de la santé publique" prévue par l'article 9, paragraphe 2, i), du RGPD, moyennant l'adoption de "mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel".

L'auteur de l'avant-projet vérifiera que le dispositif ne doit pas être complété à ce sujet.

4. La notion d'"établissement d'utilité publique" ayant été remplacée dans la loi du 27 juin 1921 "sur les associations sans but lucratif, les fondations, les partis politiques européens et les fondations politiques européennes" par celle de "fondation", l'article 8 doit être revu en ce sens.

Article 9

1. Il ressort du commentaire de l'article 9, § 2, que

"les personnes, ou la fondation visées au § 1er, ne peuvent pas disposer d'un accès direct ou d'une remise d'extrait du système de traitement de données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes. Ces mêmes principes valent dans le cadre de la recherche scientifique".

Un tel l'accès indirect aux données traitées serait de nature à garantir la proportionnalité de l'ingérence mise en place.

Cependant, ce principe de l'accès indirect n'apparaît pas dans le dispositif.

Il convient, dès lors, de compléter le dispositif à cet égard.

2. L'auteur de l'avant-projet doit être mesure de justifier, au regard du principe constitutionnel d'égalité et de non-discrimination, les raisons pour lesquelles l'article 9, § 1er, 4°, ne vise que la "recherche scientifique" et non pas l'ensemble des traitements couverts par le titre 4 (sans préjudice des observations formulées ci-dessous à l'égard de ce titre). À défaut,

dienen de woorden “wetenschappelijk onderzoek” te worden vervangen door de woorden “wetenschappelijk, historisch of statistisch onderzoek of met het oog op archivering”, en dient ter wille van de evenredigheid te worden bepaald dat enkel onderzoekers gegevens die in het algemeen belang worden gearchiveerd kunnen verwerken.

Artikelen 10 en 11

1.1. De artikelen 10 en 11 beogen uitvoering te geven aan artikel 23 van de AVG, dat de lidstaten machtigt de reikwijdte te beperken van de rechten en verplichtingen van de betrokkenen waarin de AVG voorziet.

Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer opmerkt, beperkt artikel 10 de rechten van de betrokkene in zeer hoge mate. Wanneer is voldaan aan de voorwaarden die in de paragrafen 1 tot 3 op niet-cumulatieve wijze worden opgesomd en die overeenstemmen met de litterae d), e) en h), van artikel 23, lid 1, van de AVG, zijn de overheden immers gemachtigd om alle rechten vermeld in hoofdstuk III “Rechten van de betrokkene” (artikelen 12 tot 22) van de AVG alsook artikel 34 van dezelfde verordening, betreffende de “mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene” volledig niet-toepasselijk te verklaren.

1.2. Artikel 23 van de AVG maakt het weliswaar mogelijk dat de reikwijdte van de rechten vastgelegd in de artikelen 12 tot 22 en 34 van de AVG wordt beperkt, maar schrijft ook voor dat de lidstaat daartoe het bewijs levert van een gerechtvaardigd doel, in de zin van artikel 23, lid 1, van de AVG, dat “die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is”. Die bepaling moet trouwens strikt worden geïnterpreteerd aangezien ze een afwijkende bepaling is.

Zoals in algemene opmerking 1 is gezegd, moet de steller van het voorontwerp er in dat kader op toezien dat hij een billijk evenwicht tot stand brengt tussen alle rechten en belangen die in het geding zijn.

De uitoefening van de rechten waarin de artikelen 12 tot 22 en 34 van de AVG voorzien, draagt bij tot een dergelijk evenwicht, mede gelet op de inmenging in het recht op eerbiediging van het privéleven die de AVG en de ontworpen wet toestaan.

Het voorontwerp voldoet niet aan het vereiste van evenredigheid waaraan het moet beantwoorden, doordat het de totale uitsluiting (1) mogelijk maakt van alle (2) rechten waarin de artikelen 12 tot 22 en 34 van de AVG voorzien voor categorieën verwerkingen – en onrechtstreeks voor categorieën verwerkingsverantwoordelijken – die zeer ruim worden gedefinieerd (3).

Het noodzakelijkheidsvereiste, vervat in artikel 11, § 1, van het voorontwerp, is ontoereikend om de evenredigheid van de inmenging te waarborgen.

il convient de remplacer les mots “recherche scientifique” par les mots “recherche scientifique, historique ou statistique ou à des fins d’archives” en prévoyant, dans un souci de proportionnalité, que le traitement des données archivées dans l’intérêt du public est limité aux chercheurs.

Articles 10 et 11

1.1. Les articles 10 et 11 entendent mettre en œuvre l’article 23 du RGPD, qui autorise les États membres à limiter la portée des droits et obligations des personnes concernées prévus par le RGPD.

Comme le relève la Commission de la protection de la vie privée, l’article 10 prévoit une limitation extrêmement large des droits de la personne concernée. C’est en effet l’ensemble des droits repris par le chapitre III “Droits de la personne concernée” (articles 12 à 22) du RGPD, ainsi que l’article 34, du même règlement, relatif à la “communication à la personne concernée d’une violation de données à caractère personnel”, que l’on autorise les autorités à rendre inapplicable dans leur entièreté lorsque les conditions énoncées de manière non cumulative par les paragraphes 1 à 3 sont remplies, ces paragraphes correspondant aux litteras d), e) et h), de l’article 23, paragraphe 1er, du RGPD.

1.2. Si l’article 23 du RGPD permet la limitation de la portée des droits prévus par les articles 12 à 22 et 34 du RGPD, il exige également que l’État membre justifie pour ce faire d’un objectif légitime au sens de l’article 23, paragraphe 1er, du RGPD, qu’“une telle limitation respecte l’essence des libertés et droits fondamentaux et qu’elle constitue une mesure nécessaire et proportionnée dans une société démocratique”. Compte tenu de son caractère dérogatoire, cette disposition doit, du reste, faire l’objet d’une interprétation stricte.

Comme évoqué dans l’observation générale n° 1, dans ce cadre, l’auteur de l’avant-projet doit veiller à établir un juste équilibre entre tous les droits et intérêts en cause.

L’exercice des droits prévus par les articles 12 à 22 et 34 du RGPD participe à l’existence d’un tel équilibre au vu des ingérences dans le droit au respect de la vie privée qui sont autorisées par le RGPD et la loi en projet.

En autorisant l’exclusion totale (1) de l’ensemble (2) des droits prévus par les articles 12 à 22 et 34 du RGPD pour des catégories de traitements – et indirectement des catégories de responsables de traitement – définies de manière très large (3), l’avant-projet ne répond pas à l’exigence de proportionnalité qui s’impose à lui.

L’exigence de nécessité contenue à l’article 11, § 1er, de l’avant-projet ne suffit pas à garantir le caractère proportionné de l’ingérence.

Artikel 10 van het voorontwerp is immers te ruim gesteld om een passende afweging mogelijk te hebben kunnen maken van de rechten die in het geding zijn, om ervoor te zorgen dat de rechten van de betrokkenen niet méér worden ingeperkt dan wat strikt noodzakelijk is voor de realisatie van het nagestreefde gerechtvaardigde doel.

Een dergelijke machtiging om beperkingen in te voeren is des te minder aanvaardbaar daar in het kader van titel 2 van het voorontwerp – dat ten aanzien van de rechten van de betrokkenen restrictiever is, gelet op de gevoelige terreinen waarop de gegevensverwerking geschiedt – de betrokkenen in principe een aanzienlijk deel van hun rechten behouden. Die rechten kunnen indien nodig immers enkel worden beperkt indien daartoe specifieke wetsbepalingen worden aangenomen (cf. de artikelen 42, 43 en 44 van het voorontwerp).

1.3. Voorts wordt de periode waarbinnen de rechten en verplichtingen van de betrokkene kunnen worden beperkt, bij artikel 11, § 1, zeer ruim gedefinieerd. De bepaling heeft het namelijk over "de periode waarbinnen de betrokkene deel uitmaakt van een controle, onderzoek, strafrechtelijke vervolging, hierop *voorbereidende handelingen* of procedures in het kader van de uitoefening van wettelijke opdrachten, voor zover de toepassing ervan de behoeften van de controle, het onderzoek, de strafrechtelijke vervolging, de *voorbereidende handelingen* of de procedures zou schaden en zolang vereist ter bescherming van de belangrijke doelstellingen van algemeen openbaar belang, zoals bedoeld in artikel 10, 2°" (eigen cursivering).

Voor zover in de afbakening van de aldus toegestane periode om beperkingen toe te passen, gewag wordt gemaakt van voorbereidende handelingen zonder meer, houdt artikel 11, § 1, een schending van het evenredigheidsbeginsel in.

In dat verband wijst de afdeling Wetgeving op de rechtspraak van het Grondwettelijk Hof in arrest 51/2014 van 27 maart 2014 over een soortgelijke problematiek. Dat arrest gaat over artikel 11 van de wet van 3 augustus 2012 "houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten", waarbij artikel 3, § 7, in de wet van 8 december 1992 is ingevoegd. Het Hof heeft geoordeeld dat die bepaling om de volgende reden ongrondwettig was:

"B.8.5. De bepaling preciseert evenwel niet hoe lang de voorbereidende werkzaamheden die de schorsing van de rechten verantwoorden, kunnen duren. Hieruit kan voortvloeien dat, wanneer die voorbereidende werkzaamheden voortduren of wanneer de belastingadministratie vervolgens geen onderzoek of controle opent, de schorsing van de rechten langer kan duren dan wat strikt noodzakelijk is. In die mate schendt artikel 11 van de wet van 3 augustus 2012 het beginsel van gelijkheid en niet-discriminatie."

Als gevolg van dat arrest is artikel 3, § 7, van de wet van 8 december 1992 gewijzigd zodat het thans stelt dat "[d]e duur van deze voorbereidende werkzaamheden binnen dewelke het genoemde artikel 10 niet van toepassing is, (…) echter niet meer [mag] bedragen dan een jaar vanaf de aanvraag die is ingediend bij toepassing van dat artikel 10" en dat "[d]e Dienst

L'article 10 de l'avant-projet est en effet rédigé de manière trop large pour avoir permis une mise en balance adéquate des droits en présence afin que les limitations apportées aux droits des personnes concernées ne dépassent pas ce qui est strictement nécessaire à la réalisation de l'objectif légitime poursuivi.

Une telle autorisation de limitation est d'autant moins admissible que, dans le cadre du titre 2 de l'avant-projet – qui se veut plus restrictif à l'égard des droits des personnes concernées compte tenu des domaines sensibles dans lesquels le traitement intervient –, les personnes concernées conservent en principe une grande partie de leurs droits, ces derniers ne pouvant être limités, en cas de nécessité, que moyennant l'adoption d'une disposition législative spécifique (cf. articles 42, 43 et 44 de l'avant-projet).

1.3. Par ailleurs, l'article 11, § 1er, prévoit une durée de limitation des droits et obligations de la personne concernée définie de manière très large. Il vise en effet "la période durant laquelle la personne concernée fait l'objet d'un contrôle, d'une enquête, d'une poursuite pénale, d'*actes préparatoires* à ceux-ci ou de procédures dans le cadre de l'exécution de missions légales, dans la mesure où cette application nuirait aux besoins du contrôle, de l'enquête, de la poursuite pénale, des *actes préparatoires* ou des procédures, soit aussi longtemps que la protection d'objectifs importants d'intérêt général visés à l'article 10, 2°, l'exige" (italiques ajoutés).

En ce que la période de limitation qui est ainsi autorisée vise les actes préparatoires sans autre précision, l'article 11, § 1er, porte atteinte au principe de proportionnalité.

La section de législation rappelle à cet égard la jurisprudence de la Cour constitutionnelle dans son arrêt n° 51/2014 du 27 mars 2014 concernant une problématique similaire. Cet arrêt porte sur l'article 11 de la loi du 3 août 2012 "portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions", qui insère l'article 3, § 7, au sein de la loi du 8 décembre 1992. La Cour a considéré que cette disposition était inconstitutionnelle pour le motif suivant:

"B.8.5. Toutefois, la disposition ne précise pas quelle peut être la durée des actes préparatoires justifiant la suspension des droits. Il peut en résulter que, si ces actes préparatoires se prolongent ou si l'administration fiscale n'ouvre pas, ensuite, une enquête ou un contrôle, la suspension des droits peut se prolonger au-delà de ce qui est strictement nécessaire. Dans cette mesure, l'article 11 de la loi du 3 août 2012 viole le principe d'égalité et de non-discrimination".

À la suite de cet arrêt, l'article 3, § 7, de la loi du 8 décembre 1992 a été modifié afin de prévoir que "La durée de ces actes préparatoires pendant laquelle ledit article 10 n'est pas applicable, ne peut excéder un an à partir de la demande introduite en application de cet article 10" et que "Le Service de Sécurité de l'Information et Protection de

voor Informatieveiligheid en Bescherming van de Persoonlijke Levenssfeer (…) de betrokken belastingplichtige onverwijld op de hoogte [brengt] van die opheffing en (…) hem de volledige motivatie [meedeelt] die is opgenomen in de beslissing van de verantwoordelijke van de verwerking die van de uitzondering gebruik heeft gemaakt".[11]

Het ontworpen dispositief moet worden aangevuld zodat daar soortgelijke waarborgen in worden opgenomen.

2. Voorts heeft de lidstaat in het kader van de tenuitvoerlegging van artikel 23 van de AVG de verplichting om specifieke bepalingen vast te stellen betreffende de verschillende punten die in artikel 23, lid 2, van de AVG zijn opgesomd.

Artikel 23, lid 2, f), van de AVG schrijft voor dat specifieke maatregelen moeten worden genomen betreffende "de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking".

Het dispositief moet in die zin worden aangevuld.

Artikel 13

De vraag rijst wat het nut is van artikel 13, eerste lid, rekening houdend met de definitie die in artikel 4, punt 9, van de AVG gegeven wordt van het begrip "ontvanger", die de overheden bedoeld in titel 3 lijkt uit te sluiten.

Artikel 14

1. Voor zover artikel 14, eerste lid, 5°, en derde lid, de uitbreiding toestaat van het toegangsrecht waarin het voorziet middels protocolakkoorden tussen de verwerkingsverantwoordelijken, is dat artikel in strijd met het wettelijkheids- en voorzienbaarheidsvereiste waaraan elke inmenging in het recht op de bescherming van de persoonlijke levenssfeer getoetst dient te worden.

2. Zoals de commissie voor de bescherming van de persoonlijke levenssfeer opmerkt, is artikel 14, laatste lid, niet

[11] Zie in die zin de ontworpen artikelen 100/14, §§ 2, derde lid, en 3, tweede lid, 100/15, §§ 2, derde lid, en 3, tweede lid, 100/16, §§ 2, derde lid, en 3, tweede lid, en 100/17, §§ 2, derde lid, en 3, tweede lid, van het Sociaal Strafwetboek, en de artikelen 11, §§ 2, derde lid, en 3, tweede lid, 11*bis*, §§ 2, derde lid, en 3, tweede lid, 11*ter*, §§ 2, derde lid, en 3, tweede lid, 11*quater*, §§ 2, derde lid, en 3, tweede lid, van de wet van 3 augustus 2012 "houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten", in respectievelijk de artikelen 62, 64, 66, 68, 73, 75, 77 en 79 van het voorontwerp van wet "tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG" dat aan de afdeling Wetgeving van de Raad van State om advies is voorgelegd onder rolnummer 63.202/2.

la Vie Privée en informe le contribuable concerné sans délai et lui communique dans son entièreté la motivation contenue dans la décision du responsable du traitement ayant fait usage de l'exception"[11].

Il convient de compléter le dispositif en projet afin d'y insérer des garanties similaires.

2. L'État membre a par ailleurs l'obligation, dans le cadre de la mise en œuvre de l'article 23 du RGPD, d'adopter des dispositions spécifiques relatives aux différents points listés par l'article 23, paragraphe 2, du RGPD.

L'article 23, paragraphe 2, f), du RGPD impose l'adoption de mesures spécifiques relatives "aux durées de conservation et aux garanties applicables en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement".

Le dispositif sera complété en ce sens.

Article 13

La question se pose de l'utilité de l'article 13, alinéa 1er, compte tenu de la définition qui est donnée à la notion de "destinataire" par l'article 4, point 9, du RGPD, qui paraît exclure les autorités visées au titre 3.

Article 14

1. L'article 14, alinéa 1er, 5°, et alinéa 3, en ce qu'il autorise l'extension du droit d'accès qu'il organise par le biais de protocoles d'accord conclus entre les responsables du traitement, porte atteinte à l'exigence de légalité et de prévisibilité qui sous-tend toute ingérence dans le droit au respect de la vie privée.

2. Comme le relève la Commission de la protection de la vie privée, l'article 14, dernier alinéa, n'est pas admissible en

[11] Voir en ce sens les articles 100/14, §§ 2, alinéa 3, et 3, alinéa 2, 100/15, §§ 2, alinéa 3, et 3, alinéa 2, 100/16, §§ 2, alinéa 3, et 3, alinéa 2, et 100/17, §§ 2, alinéa 3, et 3, alinéa 2, du Code pénal social, et les articles 11, §§ 2, alinéa 3, et 3, alinéa 2, 11*bis*, §§ 2, alinéa 3, et 3, alinéa 2, 11*ter*, §§ 2, alinéa 3, et 3, alinéa 2, 11*quater*, §§ 2, alinéa 3, et 3, alinéa 2, de la loi du 3 août 2012 "portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions", en projet respectivement aux articles 62, 64, 66, 68, 73, 75, 77 et 79 de l'avant-projet de loi "instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE", soumis pour avis à la section de législation du Conseil d'État sous le n° 63.202/2 de son rôle.

toelaatbaar in zoverre daarbij aan de overheid een discretionaire bevoegdheid wordt toegekend inzake het al dan niet toepassen van die bepaling. Overeenkomstig het wettelijkheids- en voorzienbaarheidsvereiste dient in het dispositief zelf gepreciseerd te worden voor welke gegevensbanken de toepassing van artikel 14 niet gerechtvaardigd is of dienen minstens de criteria vastgesteld te worden op basis waarvan de beoordelingsbevoegdheid van de overheid afgebakend kan worden.

Artikelen 15 en 16

1. Artikel 23, lid 2, van de AVG bepaalt dat de specifieke bepalingen met betrekking tot de punten die daarin worden opgelijst, opgenomen dienen te worden in de wet die de afwijkingsmogelijkheid bedoeld in lid 1 van die bepaling ten uitvoer legt. Bijgevolg zijn de artikelen 15, vijfde lid, en 16, vijfde lid, van het voorontwerp niet aanvaardbaar voor zover het daarbij aan de ontvangers overgelaten wordt om "gepaste waarborgen [te] voorzien voor de rechten en vrijheden van de betrokkenen zoals bedoeld in artikel 23.2 van de Verordening".

2. Artikel 16, eerste lid, van het voorontwerp bepaalt dat de beperking van de rechten van de betrokkenen die bij dat artikel wordt ingesteld niet van toepassing is wanneer "(1) de wet hem hiertoe verplicht in het kader van een geschillenprocedure of (2) de betrokken gerechtelijke overheden hem dit toesta[an]".

Gelet op het grondwettelijk beginsel van gelijkheid en non-discriminatie, moet de steller van het voorontwerp bij machte zijn het feit te rechtvaardigen dat artikel 15 niet in een dergelijke bepaling voorziet en zulks des te meer daar een dergelijke regel voorkomt in artikel 18, § 3, in geval van gemeenschappelijke verwerking.

Artikel 18

De bij artikel 18 opgelegde totale beperking van de rechten van de betrokkenen is niet aanvaardbaar wanneer die gegevens rechtstreeks of onrechtstreeks afkomstig zijn van op zijn minst een bevoegde overheid als bedoeld in titel 2, aangezien in het raam van die titel – die gelet op de gevoelige terreinen waarop de verwerking gebeurt, restrictiever is ten aanzien van de rechten van de betrokkenen – de betrokkenen in principe een groot deel van hun rechten behouden. Die rechten kunnen alleen beperkt worden in geval dat het noodzakelijk is en alleen door het vaststellen van een specifieke wettelijke bepaling (cf. artikelen 42, 43 en 44 van het voorontwerp).

Voorts zou het nuttig zijn om in het ontwerp het begrip "gemeenschappelijke verwerking" te definiëren.

Artikel 19

Zoals de commissie voor de bescherming van de persoonlijke levenssfeer opmerkt, moet de maximumtermijn van één maand die aan de verwerkingsverantwoordelijke opgelegd wordt om een ontvangstbewijs te verzenden, ingekort worden aangezien hij bij artikel 12, lid 3, van de AVG verplicht wordt

ce qu'il octroie un pouvoir discrétionnaire à l'autorité quant à l'application ou non de cette disposition. Conformément à l'exigence de légalité et de prévisibilité, il convient de préciser dans le dispositif lui-même les banques de données pour lesquels l'application de l'article 14 ne se justifie pas ou, à tout le moins, de fixer les critères permettant d'encadrer le pouvoir d'appréciation de l'autorité.

Articles 15 et 16

1. L'article 23, paragraphe 2, du RGPD exige que les dispositions spécifiques relatives aux points qu'il liste soient prévues par la loi qui met en œuvre la faculté de dérogation prévue par le paragraphe 1er de cette disposition. Par conséquent, les articles 15, alinéa 5, et 16, alinéa 5, de l'avant-projet ne peuvent pas être admis dans la mesure où ils laissent aux destinataires le soin de définir "les garanties appropriées pour les droits et libertés des personnes concernées, telles que visées par l'article 23.2 du Règlement".

2. L'article 16, alinéa 1er, de l'avant-projet prévoit que la limitation des droits des personnes concernées qu'il instaure n'est pas applicable lorsque "(1) la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que (2) les autorités judiciaires concernées ne l'y autorise[nt]".

Compte tenu du principe constitutionnel d'égalité et de non-discrimination, l'auteur de l'avant-projet doit être en mesure de justifier le fait qu'une disposition similaire n'est pas prévue à l'article 15 et ce, d'autant plus qu'une telle règle figure à l'article 18, § 3, en cas de traitement commun.

Article 18

La limitation totale apportée aux droits des personnes concernées par l'article 18 n'est pas admissible lorsque ces données émanent directement ou indirectement d'au moins une autorité compétente du titre 2 dès lors que, dans le cadre de ce dernier – qui se veut plus restrictif à l'égard des droits des personnes concernées compte tenu des domaines sensibles dans lesquels le traitement intervient –, les personnes concernées conservent en principe une grande partie de leurs droits. Ceux-ci ne peuvent être limités qu'en cas de nécessité et uniquement moyennant l'adoption d'une disposition législative spécifique (cf. articles 42, 43 et 44 de l'avant-projet).

Par ailleurs, il serait utile de définir dans le projet la notion de "traitement commun".

Article 19

Comme le relève la Commission de la protection de la vie privée, le délai maximum d'un mois qui est imposé au responsable du traitement pour envoyer un accusé de réception doit être réduit dès lors que l'article 12, paragraphe 3, du RGPD lui impose d'informer la personne concernée des mesures

de betrokkene in te lichten over de maatregelen die genomen zijn als gevolg van diezelfde verzoeken binnen een termijn van één maand na de ontvangst ervan.

Artikel 21

1. In de voorliggende bepaling worden de begrippen "overheidsinstantie" en "openbaar orgaan" gedefinieerd. Het definiëren ervan is in het interne recht immers vereist, aangezien de AVG voorziet in maatregelen die specifiek de "overheidsinstanties" en de "overheidsorganen" beogen,[12] zonder dat die begrippen in de verordening gedefinieerd worden. De Groep Gegevensbescherming Artikel 29 bevestigt in zijn "Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO)" dat die begrippen gedefinieerd moeten worden rekening houdend met het nationaal recht.[13]

Toch is de definitie van die begrippen enkel van toepassing op afdeling 2 van hoofdstuk IV van titel 1 van het voorontwerp. Ze kan dus geen betrekking hebben op de begrippen "overheidsinstantie" en "openbaar orgaan", die elders voorkomen in de tekst (bijvoorbeeld in artikel 234, § 2, dat de administratieve geldboeten betreft en opgenomen is in titel 6).

Bijgevolg dienen de begrippen "overheidsinstantie" en "openbaar orgaan" gedefinieerd te worden in de voorafgaande titel van de tekst, bijvoorbeeld in artikel 5, waarin verwezen wordt naar de definities van de AVG.

2. Ter wille van de leesbaarheid van de tekst zouden die twee begrippen samengevoegd moeten worden in een enkele generieke term, naar het voorbeeld van de term "overheid", zoals die gedefinieerd is in de wet van 4 mei 2016 "inzake het hergebruik van overheidsinformatie".

3. Luidens de memorie van toelichting vallen de "autonome overheidsbedrijven bedoeld in de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven niet onder de begrippen "overheidsinstantie" en "openbaar orgaan", zonder dat daarvoor een reden wordt opgegeven.

Wanneer een autonoom overheidsbedrijf de opdrachten van openbare dienst vervult waarmee het belast is, kan het ook beschouwd worden als "een overheidsinstelling of een privaat- of publiekrechtelijke instelling die een openbare dienst verleent".

Bij gebrek aan een objectieve en redelijke rechtvaardiging ervoor, is een dergelijke uitzondering overigens niet toelaatbaar.

[12] Men denke inzonderheid aan de verplichting om een functionaris voor gegevensbescherming aan te wijzen (artikel 37, lid 1, a), van de AVG) en aan de mogelijkheid voor een lidstaat te bepalen dat de administratieve geldboeten niet van toepassing zijn op die overheden (artikel 83, lid 7, van de AVG).

[13] Groep Gegevensbescherming Artikel 29, Richtlijnen voor functionarissen voor gegevensbescherming, WP 243 rev.01, 13 december 2016.

prises suite à ces mêmes demandes dans un délai d'un mois à compter de leur réception.

Article 21

1. La disposition à l'examen définit les notions d'"autorité publique" et d'"organisme public". Cette définition est en effet requise en droit interne puisque le RGPD organise des mesures qui visent spécifiquement les "autorités publiques" et les "organismes publics"[12], sans toutefois définir ces notions. Dans ses "lignes directrices concernant les délégués à la protection des données (DPD)", le Groupe de travail "Article 29" sur la protection des données affirme que ces notions doivent être définies "en fonction du droit national"[13].

Néanmoins, la définition de ces notions ne s'applique qu'à la section 2 du chapitre IV du titre 1er de l'avant-projet. Elle ne peut donc s'appliquer aux termes "autorité publique" et "organisme public" figurant ailleurs dans le texte (par exemple, à l'article 234, § 2, qui concerne les sanctions administratives et qui figure dans le titre 6).

Il convient dès lors de définir les notions d'"autorité publique" et d'"organisme public" dans le titre préliminaire du texte, par exemple à l'article 5, qui évoque les définitions du RGPD.

2. Par souci de lisibilité du texte, ces deux notions devraient être reprises en un seul terme générique. Elles pourraient s'inspirer du terme "autorité publique", telle qu'elle est définie dans la loi du 4 mai 2016 "relative à la réutilisation des informations du secteur public".

3. L'exposé des motifs exclut de la notion d'"autorité publique" et d'"organisme public", et ce, sans motif, les "entreprises publiques autonomes visées dans la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques".

Lorsqu'elle accomplit les missions de service public dont elle a la charge, une entreprise publique autonome peut également être qualifiée d'"institution publique ou [d]'institution de droit privé ou de droit public qui fournit un service public".

Du reste, à défaut de justification objective et raisonnable qui fonde une telle exception, celle-ci ne peut valoir.

[12] On pense notamment à l'obligation de désigner un délégué à la protection des données (article 37, paragraphe 1, a), du RGPD) et à la possibilité pour l'État membre de prévoir que les amendes administratives ne sont pas applicables à ces autorités (article 83, paragraphe 7, du RGPD).

[13] Groupe de travail "Article 29" sur la protection des données, Lignes directrices concernant les délégués à la protection des données, WP 243 rev. 01, 13 décembre 2016.

Artikel 22

1. Artikel 22 organiseert de doorgifte van de persoonsgegevens van de burgers tussen overheidsinstanties waarbij aan die instanties de mogelijkheid wordt geboden die doorgifte te formaliseren aan de hand van een protocol gesloten tussen de overheidsinstantie die de gegevens doorgeeft en die welke ze ontvangt.

Die mogelijkheid om protocollen op te maken, vervangt het toezicht dat tot nu toe uitgeoefend werd door de sectorale comités die binnen de Commissie voor de bescherming van de persoonlijke levenssfeer opgericht waren. Die comités konden de doorgifte van gegevens tussen overheidsinstanties toestaan of weigeren. Dat toezichtmechanisme is opgeheven bij de wet van 3 december 2017.

2. Er dient benadrukt te worden dat de doorgifte van gegevens tussen overheidsinstanties niet onbelangrijk is. Het bijzondere aan de Belgische administratie is dat ze onder andere gebaseerd is op het beginsel van de eenmalige gegevensinzameling van de persoonsgegevens (het zogeheten "*only-oncebeginsel*"): wanneer een burger een gegeven verstrekt heeft aan een administratie, mag dat gegeven hem in principe niet meer opnieuw gevraagd worden, en wanneer een overheidsinstantie een gegeven nodig heeft waarover ze niet beschikt, is ze verplicht dat op te vragen bij de administratie die dat gegeven bewaart in een authentieke gegevensbron en niet bij de burger. Verscheidene wetten maken dat systeem van onrechtstreekse inzameling verplicht voor de Belgische overheden.[14] Bijgevolg is de doorgifte van gegevens tussen overheidsinstanties de regel en is het hergebruik van de gegevens maximaal.

De wetgever moet het kader voor die doorgiften zeer nauwkeurig afbakenen om niet het risico te lopen opnieuw een situatie te creëren zoals die bestond vóór het toezicht door de sectorale comités. Bij gebrek aan een duidelijke procedure en aan toezicht op de doorgifte van gegevens binnen de administratie gebeurde het destijds regelmatig dat de personeelsleden van de administratie elkaar belden en afspraken om per mail de gegevens uit te wisselen die ze nodig hadden om hun opdrachten te vervullen. Die doorgiften van gegevens ontsnapten aan elke juridische toetsing en vonden plaats in de grootste ondoorzichtigheid. Het kan niet de bedoeling zijn dat het ontbreken van de verplichting om de doorgiften van gegevens te formaliseren in een protocol, in combinatie met het niet opleggen van geldboeten aan de overheidssector (zoals beoogd in artikel 234, § 2, van het voorontwerp), ertoe leidt dat een situatie ontstaat zoals die van weleer. Dat zou een serieuze stap achterwaarts betekenen op het vlak van de bescherming van de persoonlijke levenssfeer van de burgers. De wetgever moet dus een procedure organiseren die garandeert dat elke doorgifte van gegevens tussen overheidsinstanties getoetst wordt aan de juridisch bakens waarvan hierna sprake is en op adequate wijze bekendgemaakt wordt.

3. Het doorgeven van gegevens van een overheidsinstantie aan een andere is een vorm van inmenging in het recht

[14] Zie inzonderheid artikel 8 van de wet van 15 augustus 2012 "houdende oprichting en organisatie van een federale dienstenintegrator".

Article 22

1. L'article 22 organise le transfert des données à caractère personnel des citoyens entre les autorités publiques en prévoyant la possibilité pour ces dernières de formaliser le transfert de données dans un protocole conclu entre l'autorité publique qui transfère les données et l'autorité publique qui les reçoit.

Cette possibilité de rédiger des protocoles remplace le contrôle jusqu'ici effectué par les comités sectoriels institués au sein de la Commission de la protection de la vie privée chargés d'autoriser ou de refuser les transferts de données entre autorités publiques. Ce mécanisme de contrôle a été supprimé par la loi du 3 décembre 2017.

2. Il y a lieu de souligner que le transfert de données entre autorités publiques n'est pas anecdotique. L'administration belge présente la particularité d'être fondée notamment sur le principe de la collecte unique des données à caractère personnel (principe dit "*only once*"): lorsque le citoyen a fourni une donnée à une administration, cette donnée ne peut en principe plus lui être demandée à nouveau et, lorsqu'une autorité publique a besoin d'une donnée dont elle ne dispose pas, elle est contrainte de la demander non pas au citoyen mais à l'administration qui la détient dans une source authentique de données. Plusieurs lois imposent ce système de collecte indirecte aux autorités publiques[14]. Par conséquent, le transfert de données entre autorités publiques est la règle et la réutilisation des données est maximale.

Ces transferts doivent être scrupuleusement encadrés par le législateur pour ne pas risquer de recréer la situation antérieure à celle du contrôle des comités sectoriels. À l'époque, à défaut de procédure claire et de contrôle encadrant les transferts de données dans l'administration, il arrivait régulièrement que, pour obtenir les données dont ils avaient besoin pour accomplir leurs missions, les agents de l'administration se téléphonent et s'accordent sur l'envoi par courriel des données concernées. Ces transferts de données se faisaient en dehors de l'examen de toute règle juridique et en toute opacité. Il ne faudrait pas que l'absence d'obligation de formaliser, dans un protocole, les transferts de données, combinée à l'absence d'amende applicables au secteur public (comme l'envisage l'article 234, § 2 de l'avant-projet), aboutisse à recréer une situation semblable à celle de jadis. Il s'agirait d'un grave retour en arrière sur le plan de la protection de la vie privée des citoyens. Le législateur doit donc organiser une procédure qui garantit que chaque transfert de données entre autorités publiques fera l'objet d'un examen au regard des balises juridiques dont il est question ci-après, ainsi que d'une publicité adéquate.

3. Un transfert de données d'une autorité publique à une autre constitue une ingérence dans le droit à la protection

[14] Voir notamment l'article 8 de la loi du 15 août 2012 "relative à la création et à l'organisation d'un intégrateur de services fédéral".

op de bescherming van de persoonlijke levenssfeer van de betrokkenen. Krachtens artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 22 van de Grondwet, zoals dat wordt geïnterpreteerd in de vaste rechtspraak van het Grondwettelijk Hof, moet een dergelijke inmenging inzonderheid een wettelijke grondslag hebben, evenredig zijn ten opzichte van de nagestreefde doelstelling en op voldoende duidelijke wijze georganiseerd zijn opdat ze voorzienbaar is voor de burger.

Artikel 6 van de AVG bevestigt dat voorzienbaarheidsvereiste voor de gegevensverwerking in de overheidssector en legt bijzondere vereisten op wanneer "de verwerking […] noodzakelijk [is] om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust" (artikel 6, paragraaf 1, c)) en wanneer "de verwerking […] noodzakelijk [is] voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen" (artikel 6, paragraaf 1, e)). Het bepaalt dat, in die twee gevallen, de "rechtsgrond voor de […] verwerking moet worden vastgesteld bij: a) Unierecht; of b), lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is". En dat het "doel van de verwerking […] in die rechtsgrond vastgesteld [wordt] of […] met betrekking tot de in lid 1, punt e), bedoelde verwerking noodzakelijk [is] voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend".

4. Hoewel het protocol, uit het oogpunt van de evenredigheid van de gegevensdoorgifte, beschouwd kan worden als een nuttige procedurele waarborg – aangezien de verwerkingsverantwoordelijken daardoor geval per geval moeten nagaan of de vereisten die van toepassing zijn op de beoogde gegevensdoorgiften in acht worden genomen en de bakens voor die doorgifte uitdrukkelijk moeten vaststellen en dat daardoor ook de gegevensverwerking binnen de administratie transparanter zal kunnen worden – beantwoordt de regeling van die kwestie in het voorontwerp niet aan het wettelijkheidsvereiste aangezien, enerzijds, het protocol niet verplicht gemaakt wordt, terwijl het dat wel zou moeten zijn en dat, anderzijds, de verschillende elementen waarop die protocollen betrekking zouden moeten hebben niet op voldoende duidelijke wijze vermeld worden in het voorontwerp.

De inhoud van het protocol moet inderdaad verfijnd worden. Dat ligt overigens in lijn van de mogelijkheid die bij artikel 6, lid 3, tweede alinea, van de AVG wordt gecreëerd en waarbij aangegeven wordt dat de "rechtsgrond [die ten grondslag ligt aan de gegevensdoorgift] […] specifieke bepalingen [kan] bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, […]".

In punt 1 schrijve men "de identificatie van de overheidsinstantie die de gegevens doorgeeft alsook van die welke

de la vie privée des personnes concernées. En vertu de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, tel qu'interprété par une jurisprudence constante de la Cour constitutionnelle, pareille ingérence doit notamment reposer sur une base légale, être proportionnée par rapport à l'objectif poursuivi et être organisée de manière suffisamment précise pour être prévisible pour le citoyen.

Confirmant cette exigence de prévisibilité pour les traitements de données dans le secteur public, l'article 6 du RGPD impose des exigences particulières lorsque "le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis" (article 6, paragraphe 1er, c)) et lorsque "le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement" (article 6, paragraphe 1er, e)). Il impose que, dans ces deux hypothèses, "le fondement du traitement […] [soit] défini par a) le droit de l'Union; ou b), le droit de l'État membre auquel le responsable du traitement est soumis". Et que "les finalités du traitement [soient] définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1er, e), [soient] nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement".

4. S'il est vrai que, du point de vue de la proportionnalité du transfert de données, le protocole peut être considéré comme une garantie procédurale utile étant donné qu'il amène les responsables de traitements à examiner au cas par cas le respect des exigences applicables aux transferts de données envisagés et à fixer explicitement les balises du transfert et que, de cette manière également, la transparence des traitements de données dans l'administration pourra être renforcée, le règlement de cette question par l'avant-projet ne satisfait pas à l'exigence de légalité dès lors, d'une part, que le protocole n'est pas rendu obligatoire alors qu'il devrait l'être et que, d'autre part, l'avant-projet n'énonce pas, de manière suffisamment précise, les différents éléments sur lesquels doivent porter ces protocoles.

En effet, le contenu du protocole doit être affiné. Cela s'inscrit d'ailleurs dans la lignée de la possibilité organisée par l'article 6, paragraphe 3, second alinéa, du RGPD, qui affirme que la "base juridique [qui fonde le transfert de données] peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, […]".

Au point 1, il convient d'écrire "l'identification de l'autorité publique qui transfère les données et de celle qui les reçoit"

ze ontvangt" of "of de identificatie van de overheidsinstantie waarvan de gegevens uitgaan en de identificatie van de overheidsinstantie waarvoor de gegevens bestemd zijn".

In punt 2 schrijve men "de identiteit van de verwerkingsverantwoordelijke bij de overheidsinstantie die de gegevens doorgeeft en de identiteit van de verwerkingsverantwoordelijke bij de instantie die ze ontvangt".

In punt 3 schrijve men "de identiteit van de functionaris voor gegevensbescherming van de overheidsinstantie die de gegevens doorgeeft en de identiteit van de functionaris voor gegevensbescherming van de overheidsinstantie die ze ontvangt".

In punt 4 schrijve men "het doeleinde of de doeleinden waarvoor de gegevens doorgegeven worden, dat/die een doel op zich moet(en) vormen en niet beperkt mag/mogen zijn tot de vermelding "uitoefening van de wettelijke opdrachten van de overheidsinstantie"".

In punt 5 schrijve men "de categorie of de categorieën van doorgegeven gegevens, alsook het formaat ervan".[15]

In punt 6 schrijve men "de categorie of de categorieën van ontvangers van gegevens".

In punt 7 schrijve men "de wettelijke grondslag voor de doorgifte van gegevens en de wettelijke grondslag voor de ontvangst ervan".

In punt 9 schrijve men "de gepaste beveiligingsmaatregelen om de gegevensdoorgifte in kwestie te beveiligen", zoals onderstreept door de Commissie voor de bescherming van de persoonlijke levenssfeer.

In punt 10 dient de opmerking van de Commissie voor de bescherming van de persoonlijke levenssfeer gevolgd te worden en dient die precisering dus geschrapt te worden.

Punt 11 zou men zo kunnen begrijpen dat aan de hand van het protocol in kwestie de rechten van de betrokkenen beperkt kunnen worden. Dat is onmogelijk, aangezien alleen de wetgever bevoegd is zulks te doen, met inachtneming van artikel 23 van de AVG. De bepaling dient geherformuleerd te worden door in punt 11 te schrijven "de wettelijke beperking(en) die toepasselijk is/zijn op de rechten van de betrokkenen en de rechtvaardiging van de toepassing ervan ter zake".

Ook dienen de door de Commissie voor de bescherming van de persoonlijke levenssfeer vermelde punten toegevoegd te worden, namelijk:

"1- De beschrijving van de precieze doeleinden waarvoor de gegevens oorspronkelijk werden ingezameld door de

[15] Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer aangeeft, volstaat de vermelding "ja-nee" wanneer het erom gaat te weten te komen of een bepaalde persoon een inkomen ontvangt onder een bepaalde drempel (voor de toekenning van een toelage bijvoorbeeld). Het is niet nodig om het exacte bedrag van het ontvangen inkomen door te geven.

ou "l'identification de l'autorité publique émettrice des données et celle de l'autorité publique destinataire de celles-ci".

Au point 2, il convient d'écrire "l'identité du responsable de traitement au sein de l'autorité publique qui transfère les données et l'identité du responsable de traitement au sein de l'autorité qui les reçoit".

Au point 3, il convient d'écrire "l'identité du délégué à la protection des données de l'autorité publique qui transfère les données et l'identité du délégué à la protection des données de l'autorité publique qui les reçoit".

Au point 4, il convient d'écrire "la ou les finalités pour laquelle/lesquelles les données sont transférées, qui doivent constituer une fin en soi, et ne pas se limiter à la mention "exercice des missions légales de l'autorité publique"".

Au point 5, il convient d'écrire "la ou les catégories de données transférées ainsi que leur format"[15].

Au point 6, il convient d'écrire "la ou les catégories de destinataires de données".

Au point 7, il convient d'écrire "la base légale qui fonde le transfert de données et la base légale qui en fonde la réception".

Au point 9, il convient d'écrire "les mesures de sécurité propres à sécuriser le transfert de données concerné", comme le souligne la Commission de la protection de la vie privée.

Au point 10, il y a lieu de suivre la remarque de la Commission de la protection de la vie privée et de supprimer cette précision.

À la lecture du point 11, on pourrait comprendre qu'une restriction des droits des personnes concernées peut être organisée par ledit protocole. C'est une chose impossible puisque seul le législateur est compétent pour ce faire, dans le respect de l'article 23 du RGPD. Il convient de reformuler la disposition en indiquant au point 11 "la ou les restriction(s) légale(s) applicable(s) aux droits des personnes concernées et la justification de leur application en l'espèce".

Il convient d'ajouter également les points mentionnés par la Commission de la protection de la vie privée à savoir:

"1- La description des finalités précises pour lesquelles les données ont été collectées à l'origine par l'organisme

[15] Comme l'indique la Commission de la protection de la vie privée, lorsqu'il s'agit de savoir si telle personne perçoit un revenu en dessous de tel seuil (pour l'octroi d'une allocation, par exemple), une mention "oui-non" suffit. Il n'est pas nécessaire de transférer le montant du revenu exact perçu.

voormelde openbare of private instelling, beheerder van de geraadpleegde gegevensbron;

2- Ingeval van latere verwerking[16] van de ingezamelde gegevens, vermelding van de verenigbaarheidsanalyse van de doeleinden van deze verwerking met het doeleinde waarvoor de gegevens aanvankelijk zijn verzameld overeenkomstig artikel 6.4 van de AVG;

3- Controle op de naleving van het beginsel "inzameling bij de authentieke gegevensbron" die de kwaliteit van de gegevens garandeert alsook de eerbiediging van het wettelijk kader dat de toegang tot de authentieke bron regelt;

4- Alle specifieke maatregelen die de gegevensflux omkaderen conform het proportionaliteitsbeginsel en de vereisten inzake gegevensbescherming by design en default (keuze van het formaat van de mededeling, logging van de toegangen zodat men kan controleren wie wanneer toegang had tot welke gegevens en waarom, invoering van een verwijzingsrepertorium ingeval van automatische mededeling van de wijzigingen aan de gegevens om zich ervan te verzekeren dat enkel de noodzakelijke gegevens worden bijgewerkt en dit voor de nodige termijn, …)".

5. Artikel 22, § 2, dient eveneens geherformuleerd te worden als volgt:

"Het protocol wordt afgesloten nadat de verwerkingsverantwoordelijken het advies ingewonnen hebben van de functionaris voor gegevensbescherming van de overheidsinstantie die de gegevens doorgeeft en van de functionaris voor gegevensbescherming van de overheidsinstantie die ze ontvangt. Die adviezen worden als bijlage bij het protocol gevoegd. Wanneer minstens één van die adviezen niet gevolgd wordt door de verwerkingsverantwoordelijken, moet(en) in de voorafgaande bepalingen van het protocol de reden(en) vermeld worden waarom dat advies of die adviezen niet gevolgd is/zijn.".

6. Aangezien bij die protocollen een inmenging in de persoonlijke levenssfeer georganiseerd wordt, moeten die protocollen krachtens artikel 22 van de Grondwet toegankelijk zijn voor de betrokkenen, zodat de voorzienbaarheid van de doorgiften en van de verwerkingen gewaarborgd wordt. Het protocol wordt evenwel niet bekendgemaakt, in tegenstelling tot de wet die er de rechtsgrond van vormt, welke wet, uiteraard, niet de in het protocol vervatte essentiële elementen van de doorgifte bevat.

Het is dan ook noodzakelijk dat die protocollen bekendgemaakt worden.

7. De wetgever moet rekening houden met de mogelijkheid dat de verwerkingsverantwoordelijken het niet eens raken over de gegevensdoorgifte en over de inhoud van het protocol.

[16] *Voetnoot 48 van het geciteerde advies*: Gebruik van de gegevens voor (een) ander(e) doeleinde(n) dan waarvoor de gegevens oorspronkelijk werden ingezameld door de overheid of openbare instelling die de gegevens meedeelt.

public ou privé susvisé, gestionnaire de la source de données accédée;

2- En cas de traitement ultérieur[16] des données collectées, mention de l'analyse de compatibilité des finalités de ce traitement avec celle pour lesquelles les données ont été initialement collectées conformément à l'article 6.4 du RGPD;

3- La vérification du respect du principe de "collecte auprès de la source authentique des données" qui garantit la qualité des données ainsi que le respect du cadre légal encadrant l'accès à la source authentique;

4- Toutes mesures spécifiques encadrant le flux conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut (choix du format de la communication, journalisation des accès de manière telle que l'on puisse savoir qui a eu accès à quoi quand et pourquoi, mise en place d'un répertoire de références en cas de communication automatique des actualisations des données afin d'assurer que seules les données nécessaires soient actualisées et pour la durée nécessaire, …)".

5. Il convient également de reformuler l'article 22, § 2, comme suit:

"Le protocole est adopté après que les responsables de traitements ont recueilli l'avis du délégué à la protection des données de l'autorité publique qui transfère les données et l'avis du délégué à la protection des données de l'autorité publique qui les reçoit. Ces avis sont annexés au protocole. Lorsqu'au moins un de ces avis n'est pas suivi par les responsables de traitement, le protocole mentionne, en ses dispositions préliminaires, la ou les raison(s) selon laquelle/lesquelles cet ou ces avis n'ont pas été suivis".

6. Étant donné que ces protocoles organisent une ingérence dans la vie privée, ils doivent être accessibles pour les personnes concernées en vertu de l'article 22 de la Constitution de manière à assurer la prévisibilité des transferts et des traitements. Or, le protocole ne bénéficie pas de la publicité réservée à la loi qui lui sert de base légale et cette dernière, par nature, ne contient pas les éléments essentiels du transfert qui sont contenus dans le protocole.

Dès lors, il s'impose que les protocoles soient publiés.

7. L'hypothèse selon laquelle les responsables de traitement ne parviendraient pas à s'accorder à propos du transfert de données et du contenu du protocole doit être envisagée par le législateur.

[16] *Note de bas de page 48 de l'avis cité:* Utilisation des données pour une ou des finalité(s) différente(s) de celle(s) pour la(les) quelle(s) elle(s) a(ont) été collectée(s) à l'origine par l'autorité ou l'organisme public qui communique les données.

Artikel 24

Hoewel het register van de verwerking van persoonsgegevens dat bijgehouden wordt door de overheidsinstanties, in de geest van de AVG, een intern instrument is dat erop gericht is de verwerkingsverantwoordelijken te responsabiliseren, mag niet uit het oog verloren worden dat in België het gebruik van de gegevens door de overheidsinstanties (de registratie en de doorgifte ervan) eveneens valt onder het fundamenteel recht op bestuurlijke transparantie, dat verankerd is in artikel 32 van de Grondwet en dat op federaal niveau georganiseerd is bij de wet van 11 april 1994 "betreffende de openbaarheid van bestuur". Die laatste wet verplicht de administratieve overheid actieve openbaarheid na te streven door, op eigen initiatief, "een duidelijke en objectieve voorlichting van het publiek over het optreden van de federale administratieve overheden" te verstrekken.[17]

In de context van de elektronische administratie die gebaseerd is op de eenmalige gegevensinzameling, dient ervan uitgegaan te worden dat het fundamenteel recht op bestuurlijke transparantie veronderstelt dat elke persoon toegang moet kunnen hebben tot een totaaloverzicht van de plaats alsook van het gebruik van de door de overheidsinstanties ingezamelde gegevens zodat hij begrijpt in welke administratieve omgeving hij zich bevindt. Met alle beschikbare technologische tools is het vandaag voor de administratieve overheid heel eenvoudig om een internetportaal te creëren dat toegang geeft tot alle gewenste documenten. Het Handvest van de gebruiker van de openbare diensten is overigens in die zin opgevat en verplicht uitdrukkelijk de openbare diensten om gebruik te maken van technologische middelen om zich aan te passen aan de behoeften van het publiek, zoals blijkt uit de volgende zin uit afdeling 2, hoofdstuk II, van deel I:

"In toepassing van de wet van de veranderlijkheid, moeten de openbare diensten zich inspannen om een dienst te leveren die zowel aangepast is aan de behoeften van de gebruikers als aan de beschikbare middelen en technieken".[18]

Teneinde tegemoet te komen aan de doelstelling inzake bestuurlijke transparantie in de context van de elektronische administratie zou artikel 24 verduidelijkt moeten worden.

De steller van het voorontwerp dient duidelijk de openbare aard van die registers voorop te stellen en te organiseren en dient, in voorkomend geval, te voorzien in uitzonderingen erop waarbij die welke vervat zijn in de wet van 11 april 1994 tot voorbeeld zouden kunnen dienen. Als hij het nodig acht de Koning te machtigen om de nadere regels voor die bekendmaking te bepalen, dient hij die machtiging op duidelijkere wijze af te bakenen. Voorts is het idee om alle registers en doorgifteprotocollen te bundelen en aldus een kadaster te creëren van de bij de administratie beschikbare gegevens en van de tussen de overheidsinstanties georganiseerde doorgiften, het overwegen waard. Dat kadaster zou online beschikbaar moeten zijn.

[17] Artikel 2 van de wet van 11 april 1994.

[18] Handvest van de gebruiker van de openbare diensten van 4 december 1992, *SB,* 22 januari 1993, deel I, hoofdstuk II, afdeling 2.

Article 24

Bien que le registre des traitements des données à caractère personnel détenu par les autorités publiques constitue, dans la philosophie du RGPD, un outil interne visant à responsabiliser les responsables de traitement, il ne faut pas ignorer qu'en Belgique, l'utilisation des données par les autorités publiques (leur enregistrement et leur transfert) relève également du droit fondamental à la transparence administrative consacré par l'article 32 de la Constitution et organisé au niveau fédéral par loi du 11 avril 1994 "relative à la publicité de l'administration". Cette dernière impose à l'administration des obligations de publicité active qui consistent à fournir, d'initiative, "une information claire et objective sur l'action des autorités administratives fédérales"[17].

Dans le contexte de l'administration électronique fondée sur la collecte unique des données, il y a lieu de considérer que le droit fondamental à la transparence administrative suppose que toute personne doit pouvoir accéder à une vue d'ensemble de la localisation des données détenues par les autorités publiques et de leur utilisation pour comprendre l'environnement administratif dans lequel elle se trouve. C'est d'autant plus aisé à mettre en place aujourd'hui que l'administration dispose de tous les outils technologiques permettant de créer un portail internet et d'y faire figurer les documents qu'elle souhaite. La Charte des services publics est d'ailleurs conçue en ce sens en imposant clairement aux services publics de recourir aux technologies pour s'adapter aux besoins du public, affirmant dans sa partie I, chapitre II, section 2, que,

"par application de la loi de mutabilité, les services publics doivent s'efforcer de procurer un service adapté aux besoins des utilisateurs, comme aux techniques et moyens disponibles"[18].

Pour répondre à l'objectif de transparence administrative dans le contexte de l'administration électronique, l'article 24 devrait être précisé.

Il revient à l'auteur de l'avant-projet d'affirmer et d'organiser clairement le caractère public de ces registres en l'assortissant, le cas échéant, d'exceptions qui pourraient s'inspirer de celles énoncées par la loi du 11 avril 1994. S'il estime nécessaire d'habiliter le Roi à déterminer les modalités de cette publicité, il lui appartient d'encadrer cette habilitation de manière plus précise. Par ailleurs, l'idée d'intégrer l'ensemble des registres et des protocoles de transferts pour créer un cadastre des données disponibles dans l'administration et des transferts organisés entre les autorités publiques mérite d'être retenue. Ce cadastre devrait être accessible en ligne.

[17] Article 2 de la loi du 11 avril 1994.

[18] Charte de l'utilisateur des services publics du 4 décembre 1992, *M.B.,* 22 janvier 1993, partie I, chapitre II, section 2.

Hoe dan ook, aangezien artikel 24, § 2, inzonderheid een machtiging aan de Koning bevat “onverminderd het besluit bedoeld in artikel 57, § 3” van het voorontwerp, dat opgenomen is in titel 2 van het ontwerp, zou het, gelet eveneens op de artikelen 21, tweede lid, en 73, derde lid 3, 1°, van het voorontwerp, bijzonder nuttig zijn dat in de memorie van toelichting wordt uitgelegd hoe de eerste twee titels ervan zich tot elkaar verhouden voor de toepassing op de politiediensten.

Artikel 25

Artikel 25, § 2, is niet relevant in zoverre daarin een machtiging wordt verleend aan de wetgever.

Artikel 27

Artikel 27 moet aldus worden aangevuld dat daarin vermeld wordt welke overheid gemachtigd is om op federaal niveau de expertengroep op te richten waarvan sprake in die bepaling.

Artikel 28

Paragraaf 1 dient te vervallen, daar deze een onnodige herhaling is van artikel 35, § 2, van de AVG.

Artikel 29

1.1. Artikel 29 van het voorontwerp is opgenomen in een hoofdstuk V dat gewijd is aan de verwerking van persoonsgegevens “voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen”.

Aangezien het om een aangelegenheid gaat die valt onder de vrijheid van meningsuiting, die een fundamentele vrijheid vormt welke op internationaal vlak erkend wordt door zowel artikel 10 van het Europees Verdrag voor de rechten van de mens, als de artikelen 11 en 13 van het Handvest van de grondrechten van de Europese Unie, en op nationaal vlak door de artikelen 19 en 25 van de Grondwet, dient voorzien te worden in een uitzonderingsregeling wat betreft de regels die gelden voor de verwerking van de persoonsgegevens, zodat deze regels geen beletsel vormen voor de uitoefening van die vrijheid.

In artikel 85 van de AVG zijn de volgende bijzondere bepalingen opgenomen wat betreft de verwerking van persoonsgegevens in het licht van de “vrijheid van meningsuiting en van informatie”:

“1. De lidstaten brengen het recht op bescherming van persoonsgegevens overeenkomstig deze verordening wettelijk in overeenstemming met het recht op vrijheid van meningsuiting en van informatie, daaronder begrepen de verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen.

2. Voor verwerking voor journalistieke doeleinden of ten behoeve van academische, artistieke of literaire

Ceci étant, dès lors, notamment, que l’article 24, § 2, contient une habilitation au Roi “sans préjudice de l’arrêté visé à l’article 57, § 3” de l’avant-projet, lequel se situe au sein du titre 2 de celui-ci, il serait particulièrement utile, compte tenu également des articles 21, alinéa 2, et 73, alinéa 3, 1°, de l’avant-projet, que l’exposé des motifs explique l’articulation de l’applicabilité des deux premiers titres de celui-ci aux services de police.

Article 25

L’article 25, § 2, est dépourvu de pertinence en ce qu’il prévoit une habilitation en faveur du législateur.

Article 27

L’article 27 doit être complété pour indiquer quelle autorité est habilitée à créer, au niveau fédéral, le groupe d’experts dont il est question dans cette disposition.

Article 28

Le paragraphe 1er faisant double emploi avec l’article 35, § 2, du RGPD, il doit être omis.

Article 29

1.1. L’article 29 de l’avant-projet s’inscrit dans un chapitre V consacré aux traitements des données à caractère personnel “à des fins journalistiques et à des fins d’expression universitaire, artistique ou littéraire”.

Dès lors que la matière relève de la liberté d’expression, qui constitue une liberté fondamentale reconnue, au niveau international, tant par l’article 10 de la Convention européenne des droits de l’homme que par les articles 11 et 13 de la Charte des droits fondamentaux de l’Union européenne, qu’au niveau national par les articles 19 et 25 de la Constitution, un régime d’exception doit être prévu dans les règles s’imposant au traitement des données à caractère personnel, afin que celles-ci n’entravent pas l’exercice de cette liberté.

L’article 85 du RGPD prévoit ainsi les dispositions particulières suivantes concernant le traitement des données à caractère personnel au regard de la “liberté d’expression et d’information”:

“1. Les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d’expression et d’information, y compris le traitement à des fins journalistiques et à des fins d’expression universitaire, artistique ou littéraire.

2. Dans le cadre du traitement réalisé à des fins journalistiques ou à des fins d’expression universitaire, artistique

uitdrukkingsvormen stellen de lidstaten uitzonderingen of afwijkingen vast van hoofdstuk II (beginselen), hoofdstuk III (rechten van de betrokkene), hoofdstuk IV (de verwerkingsverantwoordelijke en de verwerker), hoofdstuk V (doorgifte van persoonsgegevens naar derde landen of internationale organisaties), hoofdstuk VI (onafhankelijke toezichthoudende autoriteiten), hoofdstuk VII (samenwerking en coherentie) en hoofdstuk IX (specifieke gegevensverwerkingssituaties) indien deze noodzakelijk zijn om het recht op bescherming van persoonsgegevens in overeenstemming te brengen met de vrijheid van meningsuiting en van informatie."

Voorts staat in overweging nr. 153 van de AVG het volgende:

"In de wetgeving van de lidstaten moeten de regels betreffende de vrijheid van meningsuiting en van informatie, met inbegrip van journalistieke, academische, artistieke en/of literaire uitdrukkingsvormen in overeenstemming worden gebracht met het recht op bescherming van persoonsgegevens uit hoofde van deze verordening. Voor de verwerking van persoonsgegevens enkel voor journalistieke doeleinden of ten behoeve van academische, artistieke en literaire uitdrukkingsvormen moeten afwijkingen van of uitzonderingen op een aantal bepalingen van deze verordening worden ingesteld, teneinde indien nodig het recht op bescherming van persoonsgegevens te verzoenen met het recht op de vrijheid van meningsuiting en van informatie, zoals dat in artikel 11 van het Handvest is vastgelegd. Dit dient met name te gelden voor de verwerking van persoonsgegevens voor audiovisuele doeleinden en in nieuws- en persarchieven. De lidstaten moeten derhalve wettelijke maatregelen treffen om de uitzonderingen en afwijkingen vast te stellen die nodig zijn om een evenwicht tussen die grondrechten tot stand te brengen. De lidstaten dienen dergelijke uitzonderingen en afwijkingen vast te stellen met betrekking tot de algemene beginselen, de rechten van betrokkenen, de verwerkingsverantwoordelijke en de verwerker, de doorgifte van persoonsgegevens naar derde landen of internationale organisaties, de onafhankelijke toezichthoudende autoriteiten, samenwerking en coherentie, en betreffende specifieke situaties op het gebied van gegevensverwerking. Indien die uitzonderingen of afwijkingen per lidstaat verschillen, is het recht van de lidstaat waaraan de verwerkingsverantwoordelijke is onderworpen, van toepassing. Gelet op het belang van het recht van vrijheid van meningsuiting in elke democratische samenleving, dienen begrippen die betrekking hebben op die vrijheid, zoals journalistiek, ruim te worden uitgelegd."

Het voornoemde artikel 11 van het Handvest van de grondrechten van de Europese Unie bepaalt het volgende:

"1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen.

2. De vrijheid en de pluriformiteit van de media worden geëerbiedigd."

ou littéraire, les États membres prévoient des exemptions ou des dérogations au chapitre II (principes), au chapitre III (droits de la personne concernée), au chapitre IV (responsable du traitement et sous-traitant), au chapitre V (transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales), au chapitre VI (autorités de contrôle indépendantes), au chapitre VII (coopération et cohérence) et au chapitre IX (situations particulières de traitement) si celles-ci sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information".

Il est par ailleurs précisé au considérant n° 153 du RGPD que

"Le droit des États membres devrait concilier les règles régissant la liberté d'expression et d'information, y compris l'expression journalistique, universitaire, artistique ou littéraire, et le droit à la protection des données à caractère personnel en vertu du présent règlement. Dans le cadre du traitement de données à caractère personnel uniquement à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, il y a lieu de prévoir des dérogations ou des exemptions à certaines dispositions du présent règlement si cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, consacré par l'article 11 de la Charte. Tel devrait notamment être le cas des traitements de données à caractère personnel dans le domaine de l'audiovisuel et dans les documents d'archives d'actualités et bibliothèques de la presse. En conséquence, les États membres devraient adopter des dispositions législatives qui fixent les exemptions et dérogations nécessaires aux fins d'assurer un équilibre entre ces droits fondamentaux. Les États membres devraient adopter de telles exemptions et dérogations en ce qui concerne les principes généraux, les droits de la personne concernée, le responsable du traitement et le sous-traitant, le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, les autorités de contrôle indépendantes, la coopération et la cohérence, ainsi que les situations particulières de traitement des données. Lorsque ces exemptions ou dérogations diffèrent d'un État membre à l'autre, le droit de l'État membre dont relève le responsable du traitement devrait s'appliquer. Pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique, il y a lieu de retenir une interprétation large des notions liées à cette liberté, telles que le journalisme".

L'article 11, précité, de la Charte des droits fondamentaux de l'Union européenne énonce que

"1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

2. La liberté des médias et leur pluralisme sont respectés".

Uit die preciseringen blijkt dat de nationale wetgevers verzocht worden erop toe te zien dat het recht op de bescherming van de persoonsgegevens, in de AVG en omgezet door de nationale wetgevers, eerst en vooral geen schending inhoudt van "het recht op de vrijheid van meningsuiting" waarop elke burger zich mag beroepen en dat de vrijheid "omvat" om een mening te hebben en de vrijheid om informatie te ontvangen en te verstrekken.

1.2. Hoewel de steller van het voorontwerp in de bespreking van de artikelen wel degelijk preciseert dat artikel 85 van de AVG ertoe strekt "de gegevensbescherming te harmoniseren met de vrijheid van meningsuiting en de journalistieke doeleinden", blijkt dat de strekking van artikel 29 van het voorontwerp, dat volgens de steller van het voorontwerp artikel 85 van de AVG "omzet" "met de instelling van uitzonderingen voor verwerkingen met literaire, artistieke of academische doeleinden, evenals voor verwerkingen met journalistieke doeleinden, nodig voor de harmonisering van de gegevensbescherming met de vrije meningsuiting", veel beperkter is aangezien het de vrijheid van meningsuiting herleidt tot de literaire, artistieke en academische vrijheid of de vrijheid van meningsuiting voor journalistieke doeleinden.

Aldus beantwoordt het voorontwerp niet volledig aan de verplichting die voor de lidstaten geldt om "het recht op bescherming van persoonsgegevens overeenkomstig deze verordening wettelijk in overeenstemming [te brengen] met het recht op vrijheid van meningsuiting", zoals bedoeld wordt in artikel 85, lid 1, van de AVG.

2. In de Franse tekst moet de terminologie eenvormiger gemaakt worden en behoort zoals in de Nederlandse tekst bij voorkeur het adjectief "*académique*" gebezigd te worden in plaats van "*universitaire*".

3.1. In paragraaf 1 wordt bepaald wat begrepen dient te worden onder verwerking "voor journalistieke doeleinden":

"een verwerking die voornamelijk gericht is op het verzamelen, opstellen, voortbrengen of verspreiden van informatie van algemeen belang, met behulp van media, ten bate van het publiek".

Naast het feit dat in de Franse tekst het woord "*finalité*" vervangen behoort te worden door het woord "*objet*", wordt in deze definitie geen rekening gehouden met de archivering van de inlichtingen die verzameld zijn in het kader van een journalistieke activiteit. De gegevens die door journalisten of de media verzameld en gearchiveerd worden, vormen in hun geheel een belangrijke bron voor het journalistieke werk die, inzonderheid, maar niet uitsluitend, onmisbaar is bij het natrekken van feiten ("*fact checking*"), wat steeds vaker van de pers geëist wordt.

De archivering van de verzamelde informatie moet bijgevolg opgenomen worden bij de verwerking van de gegevens "voor journalistieke doeleinden". Dat wordt overigens ook uitdrukkelijk aanbevolen in overweging nr. 153.

3.2. De verwijzing in de memorie van toelichting naar een "definitie" van het begrip "journalist" in de wet van 7 april 2005

Il ressort de ces précisions que les législateurs nationaux sont invités à veiller à ce que le droit à la protection des données à caractère personnel, mis en place par le RGPD et transposé par les lois nationales, ne porte pas atteinte, avant tout, au "droit à la liberté d'expression" qui appartient à tout citoyen et "qui comprend" la liberté d'opinion et la liberté de recevoir ou de communiquer des informations.

1.2. Si, dans le commentaire des articles, l'auteur de l'avant-projet précise bien que l'article 85 du RGPD tend à "réconcilier la protection des données avec la liberté d'expression et les fins journalistiques", il apparaît que la portée de l'article 29 de l'avant-projet qui, selon l'auteur de l'avant-projet, "transpose" l'article 85 du RGPD "en instituant pour les traitements à des fins d'expression littéraire artistique ou académique ainsi que pour les traitements à des fins journalistiques des exceptions nécessaires pour concilier la protection des données avec la liberté d'expression", est sensiblement plus limité puisqu'il restreint la liberté d'expression à la liberté littéraire, artistique et académique ou à l'expression à des fins journalistiques.

Ainsi, l'avant-projet ne répond pas entièrement à l'obligation faite aux États de "concilie[r], par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression" au sens de l'article 85, paragraphe 1er, du RGPD.

2. Dans la version française, il y a lieu d'uniformiser le vocabulaire en privilégiant l'adjectif "académique" plutôt qu'"universitaire", comme dans la version néerlandaise du texte.

3.1. Le paragraphe 1er définit ce qu'il convient d'entendre par le traitement "aux fins de journalisme":

"un traitement ayant comme finalité la collecte, la rédaction, la production ou la diffusion d'informations d'intérêt général, par le biais de média, au profit du public".

Outre le fait qu'il vaudrait mieux remplacer le mot "finalité" par celui d'"objet", cette définition ne prend pas en compte l'archivage des informations récoltées dans le cadre d'une activité journalistique. Or les données récoltées et archivées par les journalistes ou les médias constituent, à part entière, une source essentielle du travail journalistique, notamment, mais pas exclusivement, indispensable dans l'activité de vérification de faits ("*fact checking*") de plus en plus souvent demandée à la presse.

L'archivage des informations collectées doit en conséquence être intégré aux traitements des données "aux fins de journalisme". C'est du reste ce que recommande expressément le considérant n° 153.

3.2. La référence faite dans l'exposé des motifs à une "définition" du "journaliste" qui figurerait dans la loi du 7 avril 2005

"tot bescherming van de journalistieke bronnen" moet worden geschrapt daar het Grondwettelijk Hof in zijn arrest 91/2006 van 7 juni 2006 inzonderheid elke verwijzing naar dat begrip "journalist" in artikel 2, 1°, van die wet vernietigd heeft.

Krachtens die wet, zoals ze aangepast is bij dat arrest, genieten weliswaar alleen de personen die bijdragen tot "het verzamelen, redigeren, produceren of verspreiden van informatie voor het publiek via een medium" van de bescherming van de bronnen. Wat betreft de bescherming van de bronnen leek het niet relevant om naast de verzameling van informatie ook de archivering ervan uitdrukkelijk op te nemen als een activiteit waarvoor de bescherming van de bronnen noodzakelijk is. Maar aangezien de verzamelde informatie vervolgens noodzakelijkerwijze gearchiveerd wordt door de media en daar die archivering op zich een verwerking van gegevens uitmaakt, behoort ook deze activiteit, die onlosmakelijk verbonden is met de activiteit van de journalistiek, opgenomen te worden binnen de afwijkende regeling voor de verwerking van gegevens "voor journalistieke doeleinden".

3.3. In het voorontwerp wordt een voorwaarde toegevoegd die niet terug te vinden is in de definitie van de activiteit die recht geeft op de eerbiediging van het bronnengeheim als bedoeld in de wet van 7 april 2005, doordat daarin gesteld wordt dat alleen de verwerking (verzamelen, opstellen, voortbrengen of verspreiden) "van informatie van algemeen belang" binnen het toepassingsgebied van artikel 29 valt. Artikel 2, 1°, van de wet van 7 april 2005 heeft het enkel over "informatie".

Volgens een vaste rechtspraak van het Europees Hof voor de Rechten van de Mens is de toegenomen bescherming inzake de vrijheid van meningsuiting die aan journalisten is toegekend gerechtvaardigd gezien hun rol van "waakhond" van de democratie die ze in hoofdzaak vervullen wanneer zij verslag uitbrengen over onderwerpen van algemeen belang[19] of wanneer zij bijdragen tot een openbaar debat over een kwestie van algemeen belang[20]. Daaruit vloeit echter niet voort dat alleen de verwerking van gegevens die op zich reeds "van algemeen belang" zouden zijn, deel uitmaakt van de journalistieke activiteit.

Het dispositief moet worden aangepast rekening houdend met hetgeen voorgaat.

Alleen deze optie maakt het mogelijk om overeenkomstig de voornoemde overweging 153 "begrippen die betrekking hebben op die vrijheid, zoals journalistiek, ruim [uit te leggen]".

3.4. Wat betreft het begrip "media" is de verwijzing in de memorie van toelichting naar artikel 25 van de Grondwet en naar het arrest van het Hof van Cassatie van 6 maart 2012

19 EHRM 30 september 1994, *Jersild v. Denemarken*, § 31.

20 EHRM (Grote Kamer) 21 januari 1999, *Fressoz en Roire v. Frankrijk*, § 50; 20 mei 999, *Bladet Tromsø en Stensaas v. Noorwegen*; 8 juli 1999, *Sürek v. Turkije (n° 2)*, § 40; 28 september 1999, *Dalban v. Roemenië*, § 49; EHRM 28 september 2000, *Lopes Gomes da Silva v. Portugal*, § 34; 26 februari 2002, *Dichand en anderen v. Oostenrijk*; 26 februari 2002, *Unabhängige Initiative Informationsvielfalt v. Oostenrijk*; 26 februari 2002, *Krone Verlag GmbH und Co. KG v. Oostenrijk*; 20 juli 2004, *Hrico v. Slovakije*; 16 november 2004, *Selistö v. Finland*.

"relative à la protection des sources" doit être retirée dès lors que, par son arrêt n° 91/2006 du 7 juin 2006, la Cour constitutionnelle a annulé à l'article 2, 1°, de cette loi notamment toute référence à cette notion de "journaliste".

Certes, en vertu de cette loi, telle qu'elle résulte de cet arrêt, seules bénéficient de la protection des sources les personnes qui contribuent à la collecte, la rédaction, la production ou la diffusion d'informations, par le biais d'un média, au profit du public. Au regard de la protection des sources, il n'apparaissait pas pertinent, en plus de la collecte d'informations, de prévoir expressément l'archivage de celles-ci comme constituant, en soi, une activité nécessitant la protection des sources. Mais, dès lors que l'information collectée est ensuite, nécessairement, archivée par les médias et que cet archivage constitue en soi un traitement de données, il s'impose d'inclure cette activité, indissociable à l'activité de journalisme, dans le régime dérogatoire pour les traitements "aux fins de journalisme".

3.3. L'avant-projet ajoute une condition qui ne se trouve pas dans la définition de l'activité donnant droit au respect du secret des sources de la loi du 7 avril 2005, en précisant que seul entre dans le champ d'application de l'article 29 le traitement (collecte, rédaction, production ou diffusion) "d'informations d'intérêt général". L'article 2, 1°, de la loi du 7 avril 2005 vise uniquement les "informations".

Selon une jurisprudence constante de la Cour européenne des droits de l'homme, la protection accrue en matière de liberté d'expression reconnue aux journalistes se justifie en raison de leur rôle de "chiens de garde" de la démocratie qui s'exprime essentiellement lorsqu'ils traitent de sujets d'intérêt général[19] ou lorsqu'ils apportent une contribution à un débat public relatif à une question d'intérêt général[20]. Il ne s'en déduit toutefois pas que seul le traitement d'informations qui seraient elles-mêmes directement "d'intérêt général", participe à l'exercice de l'activité journalistique.

Il convient de revoir le dispositif en tenant compte de ce qui précède.

Seule cette option permet, conformément au considérant n° 153 précité, "de retenir une interprétation large des notions liées à cette liberté, telles que le journalisme".

3.4. Concernant la notion de "média", la référence faite dans l'exposé des motifs à l'article 25 de la Constitution et à l'arrêt de la Cour de cassation du 6 mars 2012 est de nature

19 Cour eur. D.H., arrêt *Jersild c. Danemarck*, 30 septembre 1994, § 31.

20 Cour eur. D.H. (gde ch.), arrêts *Fressoz et Roire c. France*, 21 janvier 1999, § 50; *Bladet Tromsø et Stensaas c. Norvège*, 20 mai 1999; *Sürek c. Turquie (n° 2)*, 8 juillet 1999, § 40; *Dalban c. Roumanie,* 28 septembre 1999, § 49; Cour eur. D.H., arrêts *Lopes Gomes da Silva c. Portugal*, 28 septembre 2000, § 34; *Dichand et autres c. Autriche*, 26 février 2002; *Unabhängige Initiative Informationsvielfalt c. Autriche*, 26 février 2002; *Krone Verlag GmbH und Co. KG c. Autriche*, 26 février 2002; *Hrico c. Slovaquie*, 20 juillet 2004; *Selistö c. Finlande*, 16 novembre 2004.

van aard om de afwijkende regeling onterecht te beperken tot de geschreven journalistieke activiteiten, waarbij aldus alle audiovisuele media terzijde geschoven worden, aangezien op grond van de interpretatie die het Hof van Cassatie geeft van het begrip "pers", waarvan sprake in artikel 25 van de Grondwet, alleen de geschreven pers – ook in digitale vorm – in die bepaling bedoeld wordt.

Overeenkomstig de aanbeveling van overweging 153 behoort daarentegen gepreciseerd te worden dat het begrip "media" betrekking heeft op elke instantie die inlichtingen verspreidt die bedoeld zijn voor een niet nader bepaald publiek, ongeacht de wijze waarop die communicatie geschiedt en de vorm die deze communicatie krijgt.

4.1. In de paragrafen 2 tot 11 wordt een reeks uitzonderingen opgesomd op de regels die vastgesteld zijn door de AVG, wanneer de verwerking gebeurt voor "journalistieke, academische, artistieke of literaire doeleinden".

Een aantal regels wordt niet uitdrukkelijk uitgesloten aangezien deze niet gelden voor de verwerking van gegevens voor "journalistieke, academische, artistieke of literaire doeleinden".

4.2. Aldus wordt in de memorie van toelichting het volgende gepreciseerd: "Voor zover die verwerkingen niet gebaseerd zijn op de toestemming van de betrokken persoon, zijn artikel 7 en 8 van de Verordening inzake de reikwijdte en de regeling van de toestemming niet van toepassing op hen". Het dispositief bevat dan ook geen enkele bepaling op grond waarvan de artikelen 7 en 8 van de AVG niet van toepassing zouden zijn op de verwerking van gegevens voor journalistieke, academische, artistieke of literaire doeleinden. Het blijft echter mogelijk dat in het kader van een journalistieke activiteit gegevens verzameld worden met instemming. Dat is zelfs een courante praktijk bij het afnemen van interviews.

In het dispositief moeten dan ook uitdrukkelijk alle afwijkingen op de gemeenrechtelijke regeling worden vermeld, door inzonderheid een nieuwe paragraaf 2 in te voegen waarin gepreciseerd wordt dat de artikelen 7 en 8 van de AVG niet van toepassing zijn op de verwerking van persoonsgegevens voor "journalistieke, academische, artistieke of literaire doeleinden".

4.3. Een soortgelijke opmerking geldt voor het niet-van-toepassing verklaren van de artikelen 19 en 20 van de AVG op de verwerking van gegevens voor journalistieke, academische, artistieke of literaire doeleinden.

4.4. Wat artikel 17 van de AVG betreft, wordt in artikel 29 terecht niet bepaald dat het niet van toepassing is op de verwerking van gegevens voor journalistieke, academische, artistieke

à restreindre de façon injustifiée le régime dérogatoire aux seules activités journalistiques qui s'expriment par le biais de l'écrit, écartant ainsi tous les médias audiovisuels, puisque, selon l'interprétation que donne la Cour de cassation à la notion de "presse" visée à l'article 25 de la Constitution, seule la presse écrite – fût-ce sous forme numérique – est visée par cette disposition.

Conformément à la recommandation du considérant n° 153, il y a au contraire lieu de préciser que, par "média", est visé tout organe qui diffuse des informations à destination d'un public indéterminé, quels que soit le mode de communication et la forme que celle-ci adopte.

4.1. Les paragraphes 2 à 11 énumèrent une série d'exclusions des règles fixées par le RGPD lorsque le traitement est effectué à des "fins de journalisme ou d'expression universitaire, artistique ou littéraire".

Certaines règles ne sont pas expressément exclues au motif qu'elles ne trouveraient pas à s'appliquer aux traitements effectués à des fins de journalisme ou d'expression universitaire, artistique ou littéraire.

4.2. Ainsi, l'exposé des motifs précise que, "dans la mesure où ces traitements ne sont pas basés sur le consentement de la personne concernée, les articles 7 et 8 du règlement relatifs à la portée et au régime du consentement ne leur sont pas applicables". Le dispositif ne contient dès lors aucune disposition qui écarte l'application des articles 7 et 8 du RGPD aux traitements effectués à des fins de journalisme ou d'expression universitaire, artistique ou littéraire. Or, une collecte de données basée sur le consentement reste possible dans le cadre d'une activité aux fins de journalisme et est même une pratique courante lors des interviews.

Il conviendrait donc de prévoir expressément dans le dispositif toutes les dérogations au régime de droit commun, en insérant notamment un nouveau paragraphe 2 qui préciserait que les articles 7 et 8 du RGPD ne s'appliquent pas aux traitements des données à caractère personnel effectuées à des fins de journalisme ou d'expression universitaire, artistique ou littéraire.

4.3. Une observation analogue vaut pour l'exclusion de l'application des articles 19 et 20 du RGPD aux traitements effectués aux fins de journalisme ou d'expression universitaire, artistique ou littéraire.

4.4. S'agissant de l'article 17 du RGPD, c'est à bon escient que l'article 29 ne le déclare pas inapplicable aux traitements effectués aux fins de journalisme ou d'expression

of literaire doeleinden, aangezien reeds in die uitsluiting wordt voorzien in paragraaf 3, a), zelf van dat artikel 17.[21]

4.5. In artikel 85 van de AVG worden de nationale wetgevers verzocht de regels die verband houden met het recht op de eerbiediging van het privéleven en de regels die gelden inzake de vrijheid van meningsuiting en van informatie met elkaar te verzoenen. Daaraan wordt gevolg gegeven in de leden 2 tot 7 en 9 tot 11, door de betreffende bepalingen van de AVG onder bepaalde voorwaarden niet van toepassing te verklaren.[22] Aldus wordt bijvoorbeeld in paragraaf 2 bepaald dat de artikelen 9 en 10 van de AVG ter zake niet van toepassing

universitaire, artistique ou littéraire dès lors que cette exclusion est déjà prévue par le paragraphe 3, a), lui-même de cet article 17[21].

4.5. La conciliation que l'article 85 du RGPD invite les législateurs nationaux à opérer entre les impératifs touchant au droit au respect de la vie privée et ceux relatifs aux libertés d'expression et d'information est mise en œuvre dans les paragraphes 2 à 7 et 9 à 11 de manière à n'écarter l'applicabilité des dispositions visées du RGPD qu'à certaines conditions[22]. Ainsi, par exemple, le paragraphe 2 déclare les articles 9 et 10 du RGPD inapplicables en la matière "lorsque le traitement se rapporte à des données rendues

[21] De precisering in de bespreking van het artikel, volgens welke artikel 17, lid 3, van de AVG niet van toepassing zou zijn op "de online persarchieven" is strijdig met de AVG en die stelling wordt ook niet bevestigd in de rechtspraak die wordt aangehaald. In de AVG wordt geen enkel onderscheid gemaakt tussen de persarchieven die niet online staan en de onlinepersarchieven. De strekking van artikel 17, lid 3, van de AVG is algemeen en is in zeer ruime bewoordingen gesteld: "De leden 1 en 2 zijn niet van toepassing voor zover verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie". Dat artikel van de AVG laat op dat punt geen enkele beoordelingsbevoegdheid aan de lidstaten (in tegenstelling tot de aanbevelingen die geformuleerd worden in artikel 85, lid 2, van de AVG). De ontworpen tekst mag derhalve de strekking ervan niet inperken. De afdeling Wetgeving wijst er overigens op dat in overweging 153 uitdrukkelijk staat dat er "uitzonderingen op een aantal bepalingen van deze verordening [moeten] worden ingesteld, teneinde indien nodig het recht op bescherming van persoonsgegevens te verzoenen met het recht op de vrijheid van meningsuiting en van informatie (...) met name (...) voor de verwerking van persoonsgegevens (...) in nieuws- en persarchieven". De steller van het voorontwerp oordeelt ten onrechte dat die uitsluiting bekrachtigd is bij het arrest *Google* Spain, nr. C–131/12 van 3 mei 2014, van het Hof van Justitie van de Europese Unie. De zaak waarover het Hof van Justitie moest oordelen, had geen betrekking op de uitoefening van het recht tot uitwissing van gegevens in het kader van een onlinepersarchief, maar wel op de verplichting die opgelegd werd aan een zoekmachine van een aanbieder van internetdiensten om bepaalde zoekresultaten uit de lijst van resultaten te schrappen. Dat arrest legt derhalve geenszins de verplichting op om de inhoud van onlinepersarchieven uit websites van media-instanties te schrappen of ontoegankelijk te maken wanneer de betrokken persoon gebruik wil maken van zijn recht tot uitwissing. Het onderscheid tussen de verplichtingen die eventueel opgelegd worden aan de aanbieders van internetdiensten en de media is volstrekt gerechtvaardigd en maakt het mogelijk om niet te raken aan de persarchieven die een onschatbare bron zijn van informatie van algemeen belang: zoekmachines streven uitsluitend een commerciële doelstelling na, terwijl de archieffunctie van de media het algemeen belang dient, namelijk de vrije meningsuiting van de media alsook het recht op informatie. De verwijzing in de bespreking van het artikel naar het arrest van 29 april 2016 van het Hof van cassatie is voorts eveneens onjuist. In de zaak die geleid heeft tot dat arrest steunde het "recht op vergetelheid" toegekend door het Hof van Cassatie, niet op het recht tot het uitwissen van gegevens op grond van de wet van 8 december 1992, maar op artikel 1382 van het Burgerlijk Wetboek en op het fundamentele recht op eerbiediging van het privéleven.

[22] Paragraaf 8 verklaart artikel 21, lid 1, van de AVG uitsluitend niet van toepassing op de verwerking van gegevens voor journalistieke doeleinden en niet op de verwerking van gegevens voor academische, artistieke of literaire doeleinden.

[21] La précision du commentaire de l'article, selon laquelle l'article 17, paragraphe 3, du RGPD ne serait pas applicable aux "archives de presse mise en ligne sur internet", est contraire au RGPD et la jurisprudence citée n'est pas de nature à confirmer cette affirmation. Aucune distinction n'est faite par le RGPD entre les archives de presse tenues hors ligne et les archives de presse mises en ligne. La portée de l'article 17, paragraphe 3, du RGPD est générale et exprimée en termes très larges: "Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire à l'exercice du droit à la liberté d'expression et d'information". Cet article du RGPD ne laisse sur ce point aucun pouvoir d'appréciation aux États membres (à l'inverse des recommandations formulées à l'article 85, paragraphe 2, du RGPD). Le texte en projet ne peut dès lors pas en réduire la portée. La section de législation rappelle par ailleurs que le considérant n° 153 précise expressément qu'"il y a lieu de prévoir […] des exemptions à certaines dispositions du présent règlement si cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information […] notamment […] le cas des traitements de données à caractère personnel […] dans les documents d'archives d'actualités". C'est à tort que l'auteur de l'avant-projet considère que cette exclusion aurait été confirmée par l'arrêt *Google Spain*, n° C-131/12 du 3 mai 2014, de la Cour de justice de l'Union européenne. L'affaire portée devant la Cour de justice ne concernait pas l'exercice du droit à l'effacement de données dans le cadre d'une archive de presse en ligne, mais bien l'exigence faite à un moteur de recherche d'un intermédiaire de services sur internet de supprimer certains résultats de recherche de la liste des résultats. Cet arrêt n'impose dès lors nullement que le contenu des archives de presse mises en ligne devrait être retiré des sites des médias ou rendu inaccessible lorsque la personne concernée entend faire valoir son droit à l'effacement. La distinction entre les obligations éventuellement imposées aux intermédiaires sur internet et les médias est parfaitement justifiée et permet de conserver intactes les archives de presse, source inestimable d'information d'intérêt général: les moteurs de recherche ne poursuivent qu'un intérêt commercial, tandis que la fonction archivistique des médias sert un intérêt général, à savoir la liberté d'expression des médias ainsi que le droit à l'information. La référence encore faite, dans le commentaire de l'article, à l'arrêt du 29 avril 2016 de la Cour de cassation est également erronée. Dans l'affaire ayant donné lieu à cet arrêt, le "droit à l'oubli" accordé par la Cour de cassation n'était pas fondé sur le droit d'effacer des données sur la base de la loi du 8 décembre 1992 mais sur l'article 1382 du Code civil et le droit fondamental au respect de la vie privée.

[22] Le paragraphe 8 écarte l'application de l'article 21, paragraphe 1, du RGPD uniquement pour les traitements à des fins de journalisme et pas pour ceux à des fins académique, artistique ou littéraire.

zijn “wanneer de verwerking betrekking heeft op persoonsgegevens die kennelijk publiek zijn gemaakt door de betrokkene of die in nauw verband staan met het publieke karakter van de betrokkene of van het feit waarin die persoon betrokken is” en wordt in de paragrafen 3 tot 5 de niet-toepasselijkheid van artikel 11, lid 2, en van de artikelen 13, 14 en 15, lid 1, van de AVG beperkt tot de gevallen waarbij “door de toepassing (ervan) (...) de verzameling van gegevens [of] (…) een voorgenomen publicatie in het gedrang [zou komen] [of] in verband met de verwerkingen voor journalistieke doeleinden (...) de toepassing [ervan] aanwijzingen [zou] verschaffen over de bronnen van informatie”.

Binnen de korte termijn die de afdeling Wetgeving is toegemeten, is ze, wat deze gevoelige en complexe aangelegenheden betreft, niet kunnen nagaan of deze aanpak, waarbij de vrijheid van meningsuiting en van informatie beperkt wordt, op afdoende wijze aansluit bij de huidige stand van het recht, met betrekking tot het afwegen van belangen wanneer die vrijheden tegenover het recht op de eerbiediging van het privéleven komen te staan, zoals dat recht inzonderheid voortvloeit uit de rechtspraak van de hogere rechtscolleges.[23]

Hetzelfde geldt, omgekeerd, voor paragraaf 8 van de voorliggende bepaling, die volstrekte voorrang verleent aan de persvrijheid boven het recht op de eerbiediging van het privéleven wat betreft de niet-toepasselijkheid van artikel 18 van de AVG, dat betrekking heeft op het recht op de beperking van de verwerking.

4.6. Paragraaf 6 geeft evenwel aanleiding tot de volgende opmerking.

In die paragraaf wordt de verantwoordelijke voor de verwerking van gegevens voor journalistieke, academische, artistieke of literaire doeleinden vrijgesteld van de toepassing van artikel 16 van de AVG (recht op rectificatie voor elke persoon die verneemt dat van hem onjuiste persoonsgegevens bewaard worden) “wanneer door de toepassing een voorgenomen publicatie in het gedrang wordt gebracht” maar “inzoverre de betrokkene beschikt over het recht om, na de publicatie, aanvullende verklaringen af te leggen en een soortgelijke publiciteit daarbij wordt verzekerd door de verwerkingsverantwoordelijke en de verwerker, tenzij de aanvullende verklaring beledigend zou zijn of in strijd met de wetten en de goede zeden”.

In de bespreking van het artikel wordt gepreciseerd dat de betrokken persoon “zijn recht tot antwoord [moet kunnen] doen gelden”. Daaruit blijkt dat er verwarring bestaat tussen enerzijds het recht op de bescherming van de persoonsgegevens en het recht dat daaruit voortvloeit op de rectificatie van onjuiste gegevens, en, anderzijds, het recht op persvrijheid dat het recht van antwoord omvat, waarin voorzien wordt bij de wet van 23 juni 1961 “betreffende het recht tot antwoord”. De voorwaarden waaronder een verzoek tot verspreiding van

[23] Zie inzonderheid EHRM (Grote Kamer) 27 juni 2017, *Satakunnan Markkinapörssi Oy en Satamedia Oy v. Finland.*

manifestement publiques par la personne concernée ou sur des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée” et les paragraphes 3 à 5 limitent l’inapplicabilité des articles 11, paragraphe 2, 13, 14 et 15, paragraphe 1er, du RGPD aux cas où “[leur] application compromettrait la collecte des données [ou] une publication en projet [ou encore], concernant les traitements aux fins journalistiques, […] fournirait des indications sur les sources d’information”.

Dans le bref délai qui lui a été accordé, la section de législation n’a pas été en mesure de vérifier, sur ces questions délicates et complexes, que ces approches, qui limitent les libertés d’expression et d’information, concordent de manière adéquate avec l’état actuel du droit, résultant notamment de la jurisprudence des juridictions supérieures[23], quant à la balance des intérêts qui résulte de la confrontation de ces libertés avec le droit au respect de la vie privée.

Il en va de même, à l’inverse, pour ce qui concerne le paragraphe 8 de la disposition à l’examen, qui fait prévaloir de manière absolue la liberté de la presse sur le droit au respect de la vie privée pour ce qui concerne la non-applicabilité de l’article 18 du RGPD, qui concerne le droit à la limitation du traitement.

4.6. Le paragraphe 6 appelle toutefois l’observation suivante.

Il exempte le responsable du traitement à des fins de journalisme, d’expression universitaire, artistique ou littéraire, de l’application de l’article 16 du RGPD (droit de rectification pour toute personne qui apprend que des données à caractère personnel inexactes sont conservées à son sujet) si “son application compromettrait une publication en projet”, mais “pour autant que la personne concernée dispose, après publication, du droit de faire des déclarations complémentaires et qu’une publicité similaire y soit assurée par le responsable du traitement et le sous-traitant sauf dans la mesure où la déclaration complémentaire est injurieuse ou contraire aux lois et aux bonnes mœurs”.

Le commentaire de l’article précise qu’il faut que la personne concernée puisse exercer son “droit de réponse”. Cette précision révèle une confusion entre le droit à la protection des données personnelles et le droit qui en découle à la rectification de données inexactes, et le droit de la presse qui englobe le droit de réponse, prévu par la loi du 23 juin 1961 “relative au droit de réponse”. Les conditions dans lesquelles doit s’exercer la demande de diffusion d’une réponse, différentes selon que l’information mettant en cause la personne concernée,

[23] Voir notamment Cour eur D.H. (gde ch.), arrêt *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, 27 juin 2017.

een antwoord moet plaatsvinden, die verschillen naar gelang van het feit of de informatie waarmee de betrokken persoon in opspraak wordt gebracht uitgaat van de geschreven pers dan wel van de audiovisuele pers, stemmen hoegenaamd niet overeen met het recht om “aanvullende verklaringen af te leggen” waarvan sprake in de ontworpen tekst.

De wetgeving inzake de verwerking van persoonsgegevens behoort niet te leiden tot een wijziging van het subtiele evenwicht dat de wetgever al sedert verschillende jaren tot stand heeft gebracht tussen de vrijheid van informatie en het recht van elke persoon op wie die informatie betrekking heeft om te vragen een antwoord te verspreiden. Dat geldt des te meer daar het recht van antwoord waarover eenieder die in opspraak wordt gebracht beschikt, binnen de geschreven pers geen recht op rectificatie vormt.

Daar het recht om de verspreiding van een antwoord te vragen verworven is, aangezien men zich hier noodgedwongen binnen een journalistiek kader bevindt, behoort geen enkele voorwaarde te worden gesteld aan het terzijde schuiven van artikel 16 in het kader van de verwerking van gegevens met die doelstelling.

4.7. Aansluitend op opmerking 4.5. wijst de afdeling Wetgeving erop dat de steller van het voorontwerp, met betrekking tot paragraaf 9 van artikel 29 van het voorontwerp, de redenen moet toelichten die hem ertoe gebracht hebben om de toepassing van slechts een aantal artikelen van hoofdstuk IV van de AVG te weren in het kader van de verwerking van persoonsgegevens voor journalistieke, academische, artistieke of literaire doeleinden, rekening houdend met de verplichting die de wetgever, overeenkomstig artikel 85 van de AVG, heeft om de betreffende vrijheden met elkaar te verzoenen.

émane de la presse écrite ou de la presse audiovisuelle, ne correspondent en rien au droit de “faire des déclarations complémentaires” visé dans le texte en projet.

Ce n’est pas la législation en matière de traitement des données à caractère personnel qui doit être le siège d’une modification du subtil équilibre établi par le législateur depuis de nombreuses années entre la liberté de l’information et le droit pour toute personne concernée par cette information de solliciter la diffusion d’une réponse, et ce d’autant moins que, dans la presse écrite, le droit de réponse, ouvert à toute personne mise en cause, n’est pas un droit de rectification.

Le droit de solliciter la diffusion d’une réponse étant acquis, dès lors que l’on se situe ici nécessairement dans un cadre journalistique, l’écartement de l’article 16 aux traitements ayant cette dernière finalité ne devrait être soumis à aucune condition.

4.7. Quant au paragraphe 9 de l’article 29 de l’avant-projet, en complément à l’observation n° 4.5, il appartient à l’auteur de l’avant-projet d’exposer les motifs qui le conduisent à n’écarter l’application que de certains articles du chapitre IV du RGPD aux traitements à des fins de journalisme, académique, artistique ou littéraire, compte tenu de l’obligation qui est celle du législateur, conformément à l’article 85 du RGPD, d’assurer la conciliation entre les libertés en cause.

TITEL 2

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid

Artikel 34

In de Franse tekst van artikel 34, § 1, moet niet verwezen worden naar “la Convention internationale” maar naar “l’accord international”, gelet op de definitie in artikel 31, 17°, van het voorontwerp.

Dezelfde opmerking geldt voor artikel 35.

Artikel 35

Het staat niet aan de nationale wetgever om de wetgever van de Europese Unie, noch de partijen bij een internationale

TITRE 2

De la protection des personnes physiques à l’égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière ou d’exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces

Article 34

Dans la version française de l’article 34, § 1er, il convient de viser non pas “la Convention internationale” mais bien “l’accord international”, compte tenu de la définition figurant à l’article 31, 17°, de l’avant-projet.

La même observation vaut pour l’article 35.

Article 35

Il n’appartient pas au législateur national d’habiliter celui de l’Union européenne ni les parties à un accord international

overeenkomst te machtigen om te voorzien in een nieuw dispositief, noch om inhoudelijke voorwaarden voor zulk een dispositief te bepalen.

Het tweede en derde lid moeten dienovereenkomstig worden herzien.

Artikel 41

Artikel 12 van richtlijn 2016/680/EU luidt als volgt: “In de regel verstrekt de verwerkingsverantwoordelijke de informatie in dezelfde vorm als de vorm van het verzoek”.

Die verplichting wordt evenwel niet omgezet in het ontworpen dispositief.

Dat dispositief dient vervolledigd te worden.

Artikel 46

1. Artikel 17, leden 1 en 2, van richtlijn 2016/680/EU, luidt als volgt:

“1. In de in artikel 13, lid 3[24], artikel 15, lid 3, en artikel 16, lid 4, bedoelde gevallen treffen de lidstaten maatregelen die ertoe strekken dat de betrokkene zijn rechten *ook* via de bevoegde toezichthoudende autoriteit *kan* uitoefenen.

2. De lidstaten schrijven voor dat de verwerkingsverantwoordelijke de betrokkene in kennis stelt *van de mogelijkheid* uit hoofde van lid 1 zijn rechten via de toezichthoudende autoriteit uit te oefenen” (eigen cursivering).

Deze bepaling strekt er dus toe de betrokken personen een extra middel te geven om op te treden.

In uitvoering van die bepaling wordt in artikel 46, § 1, van het voorontwerp het volgende bepaald:

“In de in artikel 42, § 2, artikel 43, § 4, artikel 44, § 4, en artikel 64, § 1, bedoelde gevallen, *kan* de wet, het decreet of de ordonnantie, *voorzien* dat de rechten van de betrokkene via de bevoegde toezichthoudende autoriteit *worden* uitgeoefend, met respect voor de principes van noodzakelijkheid en proportionaliteit in een democratische samenleving” (eigen cursivering).

Met deze bepaling zet het voorontwerp de mogelijkheid die de betrokken persoon heeft om zijn rechten op indirecte wijze uit te oefenen, zoals bepaald wordt in artikel 17 van de richtlijn, om in een mogelijkheid voor de wetgever om zulk een handelswijze op te leggen aan de betrokken personen. Dat zou erop neerkomen dat de rechten van die personen beperkt worden, hetgeen strijdig is met artikel 17 van de richtlijn. Overigens is het irrelevant om in een wet een machtiging te verlenen aan de wetgever.

[24] Waarnaar verwezen wordt in artikel 31, lid 5, van de richtlijn die omgezet wordt bij artikel 64 van de ontworpen wet.

à prévoir un dispositif nouveau ni à en énoncer les conditions d’adoption quant au fond.

Les alinéas 2 et 3 seront revus en conséquence.

Article 41

L’article 12 de la directive n° 2016/680/UE prévoit que, “de manière générale, le responsable du traitement fournit les informations sous la même forme que la demande”.

Cette obligation n’est cependant pas transposée par le dispositif en projet.

Celui-ci sera complété.

Article 46

1. Aux termes de l’article 17, paragraphes 1er et 2, de la directive n° 2016/680/UE,

“1. Dans les cas visés à l’article 13, paragraphe 3[24], à l’article 15, paragraphe 3 et à l’article 16, paragraphe 4, les États membres adoptent des mesures afin que les droits de la personne concernée *puissent également* être exercés par l’intermédiaire de l’autorité de contrôle compétente.

2. Les États membres prévoient que le responsable du traitement informe la personne concernée *de la possibilité* qu’elle a d’exercer ces droits par l’intermédiaire de l’autorité de contrôle en application du paragraphe 1” (italiques ajoutés).

Cette disposition tend donc à ajouter un moyen d’action en faveur des personnes concernées.

En exécution de cette disposition, l’article 46, § 1er, de l’avant-projet prévoit que,

“dans les cas visés à l’article 42, § 2, à l’article 43, § 4, à l’article 44, § 4, et à l’article 64, § 1er, la loi, le décret ou l’ordonnance, *peut prévoir* que les droits de la personne concernée *sont* exercés par l’intermédiaire de l’autorité de contrôle compétente, dans le respect des principes de nécessité et de proportionnalité dans une société démocratique” (italiques ajoutés).

Par cette disposition, l’avant-projet transforme la faculté, pour la personne concernée, d’exercer ses droits de manière indirecte prévue par l’article 17 de la directive en une possibilité pour le législateur d’imposer un tel mode d’action aux personnes concernées. Cela reviendrait à limiter les droits de ces personnes, ce qui est contraire à l’article 17 de la directive. Du reste, il n’est pas pertinent de prévoir dans une loi une habilitation en faveur du législateur.

[24] Auquel renvoie l’article 31, paragraphe 5, de la directive qui est transposé par l’article 64 de la loi en projet.

Het dispositief moet dienovereenkomstig worden herzien.

2. In artikel 46, § 4, vierde lid, en § 5, vierde lid, wordt bepaald dat de categorieën van contextuele informatie die door de bevoegde toezichthoudende autoriteit aan de betrokkene kunnen worden medegedeeld, bij "richtlijn" bepaald worden door de bevoegde ministers nadat daarover het advies van de bevoegde toezichthoudende autoriteit ingewonnen is.

Dat het recht op de eerbiediging van het privéleven in beginsel bij wet geregeld moet worden, neemt weliswaar niet weg dat delegatie kan worden verleend aan een ander bevoegdheidsniveau, maar een dergelijke delegatie is enkel aanvaardbaar op voorwaarde dat deze voldoende nauwkeurig omschreven wordt en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de belangrijkste onderdelen op voorhand vastgesteld zijn door de wetgever.

A fortiori is het niet denkbaar dat de nadere regels met betrekking tot de waarborgen waarin voorzien wordt teneinde een kader te creëren voor de beperking van het recht op het privéleven die het gevolg is van de verwerking van persoonsgegevens, vastgesteld worden in een tekst die geenszins bindend is en bijgevolg ook niet beantwoordt aan de vereisten van voorzienbaarheid en rechtszekerheid.

Overigens staan de artikelen 33 en 108 van de Grondwet eraan in de weg dat de wetgever bepaalde uitvoeringstaken rechtstreeks aan een minister opdraagt. Het staat immers aan de uitvoerende macht om de werkwijze en de organisatie van haar diensten te regelen. De wet moet de Koning machtigen om de verschillende taken uit te voeren die worden genoemd. De Koning kan deze taken dan eventueel zelf delegeren.

Artikel 50

1. In zoverre artikel 50, eerste lid, e), en derde lid, bepaalt dat nadere regels inzake de verwerking van persoonsgegevens vastgesteld kunnen worden in een protocol tussen de verwerkingsverantwoordelijken, doet het afbreuk aan het vereiste van wettelijkheid en voorzienbaarheid dat bij elke inmenging in het recht op eerbiediging van het privéleven in acht moet worden genomen.

2. Er dient een definitie gegeven te worden van het begrip "controlesysteem" dat in artikel 50, vierde lid, gebruikt wordt.

Artikel 51

Artikel 51, § 1, luidt als volgt:

"De persoon die betrokken is bij een gemeenschappelijke behandeling van zijn persoonsgegevens, rechtstreeks of onrechtstreeks afkomstig van ten minste één bevoegde autoriteit van titel 2 of ten minste één autoriteit, één dienst of orgaan bedoeld in titel 3, voor wat zijn gegevens bij de verantwoordelijken voor de verwerking betreft, geniet niet van de in de artikelen 41 tot 47 en 64 genoemde rechten waarnaar wordt verwezen."

Le dispositif sera revu en conséquence.

2. L'article 46, § 4, alinéa 4, et § 5, alinéa 4, prévoit que les catégories d'informations contextuelles qui peuvent être communiquées à la personne concernée par l'autorité de contrôle compétente sont déterminées par les ministres compétents dans des "directives" ayant fait l'objet d'un avis de l'autorité de contrôle compétente.

Si le principe de légalité qui sous-tend le droit au respect de la vie privée n'interdit pas toute délégation à un autre niveau de pouvoir, une telle délégation n'est admissible qu'à la condition que celle-ci soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

A fortiori, il n'est pas envisageable que les modalités des garanties mises en place afin d'encadrer la limitation du droit à la vie privée apportée par le traitement de données à caractère personnel soient fixées dans un texte dépourvu de caractère contraignant et, par voie de conséquence, de la prévisibilité et de la sécurité juridique qui s'imposent.

En outre, les articles 33 et 108 de la Constitution s'opposent à ce que le législateur attribue directement certaines missions d'exécution à un ministre. Il appartient en effet au pouvoir exécutif de régler le fonctionnement et l'organisation de ses services. La loi doit habiliter le Roi à effectuer les différentes tâches visées, celui-ci pouvant éventuellement les déléguer lui-même.

Article 50

1. L'article 50, alinéa 1er, e), et alinéa 3, en ce qu'il prévoit que des modalités du traitement de données à caractère personnel peuvent être fixées dans un protocole entre les responsables du traitement, porte atteinte à l'exigence de légalité et de prévisibilité qui sous-tend toute ingérence au droit au respect de la vie privée.

2. Il convient de définir la notion de "système de contrôle" utilisée par l'article 50, alinéa 4.

Article 51

L'article 51, § 1er, prévoit que

"la personne concernée par un traitement commun de ses données à caractère personnel, émanant directement ou indirectement d'au moins une autorité compétente du titre 2 ou d'au moins une autorité, un service ou organe du titre 3 ne bénéficie pas des droits visés aux articles 41 à 47 et 64, à l'égard de ses données auprès du ou des responsables du traitement commun".

Aangezien de artikelen 41 tot 47 en 64 van het voorontwerp per definitie van toepassing zijn op de verwerkingen van persoonsgegevens door een bevoegde autoriteit van titel 2, is het discriminerend om de toepassing van die rechten uit te sluiten in geval van een gemeenschappelijke verwerking van persoonsgegevens die rechtstreeks of onrechtstreeks afkomstig zijn van ten minste één bevoegde autoriteit van titel 2, zonder dat de hoedanigheid van de andere bij die gemeenschappelijke verwerking betrokken autoriteit dit rechtvaardigt.

Bij deze bepaling moet hoe dan ook toelichting worden gegeven, hetgeen thans niet het geval is.

Artikel 52

De tweede zin van het eerste lid moet aldus herzien worden dat hij beter overeenstemt met artikel 19, lid 2, van richtlijn 2016/680/EU, gelezen in het licht van overweging 53 van deze richtlijn.

Artikel 58

Artikel 58 strekt tot omzetting van artikel 25 van richtlijn 2016/680/EU.

Lid 1 van dat laatstgenoemde artikel is als volgt gesteld:

"De lidstaten voorzien erin dat logbestanden worden bijgehouden van ten minste de volgende verwerkingen in systemen voor geautomatiseerde verwerking: verzameling, wijziging, raadpleging, bekendmaking onder meer in de vorm van doorgiften, *combinatie* en wissing. (…)" (eigen cursivering).

In artikel 58, § 1, eerste lid, van het voorontwerp is geen sprake van "combinatie".

De bepaling moet op dat punt aangevuld worden.

Artikel 61

Artikel 61, § 1, c), zou een aparte bepaling moeten vormen en de redactie ervan zou meer in overeenstemming moeten zijn met artikel 28, lid 2, van richtlijn 2016/680/EU.

Artikel 66

In tegenstelling tot wat in de memorie van toelichting voorgehouden wordt, staat, gelet op de formulering van artikel 458 van het Strafwetboek, een strafrechtelijke straf op de niet-inachtneming van de verplichting tot geheimhouding of vertrouwelijkheid die bij artikel 66, § 5, aan de functionaris voor gegevensbescherming opgelegd wordt. Dat artikel 458 luidt als volgt:

"Geneesheren, heelkundigen, officieren van gezondheid, apothekers, vroedvrouwen en alle andere personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, en deze bekendmaken buiten het

Dès lors que les articles 41 à 47 et 64 de l'avant-projet s'appliquent par définition aux traitements de données à caractère personnel par une autorité compétente du titre 2, il est discriminatoire d'exclure l'application de ces droits dans l'hypothèse d'un traitement commun de données à caractère personnel émanant directement ou indirectement d'au moins une autorité compétente du titre 2, sans que la qualité de l'autre autorité impliquée dans ce traitement commun le justifie.

Cette disposition doit, en tout état de cause, faire l'objet d'un commentaire, actuellement absent.

Article 52

La deuxième phrase de l'alinéa 1er doit être revue de manière à mieux correspondre à l'article 19, paragraphe 2, de la directive n° 2016/680/UE, lu à la lumière du considérant n° 53 de cette directive.

Article 58

L'article 58 tend à transposer l'article 25 de la directive n° 2016/680/UE.

Cette disposition prévoit en son paragraphe 1er que

"les États membres prévoient que des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé: la collecte, la modification, la consultation, la communication, y compris des transferts, *l'interconnexion* et l'effacement […]" (italiques ajoutés).

L'article 58, § 1er, alinéa 1er, de l'avant-projet ne mentionne pas "l'interconnexion".

Le dispositif sera complété à ce sujet.

Article 61

L'article 61, § 1er, c), devrait faire l'objet d'une disposition distincte et comporter une rédaction plus conforme à l'article 28, paragraphe 2, de la directive n° 2016/680/UE.

Article 66

Contrairement à ce qui est avancé par l'exposé des motifs, l'obligation de secret ou de confidentialité qui est imposée au délégué à la protection des données par l'article 66, § 5, est soumise à une sanction pénale, compte tenu du libellé de l'article 458 du Code pénal, qui prévoit que

"les médecins, chirurgiens, officiers de santé, pharmaciens, sages-femmes et toutes autres personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où ils sont appelés à rendre témoignage en justice

geval dat zij geroepen worden om in rechte (of voor een parlementaire onderzoekscommissie) getuigenis af te leggen en buiten het geval dat de wet, het decreet of de ordonnantie hen verplicht of toelaat die geheimen bekend te maken, worden gestraft met gevangenisstraf van een jaar tot drie jaar en een geldboete van honderd euro tot duizend euro of met een van die straffen alleen."

TITEL 3

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door andere overheden dan die bedoeld in titels 1 en 2

ONDERTITEL 1

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Artikel 91

Gelet op het beginsel van gelijkheid en non-discriminatie en gelet op het evenredigheidsbeginsel dat bij elke beperking van het recht op eerbiediging van het privéleven in acht moet worden genomen, dient bepaald te worden dat de melding zo snel mogelijk en ten laatste binnen tweeënzeventig uur moet gebeuren, zoals bepaald in artikel 63 in titel 2.

Artikel 93

Krachtens het derde lid van paragraaf 1

"[kan d]e functionaris voor gegevensbescherming (…) niet van zijn functie ontheven of gestraft worden omwille van de uitvoering van zijn opdrachten".

Deze bepaling strekt ertoe de noodzakelijke onafhankelijkheid van de functionaris voor gegevensbescherming te garanderen.

Letterlijk genomen zorgt deze bepaling er evenwel voor dat er geen oplossing is voor situaties waarin de functies van de functionaris niet correct uitgevoerd worden en overwogen zou worden om hem van zijn functie te ontheffen, zonder dat die sanctie opgelegd wordt wegens de handelingen die de betrokkene gesteld heeft om de AVG, de ontworpen wet en, in ruimere zin, de vereisten in verband met de eerbiediging van het privéleven te doen naleven.

Er zou een adequate regeling ingevoerd moeten worden teneinde aan dergelijke situaties tegemoet te komen.

Dezelfde opmerking geldt voor de artikelen 126, § 1, derde lid, en 159, § 1, derde lid, van het voorontwerp.

(ou devant une commission d'enquête parlementaire) et celui où la loi, le décret ou l'ordonnance les oblige ou les autorise à faire connaître ces secrets, les auront révélés, seront punis d'un emprisonnement d'un an à trois ans et d'une amende de cent euros à mille euros ou d'une de ces peines seulement".

TITRE 3

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par d'autres autorités que celles visées aux titres 1 et 2

SOUS-TITRE 1ER

DE LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR LES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

Article 91

Compte tenu du principe d'égalité et de non-discrimination, ainsi que du principe de proportionnalité sous-jacent à toute limitation du droit au respect de la vie privée, il convient de prévoir que la notification doit avoir lieu dans les meilleurs délais et au maximum dans les septante-deux heures, tout comme cela est prévu à l'article 63 au sein du titre 2.

Article 93

En vertu de l'alinéa 3 du paragraphe 1er,

"[l]e délégué à la protection des données ne peut pas être relevé de ses fonctions ou sanctionné en raison de l'exercice de ses missions".

Cette disposition tend à garantir la nécessaire indépendance du délégué à la protection des données.

Il n'en reste pas moins que, prise à la lettre, elle laisse sans solution les situations dans lesquelles les fonctions du délégué sont exercées de manière fautive, d'une manière qui mériterait que puisse être envisagée une cessation de ses fonctions sans que cette sanction soit prise en raison des actes posés par l'intéressé en vue de faire respecter le RGPD, la loi en projet et, plus largement, les impératifs liés au respect de la vie privée.

Des mécanismes adéquats devraient être mis en place pour rencontrer ce type de situation.

La même observation vaut pour les articles 126, § 1er, alinéa 3, et 159, § 1er, alinéa 3, de l'avant-projet.

Artikel 101

Gelet op het beginsel van wettelijkheid en voorzienbaarheid dat bij elke inmenging in het recht op eerbiediging van het privéleven in acht genomen moet worden, is het onaanvaardbaar dat de betrokken inlichtingen- en veiligheidsdienst gemachtigd wordt om een verdere verwerking toe te staan in de zin van artikel 101, tweede lid, van het voorontwerp en om de voorwaarden daarvoor op volledig discretionaire wijze te bepalen, in afwijking van het principiële verbod dat in diezelfde bepaling vervat is.

Een soortgelijke opmerking geldt voor artikel 164 van het voorontwerp wat het OCAD betreft.

Een soortgelijke opmerking geldt eveneens voor de machtigingen tot publicatie of mededeling waarvan sprake in de artikelen 104, 137 en 167 van het voorontwerp.

ONDERTITEL 2

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR DE KRIJGSMACHT

Artikel 107

1. Bij artikel 107 moet toelichting gegeven worden, hetgeen thans niet het geval is.

2. Teneinde te waarborgen dat de inmenging in het privéleven van de betrokkenen evenredig is, dient de uitzondering op de rechten beperkt te worden tot de doeleinden waarvoor die uitzondering vereist is. De bewoordingen “aanwending van de krijgsmacht” en “paraatstelling van de krijgsmacht” zijn te ruim en moeten gepreciseerd worden door voor de omschrijving van de nagestreefde doeleinden een functioneel (en geen organiek) criterium te hanteren en door een doel op zich aan te geven (in plaats van een middel om dat doel te bereiken).

3. Artikel 107, § 7, luidt als volgt:

“met betrekking tot de verwerking van persoonsgegevens worden *de volgende rechten* slechts beperkt indien dit een noodzakelijke en evenredige maatregel vormt voor de aanwending van de krijgsmacht of paraatstelling met het oog op aanwending van de krijgsmacht: (…)” (eigen cursivering).

Het voorontwerp lijkt daarmee te verwijzen naar een lijst van rechten die aan de betrokken persoon zijn toegekend. Artikel 107 zegt daarover echter niets meer, behalve dat in punt 6 ervan verwezen wordt naar artikel 80 van het voorontwerp, welk artikel luidt als volgt:

“Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.”

Article 101

Compte tenu du principe de légalité et de prévisibilité qui sous-tend toute ingérence au droit au respect de la vie privée, il n’est pas admissible que le service de renseignement et de sécurité concerné soit habilité à autoriser un traitement ultérieur au sens de l’article 101, alinéa 2, de l’avant-projet et à en fixer de manière entièrement discrétionnaire les conditions, par dérogation à l’interdiction de principe énoncée par cette même disposition.

Une observation similaire vaut pour l’article 164 de l’avant-projet pour ce qui concerne l’OCAM.

Une observation similaire vaut également pour les autorisations de publication ou de communication visées par les articles 104, 137 et 167 de l’avant-projet.

SOUS-TITRE 2

LA PROTECTION DES PERSONNES PHYSIQUES CONCERNANT LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR LES FORCES ARMÉES

Article 107

1. L’article 107 doit faire l’objet d’un commentaire, actuellement absent.

2. Afin de garantir la proportionnalité de l’ingérence dans la vie privée des personnes concernées, il convient de limiter l’exception aux droits aux seules finalités pour lesquelles cette exception est nécessaire. Les termes “mise en œuvre des forces armées” et “mise en condition des forces armées” sont trop larges et doivent être précisés en utilisant, pour la définition des finalités poursuivies, un critère fonctionnel (et non organique) et en indiquant une fin en soi (et non un moyen pour parvenir à cette fin).

3. L’article 107, § 7, dispose ce qui suit:

“concernant le traitement des données à caractère personnel, *les droits suivants* sont limités lorsqu’il s’agit d’une mesure nécessaire et proportionnelle pour la mise en œuvre des forces armées, ou la mise en condition des forces armées en vue de leur mise en œuvre: […]” (italiques ajoutés).

L’avant-projet semble ainsi se référer à une liste de droits reconnus à la personne concernée. Cependant, l’article 107 ne précise rien à cet égard si ce n’est que son point 6 renvoie à l’article 80 de l’avant-projet, qui dispose que,

“lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel”.

Los van het feit dat het een onsamenhangende bepaling is, is de afdeling Wetgeving van oordeel dat die precisering alleen niet voldoende waarborgen biedt voor de rechten van de betrokkenen en daarmee bijgevolg niet op adequate wijze tegemoetgekomen kan worden aan het vereiste van voorzienbaarheid en het vereiste van evenredigheid die bij elke beperking van het recht op bescherming van het privéleven in acht moeten worden genomen.

ONDERTITEL 3

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS IN HET KADER VAN DE WET VAN 11 DECEMBER 1998 BETREFFENDE DE CLASSIFICATIE EN DE VEILIGHEIDSMACHTIGINGEN, VEILIGHEIDSATTESTEN EN VEILIGHEIDSADVIEZEN

Artikel 108

De definitie van het begrip “ontvanger”, die in artikel 31, 10°, van het voorontwerp staat, is ook belangrijk voor een goed begrip van ondertitel 3, aangezien dat begrip in artikel 125, § 1, tweede lid, 5°, van het voorontwerp gebruikt wordt.

ONDERTITEL 4

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR HET COÖRDINATIEORGAAN VOOR DE DREIGINGSANALYSE

Artikel 140

De definitie van het begrip “ontvanger”, die in artikel 31, 10°, van het voorontwerp staat, is ook belangrijk voor een goed begrip van ondertitel 4, aangezien dat begrip in artikel 158, § 1, tweede lid, 1°, c), van het voorontwerp gebruikt wordt.

ONDERTITEL 5

DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT BEPAALDE VERWERKINGEN VAN PERSOONSGEGEVENS DOOR DE PASSAGIERSINFORMATIE-EENHEID

Artikel 170

De definitie van het begrip “ontvanger”, die in artikel 31, 10°, van het voorontwerp staat, is ook belangrijk voor een goed begrip van ondertitel 5, aangezien dat begrip in artikel 183, § 1, tweede lid, 1°, c), van het voorontwerp gebruikt wordt.

Outre le caractère incohérent du dispositif, la section de législation considère que cette seule précision ne constitue pas une garantie suffisante des droits des personnes concernées et ne permet dès lors pas de répondre de manière adéquate aux exigences de prévisibilité et de proportionnalité sous-jacentes à toute ingérence au droit au respect de la vie privée.

SOUS-TITRE 3

DE LA PROTECTION DES PERSONNES PHYSIQUES À L’ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE DE LA LOI DU 11 DÉCEMBRE 1998 RELATIVE À LA CLASSIFICATION ET AUX HABILITATIONS, ATTESTATIONS ET AVIS DE SÉCURITÉ

Article 108

La définition de la notion de “destinataire” énoncée à l’article 31, 10°, de l’avant-projet est également pertinente pour la bonne compréhension du sous-titre 3 dès lors que cette notion est utilisée par l’article 125, § 1er, alinéa 2, 5°, de l’avant-projet.

SOUS-TITRE 4

DE LA PROTECTION DES PERSONNES PHYSIQUES À L’ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR L’ORGANE DE COORDINATION POUR L’ANALYSE DE LA MENACE

Article 140

La définition de la notion de “destinataire” énoncée à l’article 31, 10°, de l’avant-projet est également pertinente pour la bonne compréhension du sous-titre 4 dès lors que cette notion est utilisée par l’article 158, § 1er, alinéa 2, 1°, c), de l’avant-projet.

SOUS-TITRE 5

DE LA PROTECTION DES PERSONNES PHYSIQUES À L’ÉGARD DE CERTAINS TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL PAR L’UNITÉ D’INFORMATION DES PASSAGERS

Article 170

La définition de la notion de “destinataire” énoncée à l’article 31, 10°, de l’avant-projet est également pertinente pour la bonne compréhension du sous-titre 5 dès lors que cette notion est utilisée par l’article 183, § 1er, alinéa 2, 1°, c), de l’avant-projet.

Artikelen 175 en 176

Artikel 175 somt de rechten van de betrokkene op en vermeldt het recht om onjuiste gegevens te laten verbeteren of te laten verwijderen evenals het recht op verificatie door de bevoegde toezichthoudende autoriteit.

In artikel 176 wordt echter ook verwezen naar het recht van de betrokkene op toegang tot zijn persoonsgegevens. Dat recht wordt niet vermeld in artikel 175.

Er dient voor samenhang tussen die beide bepalingen gezorgd te worden.

Artikel 177

Het heeft geen zin om in een wetgevende tekst naar de wet te verwijzen teneinde de nadere regels te bepalen voor het instellen van het beroep waarin artikel 177 voorziet.

Die nadere regels moeten vastgelegd worden in de ontworpen wet.

Gesteld dat het de bedoeling is van de steller van het voorontwerp om te verwijzen naar de toepasselijke sectorale wet, namelijk de wet van 25 december 2016 “betreffende de verwerking van passagiersgegevens” (de zogenaamde PNR-wet), dient daar uitdrukkelijk naar verwezen te worden.

ONDERTITEL 6

BIJZONDERE BEPALINGEN

Artikel 187

Artikel 187, § 4, luidt als volgt:

“De [verwerking] van persoonsgegevens door de overheden bedoeld in [paragraaf 1] is niet onderworpen aan het toezicht van de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit.”

Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer opmerkt, kunnen de autoriteiten bedoeld in ondertitel 6 evenwel ook verwerkingen van persoonsgegevens uitvoeren die binnen het toepassingsgebied van de AVG vallen en bijgevolg onder toezicht van de Gegevensbeschermingsautoriteit vallen, tenzij uitdrukkelijk een andere toezichthoudende autoriteit aangewezen wordt.

Bijgevolg moet het dispositief aldus herzien worden dat het geen afbreuk doet aan de AVG en het recht op eerbiediging van het privéleven gewaarborgd wordt.

Articles 175 et 176

L’article 175 énonce les droits de la personne concernée et cite le droit à la rectification et la suppression des données inexactes ainsi que le droit à la vérification auprès de l’autorité de contrôle compétente.

L’article 176 se réfère cependant également au droit d’accès, par la personne concernée, à ses données à caractère personnel. Ce droit n’est pourtant pas visé par l’article 175.

Il convient de rendre ces deux dispositions cohérentes l’une à l’égard de l’autre.

Article 177

Il n’est pas pertinent de renvoyer à la loi dans un texte législatif pour fixer les modalités d’exercice du recours organisé par l’article 177.

Il convient de définir ces modalités d’exercice dans la loi en projet.

À supposer que l’intention de l’auteur de l’avant-projet soit de renvoyer à la loi sectorielle applicable, à savoir la loi du 25 décembre 2016 “relative au traitement des données des passagers” (la loi dite PNR), il convient de viser celle-ci expressément.

SOUS-TITRE 6

DISPOSITIONS PARTICULIÈRES

Article 187

L’article 187, § 4, prévoit que

“[l]e traitement de données à caractère personnel par les autorités visées au [paragraphe] premier n’est pas soumis au contrôle de l’autorité de protection des données visées dans la loi du 3 décembre 2017 portant création de l’autorité de protection des données”.

Cependant, comme le souligne la Commission de la protection de la vie privée, les autorités couvertes par le sous-titre 6 peuvent également se livrer à des traitements de données à caractère personnel entrant dans le champ d’application du RGPD et qui relèvent, dès lors, du contrôle de l’Autorité pour la protection des données, à moins qu’une autre autorité de contrôle ne soit expressément désignée.

Par conséquent, le dispositif sera revu afin de ne pas porter atteinte au RGPD et de garantir le droit au respect de la vie privée.

TITEL 4

Verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden

Artikel 188

1. Artikel 188 bevat verscheidene definities die verwijzen naar definities vervat in artikel 4 van de AVG.

Aangezien die verordening rechtstreeks toepasselijk is, heeft een dergelijke verwijzing geen zin en geeft ze aanleiding tot rechtsonzekerheid.

2. Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer opmerkt wordt, wekt het gebruik van de woorden "*afin d'être rendue publique*" in de Franse tekst van artikel 188, 2°, de indruk dat het de bedoeling zou zijn om de archieven openbaar te maken. Dat stemt niet overeen met het begrip archieven in de zin van de AVG (zie inzonderheid overweging 158), noch met de organieke wetgeving inzake de archieven.[25]

In de Franse tekst dienen die woorden dan ook vervangen te worden door de woorden "*afin d'y donner accès*".

3. Er is een gebrek aan samenhang tussen de definitie die in artikel 188, 5°, van het begrip "verwerkingsverantwoordelijke" gegeven wordt en die specifiek geldt voor titel 4, en de autonome definitie, die in artikel 4, 7°, van de AVG van datzelfde begrip gegeven wordt, en die trouwens in artikel 188, 5°, gehanteerd wordt.

4. In artikel 188, 12°, is de verwijzing naar overweging 33 van de AVG niet relevant, aangezien die bepaling geen normatieve strekking heeft en de definitie die in artikel 4, 11°, van de AVG van het begrip "toestemming" gegeven wordt, rechtstreeks toepasselijk is.

Artikelen 189 en 190

1. Uit artikel 190 volgt dat titel 4 van toepassing is op elke verwerking met het oog op archivering of onderzoek of statistische doeleinden die onder titel 1 valt, ook al is de verwerkingsverantwoordelijke niet van plan om zich te beroepen op de afwijkende regeling die aldus bij de wet ingevoerd wordt.

Overeenkomstig artikel 89, lid 2 en 3, van de AVG en zoals de Commissie voor de bescherming van de persoonlijke levenssfeer opmerkt, mogen afwijkingen van bepaalde rechten van de betrokkenen in geval van verwerking met het oog op archivering of wetenschappelijk of historisch onderzoek of

[25] Zie bijvoorbeeld artikel 2 van het decreet van het Waals Gewest van 6 december 2001 "betreffende de openbare archieven" dat bepaalt dat "[d]e stukken die, hoewel ze uit een administratief of rechtskundig oogpunt geen belang meer vertonen, doch een historische waarde behouden als administratieve, wetenschappelijke of culturele informatiebron waarvoor de bewaring zonder tijdsbeperking gerechtvaardigd is, (…) als definitief archief beschouwd [worden]".

TITRE 4

Traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

Article 188

1. Plusieurs des définitions de l'article 188 renvoient à des définitions précisées par l'article 4 du RGPD.

Dès lors que celui-ci est directement applicable, un tel renvoi n'est pas pertinent et est source d'insécurité juridique.

2. Comme le relève la Commission de la protection de la vie privée, l'utilisation par la version française de l'article 188, 2°, des termes "afin d'être rendue publique" laisse à penser que les archives auraient vocation à être publiées. Cela ne correspond pas à la notion d'archives au sens du RGPD (cf. notamment le considérant n° 158) et à la législation organique en matière d'archives[25].

Il convient dès lors, dans la version française, de remplacer ces termes par les mots "afin d'y donner accès".

3. La définition propre au titre 4 qui est donnée par l'article 188, 5°, à la notion de "responsable du traitement" est source d'incohérence avec la définition autonome qui est donnée à cette même notion – et qui est d'ailleurs utilisée par l'article 188, 5°, – par l'article 4, 7°, du RGPD.

4. À l'article 188, 12°, le renvoi au considérant n° 33 du RGPD n'est pas pertinent dès lors que cette disposition est dépourvue de portée normative et que la définition donnée par l'article 4, 11°, du RGPD à la notion de "consentement" est directement applicable.

Articles 189 et 190

1. Il résulte de l'article 190 que le titre 4 s'applique à tout traitement à des fins d'archives ou de recherche ou statistiques relevant du titre 1er et ce, même si le responsable de traitement n'entend pas se prévaloir du régime dérogatoire qui est ainsi organisé par la loi.

Conformément à l'article 89, paragraphes 2 et 3, du RGPD et comme le relève la Commission de la protection de la vie privée, les dérogations à certains droits des personnes concernées en cas de traitement à des fins archivistiques ou de recherches scientifiques ou historiques ou à des fins

[25] Voir par exemple l'article 2 du décret de la Région wallonne du 6 décembre 2001 "relatif aux archives publiques" qui précise que "[s]ont considérés comme archives définitives, les documents qui, ne présentant plus d'utilité administrative ou juridique, gardent une valeur historique comme source d'informations administratives, scientifiques ou culturelles justifiant leur conservation sans limitation de durée".

statistische doeleinden slechts bij de wet toegestaan worden "voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken".

De AVG staat de lidstaten dan ook niet toe om een algemeen afwijkende regeling in te voeren die van toepassing is op om het even welke verwerking met het oog op archivering of wetenschappelijk of historisch onderzoek of statistische doeleinden.

Titel 4 moet grondig herzien worden in het licht van die opmerking.

2. Zowel in het ontworpen artikel 189 als in het ontworpen artikel 190 moet "Dit hoofdstuk" vervangen worden door "Deze titel".

3. Ter wille van de rechtszekerheid moet artikel 190 aldus aangevuld worden dat daarin gepreciseerd wordt dat hoofdstuk I van titel 4 evenmin van toepassing is op de verwerkingen die verricht worden door de diensten bedoeld in titel 2 van het voorontwerp.

Artikel 192

1. De verplichting dat de verwerkingsverantwoordelijken een register moeten bijhouden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden wordt opgelegd bij artikel 30 van de AVG, dat ter zake ook nadere regels vaststelt.

Overeenkomstig lid 5 van die bepaling geldt de verplichting om een register bij te houden slechts onder bepaalde voorwaarden voor kleine ondernemingen of organisaties die in die bepaling omschreven worden. Artikel 89 van de AVG staat de lidstaten niet toe om van die bepaling af te wijken door alle verwerkingsverantwoordelijken te verplichten een register bij te houden, ongeacht de grootte van de onderneming of de organisatie. De steller van het voorontwerp moet kunnen aantonen dat aan de voorwaarden van artikel 30, lid 5, van de AVG voldaan is.

2. Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer opmerkt, staat artikel 89 van AVG de Belgische Staat evenmin toe om van de artikelen 13 en 14 van de AVG af te wijken. Van artikel 14 van de AVG mag maar afgeweken worden binnen de grenzen van lid 5 van die bepaling.

Artikel 194

In artikel 89, lid 1, van de AVG wordt het volgende bepaald:

"(….). Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt."

statistiques ne peuvent être autorisées par la loi que "dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités".

Le RGPD n'autorise dès lors pas les États membres à instaurer un régime dérogatoire général applicable à tout traitement à des fins archivistiques ou de recherches scientifiques ou historiques ou à des fins statistiques quel qu'il soit.

Le titre 4 doit être fondamentalement revu à la lumière de cette observation.

2. Tant au sein de l'article 189 que de l'article 190 en projet, il convient de viser non pas le "présent chapitre", mais le "présent titre".

3. Dans un souci de sécurité juridique, l'article 190 sera complété afin de préciser que le chapitre I du titre 4 ne vise pas non plus les traitements effectués par les services visés dans le titre 2 de l'avant-projet.

Article 192

1. C'est l'article 30 du RGPD qui prévoit et encadre l'obligation des responsables du traitement de tenir un registre des activités de traitement effectuées sous leur responsabilité.

Conformément au paragraphe 5 de cette disposition, l'obligation de tenir un registre n'est applicable aux petites entreprises ou aux organisations définies par cette disposition qu'à certaines conditions. L'article 89 du RGPD n'autorise pas les États membres à déroger à cette disposition en imposant la tenue d'un registre à tous les responsables de traitement, quelle que soit la taille de l'entreprise ou de l'organisation. L'auteur de l'avant-projet doit être en mesure de démontrer que les conditions de l'article 30, paragraphe 5, du RGPD sont remplies.

2. Comme le relève la Commission de la protection de la vie privée, de même, l'article 89 du RGPD n'autorise pas l'État belge à déroger aux articles 13 et 14 du RGPD. Il ne peut être dérogé à l'article 14 du RGPD que dans les limites du paragraphe 5 de cette disposition.

Article 194

Il ressort de l'article 89, paragraphe 1er, du RGPD, que:

"[…] [c]haque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière".

Artikel 194 van het voorontwerp gaat evenwel verder dan dat vereiste, aangezien daarbij wordt opgelegd dat in principe de verdere verwerking gehanteerd wordt, zelfs wanneer de identificatie van de betrokkenen mogelijk is. Bovendien wordt zo afbreuk gedaan aan de transparantie en de voorzienbaarheid van de gegevensverwerkingen die artikel 6, lid 2, van de AVG wil waarborgen, terwijl artikel 89 niet toestaat dat van dat artikel 6, lid 2 wordt afgeweken.

Bijgevolg moet het dispositief aldus herzien worden dat het binnen de grenzen van artikel 89, lid 1, van de AVG blijft.

Artikel 197

1. Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer opmerkt wordt, heeft het geen zin om in artikel 197, eerste lid, de verwerkingsverantwoordelijken die bij de betrokkene niet-gevoelige gegevens verzamelen te verplichten om hem daarvan op de hoogte te stellen, aangezien artikel 13 van de AVG reeds in een dergelijke verplichting voorziet.

2. Dat de verwerkingsverantwoordelijken die bij de betrokkene gevoelige gegevens verzamelen, hiervoor luidens artikel 197, tweede lid, van de betrokkene toestemming moeten krijgen, is in strijd met artikel 9, lid 2, van de AVG en gaat verder dan hetgeen bij lid 4 van diezelfde bepaling toegestaan wordt. De toestemming om op grond van artikel 9, lid 2, j), gevoelige gegevens te verwerken vormt immers een alternatief voor de toestemming waarin voorzien is in artikel 9, lid 2, a) tot i), om dergelijke gegevens te verwerken, terwijl de ontworpen bepaling de mogelijkheden waarin artikel 9, lid 2, voorziet om gevoelige gegevens te verwerken, beperkt. Gelet op de rechtstreekse werking van dat artikel 9, lid 2, heeft de voorliggende bepaling zelfs geen daadwerkelijke strekking.[26]

Het dispositief moet dienovereenkomstig herzien worden.

Artikel 201

Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer opmerkt, worden de beperkingen van het recht op gegevenswissing ("recht op vergetelheid") vastgelegd in artikel 17 van de AVG, opgesomd in lid 3 van die bepaling, en moet aan die bepaling geen uitvoering gegeven worden bij een nationale maatregel.

Een soortgelijke opmerking geldt voor artikel 209 van het voorontwerp.

Artikel 212

Volgens de bespreking van artikel 212 mogen de gegevens onder meer "gedepseudonimiseerd" worden

[26] Er wordt ook verwezen naar de opmerking die de Commissie voor de bescherming van de persoonlijke levenssfeer in haar advies maakt bij artikel 197.

L'article 194 de l'avant-projet va cependant au-delà de cette exigence puisqu'il impose le principe du recours au traitement ultérieur même lorsque l'identification des personnes concernées est possible. Cela porte par ailleurs atteinte à la transparence et à la prévisibilité des traitements de données que tend à garantir l'article 6, paragraphe 2, du RGPD, auquel l'article 89 n'autorise pas à déroger.

Par conséquent, le dispositif sera revu afin de rester dans les limites de l'article 89, paragraphe 1er, du RGPD.

Article 197

1. Comme le relève la Commission de la protection de la vie privée, à l'article 197, alinéa 1er, il n'est pas pertinent d'imposer aux responsables du traitement qui collectent des données non sensibles auprès de la personne concernée d'en informer celle-ci dès lors qu'une telle obligation est déjà prévue par l'article 13 du RGPD.

2. À l'article 197, alinéa 2, l'obligation qui est imposée aux responsables du traitement qui collectent des données sensibles auprès de la personne concernée d'en recueillir le consentement est contradictoire avec l'article 9, paragraphe 2, du RGPD et va au-delà de ce qui est autorisé par le paragraphe 4 de cette même disposition. En effet, l'autorisation de traiter des données sensibles sur la base de l'article 9, paragraphe 2, j), constitue une alternative à l'autorisation de traiter de telles données prévue par l'article 9, paragraphe 2, a) à i), alors que la disposition en projet restreint les possibilités de traiter des données sensibles telles qu'elles sont énoncées à l'article 9, paragraphe 2. Vu l'effet direct de cet article 9, paragraphe 2, la disposition à l'examen est même dépourvue de toute portée effective[26].

Le dispositif sera revu en conséquence.

Article 201

Comme le relève la Commission de la protection de la vie privée, les limitations au droit à l'effacement ("droit à l'oubli") reconnu par l'article 17 du RGPD sont prévues par le paragraphe 3 de cette disposition sans que celle-ci doive être exécutée par une mesure nationale.

Une observation similaire vaut pour l'article 209 de l'avant-projet.

Article 212

Selon le commentaire de l'article 212, les données peuvent être "dépseudonymisées" notamment

[26] Il est également renvoyé, dans l'avis de la Commission de la protection de la vie privée, à son observation sur l'article 197.

"om een maatregel te treffen ten aanzien van de betrokkene, bijvoorbeeld een medische behandeling".

Die mogelijkheid staat niet in het dispositief.

Artikel 215

Artikel 215, tweede lid, is nutteloos, gelet op de definitie van het begrip "verwerker" in artikel 4, 8°, van de AVG.

Dat lid moet dus worden geschrapt. De betreffende uitleg kan daarentegen in de bespreking van het artikel staan.

Artikel 217

1. Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer heeft opgemerkt, definieert artikel 4, punt 1, van de AVG het begrip "persoonsgegeven" als volgt:

"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon".

Geanonimiseerde gegevens kunnen bijgevolg niet meer worden aangemerkt als "persoonsgegevens" en vallen dan ook niet meer onder de AVG.

De term "geanonimiseerd" in artikel 217 dient dus te worden geschrapt.

2. Artikel 11, lid 2, van de AVG luidt als volgt:

"Wanneer de verwerkingsverantwoordelijke in de in lid 1 van dit artikel bedoelde gevallen kan aantonen dat hij de betrokkene niet kan identificeren, stelt hij de betrokkene daarvan indien mogelijk in kennis. In dergelijke gevallen zijn de artikelen 15 tot en met 20 niet van toepassing, *behalve wanneer de betrokkene, met het oog op de uitoefening van zijn rechten uit hoofde van die artikelen, aanvullende gegevens verstrekt die het mogelijk maken hem te identificeren*" (eigen cursivering).

Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer heeft toegelicht, voorziet artikel 11, lid 2, van de AVG derhalve reeds in een uitzondering op de artikelen 15, 16 en 18 van de AVG in het geval van gepseudonimiseerde gegevens.

Voorts staat artikel 89, lid 2, van de AVG niet toe dat de nationale wetgevers van die bepaling afwijken. Artikel 217 is echter in strijd met de uitzondering waarin is voorzien in artikel 11, lid 2, van de AVG, doordat het bepaalt dat van de rechten vastgelegd in de artikelen 15, 16 en 18 van de AVG in

"pour prendre une mesure à l'égard de la personne concernée, par exemple un traitement médical".

Cette éventualité n'est pas traduite dans le dispositif.

Article 215

L'article 215, alinéa 2, est inutile compte tenu de la définition de la notion de "sous-traitant" énoncée à l'article 4, 8°, du RGPD.

Cet alinéa sera dès lors supprimé. Cette explication peut, par contre, figurer dans le commentaire de l'article.

Article 217

1. Comme le relève la Commission de la protection de la vie privée, l'article 4, point 1, du RGPD définit la notion de "donnée à caractère personnel" comme étant

"toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommé "personnes concerné"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un n° d'identification, des données de localisation, un identifiant en ligne, un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale".

Par conséquent, des données anonymisées ne peuvent plus être qualifiées de "données à caractère personnel" et ne sont, dès lors, plus soumises au RGPD.

Il convient dès lors de supprimer le terme "anonymisées" à l'article 217.

2. Il résulte de l'article 11, paragraphe 2, du RGPD que,

"lorsque, dans les cas visés au paragraphe 1er du présent article, le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible. En pareil cas, les articles 15 à 20 ne sont pas applicables, *sauf lors que la personne concernée fournit, aux fins d'exercer les droits que lui confèrent ces articles, des informations complémentaires qui permettent de l'identifier*" (italiques ajoutés).

Ainsi que l'expose la Commission de la protection de la vie privée, une exception aux articles 15, 16 et 18 du RGPD est, dès lors, déjà prévue par l'article 11, paragraphe 2, du RGPD en cas de données pseudonymisées.

Par ailleurs, l'article 89, paragraphe 2, du RGPD n'autorise pas les législateurs nationaux à déroger à cette disposition. Or, l'article 217, en ce qu'il prévoit une dérogation aux droits prévus par les articles 15, 16 et 18 du RGPD en toutes circonstances lorsque les données sont anonymisées ou

alle omstandigheden wordt afgeweken wanneer de gegevens geanonimiseerd of gepseudonimiseerd zijn.

TITEL 5

Rechtsmiddelen en vertegenwoordiging van de betrokkenen

HOOFDSTUK I

Vordering tot staking

1. Gelet op het feit dat een daadwerkelijke controle van de regelgeving inzake bescherming van de persoonlijke levenssfeer uitermate belangrijk is om te waarborgen dat de inmenging in de uitoefening van het recht op eerbiediging van het privéleven evenredig is, rijst de vraag waarom het voorliggende voorontwerp, net zo min als de wet van 3 december 2017 niet, mogelijk maakt dat de Gegevensbeschermingsautoriteit zelf in eigen naam het bevoegde rechtscollege adieert ingeval de wet niet is nageleefd.

Momenteel voorziet de wet van 8 december 1992 nochtans in dat recht voor de Commissie voor de bescherming van de persoonlijke levenssfeer. Artikel 32, § 3, van die wet bepaalt dat "(…) de voorzitter van de Commissie ieder geschil aangaande de toepassing van deze wet en haar uitvoeringsmaatregelen aan de rechtbank van eerste aanleg [kan] voorleggen".

De aldus geboden mogelijkheid heeft het voordeel dat ze de Commissie voor de bescherming van de persoonlijke levenssfeer in staat stelt om op te treden om het belang van alle burgers te verdedigen, zonder dat die haar daartoe zelfs opdracht hoeven te geven. Het aldus verleende vorderingsrecht maakt het mogelijk de moeilijkheden te ondervangen die de burgers ondervinden bij de controle op de verwerking van hun gegevens, daar ze zich niet altijd bewust zijn van het bestaan van illegale praktijken.

De AVG schrijft in zijn artikel 58, lid 5, uitdrukkelijk voor dat een vorderingsrecht moet worden toegekend aan de Gegevensbeschermingsautoriteit:

"Elke lidstaat bepaalt bij wet dat zijn toezichthoudende autoriteit bevoegd is inbreuken op deze verordening ter kennis te brengen van de gerechtelijke autoriteiten en, waar passend, daartegen een rechtsvordering in te stellen of anderszins in rechte op te treden, teneinde de bepalingen van deze verordening te doen naleven".

Het ontwerp moet in het licht van deze opmerking opnieuw worden onderzocht.

2. De steller van het voorontwerp wordt erop gewezen dat de vordering tot staking weliswaar de vorm aanneemt van de vordering in kort geding, maar dat het wel gaat om een procedure na afloop waarvan de rechter een uitspraak ten gronde doet, en niet een uitspraak "alvorens recht [te doen]", zoals

pseudonymisées, porte atteinte à l'exception prévue par l'article 11, paragraphe 2, du RGPD.

TITRE 5

Voies de recours et représentation des personnes concernées

CHAPITRE I^ER

Recours en cessation

1. Compte tenu du fait que l'existence d'un contrôle effectif de la réglementation en matière de protection de la vie privée constitue une mesure essentielle afin de garantir la proportionnalité de l'ingérence dans l'exercice du droit au respect de la vie privée, la question se pose de savoir pourquoi l'avant-projet à l'examen, pas davantage que la loi du 3 décembre 2017, ne permet pas à l'Autorité de protection des données de saisir elle-même, en son propre nom, la juridiction compétente en cas de manquement aux exigences de la loi.

Actuellement, la loi du 8 décembre 1992 organise pourtant ce droit au bénéfice de la Commission de la protection de la vie privée: l'article 32, § 3, de cette loi dispose que "[…] le président de la Commission peut soumettre au tribunal de première instance tout litige concernant l'application de la présente loi et de ses mesures d'exécution".

La possibilité ainsi offerte présente cet intérêt qu'elle permet à la Commission de la protection de la vie privée d'agir pour défendre l'intérêt des citoyens dans leur ensemble, sans que ceux-ci doivent même la mandater. Le droit d'action ainsi conféré permet de pallier les difficultés que rencontrent les citoyens pour contrôler le traitement de leurs données dès lors que ceux-ci ne sont pas toujours conscients de l'existence de pratiques illégales.

La reconnaissance d'un droit d'action au profit de l'Autorité de protection des données est expressément envisagée par le RGPD, qui affirme, en son article 58, paragraphe 5, que

"[c]haque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation du présent règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement".

Le projet sera réexaminé à la lumière de cette observation.

2. L'attention de l'auteur de l'avant-projet est attirée sur le fait que, si l'action en cessation prend les formes de l'action en référé, il s'agit bien d'une procédure à l'issue de laquelle le juge statue au fond et non "avant dire droit", comme le précise à tort le commentaire des articles 222 à 232 et de façon par

in de bespreking van de artikelen 222 tot 232 ten onrechte en bovendien op tegenstrijdige wijze wordt gesteld daar in dezelfde bespreking voorts wordt gepreciseerd dat het om "een rechtsmiddel ten gronde" gaat.

3. De gebruikmaking van de procedure "zoals in kort geding", die onderstelt dat er een vermoeden van spoedeisendheid is, is weliswaar gerechtvaardigd voor maatregelen tot staking, mededeling, opschorting en rectificatie, vermeld in het voorontwerp, maar niets rechtvaardigt dat diezelfde procedure ook wordt gevolgd in het geval van een vordering tot vergoeding van de schade die is veroorzaakt door de eventuele schending van de regels betreffende de verwerking van persoonsgegevens (artikel 229). Aangezien het gaat om een vordering inzake gemeenrechtelijke contractuele of buitencontractuele aansprakelijkheid, zou ze moeten worden ingesteld en onderzocht volgens de gemeenrechtelijke procedure omdat ze anders de procedure tot staking zou verzwaren en daardoor de behandeling ervan zou vertragen, hetgeen het nut van de vordering "zoals in kort geding" gevoelig zou beperken.

Artikel 222

1. Het verdient aanbeveling de term "beroep" te vervangen door de term "vordering", aangezien het ontwerp betrekking heeft op iedere vordering die een verwerking waarmee de wet wordt geschonden, beoogt stop te zetten, of die de mededeling, opschorting of rectificatie van gegevens beoogt te verkrijgen. Het vervolg van de bepaling moet dienovereenkomstig worden aangepast.

Dezelfde opmerking geldt voor het vervolg van het voorontwerp.

2. Volgens de bespreking van de artikelen moet onder vordering "tot staking" worden verstaan:

"de vorderingen betreffende het door of krachtens de wet, ongeacht het criminele karakter van het strafbare feit, verleende recht op mededeling van persoonsgegevens [en] de vorderingen tot verbetering, tot verwijdering of tot het verbieden van de aanwending van onjuiste, onvolledige of niet ter zake dienende persoonsgegevens, waarvan de registratie, de mededeling of de bewaring verboden is en waartegen de betrokkene zich heeft verzet of die langer bewaard werden dan de toegestane duur".

Het gaat met andere woorden, nog steeds volgens de bespreking van de artikelen, om "een vordering tot staking en een vordering tot verkrijging van mededeling, opschorting en rectificatie van gegevens".

Daar de bevoegdheid van de voorzitter die zitting houdt zoals in kort geding verder gaat dan het strikte kader van het bevel tot staking, zou de precieze omvang van zijn bevoegdheden nader moeten worden omschreven in het dispositief.

ailleurs contradictoire puisque, dans le même commentaire, il est encore précisé qu'il s'agit "d'un recours sur le fond".

3. Si le recours à la procédure "comme en référé", qui bénéficie d'une présomption d'urgence, se justifie pour les mesures de cessation, de communication, de suspension et de rectification, visées à l'avant-projet, rien ne justifie par contre que la demande de réparation du préjudice causé par l'éventuelle violation des règles régissant le traitement des données à caractère personnel emprunte la même voie procédurale de l'action "comme en référé" (article 229). S'agissant d'une action en responsabilité contractuelle ou extracontractuelle de droit commun, elle devrait être introduite et instruite selon la procédure de droit commun, sous peine d'alourdir la procédure en cessation et d'en retarder corrélativement son traitement, ce qui amoindrirait sensiblement l'intérêt d'une action "comme en référé".

Article 222

1. Le terme "recours" sera avantageusement remplacé par celui d'"action" dès lors que le projet vise toute action ayant pour but de faire cesser un traitement poursuivi en violation de la loi ou tendant à obtenir la communication, la suspension et la rectification de données. La suite de la disposition sera adaptée en conséquence.

La même observation vaut pour la suite de l'avant-projet.

2. Selon le commentaire des articles, il faut comprendre que l'action "en cessation" recouvre

"toute demande relative au droit accordé par ou en vertu de la loi indépendamment du caractère pénal de l'infraction, d'obtenir communication de données à caractère personnel [et] toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, et pour laquelle la personne concernée s'est opposée au traitement ou qui a été conservée au-delà de la période autorisée".

En d'autres termes, il s'agit, toujours selon le commentaire des articles, "d'un recours en cessation ainsi que d'un recours tendant à obtenir communication, suspension et rectification de données".

Dès lors que la compétence du président siégeant comme en référé dépasse le cadre strict de l'ordre de cessation, il conviendrait que l'étendue exacte de ses compétences soit précisée dans le dispositif.

Artikel 223

1. Volgens artikel 223 is een vordering tot staking bij de voorzitter van de rechtbank van eerste aanleg uitgesloten wanneer de gegevensverwerking plaatsvindt

"in de loop van een opsporingsonderzoek, van een gerechtelijk onderzoek, een strafrechtelijke procedure voor de bodemrechter of een procedure voor de uitvoering van een strafrechtelijk vonnis".

Dezelfde bepaling stelt immers dat in die gevallen

"de beslissing over de rectificatie, schrapping, beperking van de behandeling, het verbod op gebruik of verwijdering van persoonsgegevens echter uitsluitend, volgens de fase van de procedure, tot het openbaar ministerie of de bevoegde strafrechter [behoort]".

2. Tijdens een opsporingsonderzoek treedt het openbaar ministerie op als vervolgende partij en verschijnt het als verwerende partij ten opzichte van de partij die een bevel tot staking of een maatregel bedoeld in het ontworpen artikel zou kunnen nastreven.

In die omstandigheden is het niet aanvaardbaar dat het openbaar ministerie zowel het opsporingsonderzoek voert als de bevoegdheid krijgt om uitspraak te doen over de vorderingen die ingesteld worden door de partij waarop de gegevensverwerking betrekking heeft. Een dergelijke regel zou de betrokken partij het recht ontnemen een vordering in te stellen bij een onafhankelijke en onpartijdige rechter.

De bepaling moet dientengevolge worden herzien.

3. Omwille van de rechtszekerheid en om elke controverse te voorkomen, zou in de artikelen 222 en 223 eenzelfde terminologie moeten worden gebruikt voor de vorderingen waaromtrent de rechter kan worden geadieerd. Beide bepalingen moeten in die zin worden herzien waarbij rekening moet worden gehouden met opmerking 2 die bij artikel 222 is gemaakt.

4. Het begrip "bevoegde strafrechter" is onduidelijk. Het kan namelijk gaan om de onderzoeksrechter, om de raadkamer of om de kamer van inbeschuldigingstelling, om de strafrechter die uitspraak ten gronde doet (correctionele rechtbank), of nog om de strafuitvoeringsrechtbank.

Om de preciseringen aan te brengen die nodig zijn om elke controverse te voorkomen en om de gevolgen van opmerking 2 te ondervangen, zou gepreciseerd moeten worden dat in de fase van het opsporingsonderzoek of het gerechtelijk onderzoek enkel de raadkamer bevoegd is om maatregelen in verband met de gegevensverwerking te nemen, tot uitspraak wordt gedaan over de procedure (verwijzing of buitenvervolgingstelling). De wet zou de procedureregels voor de adiëring van die rechtbank en voor het onderzoek van de zaak moeten vaststellen. Het moet mogelijk zijn een beroep in te stellen bij de kamer van inbeschuldigingstelling, wat in de bespreking van het artikel zou moeten worden bevestigd.

Article 223

1. Aux termes de l'article 223, l'action en cessation devant le président du tribunal de première instance est exclue lorsque le traitement des données s'effectue

"lors d'une information, d'une instruction, d'une procédure pénale devant le juge de fond ou d'une procédure d'exécution d'une peine pénale".

En effet, dans ces hypothèses, selon la même disposition,

"la décision concernant la rectification, la suppression, la limitation du traitement, l'interdiction d'utiliser, ou l'effacement de données à caractère personnel appartient toutefois exclusivement, suivant la phase de la procédure, au ministère public ou au juge pénal compètent".

2. Lors d'une information, le ministère public agit comme partie poursuivante et apparaît comme la partie adverse de celle qui pourrait souhaiter un ordre de cessation ou une mesure visée dans l'article en projet.

Il n'est pas admissible, dans ces conditions, que le ministère public se voie, concomitamment à l'information qu'il mène, reconnaître la compétence de statuer sur les demandes de la partie concernée par le traitement. Une telle règle priverait la partie concernée d'un droit d'action devant un juge indépendant et impartial.

La disposition sera revue en conséquence.

3. Dans un souci de sécurité juridique et afin d'éviter toute controverse, il conviendrait de recourir à une terminologie identique aux articles 222 et 223 en ce qui concerne les demandes dont le juge peut être saisi. Ces deux dispositions seront revues en ce sens en tenant compte de l'observation n° 2 formulée sous l'article 222.

4. La notion de "juge pénal compétent" est incertaine. Il peut en effet s'agir du juge d'instruction, de la chambre du conseil ou de la chambre des mises en accusation, du juge pénal statuant au fond (tribunal correctionnel) ou encore du tribunal de l'application des peines.

En vue d'apporter les précisions nécessaires à éviter toute controverse et pour rencontrer les conséquences de l'observation n° 2, il conviendrait de préciser que, dans la phase d'information ou d'instruction, jusqu'à la décision de règlement de la procédure (renvoi ou non-lieu), seule la chambre du conseil est compétente pour prendre les mesures concernant le traitement des données. Il conviendrait que la loi fixe les règles de procédure pour la saisine de cette juridiction et pour l'instruction de la cause. Un appel doit pouvoir être introduit devant la chambre des mises en accusation, ce que le commentaire de l'article devrait confirmer.

Er zou bepaald moeten worden dat, nadat uitspraak is gedaan over de procedure en beslist is tot buitenvervolgingstelling, de voorzitter van de rechtbank van eerste aanleg zijn algemene bevoegdheid weer terugkrijgt zodra de beslissing tot buitenvervolgingstelling genomen is en nadat de rechtsmiddelen zijn vervallen of aangewend. Indien de verwijzing wordt uitgesproken, zou daarentegen enkel de correctionele rechtbank bevoegd zijn. De wet zou de procedureregels voor de adiëring van die rechtbank en voor het onderzoek van de zaak moeten vaststellen. Het moet mogelijk zijn beroep in te stellen bij het hof van beroep, wat in de bespreking van het artikel zou moeten worden bevestigd.

Tot slot moet uitdrukkelijk worden bepaald dat tijdens de hele duur van de strafuitvoering enkel de strafuitvoeringsrechtbank bevoegd is voor vorderingen betreffende de gegevensverwerking.

5. Die bevoegdheid die een afwijking inhoudt ten gunste van de strafrechter dient enkel toepasselijk te zijn voor gegevensverwerkingen die rechtstreeks verband houden met de lopende strafprocedure. Die precisering moet in het dispositief worden aangebracht.

6. De steller van het voorontwerp zou moeten uitleggen hoe artikel 223 zich verhoudt tot de tekst van artikel 232, in het bijzonder ten aanzien van de exclusieve bevoegdheid die artikel 223 aan de “strafrechter” verleent.

Artikel 226

1. Aangezien het gaat om het gemene recht, is het niet relevant in paragraaf 1 te bepalen dat de beschikkingen tot staking in openbare terechtzitting moeten worden uitgesproken.

2. In paragraaf 2 dient te worden vermeld vanaf wanneer de daarin bepaalde termijn van acht dagen begint te lopen.

Artikel 228

Wat paragraaf 3 betreft, lijkt de beroepsrechter die de beslissing van de eerste rechter zou herzien, het best geplaatst te zijn om het bedrag te bepalen dat moet worden betaald aan de partij die de maatregel heeft uitgevoerd die herzien is.

Wanneer het evenwel gaat om de vergoeding van de partij die de voorlopige beslissing heeft uitgevoerd, valt evenwel niet te begrijpen waarom zou moeten worden afgeweken van het gemene recht betreffende de tenuitvoerlegging en het herstel van de schade veroorzaakt door een voorlopige tenuitvoerlegging die in beroep is herzien. Die vergoeding zou in een afzonderlijke procedure moeten worden geregeld.

Het is enkel zinvol dat de eerste rechter de maatregel neemt, indien het er in werkelijkheid om gaat het bedrag vast te stellen van een waarborg die de partij die last geeft tot de voorlopige tenuitvoerlegging van een bevel tot staking, dient te betalen.

Après la décision sur le règlement de la procédure, il conviendrait de préciser que, s’il s’agit d’une décision de non-lieu, à partir de celle-ci et après l’expiration des voies de recours ou après leur exercice, le président du tribunal de première instance recouvre sa compétence générale. Par contre, en cas de décision de renvoi, seul le tribunal correctionnel serait compétent. Il conviendrait que la loi fixe les règles de procédure pour la saisine de cette juridiction et pour l’instruction de la cause. Un appel doit pouvoir être introduit devant la cour d’appel, ce que le commentaire de l’article devrait confirmer.

Enfin, il convient de préciser expressément que, pendant toute la durée de l’exécution de la peine, seul le tribunal d’application des peines est compétent pour une demande concernant le traitement de données.

5. Cette compétence dérogatoire en faveur du juge pénal ne doit trouver à s’appliquer que pour les traitements de données en rapport direct avec la procédure pénale en cours. Cette précision doit être apportée dans le dispositif.

6. L’auteur de l’avant-projet est invité à s’expliquer quant à l’agencement de l’article 223 avec le dispositif de l’article 232, spécialement au regard de la compétence exclusive accordée par l’article 223 “au juge pénal”.

Article 226

1. S’agissant du droit commun, il n’est pas pertinent de préciser, au paragraphe 1er, que les ordonnances de cessation doivent être prononcées en audience publique.

2. Au paragraphe 2, il convient de préciser à partir de quel moment commence à courir le délai de huit jours qui y est prévu.

Article 228

Au paragraphe 3, il semble que le juge d’appel qui réformerait la décision du premier juge est le mieux placé pour fixer le montant à payer à la partie qui a exécuté la mesure réformée.

Toutefois, s’il s’agit d’indemniser la partie qui a exécuté la décision provisoire, on ne voit pas pour quels motifs il conviendrait de déroger au droit commun de l’exécution et de la réparation du préjudice causé par une exécution provisoire réformée en appel. Cette indemnisation devrait faire l’objet d’une procédure autonome.

La mesure ne pourrait être utilement prise par le premier juge que s’il s’agit en réalité de fixer le montant d’une caution à fournir par la partie qui poursuit l’exécution provisoire d’un ordre de cessation.

De bepaling moet worden herzien zodat ze de bedoelingen van de steller van het voorontwerp duidelijker weergeeft.

Artikel 231

Indien de steller van het voorontwerp wenst af te wijken van de artikelen 1026, 5°, en 1027, eerste lid, van het Gerechtelijk Wetboek, die voorschrijven dat een beroep wordt gedaan op een advocaat om een procedure op eenzijdig verzoekschrift in te leiden, moet hij uitleggen waarom die afwijkende regeling gerechtvaardigd is en dient, onder dat voorbehoud, de tekst in die zin explicieter te worden geformuleerd.

Artikel 233

1. In paragraaf 1 dienen de woorden ", het Gerechtelijk Wetboek" te worden ingevoegd tussen de woorden "bijzondere wetten" en de woorden "en het Wetboek van Strafvordering".

In de Franse tekst moet de verwijzing naar dat Wetboek bovendien worden vervangen door de vermelding "Code d'instruction criminelle".

2. De ontworpen bepaling maakt het louter mogelijk dat de rechtspersonen die door het slachtoffer of de slachtoffers van een schending van de wet zijn aangewezen, gemachtigd worden om in hun naam een rechtsvordering in te stellen. *A contrario* kan worden gesteld dat diezelfde rechtspersonen geen echt vorderingsrecht ter verdediging van collectieve belangen verleend wordt waardoor ze het bevoegde rechtscollege op eigen initiatief en in hun eigen naam zouden kunnen adiëren omtrent de tekortkomingen aan de wettelijke vereisten, bijvoorbeeld wanneer er geen "slachtoffer" gekend is of aangewezen kan worden.[27]

Naar aanleiding van het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en aangezien een daadwerkelijke controle van de regelgeving inzake de bescherming van de persoonlijke levenssfeer uitermate belangrijk is om te waarborgen dat de inmenging in het recht op eerbiediging van het privéleven evenredig is, vraagt de afdeling Wetgeving zich af waarom de steller van het voorontwerp geen gebruik wenst te maken van de mogelijkheid die artikel 80, lid 2, van de AVG biedt. Die bepaling luidt immers als volgt:

"De lidstaten kunnen bepalen dat een orgaan, organisatie of vereniging als bedoeld in lid 1 van dit artikel, over het recht beschikt om onafhankelijk van de opdracht van een betrokkene in die lidstaat klacht in te dienen bij de overeenkomstig artikel 77 bevoegde toezichthoudende autoriteit en de in de artikelen 78 en 79 bedoelde rechten uit te oefenen, indien het/zij van mening is dat de rechten van een betrokkene uit hoofde van deze verordening zijn geschonden ten gevolge van de verwerking".

[27] Vergelijk bijvoorbeeld met de artikelen 30 en 31 van de wet van 10 mei 2007 "ter bestrijding van bepaalde vormen van discriminatie".

La disposition sera revue pour exprimer plus clairement les intentions de l'auteur de l'avant-projet.

Article 231

Si l'auteur de l'avant-projet entend déroger aux articles 1026, 5°, et 1027, alinéa 1er, du Code judiciaire, qui imposent le recours à un avocat pour introduire une procédure sur requête unilatérale, il conviendrait qu'il explique les raisons qui justifieraient ce régime dérogatoire et que, sous cette réserve, le texte soit plus explicite en ce sens.

Article 233

1. Au paragraphe 1er, il convient d'ajouter les mots ", le Code judiciaire" entre les mots "les lois particulières" et les mots "et le Code de procédure pénale".

Dans la version française, la référence à ce Code sera en outre remplacée par la mention du "Code d'instruction criminelle"

2. La disposition en projet se borne à permettre que les personnes morales désignées par la ou les victimes d'une méconnaissance de la loi soient mandatées pour introduire, en leur nom, une action en justice. *A contrario*, lesdites personnes morales ne se voient pas reconnaître un véritable droit d'action d'intérêt collectif, qui leur permettrait de saisir la juridiction compétente, de leur propre initiative et en leur nom propre, des manquements aux exigences de la loi, par exemple en l'absence de "victime" identifiée ou identifiable[27].

À la suite de l'avis de la Commission de la protection de la vie privée, et dès lors que l'existence d'un contrôle effectif de la réglementation en matière de protection de la vie privée constitue une mesure essentielle afin de garantir la proportionnalité de l'ingérence au droit au respect de la vie privée, la section de législation se demande pourquoi l'auteur de l'avant-projet n'entend pas faire usage de la possibilité offerte par l'article 80, paragraphe 2, du RGPD, qui énonce en effet que

"les États membres peuvent prévoir que tout organisme, organisation ou association visé au paragraphe 1er du présent article, indépendamment de tout mandat confié par une personne concernée, a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle qui est compétente en vertu de l'article 77, et d'exercer les droits visés aux articles 78 et 79 s'il considère que les droits d'une personne concernée prévus dans le présent règlement ont été violés du fait du traitement".

[27] Comp. par exemple avec les articles 30 et 31 de la loi du 10 mai 2007 "luttant contre certaines formes de discrimination".

Momenteel zijn de gegevensverwerkingen immers zo talrijk, complex en vaak ondoorzichtig, dat het niet aangaat de burger ermee te belasten als enige te waken over de bescherming van zijn privéleven ten aanzien van technische problemen, die hem vaak te boven gaan, noch hem ermee te belasten de instellingen *ad hoc* op te dragen, en soms zelfs te overtuigen, in rechte op te treden.

De afdeling Wetgeving merkt overigens op dat het Grondwettelijk Hof in zijn arresten 133/2013 van 10 oktober 2013 en 87/2017 van 6 juli 2017 in wezen heeft geoordeeld dat de verschillen in behandeling die de wetgever in het leven roept bij de erkenning van het collectief vorderingsrecht ten voordele van rechtspersonen die de verdediging van de fundamentele rechten nastreven, discriminaties inhoudt die strijdig zijn met de artikelen 10 en 11 van de Grondwet, indien geen objectieve en redelijke verantwoording voorhanden is.

Het voorontwerp moet in het licht van de bovenstaande opmerking opnieuw worden onderzocht.

TITEL 6

Sancties

Artikel 234

1. Krachtens paragraaf 2 gelden de administratieve geldboeten niet voor de verwerkingsverantwoordelijken die de hoedanigheid van overheidsinstantie of openbaar orgaan hebben. Ze gelden daarentegen wel voor de verwerkingsverantwoordelijken van de privésector.

De verwerkingsverantwoordelijken van de openbare en de privésector verwerken echter gelijksoortige gegevens betreffende de burgers. Te denken valt onder meer aan de identificatiegegevens (naam, voornaam, adres, geboortedatum, enz., die zowel door administraties als privéondernemingen worden verwerkt), de fiscale gegevens (verwerkt door de FOD Financiën en bijvoorbeeld banken), de gezondheidsgegevens (verwerkt door socialezekerheidsinstellingen maar ook door verzekeringsinstellingen), enz.

In een digitale omgeving vormt de mogelijkheid om een administratieve geldboete op te leggen, een pressiemiddel om iedere verwerkingsverantwoordelijke de regels inzake gegevensbescherming scrupuleus te doen naleven. Daardoor is de administratieve geldboete een extra garantie voor de burger dat de regels inzake gegevensbescherming in principe zullen worden nageleefd.

Op de verwerkingsverantwoordelijken van de openbare sector moeten pressiemiddelen worden toegepast die minstens vergelijkbaar zijn met die welke voor de privésector gelden, en wel om vier hoofdredenen.

Ten eerste houden de verwerkingsverantwoordelijken van de openbare sector de gegevens bij die de burgers hun dienen te overhandigen om hun wettelijke en zelfs burgerlijke verplichtingen na te komen.

En effet, à l'heure actuelle, les traitements de données sont si nombreux, complexes et bien souvent opaques, qu'on ne peut faire reposer sur le citoyen la charge de veiller seul à la protection de sa vie privée à l'égard de problèmes techniques qui bien souvent le dépassent, ni de faire peser sur lui la démarche de mandater, et parfois même de convaincre, les institutions *ad hoc* pour agir en justice.

La section de législation rappelle au demeurant que la Cour constitutionnelle, dans ses arrêts n^{os} 133/2013 du 10 octobre 2013 et 87/2017 du 6 juillet 2017, a en substance estimé que, à défaut de justification objective et raisonnable, les différences de traitement réalisées par le législateur dans la reconnaissance d'un droit d'action collectif au profit de personnes morales ayant pour objectif la défense des droits fondamentaux, sont constitutives de discriminations contraires aux articles 10 et 11 de la Constitution.

L'avant-projet sera réexaminé à la lumière de l'observation qui précède.

TITRE 6

Sanctions

Article 234

1. En vertu du paragraphe 2, les amendes administratives ne sont pas applicables aux responsables de traitement ayant la qualité d'autorité publique ou d'organisme public. Par contre, les amendes administratives sont applicables aux responsables de traitement du secteur privé.

Or, les responsables de traitement du secteur public et du secteur privé traitent des données similaires relatives aux citoyens. On songe notamment aux données d'identification (nom, prénom, adresse, date de naissance, etc. traitées tant par les administrations que les sociétés privées), aux données fiscales (traitées par le SPF Finances et par les banques par exemple), aux données de santé (traitées par les institutions de sécurité sociale mais aussi les sociétés d'assurances), etc.

Dans l'environnement numérique, la possibilité d'infliger une amende administrative constitue un moyen de pression devant amener chaque responsable de traitement à veiller scrupuleusement au respect des règles de protection des données. De ce fait, l'amende administrative est une garantie supplémentaire, pour le citoyen, que les règles de protection des données seront en principe respectées.

Les responsables de traitement du secteur public doivent être soumis à des moyens de pression au moins équivalents à ceux qui pèsent sur le secteur privé, et ce pour quatre raisons principales.

Premièrement, les responsables de traitement du secteur public détiennent des données que les citoyens sont obligés de leur fournir sous peine de ne pas remplir leurs obligations légales, voire civiques.

Ten tweede kan, wanneer een overheidsinstantie of een openbaar orgaan de regels inzake de gegevensbescherming schendt, dus niet alleen het privéleven van de burgers, maar ook het vertrouwen van de burger in de Staat geschaad worden.[28]

Ten derde beperkt de AVG de rechten van de burgers ten aanzien van tal van die verwerkingen, zoals in de memorie van toelichting wordt vermeld (uitzondering op het verbod om gevoelige gegevens te verwerken om redenen van algemeen belang bepaald in een wet, uitzondering op het recht op vergetelheid, uitzondering op het recht op overdraagbaarheid, uitzondering op het recht op bezwaar, uitzondering op het verbod van profilering zonder menselijke tussenkomst, enz.). Die beperking van de rechten moet worden gecompenseerd door een passend toezicht op de verwerkingsverantwoordelijken.

Ten vierde is bij de wet van 3 december 2017 de controle afgeschaft die de sectorale comités belast met het toestaan of weigeren van de uitwisseling van gegevens binnen de administratie, uitoefenden. De afschaffing van die voorafgaande controle moet eveneens passend worden gecompenseerd opdat de openbare sector niet aan elke sanctie zou ontsnappen.

Weliswaar dreigt de continuïteit van de openbare dienst in het gedrang te komen indien boetes tot 20 miljoen euro worden opgelegd. Het zou aanvaardbaar zijn dat het voorontwerp, zonder van de boete af te zien, bijzondere plafonds vaststelt voor boetes die aan de openbare sector worden opgelegd. De steller van het voorontwerp zou zich in dat verband kunnen laten leiden door de boetes die aan de overheidsinstanties worden opgelegd op basis van artikel 101 van het Sociaal Strafwetboek of op basis van artikel 31 van de wet van 29 april 1999 “betreffende de organisatie van de elektriciteitsmarkt”.

Aangezien de verschillende behandeling van de verwerkingsverantwoordelijken van de openbare sector en die van de privésector niet op passende wijze wordt gerechtvaardigd, moet het dispositief dus worden herzien met inachtneming van de artikelen 10 en 11 van de Grondwet.

2. Vastgesteld wordt dat het voorontwerp aan de administratieve geldboete geen uitstel verbindt. Op dat punt wordt verwezen naar advies 62.383/2, op 7 december 2017 gegeven over een voorontwerp dat ontstaan heeft gegeven aan de wet van 11 maart 2018 “betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen”.[29]

Deuxièmement, la violation des règles de protection des données par une autorité publique ou un organisme public est donc susceptible non seulement de porter atteinte à la vie privée des citoyens mais également d’ébranler la confiance du citoyen en l’État[28].

Troisièmement, le RGPD restreint les droits de citoyens à l’égard de nombre de ces traitements, comme le rappelle l’exposé des motifs (exception à l’interdiction de traiter des données sensibles pour des raisons d’intérêt public déterminé dans une loi, exception au droit à l’oubli, exception au droit à la portabilité, exception au droit d’objecter, exception à l’interdiction de profilage sans intervention humaine, etc.). Cette limitation des droits doit être compensée par un contrôle adéquat des responsables de traitement.

Quatrièmement, la loi du 3 décembre 2017 a supprimé le contrôle qu’exerçaient les comités sectoriels chargés d’autoriser ou de refuser les échanges de données au sein de l’administration. La suppression de ce contrôle en amont doit également pouvoir être adéquatement compensée, au risque d’immuniser le secteur public de toute sanction.

Certes, imposer des amendes d’un montant pouvant aller jusqu’à 20 millions d’euros risquerait de mettre en péril la continuité du service public. Il serait donc admissible que l’avant-projet, sans renoncer à l’amende, fixe des plafonds particuliers lorsque ces amendes sont imposées au secteur public. À cet égard, l’auteur de l’avant-projet pourrait s’inspirer des montants des amendes imposées aux autorités publiques sur la base de l’article 101 du Code pénal social ou l’article 31 de la loi du 29 avril 1999 “relative à l’organisation du marché de l’électricité”.

Ainsi donc, à défaut d’une justification adéquate de la différence de traitement organisée entre les responsables de traitement du secteur public et les responsables de traitement du secteur privé, le dispositif doit être revu dans le respect des articles 10 et 11 de la Constitution.

2. Constatant que l’avant-projet ne prévoit pas d’assortir l’amende administrative du sursis, il est renvoyé sur ce point à l’avis n° 62.383/2 donné le 7 décembre 2017 sur un avant-projet devenu la loi du 11 mars 2018 “relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l’accès à l’activité de prestataire de services de paiement, et à l’activité d’émission de monnaie électronique, et à l’accès aux systèmes de paiement”[29].

---

28 Zie RvS 26 april 2005, nr. 143 683, Van Merris, *http://www.raadvst-consetat.be/Arrets/143000/600/143683.pdf#xml=http://www.raadvst-consetat.be/apps/dtsearch/getpdf.asp?DocId=6195&Index=c* %3a %5csoftware %5cdtsearch %5cindex %5carrets %5ffr %5c&HitCount=1&hits=e40+&04274620182712.

29 Opmerking geformuleerd over de artikelen 148, 161, 230 en 244 van het voorontwerp, *Parl.St.* Kamer 2017-18, nr. 54-2896/001, 323 tot 326 en 329.

28 Voir C.E., 26 avril 2005, n° 143 683, Van Merris, *http://www.raadvst-consetat.be/Arrets/143000/600/143683.pdf#xml=http://www.raadvst-consetat.be/apps/dtsearch/getpdf.asp?DocId=6195&Index=c* %3a %5csoftware %5cdtsearch %5cindex %5carrets %5ffr %5c&HitCount=1&hits=e01+&94305120182018.

29 Observation formulée sur les articles 148, 161, 230 et 244 de l’avant-projet, *Doc. parl.*, Chambre, 2017-2018, n° 54-2896/1, pp. 323 à 326 et 329.

Artikel 242

1. Uit de bespreking van artikel 242, § 1, blijkt dat gedragingen die strijdig zijn met de wet en/of met de AVG, zowel kunnen worden bestraft met administratieve sancties bepaald bij de artikelen 58, lid 2, en 83 van de AVG en bij artikel 234 van het voorontwerp, als met strafsancties bepaald bij de artikelen 235 of 236 van het voorontwerp.

De aldus gecreëerde mogelijkheid om strafsancties en administratieve sancties die als "strafsancties" in de zin van de gebruikelijke betreffende bepalingen kunnen worden aangemerkt, gecumuleerd toe te passen, wordt door de AVG zelf weliswaar niet categorisch uitgesloten (zie immers overweging 149 van de aanhef van de AVG), maar doet niettemin een moeilijkheid rijzen ten aanzien van het beginsel "*non bis in idem*", gewaarborgd bij onder meer artikel 4 van Protocol 7 bij het Europees Verdrag voor de rechten van de mens en artikel 50 van het Handvest van de grondrechten van de Europese Unie.

2. De strekking van het beginsel "*non bis in idem*", zoals dat naar voren komt uit artikel 4 van het voornoemde Protocol, is op 15 november 2016 bij het arrest *A. en B. v. Noorwegen* van de Grote Kamer van het Europees Hof voor de Rechten van de Mens, in wezen geherdefinieerd.[30]

Overeenkomstig dat arrest is de voortzetting en de voltooiing van parallelle strafrechtelijke procedures aanvaardbaar wanneer tussen beide procedures een voldoende nauw verband *ratione materiae* en *ratione temporis* bestaat.

Volgens het Europees Hof voor de rechten van de mens bestaat er een voldoende nauw verband *ratione temporis* wanneer er niet te veel tijd ligt tussen de procedures, zodat de rechtzoekende geen slachtoffer wordt van onzekerheid en van de langzame afwikkeling van de zaak.

Het bestaan van een voldoende nauw verband *ratione materiae* kan volgens het Europees Hof voor de rechten van de mens worden beoordeeld aan de hand van vier enuntiatief opgesomde criteria.[31]

Het eerste criterium houdt verband met het feit dat de verschillende procedures complementaire doelen nastreven en aldus niet alleen *in abstracto* maar ook *in concreto* betrekking hebben op verschillende aspecten van de handeling in kwestie die voor de vennootschap schadelijk is.

Het feit dat slechts een van de procedures van repressieve aard is of dat slechts een van de procedures een element van fraude impliceert, is in dat verband veelzeggend.[32] Het Hof stelt, steunend op zijn arrest-*Jussila* betreffende artikel 6 van het Europees Verdrag voor de rechten van de mens, het volgende:[33]

"La mesure dans laquelle la procédure administrative présente les caractéristiques d'une procédure pénale ordinaire

30 Zie in het bijzonder de paragrafen 130 tot 134 van dat arrest.
31 EHRM 15 november 2016, *A. en B. v. Noorwegen*, § 132.
32 *Ibid.*, § 144.
33 EHRM 23 november 2006, *Jussila v. Finland*.

Article 242

1. Il résulte du commentaire de l'article 242, § 1er, que des comportements contraires à la loi et/ou au RGPD peuvent faire l'objet tant de sanctions administratives prévues par les articles 58, paragraphe 2, et 83 du RGPD et par l'article 234 de l'avant-projet, que de sanctions pénales prévues par les articles 235 ou 236 de l'avant-projet.

La possibilité ainsi créée de cumuler l'application de sanctions pénales et d'amendes administratives qualifiables de "pénales" au sens des dispositions conventionnelles concernées, quoique n'étant pas catégoriquement exclue par le RGPD lui-même (voir en effet le considérant n° 149 de son préambule), n'en suscite pas moins une difficulté au regard du principe "*non bis in idem*" garanti notamment par l'article 4 du Protocole n° 7 à la Convention européenne des droits de l'homme et l'article 50 de la Charte des droits fondamentaux de l'Union européenne.

2. La portée du principe "*non bis in idem*", tel qu'il résulte de l'article 4 du Protocole précité, a été récemment redéfinie, en substance, par l'arrêt *A. et B. c. Norvège* rendu par la Grande Chambre de la Cour européenne des droits de l'homme, le 15 novembre 2016 [30].

Conformément à cet arrêt, la poursuite et l'aboutissement de procédures parallèles à caractère pénal est admissible lorsqu'il existe un lien à la fois matériel et temporel suffisamment étroit entre les procédures.

Selon la Cour européenne des droits de l'homme, il existe un lien temporel suffisamment étroit lorsque les procédures ne s'étalent pas trop dans le temps, de telle sorte que le justiciable ne soit pas en proie à l'incertitude et à des lenteurs.

En ce qui concerne l'existence d'un lien matériel suffisamment étroit, la Cour européenne des droits de l'homme indique quatre critères non exhaustifs permettant d'évaluer celui-ci[31].

Le premier tient au fait que les différentes procédures visent des buts complémentaires et concernent ainsi, non seulement *in abstracto* mais aussi *in concreto*, des aspects différents de l'acte préjudiciable à la société en cause.

Le fait que seule l'une des procédures ait un caractère répressif ou encore que seule l'une d'entre elles implique un élément de fraude est à cet égard révélateur[32]. La Cour précise, en se fondant sur son arrêt *Jussila*[33] relatif à l'article 6 de la Convention européenne des droits de l'homme, que

"la mesure dans laquelle la procédure administrative présente les caractéristiques d'une procédure pénale ordinaire

30 Voir spécialement les paragraphes 130 à 134 de cet arrêt.
31 Cour eur. D.H., arrêt *A et B c. Norvège*, 15 novembre 2016, § 132.
32 *Ibidem*, § 144.
33 Cour eur. D.H., arrêt *Jussila c. Finlande*, 23 novembre 2006.

est un élément important. Des procédures mixtes satisferont plus vraisemblablement aux critères de complémentarité et de cohérence si les sanctions imposables dans la procédure non formellement qualifiée de “pénale” sont spécifiques au comportement en question et ne font donc pas partie du “noyau dur du droit pénal” (…). Si, à titre additionnel, cette procédure n’a pas de caractère véritablement infamant, il y a moins de chances qu’elle fasse peser une charge disproportionnée sur l’accusé. À l’inverse, plus la procédure administrative présente de caractéristiques infamantes la rapprochant dans une large mesure d’une procédure pénale ordinaire, plus les finalités sociales poursuivies par la punition du comportement fautif dans des procédures différentes risquent de se répéter (*bis*) au lieu de se compléter”.[34]

Het tweede criterium slaat op de voorzienbaarheid van het gemengd-zijn van de procedures tot bestraffing van eenzelfde gedraging, zowel in rechte als in de praktijk.

Het derde criterium houdt in dat het verwijt van de dubbele bestraffing kan worden ondervangen door het feit dat de procedures in kwestie zo zijn gevoerd dat bij het verzamelen en beoordelen van bewijsmateriaal herhalingen zoveel mogelijk worden voorkomen, in het bijzonder dankzij een passende interactie tussen de verschillende bevoegde overheden, waaruit blijkt dat de vaststelling der feiten die in de ene procedure is gebeurd, in de andere procedure wordt overgenomen.

Het vierde criterium gaat over het feit dat de sanctie, opgelegd na de procedure die als eerste is afgelopen, in aanmerking is genomen in de procedure die als laatste is afgelopen, zodat de betrokkene *in fine* geen bovenmatige last moet torsen; dat laatste risico is minder waarschijnlijk indien er een compensatieregeling bestaat die ervoor moet zorgen dat de totale som van alle uitgesproken straffen evenredig is.

Uit arrest *A. en B. v. Noorwegen* blijkt dat het Europees Hof voor de rechten van de mens aan dat laatste criterium een doorslaggevend belang toekent[35] en aldus een centrale plaats inruimt voor het evenredigheidsbeginsel.

3. Zoals overweging 149 van de aanhef van de AVG uitdrukkelijk stelt, dient ook rekening te worden gehouden met de rechtspraak van het Hof van Justitie van de Europese Unie betreffende artikel 50 van het Handvest van de grondrechten van de Europese Unie. Die rechtspraak luidt als volgt:

“artikel 50 van het Handvest (…) moet [aldus] worden uitgelegd dat het zich niet verzet tegen een nationale regeling op grond waarvan tegen een persoon een strafvervolging kan worden ingesteld wegens het verzuim de verschuldigde btw binnen de wettelijke termijnen te betalen, terwijl die persoon voor dezelfde feiten reeds een onherroepelijk geworden administratieve sanctie van strafrechtelijke aard in de zin van dat artikel 50 is opgelegd, op voorwaarde dat die regeling

— een doel van algemeen belang nastreeft dat een dergelijke cumulatie van vervolgingsmaatregelen en sancties

[34] EHRM 15 november 2016, *A. en B. v. Noorwegen*, § 133.
[35] *Ibid.*, §§ 133 en 151.

est un élément important. Des procédures mixtes satisferont plus vraisemblablement aux critères de complémentarité et de cohérence si les sanctions imposables dans la procédure non formellement qualifiée de “pénale” sont spécifiques au comportement en question et ne font pas partie du noyau dur du droit pénal […]. Si, à titre additionnel, cette procédure n’a pas un caractère infamant, il y a moins de chance qu’elle fasse peser une charge disproportionnée sur l’accusé. À l’inverse, plus la procédure administrative présente de caractéristiques infamantes la rapprochant dans une large mesure d’une procédure pénale ordinaire, plus les finalités sociales poursuivies par la punition du comportement fautif dans les procédures différentes risquent de se répéter (*bis*) au lieu de se compléter”[34].

Le deuxième critère porte sur le caractère prévisible de la mixité des procédures de répression d’un même comportement, aussi bien en droit qu’en pratique.

En vertu du troisième critère, le fait que les procédures en question ont été conduites d’une manière qui évite autant que possible toute répétition dans le recueil et dans l’appréciation des éléments de preuve, notamment grâce à une interaction adéquate entre les diverses autorités compétentes, faisant apparaître que l’établissement des faits effectué dans l’une des procédures a été repris dans l’autre, permet d’éviter le reproche de la double répression.

Le quatrième critère est relatif au fait que la sanction imposée à l’issue de la procédure arrivée à son terme en premier a été prise en compte dans la procédure qui a pris fin en dernier, de manière à ne pas faire porter *in fine* à l’intéressé un fardeau excessif, ce dernier risque étant moins susceptible de se présenter s’il existe un mécanisme compensatoire conçu pour assurer que le montant global de toutes les peines prononcées est proportionné.

Il ressort de l’arrêt *A et B c. Norvège* que la Cour européenne des droits de l’homme accorde une importance prépondérante à ce dernier critère[35] et confère ainsi au principe de proportionnalité une place centrale.

3. Ainsi que le rappelle expressément le considérant n° 149 du préambule du RGPD, il y a également lieu d’avoir égard à la jurisprudence de la Cour de justice de l’Union européenne relative à l’article 50 de la Charte des droits fondamentaux de l’Union européenne. Selon cette jurisprudence,

“l’article 50 de la Charte doit être interprété en ce sens qu’il ne s’oppose pas à une réglementation nationale en vertu de laquelle des poursuites pénales peuvent être engagées contre une personne pour omission de verser la TVA due dans les délais légaux, alors que cette personne s’est déjà vu infliger, pour les mêmes faits, une sanction administrative définitive de nature pénale au sens de cet article 50, à condition que cette réglementation

— vise un objectif d’intérêt général qui est de nature à justifier un tel cumul de poursuites et de sanctions, à savoir la

[34] Cour eur. D.H., arrêt *A et B c. Norvège*, 15 novembre 2016, § 133.
[35] *Ibidem*, §§ 133 et 151.

kan rechtvaardigen, te weten de strijd tegen btw-delicten, waarbij die vervolgingsmaatregelen en die sancties elkaar aanvullende doelen moeten hebben,

— regels bevat waarmee voor onderlinge afstemming kan worden gezorgd, opdat de extra belasting die voor de betrokkenen uit een cumulatie van procedures voortvloeit, tot het strikt noodzakelijke wordt beperkt, en

— voorziet in regels waarmee ervoor kan worden gezorgd dat de zwaarte van het geheel van de opgelegde sancties is beperkt tot het strikt noodzakelijke in verhouding tot de ernst van het delict in kwestie".[36]

4. De steller van het voorontwerp moet aantonen dat hij een regeling invoert die, voor zowel de administratieve als de strafsancties waarin ze voorziet, de complementaire logica volgt die als enige wordt aanvaard door de hierboven vermelde Europese rechtspraken.

In dat verband dient te worden vastgesteld dat artikel 83, lid 2, b), van de AVG het volgende bepaalt:

"Bij het besluit over de vraag of een administratieve geldboete wordt opgelegd en over de hoogte daarvan wordt voor elk concreet geval naar behoren rekening gehouden met het volgende:

(…)

b) de opzettelijke of nalatige aard van de inbreuk;

(…)".

Bij het opleggen van een administratieve geldboete moet dus voortaan in voorkomend geval rekening worden gehouden met een vorm van opzet, zoals artikel 235, b) en d), van het voorontwerp daarin voorziet in strafzaken.

Om tegemoet te komen aan de vereisten van de voornoemde Europese rechtspraken, dient hoe dan ook op zijn minst uitdrukkelijk te worden voorzien in een compensatieregeling opdat de sanctie die aan het einde van de eerst aflopende procedure wordt opgelegd, in aanmerking wordt genomen in het kader van de tweede procedure.

Bovendien is het belangrijk dat de procedures worden gevoerd met concrete naleving van de criteria die het Europees Hof voor de rechten van de mens en het Hof van Justitie van de Europese Unie naar voren hebben geschoven. Teneinde de naleving van dat principe te waarborgen, zou het beter zijn om het voorontwerp aan te vullen met een regeling ter organisatie van de integratie van beide procedures die eventueel gevoerd kunnen worden. Het verdient hoe dan ook aanbeveling om in de memorie van toelichting uitleg te verschaffen over deze kwesties wat artikelen 234, 235 en 242 van het voorontwerp betreft.

[36] HvJ 20 maart 2018, C-524/15, *Menci*, punt 63.

lutte contre les infractions en matière de TVA, ces poursuites et ces sanctions devant avoir des buts complémentaires,

— contienne des règles assurant une coordination limitant au strict nécessaire la charge supplémentaire qui résulte, pour les personnes concernées, d'un cumul de procédures, et

— prévoie des règles permettant d'assurer que la sévérité de l'ensemble des sanctions imposées soit limitée à ce qui est strictement nécessaire par rapport à la gravité de l'infraction concernée"[36].

4. Il appartient à l'auteur de l'avant-projet d'établir qu'il met sur pied un mécanisme qui, prévoyant à la fois des sanctions administratives et des sanctions pénales, se situe dans la logique complémentaire qui est la seule admise par les jurisprudences européennes dont il est question ci-avant.

À cet égard, il y a lieu de constater qu'en vertu de l'article 83, paragraphe 2, b), du RGPD,

"[p]our décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants:

[…]

b) le fait que la violation a été commise délibérément ou par négligence;

[…]".

L'imposition d'une amende administrative tiendra donc compte, d'ores et déjà, d'un élément intentionnel, le cas échéant, tout comme cela est prévu en matière pénale par l'article 235, b) et d), de l'avant-projet.

En toute hypothèse, afin de répondre aux exigences des jurisprudences européennes précitées, il convient à tout le moins de prévoir expressément un mécanisme compensatoire afin que la sanction imposée à l'issue de la première procédure arrivant à son terme soit prise en considération dans le cadre de la seconde procédure.

Au surplus, il importe que les procédures soient conduites de manière à respecter concrètement les critères dégagés par la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne. Afin de garantir le respect de ce principe, mieux vaut compléter l'avant-projet par un dispositif organisant le caractère intégré des deux éventuelles procédures pouvant être menées. L'exposé des motifs gagnerait en tout état de cause à fournir des explications sur ces questions au sujet des articles 234, 235 et 242 de l'avant-projet.

[36] C.J.U.E., arrêt *Menci*, 20 mars 2018, C-524/15, § 63.

5. Het is, ten slotte, evident dat de protocolakkoorden tussen de bevoegde toezichthoudende autoriteiten en het college van procureurs-generaal, waarvan sprake is in artikel 242, noch de grondwettelijke prerogatieven van het openbaar ministerie noch de bevoegdheden van de wetgever inzake de strafrechtelijke procedure mogen aantasten.

TITEL 7

Het controleorgaan op de politionele informatie

De artikelen 36, § 2, en 40, § 2, van de wet van 3 december 2017 bepalen dat de leden van respectievelijk het directiecomité en het kenniscentrum van de Gegevensbeschermingsautoriteit "een functionele kennis hebben van de tweede landstaal en van het Engels. Ten minste één lid (…) moet ook een functionele kennis hebben van het Duits", en dat "[t]en hoogste twee derden van de leden van het kenniscentrum (…) van hetzelfde geslacht [is]".

De steller van het voorontwerp moet kunnen rechtvaardigen dat geen soortgelijke eisen worden gesteld aan de leden van het Controleorgaan op de politionele informatie, gelet op het grondwettelijke beginsel van gelijkheid en non-discriminatie.

Dat geldt des te meer daar de memorie van toelichting aanvoert dat het de bedoeling is de statuten van de verschillende toezichthoudende autoriteiten onderling in overeenstemming te brengen.

TITEL 8

Slotbepalingen

Artikel 283

Gelet op de datum waarop dit advies wordt gegeven, is het weinig waarschijnlijk dat de ontworpen wet voor 6 mei 2018 in het *Belgisch Staatsblad* wordt bekendgemaakt.

Ze zou dus terugwerkende kracht hebben voor titel 2 en eventueel voor andere artikelen van het voorontwerp die voor die datum in werking zouden moeten treden. Dat is niet aanvaardbaar, zelfs niet indien die datum overeenkomt met de datum waarop richtlijn 2016/680/EU moet zijn omgezet.

De bepaling moet dienovereenkomstig worden herzien.

Artikel 287

Paragraaf 2 van artikel 287 is niet duidelijk genoeg.

Die bepaling moet worden herzien.

5. S'agissant enfin des protocoles d'accord entre les autorités de contrôle compétentes et le Collège des procureurs généraux, envisagés par l'article 242, il va sans dire qu'ils ne peuvent empiéter ni sur les prérogatives constitutionnelles du ministère public ni sur les compétences du législateur en matière de procédure pénale.

TITRE 7

L'organe de contrôle de l'information policière

En vertu des articles 36, § 2, et 40, § 2, de la loi du 3 décembre 2017, les membres respectivement du comité de direction et du centre de connaissance de l'Autorité de protection des données "doivent avoir une connaissance fonctionnelle de la deuxième langue nationale et de l'anglais. Au moins un membre […] doit aussi posséder une connaissance fonctionnelle de l'allemand" et "deux tiers au maximum des membres […] sont du même sexe".

L'auteur de l'avant-projet doit être en mesure de justifier le fait que des exigences similaires ne sont pas reprises pour les membres de l'Organe de contrôle de l'information policière compte tenu du principe constitutionnel d'égalité et de non-discrimination.

Il en va d'autant plus ainsi que l'exposé des motifs invoque la volonté d'aligner les statuts des différentes autorités de contrôle entre eux.

TITRE 8

Dispositions finales

Article 283

Compte tenu de la date à laquelle le présent avis est donné, il est peu probable que la loi en projet soit publiée au *Moniteur belge* avant le 6 mai 2018.

Elle aurait donc un effet rétroactif pour ce qui concerne son titre 2 et éventuellement d'autres articles de l'avant-projet qui seraient indiqués comme devant entrer en vigueur à cette date, ce qui ne saurait être admis, même si celle-ci correspond à l'échéance à laquelle la directive n° 2016/680/UE doit être transposée.

La disposition sera revue en conséquence.

Article 287

Le paragraphe 2 de l'article 287 manque de clarté.

Cette disposition sera revue.

SLOTOPMERKINGEN

Het voorontwerp moet worden herzien zodat het in overeenstemming is met de regels van de wetgevingstechniek, de Nederlandse en de Franse tekst onderling overeenstemmen en manifest foute interne verwijzingen worden gecorrigeerd. Van de moeilijkheden die in de tekst voorkomen, worden hieronder slechts enkele voorbeelden gegeven:[37]

A. Wat betreft de regels der wetgevingstechniek:

1° Opsommingen moeten als 1°, 2°, 3°, enz. worden weergegeven in plaats van als "1.", "2.", "3.", enz. (bijvoorbeeld in artikel 8).

2° In artikel 10 moet de onderverdeling in paragrafen ("§ 1.", "§ 2.", enz.) worden vervangen door een opsomming van punten 1°, 2°, enz.

3° Wanneer een artikel in paragrafen is onderverdeeld, mag niets van dat artikel, ook niet het eerste lid ervan, buiten die onderverdeling vallen, zoals het geval is in artikel 11.

4° De verwijzingen, binnen een artikel, naar onderverdelingen van andere artikelen moeten correct zijn. De vermelding van de paragrafen of de leden waarin de betreffende onderverdelingen mag vermeld, mogen bijvoorbeeld niet worden weggelaten. Zo dient bijvoorbeeld in de inleidende zin van artikel 73, § 1, te worden verwezen naar artikel 31, § 1, 7°, a), c), d) en f), in plaats van naar artikel 31, 7°, a), c), d) en f), en dient in artikel 170, § 1, te worden verwezen naar artikel 74, § 2, 6°, in plaats van naar artikel 74, 6°.

5° De wijzigingen en opheffingen die het voorontwerp tot stand brengt, moeten melding maken van de nog geldende wijzigingen die in de betreffende teksten zijn aangebracht. Dat is bijvoorbeeld niet het geval voor de opheffing van de wet van 8 december 1992 bij artikel 282, eerste lid, van het voorontwerp van wet.

B. Wat betreft het gebrek aan overeenstemming tussen de Nederlandse en de Franse tekst: de artikelen 9, § 1, 2°, 18, § 3, 25, § 1, 50, eerste lid, en 88.

C. Wat betreft de manifest foute interne verwijzingen: de artikelen 43, § 3, 46, 68, 71 en 72, 177, 187, 243 en 287.

De griffier, *De voorzitter,*

Béatrice DRAPIER Pierre VANDERNOOT

[37] Er wordt verwezen naar de Handleiding die de Raad van State daarover heeft gepubliceerd: *Beginselen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten*, *www.raadvst-consetat.be,* tab "Wetgevingstechniek".

OBSERVATIONS FINALES

L'avant-projet doit être revu pour se conformer aux règles de la légistique, pour assurer la concordance des textes français et néerlandais et pour corriger des renvois internes manifestement inexacts. Seuls quelques exemples sont donnés ci-après des difficultés rencontrées[37].

A. En ce qui concerne les règles de légistique:

1° Les énumérations doivent être énoncées sous la forme de 1°, 2°, 3°, etc., et non "1.", "2.", "3.", etc. (par exemple à l'article 8).

2° À l'article 10, la division en paragraphes ("§ 1er.", "§ 2.", etc.) doit être remplacée par une énumération en 1°, 2°, etc.

3° Lorsqu'un article est divisé en paragraphe, aucune partie de cet article, pas même son premier alinéa, ne peut se soustraire à cette division, comme à l'article 11.

4° Les renvois, au sein des articles, à des subdivisions d'autres articles, doivent être opérées correctement, par exemple sans omettre la mention des paragraphes ou des alinéas au sein desquels les subdivisions concernées sont mentionnées. Ainsi, par exemple, dans la phrase introductive de l'article 73, § 1er, il y a lieu de se référer à l'article 31, § 1er, 7°, a), c), d) et f), et non à l'article 31, 7°, a), c), d) et f), et, à l'article 170, § 1er, c'est à l'article 74, § 2, 6°, et non à l'article 74, 6°, qu'il faut se référer.

5° Les modifications et abrogations portées par l'avant-projet doivent mentionner les modifications encore en vigueur subies par les textes concernés. Tel n'est par exemple pas le cas de l'abrogation par l'article 282, alinéa 1er, de l'avant-projet de la loi du 8 décembre 1992.

B. En ce qui concerne les discordances entre le texte français et le texte néerlandais: les articles 9, § 1er, 2°, 18, § 3, 25, § 1er, 50, alinéa 1er, et 88.

C. En ce qui concerne les renvois internes manifestement incorrects: les articles 43, § 3, 46, 68, 71 et 72, 177, 187, 243 et 287.

Le greffier, *Le président,*

Béatrice DRAPIER Pierre VANDERNOOT

[37] Il est renvoyé au *Guide* publié en la matière par le Conseil d'État, *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, *www.raadvst-consetat.be,* onglet "Technique législative".

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,
ONZE GROET.

Op de voordracht van de minister van Sociale zaken en Volksgezondheid, van de minister van Justitie, van de minister van Veiligheid en Binnenlandse Zaken, van de minister van Defensie en van de Staatssecretaris voor Privacy

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Sociale zaken en Volksgezondheid, de minister van Justitie, de minister van Veiligheid en Binnenlandse Zaken, de minister van Defensie en de Staatssecretaris voor Privacy zijn ermee belast in onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna volgt:

VOORAFGAANDE TITEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Deze wet is van toepassing op elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op elke niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

De Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG, hierna “de Verordening”, geldt ook voor de verwerking van persoonsgegevens bedoeld in de artikelen 2.2.a) en 2.2.b) van de Verordening.

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,
SALUT.

Sur la proposition de la ministre des Affaires sociales et de la Santé publique, du ministre de la Justice, du ministre de la Sécurité et de l’Intérieur, du ministre de la Défense et du Secrétaire d’État à la Protection de la vie privée

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

La ministre des Affaires sociales et de la Santé publique, le ministre de la Justice, le ministre de la Sécurité et de l’Intérieur, le ministre de la Défense et le Secrétaire d’État à la Protection de la vie privée sont chargés de présenter en notre nom à la Chambre des représentants le projet de loi dont la teneur suit:

TITRE PRÉLIMINAIRE

Article 1er

La présente loi règle une matière visée à l’article 74 de la Constitution.

Art. 2

La présente loi s’applique à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu’au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après “le Règlement” s’applique également au traitement de données à caractère personnel visés aux articles 2.2.a) et 2.2.b) du Règlement.

Art. 3

Het vrije verkeer van persoonsgegevens wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.

In het bijzonder kan de uitwisseling van persoonsgegevens tussen de verwerkingsverantwoordelijken, de bevoegde overheden, de diensten, organen en de ontvangers die zich in de titels 1 tot 3 van deze wet bevinden en die binnen het kader van de doelstellingen bedoeld in artikel 23.1.a) tot h), van de Verordening werken niet worden beperkt noch verboden omwille van dergelijke redenen, onverminderd de bevoegdheden van de bevoegde toezichthoudende autoriteit.

Een beperking of verbod kan evenwel plaatsvinden indien er een hoog risico bestaat dat de uitwisseling van gegevens zou leiden tot het omzeilen van deze wet, onverminderd de bevoegdheden van de bevoegde toezichthoudende autoriteit.

Art. 4

§ 1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker op het Belgische grondgebied, ongeacht of de verwerking al dan niet op het Belgische grondgebied plaatsvindt.

§ 2. Deze wet is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich op het Belgische grondgebied bevinden, door een niet in de Europese Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:

1° het aanbieden van goederen of diensten aan deze betrokkenen op het Belgische grondgebied, ongeacht of een betaling door de betrokkenen is vereist; of

2° het monitoren van het gedrag van deze personen, voor zover dit gedrag op het Belgische grondgebied plaatsvindt.

§ 3. In afwijking van de eerste paragraaf, wanneer de verwerkingsverantwoordelijke gevestigd is in een lidstaat van de Europese Unie en beroep doet op een verwerker met vestiging op het Belgische grondgebied is het recht van de lidstaat in kwestie van toepassing op de verwerker voor zover de verwerking plaatsvindt op het grondgebied van deze lidstaat.

Art. 3

La libre circulation des données à caractère personnel n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

En particulier, le partage des données à caractère personnel entre les responsables du traitement, les autorités compétentes, les services, organes et les destinataires, qui se situent dans les titres 1 à 3 de la présente loi et qui travaillent dans le cadre des finalités visées à l'article 23.1.a) à h), du Règlement ne peut être ni limité ni interdit pour de tels motifs, sans préjudice des compétences de l'autorité de contrôle compétente.

Une limitation ou une interdiction peut toutefois avoir lieu s'il y a un risque élevé que le partage des données aboutirait à contourner la présente loi, sans préjudice des compétences de l'autorité de contrôle compétente.

Art. 4

§ 1er. La présente loi s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire belge, que le traitement ait lieu ou non sur le territoire belge.

§ 2. La présente loi s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire belge par un responsable du traitement ou un sous-traitant qui n'est pas établi sur le territoire de l'Union européenne, lorsque les activités de traitement sont liées:

1° à l'offre de biens ou de services à ces personnes concernées sur le territoire belge, qu'un paiement soit exigé ou non desdites personnes; ou

2° au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu sur le territoire belge.

§ 3. Par dérogation du paragraphe premier, lorsque le responsable de traitement est établi dans un État membre de l'Union européenne et fait appel à un sous-traitant établi sur le territoire belge, le droit de l'État membre en question s'applique au sous-traitant pour autant que le traitement a lieu sur le territoire de cet État membre.

§ 4. Deze wet is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet op het Belgische grondgebied is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het Belgische recht van toepassing is.

Art. 5

De definities van de Verordening zijn van toepassing.

Voor de toepassing van deze wet wordt verstaan onder “overheid”:

1° de Federale Staat, de deelstaten en lokale overheden;

2° de rechtspersonen van publiek recht die van de Federale Staat, de deelstaten en lokale overheden afhangen;

3° de personen, ongeacht hun vorm en aard, die:

— opgericht zijn met het specifieke doel te voorzien in behoeften van algemeen belang die niet van industriële of commerciële aard zijn; en

— rechtspersoonlijkheid hebben; en

— waarvan hetzij de activiteiten in hoofdzaak door de overheden of instellingen vermeld in 1° of 2°, worden gefinancierd, hetzij het beheer onderworpen is aan toezicht door deze overheden of instellingen, hetzij de leden van het bestuursorgaan, leidinggevend orgaan of toezichthoudend orgaan voor meer dan de helft door deze overheden of instellingen zijn aangewezen;

4° de verenigingen bestaande uit één of meer overheden als bedoeld onder 1°, 2° of 3°.

TITEL 1

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

HOOFDSTUK I

Algemene bepalingen

Art. 6

Onverminderd bijzondere bepalingen, geeft deze titel uitvoering aan de Verordening.

§ 4. La présente loi s’applique au traitement de données à caractère personnel par un responsable du traitement qui n’est pas établi sur le territoire belge mais dans un lieu où le droit belge s’applique en vertu du droit international public.

Art. 5

Les définitions prévues dans le Règlement s’appliquent.

Pour l’application de la présente loi, on entend par “autorité publique”:

1° l’état fédéral, les entités fédérées et les autorités locales;

2° les personnes morales de droit public qui dépendent de l’État fédéral, des entités fédérées et des autorités locales;

3° les personnes, quelles que soient leur forme et leur nature qui:

— ont été créées pour satisfaire spécifiquement des besoins d’intérêt général ayant un caractère autre qu’industriel ou commercial; et

— sont dotées d’une personnalité juridique; et

— dont soit l’activité est financée majoritairement par les autorités publiques ou organismes mentionnés au 1° ou 2°, soit la gestion est soumise à un contrôle de ces autorités ou organismes, soit plus de la moitié des membres de l’organe d’administration, de direction ou de surveillance sont désignés par ces autorités ou organismes;

4° les associations formées par une ou plusieurs autorités publiques visées au 1°, 2° ou 3°.

TITRE 1ER

De la protection des personnes physiques a l’égard du traitement des données à caractère personnel

CHAPITRE IER

Dispositions générales

Art. 6

Sous réserve de dispositions particulières, le présent titre exécute le Règlement.

HOOFDSTUK II

Beginselen van verwerking

Art. 7

In uitvoering van artikel 8.1 van de Verordening is de verwerking van de persoonsgegevens van een kind met betrekking tot een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, rechtmatig indien de toestemming verleend wordt door kinderen van 13 jaar of ouder.

Wanneer deze verwerking betrekking heeft op de persoonsgegevens van een kind jonger dan 13 jaar, is die slechts rechtmatig indien de toestemming wordt verleend door de wettelijke vertegenwoordiger van dit kind.

Art. 8

§ 1. In uitvoering van artikel 9.2.g) van de Verordening worden de hieronder vermelde verwerkingen beschouwd als noodzakelijke verwerkingen om redenen van zwaarwegend algemeen belang:

1° de verwerking door verenigingen met rechtspersoonlijkheid of stichtingen die als hoofddoel de verdediging van de rechten van de mens en van de fundamentele vrijheden hebben, verricht voor de verwezenlijking van dat doel, op voorwaarde dat voor de verwerking een machtiging is verleend door de Koning bij een in Ministerraad overlegd besluit, na advies van de bevoegde toezichthoudende autoriteit. De Koning kan nadere regels bepalen voor die verwerking;

2° de verwerking beheerd door de stichting van openbaar nut "Stichting voor Vermiste en Seksueel Uitgebuite Kinderen" voor de ontvangst, de overzending aan de gerechtelijke overheid en de opvolging van gegevens betreffende personen die ervan verdacht worden in een bepaald dossier van vermissing of seksuele uitbuiting, een misdaad of wanbedrijf te hebben begaan;

3° de verwerking van persoonsgegevens die het seksuele leven betreffen, verricht door een vereniging met rechtspersoonlijkheid of door een stichting met als statutair hoofddoel de evaluatie, de begeleiding en de behandeling van personen van wie het seksueel gedrag gekwalificeerd kan worden als een misdrijf en die voor de verwezenlijking van dat doel door de bevoegde overheid worden erkend en gesubsidieerd. Voor dergelijke verwerkingen, waarvan de bedoeling moet bestaan in de evaluatie, begeleiding en behandeling van de in deze paragraaf bedoelde personen en de verwerking uitsluitend persoonsgegevens betreft die, wanneer ze

CHAPITRE II

Principes de traitement

Art. 7

En exécution de l'article 8.1 du Règlement, le traitement des données à caractère personnel relatif aux enfants en ce qui concerne l'offre directe de services de la société de l'information aux enfants, est licite lorsque le consentement a été donné par des enfants âgés de 13 ans ou plus.

Lorsque ce traitement porte sur des données à caractère personnel de l'enfant âgé de moins de 13 ans, il n'est licite que si le consentement est donné par le représentant légal de cet enfant.

Art. 8

§ 1er. En exécution de l'article 9.2.g) du Règlement, les traitements ci-après sont considérés comme traitements nécessaires pour des motifs d'intérêt public important:

1° le traitement effectué par des associations dotées de la personnalité juridique ou par des fondations qui ont pour objet social principal la défense et la promotion des droits de l'homme et des libertés fondamentales, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par le Roi, par arrêté délibéré en Conseil des ministres, après avis de l'autorité de contrôle compétente. Le Roi peut prévoir des modalités de ce traitement;

2° le traitement géré par la fondation d'utilité publique "Fondation pour Enfants Disparus et Sexuellement Exploités" pour la réception, la transmission à l'autorité judiciaire et le suivi de données concernant des personnes qui sont suspectées dans un dossier déterminé de disparition ou d'exploitation sexuelle, d'avoir commis un crime ou un délit;

3° le traitement de données à caractère personnel concernant la vie sexuelle, effectué par une association dotée de la personnalité juridique ou par une fondation, qui a pour objet statutaire principal l'évaluation, la guidance et le traitement des personnes dont le comportement sexuel peut être qualifié d'infraction, et qui est agréée et subventionné par l'autorité compétente en vue de la réalisation de ce but. Ces traitements, qui doivent être destinés à l'évaluation, la guidance et le traitement des personnes visées dans le présent paragraphe et qui ne peuvent porter que sur des données à caractère personnel qui, pour autant qu'elles soient relatives à

het seksueel leven betreffen, enkel betrekking hebben op laatstgenoemde personen, moet door de Koning bij een in een Ministerraad overlegd besluit, na advies van de bevoegde toezichthoudende autoriteit, een bijzondere, individuele machtiging worden verleend.

Het in eerste lid, 3°, bedoelde besluit verduidelijkt de duur van de machtiging, de nadere regels voor de gegevensverwerking, de nadere regels voor de controle van de gemachtigde vereniging of stichting door de bevoegde overheid en de wijze waarop door deze overheid aan de bevoegde toezichthoudende autoriteit verslag moet worden uitgebracht over de verwerking van persoonsgegevens in het kader van de verleende machtiging.

Behoudens bijzondere wettelijke bepalingen is de verwerking van genetische en biometrische gegevens door deze verenigingen en stichtingen, met als doel het op een unieke wijze identificeren van een fysieke persoon, verboden.

§ 2. De verwerkingsverantwoordelijke, en in voorkomend geval, de verwerker stelt een lijst op van de categorieën van personen die de persoonsgegevens kunnen raadplegen, met een beschrijving van hun hoedanigheid ten opzichte van de verwerking van de beoogde gegevens. Deze lijst wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit.

De verwerkingsverantwoordelijke, en in voorkomend geval, de verwerker zorgt dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling, ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.

§ 3. De stichting bedoeld in paragraaf 1, 2°, kan geen bestand houden betreffende personen die ervan verdacht worden een misdaad of wanbedrijf te hebben begaan of van veroordeelde personen. Zij wijst een functionaris voor gegevensbescherming aan.

Art. 9

In uitvoering van artikel 9.4 van de Verordening moet de verwerkingsverantwoordelijke, bij de verwerking van genetische, biometrische of gezondheidsgegevens, bovendien de volgende maatregelen nemen:

1° hij of, in voorkomend geval, de verwerker moet de categorieën van personen die de persoonsgegevens kunnen raadplegen, aanwijzen waarbij hun

la vie sexuelle, concernent les personnes visées dans le présent paragraphe, sont soumis à une autorisation spéciale individuelle accordée par le Roi, dans un arrêté royal délibéré en Conseil des ministres, après avis de l'autorité de contrôle compétente.

L'arrêté visé à l'alinéa premier, 3°, précise la durée de validité de l'autorisation, les modalités du traitement des données, les modalités de contrôle de l'association ou de la fondation par l'autorité compétente et la façon dont cette autorité informera l'autorité de contrôle compétente sur le traitement de données à caractère personnel effectué dans le cadre de l'autorisation accordée.

Sauf dispositions légales particulières, le traitement de données génétiques et biométriques aux fins d'identifier une personne physique de manière unique par ces associations et fondations est interdit.

§ 2. Le responsable du traitement et, le cas échéant, le sous-traitant établit une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l'autorité de contrôle compétente.

Le responsable du traitement et, le cas échéant, le sous-traitant veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

§ 3. La fondation visée au paragraphe premier, 2°, ne peut tenir un fichier de personnes suspectes d'avoir commis un crime ou un délit ou de personnes condamnées. Elle désigne également un délégué à la protection des données.

Art. 9

En exécution de l'article 9.4 du Règlement, le responsable du traitement doit prendre les mesures supplémentaires suivantes lors du traitement de données génétiques, biométriques ou des données concernant la santé:

1° les catégories de personnes, ayant accès aux données à caractère personnel, doivent être désignées par le responsable du traitement ou, le cas échéant, par

hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig moet worden omschreven;

2° hij of, in voorkomend geval, de verwerker moet de lijst van de aldus aangewezen categorieën van personen ter beschikking houden van de bevoegde toezichthoudende autoriteit;

3° hij moet ervoor zorgen dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken gegevens in acht te nemen.

Art. 10

§ 1. In uitvoering van artikel 10 van de Verordening wordt de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafrechtelijke inbreuken of daarmee verband houdende veiligheidsmaatregelen uitgevoerd:

1° door natuurlijke personen of door privaatrechtelijke of publiekrechtelijke rechtspersonen voor zover dat noodzakelijk is voor het beheer van hun eigen geschillen; of

2° door advocaten of andere juridische raadgevers in zoverre de verdediging van de belangen van hun cliënten dit vereist; of

3° door andere personen, indien de verwerking noodzakelijk is voor redenen van zwaarwegend algemeen belang voor het vervullen van taken van algemeen belang die door of krachtens een wet, een decreet, een ordonnantie of de Europese regelgeving zijn vastgesteld; of

4° voor zover de verwerking noodzakelijk is voor wetenschappelijk, historisch of statistisch onderzoek of met het oog op archivering.

§ 2. De verwerkingsverantwoordelijke, en in voorkomend geval, de verwerker stelt een lijst op van de categorieën van personen die de persoonsgegevens kunnen raadplegen, met een beschrijving van hun hoedanigheid ten opzichte van de verwerking van de beoogde gegevens. Deze lijst wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit.

De verwerkingsverantwoordelijke, en in voorkomend geval, de verwerker zorgt dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een

le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;

2° la liste des catégories des personnes ainsi désignées doit être tenue à la disposition de l'autorité de contrôle compétente ou, le cas échéant, par le sous-traitant;

3° il doit veiller à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Art. 10

§ 1er. En exécution de l'article 10 du Règlement, le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions pénales ou aux mesures de sûreté connexes est effectué:

1° par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige; ou

2° par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige; ou

3° par d'autres personnes lorsque le traitement est nécessaire pour des motifs d'intérêt public important pour l'accomplissement de tâches d'intérêt général confiées par ou en vertu d'une loi, d'un décret, d'une ordonnance ou du droit de l'Union européenne; ou

4° pour les nécessités de la recherche scientifique, historique ou statistique ou à des fins d'archives.

§ 2. Le responsable du traitement et, le cas échéant, le sous-traitant établit une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l'autorité de contrôle compétente.

Le responsable du traitement et, le cas échéant, le sous-traitant veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire,

evenwaardige contractuele bepaling, ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.

HOOFDSTUK III

Beperkingen op de rechten van de betrokkene

Art. 11

§ 1. In toepassing van artikel 23 van de Verordening, zijn de artikelen 12 tot 22 en 34 van de Verordening alsook het principe van transparantie van de verwerking bedoeld in artikel 5 van de Verordening, niet van toepassing op verwerkingen van persoonsgegevens rechtstreeks of onrechtstreeks afkomstig van de overheden bedoeld in titel 3, ten aanzien van:

1° de overheden en personen bedoeld in artikelen 14, 16 en 19 van de wet van 30 november 1998 naar wie deze gegevens werden overgebracht door de overheden bedoeld in titel 3;

2° tot de overheden en personen bedoeld in artikel 2, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging en in artikel 44/11/3*ter*, § § 2 en 3 en artikel 44/11/3*quater* van de wet op het politieambt, en die onder het toepassingsgebied van titel 1 vallen, en aan wie deze gegevens werden overgemaakt.

§ 2. De verwerkingsverantwoordelijke bedoeld in deze titel die in het bezit is van zulke gegevens deelt deze niet mee aan de betrokkene tenzij:

1° de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2° de betrokken overheid bedoeld in de eerste paragraaf hem dit toestaat.

De verwerkingsverantwoordelijke of de bevoegde overheid deelt niet mee dat hij in het bezit is van gegevens die van overheden bedoeld in titel 3 afkomstig zijn.

§ 3. De beperkingen bedoeld in de eerste paragraaf hebben eveneens betrekking op de logbestanden van de verwerkingen van een overheid bedoeld in titel 3 van deze wet in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel waartoe de overheid rechtstreeks toegang heeft.

§ 4. De verwerkingsverantwoordelijke bedoeld in deze titel die gegevens verwerkt rechtstreeks of onrechtstreeks afkomstig zijn van de overheden bedoeld in titel 3 beantwoordt minstens aan de volgende voorwaarden:

ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

CHAPITRE III

Limitations aux droits de la personne concernée

Art. 11

§ 1er. En application de l'article 23 du Règlement, les articles 12 à 22 et 34 du Règlement, ainsi que le principe de transparence du traitement visée à l'article 5 du Règlement, ne s'appliquent pas aux traitements de données à caractère personnel émanant directement ou indirectement des autorités visées au titre 3, à l'égard:

1° des autorités et personnes visées aux articles 14, 16 et 19 de la loi du 30 novembre 1998 auxquelles ces données ont été transmises par les autorités visées au titre 3;

2° des autorités et personnes visées à l'article 2, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace ainsi que celles mentionnées à l'article 44/11/3 ter § § 2 et 3 et à l'article 44/11/3 quater de la loi sur la fonction de police, et qui ressortent du titre 1er, et auxquelles ces données ont été transmises.

§ 2. Le responsable du traitement visé dans le présent titre qui est en possession de telles données ne les communique pas à la personne concernée à moins que:

1° la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que

2° l'autorité visée au paragraphe premier concernée l'y autorise.

Le responsable du traitement ou l'autorité compétente ne fait aucune mention qu'il est en possession de données émanant des autorités visées au titre 3.

§ 3. Les limitations visées au paragraphe premier portent également sur la journalisation des traitements d'une autorité visée au titre 3 de la présente loi dans les banques de données des responsables du traitement visés par le présent titre auxquelles l'autorité a directement accès.

§ 4. Le responsable de traitement visé dans le présent titre qui traite les données émanant directement ou indirectement des autorités visées au titre 3 répond au minimum aux conditions suivantes:

1° hij neemt de gepaste technische of organisatorische maatregelen om ervoor te zorgen dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt zijn tot hetgeen de personen nodig hebben om hun functies uit te oefenen of tot hetgeen nodig is voor de behoeften van de dienst;

2° hij neemt de gepaste technische of organisatorische maatregelen om de persoonsgegevens te beschermen tegen toevallige of niet-toegestane vernietiging, tegen toevallig verlies en tegen wijziging of elke andere niet-toegestane verwerking van die gegevens.

De leden van het personneel van de verwerkingsverantwoordelijke die de gegevens bedoeld in het eerste lid verwerken, zijn bovendien gebonden door de discretieplicht.

§ 5. Wanneer een verzoek of een klacht aanhangig wordt gemaakt bij de toezichthoudende autoriteit bedoeld in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, waarbij de verwerkingsverantwoordelijke melding maakt van de toepassing van dit artikel, wendt deze eerste zich tot het Vast Comité I opdat het de nodige verificaties verricht bij de autoriteit bedoeld in titel 3.

Na ontvangst van het antwoord van het Vast Comité I, brengt de Gegevensbeschermingsautoriteit de betrokkene enkel op de hoogte van de resultaten van de verificatie die betrekking hebben op persoonsgegevens die niet van de autoriteiten bedoeld in titel 3 afkomstig zijn, die ze wettelijk gehouden is mee te delen.

Indien het verzoek of de klacht enkel betrekking heeft op persoonsgegevens afkomstig van een autoriteit bedoeld in titel 3, antwoordt de Gegevensbeschermingsautoriteit, na ontvangst van het antwoord van het Vast Comité I, dat de nodige verificaties werden verricht.

Wanneer de Gegevensbeschermingsautoriteit gevat werd door de betrokkene, informeert ze deze volgens de vastgelegde wettelijke modaliteiten.

Art. 12

In toepassing van artikel 23 van de Verordening, is een verwerkingsverantwoordelijke die persoonsgegevens meedeelt aan een overheid bedoeld in ondertitels 2 en 4 van titel 3 van deze wet niet onderworpen aan de artikelen 14.1.e en 15.1.c van de Verordening en aan artikel 20 § 1 van deze wet en mag de betrokkene niet van deze overdracht op de hoogte brengen.

1° il adopte des mesures techniques ou organisationnelles appropriées pour assurer que l'accès aux données et les possibilités de traitement soient limités à ce dont les personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service;

2° il adopte des mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données.

Les membres du personnel du responsable de traitement qui traitent les données visées à l'alinéa 1er sont en outre tenus au devoir de discrétion.

§ 5. Lorsque l'autorité de contrôle visée dans la loi du 3 décembre 2017 portant création de l'autorité de protection des données est saisie d'une requête ou d'une plainte où le responsable du traitement fait état de l'application du présent article, celle-ci s'adresse au Comité permanent R pour qu'il fasse les vérifications nécessaires auprès de l'autorité visée au titre 3.

Après réception de la réponse du Comité permanent R, l'Autorité de protection des données n'informe la personne concernée que des résultats de la vérification portant sur les données à caractère personnel n'émanant pas des autorités visées au titre 3 qu'elle est légalement tenue de communiquer.

Si la requête ou la plainte ne porte que sur des données à caractère personnel émanant d'une autorité visée au titre 3, l'Autorité de protection des données répond, après réception de la réponse du Comité permanent R, que les vérifications nécessaires ont été effectuées.

Lorsque l'Autorité de protection des données a été saisie par la personne concernée, elle informe la personne concernée selon les modalités légales prévues.

Art. 12

En application de l'article 23 du Règlement, un responsable du traitement qui communique des données à caractère personnel à une autorité visée aux sous-titres 2 et 4 du titre 3 de la présente loi n'est pas soumis aux articles 14.1.e. et 15.1.c. du Règlement et à l'article 20 § 1er de la présente loi et ne peut informer la personne concernée de cette transmission.

Art. 13

Wanneer een overheid bedoeld in ondertitels 1 en 6 van titel 3 over een rechtstreekse toegang of over een rechtstreekse bevraging van een gegevensbank van de openbare of private sector beschikt, worden zijn verwerkingen van persoonsgegevens in deze gegevensbank beschermd door technische, organisatorische en individuele beveiligingsmaatregelen zodat alleen de volgende actoren toegang kunnen hebben tot de inhoud van deze verwerkingen om hun wettelijke toezichtsopdrachten uit te voeren:

1° de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke van de gegevensbank;

2° de functionaris voor gegevensbescherming van de overheid bedoeld in titel 3;

3° de verwerkingsverantwoordelijke van de gegevensbank of zijn gemachtigde;

4° de verwerkingsverantwoordelijke van de overheid bedoeld in titel 3;

5° elke andere persoon bepaald in een protocol tussen de verwerkingsverantwoordelijken voor zover de toegang past in de uitvoering van de wettelijke toezichtsopdrachten van de functionarissen voor gegevensbescherming en de verwerkingsverantwoordelijken.

De in het eerste lid vermelde beveiligingsmaatregelen zijn bedoeld om de wettelijke verplichtingen met betrekking tot de bescherming van bronnen, de bescherming van de identiteit van de agenten of de discretie van de onderzoeken van de overheden bedoeld in titel 3 te beschermen. Zij worden ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Deze verwerkingen mogen enkel toegankelijk zijn voor andere doeleinden dan deze die verband houden met het toezicht indien deze doeleinden vastgelegd zijn in een protocolakkoord door de betrokken verwerkingsverantwoordelijken binnen de doeleinden voorzien door of krachtens een wet.

Het protocolakkoord duidt de persoon of personen aan waarvoor de toegang tot de logbestanden noodzakelijk is ter vervulling van elke doeleinde toegelaten in het vorige lid.

De logbestanden en de in het eerste lid vermelde beveiligingsmaatregelen worden ter beschikking gesteld van het Vast Comité I.

Art. 13

Lorsqu'une autorité visée aux sous-titres 1 et 6 du titre 3 dispose d'un accès direct ou d'une interrogation directe à une banque de données du secteur public ou du secteur privé, ses traitements de données à caractère personnel dans cette banque de données sont protégés par des mesures de sécurité techniques, organisationnelles et individuelles de sorte que seuls les acteurs suivants puissent accéder au contenu de ces traitements pour assurer leurs missions légales de contrôle:

1° le délégué à la protection des données du responsable du traitement de la banque de données;

2° le délégué à la protection des données de l'autorité visée au titre 3;

3° le responsable du traitement de la banque de données ou son délégué;

4° le responsable du traitement de l'autorité visée au titre 3;

5° toute autre personne précisée dans un protocole entre les responsables du traitement, pour autant que l'accès s'inscrive dans l'exercice des missions légales de contrôle des délégués à la protection des données et des responsables du traitement.

Les mesures de sécurité mentionnées à l'alinéa premier visent à protéger les obligations légales portant sur la protection des sources, la protection de l'identité de leurs agents ou la discrétion des enquêtes des autorités visées au titre 3. Elles sont mises à la disposition de l'autorité de contrôle compétente.

Ces traitements ne peuvent être accessibles pour d'autres finalités que celles liées au contrôle que si ces finalités sont consignées dans un protocole d'accord par les responsables du traitement concernés parmi des finalités déterminées par ou en vertu d'une loi.

Le protocole d'accord désigne la ou les personne(s) dont l'accès aux journaux est nécessaire pour remplir chaque finalité autorisée à l'alinéa précédent.

Les journaux et les mesures de sécurité mentionnées à l'alinéa premier sont mis à la disposition du Comité permanent R.

De betrokken overheid bedoeld in titel 3 kan afwijken van het eerste lid wanneer de toegang tot zijn verwerkingen in een gegevensbank en de logbestanden geen afbreuk kan doen aan de beschermings- en discretiemaatregelen bedoeld in lid 2.

Art. 14

§ 1. In toepassing van artikel 23 van de Verordening zijn de in de artikelen 12 tot 22 en 34 van de Verordening bedoelde rechten en het principe van transparantie van de verwerking bedoeld in artikel 5 van de Verordening niet van toepassing op de verwerking van gegevens die rechtstreeks of onrechtstreeks afkomstig zijn van de gerechtelijke overheden, de politiediensten, de algemene inspectie van de federale politie en de lokale politie, de Cel voor Financiële Informatieverwerking, de algemene administratie van douane en accijnzen en de Passagiersinformatie-eenheid als bedoeld in titel 2, ten aanzien van:

1° de overheid, in de zin van artikel 5 van deze wet, aan wie de gegevens door de politiediensten werden bezorgd door of krachtens een wet, een decreet of een ordonnantie;

2° andere instanties en organen waarnaar de gegevens zijn verzonden door of krachtens een wet, een decreet of een ordonnantie.

§ 2. De verwerkingsverantwoordelijke bedoeld in deze titel die in het bezit is van dergelijke gegevens deelt deze niet mee aan de betrokkene tenzij:

1° de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2° de gerechtelijke overheden, de politiediensten, de algemene inspectie van de federale politie en de lokale politie, de Cel voor Financiële Informatieverwerking, de algemene administratie van douane en accijnzen en de Passagiersinformatie-eenheid als bedoeld in de eerste paragraaf, elk voor de gegevens die hen betreffen, hem dit toestaan.

De verwerkingsverantwoordelijke of de bevoegde overheid deelt niet mee dat hij in het bezit is van gegevens die van hen afkomstig zijn.

§ 3. De beperkingen bedoeld in de eerste paragraaf hebben eveneens betrekking op de logbestanden van de verwerkingen van de gerechtelijke overheden, de politiediensten, de algemene inspectie van de federale politie en de lokale politie, de Cel voor Financiële Informatieverwerking, de Algemene administratie van

L'autorité visée au titre 3 concernée peut déroger à l'alinéa premier lorsque l'accès à ses traitements dans une banque de données et aux journaux n'est pas susceptible de porter atteinte aux mésures de protection et de discrétion visées à l'alinéa 2.

Art. 14

§ 1er. En application de l'article 23 du Règlement, les articles 12 à 22 et 34 du Règlement, ainsi que le principe de transparence visé à l'article 5 du Règlement ne s'appliquent pas aux traitements de données émanant directement ou indirectement des autorités judiciaires, des services de police, de l'Inspection générale de la police fédérale et de la police locale, de la Cellule de Traitement des Informations Financières, de l'Administration générale des douanes et accises, et de l'Unité d'information des passagers visés au titre 2, à l'égard:

1° des autorités publiques, dans le sens de l'article 5 de la présente loi, auxquelles les données ont été transmises par ou en vertu de la loi, d'un décret ou d'une ordonnance;

2° d'autres organes et des organismes auxquelles les données ont été transmises par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

§ 2. Le responsable du traitement visé dans le présent titre qui est en possession de telles données ne les communique pas à la personne concernée à moins que:

1° la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que

2° les autorités judiciaires, les services de police, l'Inspection générale de la police fédérale et de la police locale, la Cellule de Traitement des Informations Financières, l'Administration générale des douanes et accises, et l'Unité d'information des passagers visés au paragraphe premier, chacun pour les données les concernant, l'y autorisent.

Le responsable du traitement ou l'autorité compétente ne fait aucune mention qu'il est en possession de données émanant de ceux-ci.

§ 3. Les limitations visées au paragraphe premier portent également sur la journalisation des traitements des autorités judiciaires, des services de police, de l'Inspection générale de la police fédérale et de la police locale, de la Cellule de Traitement des Informations Financières, de l'Administration générale des douanes

douane en accijnzen en de Passagiersinformatie-eenheid in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel waartoe deze rechstreeks toegang hebben.

Deze beperkingen zijn slechts van toepassing op de gegevens die aanvankelijk verwerkt werden voor de doeleinden bedoeld in artikel 27 van deze wet.

§ 4. De wettelijke waarborgen bedoeld in artikel 23.2 van de Verordening waaraan de overheden, organen of instellingen moeten beantwoorden, worden door of krachtens de wet bepaald.

De overheden, organen of instellingen die de gegevens verwerken die rechtstreeks of onrechtstreeks afkomstig zijn van de gerechtelijke overheden, de politiediensten, de algemene inspectie van de federale politie en de lokale politie, de Cel voor Financiële Informatieverwerking, de Algemene administratie van douane en accijnzen en de Passagiersinformatie-eenheid, beantwoorden minstens aan de volgende voorwaarden:

1° ze nemen de gepaste technische of organisatorische maatregelen om ervoor te zorgen dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt zijn tot hetgeen de personen nodig hebben om hun functies uit te oefenen of tot hetgeen nodig is voor de behoeften van de dienst;

2° ze nemen de gepaste technische of organisatorische maatregelen om de persoonsgegevens te beschermen tegen toevallige of niet-toegestane vernietiging, tegen toevallig verlies en tegen wijziging of elke andere niet-toegestane verwerking van die gegevens.

De leden van de overheden, organen of instellingen die de gegevens bedoeld in § 1 verwerken, zijn bovendien gebonden door de discretieplicht.

§ 5. Elk verzoek dat betrekking heeft op de uitoefening van de rechten bedoeld in de artikelen 12 tot 22 van de Verordening en dat gericht is aan een overheid, orgaan en organisme vermeld in § 1, 1° en 2°, wordt zo snel mogelijk en in elk geval binnen een maand na de ontvangst van het verzoek aan de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit bezorgd.

Wanneer de Gegevensbeschermingsautoriteit rechtstreeks gevat wordt door de betrokkene of door de verwerkingsverantwoordelijke die melding maakt van de

et accises et de l'Unité d'information des passagers dans les banques de données des responsables du traitement visés par le présent titre auxquelles ceux-ci ont directement accès.

Ces limitations ne valent que pour les données traitées initialement pour les finalités visées à l'article 27 de la présente loi.

§ 4. Les garanties légales visées à l'article 23.2 du Règlement auxquelles les autorités publiques, organes ou organismes doivent répondre sont consacrées par ou en vertu de la loi.

Les autorités publiques, organes ou organismes qui traitent les données émanant directement ou indirectement des autorités judiciaires, des services de police, de l'Inspection générale de la police fédérale et de la police locale, de la Cellule de Traitement des Informations Financières, de l'Administration générale des douanes et accises et de l'Unité d'information des passagers répondent au minimum aux conditions suivantes:

1° ils adoptent des mesures techniques ou organisationnelles appropriées pour assurer que l'accès aux données et les possibilités de traitement soient limités à ce dont les personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service;

2° ils adoptent des mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données.

Les membres des autorités publiques, organes ou organismes qui traitent les données visées au § 1er sont en outre tenus au devoir de discrétion.

§ 5. Toute demande portant sur l'exercice des droits visés aux articles 12 à 22 du Règlement, adressée à une autorité publique, organe et organisme mentionné au § 1er, 1° en 2° est transmise dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, à l'Autorité de protection des données visée dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

Lorsque l'Autorité de protection des données est saisie directement par la personne concernée ou par le responsable du traitement qui fait état de l'application

toepassing van dit artikel, verricht ze de nodige verificaties bij de betrokken overheid, organen, of organismes.

Wanneer de Gegevensbeschermingsautoriteit gevat werd door de betrokkene, informeert ze deze volgens de vastgelegde wettelijke modaliteiten.

§ 6. Wanneer de verwerking betrekking heeft op gegevens die aanvankelijk verwerkt werden door de politiediensten of de Algemene Inspectie van de federale politie en de lokale politie, richt de Gegevensbeschermingsautoriteit die rechtstreeks gevat wordt door de betrokkene of de verwerkingsverantwoordelijke die melding maakt van de toepassing van dit artikel, zich tot de toezichthoudende autoriteit bedoeld in artikel 71 opdat deze de nodige verificaties bij de bevoegde overheden, organen of instellingen verricht.

Wanneer de Gegevensbeschermingsautoriteit gevat werd door de betrokkene, na ontvangst van het antwoord van de autoriteit bedoeld in artikel 71, informeert de Gegevensbeschermingsautoriteit de betrokkene volgens de vastgelegde wettelijke modaliteiten.

§ 7. Wanneer de verwerking betrekking heeft op gegevens die aanvankelijk verwerkt werden door de gerechtelijke overheden, richt de Gegevensbeschermingsautoriteit die rechtstreeks gevat wordt door de betrokkene of de verwerkingsverantwoordelijke die melding maakt van de toepassing van dit artikel, zich tot de toezichthoudende autoriteit die bevoegd is voor de gerechtelijke overheden opdat deze de nodige verificaties bij de bevoegde overheden, organen of instellingen, bedoeld in § 1, 1° en 2°, verricht.

Wanneer de gegevensbeschermingsautoriteit gevat werd door de betrokkene, na ontvangst van het antwoord van de toezichthoudende autoriteit die bevoegd is voor de gerechtelijke overheden, informeert de Gegevensbeschermingsautoriteit de betrokkene volgens de vastgelegde wettelijke modaliteiten.

Art. 15

§ 1. In toepassing van artikel 23 van de Verordening, zijn de artikelen 12 tot 22 en 34 van de Verordening, evenals het principe van transparantie van de verwerking bedoeld in artikel 5 van de Verordening, niet van toepassing op de verwerkingen van persoonsgegevens door de Passagiersinformatie-eenheid zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

du présent article, elle procède aux vérifications nécessaires auprès des autorités, organes ou organismes concernés.

Lorsque l'Autorité de protection des données a été saisie par la personne concernée, elle informe la personne concernée selon les modalités légales prévues.

§ 6. Lorsque le traitement porte sur des données initialement traitées par les services de police ou l'Inspection générale de la police fédérale et de la police locale, l'Autorité de protection de données saisie directement par la personne concernée ou par le responsable du traitement qui fait état de l'application du présent article, s'adresse à l'autorité de contrôle visée à l'article 71 pour qu'elle réalise les vérifications nécessaires auprès des autorités, organes ou organismes compétents.

Lorsque l'Autorité de protection des données a été saisie par la personne concernée, après réception de la réponse de l'autorité visée à l'article 71, l'Autorité de protection des données informe la personne concernée selon les modalités légales prévues.

§ 7. Lorsque le traitement porte sur des données initialement traitées par les autorités judiciaires, l'Autorité de protection de données saisie directement par la personne concernée ou par le responsable du traitement qui fait état de l'application du présent article, s'adresse à l'autorité de contrôle compétente pour les autorités judiciaires pour qu'elle réalise les vérifications nécessaires auprès des autorités, organes ou organismes compétents, visés au § 1er, 1° et 2° .

Lorsque l'autorité de protection des données a été saisie par la personne concernée, après réception de la réponse de l'autorité de contrôle compétente pour les autorités judiciaires, l'Autorité de protection des données informe la personne concernée selon les modalités légales prévues.

Art. 15

§ 1er. En application de l'article 23 du Règlement, les articles 12 à 22 et 34 du Règlement, ainsi que le principe de transparence du traitement visé à l'article 5 du Règlement, ne s'appliquent pas aux traitements de données à caractère personnel par l'Unité d'information des passagers, telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers.

§ 2. De verwerkingsverantwoordelijke deelt de gegevens bedoeld in de eerste paragraaf niet mee aan de betrokkene tenzij de wet hem hiertoe verplicht in het kader van een geschillenprocedure.

§ 3. De verwerkingsverantwoordelijke doet geen enkele melding aan de betrokkene dat hij in het bezit is van gegevens die betrekking hebben op hem.

§ 4. De beperkingen bedoeld in de eerste paragraaf hebben eveneens betrekking op de logbestanden van de verwerkingen door de bovengenoemde Passagiersinformatie-eenheid, in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel.

§ 5. Wanneer een verzoek of een klacht aanhangig wordt gemaakt bij de bevoegde toezichthoudende autoriteit waarbij de verwerkingsverantwoordelijke zich beroept op de toepassing van dit artikel, antwoordt deze alleen dat de nodige verificaties zijn verricht.

Art. 16

Wanneer de persoonsgegevens in een rechterlijke beslissing of een gerechtelijk dossier zijn opgenomen of in het kader van strafrechtelijke onderzoeken en procedures worden verwerkt, worden de rechten bedoeld in de artikelen 12 tot 22 en 34 van de Verordening uitgeoefend overeenkomstig het Gerechtelijk wetboek, het wetboek van Strafvordering, de bijzondere wetten die betrekking hebben op de strafrechtspleging en hun uitvoeringsbesluiten.

Art. 17

§ 1. In toepassing van artikel 23 van de Verordening, mag een verwerkingsverantwoordelijke bedoeld in deze titel die persoonsgegevens meedeelt aan een gezamenlijke gegevensbank de betrokkene niet van deze overdracht op de hoogte brengen.

§ 2. Onder “gezamenlijke gegevensbank” wordt het gemeenschappelijk uitoefenen van de opdrachten uitgevoerd in het kader van titel 1 en de titels 2 of 3 door meerdere overheden, gestructureerd met behulp van geautomatiseerde procédés en toegepast op persoonsgegevens, bedoeld.

§ 2. Le responsable du traitement ne communique pas les données visées au paragraphe premier à la personne concernée à moins que la loi l’y oblige dans le cadre d’une procédure contentieuse.

§ 3. Le responsable du traitement ne fait aucune mention à la personne concernée qu’il est en possession de données la concernant.

§ 4. Les limitations visées au paragraphe premier portent également sur la journalisation des traitements effectués par l’Unité d’information des passagers précitée dans les banques de données des responsables du traitement visés par le présent titre.

§ 5. Lorsque l’autorité de contrôle compétente est saisie d’une requête ou d’une plainte où le responsable du traitement fait état de l’application du présent article, celle-ci répond uniquement que les vérifications nécessaires ont été effectuées.

Art. 16

Lorsque les données à caractère personnel figurent dans une décision judiciaire ou un dossier judiciaire, ou font l’objet d’un traitement lors d’une enquête judiciaire et d’une procédure pénale, les droits visés aux articles 12 à 22 et 34 du Règlement sont exercés conformément au Code judiciaire, au Code d’instruction criminelle, aux lois particulières relatives à la procédure pénale ainsi qu’aux arrêtés d’exécution.

Art. 17

§ 1er. En application de l’article 23 du Règlement, un responsable du traitement visé dans le présent titre qui communique des données à caractère personnel à une banque de données conjointe ne peut informer la personne concernée de cette transmission.

§ 2. Par “banque de données conjointe”, on entend l’exercice commun des missions effectuées dans le cadre du titre 1er et des titres 2 ou 3 par plusieurs autorités, structurée à l’aide de procédés automatisés et appliqués aux données à caractère personnel.

HOOFDSTUK IV

Verwerkingsverantwoordelijke en verwerker

Afdeling 1

Algemene bepalingen

Art. 18

In uitvoering van artikel 43 van de Verordening worden de certificeringsorganen geaccrediteerd, op basis van de norm EN-ISO/IEC 17065 en de aanvullende eisen die door de bevoegde toezichthoudende autoriteit zijn vastgesteld, door de nationale accreditatie-instantie die is aangewezen in overeenstemming met Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad.

Afdeling 2

Publieke sector

Art. 19

Deze afdeling is van toepassing op de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, die als een overheid worden beschouwd.

Art. 20

§ 1. Tenzij anders bepaald in bijzondere wetten, in uitvoering van artikel 6.2 van de Verordening moet de federale overheid, wanneer zij op basis van artikel 6.1.c) en e), van de Verordening persoonsgegevens doorgeeft aan enig andere overheid of privéorgaan, voor elke type van verwerking deze doorgifte formaliseren aan de hand van een protocol dat tot stand komt tussen de initiële verwerkingsverantwoordelijke en de verwerkingsverantwoordelijke ontvanger van de gegevens.

Dit protocol kan in het bijzonder voorzien in:

1° de identificatie van de federale overheid die de persoonsgegevens doorgeeft alsook die van de ontvanger;

2° de identificatie van de verwerkingsverantwoordelijke binnen de overheid die de gegevens doorgeeft alsook van de bestemmeling;

CHAPITRE IV

Responsable du traitement et sous-traitant

Section 1re

Dispositions générales

Art. 18

En exécution de l'article 43 du Règlement, les organismes de certification sont accrédités conformément à la norme EN-ISO/IEC 17065 et aux exigences supplémentaires établies par l'autorité de contrôle par l'organisme national d'accréditation désigné conformément au Règlement (CE) no 765/2008 du Parlement européen et du Conseil.

Section 2

Secteur public

Art. 19

La présente section est applicable aux services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police structuré organisé à deux niveaux qui sont considérés comme une seule autorité publique.

Art. 20

§ 1er. Sauf indication contraire dans des lois particulières, en exécution de l'article 6.2 du Règlement, l'autorité publique fédérale qui transfert des données à caractère personnel sur la base de l'article 6.1.c) et e), du Règlement à toute autre autorité publique, ou organisation privée, doit formaliser cette transmission pour chaque type de traitement par un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données.

Ce protocole peut prévoir notamment:

1° l'identification de l'autorité publique fédérale qui transfère les données à caractère personnel et celle du destinataire;

2° l'identification du responsable du traitement au sein de l'autorité publique qui transfère les données et au sein du destinataire;

3° de contactgegevens van de functionarissen voor gegevensbescherming binnen de overheid die de gegevens doorgeeft alsook van de bestemmeling;

4° de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5° de categorieën van doorgegeven persoonsgegevens en hun formaat;

6° de categorieën van ontvangers;

7° de wettelijke grondslag van de doorgifte;

8° de modaliteiten inzake gehanteerde communicatie;

10° elke specifieke maatregel die de doorgifte omkadert conform het proportionaliteitsbeginsel en de vereisten inzake gegevensbescherming door ontwerp en door standaardinstellingen;

11° de toepasselijke wettelijke beperkingen met betrekking tot de rechten van de betrokkene;

12° de modaliteiten inzake de rechten van de betrokkene bij de ontvanger;

14° de periodiciteit van de doorgifte;

15° de duur van het protocol;

16° de sancties die van toepassing zijn in geval van niet naleving van het protocol onverminderd titel 6.

§ 2. Het protocol wordt afgesloten na de respectievelijke adviezen van de functionaris voor gegevensbescherming van de federale overheid die houder is van de persoonsgegevens en van de bestemmeling. Deze adviezen worden toegevoegd aan het protocol. Wanneer ten minste een van deze adviezen niet gevolgd wordt door de verwerkingsverantwoordelijken vermeldt het protocol, in zijn inleidende bepalingen, de reden of redenen volgens dewelke het advies of de adviezen niet werden gevolgd.

§ 3. Het protocol wordt openbaar gemaakt op de website van de betrokken verwerkingsverantwoordelijken.

Art. 21

In uitvoering van artikel 37.4 van de Verordening wijst een privéorgaan dat persoonsgegevens verwerkt voor rekening van een federale overheid, of waaraan een federale overheid persoonsgegevens doorgeeft, een functionaris voor gegevensbescherming aan indien de

3° les coordonnées des délégués à la protection des données concernés au sein de l'autorité publique qui transfère les données ainsi que du destinataire;

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° les catégories de données à caractère personnel transférées et leur format;

6° les catégories de destinataires;

7° la base légale du transfert;

8° les modalités de communication utilisée;

10° toute mesure spécifique encadrant le transfert conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut;

11° les restrictions légales applicables aux droits de la personne concernée;

12° les modalités des droits de la personne concernées auprès du destinataire;

14° la périodicité du transfert;

15° la durée du protocole;

16° des sanctions applicables en cas de non- respect du protocole, sans préjudice du titre 6;

§ 2. Le protocole est adopté après les avis respectifs du délégué à la protection des données de l'autorité publique fédérale détendeur des données à caractère personnel et du destinataire. Ces avis sont annexés au protocole. Lorsqu'au moins un de ces avis n'est pas suivi par les responsables du traitement, le protocole mentionne, en ses dispositions introductives, la ou les raisons par laquelle ou lesquelles cet ou ces avis n'ont pas été suivis.

§ 3. Le protocole est publié sur le site internet des responsables du traitement concernés.

Art. 21

En exécution de l'article 37.4 du Règlement, un organisme privé qui traite des données à caractère personnel pour le compte d'une autorité publique fédérale ou à qui une autorité publique fédérale a transféré des données à caractère personnel désignent un délégué à

verwerking van deze gegevens een hoog risico kan inhouden zoals bedoeld in artikel 35 van de Verordening.

Art. 22

Indien de verwerking van persoonsgegevens een hoog risico kan inhouden zoals bedoeld in artikel 35 van de Verordening vraagt de federale overheid voorafgaand aan de verwerking het advies van de functionaris voor gegevensbescherming.

Wanneer de federale overheid doorgaat met de uitvoering van deze verwerking tegen het advies en de aanbevelingen van de functionaris voor gegevensbescherming in, dan moet hij zijn beslissing motiveren.

De motivering moet de redenen aangeven voor het niet volgen van het advies of de aanbevelingen.

Art. 23

In uitvoering van artikel 35.10 van de Verordening moet een specifieke gegevensbeschermingseffectbeoordeling worden verricht vóór de verwerkingsactiviteit, ook al werd reeds een algemene gegevensbeschermingseffectbeoordeling uitgevoerd in het kader van de vaststelling van de wettelijke grondslag.

HOOFDSTUK V

Verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen

Art. 24

§ 1. Onder verwerking van persoonsgegevens voor journalistieke doeleinden wordt verstaan de voorbereiding, het verzamelen, opstellen, voortbrengen, verspreiden of archiveren ten behoeve van het informeren van het publiek, met behulp van elke media en waarbij de verwerkingsverantwoordelijke zich de naleving van journalistieke deontologische regels tot taak stelt.

§ 2. De artikelen 7 tot 10, 11.2, 13 tot 16, 18 tot 20 en 21.1 van de Verordening zijn niet van toepassing op verwerkingen van persoonsgegevens voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen.

§ 3. De artikelen 30.4, 31, 33 en 36 van de Verordening zijn niet van toepassing op de verwerkingen

la protection des données lorsque le traitement de ces données peut engendrer un risque élevé tel que visé par l'article 35 du Règlement.

Art. 22

Lorsque le traitement de données à caractère personnel peut engendrer un risque élevé tel que visé par l'article 35 du Règlement, l'autorité publique fédérale demande préalablement au traitement l'avis du délégué à la protection des données.

Lorsque l'autorité publique fédérale poursuit la mise en œuvre de ce traitement contrairement à l'avis et aux recommandations du délégué à la protection des données, il doit motiver sa décision.

La motivation doit indiquer les raisons du non-suivi de l'avis ou des recommandations.

Art. 23

En exécution de l'article 35.10 du Règlement, une analyse d'impact spécifique de protection des données doit être effectuée avant l'activité de traitement, même si une analyse d'impact générale relative à la protection des données a déjà été réalisée dans le cadre de l'adoption de la base légale.

CHAPITRE V

Traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire

Art. 24

§ 1er. On entend par traitement de données à caractère personnel à des fins journalistiques la préparation, la collecte, la rédaction, la production, la diffusion ou l'archivage à des fins d'informer le public, par le biais de tout média et dont le responsable du traitement s'impose des règles de déontologie journalistique.

§ 2. Les articles 7 à 10, 11.2, 13 à 16, 18 à 20 et 21.1 du Règlement ne s'appliquent pas aux traitements de données à caractère personnel effectués à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire

§ 3. Les articles 30.4, 31, 33 et 36 du Règlement ne s'appliquent pas aux traitements à des fins

voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen wanneer door de toepassing ervan een voorgenomen publicatie in het gedrang wordt gebracht of het een controlemaatregel voorafgaandelijk aan de publicatie van een artikel zou uitmaken.

§ 4. De artikelen 44 tot 50 van de Verordening zijn niet van toepassing op doorgiften van persoonsgegevens verricht voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen aan derde landen of internationale organisaties in de mate dat het nodig is om het recht op bescherming van persoonsgegevens in overeenstemming te brengen met de vrijheid van meningsuiting en van informatie.

§ 5. Artikel 58 van de Verordening is niet van toepassing op verwerkingen van persoonsgegevens voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen wanneer de toepassing ervan aanwijzingen zou verschaffen over de bronnen van informatie of een controlemaatregel voorafgaandelijk aan de publicatie van een artikel zou uitmaken.

journalistiques et à des fins d'expression universitaire, artistique ou littéraire dans la mesure où leur application compromettrait une publication en projet ou constituerait une mesure de contrôle préalable à la publication d'un article.

§ 4. Les articles 44 à 50 du Règlement ne s'appliquent pas aux transferts de données à caractère personnel effectués à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire vers des pays tiers ou à des organisations internationales dans la mesure cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information.

§ 5. L'article 58 du Règlement ne s'applique pas aux traitements de données à caractère personnel effectués à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire lorsque son application fournirait des indications sur les sources d'information ou constituerait une mesure de contrôle préalable à la publication d'un article.

TITEL 2

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inebgrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid

TITRE 2

De la protection des personnes physiques a l'egard du traitement des donnees a caractere personnel par les autorites competentes a des fins de prevention et de detection des infractions penales, d'enquetes et de poursuites en la matiere ou d'execution de sanctions penales, y compris la protection contre les menaces pour la securite publique et la prevention de telles menaces

HOOFDSTUK I

Algemene bepalingen

Art. 25

Deze titel voorziet in de omzetting van de richtlijn 2016/680/EU van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

CHAPITRE I^ER

Dispositions générales

Art. 25

Le présent titre transpose la directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Art. 26

Voor de toepassing van deze titel wordt verstaan onder:

1° “persoonsgegevens”: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon – “de betrokkene”; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatiemiddel zoals een naam, een identificatienummer, locatiegegevens, een online identificatiemiddel of van èèn of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

2° “verwerking”: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, bekendmaking door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

3° “verwerkingsbeperking”: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken.

4° “profilering”: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling aspecten betreffende zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

5° “pseudonimisering”: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om te waarborgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

6° “bestand”: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn,

Art. 26

Pour l’application du présent titre, on entend par:

1° “données à caractère personnel”: toute information se rapportant à une personne physique identifiée ou identifiable, ci-après dénommée “personne concernée”; est réputée “identifiable” une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu’un nom, un numéro d’identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

2° “traitement”: toute opération ou tout ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l’enregistrement, l’organisation, la structuration, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l’interconnexion, la limitation, l’effacement ou la destruction.

3° “limitation du traitement”: le marquage de données à caractère personnel conservées en vue de limiter leur traitement futur.

4° “profilage”: toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

5° “pseudonymisation”: le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

6° “fichier”: tout ensemble structuré de données à caractère personnel accessibles selon des critères

ongeacht of dit gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

7° “bevoegde overheden”:

a) de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus;

b) de gerechtelijke overheden, te verstaan als de gemeenrechtelijke hoven en rechtbanken en het openbaar ministerie;

c) de Dienst Enquêtes van het Vast Comité van Toezicht op de politiediensten in het kader van zijn gerechtelijke opdrachten zoals bedoeld in artikel 16, 3e lid van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

d) de Algemene Inspectie van de federale politie en van de lokale politie zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten;

a) De Algemene administratie van de douane en accijnzen, in het kader van haar taak inzake opsporing, vaststelling en vervolging van de misdrijven die onder haar bevoegdheid vallen zoals bepaald in de Algemene Wet inzake douane en accijnzen van 18 juli 1977, en desgevallend in de Wet van 22 april 2003 houdende toekenning van de hoedanigheid van officier van gerechtelijke politie aan bepaalde ambtenaren van de administratie der douane en accijnzen.

b) de Passagiersinformatie-eenheid zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens;

g) de Cel voor financiële informatieverwerking bedoeld in artikel 76 van de wet van 18 septembre 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten.

h) de Dienst Enquêtes van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van zijn gerechtelijke opdrachten zoals bedoeld in artikel 40, 3e lid van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

7° “autorités compétentes”:

a) les services de police au sens de l’article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

b) les autorités judiciaires, entendues comme les cours et tribunaux du droit commun et le ministère public;

c) le service d’enquêtes du Comité permanent de contrôle des services de police dans le cadre de ses missions judiciaires telles que prévues à l’article 16, alinéa 3, de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l’Organe de coordination pour l’analyse de la menace;

d) l’Inspection générale de la police fédérale et de la police locale, tel que visé à l’article 2 de la loi du 15 mai 2007 sur l’Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police;

e) l’Administration générale des douanes et accises, dans le cadre de sa mission relative à la recherche, la constatation et la poursuite des infractions déterminée par la Loi générale du 18 juillet 1977 sur les douanes et accises et, le cas échéant, par la Loi du 22 avril 2003 octroyant la qualité d’officier de police judiciaire à certains agents de l’Administration des douanes et accises.

f) l’Unité d’information des passagers, telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers;

g) la Cellule de traitement des informations financières visée à l’article 76 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l’utilisation des espèces.

h) le service d’enquêtes du Comité permanent de contrôle des services de renseignement dans le cadre de ses missions judiciaires telles que prévues à l’article 40, alinéa 3, de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l’Organe de coordination pour l’analyse de la menace;

8° “verwerkingsverantwoordelijke”: de bevoegde overheid die, alleen of samen met andere, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer de doeleinden van en de middelen voor die verwerking door of krachtens een wet, een decreet of een ordonnantie zijn bepaald, is de verwerkingsverantwoordelijke de entiteit die door of krachtens de wet, het decreet of de ordonnantie als de verwerkingsverantwoordelijke wordt aangewezen.

9° “verwerker”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat namens de verwerkingsverantwoordelijke of een andere verwerker persoonsgegevens verwerkt.

10° “ontvanger”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie of waaraan de persoonsgegevens worden bekendgemaakt. Overheden die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig de wet, het decreet of de ordonnantie, gelden echter niet als ontvangers; de verwerking van die persoonsgegevens door deze overheidsinstanties voldoet aan de toepasselijke regels inzake gegevensbescherming overeenkomstig de doeleinden van de verwerking.

11° “inbreuk op de beveiliging”: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

12° “genetische gegevens”: persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.

13° “biometrische gegevens”: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

14° “gezondheidsgegevens”: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, met inbegrip van

8° “responsable du traitement”: l’autorité compétente qui, seule ou conjointement avec d’autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens de ce traitement sont déterminés par la loi, le décret ou l’ordonnance, le responsable du traitement est l’entité désignée comme responsable du traitement par ou en vertu de cette loi, ce décret ou cette ordonnance.

9° “sous-traitant”: la personne physique ou morale, l’autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ou d’un autre sous-traitant.

10° “destinataire”: la personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu’il s’agisse ou non d’un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d’une mission d’enquête particulière conformément à la loi, au décret ou à l’ordonnance, ne sont pas considérées comme des destinataires; le traitement de ces données par ces autorités publiques est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

11° “brèche de sécurité”: une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l’altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d’une autre manière, ou l’accès non autorisé à de telles données.

12° “données génétiques”: les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d’une personne physique qui donnent des informations uniques sur la physiologie ou l’état de santé de cette personne physique et qui résultent, notamment, d’une analyse d’un échantillon biologique de la personne physique en question.

13° “données biométriques”: les données à caractère personnel résultant d’un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d’une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

14° “données concernant la santé”: les données à caractère personnel relatives à la santé physique ou mentale d’une personne physique, y compris la

de gegevens over verleende gezondheidsdiensten, waarmee informatie over zijn gezondheidstoestand wordt gegeven.

15° “toezichthoudende autoriteit”: de onafhankelijke overheidsinstantie die bij wet belast is met het toezicht op de toepassing van deze titel.

16° “internationale organisatie”: een organisatie en de daaronder vallende internationaal publiekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.

17° “internationale overeenkomst”: een van kracht zijnde bilaterale of multilaterale internationale overeenkomst tussen lidstaten van de Europese Unie en derde landen op het gebied van justitiële samenwerking en/of politiële samenwerking.

Art. 27

Deze titel is van toepassing op de verwerkingen van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

HOOFDSTUK II

Beginselen van verwerking

Art. 28

De persoonsgegevens moeten:

1° rechtmatig en eerlijk worden verwerkt;

2° voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt;

3° toereikend, ter zake dienend en niet bovenmatig zijn in verhouding tot de doeleinden waarvoor zij worden verwerkt;

4° juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren;

prestation de services de soins de santé, qui révèlent des informations sur l’état de santé de cette personne.

15° “autorité de contrôle”: l’autorité publique indépendante chargée par la loi de surveiller l’application du présent titre.

16° “organisation internationale”: une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d’un tel accord.

17° “accord international”: tout accord international bilatéral ou multilatéral en vigueur entre les États membres de l’Union européenne et des pays tiers dans les domaines de la coopération judiciaire et/ou de la coopération policière.

Art. 27

Le présent titre s’applique aux traitements de données à caractère personnel effectués par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière ou d’exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

CHAPITRE II

Principes de traitement

Art. 28

Les données à caractère personnel doivent être:

1° traitées de manière licite et loyale;

2° collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d’une manière incompatible avec ces finalités;

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées;

4° exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder;

5° worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt;

6° met gebruikmaking van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Art. 29

§ 1. Verdere verwerking door dezelfde of een andere verwerkingsverantwoordelijke voor een doeleinde vermeld in artikel 27, ander dan dat waarvoor de persoonsgegevens werden verzameld, is toegelaten voor zover:

1° de verwerkingsverantwoordelijke overeenkomstig de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst gemachtigd is deze persoonsgegevens voor een dergelijk doeleinde te verwerken; en

2° de verwerking noodzakelijk is en in verhouding staat overeenkomstig de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst.

§ 2. De persoonsgegevens kunnen niet verder verwerkt worden door dezelfde of een andere verwerkingsverantwoordelijke voor een ander doeleinde dan dat waarvoor de persoonsgegevens werden verzameld, indien dat doeleinde niet ondergebracht kan worden onder de doeleinden vermeld in artikel 27, tenzij deze verdere verwerking is toegestaan overeenkomstig de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst.

§ 3. Wanneer de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst specifieke voorwaarden oplegt voor de verwerking, stelt de bevoegde overheid die de gegevens doorzendt, de ontvanger van die persoonsgegevens in kennis van de voorwaarden en de verplichting om die na te leven.

§ 4. De bevoegde overheden die de gegevens doorzenden aan de ontvangers in de andere lidstaten van de Europese Unie, mogen geen bijkomende specifieke voorwaarden doen gelden dan degene die gelden voor de nationale gegevensdoorgifte.

5° conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées;

6° traitées avec des mesures techniques et organisationnelles adéquates de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Art. 29

§ 1er. Le traitement ultérieur, par le même ou par un autre responsable du traitement, pour l'une des finalités énoncées à l'article 27, autre que celles pour lesquelles les données ont été collectées, est autorisé aux conditions suivantes:

1° le responsable du traitement est autorisé à traiter ces données à caractère personnel pour une telle finalité conformément à la loi, au décret ou à l'ordonnance, au droit de l'Union européene et à l'accord international; et

2° le traitement est nécessaire et proportionné conformément, à la loi, au décret ou à l'ordonnance au droit de l'Union européene et à l'accord international.

§ 2. Les données à caractère personnel ne peuvent pas être traitées par le même ou un autre responsable du traitement à d'autres fins que celles pour lesquelles les données à caractère personnel ont été collectées, et non comprises dans les finalités énoncées à l'article 27, à moins que cette finalité ne soit permise conformément à la loi, le décret, l'ordonnance, le droit de l'Union européenne et à l'accord international.

§ 3. Lorsque la loi, le décret, l'ordonnance, le droit de l'Union européene ou l'accord international, soumet le traitement à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter.

§ 4. Les autorités compétentes qui transmettent les données aux destinataires dans les autres États membres de l'Union européenne ne peuvent faire appliquer des conditions spécifiques supplémentaires de celles applicables aux transferts nationaux.

§ 5. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van dit artikel en kan de naleving ervan aantonen.

Art. 30

Behoudens de gevallen waarin de maximale bewaartermijn van de gegevens wordt bepaald in de Europese regelgeving of de internationale overeenkomst die de basis vormt voor de betrokken bewaring, bepaalt de wet, het decreet of de ordonnantie de maximale bewaartermijn. Na afloop van die termijn worden de gegevens gewist.

In afwijking van het eerste lid, kan de wet, het decreet of de ordonnantie voorzien dat na afloop van een eerste bewaartermijn een analyse moet worden uitgevoerd op basis van verschillende noodzakelijkheids- en proportionaliteitscriteria om te bepalen of het nodig is dat de gegevens bewaard blijven, en in voorkomend geval, de nieuwe bewaartermijn.

In dat geval voorziet de wet, het decreet of de ordonnantie een maximale bewaartermijn.

Art. 31

De verwerkingsverantwoordelijke maakt in voorkomend geval en voor zover mogelijk een duidelijk onderscheid tussen persoonsgegevens betreffende verschillende categorieën van betrokkenen, zoals:

1° personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;

2° personen die voor een strafbaar feit zijn veroordeeld;

3° slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit;

4° andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld in 1° en 2°.

§ 5. Le responsable du traitement est responsable du respect du présent article et est en mesure de le démontrer.

Art. 30

Sauf dans les cas où la durée maximale de conservation des données est déterminée dans le droit de l'Union européenne ou l'accord international qui est à la base de la conservation concernée, la loi, le décret, ou l'ordonnance détermine la durée maximale de conservation. A l'échéance de cette durée, les données sont effacées.

Par dérogation à l'alinéa premier, la loi, le décret ou l'ordonnance peut prévoir qu'à l'échéance d'un premier délai de conservation, une analyse soit effectuée sur base de différents critères de nécessité et de proportionnalité afin de déterminer si la conservation des données doit être maintenue et, le cas échéant, le nouveau délai de conservation.

Dans ce cas, la loi, le décret ou l'ordonnance prévoit un délai maximum de conservation.

Art. 31

Le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que:

1° les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale;

2° les personnes reconnues coupables d'une infraction pénale;

3° les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale;

4° les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux points 1° et 2°.

Art. 32

§ 1. Persoonsgegevens die op feiten zijn gebaseerd, worden voor zover mogelijk onderscheiden van persoonsgegevens die op een persoonlijk oordeel zijn gebaseerd.

§ 2. De bevoegde overheden nemen alle redelijke maatregelen om ervoor te zorgen dat persoonsgegevens die onjuist, onvolledig of niet meer actueel zijn, niet worden doorgezonden of beschikbaar worden gesteld. Daartoe controleert iedere bevoegde overheid, voor zover mogelijk, de kwaliteit van de persoonsgegevens voordat de gegevens worden doorgezonden of beschikbaar worden gesteld.

Voor zover mogelijk wordt bij de doorzending van persoonsgegevens te allen tijde de noodzakelijke aanvullende informatie worden toegevoegd aan de hand waarvan de ontvangende bevoegde overheid de mate van juistheid, volledigheid en betrouwbaarheid van persoonsgegevens kan beoordelen, alsmede de mate waarin ze actueel zijn.

§ 3. Indien blijkt dat onjuiste persoonsgegevens zijn doorgezonden, of dat de persoonsgegevens op onrechtmatige wijze zijn doorgezonden, wordt de ontvanger daarvan onverwijld in kennis gesteld. In dat geval worden de persoonsgegevens gerectificeerd of gewist, of wordt de verwerking beperkt overeenkomstig artikel 39.

Art. 33

§ 1. De verwerking is rechtmatig indien:

1° ze noodzakelijk is voor de uitvoering van een opdracht uitgevoerd door een overheid bevoegd voor de in artikel 27, bedoelde doeleinden, en

2° ze gebaseerd is op een wettelijke of reglementaire verplichting.

§ 2. De wettelijke of reglementaire verplichting regelt ten minste de categorieën van persoonsgegevens die verwerkt moeten worden en de doeleinden van de verwerking.

Art. 34

§ 1. Verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, en

Art. 32

§ 1er. Les données à caractère personnel fondées sur des faits sont dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles.

§ 2. Les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour ne soient pas transmises ou mises à disposition. À cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition.

Dans la mesure du possible, lors de toute transmission de données à caractère personnel, sont ajoutées des informations nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, et de la fiabilité des données à caractère personnel, et de leur niveau de mise à jour.

§ 3. S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 39.

Art. 33

§ 1er. Le traitement est licite si:

1° il est nécessaire à l'exécution d'une mission effectuée par l'autorité compétente pour les finalités énoncées à l'article 27, et

2° s'il est fondé sur une obligation légale ou réglementaire.

§ 2. L'obligation légale ou réglementaire régit au moins, les catégories de données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement.

Art. 34

§ 1er. Le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des

verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid of gegevens over seksueel gedrag of seksuele gerichtheid van een natuurlijke persoon zijn slechts toegelaten wanneer de verwerking strikt noodzakelijk is en geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene, en enkel in een van de volgende gevallen:

1° wanneer de verwerking door de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst is toegestaan;

2° wanneer de verwerking noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een andere fysieke persoon;

3° wanneer de verwerking betrekking heeft op gegevens die kennelijk openbaar zijn gemaakt door de betrokkene.

§ 2. De passende waarborgen zoals bedoeld in de eerste paragraaf moeten ten minste voorzien dat de bevoegde overheid of de verwerkingsverantwoordelijke een lijst van de categorieën van personen die de persoonsgegevens kunnen raadplegen opstelt, met een beschrijving van hun hoedanigheid ten opzichte van de verwerking van de beoogde gegevens. Deze lijst wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit.

De bevoegde overheid waakt erover dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.

Art. 35

§ 1. Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten, met inbegrip van profilering, die voor de betrokkene nadelige rechtsgevolgen hebben of hem in aanmerkelijke mate treffen, zijn toegestaan als de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkene, met inbegrip van ten minste het recht op menselijke interventie van de verwerkingsverantwoordelijke.

§ 2. Profilering die leidt tot discriminatie van natuurlijke personen op grond van de in artikel 34 bedoelde bijzondere categorieën van persoonsgegevens, is verboden.

données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, n'est autorisé qu'en cas de stricte nécessité et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement dans l'un des cas suivants:

1° lorsque le traitement est autorisé par la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international;

2° lorsque le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne physique;

3° lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

§ 2. Les garanties nécessaires visées au paragraphe premier doivent au moins prévoir que l'autorité compétente ou le responsable de traitement établisse une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l'autorité de contrôle compétente.

L'autorité compétente veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Art. 35

§ 1er. Toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est autorisée si la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement.

§ 2. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 34 est interdit.

HOOFDSTUK III

Rechten van de betrokkene

Art. 36

§ 1. De verwerkingsverantwoordelijke neemt passende maatregelen om de in artikel 37 bedoelde informatie te verstrekken en mededelingen te doen bedoeld in de artikelen 35, 38 tot 41 en artikel 62 in een beknopte, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. De informatie wordt op elke passende manier, ook elektronisch, verstrekt. Over het algemeen, verstrekt de verwerkingsverantwoordelijke de informatie in dezelfde vorm als de aanvraag.

§ 2. De verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene waarop de artikelen 35 en 38 tot 41 betrekking hebben.

§ 3. De verwerkingsverantwoordelijke of de toezichthoudende autoriteit, in het geval bedoeld in artikel 41, informeert de betrokkene schriftelijk, zonder onnodige vertraging met betrekking tot het gevolg dat werd gegeven aan zijn verzoek.

§ 4. Eenieder heeft het recht om kosteloos de informatie bedoeld in artikel 37, te verkrijgen en de maatregelen bedoeld in de artikelen 35, 38 tot 41 en 62, te laten nemen. Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de verwerkingsverantwoordelijke ofwel:

1° een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het nemen van de gevraagde maatregelen gepaard gaan; ofwel

2° weigeren gevolg te geven aan het verzoek.

Het is aan de verwerkingsverantwoordelijke om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

§ 5. Wanneer de verwerkingsverantwoordelijke redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het in artikel 38 of 39 bedoelde verzoek indient, kan hij om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

CHAPITRE III

Droits de la personne concernée

Art. 36

§ 1er. Le responsable du traitement prend des mesures appropriées pour fournir toute information visée à l'article 37 ainsi que pour procéder à toute communication au titre des articles 35, 38 à 41 et de l'article 62 d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par tout moyen approprié, y compris par voie électronique. De manière générale, le responsable du traitement fournit les informations sous la même forme que la demande.

§ 2. Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée par les articles 35 et 38 à 41.

§ 3. Le responsable du traitement, ou l'autorité de contrôle dans le cas visé à l'article 41, informe par écrit, dans les meilleurs délais, la personne concernée des suites données à sa demande.

§ 4. Toute personne a le droit d'obtenir sans frais les informations visées à l'article 37 ainsi que toute mesure au titre des articles 35, 38 à 41 et 62. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut:

1° exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées; ou

2° refuser de donner suite à la demande.

Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

§ 5. Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée à l'article 38 ou 39, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

Art. 37

§ 1. Teneinde de betrokkene de mogelijkheid te bieden zijn recht op informatie uit te oefenen, stelt de verwerkingsverantwoordelijke de betrokkene de volgende informatie ter beschikking:

1° de identiteit en de contactgegevens van de verwerkingsverantwoordelijke;

2° in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;

3° de doeleinden van de verwerking;

4° het bestaan van het recht om klacht in te dienen bij de toezichthoudende autoriteit, en de contactgegevens van voornoemde autoriteit;

5° het bestaan van het recht de verwerkingsverantwoordelijke te verzoeken om toegang tot en rectificatie of wissing van hem betreffende persoonsgegevens, en beperking van de verwerking van hem betreffende persoonsgegevens;

6° de rechtsgrond van de verwerking;

7° de termijn gedurende welke de persoonsgegevens zullen worden bewaard, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

8° in voorkomend geval, de categorieën van ontvangers van de persoonsgegevens;

9° indien noodzakelijk, bijkomende informatie, in het bijzonder wanneer de persoonsgegevens zonder medeweten van de betrokkene worden verzameld.

§ 2. De in de eerste paragraaf bedoelde informatie kan bij wet worden uitgesteld of beperkt dan wel achterwege worden gelaten, voor zover een dergelijke maatregel in een democratische samenleving, met naar behoren inachtneming van de fundamentele rechten en de legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

1° belemmering van strafrechtelijke of andere gereglementeerde onderzoeken, opsporingen of procedures te voorkomen;

2° nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

3° de openbare veiligheid te beschermen;

Art. 37

§ 1er. Afin de permettre à la personne concernée d'exercer son droit à l'information, le responsable du traitement met à la disposition de la personne concernée les informations suivantes:

1° l'identité et les coordonnées du responsable du traitement;

2° le cas échéant, les coordonnées du délégué à la protection des données;

3° les finalités du traitement;

4° le droit d'introduire une plainte auprès de l'autorité de contrôle et les coordonnées de ladite autorité;

5° l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel le concernant;

6° la base juridique du traitement;

7° la durée de conservation des données à caractère personnel ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée;

8° le cas échéant, les catégories de destinataires des données à caractère personnel;

9° si besoin est, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.

§ 2. L'information visée au paragraphe premier, peut être retardée, limitée ou exclue par la loi dès lors qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour:

1° éviter de gêner des enquêtes, des recherches, des procédures pénales ou autres procédures réglementées;

2° éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

3° protéger la sécurité publique;

4° de nationale veiligheid te beschermen;

5° de rechten en vrijheden van anderen te beschermen.

§ 3. Behoudens de gevallen waarin de Europese regelgeving of internationale overeenkomst dit bepaalt, kan de wet, het decreet of de ordonnantie bepalen welke verwerkingscategorieën geheel of gedeeltelijk onder één van de punten opgesomd in paragraaf 2 kunnen vallen.

§ 4. De rechten geviseerd in dit hoofdstuk, voor wat betreft de gegevensverwerkingen van de hoven en rechtbanken van het gemeen recht en het openbaar ministerie, worden uitsluitend uitgeoefend binnen de grenzen en conform de regels en modaliteiten van het Gerechtelijk Wetboek, het wetboek van Strafvordering, de bijzondere wetten die betrekking hebben op de strafrechtspleging en hun uitvoeringsbesluiten.

Art. 38

§ 1. Teneinde de betrokkene de mogelijkheid te bieden zijn recht op verzoek tot toegang tot zijn persoonsgegevens uit te oefenen, stelt de verwerkingsverantwoordelijke de betrokkene de volgende informatie ter beschikking:

1° de bevestiging dat de hem betreffende persoonsgegevens al dan niet worden verwerkt en toegang tot die persoonsgegevens;

2° de doeleinden en de rechtsgrond van de verwerking;

3° de betreffende categorieën van persoonsgegevens;

4° de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn bekendgemaakt;

5° de bewaartermijn, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

6° dat hij het recht heeft van de verwerkingsverantwoordelijke de rectificatie of wissing van hem betreffende persoonsgegevens of beperking van verwerking van hem betreffende persoonsgegevens te vragen;

7° dat hij het recht heeft klacht in te dienen bij de toezichthoudende autoriteit, en de contactgegevens van deze autoriteit;

4° protéger la sécurité nationale;

5° protéger les droits et libertés d'autrui.

§ 3. Sauf dans les cas où le droit de l'Union européenne ou l'accord international le détermine, la loi, le décret ou l'ordonnance peut déterminer des catégories de traitements susceptibles de relever, dans leur intégralité ou en partie, d'un quelconque des points énumérés au paragraphe 2.

§ 4. Les droits visés dans ce chapitre, pour ce qui concernent les traitements de données des cours et tribunaux du droit commun et le ministère public, sont exercés exclusivement dans les limites et conformément aux règles et modalités précisées dans le Code judiciaire, le Code d'instruction criminelle, les lois particulières relatives à la procédure pénale et leurs arrêtés d'exécution.

Art. 38

§ 1er. Afin de permettre à la personne concernée de demander l'accès à ses données personnelles, le responsable du traitement met à la disposition de la personne concernée, les informations suivantes:

1° la confirmation que des données la concernant sont ou ne sont pas traitées ainsi que l'accès à ces données;

2° les finalités du traitement ainsi que sa base juridique;

3° les catégories de données à caractère personnel concernées;

4° les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées;

5° la durée de conservation ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée;

6° l'existence du droit de demander au responsable du traitement, la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement des données à caractère personnel relatives à la personne concernée;

7° le droit d'introduire une plainte auprès de l'autorité de contrôle et les coordonnées de cette autorité;

8° de persoonsgegevens die worden verwerkt, en alle beschikbare informatie over de oorsprong van die gegevens.

§ 2. De wet, het decreet of de ordonnantie kan het recht op toegang van de betrokkene geheel of gedeeltelijk beperken, voor zover en zolang die volledige of gedeeltelijke beperking in een democratische samenleving, met inachtneming van de grondrechten en legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

1° belemmering van strafrechtelijke of andere gereglementeerde onderzoeken, opsporingen of procedures te voorkomen;

2° nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

3° de openbare veiligheid te beschermen;

4° de nationale veiligheid te beschermen;

5° de rechten en vrijheden van anderen te beschermen.

§ 3. In de in paragraaf 2 bedoelde gevallen stelt de verwerkingsverantwoordelijke de betrokkene zonder onnodige vertraging schriftelijk in kennis van een eventuele weigering of beperking van de toegang en van de redenen voor die weigering of beperking. Die informatie kan achterwege worden gelaten wanneer de verstrekking daarvan een van de doeleinden van paragraaf 2 zou ondermijnen. De verwerkingsverantwoordelijke licht de betrokkene in over de mogelijkheid om klacht in te dienen bij de bevoegde toezichthoudende autoriteit of om een beroep in te stellen bij de rechter.

§ 4. De verwerkingsverantwoordelijke documenteert de feitelijke of juridische redenen die aan het besluit ten grondslag liggen. Die informatie wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Art. 39

§ 1. De betrokkene heeft het recht om zonder onnodige vertraging van de verwerkingsverantwoordelijke de rectificatie en eventueel de aanvulling te verkrijgen van hem betreffende onjuiste persoonsgegevens.

§ 2. De verwerkingsverantwoordelijke wist de persoonsgegevens zonder onnodige vertraging wanneer de verwerking indruist tegen de bepalingen goedgekeurd

8° la communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source.

§ 2. La loi, le décret ou l'ordonnance peut limiter entièrement ou partiellement, le droit d'accès de la personne concernée, dès lors et aussi longtemps qu'une telle limitation partielle ou totale constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour:

1° éviter de gêner des enquêtes, des recherches, des procédures pénales ou autres procédures réglementées;

2° éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

3° protéger la sécurité publique;

4° protéger la sécurité nationale;

5° protéger les droits et libertés d'autrui.

§ 3. Dans les cas visés au paragraphe 2 le responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au paragraphe 2. Le responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel.

§ 4. Le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition de l'autorité de contrôle compétente.

Art. 39

§ 1er. La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification, et éventuellement la complétude, des données à caractère personnel la concernant qui sont inexactes.

§ 2. Le responsable du traitement efface dans les meilleurs délais les données à caractère personnel lorsque le traitement constitue une violation des

krachtens artikelen 28, 29, 33 of 34 of wanneer de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting waaraan de verwerkingsverantwoordelijke gehouden is.

§ 3. In plaats van tot wissing over te gaan, mag de verwerkingsverantwoordelijke de verwerking beperken wanneer:

1° de juistheid van de persoonsgegevens door de betrokkene wordt betwist en niet kan worden geverifieerd of de gegevens al dan niet juist zijn; of

2° de persoonsgegevens als bewijsmateriaal moeten worden bewaard.

Wanneer de verwerking op grond van punt 1° van het eerste lid wordt beperkt, informeert de verwerkingsverantwoordelijke de betrokkene alvorens de verwerkingsbeperking op te heffen.

§ 4. De verwerkingsverantwoordelijke stelt de betrokkene schriftelijk in kennis van een eventuele weigering tot rectificatie of wissing van persoonsgegevens of verwerkingsbeperking, en van de redenen voor die weigering. De hierboven bedoelde informatie kan bij wet, decreet of ordonnantie, worden beperkt, voor zover een dergelijke verwerkingsbeperking in een democratische samenleving, met inachtneming van de grondrechten en legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

1° belemmering van strafrechtelijke of andere gereglementeerde onderzoeken, opsporingen of procedures te voorkomen;

2° nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

3° de openbare veiligheid te beschermen;

4° de nationale veiligheid te beschermen;

5° de rechten en vrijheden van anderen te beschermen.

De verwerkingsverantwoordelijke licht de betrokkene in over de mogelijkheid om klacht in te dienen bij de bevoegde toezichthoudende autoriteit of om beroep in rechte in te stellen.

§ 5. De verwerkingsverantwoordelijke deelt de rectificatie van de onjuiste persoonsgegevens mee aan de overheid van wie de onjuiste persoonsgegevens afkomstig zijn.

dispositions adoptées en vertu des articles 28, 29, 33 ou 34 ou lorsque les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

§ 3. Au lieu de procéder à l'effacement, le responsable du traitement peut limiter le traitement lorsque:

1° l'exactitude des données à caractère personnel est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non; ou

2° les données à caractère personnel doivent être conservées à des fins probatoires.

Lorsque le traitement est limité conformément au premier alinéa, point 1°, le responsable du traitement informe la personne concernée avant de lever la limitation du traitement.

§ 4. Le responsable du traitement informe la personne concernée par écrit de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus. L'information visée ci-dessus, peut être limitée par la loi, le décret, ou l'ordonnance, dès lors qu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour:

1° éviter de gêner des enquêtes, des recherches, des procédures pénales ou autres procédures réglementées;

2° éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

3° protéger la sécurité publique;

4° protéger la sécurité nationale;

5° protéger les droits et libertés d'autrui.

Le responsable du traitement informe la personne concernée des possibilités d'introduire une plainte auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel.

§ 5. Le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité d'oùont proviennent les données à caractère personnel inexactes.

§ 6. In geval van rectificatie, wissing of verwerkingsbeperking bedoeld in paragrafen 1, 2 en 3, stelt de verwerkingsverantwoordelijke de ontvangers daarvan in kennis, en rectificeren of wissen de ontvangers de persoonsgegevens of beperken ze de onder hun bevoegdheid vallende verwerking van persoonsgegevens.

Art. 40

De verwerkingsverantwoordelijke die een verzoek ontvangt om een recht uit te oefenen bedoeld in de artikelen 36 tot 39 van deze titel, bezorgt de verzoeker onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek een gedagtekende ontvangstbevestiging.

Art. 41

§ 1. In de in artikel 37, § 2, artikel 38, § 2, artikel 39, § 4, en artikel 62, § 1, bedoelde gevallen, kan de wet, het decreet of de ordonnantie, voorzien dat de rechten van de betrokkene via de bevoegde toezichthoudende autoriteit worden uitgeoefend, met respect voor de principes van noodzakelijkheid en proportionaliteit in een democratische samenleving.

§ 2. Onverminderd artikel 44, in het geval bedoeld in de eerste paragraaf stelt de verwerkingsverantwoordelijke de betrokkene ervan in kennis dat hij zijn rechten via de bevoegde toezichthoudende autoriteit uitoefent.

§ 3. In het geval bedoeld in de eerste paragraaf, dient de betrokkene het verzoek om zijn rechten uit te oefenen in bij de bevoegde toezichthoudende autoriteit.

Art. 42

Het verzoek tot uitoefening van de rechten voor wat betreft de politiedienst in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus of de algemene inspectie van de federale politie en de lokale politie,, wordt aan de toezichthoudende autoriteit bedoeld in artikel 71 gericht.

In de in artikel 37, § 2, artikel 38, § 2, artikel 39, § 4, en artikel 62, § 1, bedoelde gevallen deelt de toezichthoudende autoriteit bedoeld in artikel 71 uitsluitend mee aan de betrokkene dat de nodige verificaties werden verricht.

§ 6. En cas de rectification, effacement ou de limitation de traitement tel que visés aux paragraphes 1, 2 et 3, le responsable du traitement adresse une notification aux destinataires afin que ceux-ci rectifient ou effacent les données à caractère personnel ou limitent le traitement des données à caractère personnel sous leur responsabilité.

Art. 40

Le responsable du traitement qui reçoit une demande d'exercer un droit visé aux articles 36 à 39 du présent titre délivre dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande un accusé de réception daté à l'auteur de la demande.

Art. 41

§ 1er. Dans les cas visés à l'article 37, § 2, à l'article 38, § 2, à l'article 39, § 4, et à l'article 62, § 1er, la loi, le décret ou l'ordonnance, peut prévoir que les droits de la personne concernée sont exercés par l'intermédiaire de l'autorité de contrôle compétente, dans le respect des principes de nécessité et de proportionnalité dans une société démocratique.

§ 2. Sans préjudice de l'article 44, dans le cas visé au paragraphe premier, le responsable du traitement informe la personne concernée qu'elle exerce ses droits par l'intermédiaire de l'autorité de contrôle compétente.

§ 3. Dans le cas visé au paragraphe premier, la demande d'exercer ses droits est introduite par la personne concernée auprès de l'autorité de contrôle compétente.

Art. 42

La demande d'exercer les droits visés au présent chapitre à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant la police intégrée, structurée à deux niveaux ou de l'Inspection générale de la police fédérale et de la police locale, est adressée à l'autorité de contrôle visée à l'article 71.

Dans les cas visés à l'article 37, § 2, à l'article 38, § 2, à l'article 39, § 4, et à l'article 62, § 1er, l'autorité de contrôle visée à l'article 71 communique uniquement à la personne concernée qu'il a été procédé aux vérifications nécessaires.

Niettegenstaande lid 2 kan de toezichthoudende autoriteit bedoeld in artikel 71 aan de betrokkene bepaalde contextuele informatie verstrekken.

De Koning, na advies van de toezichthoudende autoriteit bedoeld in artikel 71, bepaalt de categorieën van contextuele informatie die door deze toezichthoudende autoriteit aan de betrokkene kunnen worden medegedeeld.

Art. 43

Voor wat betreft de gegevensverwerkingen van de douanediensten bedoeld in artikel 26, 7°, e), en de Cel voor financiële informatieverwerking bedoeld in artikel 26, 7°, g), worden de rechten van de betrokkene zoals bedoeld in dit hoofdstuk uitgeoefend door de bevoegde toezichthoudende autoriteit.

Deze deelt uitsluitend aan de betrokkene mede dat de nodige verificaties werden verricht.

In afwijking van lid 2 kan de bevoegde toezichthoudend autoriteit aan de betrokkene bepaalde contextuele informatie verstrekken.

De Koning bepaalt na advies van de bevoegde toezichthoudende autoriteit de categorieën van contextuele informatie die via de bevoegde toezichthoudende autoriteit aan de betrokkene kunnen worden mede gedeeld.

Art. 44

Wanneer de persoonsgegevens in een rechterlijke beslissing of een gerechtelijk dossier zijn opgenomen of in het kader van strafrechtelijke onderzoeken en procedures worden verwerkt, worden de in de artikelen 37, 38, § 1, 39 en 41, § 2, bedoelde rechten uitgeoefend overeenkomstig het Gerechtelijk wetboek, het wetboek van Strafvordering, de bijzondere wetten die betrekking hebben op de strafrechtspleging en zijn uitvoeringsbesluiten.

Art. 45

§ 1. De artikelen 36 tot 44 en 62 zijn niet van toepassing op de verwerkingen van persoonsgegevens die rechtstreeks of onrechtstreeks afkomstig zijn van de overheden bedoeld in titel 3 van deze wet, met betrekking tot de verwerkingsverantwoordelijken en de bevoegde overheden bedoeld in deze titel naar wie deze gegevens werden overgebracht.

Nonobstant l'alinéa 2, l'autorité de contrôle visée à l'article 71 peut communiquer à la personne concernée certaines informations contextuelles.

Le Roi détermine, après avis de l'autorité de contrôle visée à l'article 71, les catégories d'informations contextuelles qui peuvent être communiquées à la personne concernée, par cette autorité de contrôle.

Art. 43

Pour ce qui concerne les traitements des services de douanes visés à l'article 26, 7°, e), et la Cellule de traitement des informations financières visée à l'article 26, 7°, g), les droits des personnes concernées visés au présent chapitre sont exercés via l'autorité de contrôle compétente.

Celle-ci communique uniquement à la personne concernée qu'il a été procédé aux vérifications nécessaires.

Par dérogation à l'alinéa 2, l'autorité de contrôle compétente peut communiquer à la personne concernée certaines informations contextuelles.

Le Roi détermine après avis de l'autorité de contrôle compétente les catégories d'informations contextuelles qui peuvent être communiquées à la personne concernée, via l'autorité de contrôle compétente.

Art. 44

Lorsque les données à caractère personnel figurent dans une décision judiciaire ou un dossier judiciaire, ou faisant l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale, les droits visés aux articles 37, 38, § 1er, 39 et 41, § 2, sont exercés conformément au Code judiciaire, au Code d'instruction criminelle, aux lois particulières relatives à la procédure pénale ainsi qu'aux arrêtés d'exécution.

Art. 45

§ 1er. Les articles 36 à 44 et 62 ne s'appliquent pas aux traitements de données à caractère personnel émanant directement ou indirectement des autorités visées au titre 3 de la présente loi à l'égard des responsables du traitement et des autorités compétentes visées dans le présent titre auxquelles ces données ont été transmises.

§ 2. De verwerkingsverantwoordelijke of de bevoegde overheid bedoeld in deze titel die in het bezit is van zulke gegevens deelt deze niet mee aan de betrokkene tenzij:

1° de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2° de betrokken overheid bedoeld in titel 3 hem dit toestaat.

§ 3. De verwerkingsverantwoordelijke of de bevoegde overheid deelt niet mee dat hij of zij in het bezit is van gegevens die van overheden bedoeld in titel 3 afkomstig zijn.

§ 4. De verwerkingsverantwoordelijke bedoeld in deze titel die gegevens verwerkt die rechtstreeks of onrechtstreeks afkomstig zijn van de overheden bedoeld in titel 3 beantwoordt minstens aan de volgende voorwaarden:

1° hij neemt nemen de gepaste technische of organisatorische maatregelen om ervoor te zorgen dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt zijn tot hetgeen de personen nodig hebben om hun functies uit te oefenen of tot hetgeen nodig is voor de behoeften van de autoriteit bedoeld in titel 3;

2° hij neemt de gepaste technische of organisatorische maatregelen om de persoonsgegevens te beschermen tegen toevallige of niet-toegestane vernietiging, tegen toevallig verlies en tegen wijziging of elke andere niet-toegestane verwerking van die gegevens.

De leden van het personeel van de verwerkingsverantwoordelijke die de gegevens bedoeld in het eerste lid verwerken, zijn bovendien gebonden door de discretieplicht.

§ 5. De beperkingen bedoeld in paragraaf 1 hebben eveneens betrekking op de logbestanden van de verwerkingen van een overheid bedoeld in titel 3 van deze wet in de gegevensbanken van de verwerkingsverantwoordelijken en van de bevoegde overheden bedoeld in deze titel waartoe de overheid bedoeld in titel 3 rechtstreeks toegang heeft.

§ 6. Wanneer een verzoek of een klacht aanhangig wordt gemaakt bij de bevoegde toezichthoudende autoriteit waarbij de verwerkingsverantwoordelijke zich beroept op de toepassing van dit artikel, wendt deze eerste zich tot het Vast Comité I opdat het de nodige verificaties bij de overheid bedoeld in titel 3 verricht.

§ 2. Le responsable du traitement ou l'autorité compétente visé dans le présent titre qui est en possession de telles données ne les communique pas à la personne concernée à moins que:

1° la loi l'y oblige dans le cadre d'une procédure contentieuse; ou que

2° l'autorité visée au titre 3 concernée l'y autorise.

§ 3. Le responsable du traitement ou l'autorité compétente ne fait aucune mention qu'il ou elle est en possession de données émanant des autorités visées au titre 3.

§ 4. Le responsable de traitement visé dans le présent titre qui traite les données émanant directement ou indirectement autorités visées au titre 3 répond au minimum aux conditions suivantes:

1° il adopte des mesures techniques ou organisationnelles appropriées pour assurer que l'accès aux données et les possibilités de traitement soient limités à ce dont les personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités de l'autorité visée au titre 3;

2° il adopte des mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données.

Les membres du personnel du responsable de traitement qui traitent les données visées à l'alinéa 1er sont en outre tenus au devoir de discrétion.

§ 5. Les limitations visées au paragraphe premier porte également sur la journalisation des traitements d'une autorité visée dans le titre 3 de la présente loi dans les banques de données des responsables du traitement et des autorités compétentes visés par le présent titre, auxquelles l'autorité visée au titre 3 a directement accès.

§ 6. Lorsque l'autorité de contrôle compétente est saisie d'une requête ou d'une plainte où le responsable du traitement fait état de l'application du présent article, celle-ci s'adresse au Comité permanent R pour qu'il fasse les vérifications nécessaires auprès de l'autorité visée au titre 3.

Na ontvangst van het antwoord van het Vast Comité I brengt de bevoegde toezichthoudende autoriteit de betrokkene enkel op de hoogte van de resultaten van de verificatie, die betrekking hebben op persoonsgegevens die niet van een overheid bedoeld in titel 3 afkomstig zijn, die ze wettelijk gehouden is mee te delen.

Indien het verzoek of de klacht enkel betrekking heeft op persoonsgegevens afkomstig van een overheid bedoeld in titel 3, antwoordt de bevoegde toezichthoudende autoriteit, na ontvangst van het antwoord van het Vast Comité I, dat de nodige verificaties werden verricht.

Art. 46

Een verwerkingsverantwoordelijke of een bevoegde overheid bedoeld in deze titel die persoonsgegevens meedeelt aan een overheid bedoeld in ondertitels 2 en 4 van titel 3 van deze wet is niet onderworpen aan de artikelen 37, § 1,8° en 38, § 1,4° en mag de betrokkene niet van deze overdracht op de hoogte brengen.

Art. 47

Wanneer een overheid bedoeld in ondertitels 1 en 6 van titel 3 van deze wet over een rechtstreekse toegang of over een rechtstreekse bevraging van een gegevensbank van de publieke sector beschikt, wordt de verwerking van de persoonsgegevens beschermd door technische, organisatorische en persoonlijke beveiligingsmaatregelen zodat alleen de volgende actoren toegang kunnen hebben tot de inhoud van deze verwerkingen in het kader van de doeleinden bedoeld in artikel 56, § 2:

1° de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke van de gegevensbank of de persoon die hij daartoe machtigt;

2° de functionaris voor gegevensbescherming van de overheid bedoeld in ondertitels 1 en 6 van titel 3;

3° de verwerkingsverantwoordelijke van de gegevensbank of de persoon die hij daartoe machtigt;

4° de verwerkingsverantwoordelijke van de overheid bedoeld in ondertitels 1 en 6 van titel 3;

5° elke andere persoon bepaald in een protocol tussen de verwerkingsverantwoordelijken, voor wie de toegang noodzakelijk is om de wettelijke toezichtsopdrachten te vervullen.

Après réception de la réponse du Comité permanent R, l'autorité de contrôle compétente n'informe la personne concernée que des résultats de la vérification portant sur les données à caractère personnel n'émanant pas des autorités visées au titre 3 qu'elle est légalement tenue de communiquer.

Si la requête ou la plainte ne porte que sur des données à caractère personnel émanant d'une autorité visée au titre 3, l'autorité de contrôle compétente répond, après réception de la réponse du Comité permanent R, que les vérifications nécessaires ont été effectuées.

Art. 46

Un responsable du traitement ou une autorité compétente visés dans le présent titre qui communique des données à caractère personnel à une autorité visée aux sous-titres 2 et 4 du titre 3 de la présente loi, n'est pas soumis aux articles 37, § 1er, 8°) et 38, § 1er, 4°) et ne peut informer la personne concernée de cette transmission.

Art. 47

Lorsqu'une autorité visée aux sous-titres 1 et 6 du titre 3 de la présente loi dispose d'un accès direct ou d'une interrogation directe à une banque de données du secteur public, le traitement de données à caractère personnel est protégé par des mesures de sécurité techniques, organisationnelles et personnelles de sorte que seuls les acteurs suivants puissent accéder au contenu de ces traitements dans le cadre des finalités visées à l'article 56, § 2:

1° le délégué à la protection des données du responsable du traitement de la banque de donnée ou la personne qu'il délègue à cet effet;

2° le délégué à la protection des données de l'autorité visée aux sous-titres 1 et 6 du titre 3;

3° le responsable du traitement de la banque de données ou la personne qu'il délègue à cet effet;

4° le responsable du traitement de l'autorité visée aux sous-titres 1 et 6 du titre 3;

5° toute autre personne précisée dans un protocole entre les responsables du traitement, dont l'accès est nécessaire pour remplir les missions légales de contrôle.

Deze beveiligingsmaatregelen zijn bedoeld om de wettelijke verplichtingen met betrekking tot de bescherming van bronnen, de bescherming van de identiteit van de agenten of het geheim van de onderzoeken van de overheden bedoeld in ondertitels 1 en 6 van titel 3 te beschermen.

Deze verwerkingen mogen enkel toegankelijk zijn voor andere doeleinden dan diegene die verband houden met het toezicht indien deze doeleinden, uit de door of krachtens een wet vastgelegde doeleinden, zijn vastgelegd in een protocolakkoord tussen de betrokken verwerkingsverantwoordelijken.

Het protocol wijst de perso(o)n(en) aan waarvoor de toegang tot de logbestanden noodzakelijk is om elk van de doeleinden vermeld in voorgaand lid te vervullen.

De logbestanden en de daaraan gekoppelde technische, organisatorische en persoonlijke veiligheidsmaatregelen worden ter beschikking gesteld van het Vast Comité I.

De betrokken overheid bedoeld in ondertitels 1 en 6 van titel 3 kan afwijken van het eerste lid wanneer de toegang tot haar verwerkingen in een gegevensbank en tot de logbestanden hiervan geen afbreuk kan doen aan de belangen bedoeld in het derde lid.

Art. 48

§ 1. Een verwerkingsverantwoordelijke bedoeld in deze titel die persoonsgegevens meedeelt aan een gezamenlijke databank mag de betrokkene niet van deze overdracht op de hoogte brengen.

§ 2. Onder “gezamenlijke databank” wordt “het gemeenschappelijk uitoefenen van de opdrachten uitgevoerd in het kader van titels 2 en 3 door meerdere overheden, gestructureerd met behulp van geautomatiseerde procédés en toegepast op persoonsgegevens” bedoeld.

Art. 49

§ 1. De artikelen 36 tot 44 en 62 zijn niet van toepassing op de verwerkingen van persoonsgegevens door de Passagiersinformatie-eenheid.

§ 2. De verwerkingsverantwoordelijke deelt de gegevens bedoeld in de eerste paragraaf niet mee aan de betrokkene tenzij de wet hem hiertoe verplicht in het kader van een geschillenprocedure.

Ces mesures de sécurité visent à protéger les obligations légales portant sur la protection des sources, la protection de l’identité des agents ou au secret des enquêtes des autorités visées aux sous-titres 1 et 6 du titre 3.

Ces traitements ne peuvent être accessibles pour d’autres finalités que celles liées au contrôle que si ces finalités sont consignées dans un protocole d’accord par les responsables du traitement concernés parmi des finalités déterminées par ou en vertu d’une loi.

Le protocole désigne la ou les personne(s) dont l’accès aux journaux est nécessaire pour remplir chaque finalité autorisée à l’alinéa précédent.

Les journaux et les mesures de sécurité techniques, organisationnelles et personnelles y afférentes sont mis à la disposition du Comité permanent R.

L’autorité visée aux sous-titres 1 et 6 du titre 3 concernée peut déroger à l’alinéa premier lorsque l’accès à ses traitements dans une banque de données et à leur journalisation n’est pas susceptible de porter atteinte aux intérêts visés à l’alinéa 3 .

Art. 48

§ 1er. Un responsable du traitement visé dans le présent titre qui communique des données à caractère personnel à une banque de données conjointe ne peut informer la personne concernée de cette transmission.

§ 2. Par “banque de données conjointe”, on entend “l’exercice commun des missions effectuées dans le cadre des titres 2 et 3 par plusieurs autorités, structuré à l’aide de procédés automatisés et appliqués aux données à caractère personnel”.

Art. 49

§ 1er. Les articles 36 à 44 et 62 ne s’appliquent pas aux traitements de données à caractère personnel par l’Unité d’information des passagers.

§ 2. Le responsable du traitement ne communique pas les données visées au paragraphe premier à la personne concernée à moins que la loi l’y oblige dans le cadre d’une procédure contentieuse.

§ 3. De verwerkingsverantwoordelijke doet geen enkele melding aan de betrokkene dat hij in het bezit is van gegevens die betrekking hebben op hem.

§ 4. De beperkingen bedoeld in de eerste paragraaf hebben eveneens betrekking op de logbestanden van de verwerkingen door de Passagiersinformatie-eenheid, in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel.

§ 5. Wanneer een verzoek of een klacht aanhangig wordt gemaakt bij de bevoegde toezichthoudende autoriteit waarbij de verwerkingsverantwoordelijke zich beroept op de toepassing van dit artikel, antwoordt deze alleen dat de nodige verificaties zijn verricht.

HOOFDSTUK IV

Verwerkingsverantwoordelijke en verwerker

Afdeling 1

Organisatorische en technische maatregelen

Art. 50

Rekening houdend met de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten deze maatregelen de uitvoering van een passend gegevensbeschermingsbeleid door de verwerkingsverantwoordelijke.

De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerking in overeenstemming met de wet wordt uitgevoerd.

Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

Art. 51

§ 1. Rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, dienen de technische en organisatorische maatregelen, bedoeld in artikel 50, om de gegevensbeschermingsbeginselen op een doeltreffende manier door te voeren en

§ 3. Le responsable du traitement ne fait aucune mention à la personne concernée qu'il est en possession de données la concernant.

§ 4. Les limitations visées au paragraphe premier portent également sur la journalisation des traitements effectués par l'Unité d'information des passagers dans les banques de données des responsables du traitement visés par le présent titre.

§ 5. Lorsque l'autorité de contrôle compétente est saisie d'une requête ou d'une plainte où le responsable du traitement fait état de l'application du présent article, celle-ci répond uniquement que les vérifications nécessaires ont été effectuées.

CHAPITRE IV

Responsable du traitement et sous-traitant

Section 1re

Mesures organisationnelles et techniques

Art. 50

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées. Lorsque cela est proportionné au regard des activités de traitement, ces mesures comprennent la mise en oeuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

Le responsable du traitement doit être en mesure de démontrer que le traitement est effectué conformément à la loi.

Ces mesures sont réexaminées et actualisées si nécessaire.

Art. 51

§ 1er. Compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, les mesures techniques et organisationnelles visées à l'article 50, sont destinées à mettre en œuvre les principes relatifs à la protection

de nodige waarborgen in de verwerking in te bouwen ter bescherming van de rechten van de betrokkenen, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf.

§ 2. De technische en organisatorische maatregelen bedoeld in artikel 50 waarborgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. In het bijzonder, waarborgen deze maatregelen dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 52

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken.

Een onderlinge regeling stelt op transparante wijze de respectieve verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en om de in de artikelen 37 en 38 bedoelde informatie te verstrekken, tenzij hun respectieve verantwoordelijkheden zijn vastgesteld bij de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst.

In de onderlinge regeling kan één enkel contactpunt voor de betrokkenen worden aangewezen.

Afdeling 3

Verwerker

Art. 53

§ 1. Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verwerkingsverantwoordelijke een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de verwerking.

§ 2. De verwerker neemt een andere verwerker in dienst met voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke.

des données de façon effective et à assortir le traitement des garanties nécessaires afin de protéger les droits de la personne concernée, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même.

§ 2. Les mesures techniques et organisationnelles appropriées visées à l'article 50 garantissent que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans une intervention humaine.

Section 2

Responsables conjoints du traitement

Art. 52

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Un accord définit de manière transparente les obligations respectives des responsables conjoints de traitement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et la communication des informations visées aux articles 37 et 38, sauf si, leurs obligations respectives sont définies par la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international.

Un seul point de contact pour les personnes concernées peut être désigné dans l'accord.

Section 3

Sous-traitant

Art. 53

§ 1er. Lorsque le traitement est confié à un sous-traitant, le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements.

§ 2. Le sous-traitant recrute un autre sous-traitant avec l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement.

In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

§ 3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het type persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.

Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:

1° uitsluitend volgens de instructies van de verwerkingsverantwoordelijke handelt;

2° ervoor zorgt dat personen die gemachtigd zijn de persoonsgegevens te verwerken zich ertoe hebben verplicht geheimhouding in acht te nemen of door een passende wettelijke verplichting van geheimhouding gebonden zijn;

3° de verwerkingsverantwoordelijke met passende middelen bijstaat om de naleving van de bepalingen betreffende de rechten van de betrokkene te verzekeren;

4° na afloop van de gegevensverwerkingsdiensten, alle persoonsgegevens wist of die terugbezorgt aan de verwerkingsverantwoordelijke, en bestaande kopieën verwijdert, tenzij de bewaring van de persoonsgegevens verplicht is bij de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst;

5° aan de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de naleving van dit artikel aan te tonen;

6° aan de in de paragrafen 2 en 3 bedoelde voorwaarden voor indienstneming van een andere verwerker voldoet.

§ 4. De in paragraaf 3 bedoelde overeenkomst of andere rechtshandeling is gesteld in schriftelijke vorm, daaronder begrepen in elektronische vorm.

§ 5. Indien een verwerker in strijd met deze titel de doeleinden en middelen van de verwerking bepaalt, wordt die verwerker met betrekking tot deze verwerking als de verwerkingsverantwoordelijke beschouwd.

Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

§ 3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique qui lie le sous-traitant à l'égard du responsable du traitement, et définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant:

1° n'agit que sur instruction du responsable du traitement;

2° veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;

3° aide le responsable du traitement, par tout moyen approprié, à veiller au respect des dispositions relatives aux droits de la personne concernée;

4° supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation des services de traitement des données, et détruit les copies existantes, à moins que la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international n'exige la conservation des données à caractère personnel;

5° met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect du présent article;

6° respecte les conditions visées aux paragraphes 2 et 3 pour recruter un autre sous-traitant.

§ 4. Le contrat ou l'autre acte juridique visé au paragraphe 3 revêt la forme écrite, y compris la forme électronique.

§ 5. Si, en violation du présent titre, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme le responsable du traitement pour ce qui concerne ce traitement.

Art. 54

De verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt die uitsluitend in opdracht van de verwerkingsverantwoordelijke, of krachtens de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst.

Afdeling 4

Verplichtingen

Art. 55

§ 1. Elke verwerkingsverantwoordelijke en verwerker houdt een register bij van de categorieën van verwerkingsactiviteiten die onder zijn verantwoordelijkheid worden verricht. Dat register bevat de volgende elementen:

1° de naam en de contactgegevens van de verwerkingsverantwoordelijke of de verwerker, en van zijn gedelegeerde of vertegenwoordiger;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming;

3° de verwerkingsdoeleinden;

4° de categorieën van betrokkenen;

5° de categorieën van persoonsgegevens;

6° de categorieën van ontvangers;

7° de doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in voorkomend geval, de documenten getuigen van het bestaan van passende waarborgen;

8° de beoogde termijnen voor het wissen van de verschillende gegevenscategorieën;

9° een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 50 van deze wet;

10° het gebruik van profilering;

11° de rechtsgrondslag;

12° de categorie van externe bronnen;

Art. 54

Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut traiter ces données, que sur instruction du responsable du traitement, ou en vertu de la loi, du décret, de l'ordonnance, du droit de l'Union européenne ou de l'accord international.

Section 4

Obligations

Art. 55

§ 1er. Chaque responsable du traitement et sous-traitant tient un registre des catégories d'activités de traitement effectuées sous sa responsabilité. Ce registre contient les éléments suivants:

1° le nom et les coordonnées du responsable du traitement ou sous-traitant, de son délégué ou représentant;

2° le nom et les coordonnées du délégué à la protection des données;

3° les finalités du traitement;

4° les catégories de personnes concernées;

5° les catégories de données à caractère personnel;

6° les catégories de destinataires;

7° les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, le cas échéant, les documents attestant de l'existence de garanties appropriées;

8° les délais prévus pour l'effacement des différentes catégories de données;

9° une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 50 de la présente loi;

10° le recours au profilage;

11° la base juridique;

12° la catégorie de sources externes;

13° het protocol bedoeld in artikel 20 evenals het advies van de functionaris voor gegevensbescherming en de motivering bedoeld in artikel 22.

§ 2. De functionaris voor gegevensbescherming wordt betrokken bij de uitwerking en het bijhouden van het register.

§ 3. Het register wordt ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Art. 56

§ 1. De logbestanden van tenminste de volgende verwerkingen worden bijgehouden in systemen voor geautomatiseerde verwerking: de verzameling, wijziging, raadpleging, bekendmaking, met inbegrip van de doorgiften, de combinatie en de wissing.

De logbestanden van de raadpleging en de bekendmaking maken het mogelijk om het volgende te achterhalen:

1° de redenen, de datum en het tijdstip van die verwerkingen;

2° de categorieën van personen die persoonsgegevens hebben geraadpleegd, en indien mogelijk, de identiteit van de persoon die persoonsgegevens heeft geraadpleegd;

3° de systemen die deze persoonsgegevens bekendgemaakt hebben;

4° en de categorieën van de ontvangers van die persoonsgegevens ontvangen, en indien mogelijk, de identiteit van de ontvangers van die persoonsgegevens.

De Koning kan, bij een in de Ministerraad overlegd besluit en na advies van de bevoegde toezichthoudende autoriteit, andere soorten van verwerking bepalen waarvoor logbestanden moeten worden opgesteld.

§ 2. De logbestanden worden uitsluitend gebruikt om te controleren of de verwerking rechtmatig is, voor interne controles, ter waarborging van de integriteit en de beveiliging van de persoonsgegevens en voor doeleinden bedoeld in artikel 27.

§ 3. De verwerkingsverantwoordelijke en de verwerker stellen de logbestanden op vraag ter beschikking van de bevoegde toezichthoudende autoriteit.

13° le protocole visé à l'article 20 ainsi que l'avis du délégué à la protection des données et la motivation visés à l'article 22.

§ 2. Le délégué à la protection des données est associé à l'élaboration et au maintien du registre.

§ 3. Le registre est mis à la disposition de l'autorité de contrôle compétente.

Art. 56

§ 1er. Les fichiers de journalisation sont établis dans des systèmes de traitement automatisé au moins pour les traitements suivants: la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement.

Les fichiers de journalisation de consultation et de communication permettent d'établir:

1° le motif, la date et l'heure de ces traitements;

2° les catégories de personnes qui ont consulté les données à caractère personnel, et si possible, l'identification de la personne qui a consulté ces données;

3° les systèmes qui ont communiqué ces données;

4° et les catégories de destinataires des données à caractère personnel, et si possible, l'identité des destinataires de ces données.

Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres après avis de l'autorité de contrôle compétente, d'autres types de traitements pour lesquels les fichiers de journalisation sont établis.

§ 2. Les fichiers de journalisation sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins visées à l'article 27.

§ 3. Le responsable du traitement et le sous-traitant mettent les journaux à la disposition de l'autorité de contrôle compétente, sur demande.

Art. 57

De verwerkingsverantwoordelijke en de verwerker werken op vraag van de bevoegde toezichthoudende autoriteit met deze laatste samen bij het vervullen van haar taken.

Art. 58

§ 1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert, verricht de verwerkingsverantwoordelijke vóór de verwerking een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

§ 2. De in de eerste paragraaf bedoelde beoordeling bevat ten minste een algemene beschrijving van de beoogde verwerkingen, een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen, de beoogde maatregelen ter beperking van de risico's, de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te beschermen en aan te tonen dat aan deze titel is voldaan, met inachtneming van de rechten en legitieme belangen van de betrokkenen en de andere belanghebbenden.

Art. 59

§ 1. De verwerkingsverantwoordelijke of zijn verwerker raadpleegt de bevoegde toezichthoudende autoriteit van de verwerkingsverantwoordelijke voordat de verwerking van persoonsgegevens in een nieuw bestand wordt opgenomen:

1° indien uit een gegevensbeschermingseffectbeoordeling als bedoeld in artikel 58 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken; of

2° indien de aard van de verwerking, in het bijzonder wanneer wordt gebruikgemaakt van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

De bevoegde toezichthoudende autoriteit wordt geraadpleegd bij het opstellen van een wet, een decreet of

Art. 57

Le responsable du traitement et le sous-traitant coopèrent avec l'autorité de contrôle compétente, à la demande de celle-ci, dans l'exécution de ses missions.

Art. 58

§ 1er. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, le responsable du traitement effectue préalablement au traitement une analyse d'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

§ 2. L'analyse visée au paragraphe premier contient au moins une description générale des traitements envisagés, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent titre, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes intéressées.

Art. 59

§ 1er. Le responsable du traitement ou son sous-traitant consulte l'autorité de contrôle compétente du responsable du traitement préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer:

1° lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 58, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; ou

2° lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

L'autorité de contrôle compétente est consultée dans le cadre de l'élaboration d'une loi, d'un décret ou d'une

een ordonnantie, of een daarop gebaseerde reglementaire maatregel in verband met de verwerking.

§ 2. De bevoegde toezichthoudende autoriteit kan een lijst opstellen van de verwerkingen waarvoor overeenkomstig paragraaf 1 een voorafgaande raadpleging moet plaatsvinden.

§ 3. De verwerkingsverantwoordelijke verstrekt de bevoegde toezichthoudende autoriteit de gegevensbeschermingseffectbeoordeling krachtens artikel 58 en, op vraag, alle andere informatie op grond waarvan de bevoegde toezichthoudende autoriteit de conformiteit van de verwerking en met name de risico's voor de bescherming van de persoonsgegevens van de betrokkene en de betrokken waarborgen kan beoordelen.

§ 4. Wanneer de bevoegde toezichthoudende autoriteit van oordeel is dat de in de eerste paragraaf van dit artikel bedoelde voorgenomen verwerking indruist tegen deze titel, met name wanneer de verwerkingsverantwoordelijke het risico onvoldoende heeft onderkend of beperkt, geeft ze binnen de zes weken na ontvangst van het verzoek om raadpleging een niet bindend schriftelijk advies aan de verwerkingsverantwoordelijke en in voorkomend geval aan de verwerker, en kan ze al haar bij de wet verleende bevoegdheden uitoefenen. Die termijn kan, naargelang de complexiteit van de voorgenomen verwerking, met een maand worden verlengd. De bevoegde toezichthoudende autoriteit stelt de verwerkingsverantwoordelijke en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van elke verlenging, alsook van de redenen voor de vertraging.

Art. 60

§ 1. De verwerkingsverantwoordelijke en de verwerker nemen passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, met name met betrekking tot de verwerking van persoonsgegevens bedoeld in artikel 34 van deze wet en rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, om een op het risico afgestemd beveiligingsniveau te waarborgen.

ordonnance, ou d'une mesure réglementaire fondée sur une telle loi, décret, ordonnance, qui se rapporte au traitement.

§ 2. L'autorité de contrôle compétente peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable conformément au paragraphe 1er.

§ 3. Le responsable du traitement fournit à l'autorité de contrôle compétente l'analyse d'impact relative à la protection des données en vertu de l'article 58 et, sur demande, toute autre information afin de permettre à l'autorité de contrôle compétente d'apprécier la conformité du traitement et, en particulier, les risques pour la protection des données à caractère personnel de la personne concernée et les garanties qui s'y rapportent.

§ 4. Lorsque l'autorité de contrôle compétente est d'avis que le traitement prévu, visé au paragraphe premier du présent article, constituerait une violation des dispositions adoptées en vertu du présent titre, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle compétente fournit par écrit, dans un délai maximum de six semaines à compter de la réception de la demande de consultation, un avis écrit non contraignant au responsable du traitement, et le cas échéant au sous-traitant, et elle peut faire usage des pouvoirs qui lui sont conférés par la loi. Ce délai peut être prolongé d'un mois, en fonction de la complexité du traitement prévu. L'autorité de contrôle compétente informe le responsable du traitement et, le cas échéant, le sous-traitant de toute prorogation dans un délai d'un mois à compter de la réception de la demande de consultation, ainsi que des motifs du retard.

Art. 60

§ 1er. Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des données à caractère personnel, visées à l'article 34 de la présente loi, et compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque.

§ 2. Ten aanzien van de geautomatiseerde verwerking neemt de verwerkingsverantwoordelijke of de verwerker, na beoordeling van het risico, maatregelen om:

1° te verhinderen dat onbevoegden toegang krijgen tot de verwerkingsapparatuur;

2° te verhinderen dat onbevoegden de gegevensdragers kunnen lezen, kopiëren, wijzigen of verwijderen;

3° te verhinderen dat onbevoegden persoonsgegevens invoeren of opgeslagen persoonsgegevens inzien, wijzigen of verwijderen;

4° te verhinderen dat onbevoegden geautomatiseerde verwerkingssystemen gebruiken met behulp van datatransmissieapparatuur;

5° ervoor te zorgen dat personen die bevoegd zijn om een geautomatiseerd verwerkingssysteem te gebruiken, uitsluitend toegang hebben tot de persoonsgegevens waarop hun toegangsbevoegdheid betrekking heeft;

6° ervoor te zorgen dat kan worden nagegaan en vastgesteld aan welke organen persoonsgegevens zijn of kunnen worden doorgezonden of beschikbaar gesteld met behulp van datatransmissieapparatuur;

7° ervoor te zorgen dat later kan worden nagegaan en vastgesteld welke persoonsgegevens wanneer en door wie in geautomatiseerde verwerkingssystemen zijn ingevoerd;

8° te verhinderen dat onbevoegden persoonsgegevens kunnen lezen, kopiëren, wijzigen of verwijderen bij de doorgifte van persoonsgegevens of het vervoer van gegevensdragers;

9° ervoor te zorgen dat de geïnstalleerde systemen in geval van storing opnieuw kunnen worden ingezet;

10° ervoor te zorgen dat de functies van het systeem werken, dat eventuele functionele storingen worden gesignaleerd en dat de bewaarde persoonsgegevens niet kunnen worden beschadigd door het verkeerd functioneren van het systeem.

§ 2. En ce qui concerne le traitement automatisé, le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à:

1° empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement;

2° empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée;

3° empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que la consultation, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées;

4° empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données;

5° garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation;

6° garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données;

7° garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites;

8° empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée;

9° garantir que les systèmes installés puissent être rétablis en cas d'interruption;

10° garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système.

Art. 61

§ 1. De verwerkingsverantwoordelijke meldt de inbreuk op de beveiliging zonder onnodige vertraging en indien mogelijk niet meer dan 72 uur nadat hij er kennis van heeft genomen aan de bevoegde toezichthoudende autoriteit. Die verplichte kennisgeving is niet van toepassing wanneer het waarschijnlijk is dat de inbreuk op de beveiliging geen risico voor de rechten en vrijheden van personen met zich brengt.

Wanneer de kennisgeving aan de bevoegde toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat ze vergezeld van een motivering voor de vertraging.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke zonder onnodige vertraging en uiterlijk binnen 72 uur zodra hij kennis heeft genomen van een inbreuk op de beveiliging.

§ 3. In de in de eerste paragraaf bedoelde melding wordt het volgende omschreven of meegedeeld:

1° de aard van de inbreuk op de beveiliging, met inbegrip van, indien mogelijk de categorieën van betrokkenen en gegevensbestanden in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensbestanden in kwestie;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, met inbegrip, in voorkomend geval maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

§ 4. Indien en voor zover het niet mogelijk is alle informatie gelijktijdig te verstrekken, kan de informatie zonder onnodige verdere vertraging in stappen worden verstrekt.

§ 5. Wanneer de inbreuk op de beveiliging betrekking heeft op persoonsgegevens die zijn doorgezonden door of aan de verwerkingsverantwoordelijke van een andere lidstaat van de Europese Unie, wordt de in paragraaf 3 bedoelde informatie zonder onnodige vertraging aan de verwerkingsverantwoordelijke van die lidstaat meegedeeld.

Art. 61

§ 1er. Le responsable du traitement notifie la brèche de sécurité, à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, dans un délai de 72 heures après en avoir pris connaissance. Cette obligation de notification n'est pas applicable lorsqu'il est raisonnable de croire que la brèche de sécurité en question n'engendre pas de risque pour les droits et les libertés d'une personne physique.

Lorsque la notification à l'autorité de contrôle compétente n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais et au plus tard dans les 72 heures après en avoir pris connaissance.

§ 3. La notification visée au paragraphe premier contient notamment:

1° la description de la nature de la brèche de sécurité y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

2° le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° la description des conséquences probables de la brèche de sécurité;

4° la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

§ 4. Si et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

§ 5. Lorsque la brèche de sécurité porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre État membre de l'Union européenne ou à celui-ci, les informations visées au paragraphe 3 sont communiquées au responsable du traitement de cet État membre dans les meilleurs délais.

§ 6. De verwerkingsverantwoordelijke documenteert alle in de eerste paragraaf bedoelde inbreuken op de beveiliging, met inbegrip van de feiten, de gevolgen ervan en de genomen corrigerende maatregelen. Die documentatie moet de bevoegde toezichthoudende autoriteit ertoe in staat stellen de naleving van dit artikel te controleren.

Art. 62

§ 1. Wanneer de inbreuk op de beveiliging waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk op de beveiliging onverwijld mee.

§ 2. De in de eerste paragraaf van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, van de aard van de inbreuk op de beveiliging en ten minste de in artikel 61, paragraaf 3, 2°, 3° en 4°, bedoelde gegevens en maatregelen.

§ 3. De in de eerste paragraaf bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

1° de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk op de beveiliging betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

2° de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in paragraaf 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

3° de mededeling zou onevenredige inspanningen vergen. In dat geval komt er daarvan een openbare mededeling of een soortgelijke maatregel waarbij de betrokkenen even doeltreffend worden geïnformeerd.

§ 4. Indien de verwerkingsverantwoordelijke de inbreuk op de beveiliging nog niet aan de betrokkene heeft gemeld, kan de bevoegde toezichthoudende autoriteit, na beraad over de kans dat de inbreuk op de beveiliging een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in paragraaf 3 bedoelde voorwaarden is voldaan.

§ 6. Le responsable du traitement documente toute brèche de sécurité visée au paragraphe premier, en indiquant les faits, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle compétente de vérifier le respect du présent article.

Art. 62

§ 1er. Lorsqu'une brèche de sécurité est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la brèche de sécurité à caractère personnel à la personne concernée dans les meilleurs délais.

§ 2. La communication à la personne concernée visée au paragraphe premier du présent article décrit, la nature de la brèche de sécurité et contient au moins les informations et mesures visées à l'article 61, paragraphe 3, points 2°, 3° et 4°.

§ 3. La communication à la personne concernée visée au paragraphe premier n'est pas nécessaire si l'une des conditions suivantes est remplie:

1° le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite brèche de sécurité;

2° le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1er n'est plus susceptible de se matérialiser;

3° elle exigerait des efforts disproportionnés. Dans ce cas, il est procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

§ 4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la brèche de sécurité la concernant, l'autorité de contrôle compétente peut, après avoir examiné si cette brèche de sécurité est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

§ 5. De in de eerste paragraaf van dit artikel bedoelde mededeling aan de betrokkene kan worden uitgesteld, beperkt of achterwege worden gelaten onder de voorwaarden en om de redenen bedoeld in artikel 37, paragraaf 2.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 63

§ 1. De verwerkingsverantwoordelijke wijst een of meerdere functionarissen voor gegevensbescherming aan.

§ 2. De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 65 bedoelde taken te vervullen.

§ 3. Het is mogelijk om voor verschillende bevoegde overheden of verwerkingsverantwoordelijken, rekening houdend met hun organisatiestructuur en omvang, één functionaris voor gegevensbescherming aan te wijzen.

§ 4. De verwerkingsverantwoordelijke maakt de contactgegevens van de functionaris voor gegevensbescherming openbaar en deelt die mee aan de bevoegde toezichthoudende autoriteit.

§ 5. De nadere regels voor de werking, de aanwijzing en vereiste competenties worden door de Koning bepaald.

Art. 64

§ 1. De verwerkingsverantwoordelijke ziet erop toe dat de functionaris voor gegevensbescherming tijdig en naar behoren bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden, wordt betrokken.

§ 2. De verwerkingsverantwoordelijke stelt de functionaris voor gegevensbescherming de benodigde middelen ter beschikking voor het vervullen van die taken en verschaft hem toegang tot de persoonsgegevens en de verwerkingen, en biedt hem de mogelijkheid zijn deskundigheid op peil te houden.

§ 3. De verwerkingsverantwoordelijke ziet erop toe dat de functionaris voor gegevensbescherming geen

§ 5. La communication à la personne concernée visée au paragraphe premier du présent article peut être retardée, limitée ou omise, sous réserve des conditions et pour les motifs visés à l'article 37, paragraphe 2.

Section 5

Délégué à la protection des données

Art. 63

§ 1er. Le responsable du traitement désigne un ou plusieurs délégués à la protection des données.

§ 2. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à exercer les missions visées à l'article 65.

§ 3. Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes ou responsables du traitement, compte tenu de leur structure organisationnelle et de leur taille.

§ 4. Le responsable du traitement publie les coordonnées du délégué à la protection des données et les communique à l'autorité de contrôle compétente.

§ 5. Les modalités de fonctionnement, de désignation ainsi que les compétences requises sont définies par le Roi.

Art. 64

§ 1er. Le responsable du traitement veille à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

§ 2. Le responsable du traitement fournit au délégué à la protection des données les ressources nécessaires pour exercer ses missions ainsi que l'accès aux données à caractère personnel et aux traitements, et lui permet d'entretenir ses connaissances spécialisées.

§ 3. Le responsable du traitement veille à ce que le délégué à la protection des données ne reçoive

instructies ontvangt met betrekking tot de uitvoering van die taken. De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke.

§ 4. Behalve bij toepassing van de artikelen 41 en 44 kunnen de betrokkenen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten.

§ 5. De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.

§ 6. De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

Art. 65

De functionaris voor gegevensbescherming vervult in het bijzonder de volgende taken:

1° de verwerkingsverantwoordelijke en de werknemers die de verwerking verrichten informeren en adviseren over hun verplichtingen met betrekking tot de bescherming van persoonsgegevens;

2° toezien op de naleving van de regelgeving en de interne regels van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, de bewustmaking en de opleiding van het bij de verwerking betrokken personeel en de betreffende audits;

3° desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 58;

4° met de bevoegde toezichthoudende autoriteit samenwerken;

5° optreden als contactpunt voor de bevoegde toezichthoudende autoriteit inzake met de verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 59 bedoelde voorafgaande raadpleging, en, in voorkomend geval, overleg plegen over enige andere aangelegenheid.

aucune instruction en ce qui concerne l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement.

§ 4. Sauf application des articles 41 et 44, les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits qui leur sont conférés.

§ 5. Le délégué à la protection des données est soumis au secret ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.

§ 6. Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement veille à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts.

Art. 65

Les missions du délégué à la protection des données sont notamment les suivantes:

1° informer et conseiller le responsable du traitement et les employés qui procèdent au traitement sur les obligations qui leur incombent en matière de protection des données;

2° contrôler le respect de la réglementation et des règles internes du responsable du traitement en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant à des opérations de traitement, et les audits s'y rapportant;

3° dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 58;

4° coopérer avec l'autorité de contrôle compétente;

5° faire office de point de contact pour l'autorité de contrôle compétente sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 59, et mener des consultations, le cas échéant, sur tout autre sujet.

HOOFDSTUK V

Doorgiften van persoonsgegevens aan derde landen of internationale organisaties

Art. 66

§ 1. Onverminderd de bepalingen van deze titel, mogen de bevoegde overheden persoonsgegevens slechts doorgeven aan landen buiten de Europese Unie of aan een internationale organisatie, met inbegrip vanvan verdere doorgifte aan een ander land buiten de Europese Unie of een andere internationale organisatie, indien aan de volgende voorwaarden is voldaan:

1° de doorgifte is noodzakelijk met het oog op de doeleinden van artikel 27;

2° de persoonsgegevens worden doorgegeven aan een verwerkingsverantwoordelijke in een land buiten de Europese Unie of in een internationale organisatie die een bevoegde overheid is voor de in artikel 27, bedoelde doeleinden;

3° ingeval persoonsgegevens worden doorgezonden of beschikbaar gesteld vanuit een andere lidstaat van de Europese Unie, heeft die lidstaat overeenkomstig zijn nationale recht zijn voorafgaande toestemming gegeven voor de doorgifte;

4° de Europese Commissie heeft een adequaatheidsbesluit zoals bedoeld in artikel 62 vastgesteld, of, indien een dergelijk besluit er niet is, zijn er krachtens artikel 68 passende waarborgen geboden of gelden er afwijkingen voor specifieke situaties uit hoofde van artikel 69;

5° in het geval van een verdere doorgifte aan een ander land buiten de Europese Unie of een andere internationale organisatie, geeft de verwerkingsverantwoordelijke, toestemming voor de verdere doorgifte , na alle relevante factoren naar behoren in aanmerking te hebben genomen, met inbegrip van de ernst van het strafbare feit, het doel waarvoor de persoonsgegevens oorspronkelijk waren doorgegeven en het niveau van persoonsgegevensbescherming in het derde land of de internationale organisatie waaraan de persoonsgegevens verder worden doorgegeven.

§ 2. De doorgifte zonder de voorafgaande toestemming vanwege een andere lidstaat van de Europese Unie zoals bedoeld in punt 3° van de eerste paragraaf is slechts toegelaten indien deze doorgifte van

CHAPITRE V

Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

Art. 66

§ 1er. Sans préjudice des dispositions du présent titre, un transfert, par des autorités compétentes, de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale, y compris des transferts ultérieurs vers un autre pays non membre à l'Union européenne ou à une autre organisation internationale, n'a lieu, que lorsque les conditions ci-après sont respectées:

1° le transfert est nécessaire aux fins énoncées à l'article 27;

2° les données à caractère personnel sont transférées à un responsable du traitement dans un pays non membre de l'Union européenne ou à une organisation internationale qui est une autorité compétente aux fins visées à l'article 27;

3° en cas de transfert ou de mise à disposition de données à caractère personnel provenant d'un autre État membre de l'Union européenne, celui-ci a préalablement autorisé ce transfert conformément à son droit national;

4° la Commission européenne a adopté une décision d'adéquation tel que visé à l'article 62, ou, en l'absence d'une telle décision, des garanties appropriées ont été prévues ou existent en application de l'article 68 ou, des dérogations pour des situations particulières s'appliquent en vertu de l'article 69;

5° en cas de transfert ultérieur vers un autre pays non membre de l'Union européenne ou à une autre organisation internationale, le responsable du traitement qui a reçu les données autorise le transfert ultérieur, après avoir dûment pris en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, la finalité pour laquelle les données à caractère personnel ont été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données à caractère personnel sont transférées ultérieurement.

§ 2. Les transferts effectués sans l'autorisation préalable d'un autre État membre de l'Union européenne prévue au paragraphe premier, point 3°, sont autorisés uniquement lorsque le transfert de données à caractère

persoonsgegevens noodzakelijk is met het oog op de voorkoming van een acute en ernstige bedreiging van de openbare veiligheid van een lidstaat of een derde land of voor de fundamentele belangen van een lidstaat van de Europese Unie, en voorafgaande toestemming niet tijdig kan worden verkregen. De voor het geven van voorafgaande toestemming verantwoordelijke overheid wordt onverwijld in kennis gesteld.

Art. 67

Een doorgifte van persoonsgegevens aan een land buiten de Europese Unie of een internationale organisatie kan slechts plaatsvinden wanneer de Europese Commissie bij adequaatheidsbesluit bepaald heeft dat het land, een gebied of één of meerdere nader bepaalde sectoren in dat land, of de internationale organisatie in kwestie een passend beschermingsniveau waarborgt. Voor een dergelijke doorgifte is geen specifieke toestemming nodig.

Art. 68

§ 1. Bij gebreke van een adequaatheidsbesluit zoals bedoeld in artikel 67, of wanneer dat is opgeheven, gewijzigd of opgeschort, kan een doorgifte van persoonsgegevens aan een land buiten de Europese Unie of een internationale organisatie slechts plaatsvinden wanneer:

1° in een juridisch bindend instrument wordt voorzien in passende waarborgen voor de bescherming van persoonsgegevens; of

2° de verwerkingsverantwoordelijke alle omstandigheden in verband met de doorgifte van persoonsgegevens heeft beoordeeld en heeft geconcludeerd dat er passende waarborgen bestaan voor de bescherming van persoonsgegevens.

§ 2. De verwerkingsverantwoordelijke informeert de bevoegde toezichthoudende autoriteit over de categorieën van doorgiften uit hoofde van de eerste paragraaf, punt 2°.

§ 3. De doorgifte gebaseerd op de eerste paragraaf, punt 2° wordt gedocumenteerd en bevat:

1° de datum en tijd van doorgifte;

2° informatie over de ontvangende bevoegde autoriteit;

3° de reden voor de doorgifte en de doorgegeven persoonsgegevens.

personnel est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre de l'Union européenne et si l'autorisation préalable ne peut pas être obtenue en temps utile. L'autorité à laquelle il revient d'accorder l'autorisation préalable est informée sans retard.

Art. 67

Un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale peut avoir lieu lorsque la Commission européenne a constaté par voie de décision d'adéquation que le pays, un territoire ou un ou plusieurs secteurs déterminés dans ce pays, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

Art. 68

§ 1er. En l'absence de décision d'adéquation, visée à l'article 67, ou lorsque celle-ci est abrogée, modifiée ou suspendue, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale peut avoir lieu lorsque:

1° des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant; ou

2° le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.

§ 2. Le responsable du traitement informe l'autorité de contrôle compétente des catégories de transferts relevant du paragraphe premier, point 2°.

§ 3. Le transfert effectué en vertu du paragraphe premier, point 2°, est documenté et, comporte:

1° la date et l'heure du transfert;

2° des informations sur l'autorité compétente destinataire;

3° la justification du transfert et les données à caractère personnel transférées.

De documentatie wordt desgevraagd ter beschikking van de bevoegde toezichthoudende autoriteit gesteld.

Art. 69

§ 1. Bij gebreke van een adequaatheidsbesluit zoals bedoeld in artikel 67, of van passende waarborgen zoals bedoeld in artikel 68, is een doorgifte of een categorie van doorgiften van persoonsgegevens aan een land buiten de Europese Unie of een internationale organisatie slechts toegelaten indien de doorgifte noodzakelijk is:

1° om de vitale belangen van de betrokkene of van een andere persoon te beschermen;

2° om de legitieme belangen van de betrokkene te beschermen wanneer de wet daarin voorziet;

3° om een onmiddellijke en ernstige bedreiging van de openbare veiligheid te voorkomen;

4° in uitzonderlijke gevallen met het oog op de doeleinden van artikel 27;

5° in specifieke gevallen met het oog op het instellen, uitoefenen of verdedigen van rechtsvorderingen in verband met de doeleinden van artikel 27.

§ 2. Persoonsgegevens worden niet doorgegeven indien de bevoegde autoriteit die de doorgifte verricht, meent dat de grondrechten en fundamentele vrijheden van de betrokkene zwaarder wegen dan het algemeen belang van de doorgifte bedoeld in de eerste paragraaf, punten 4° en 5°.

§ 3. De doorgifte bedoeld in de eerste paragraaf, punt 2°, wordt gedocumenteerd en bevat:

1° de datum en tijd van doorgifte;

2° informatie over de ontvangende bevoegde autoriteit;

3° de reden voor de doorgifte en de doorgegeven persoonsgegevens.

De documentatie wordt desgevraagd ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Art. 70

§ 1. In afwijking van artikel 66, eerste paragraaf, punt 2°, en onverminderd de internationale overeenkomsten

La documentation est mise à la disposition de l'autorité de contrôle compétente sur demande.

Art. 69

§ 1er. En l'absence de décision d'adéquation visée à l'article 67 ou de garanties appropriées visées à l'article 68, un transfert ou une catégorie de transferts de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale ne peut avoir lieu qu'à condition que le transfert soit nécessaire:

1° à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne;

2° à la sauvegarde des intérêts légitimes de la personne concernée lorsque la loi le prévoit;

3° pour prévenir une menace grave et immédiate pour la sécurité publique;

4° dans des cas particuliers, aux fins énoncées à l'article 27;

5° dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les fins énoncées à l'article 27.

§ 2. Les données à caractère personnel ne sont pas transférées si l'autorité compétente qui transfère les données estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert visé au paragraphe premier, points 4° et 5°.

§ 3. Le transfert visé au paragraphe premier, point 2°, est documenté et indique:

1° la date et l'heure du transfert;

2° les informations sur l'autorité compétente destinataire;

3° la justification du transfert et les données à caractère personnel transférées.

La documentation est mise à la disposition de l'autorité de contrôle compétente, sur demande.

Art. 70

§ 1er. Par dérogation à l'article 66, paragraphe premier, point 2°, et sans préjudice de tout accord international et

en bepalingen van deze titel, mogen de bevoegde autoriteiten , in bepaalde specifieke gevallen, persoonsgegevens rechtstreeks doorgeven aan ontvangers in landen buiten de Europese Unie die geen bevoegde autoriteit zijn voor de doeleinden in artikel 27, voor zover aan alle onderstaande voorwaarden is voldaan:

1° de doorgifte is strikt noodzakelijk voor de uitvoering van de opdrachten van de bevoegde autoriteit die de doorgifte doet;

2° de bevoegde autoriteit die de gegevens doorgeeft, stelt vast dat er geen fundamentele rechten en vrijheden van de betrokkene voorrang hebben op het algemeen belang waarvoor de overdracht in het betreffende geval vereist is;

3° de bevoegde autoriteit die de doorgifte doet, meent dat de doorgifte aan een bevoegde autoriteit binnen het desbestreffende land ondoeltreffend of ongeschikt is, met name omdat de doorgifte niet tijdig kan worden bewerkstelligd;

4° de bevoegde autoriteit in het desbetreffende land wordt zonder onnodige vertraging op de hoogte gebracht, tenzij dat ondoeltreffend of ongeschikt is;

5° de bevoegde autoriteit die de doorgifte doet, licht de ontvanger in over het nader bepaalde doel of de nader bepaalde doeleinden waarvoor de persoonsgegevens bij uitsluiting door laatstgenoemde mogen worden verwerkt, op voorwaarde dat een dergelijke verwerking noodzakelijk is.

§ 2. De bevoegde autoriteit die de doorgifte doet, stelt de toezichthoudende autoriteit in kennis van doorgiften die gebeuren in het kader van dit artikel.

§ 3. Wanneer een doorgifte is gebaseerd op de eerste paragraaf, wordt die gedocumenteerd.

HOOFDSTUK VI

Onafhankelijke toezichthoudende autoriteiten

Art. 71

§ 1. Bij de Kamer van volksvertegenwoordigers wordt een onafhankelijke toezichthoudende autoriteit op de politionele informatie opgericht, Controleorgaan op de politionele informatie genoemd.

des dispositions du présent titre, les autorités compétentes peuvent, dans certains cas particuliers, transférer des données à caractère personnel directement aux destinataires qui ne sont pas des autorités compétentes pour les finalités visées à l'article 27, établis dans des pays non membre de l'Union européenne, uniquement lorsque toutes les conditions ci-après sont remplies:

1° le transfert est strictement nécessaire à l'exécution de la mission de l'autorité compétente qui transfère les données;

2° l'autorité compétente qui transfère les données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas en question;

3° l'autorité compétente qui transfère les données estime que le transfert à une autorité compétente, dans le pays concerné est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun;

4° l'autorité compétente dans le pays concerné est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié;

5° l'autorité compétente qui transfère les données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel ne doivent faire l'objet d'un traitement que par cette dernière, à condition qu'un tel traitement soit nécessaire.

§ 2. L'autorité compétente qui transfère les données informe l'autorité de contrôle des transferts relevant du présent article.

§ 3. Lorsqu'un transfert est effectué sur la base du paragraphe premier, ce transfert est documenté.

CHAPITRE VI

Autorités de contrôle indépendantes

Art. 71

§ 1er. Il est créé auprès de la Chambre des représentants une autorité de contrôle indépendante de l'information policière, dénommé Organe de contrôle de l'information policière.

Zij is de rechtsopvolger van het Controleorgaan op de politionele informatie bedoeld in artikel 44/6, § 1, van de wet op het politieambt.

Zij is ten aanzien van de bevoegde overheden bedoeld in artikel 26, § 1, 7°, a), d), f), belast, met:

1°het toezicht op de toepassing van de huidige titel II, zoals voorzien door artikel 26, 15°;

2°de controle van de verwerking van de informatie en de persoonsgegevens bedoeld in artikel 44/1 tot en met 44/11/13 van de wet op het politieambt, met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2;

3°elke andere opdracht haar door of krachtens andere wetten verleend.

§ 2. De zetel van het Controleorgaan op de politionele informatie is gevestigd in het administratief arrondissement Brussel-Hoofdstad.

Bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden overeenkomstig deze wet en andere wetten treedt het Controleorgaan op de politionele informatie volledig onafhankelijk op.

§ 3. Haar samenstelling, het statuut van haar leden, haar opdrachten, haar bevoegdheden evenals haar financiering worden geregeld in titel 7 van deze wet.

TITEL 3

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door andere overheden dan die bedoeld in titels 1 en 2

ONDERTITEL 1

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten

HOOFDSTUK I

Definities

Art. 72

§ 1. De definities bedoeld in de artikelen 26, 1° tot 6°, 9°, 11° tot 14°, 16° en 17° zijn van toepassing op deze ondertitel.

Elle succède à l'organe de contrôle de l'information policière visé à l'article 44/6, § 1er, de la loi sur la fonction de police.

Elle est, vis-à-vis des autorités compétentes visées à l'article 26, § 1er, 7°, a), d), f), chargée de:

1°surveiller l'application du présent titre II, comme prévu à l'article 26, 15°;

2°contrôler le traitement des informations et des données à caractère personnel visées à l'article 44/1 jusqu'au 44/11/13 de la loi sur la fonction de police y compris celles incluses dans les banques de données visées à l'article 44/2;

3°toute autre mission organisée par ou en vertu d'autres lois.

§ 2. Le siège de l'Organe de contrôle de l'information policière est établi dans l'arrondissement administratif de Bruxelles-Capitale.

Dans l'exercice de ses missions et des pouvoirs dont elle est investie conformément à la présente loi, l'Organe de contrôle de l'information policière agit en toute indépendance.

§ 3. Sa composition, le statut de ses membres, ses missions, ses compétences ainsi que son financement sont réglés dans le titre 7 de la presente loi.

TITRE 3

De la protection des personnes physiques à l'égard du traitement des données a caractère personnel par d'autres autorités que celles visées aux titres 1er et 2

SOUS-TITRE 1er

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les services de renseignements et de sécurité

CHAPITRE IER

Définitions

Art. 72

§ 1er. Les définitions visées à l'article 26, 1° à 6°, 9°, 11° à 14°, 16° et 17° sont applicables au présent sous-titre.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder:

1° “de inlichtingen- en veiligheidsdiensten”: de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° “de verwerkingsverantwoordelijke”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

3° “de wet van 30 november 1998”: de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

4° “de wet van 18 juli 1991”: de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

5° “de wet van 11 december 1998”: de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

6° “toezichthoudende autoriteit”: een onafhankelijke overheidsinstantie die bij wet belast is met het toezicht op de toepassing van deze wet;

7° “het Vast Comité I”: het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 18 juli 1991 belast met het toezicht op de toepassing van deze ondertitel in toepassing van artikel 95.

HOOFDSTUK II

Toepassingsgebied

Art. 73

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten en hun verwerkers, uitgevoerd in het kader van de opdrachten van deze diensten als bedoeld in artikelen 7 en 11 van de wet van 30 november 1998 alsook door of krachtens bijzondere wetten.

Titels 1, 2, 4, 5 en 7 van deze wet zijn niet van toepassing op de verwerkingen bedoeld in het eerste lid. Enkel de artikelen 226 en 227 van titel 6 zijn van toepassing.

§ 2. Pour l’application du présent sous-titre, on entend par:

1° “les services de renseignement et de sécurité”: la Sûreté de l’État et le Service Général du Renseignement et de la Sécurité visés dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° “le responsable du traitement”: la personne physique ou morale, l’autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement;

3° “la loi du 30 novembre 1998”: la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

4° “la loi du 18 juillet 1991”: la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l’Organe de coordination pour l’analyse de la menace;

5° “la loi du 11 décembre 1998”: la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

6° “autorité de contrôle”: une autorité publique indépendante chargée par la loi de surveiller l’application de la présente loi;

7° “Comité permanent R”: le Comité permanent de contrôle des services de renseignement visé dans la loi du 18 juillet 1991 chargé du contrôle de l’application du présent sous-titre en application de l’article 95.

CHAPITRE II

Champ d’application

Art. 73

Le présent sous-titre s’applique à tout traitement de données à caractère personnel par les services de renseignement et de sécurité et leurs sous-traitants effectués dans le cadre des missions desdits services visés aux articles 7 et 11 de la loi du 30 novembre 1998 ainsi que par ou en vertu de lois particulières.

Les titres 1, 2, 4, 5 et 7 de la présente loi ne s’appliquent pas aux traitements visés à l’alinéa premier. Dans le titre 6, seuls les articles 226 et 227 sont d’application.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 74

Persoonsgegevens mogen slechts verwerkt worden in één van de volgende gevallen:

1° wanneer de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend;

2° wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;

3° wanneer de verwerking nuttig is om een verplichting na te komen waaraan de inlichtingen- en veiligheidsdienst is onderworpen door of krachtens een wet;

4° wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verwerkingsverantwoordelijke of aan de overheidsinstantie aan wie de persoonsgegevens worden verstrekt.

Art. 75

Persoonsgegevens moeten:

1° eerlijk en rechtmatig worden verwerkt;

2° voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen en niet verder worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden. Onder de voorwaarden vastgesteld door de artikelen 99 tot 104 wordt een verdere verwerking van de gegevens voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd;

3° toereikend, terzake dienend en niet overmatig zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4° nauwkeurig zijn en, zo nodig, worden bijgewerkt. Alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij

CHAPITRE III

Conditions générales du traitement

Art. 74

Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants:

1° lorsque la personne concernée a indubitablement donné son consentement;

2° lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

3° lorsqu'il est utile au respect d'une obligation à laquelle le service de renseignement et de sécurité concerné est soumis par ou en vertu d'une loi;

4° lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou une autorité publique à laquelle les données à caractère personnel sont communiquées.

Art. 75

Les données à caractère personnel doivent être:

1° traitées loyalement et licitement;

2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et réglementaires applicables. Un traitement ultérieur à des fins historiques, scientifiques ou statistiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par les articles 99 à 104;

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement;

4° exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles

verder worden verwerkt, onnauwkeurig of onvolledig zijn, te wissen of te verbeteren.

HOOFDSTUK IV

Aard van de persoonsgegevens

Art. 76

De inlichtingen- en veiligheidsdiensten verwerken, voor het belang van de uitoefening van hun opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook genetische en biometrische gegevens, gezondheidsgegevens, gegevens die het seksuele gedrag of de seksuele gerichtheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 77

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de modaliteiten bepaald in het kader van artikel 21 van de wet van 30 november 1998.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 78

Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.

Art. 79

De betrokkene heeft het recht te vragen:

sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

CHAPITRE IV

Nature des données à caractère personnel

Art. 76

Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité traitent des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

CHAPITRE V

Conservation des données à caractère personnel

Art. 77

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées dans le cadre de l'article 21 de la loi du 30 novembre 1998.

CHAPITRE VI

Droits de la personne concernée

Art. 78

Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 79

La personne concernée a le droit de demander:

1° om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen overeenkomstig artikel 80;

2° om de verificatie bij het Vast Comité I van de naleving van de bepalingen van deze ondertitel overeenkomstig artikel 80.

Art. 80

De rechten, bedoeld in artikel 79 worden kosteloos uitgeoefend via het Vast Comité I op initiatief van de betrokkene die zijn identiteit bewijst.

Deze voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht.

De nadere regels voor de uitoefening van deze rechten worden bepaald in de wet.

Art. 81

Het Vast Comite I en de inlichtingen- en veiligheidsdiensten houden een logbestand bij van alle aanvragen van betrokkenen tot uitoefening van hun rechten.

Art. 82

Een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn, mag niet louter worden genomen op grond van een geautomatiseerde persoonsgegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.

Het in het eerste lid vastgestelde verbod geldt niet indien het besluit zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet of wanneer het noodzakelijk is vanwege een zwaarwegend algemeen belang.

1° la rectification ou la suppression de ses données à caractère personnel inexactes conformément à l'article 80;

2° la vérification auprès du Comité permanent R du respect des dispositions du présent sous-titre conformément à l'article 80.

Art. 80

Les droits visés à l'article 79 s'exercent, sans frais, par l'intermédiaire du Comité permanent R, à l'initiative de la personne concernée justifiant de son identité.

Celui-ci effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Les modalités d'exercice de ces droits sont déterminées par la loi.

Art. 81

Le Comité permanent R et les services de renseignement et de sécurité tiennent un journal des demandes d'exercice des droits par les personnes concernées.

Art. 82

Une décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

L'interdiction prévue à l'alinéa premier ne s'applique pas lorsque la décision est fondée sur une disposition prévue par ou en vertu d'une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important.

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 83

De verwerkingsverantwoordelijke moet:

1° er nauwlettend over waken dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2° ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst;

3° alle personen die onder zijn gezag handelen, informeren over de bepalingen van deze ondertitel en over alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer betreffende de verwerking van persoonsgegevens.

Art. 84

Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verwerkingsverantwoordelijke:

1° een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de verwerkingen;

2° toezien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen;

3° de verantwoordelijkheid van de verwerker vaststellen in de overeenkomst;

4° met de verwerker overeenkomen dat hij slechts handelt in opdracht van de verwerkingsverantwoordelijke en dat hij is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke in toepassing van deze ondertitel is gehouden;

5° in een geschrift of op een elektronische drager de elementen van de overeenkomst met betrekking tot de

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 83

Le responsable du traitement doit:

1° faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2° veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins du service;

3° informer les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 84

Lorsque le traitement est confié à un sous-traitant, le responsable du traitement doit:

1° choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements;

2° veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles;

3° fixer dans le contrat la responsabilité du sous-traitant;

4° convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et qu'il est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du présent sous-titre;

5° consigner par écrit ou sur un support électronique les éléments du contrat relatifs à la protection

bescherming van de persoonsgegevens en de eisen met betrekking tot de maatregelen bedoeld in 3° en 4°, vaststellen.

Art. 85

De verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke is gehouden.

Hij mag de verwerking van persoonsgegevens niet toevertrouwen aan een andere verwerker, behoudens uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Art. 86

Eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker, alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verwerkingsverantwoordelijke verwerken, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 87

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken.

Een overeenkomst bepaalt de respectievelijke verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken, met name met betrekking tot de uitoefening van de rechten van de betrokkene en de mededeling van persoonsgegevens, tenzij hun respectievelijke verplichtingen worden bepaald door of krachtens een wet.

In de overeenkomst wordt één contactpunt voor de betrokkenen aangewezen. De gezamenlijke verwerkingsverantwoordelijken nemen dit contactpunt op in het register bedoeld in artikel 90.

des données à caractère personnel et les exigences relatives aux mesures visées aux 3° et 4°.

Art. 85

Le sous-traitant est soumis aux mêmes obligations que celles qui incombent au responsable du traitement.

Il ne peut pas confier le traitement de données à caractère personnel à un autre sous-traitant, sauf autorisation expresse du responsable du traitement.

Art. 86

Toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 87

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Un accord définit les obligations respectives des responsables conjoints de traitement, notamment en ce qui concerne l'exercice des droits de la personne concernée et la communication des données à caractère personnel, sauf si leurs obligations respectives sont définies par ou en vertu d'une loi.

Un seul point de contact pour les personnes concernées est désigné dans l'accord. Les responsables conjoints du traitement incluent ce point de contact dans le registre visé à l'article 90.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 88

Om de veiligheid van de persoonsgegevens te waarborgen, treffen de verwerkingsverantwoordelijke, alsmede de verwerker, de passende technische en organisatorische maatregelen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen verzekeren een passend beveiligingsniveau, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen persoonsgegevens en de potentiële risico's.

Art. 89

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk binnen de kortste termijn aan het Vast Comité I en indien mogelijk, 72 uur nadat hij er kennis van heeft genomen.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke binnen de kortste termijn van elke inbreuk op de beveiliging.

§ 3. In de in paragrafen 1 en 2 bedoelde melding wordt, op zijn minst, het volgende omschreven of meegedeeld:

1° de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en de opgeslagen persoonsgegevens in kwestie;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt bij wie bijkomende informatie kan worden verkregen;

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de verwerkingsverantwoordelijke, of de verwerker heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder

Section 3

Sécurité des données à caractère personnel

Art. 88

Le responsable du traitement ainsi que le sous-traitant prennent les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures assurent un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels.

Art. 89

§ 1er. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie au Comité permanent R dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais.

§ 3. La notification visée aux paragraphes premier et 2 doit, à tout le moins:

1° décrire la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° décrire les conséquences probables de la brèche de sécurité;

4° décrire les mesures prises ou que le responsable du traitement ou le sous-traitant propose de prendre pour remédier à la brèche de sécurité, y compris, le cas

desgevallend maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Afdeling 4

Registers

Art. 90

§ 1. De verwerkingsverantwoordelijke houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van de gegevensbanken van de inlichtingen- en veiligheidsdiensten en deze die aan hem ter beschikking worden gesteld.

Dit register bevat de volgende gegevens:

1° voor de gegevensbanken van de inlichtingen- en veiligheidsdiensten:

a) de contactgegevens van de verwerkingsverantwoordelijke en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

a) de verwerkingsdoeleinden;

b) de categorieën van ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

c) indien mogelijk, de beoogde termijnen voor het verwijderen van de persoonsgegevens;

d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 88.

2° voor gegevensbanken die aan de inlichtingen- en veiligheidsdiensten ter beschikking gesteld worden:

a) de contactgegevens van de verwerkingsverantwoordelijke en, indien mogelijk voor de landen buiten de Europese Unie de dienst die de gegevensbank beheert en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

a) de verwerkingsdoeleinden van de inlichtingen- en veiligheidsdiensten.

§ 2. Elke verwerker houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.

échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Section 4

Registres

Art. 90

§ 1er. Le responsable du traitement tient un registre, classifié au sens de la loi du 11 décembre 1998, des banques de données des services de renseignement et de sécurité et de celles mises à leur disposition.

Ce registre comporte les informations suivantes:

1° pour les banques de données des services de renseignement et de sécurité:

a) les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) les catégories de destinataires auxquels des données à caractère personnel peuvent être communiquées;

d) dans la mesure du possible, les délais prévus pour l'effacement des données à caractère personnel;

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 88.

2° pour les banques de données mises à la disposition des services de renseignement et de sécurité:

a) les coordonnées du responsable du traitement et, si possible pour les pays hors de l'Union européenne le service gestionnaire de la banque de données et, le cas échéant, des responsables conjoints du traitement, et du délégué à la protection des données;

b) les finalités du traitement par le service de renseignement et de sécurité.

§ 2. Chaque sous-traitant tient un registre, classifié au sens de la loi du 11 décembre 1998, de toutes les catégories d'activités de traitement effectuées pour le compte d'un responsable du traitement.

Dit register bevat de volgende elementen:

1° de contactgegevens van de verwerker en van de verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, desgevallend, van de functionaris voor gegevensbescherming;

2° de categorieën van verwerkingen die voor rekening van de verwerkingsverantwoordelijke zijn uitgevoerd;

3° indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 88.

§ 3. De in de paragrafen 1 en 2 bedoelde registers worden in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 4. De verwerkingsverantwoordelijke stelt het register ter beschikking van het Vast Comité I op diens vraag.

De verwerker stelt het register ter beschikking van de verwerkingsverantwoordelijke en stelt het eveneens ter beschikking van het Vast Comité I op diens vraag.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 91

§ 1. De verwerkingsverantwoordelijke, en desgevallend de verwerker, wijzen een functionaris voor gegevensbescherming aan. Deze beslissing wordt meegedeeld aan het Vast Comité I.

De functionaris voor gegevensbescherming is titularis van een veiligheidsmachtiging “zeer geheim”, in de zin van de wet van 11 december 1998.

§ 2. De functionaris voor gegevensbescherming kan niet gestraft worden voor het uitoefenen van zijn functie. Hij kan evenmin van zijn functie ontheven worden omwille van de uitvoering van zijn opdrachten, behalve indien hij een zware fout heeft begaan of de voorwaarden noodzakelijk voor het uitoefenen van zijn functie niet langer vervult.

De functionaris voor gegevensbescherming kan zich tot het Vast Comité I wenden om deze beslissing aan te vechten.

§ 3. Hij is, op een onafhankelijke wijze, belast met:

Ce registre comprend les éléments suivants:

1° les coordonnées du sous-traitant et du responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les coordonnées du délégué à la protection des données;

2° les catégories de traitements effectués pour le compte du responsable du traitement;

3° dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l’article 88.

§ 3. Les registres visés aux paragraphes premier et 2 se présentent sous une forme écrite y compris la forme électronique.

§ 4. Le responsable du traitement met le registre à la disposition du Comité permanent R à sa demande.

Le sous-traitant met le registre à la disposition du responsable du traitement ainsi qu’à la disposition du Comité permanent R à sa demande.

Section 5

Délégué à la protection des données

Art. 91

§ 1er. Le responsable du traitement et, le cas échéant, le sous-traitant désignent un délégué à la protection des données. Cette décision est communiquée au Comité permanent R.

Le délégué à la protection des données est titulaire d’une habilitation de sécurité de niveau très secret, au sens de la loi du 11 décembre 1998.

§ 2. Le délégué à la protection des données ne peut pas être sanctionné en raison de l’exercice de ses fonctions. Il ne peut pas être relevé de ses fonctions en raison de l’exercice de ses missions, sauf s’il a commis une faute grave ou s’il ne remplit plus les conditions nécessaires à l’exercice de ses fonctions.

Le délégué à la protection des données peut s’adresser au Comité permanent R pour contester cette décision.

§ 3. Il est chargé de manière indépendante:

1° het toezien op de naleving van deze ondertitel voor elke verwerking van persoonsgegevens;

2° het adviseren over alle nuttige maatregelen teneinde de veiligheid van de opgeslagen gegevens te verzekeren;

3° het informeren en adviseren van de verwerkingsverantwoordelijke, en desgevallend de verwerker, het diensthoofd en de personeelsleden van de betrokken dienst die de verwerking verrichten over hun verplichtingen op grond van deze ondertitel;

4° het verstrekken van adviezen of aanbevelingen aan de verwerkingsverantwoordelijke, en desgevallend aan de verwerker of het diensthoofd;

5° het uitvoeren van andere opdrachten die hem door de verwerkingsverantwoordelijke, en in voorkomend geval de verwerker of het diensthoofd toevertrouwd zijn.

De functionaris voor gegevensbescherming is de contactpersoon voor het Vast Comité I met betrekking tot de toepassing van deze ondertitel.

§ 4. De verwerkingsverantwoordelijke, en desgevallend de verwerker ziet erop toe dat hun functionaris voor gegevensbescherming tijdig en naar behoren wordt betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden.

De verwerkingsverantwoordelijke, en desgevallend de verwerker ziet erop toe dat de functionaris voor gegevensbescherming de benodigde middelen ter beschikking heeft voor het vervullen van zijn taken.

De functionaris voor gegevensbescherming kan worden bijgestaan door één of meerdere adjuncten.

§ 5. Desgevallend kunnen nadere regels voor de werking, de aanwijzing en de vereiste bevoegdheden door de Koning worden bepaald.

1° de veiller au respect du présent sous-titre lors de tout traitement de données à caractère personnel;

2° de conseiller toutes mesures utiles afin d'assurer la sécurité des données enregistrées;

3° d'informer et conseiller le responsable du traitement, et le cas échéant, le sous-traitant, le dirigeant et le personnel du service concerné procédant au traitement sur les obligations qui leur incombent en vertu du présent sous-titre;

4° de fournir des avis ou des recommandations au responsable du traitement, et le cas échéant, au sous-traitant, et au dirigeant du service;

5° d'exécuter d'autres missions qui lui sont confiées par le responsable du traitement, le cas échéant le sous-traitant ou le dirigeant du service.

Le délégué à la protection des données est le point de contact avec le Comité permanent R pour l'application du présent sous-titre.

§ 4. Le responsable du traitement et, le cas échéant le sous-traitant, veille à ce que son délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Le responsable du traitement et, le cas échéant le sous-traitant veille à ce que son délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

§ 5. Le cas échéant, les modalités de fonctionnement, de désignation ainsi que les compétences requises peuvent être définies par le Roi.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van persoonsgegevens aan de publieke sector en de private sector

Art. 92

In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen een inlichtingen- en veiligheidsdienst en enig openbaar of privé orgaan, in het belang van de uitvoering van de opdrachten van de inlichtingen- en veiligheidsdiensten.

Deze mededeling vindt plaats in overeenstemming met de artikelen 14, 16 en 19 van de wet van 30 november 1998.

Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 20, § 1, tweede lid, het volgende:

1° de identificatie van de inlichtingen- en veiligheidsdienst en het openbaar of particulier orgaan die de persoonsgegevens uitwisselen;

2° de identificatie van de verwerkingsverantwoordelijken;

3° de contactgegevens van de betrokken functionarissen voor gegevensbescherming;

4° de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5° de wettelijke grondslag;

6° de beperkingen van de rechten van de betrokkene.

Het protocol draagt de markering “BEPERKTE VERSPREIDING” in de zin van het koninklijk besluit van 24 maart 2004 tot uitvoering van de wet van

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données à caractère personnel avec le secteur public et le secteur privé

Art. 92

Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d’impact relative à la protection des données et l’avis résultant de la consultation de l’autorité de contrôle compétente ne peuvent pas être exigés comme préalable à la communication de données à caractère personnel entre un service de renseignement et de sécurité et tout organisme public ou privé dans l’intérêt de l’exercice des missions des services de renseignement et de sécurité.

Cette communication se déroule conformément aux articles 14, 16 et 19 de la loi du 30 novembre 1998.

Par dérogation à l’article 20, § 1er, alinéa 2, lorsque les parties décident de conclure un protocole, celui-ci porte notamment sur:

1° l’identification du service de renseignement et de sécurité et de l’organisme public ou privé qui échangent les données à caractère personnel;

2° l’identification des responsables du traitement;

3° les coordonnées des délégués à la protection des données concernés;

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° la base légale;

6° les restrictions aux droits de la personne concernée.

Le protocole porte le marquage “DIFFUSION RESTREINTE” au sens de l’arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998,

11 december 1998, voor zover een classifcatie in de zin van de wet van 11 december 1998 niet gerechtvaardigd is.

Afdeling 2

Doorgifte van persoonsgegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 93

Persoonsgegevens mogen slechts worden doorgegeven aan een land dat geen lid is van de Europese Unie of een internationale organisatie, indien dat land of die organisatie een passend beschermingsniveau en de naleving van de andere bepalingen van deze ondertitel waarborgt.

De vraag of het beschermingsniveau passend is, wordt beoordeeld met inachtneming van alle omstandigheden die betrekking hebben op de doorgifte van persoonsgegevens of op een categorie van doorgiften van persoonsgegevens. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen of organisaties worden nageleefd.

Het passende beschermingsniveau kan verzekerd worden door veiligheidsclausules tussen de verwerkingsverantwoordelijke en de ontvanger van de persoonsgegevens.

Art. 94

In afwijking van artikel 93 mag een doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie, hetwelke geen waarborgen biedt voor een passend beschermingsniveau, slechts plaatsvinden wanneer:

1° de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven voor de beoogde doorgifte; of

2° de doorgifte verplicht is in het kader van de internationale betrekkingen; of

3° de doorgifte noodzakelijk is ter vrijwaring van het vitaal belang van de personen; of

à moins qu'une classification au sens de la loi du 11 décembre 1998 ne se justifie.

Section 2

Transfert des données à caractère personnel vers des pays non membres de l'Union européenne ou à des organisations internationales

Art. 93

Le transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale ne peut avoir lieu que si le pays ou l'organisation en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions du présent sous-titre.

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données à caractère personnel ou à une catégorie de transferts de données à caractère personnel. Il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays ou l'organisation en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

Le niveau de protection adéquat peut être assuré par des clauses de sécurité entre le responsable du traitement et le destinataire des données à caractère personnel.

Art. 94

Par dérogation à l'article 93, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale n'assurant pas un niveau de protection adéquat, peut être effectué lorsque:

1° la personne concernée a indubitablement donné son consentement au transfert envisagé; ou

2° le transfert est obligatoire dans le cadre des relations internationales; ou

3° le transfert est nécessaire à la sauvegarde de l'intérêt vital des personnes; ou

4° de doorgifte noodzakelijk of wettelijk verplicht is ter vrijwaring van een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 95

In afwijking van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, is het Vast Comité I, in zijn hoedanigheid van onafhankelijke publieke autoriteit, aangeduid als gegevensbeschermingsautoriteit belast met de controle van de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten en hun verwerkers volgens de nadere regels vastgelegd in de wet van 18 juli 1991.

Hij waakt over de toepassing van deze ondertitel ter bescherming van de fundamentele rechten en vrijheden van de natuurlijke personen met betrekking tot deze verwerking.

Art. 96

Het Vast Comité I werkt, indien nodig, samen met de andere Belgische toezichthoudende autoriteiten, zonder dat dit afbreuk doet aan de fysieke integriteit van personen, of aan de opdrachten van de inlichtingen- en veiligheidsdiensten en de wet van 11 december 1998.

In het kader van de uitoefening van het toezicht bedoeld in artikel 95, deelt het Vast Comité I in algemene termen het resultaat hiervan mee aan de andere bevoegde toezichthoudende autoriteiten. Deze maken deze resultaten niet aan de betrokkene over.

Art. 97

De inlichtingen- en veiligheidsdiensten en hun verwerkers werken samen met het Vast Comité I.

Art. 98

Een toezichthoudende autoriteit informeert het Vast Comité I over inbreuken op de reglementering inzake de verwerking van persoonsgegevens van de inlichtingen- en veiligheidsdiensten zodra zij er kennis van neemt.

4° le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

CHAPITRE X

Autorité de contrôle

Art. 95

Par dérogation à la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, le Comité permanent R, en sa qualité d'autorité publique indépendante, est désigné comme autorité de protection des données chargée du contrôle du traitement des données à caractère personnel par les services de renseignement et de sécurité et par leurs sous-traitants selon les modalités fixées par la loi du 18 juillet 1991.

Il surveille l'application du présent sous-titre afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard dudit traitement.

Art. 96

Le Comité permanent R coopère, le cas échéant, avec les autres autorités de contrôle belges, sans que cela ne porte atteinte à l'intégrité physique d'une personne, ou aux missions des services de renseignement et de sécurité et de la loi du 11 décembre 1998.

Dans le cadre de l'exercice du contrôle visé à l'article 95, le Comité permanent R communique le résultat de celui-ci en termes généraux aux autres autorités de contrôle compétentes. Celles-ci ne transmettent pas ces résultats à la personne concernée.

Art. 97

Les services de renseignement et de sécurité et leurs sous-traitants coopèrent avec le Comité permanent R.

Art. 98

Lorsqu'elle en prend connaissance, une autorité de contrôle informe le Comité permanent R des violations de la règlementation relative aux traitements de données à caractère personnel des services de renseignement et de sécurité.

Elke toezichthoudende autoriteit overlegt met het Vast Comité I wanneer zij gevat wordt in een dossier dat mogelijk gevolgen heeft voor de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden

Art. 99

In afwijking van titel 4, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens van de inlichtingen- en veiligheidsdiensten en van hun personeel toegestaan door de betrokken inlichtingen- en veiligheidsdienst indien dit geen afbreuk doet aan zijn opdrachten, aan zijn verplichtingen bedoeld in de artikelen 13, derde lid, en 13/4, tweede lid van de wet van 30 november 1998, aan een lopend opsporings- of gerechtelijk onderzoek, of aan de betrekkingen die België met vreemde staten of internationale organisaties onderhoudt en overeenkomstig de wet van 11 december 1998.

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens van de inlichtingen- en veiligheidsdiensten en van hun personeel voor overige doelen dan die bedoeld in het eerste lid wordt geweigerd voor zover het doel legitiem is en de betrokken inlichtingen- en veiligheidsdienst meent dat de verwerking geen afbreuk kan doen aan de belangen bedoeld in het voorgaande lid.

Art. 100

Vóór hun raadpleging bedoeld in artikel 99 moeten de persoonsgegevens voorzien worden van de vermelding “Bescherming van persoonsgegevens – artikelen 99 tot 104 van de wet van xx/xx/2018”.

Art. 101

De persoonsgegevens bedoeld in artikel 99 worden voorafgaand aan hun raadpleging geanonimiseerd.

Indien een verdere verwerking van anonieme gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan de

Toute autorité de contrôle saisie d’un dossier susceptible d’avoir une répercussion sur le traitement de données à caractère personnel par les services de renseignement et de sécurité se concerte avec le Comité permanent R.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 99

Par dérogation au titre 4, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel des services de renseignement et de sécurité et de leur personnel par un responsable du traitement ultérieur est autorisée par le service de renseignement et de sécurité concerné si cela ne porte pas atteinte à ses missions, à ses obligations visées aux articles 13, alinéa 3 et 13/4, alinéa 2 de la loi du 30 novembre 1998, à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales et conformément à la loi du 11 décembre 1998.

Toute demande adressée aux Archives de l’État de traitement ultérieur de données à caractère personnel des services de renseignement et de sécurité et de leur personnel à d’autres fins que celles visées à l’alinéa premier est refusée à moins que la finalité soit légitime et que le service de renseignement et de sécurité concerné estime que le traitement n’est pas susceptible de porter atteinte aux intérêts visés à l’alinéa précédent.

Art. 100

Avant leur consultation visée à l’article 99, les données à caractère personnel doivent être marquées de la mention “Protection des données à caractère personnel – articles 99 à 104 de la loi du xx/xx/2018”.

Art. 101

Les données à caractère personnel visées à l’article 99 sont rendues anonymes préalablement à leur consultation.

Si un traitement ultérieur de données anonymes ne permet pas d’atteindre les fins historiques, scientifiques ou statistiques, le service de renseignement et

inlichtingen- en veiligheidsdienst de raadpleging van gepseudonimiseerde gegevens toestaan.

Indien de anonimisering of pseudonimisering de identificatie van de gegevens niet onmogelijk maakt, weigert de inlichtingen- en veiligheidsdienst de raadpleging indien dit een onevenredige afbreuk doet aan het privéleven.

Indien een verdere verwerking van gepseudonimiseerde gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan de inlichtingen- en veiligheidsdienst de raadpleging van niet-gepseudonimiseerde gegevens toestaan indien dit geen onevenredige afbreuk doet aan het privéleven.

Art. 102

In afwijking van titel 4, is een mededeling of publicatie van niet-geanonimiseerde of niet-gepseudonimiseerde persoonsgegevens bedoeld in artikel 99, geraadpleegd door de verdere verwerkingsverantwoordelijke, enkel mogelijk met het akkoord van de betrokken inlichtingen- en veiligheidsdienst en onder de voorwaarden die hij vastlegt.

Art. 103

De verdere verwerkingsverantwoordelijke van persoonsgegevens bedoeld in artikel 99 houdt een logbestand van zijn verdere verwerkingsactiviteiten voor historische, wetenschappelijke of statistische doeleinden bij.

Dit logbestand is geclassificeerd in de zin van de wet van 11 december 1998 indien de verwerking betrekking heeft op geclassificeerde gegevens.

Dit logbestand bevat de volgende informatie:

1° de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming van deze laatste;

2° de doeleinden van de verdere verwerking;

3° de gegevens die het voorwerp uitmaken van de verdere verwerking;

4° de eventuele voorwaarden voor de verdere verwerking vastgelegd door de betrokken inlichtingen- en veiligheidsdienst;

de sécurité peut autoriser la consultation de données pseudonymisées.

Si l'anonymisation ou la pseudonymisation ne rend pas l'identification des données impossible, le service de renseignement et de sécurité refuse la consultation si cela constitue une atteinte disproportionnée à la vie privée.

Si un traitement ultérieur de données pseudonymisées ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, le service de renseignement et de sécurité peut autoriser la consultation de données non pseudonymisées si cela ne constitue pas une atteinte disproportionnée à la vie privée.

Art. 102

Par dérogation au titre 4, une communication ou publication des données à caractère personnel visées à l'article 99 non anonymisées ou non pseudonymisées, consultées par le responsable du traitement ultérieur n'est possible qu'avec l'accord du service de renseignement et de sécurité concerné et sous les conditions que celui-ci aura fixées.

Art. 103

Le responsable du traitement ultérieur des données à caractère personnel visées à l'article 99 tient un journal de ses activités de traitement ultérieur à des fins historiques, scientifiques ou statistiques.

Ce journal est classifié au sens de la loi du 11 décembre 1998 si le traitement porte sur des données classifiées.

Ce journal comporte les informations suivantes:

1° les coordonnées du responsable du traitement initial, du responsable du traitement ultérieur et du délégué à la protection des données de ce dernier;

2° les finalités du traitement ultérieur;

3° les données faisant l'objet du traitement ultérieur;

4° les éventuelles conditions du traitement ultérieur fixées par le service de renseignement et de sécurité concerné;

5° de eventuele ontvangers toegestaan door de betrokken inlichtingen- en veiligheidsdienst.

Art. 104

Elke overheidsinstantie of elke natuurlijke of rechtspersoon die persoonsgegevens bedoeld in artikel 99 verwerkt om historische, wetenschappelijke of statistische doeleinden is de verantwoordelijke van deze verwerking.

Hij mag geen handelingen verrichten die zijn gericht op de omzetting van anonieme of gepseudonimiseerde gegevens in persoonsgegevens.

ONDERTITEL 2

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de Krijgsmacht

Art. 105

Bij de aanwending van de krijgsmacht, en de paraatstelling met het oog op de aanwending van de krijgsmacht, zoals bedoeld in artikel 3 van de wet van 20 mei 1994 betreffende de perioden en de standen van de militairen van het reservekader alsook betreffende de aanwending en paraatstelling van de krijgsmacht met het oog op de vervulling van de haar opgedragen grondwettelijke taken, is het volgende regime van toepassing:

1° de krijgsmacht verwerkt, voor zover noodzakelijk voor de uitoefening van hun opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of de seksuele gerichtheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen;

2° de persoonsgegevens mogen slechts verwerkt worden wanneer de verwerking nuttig is voor de aanwending of de paraatstelling met het oog op de aanwending van de krijgsmacht en worden niet op een met die doeleinden onverenigbare wijze verwerkt;

3° de persoonsgegevens moeten rechtmatig en eerlijk worden verwerkt;

5° les éventuels destinataires autorisés par le service de renseignement et de sécurité concerné.

Art. 104

Toute autorité publique ou toute personne physique ou morale qui traite des données à caractère personnel visées à l'article 99 à des fins historiques, scientifiques ou statistiques est responsable dudit traitement.

Elle n'entreprendra aucune action pour convertir des données anonymes ou pseudonymisées en données à caractère personnel.

SOUS-TITRE 2

La protection des personnes physiques concernant le traitement des données à caractère personnel par les Forces armées

Art. 105

Lors de la mise en œuvre des forces armées et de la mise en condition en vue de la mise en œuvre des forces armées visé à l'article 3 de la loi du 20 mai 1994 relative aux périodes et aux positions des militaires du cadre de réserve, ainsi qu'à la mise en œuvre et à la mise en condition des forces armées dans l'optique de l'exécution de ses tâches constitutionnelles, le régime suivant est d'application:

1° les forces armées traitent, pour autant que cela soit nécessaire dans l'exercice de leurs missions, des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes;

2° les données à caractère personnel ne peuvent être traitées que lorsque le traitement est utile pour la mise en œuvre des forces armées ou la mise en condition des forces armées et ne sont pas traitées d'une manière incompatible avec ces finalités;

3° les données à caractère personnel doivent être traitées de manière licite et loyale;

4° de persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt;

5° de persoonsgegevens dienen toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

6° de persoonsgegevens dienen nauwkeurig te zijn en, zo nodig, te worden bijgewerkt. Alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, te wissen of te verbeteren;

7° de persoonsgegevens mogen doorgegeven worden aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie indien die doorgifte noodzakelijk is voor operationele redenen;

8° met uitzondering van de definities vervat in artikel 26, 1° tot 6°, 8° tot 14°, 16° en 17°, en van de artikelen 2, 78 en 83 tot 89 zijn de bepalingen van de andere titels niet van toepassing;

9° met betrekking tot de verwerking van persoonsgegevens worden de volgende rechten slechts beperkt indien dit een noodzakelijke en evenredige maatregel vormt binnen de beperkingen van het toepasselijk internationaal recht voor de aanwending van de krijgsmacht of paraatstelling met het oog op aanwending van de krijgsmacht:

a) het recht kennis te nemen van het bestaan van een geautomatiseerd bestand van persoonsgegevens, de voornaamste doeleinden hiervan, alsmede de identiteit en de gewone verblijfplaats of de hoofdvestiging van de houder van het bestand;

b) het recht om, indien nodig, die gegevens te doen verbeteren of uitwissen, indien deze zijn verwerkt in strijd met de wet;

c) het recht over een rechtsmiddel te beschikken, indien geen gevolg wordt gegeven aan een verzoek om bevestiging of, desgevallend, mededeling, verbetering of uitwisseling van persoonsgegevens.

10° in de mate dat de aanwending en de paraatstelling van de Krijgsmacht niet in het gedrang worden

4° les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une période n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées;

5° les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement;

6° les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;

7° les données à caractère personnel peuvent être transmises vers un pays non membre de l'Union Européenne ou vers une organisation internationale dans le cas où ce transfert est nécessaire pour des raisons opérationnelles;

8° à l'exception des définitions prevues dans l'article 26, 1° à 6°, 8° à 14°, 16° et 17°, et des articles 2, 78 et 83 à 89, les dispositions des autres titres ne sont pas d'application;

9° concernant le traitement des données à caractère personnel, les droits suivants sont seulement limités lorsqu'il s'agit d'une mesure nécessaire et proportionnelle dans le cadre des limitations du droit international applicable, pour la mise en œuvre des forces armées, ou la mise en condition des forces armées en vue de leur mise en œuvre:

a) le droit de prendre connaissance de l'existence d'un fichier de données automatisé à caractère personnel, de ses principaux objectifs ainsi que de l'identité et de la résidence habituelle ou de l'établissement principal du titulaire du fichier;

b) le droit de faire corriger ou d'effacer ces données si nécessaire, si celles-ci ont été traitées en violation de la loi;

c) le droit de disposer de voies de recours en l'absence de réponse à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'échange de données à caractère personnel.

10° dans la mesure où la mise en œuvre et la mise en condition des forces armées n'est pas mise en péril,

gebracht, zijn de verwerkingen van persoonsgegevens onderworpen aan het toezicht van de bevoegde toezichthoudende autoriteit.

ONDERTITEL 3

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens in het kader van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen

HOOFDSTUK I

Definities

Art. 106

§ 1. De definities bedoeld in artikel 26, 1° tot 6°, 9° tot 14° en 16° tot 17° zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder:

1° "de Verordening": Verordening (EU) 2016/679 van Het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;

2° "de wet van 11 december 1998": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

3° "de wet van 11 december 1998 tot oprichting van een beroepsorgaan": de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

4° "beroepsorgaan": het beroepsorgaan bedoeld in artikel 3 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan;

5° "de verwerkingsverantwoordelijke": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

6° "toezichthoudende autoriteit": de onafhankelijke overheidsinstantie die bij de wet belast is met het toezicht op de toepassing van deze ondertitel.

les traitements des données à caractère personnel sont soumis à l'autorité de contrôle compétente.

SOUS-TITRE 3

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité

CHAPITRE I^ER

Définitions

Art. 106

§ 1er. Les définitions visées à l'article 26, 1° à 6°, 9° à 14° et 16° à 17° sont applicables au présent sous-titre.

§ 2. Pour l'application du présent sous-titre, on entend par:

1° "le Règlement": le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

2° "la loi du 11 décembre 1998": la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

3° "la loi du 11 décembre 1998 portant création d'un organe de recours": la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité;

4° "l'organe de recours": l'organe de recours visé à l'article 3 de la loi du 11 décembre 1998 portant création d'un organe de recours;

5° "le responsable du traitement": la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles;

6° "autorité de contrôle": l'autorité publique indépendante chargée par la loi de surveiller l'application du présent sous-titre.

7° “het Vast Comité I”: het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 18 juli 1991 verantwoordelijk voor het toezicht op de toepassing van deze ondertitel overeenkomstig artikel 95.

HOOFDSTUK II

Toepassingsgebied

Art. 107

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens in het kader van veiligheidsmachtigingen, attesten en adviezen bedoeld in de wet van 11 december 1998 door:

1° de veiligheidsoverheid bedoeld in artikel 15, eerste lid, van de wet van 11 december 1998;

2° elk overheidslid van de overheid bedoeld in 1°;

3° de overheden bedoeld in artikelen 15, tweede lid en 22*ter* van de wet van 11 december 1998;

4° de veiligheidsofficieren bedoeld in artikel 13, 1°, van de wet van 11 december 1998;

5° de verwerkers van overheden en personen bedoeld in 1° tot 4°.

Deze ondertitel is ook van toepassing op elke verwerking van persoonsgegevens door het beroepsorgaan in het kader van de beroepsprocedures bedoeld in de wet van 11 december 1998 tot oprichting van het beroepsorgaan.

Met uitzondering van deze ondertitel en artikelen 226 en 227, zijn de titels 1 tot 7 van deze wet niet van toepassing op de verwerkingen bedoeld in het eerste en tweede lid.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 108

Persoonsgegevens mogen slechts verwerkt worden in één van de volgende gevallen:

1° wanneer de betrokkene daarvoor ondubbelzinnig zijn toestemming verleend heeft;

7° “Comité permanent R”: le Comité permanent de contrôle des services de renseignement visé dans la loi du 18 juillet 1991 chargé du contrôle de l’application du présent sous-titre en application de l’article 95.

CHAPITRE II

Champ d’application

Art. 107

Le présent sous-titre s’applique à tout traitement de données à caractère personnel dans le cadre des habilitations de sécurité, attestations et avis de sécurité visés dans la loi du 11 décembre 1998 par:

1° l’autorité de sécurité visée à l’article 15, alinéa premier, de la loi du 11 décembre 1998;

2° chaque autorité membre de l’autorité visée au 1°;

3° les autorités visées aux articles 15, alinéa 2, et 22*ter* de la loi du 11 décembre 1998;

4° les officiers de sécurité visés à l’article 13, 1°, de la loi du 11 décembre 1998 ;

5° les sous-traitants des autorités et personnes visées aux 1° à 4°.

Le présent sous-titre s’applique également à chaque traitement de données à caractère personnel par l’organe de recours dans le cadre des recours visés dans la loi du 11 décembre 1998 portant création d’un organe de recours.

À l’exception du présent sous-titre, et des articles 226 et 227, les titres 1 à 7 de la présente loi ne s’appliquent pas aux traitements visés aux alinéas premier et 2.

CHAPITRE III

Conditions générales du traitement

Art. 108

Le traitement de données à caractère personnel ne peut être effectué que dans l’un des cas suivants:

1° lorsque la personne concernée a indubitablement donné son consentement;

2° wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;

3° wanneer de verwerking noodzakelijk is om een verplichting na te komen waaraan de verwerkingsverantwoordelijke is onderworpen door of krachtens een wet;

4° wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verwerkingsverantwoordelijke of aan de derde aan wie de persoonsgegevens worden verstrekt.

Art. 109

Persoonsgegevens moeten:

1° worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig en behoorlijk is;

2° voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen en niet verder worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden. Onder de voorwaarden vastgesteld door de artikelen 132 tot 137 wordt een verdere verwerking van de gegevens voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd;

3° toereikend, ter zake dienend en niet overmatig zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4° nauwkeurig te zijn en, zo nodig, te worden bijgewerkt. Alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, te wissen of te verbeteren.

HOOFDSTUK IV

Aard van de persoonsgegevens

Art. 110

De overheden, organen en de personen bedoeld in artikel 107 verwerken, in het belang van de uitoefening

2° lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

3° lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi;

4° lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou une autorité publique à laquelle les données à caractère personnel sont communiquées.

Art. 109

Les données à caractère personnel doivent être:

1° traitées d'une manière qui est loyal et légitime à l'égard de la personne concernée;

2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et réglementaires applicables. Un traitement ultérieur à des fins historiques, scientifiques ou statistiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par les articles 132 à 137;

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement;

4° exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

CHAPITRE IV

Nature des données à caractère personnel

Art. 110

Dans l'intérêt de l'exercice de leurs missions, les autorités, les organes et les personnes visés à

van hun opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook genetische en biometrische gegevens, gezondheidsgegevens, gegevens die het seksuele gedrag of de seksuele gerichtheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 111

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de modaliteiten bepaald in artikel 25 van de wet van 11 december 1998.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 112

Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.

Art. 113

De betrokkene heeft het recht te vragen overeenkomstig artikel 114:

1° om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen;

2° om de verificatie bij de bevoegde toezichthoudende autoriteit van de naleving van de bepalingen van deze ondertitel.

Art. 114

§ 1. Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van de verwerking te waarborgen, is de toegang van de betrokkene tot zijn persoonsgegevens

l'article 107 traitent des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

CHAPITRE V

Conservation des données à caractère personnel

Art. 111

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées à l'article 25 de la loi du 11 décembre 1998.

CHAPITRE VI

Droits de la personne concernée

Art. 112

Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 113

La personne concernée a le droit de demander conformément à l'article 114:

1° la rectification ou la suppression de ses données à caractère personnel inexactes;

2° la vérification auprès de l'autorité de contrôle compétente du respect des dispositions du présent sous- titre.

Art. 114

§ 1er. Afin de garantir la confidentialité et l'efficacité de l'exécution des traitements, l'accès de la personne concernée à ses données à caractère personnel

die worden verwerkt door de overheden, organen en personen bedoeld in artikel 107, eerste lid, beperkt tot de informatie die de betrokkene hen aanlevert.

De rechten bedoeld in artikel 113, 1° en 2°, ten aanzien van de verwerkingen bedoeld in artikel 107, eerste lid, worden kosteloos uitgeoefend via het Vast Comite I op initiatief van de betrokkene, die zijn identiteit bewijst. Het Comité I voert de verificaties uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht.

§ 2. De toegang van de betrokkene tot zijn persoonsgegevens verwerkt door het beroepsorgaan verloopt overeenkomstig het artikel 6 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan.

Voor de uitoefening van zijn rechten bedoeld in artikel 113, 1°, en ten aanzien van de verwerkingen bedoeld in artikel 107, tweede lid, richt de betrokkene zich tot het beroepsorgaan overeenkomstig de modaliteiten bepaald door of krachtens de wet van 11 december 1998 tot oprichting van een beroepsorgaan.

Art. 115

Een besluit waaraan voor een persoon negatieve rechtsgevolgen verbonden zijn, mag niet louter worden genomen op grond van een geautomatiseerde persoonsgegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.

Het in het eerste lid vastgestelde verbod geldt niet indien het besluit zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet of wanneer het noodzakelijk is vanwege een zwaarwegend algemeen belang.

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 116

De verwerkingsverantwoordelijke moet:

1° er nauwlettend over waken dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en

traitées par les autorités, organes et personnes visées à l'article 107, alinéa premier, est limité à l'information que la personne concernée leur fournit.

Les droits visés à l'article 113, 1° et 2°, à l'égard des traitements visés à l'article 107, alinéa premier, s'exercent, sans frais, par l'intermédiaire du Comité permanent R, à l'initiative de la personne concernée justifiant de son identité. Le Comité R effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

§ 2. L'accès par la personne concernée à ses données à caractère personnel traitées par l'organe de recours s'effectue conformément à l'article 6 de la loi du 11 décembre 1998 portant création d'un organe de recours.

Pour l'exercice de ses droits visés à l'article 113, 1°, à l'égard des traitements visés à l'article 107, alinéa 2, la personne concernée s'adresse à l'organe de recours conformément aux modalités fixées par ou en vertu de la loi du 11 décembre 1998 portant création d'un organe de recours.

Art. 115

Une décision produisant des effets juridiques négatifs à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

L'interdiction prévue à l'alinéa premier ne s'applique pas lorsque la décision est fondée sur une disposition prévue par ou en vertu d'une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important.

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 116

Le responsable du traitement doit:

1° faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer

niet ter zake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2° ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst;

3° alle personen die onder zijn gezag handelen, informeren over de bepalingen van deze ondertitel en over alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer betreffende de verwerking van persoonsgegevens.

Art. 117

Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verwerkingsverantwoordelijke:

1° een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de verwerkingen;

2° toezien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen;

3° de verantwoordelijkheid van de verwerker vaststellen in de overeenkomst;

4° met de verwerker overeenkomen dat de verwerker slechts handelt in opdracht van de verwerkingsverantwoordelijke en dat de verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke in toepassing van deze ondertitel is gehouden.

Art. 118

De verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke is gehouden.

Hij mag de verwerking van persoonsgegevens niet toevertrouwen aan een andere verwerker, behoudens uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2° veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins du service;

3° informer les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 117

Lorsque le traitement est confié à un sous-traitant, le responsable du traitement doit:

1° choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements;

2° veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles;

3° fixer dans le contrat la responsabilité du sous-traitant;

4° convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et qu'il est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du présent sous-titre.

Art. 118

Le sous-traitant est soumis aux mêmes obligations que celles qui incombent au responsable du traitement.

Il ne peut pas confier le traitement de données à caractère personnel à un autre sous-traitant, sauf autorisation expresse du responsable du traitement.

Art. 119

Eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verwerkingsverantwoordelijke verwerken, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 120

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken.

Een overeenkomst bepaalt de respectievelijke verplichtingen van de gezamenlijke verwerkingsverantwoordelijken, met name met betrekking tot de uitoefening van de rechten van de betrokkene en de mededeling van persoonsgegevens, tenzij hun respectievelijke verplichtingen worden bepaald door of krachtens een wet.

In de overeenkomst wordt één contactpunt voor betrokkenen aangewezen. De gezamenlijke verwerkingsverantwoordelijken nemen dit contactpunt op in het register bedoeld in artikel 123.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 121

Om de veiligheid van de persoonsgegevens te waarborgen, treffen de verwerkingsverantwoordelijke, alsmede de verwerker, de passende technische en organisatorische maatregelen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen verzekeren een passend beveiligingsniveau, rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen persoonsgegevens en de potentiële risico's.

Art. 119

Toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 120

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Un accord définit les obligations respectives des responsables conjoints du traitement, notamment en ce qui concerne l'exercice des droits de la personne concernée et la communication des données à caractère personnel, sauf si leurs obligations respectives sont définies par ou en vertu d'une loi.

Un seul point de contact pour les personnes concernées est désigné dans l'accord. Les responsables conjoints du traitement incluent ce point de contact dans le registre visé à l'article 123.

Section 3

Sécurité des données à caractère personnel

Art. 121

Le responsable du traitement ainsi que le sous-traitant prennent les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures assurent un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels.

Art. 122

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk binnen de kortste termijn aan het Vast Comité I, en indien mogelijk dit ten laatste 72 uur na er kennis van te hebben genomen.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke binnen de kortste termijn van elke inbreuk op de beveiliging.

§ 3. In de in paragraaf 1 en 2 bedoelde melding wordt, op zijn minst, het volgende omschreven of meegedeeld:

1° de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en de opgeslagen persoonsgegevens in kwestie;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt bij wie bijkomende informatie kan worden verkregen;

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de verwerkingsverantwoordelijke, of de verwerker heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder desgevallend maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Afdeling 4

Registers

Art. 123

§ 1. De verwerkingsverantwoordelijke, en desgevallend zijn verwerker, houdt een register bij van de verwerkingsactiviteiten van persoonsgegevens.

Dit register bevat, desgevallend en indien mogelijk, de volgende gegevens voor wat betreft de verwerkingen:

1° de contactgegevens van de verwerkingsverantwoordelijke en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

2° de verwerkingsdoeleinden;

Art. 122

§ 1er. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie au Comité permanent R dans les meilleurs délais et, si possible, au plus tard 72 heures après en avoir pris connaissance.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais.

§ 3. La notification visée aux paragraphes premier et 2 doit, à tout le moins, décrire ou communiquer:

1° la nature de la brèche de sécurité y compris et, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° les conséquences probables de la brèche de sécurité;

4° les mesures prises ou que le responsable du traitement ou le sous-traitant propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Section 4

Registres

Art. 123

§ 1er. Le responsable du traitement, et le cas échéant son sous-traitant, tient un registre d'activités de traitement des données à caractère personnel.

Ce registre comporte, le cas échéant et si possible, les informations suivantes en ce qui concerne les traitements:

1° les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

2° les finalités du traitement;

3° de categorieën van betrokkenen;

4° de categorieën van persoonsgegevens;

5° de categorieën van voornaamste ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

6° de doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, desgevallend, de documenten die getuigen van het bestaan van passende waarborgen;

7° de beoogde termijnen voor het verwijderen van de persoonsgegevens;

8° het gebruik van profilering;

9° de rechtsgrondslag;

10° een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 121.

§ 2. De in de eerste paragraaf bedoelde registers worden in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 3. De verwerkingsverantwoordelijke stelt het register ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

De verwerker stelt het register ter beschikking van de verwerkingsverantwoordelijke en stelt het eveneens ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 124

§ 1. De verwerkingsverantwoordelijke, en desgevallend de verwerker, wijzen een functionaris voor gegevensbescherming aan. Deze beslissing wordt meegedeeld aan de bevoegde toezichthoudende autoriteit.

De functionaris voor gegevensbescherming is titularis van een veiligheidsmachtiging “zeer geheim”, in de zin van de wet van 11 december 1998.

§ 2. De functionaris voor gegevensbescherming kan niet gestraft worden voor het uitoefenen van zijn

3° les catégories des personnes concernées;

4° les catégories des données à caractère personnel;

5° les catégories de destinataires principaux auxquels des données à caractère personnel peuvent être communiquées;

6° les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris le mention de ce pays tiers ou de cette organisation internationale et, le cas échéant, les documents attestant de l’existence de garanties appropriées;

7° les délais prévus pour l’effacement des données à caractère personnel;

8° le recours au profilage;

9° la base juridique;

10° une description générale des mesures de sécurité techniques et organisationnelles visées à l’article 121.

§ 2. Le registre visé au paragraphe premier se présente sous une forme écrite y compris la forme électronique.

§ 3. Le responsable du traitement met le registre à la disposition de l’autorité de contrôle compétente à sa demande.

Le sous-traitant met le registre à la disposition du responsable du traitement ainsi qu’à la disposition de l’autorité de contrôle compétente à sa demande.

Section 5

Délégué à la protection des données

Art. 124

§ 1er. Le responsable du traitement et, le cas échéant, le sous-traitant désignent un délégué à la protection des données. Cette décision est communiquée à l’autorité de contrôle compétente.

Le délégué à la protection des données est titulaire d’une habilitation de sécurité de niveau très secret, au sens de la loi du 11 décembre 1998.

§ 2. Le délégué à la protection des données ne peut pas être sanctionné en raison de l’exercice de ses

functie. Hij kan evenmin van zijn functie ontheven worden omwille van de uitvoering van zijn opdrachten, behalve indien hij een zware fout heeft begaan of de voorwaarden noodzakelijk voor het uitoefenen van zijn functie niet langer vervult.

De functionaris voor gegevensbescherming kan zich tot het Vast Comité I wenden om deze beslissing aan te vechten.

§ 3. Hij is, op een onafhankelijke wijze, belast met:

1° het toezien op de naleving van deze ondertitel voor elke verwerking van persoonsgegevens;

2° het adviseren over alle nuttige maatregelen met het oog op het verzekeren van de beveiliging van de opgeslagen persoonsgegevens;

3° het informeren en adviseren van de verwerkingsverantwoordelijke, en desgevallend de verwerker, en hun personeelsleden die de verwerking verrichten over hun verplichtingen op grond van de huidige ondertitel;

4° het verstrekken van adviezen of aanbevelingen aan de verwerkingsverantwoordelijke, en desgevallend, aan de verwerker;

5° het uitvoeren van andere opdrachten die hem door de verwerkingsverantwoordelijke, en desgevallend de verwerker, toevertrouwd worden.

De functionaris voor gegevensbescherming is de contactpersoon voor de bevoegde toezichthoudende autoriteit met betrekking tot de toepassing van deze ondertitel.

§ 4. De verwerkingsverantwoordelijke, en desgevallend de verwerker, ziet erop toe dat hun functionaris voor gegevensbescherming tijdig en naar behoren wordt betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden.

De verwerkingsverantwoordelijke, en desgevallend de verwerker, ziet erop toe dat de functionaris voor gegevensbescherming de benodigde middelen ter beschikking heeft voor het vervullen van zijn taken.

De functionaris voor gegevensbescherming kan worden bijgestaan door één of meerdere medewerkers.

§ 5. Desgevallend kunnen nadere regels voor de werking, de aanwijzing en de vereiste bevoegdheden door de Koning worden bepaald.

fonctions. Il ne peut pas non plus être relevé de ses fonctions en raison de l'exercice de ses missions, sauf s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions.

Le délégué à la protection des données peut s'adresser au Comité permanent R pour contester cette décision.

§ 3. Il est chargé de manière indépendante:

1° de veiller au respect du présent sous-titre lors de tout traitement de données à caractère personnel;

2° de conseiller toutes mesures utiles afin d'assurer la sécurité des données enregistrées;

3° d'informer et de conseiller le responsable du traitement, et le cas échéant le sous-traitant, et leur personnel procédant au traitement des obligations qui leur incombent en vertu du présent sous-titre;

4° de fournir des avis ou des recommandations au responsable du traitement, et le cas échéant, au sous-traitant;

5° d'exécuter d'autres missions qui lui sont confiées par le responsable du traitement, et le cas échéant le sous-traitant.

Le délégué à la protection des données est le point de contact avec l'autorité de contrôle compétente pour l'application du présent sous-titre.

§ 4. Le responsable du traitement et, le cas échéant le sous-traitant, veille à ce que son délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Le responsable du traitement et, le cas échéant le sous-traitant, veille à ce que son délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

§ 5. Le cas échéant, les modalités de fonctionnement, de désignation ainsi que les compétences requises peuvent être définies par le Roi.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van persoonsgegevens aan de publieke sector en de private sector

Art. 125

§ 1. In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen de overheden, of personen bedoeld in artikel 107 en enig openbaar of privé orgaan.

Deze mededeling vindt plaats in overeenstemming met de wet van 11 december 1998.

§ 2. Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 20, § 1, tweede lid, het volgende:

1° de identificatie van de federale overheidsinstantie of het federaal openbaar orgaan die de persoonsgegevens doorgeeft;

2° de identificatie van de verwerkingsverantwoordelijke;

3° de contactgegevens van de betrokken functionarissen voor gegevensbescherming;

4° de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5° de wettelijke grondslag;

6° de modaliteiten inzake gehanteerde communicatie;

7° de beperkingen van de rechten van de betrokkene;

8° de periodiciteit van de doorgifte;

9° de duur van het protocol.

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données à caractère personnel avec le secteur public et le secteur privé

Art. 125

§ 1er. Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact relative à la protection des données et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme préalable à la communication de données à caractère personnel entre les autorités, les organes ou les personnes visés à l'article 107 et tout organisme public ou privé.

Cette communication se déroule conformément à la loi du 11 décembre 1998.

§ 2. Par dérogation à l'article 20, § 1er, alinéa 2, de la présente loi, lorsque les parties décident de conclure un protocole, celui-ci porte notamment sur:

1° l'identification du service public fédéral ou de l'organisme public fédéral qui transfère les données à caractère personnel;

2° l'identification des responsables du traitement;

3° les coordonnées des délégués à la protection des données concernés;

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° la base légale;

6° les modalités de communication utilisées;

7° les restrictions aux droits de la personne concernée;

8° la périodicité du transfert;

9° la durée du protocole.

Afdeling 2

Doorgifte van persoonsgegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 126

Persoonsgegevens mogen slechts worden doorgegeven aan een land dat geen lid is van de Europese Unie of een internationale organisatie, indien dat land of die organisatie een passend beschermingsniveau en de naleving van de andere bepalingen van deze ondertitel waarborgt.

De vraag of het beschermingsniveau passend is, wordt beoordeeld met inachtneming van alle omstandigheden die betrekking hebben op de doorgifte van persoonsgegevens of op een categorie van doorgifte van persoonsgegevens. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen of organisaties worden nageleefd.

Het passende beschermingsniveau kan verzekerd worden door veiligheidsclausules tussen de verwerkingsverantwoordelijke en de ontvanger van de persoonsgegevens.

Art. 127

In afwijking van artikel 126 mag een doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie, dewelke geen waarborgen biedt voor een passend beschermingsniveau, slechts plaatsvinden wanneer:

1° de betrokkene zijn ondubbelzinnige toestemming heeft gegeven voor de beoogde doorgifte; of

2° de doorgifte verplicht is in het kader van de internationale betrekkingen; of

3° de doorgifte noodzakelijk is ter vrijwaring van het vitaal belang van de personen; of

4° de doorgifte noodzakelijk of wettelijk verplicht is voor de vrijwaring van een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

Section 2

Transfert des données à caractère personnel vers des pays non membres de l'Union européenne ou à des organisations internationales

Art. 126

Le transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale ne peut avoir lieu que si le pays ou l'organisation en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions du présent sous-titre.

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données à caractère personnel ou à une catégorie de transferts de données à caractère personnel. Il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays ou l'organisation en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

Le niveau de protection adéquat peut être assuré par des clauses de sécurité entre le responsable du traitement et le destinataire des données à caractère personnel.

Art. 127

Par dérogation à l'article 126, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale n'assurant pas un niveau de protection adéquat, peut être effectué lorsque:

1° la personne concernée a indubitablement donné son consentement au transfert envisagé; ou

2° le transfert est obligatoire dans le cadre des relations internationales; ou

3° le transfert est nécessaire à la sauvegarde de l'intérêt vital des personnes; ou

4° le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 128

§ 1. In afwijking van het bepaalde in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, is het Vast Comité I, in zijn hoedanigheid van onafhankelijke publieke autoriteit, aangeduid als toezichthoudende autoriteit belast met de het toezicht op de verwerking van persoonsgegevens uitgevoerd in het kader van artikel 107, eerste lid, door de overheden en personen bedoeld in hetzelfde lid.

Hij waakt over de toepassing van deze ondertitel ter bescherming van de fundamentele rechten en vrijheden van de natuurlijke personen met betrekking tot deze verwerking.

§ 2. In zijn hoedanigheid van rechterlijke overheid is het beroepsorgaan niet onderworpen aan de controle door een toezichthoudende autoriteit voor de bescherming van persoonsgegevens.

Art. 129

Het Vast Comité I werkt, inzake de wet van 11 december 1998, indien nodig, samen met de andere Belgische toezichthoudende autoriteiten, zonder dat dit afbreuk doet aan de belangen bedoeld in artikel 5 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan.

In het kader van de uitoefening van het toezicht bedoeld in artikel 128, deelt het Vast Comité I in algemene termen het resultaat hiervan mee aan de andere bevoegde toezichthoudende autoriteiten.

Art. 130

De overheden en personen bedoeld in artikel 107, eerste lid, werken samen met het Vast Comité I.

Art. 131

Een toezichthoudende autoriteit informeert het Vast Comité I over inbreuken op de reglementering inzake de verwerking van persoonsgegevens in het kader van artikel 107 zodra zij er kennis van neemt.

Elke toezichthoudende autoriteit overlegt met het Vast Comité I wanneer zij gevat wordt in een dossier

CHAPITRE X

Autorité de contrôle

Art. 128

§ 1er. Par dérogation à la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, le Comité permanent R, en sa qualité d'autorité publique indépendante, est désigné comme autorité du contrôle chargée du contrôle du traitement des données à caractère personnel effectué dans le cadre de l'article 107, alinéa premier, par les autorités et personnes visées au même alinéa.

Il surveille l'application du présent sous-titre afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard dudit traitement.

§ 2. En sa qualité d'autorité juridictionnelle, l'organe de recours n'est pas soumis au contrôle d'une autorité de protection des données à caractère personnel.

Art. 129

Dans le respect de la loi du 11 décembre 1998 le Comité permanent R coopère, le cas échéant, avec les autres autorités de contrôle belges, sans que cela ne porte atteinte aux intérêts visés à l'article 5 de la loi du 11 décembre 1998 portant création d'un organe de recours.

Dans le cadre de l'exercice du contrôle visé à l'article 128, le Comité permanent R communique le résultat de celui-ci en termes généraux aux autres autorités de contrôle compétentes.

Art. 130

Les autorités et personnes visées à l'article 107, alinéa premier, coopèrent avec le Comité permanent R.

Art. 131

Lorsqu'elle en prend connaissance, une autorité de contrôle informe le Comité permanent R des violations de la règlementation relative aux traitements de données à caractère personnel dans le cadre de l'article 107.

Toute autorité de contrôle saisie d'un dossier susceptible d'avoir une répercussion sur le traitement

dat mogelijk gevolgen heeft voor de verwerking van persoonsgegevens in het kader van artikel 107.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden

Art. 132

In afwijking van titel 4, is de raadpleging voor historische, wetenschappelijke of statistische doeleinden van persoonsgegevens van de overheden, het beroepsorgaan of de personen bedoeld in artikel 107 en hun personeel door een verdere verwerkingsverantwoordelijke toegestaan indien dit geen afbreuk doet aan de belangen bedoeld in artikel 12, eerste lid, van de wet van 11 december 1998.

Art. 133

Vóór de raadpleging bedoeld in artikel 132 moeten de persoonsgegevens voorzien worden van de vermelding “Bescherming van persoonsgegevens – artikelen 132 tot 137 van de wet van xx/xx/2018”.

Art. 134

De persoonsgegevens bedoeld in artikel 132 worden voorafgaand aan hun raadpleging geanonimiseerd.

Indien een verdere verwerking van anonieme gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan de verwerkingsverantwoordelijke in het kader van artikel 107 de raadpleging van gepseudonimiseerde gegevens toestaan.

Indien de anonimisering of pseudonimisering de identificatie van de gegevens niet onmogelijk maakt, weigert de verwerkingsverantwoordelijke in het kader van artikel 107 de raadpleging indien dit een onevenredige afbreuk doet aan het privéleven.

Indien een verdere verwerking van gepseudonimiseerde gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan de verwerkingsverantwoordelijke in het kader van artikel 107 de raadpleging van niet-gepseudonimiseerde gegevens toestaan indien dit geen onevenredige afbreuk doet aan het privéleven.

de données à caractère personnel dans le cadre de l’article 107 se concerte avec le Comité Permanent R.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 132

Par dérogation au titre 4, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel des autorités, l’organe de recours ou les personnes visés à l’article 107 et de leur personnel par un responsable du traitement ultérieur est autorisée si cela ne porte pas atteinte aux intérêts visés par l’article 12, alinéa premier, de la loi du 11 décembre 1998.

Art. 133

Avant leur consultation visée à l’article 132, les données à caractère personnel doivent être marquées de la mention “Protection des données à caractère personnel – articles 132 à 137 de la loi du xx/xx/2018”.

Art. 134

Les données à caractère personnel visées à l’article 132 sont rendues anonymes préalablement à leur consultation.

Si un traitement ultérieur de données anonymes ne permet pas d’atteindre les fins historiques, scientifiques ou statistiques, le responsable du traitement, dans le cadre de l’article 107, peut autoriser la consultation de données pseudonymisées.

Si l’anonymisation ou la pseudonymisation ne rend pas l’identification des données impossible, le responsable du traitement, dans le cadre de l’article 107, refuse la consultation si cela constitue une atteinte disproportionnée à la vie privée.

Si un traitement ultérieur de données pseudonymisées ne permet pas d’atteindre les fins historiques, scientifiques ou statistiques, le responsable du traitement, dans le cadre de l’article 107, peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 135

In afwijking van titel 4, is een mededeling of publicatie van niet-geanonimiseerde of niet-gepseudonimiseerde persoonsgegevens bedoeld in artikel 132, die werden geraadpleegd door de verdere verwerkingsverantwoordelijke, is enkel mogelijk met het akkoord van de verwerkingsverantwoordelijke in het kader van artikel 107 en onder de voorwaarden die hij vastlegt.

Art. 136

De verdere verwerkingsverantwoordelijke van persoonsgegevens bedoeld in artikel 132 houdt een logbestand van zijn verdere verwerkingsactiviteiten voor historische, wetenschappelijke of statistische doeleinden bij.

Dit logbestand is geclassificeerd in de zin van de wet van 11 december 1998 indien de verwerking betrekking heeft op geclassificeerde gegevens.

Dit logbestand bevat de volgende informatie:

1° de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming van deze laatste;

2° de doeleinden van de verdere verwerking;

3° de eventuele voorwaarden voor de verdere verwerking vastgelegd door de verwerkingsverantwoordelijke in het kader van artikel 107;

4° de eventuele ontvangers toegestaan door de verwerkingsverantwoordelijke in het kader van artikel 107.

Art. 137

Elke overheidsinstantie of elke natuurlijke of rechtspersoon die persoonsgegevens bedoeld in artikel 132 verwerkt om historische, wetenschappelijke of statistische doeleinden is de verantwoordelijke van deze verwerking.

Hij mag geen handelingen verrichten die zijn gericht op de omzetting van anonieme of gepseudonimiseerde gegevens in persoonsgegevens.

Art. 135

Par dérogation au titre 4, une communication ou publication des données à caractère personnel visées à l'article 132 non anonymisées ou non pseudonymisées, consultées par le responsable du traitement ultérieur n'est possible qu'avec l'accord du responsable du traitement dans le cadre de l'article 107 concerné et sous les conditions que celui-ci aura fixées.

Art. 136

Le responsable du traitement ultérieur des données à caractère personnel visées à l'article 132 tient un journal de ses activités de traitement ultérieur à des fins historiques, scientifiques ou statistiques.

Ce journal est classifié au sens de la loi du 11 décembre 1998 si le traitement porte sur des données classifiées.

Ce journal comporte les informations suivantes:

1° les coordonnées du responsable du traitement initial, du responsable du traitement ultérieur et du délégué à la protection des données de ce dernier;

2° les finalités du traitement ultérieur;

3° les éventuelles conditions du traitement ultérieur fixées par le responsable du traitement dans le cadre de l'article 107;

4° les éventuels destinataires autorisés par le responsable du traitement dans le cadre de l'article 107.

Art. 137

Toute autorité publique ou toute personne physique ou morale qui traite des données à caractère personnel visées à l'article 132 à des fins historiques, scientifiques ou statistiques est responsable dudit traitement.

Elle n'entreprendra aucune action pour convertir des données anonymes ou pseudonymisées en données à caractère personnel.

ONDERTITEL 4

De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door het coordinatieorgaan voor de dreigingsanalyse

HOOFDSTUK I

Definities

Art. 138

§ 1. De definities bedoeld in de artikelen 26, 1° tot 6°, 9° tot 11° tot 14° en 16° tot 17°, zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder:

1° "het OCAD": Coördinatieorgaan voor de dreigingsanalyse bedoeld in de wet van 10 juli 2006 betreffende de analyse van de dreiging;

2° "de verwerkingsverantwoordelijke": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

3° "de wet van 18 juli 1991": de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

4° "de wet van 11 december 1998": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

5° "toezichthoudende autoriteit": een onafhankelijke overheidsinstantie die bij de wet belast is met het toezicht op de toepassing van deze wet;

6° "de wet van 10 juli 2006": de wet van 10 juli 2006 betreffende de analyse van de dreiging;

7° "het informatiesysteem van het OCAD": het informatiesysteem bedoeld in artikel 9 van de wet van 10 juli 2006.

SOUS-TITRE 4

De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par l'organe de coordination pour l'analyse de la menace

CHAPITRE I

Définitions

Art. 138

§ 1er. Les définitions visées à l'article 26, 1° à 6°, 9° à 11° à 14° et 16° à 17°, sont applicables au présent sous-titre.

§ 2. Pour l'application du présent sous-titre, on entend par:

1° "l'OCAM": Organe de coordination pour l'analyse de la menace visé dans la loi du 10 juillet 2006 relative à l'analyse de la menace;

2° "le responsable du traitement": la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement;

3° "la loi du 18 juillet 1991": la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace;

4° "la loi du 11 décembre 1998": la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

5° "autorité de contrôle": une autorité publique indépendante chargée par la loi de surveiller l'application de la présente loi;

6° "la loi du 10 juillet 2006": la loi du 10 juillet 2006 relative à l'analyse de la menace;

7° "le système d'informations de l'OCAM": le système d'informations visé dans l'article 9 de la loi du 10 juillet 2006.

HOOFDSTUK II

Toepassingsgebied

Art. 139

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door het OCAD en zijn verwerkers, uitgevoerd in het kader van de opdrachten als bedoeld in de wet van 10 juli 2006, en door of krachtens bijzondere wetten.

Titels 1, 2, 4, 5 en 7 van deze wet zijn niet van toepassing op de verwerkingen bedoeld in het eerste lid. Enkel de artikelen 226 en 227 van titel 6 zijn van toepassing.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 140

Persoonsgegevens mogen slechts verwerkt worden in één van de volgende gevallen:

1° wanneer de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend;

2° wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;

3° wanneer de verwerking nuttig is om een verplichting na te komen waaraan het OCAD is onderworpen door of krachtens een wet;

4° wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verwerkingsverantwoordelijke of aan de overheidsinstantie aan wie de persoonsgegevens worden verstrekt.

Art. 141

Persoonsgegevens dienen:

1° eerlijk en rechtmatig te worden verwerkt;

2° voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en

CHAPITRE II

Champ d'application

Art. 139

Le présent sous-titre s'applique à tout traitement de données à caractère personnel par l'OCAM, et ses sous-traitants effectué dans le cadre des missions visées dans la loi du 16 juillet 2006, ainsi que par ou en vertu de lois particulières.

Les titres 1, 2, 4, 5, et 7 de la présente loi ne s'appliquent pas aux traitements visés à l'alinéa premier. Dans le titre 6, seuls les articles 226 et 227 sont d'application.

CHAPITRE III

Conditions générales du traitement

Art. 140

Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants:

1° lorsque la personne concernée a indubitablement donné son consentement;

2° lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

3° lorsqu'il est utile au respect d'une obligation à laquelle l'OCAM est soumis par ou en vertu d'une loi;

4° lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou une autorité publique à laquelle les données à caractère personnel sont communiquées.

Art. 141

Les données à caractère personnel doivent être:

1° traitées loyalement et licitement;

2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement

niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden. Onder de voorwaarden vastgesteld door de artikelen 162 tot 167 wordt een verdere verwerking van de gegevens voor historische, wetenschappelijke of statistische doeleinden niet als onverenigbaar beschouwd;

3° toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4° nauwkeurig te zijn en, zo nodig, te worden bijgewerkt. Alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren.

HOOFDSTUK IV

Aard van de persoonsgegevens

Art. 142

Het OCAD verwerkt, voor zover noodzakelijk voor het belang van de uitoefening van zijn opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook genetische en biometrische gegevens, gezondheidsgegevens, gegevens die het seksuele gedrag of de seksuele gerichtheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen.

HOOFDSTUK V

Bewaring van persoonsgegevens

Art. 143

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de modaliteiten bepaald in artikel 9 van de wet van 10 juli 2006 voor wat het informatiesysteem van het OCAD betreft en artikel 44/11/3*bis* van de wet van 5 augustus 1992 op het politieambt voor wat betreft de gemeenschappelijke gegevensbanken waarvan het OCAD de operationele beheerder is.

de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et réglementaires applicables. Un traitement ultérieur à des fins historiques, scientifiques ou statistiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par les articles 162 à 167;

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4° exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

CHAPITRE IV

Nature des données à caractère personnel

Art. 142

Dans la mesure nécessaire à l'intérêt de l'exercice de ses missions, l'OCAM traite des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

CHAPITRE V

Conservation des données à caractère personnel

Art. 143

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées dans l'article 9 de la loi du 16 juillet 2006 en ce qui concerne le système d'informations de l'OCAM et l'article 44/11/3*bis* de la loi de 5 août 1992 sur la fonction de police en ce qui concerne les banques de données communes dont l'OCAM est le gestionnaire opérationnel.

HOOFDSTUK VI

Rechten van de betrokkene

Art. 144

Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.

Art. 145

De betrokkene heeft het recht te vragen:

1° om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen overeenkomstig artikel 146;

2° om de verificatie bij de bevoegde toezichthoudende autoriteit van de naleving van de bepalingen van deze ondertitel overeenkomstig artikel 146.

Art. 146

De rechten, bedoeld in artikel 145 worden kosteloos uitgeoefend via de bevoegde toezichthoudende autoriteit op initiatief van de betrokkene die zijn identiteit bewijst.

De bevoegde toezichthoudende autoriteit voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht.

De nadere regels voor de uitoefening van deze rechten worden bepaald in de wet.

Art. 147

De toezichthoudende autoriteiten bedoeld in artikel 161 en het OCAD houden een logbestand bij van alle aanvragen van betrokkenen tot uitoefening van hun rechten.

Art. 148

Een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn, mag niet louter worden genomen op grond van een geautomatiseerde persoonsgegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.

CHAPITRE VI

Droits de la personne concernée

Art. 144

Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 145

La personne concernée a le droit de demander:

1° la rectification ou la suppression de ses données à caractère personnel inexactes conformément à l'article 146;

2° la vérification auprès de l'autorité de contrôle compétente du respect des dispositions du présent sous-titre conformément à l'article 146.

Art. 146

Les droits visés à l'article 145 s'exercent, sans frais, par l'intermédiaire de l'autorité de contrôle compétente, à l'initiative de la personne concernée justifiant de son identité.

L'autorité de contrôle compétente effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Les modalités d'exercice de ces droits sont déterminées par la loi.

Art. 147

Les autorités de contrôle visées à l'article 161 et l'OCAM tiennent un journal des demandes d'exercice des droits par les personnes concernées.

Art. 148

Une décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Het in het eerste lid vastgestelde verbod geldt niet indien het besluit zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet of wanneer het noodzakelijk is vanwege een zwaarwegend algemeen belang.

HOOFDSTUK VII

Verplichtingen van de verwerkingsverantwoordelijke en de verwerker

Afdeling 1

Algemene verplichtingen

Art. 149

De verwerkingsverantwoordelijke moet:

1° er nauwlettend over waken dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2° ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot wat nuttig is voor de uitoefening van hun taken of voor de behoeften van het OCAD;

3° alle personen die onder zijn gezag handelen, informeren over de bepalingen van deze ondertitel en over alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer betreffende de verwerking van persoonsgegevens.

Art. 150

Indien de verwerking wordt toevertrouwd aan een verwerker, moet de verwerkingsverantwoordelijke:

1° een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de verwerkingen;

2° toezien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen;

3° de verantwoordelijkheid van de verwerker vaststellen in de overeenkomst;

L'interdiction prévue à l'alinéa premier ne s'applique pas lorsque la décision est fondée sur une disposition prévue par ou en vertu d'une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important.

CHAPITRE VII

Obligations du responsable du traitement et du sous-traitant

Section 1re

Obligations générales

Art. 149

Le responsable du traitement doit:

1° faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2° veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins de l'OCAM;

3° informer les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 150

Lorsque le traitement est confié à un sous-traitant, le responsable du traitement doit:

1° choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements;

2° veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles;

3° fixer dans le contrat la responsabilité du sous-traitant;

4° met de verwerker overeenkomen dat de verwerker slechts handelt in opdracht van de verwerkingsverantwoordelijke en dat de verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke in toepassing van deze ondertitel is gehouden;

5° in een geschrift of op een elektronische drager de elementen van de overeenkomst met betrekking tot de bescherming van de persoonsgegevens en de eisen met betrekking tot de maatregelen bedoeld in 3° en 4°, vaststellen.

Art. 151

De verwerker is gebonden door dezelfde verplichtingen als deze waartoe de verwerkingsverantwoordelijke is gehouden.

Hij mag de verwerking van persoonsgegevens niet toevertrouwen aan een andere verwerker, behoudens uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Art. 152

Eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker, alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verwerkingsverantwoordelijke verwerken, behoudens op grond van een verplichting door of krachtens een wet.

Afdeling 2

Gezamenlijke verwerkingsverantwoordelijken

Art. 153

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken.

Een overeenkomst bepaalt de respectievelijke verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken, met name met betrekking tot de uitoefening van de rechten van de betrokkene en de mededeling van persoonsgegevens, tenzij hun respectievelijke verplichtingen worden bepaald door of krachtens een wet.

4° convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et qu'il est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du présent sous-titre;

5° consigner par écrit ou sur un support électronique les éléments du contrat relatifs à la protection des données à caractère personnel et les exigences relatives aux mesures visées aux 3° et 4°.

Art. 151

Le sous-traitant est soumis aux mêmes obligations que celles qui incombent au responsable du traitement.

Il ne peut pas confier le traitement de données à caractère personnel à un autre sous-traitant, sauf autorisation expresse du responsable du traitement.

Art. 152

Toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi.

Section 2

Responsables conjoints du traitement

Art. 153

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Un accord définit les obligations respectives des responsables conjoints de traitement, notamment en ce qui concerne l'exercice des droits de la personne concernée et la communication des données à caractère personnel, sauf si leurs obligations respectives sont définies par ou en vertu d'une loi.

In de onderlinge overeenkomst wordt één contactpunt voor betrokkenen aangewezen. De gezamenlijke verwerkingsverantwoordelijken nemen dit contactpunt op in het register bedoeld in artikel 156.

Afdeling 3

Beveiliging van persoonsgegevens

Art. 154

Om de veiligheid van de persoonsgegevens te waarborgen, treffen de verwerkingsverantwoordelijke, alsmede de verwerker, de passende technische en organisatorische maatregelen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen verzekeren een passend beveiligingsniveau, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen persoonsgegevens en de potentiële risico's.

Art. 155

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk binnen de kortste termijn aan de bevoegde toezichthoudende autoriteit en indien mogelijk, 72 uur nadat hij er kennis van heeft genomen.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke binnen de kortste termijn van elke inbreuk op de beveiliging.

§ 3. In de in paragrafen 1 en 2 bedoelde melding wordt, op zijn minst, het volgende omschreven of meegedeeld:

1° de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en de opgeslagen persoonsgegevens in kwestie;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt bij wie bijkomende informatie kan worden verkregen;

Un seul point de contact pour les personnes concernées peut être désigné dans l'accord. Les responsables conjoints du traitement incluent ce point de contact dans le registre visé à l'article 156.

Section 3

Sécurité des données à caractère personnel

Art. 154

Le responsable du traitement ainsi que le sous-traitant prennent les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures assurent un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels.

Art. 155

§ 1er. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie à l'autorité de contrôle compétente dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais.

§ 3. La notification visée aux paragraphes premier et 2 doit, à tout le moins:

1° décrire la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de verwerkingsverantwoordelijke, of de verwerker heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder desgevallend maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Afdeling 4

Registers

Art. 156

§ 1. De verwerkingsverantwoordelijke houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van de gegevensbanken van het OCAD en deze die aan hem ter beschikking worden gesteld.

Dit register bevat de volgende gegevens:

1° voor de gegevensbanken van het OCAD:

a) de contactgegevens van de verwerkingsverantwoordelijke en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden;

c) de categorieën van ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

d) indien mogelijk, de beoogde termijnen voor het verwijderen van de persoonsgegevens;

e) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 154.

2° Voor gegevensbanken die aan het OCAD ter beschikking gesteld worden:

a) de contactgegevens van de verwerkingsverantwoordelijke en, indien mogelijk voor de landen buiten de Europese Unie de dienst die de gegevensbank beheert en, desgevallend,van de gezamenlijke verwerkingsverantwoordelijken en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden van het OCAD.

3° décrire les conséquences probables de la brèche de sécurité;

4° décrire les mesures prises ou que le responsable du traitement ou le sous-traitant propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Section 4

Registres

Art. 156

§ 1er. Le responsable du traitement tient un registre, classifié au sens de la loi du 11 décembre 1998, des banques de données de l'OCAM et de celles mises à sa disposition.

Ce registre comporte les informations suivantes:

1° pour les banques de données de l'OCAM:

a) les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement, et du délégué à la protection des données;

b) les finalités du traitement;

c) les catégories de destinataires auxquels des données à caractère personnel peuvent être communiquées;

d) dans la mesure du possible, les délais prévus pour l'effacement des données à caractère personnel;

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 154.

2° pour les banques de données mises à la disposition de l'OCAM:

a) les coordonnées du responsable du traitement et, si possible pour les pays hors de l'Union européenne le service gestionnaire de la banque de données et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement par l'OCAM.

§ 2. Elke verwerker houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.

Dit register bevat de volgende elementen:

1° de contactgegevens van de verwerker en van de verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, desgevallend, van de functionaris voor gegevensbescherming;

2° de categorieën van verwerkingen die voor rekening van de verwerkingsverantwoordelijke zijn uitgevoerd;

3° indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 154.

§ 3. De in de paragrafen 1 en 2 bedoelde registers worden in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 4. De verwerkingsverantwoordelijke stelt het register ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

De verwerker stelt het register ter beschikking van de verwerkingsverantwoordelijke en stelt het eveneens ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

Afdeling 5

Functionaris voor gegevensbescherming

Art. 157

§ 1. De verwerkingsverantwoordelijke, en desgevallend de verwerker, wijzen een functionaris voor gegevensbescherming aan. Deze beslissing wordt meegedeeld aan de bevoegde toezichthoudende autoriteit.

De functionaris voor gegevensbescherming is titularis van een veiligheidsmachtiging “zeer geheim”, in de zin van de wet van 11 december 1998.

§ 2. De functionaris voor gegevensbescherming kan niet gestraft worden voor het uitoefenen van zijn functie. Hij kan evenmin van zijn functie ontheven worden omwille van de uitvoering van zijn opdrachten, behalve indien hij een zware fout heeft begaan of de voorwaarden noodzakelijk voor het uitoefenen van zijn functie niet langer vervult.

§ 2. Chaque sous-traitant tient un registre, classifié au sens de la loi du 11 décembre 1998, de toutes les catégories d’activités de traitement effectuées pour le compte d’un responsable du traitement.

Ce registre comprend les éléments suivants:

1° les coordonnées du sous-traitant et du responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les coordonnées du délégué à la protection des données;

2° les catégories de traitements effectués pour le compte du responsable du traitement;

3° dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l’article 154.

§ 3. Les registres visés aux paragraphes premier et 2 se présentent sous une forme écrite y compris la forme électronique.

§ 4. Le responsable du traitement met le registre à la disposition de l’autorité de contrôle compétente à sa demande.

Le sous-traitant met le registre à la disposition du responsable du traitement ainsi qu’à la disposition de l’autorité de contrôle compétente à sa demande.

Section 5

Délégué à la protection des données

Art. 157

§ 1er. Le responsable du traitement et, le cas échéant, le sous-traitant désignent un délégué à la protection des données. Cette décision est communiquée à l’autorité de contrôle compétente.

Le délégué à la protection des données est titulaire d’une habilitation de sécurité de niveau très secret, au sens de la loi du 11 décembre 1998.

§ 2. Le délégué à la protection des données ne peut pas être sanctionné en raison de l’exercice de ses fonctions. Il ne peut pas non plus être relevé de ses fonctions en raison de l’exercice de ses missions, sauf s’il a commis une faute grave ou s’il ne remplit plus les conditions nécessaires à l’exercice de ses fonctions.

De functionaris voor gegevensbescherming kan zich tot het Vast Comité I wenden om deze beslissing aan te vechten.

§ 3. Hij is, op een onafhankelijke wijze, belast met:

1° het toezien op de naleving van deze ondertitel voor elke verwerking van persoonsgegevens;

2° het adviseren over alle nuttige maatregelen teneinde de veiligheid van de opgeslagen gegevens te verzekeren;

3° het informeren en adviseren van de verwerkingsverantwoordelijke, en desgevallend de verwerker, het diensthoofd en de personeelsleden van de betrokken dienst die de verwerking verrichten over hun verplichtingen op grond van deze ondertitel;

4° het verstrekken van adviezen of aanbevelingen aan de verwerkingsverantwoordelijke, en desgevallend aan de verwerker of de leidinggevende van het OCAD;

5° het uitvoeren van andere opdrachten die hem door de verwerkingsverantwoordelijke, en in voorkomend geval de verwerker of de leidinggevende van het OCAD toevertrouwd zijn.

De functionaris voor gegevensbescherming is de contactpersoon voor de bevoegde toezichthoudende autoriteit met betrekking tot de toepassing van deze ondertitel.

§ 4. De verwerkingsverantwoordelijke, en desgevallend de verwerker ziet erop toe dat hun functionaris voor gegevensbescherming tijdig en naar behoren wordt betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden.

De verwerkingsverantwoordelijke, en desgevallend de verwerker ziet erop toe dat de functionaris voor gegevensbescherming de benodigde middelen ter beschikking heeft voor het vervullen van zijn taken.

De functionaris voor gegevensbescherming kan worden bijgestaan door één of meerdere medewerkers.

§ 5. Desgevallend kunnen nadere regels voor de werking, de aanwijzing en de vereiste bevoegdheden door de Koning worden bepaald.

Le délégué à la protection des données peut s'adresser au Comité permanent R pour contester cette décision.

§ 3. Il est chargé de manière indépendante:

1° de veiller au respect du présent sous-titre lors de tout traitement de données à caractère personnel;

2° de conseiller toutes mesures utiles afin d'assurer la sécurité des données enregistrées;

3° d'informer et conseiller le responsable du traitement, et le cas échéant, le sous-traitant, le dirigeant et le personnel du service concerné procédant au traitement sur les obligations qui leur incombent en vertu du présent sous-titre;

4° de fournir des avis ou des recommandations au responsable du traitement, et le cas échéant au sous-traitant, et au dirigeant de l'OCAM;

5° d'exécuter d'autres missions qui lui sont confiées par le responsable du traitement, le cas échéant le sous-traitant ou le dirigeant de l'OCAM.

Le délégué à la protection des données est le point de contact avec l'autorité de contrôle compétente pour l'application du présent sous-titre.

§ 4. Le responsable du traitement et, le cas échéant le sous-traitant, veille à ce que son délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Le responsable du traitement et, le cas échéant le sous-traitant veille à ce que son délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

§ 5. Le cas échéant, les modalités de fonctionnement, de désignation ainsi que les compétences requises peuvent être définies par le Roi.

HOOFDSTUK IX

Mededeling en doorgifte van persoonsgegevens

Afdeling 1

Mededeling van persoonsgegevens aan de publieke sector en de private sector

Art. 158

In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen het OCAD en enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten van het OCAD.

Deze mededeling vindt plaats in overeenstemming met de artikelen 8, 9, 10, 11 en 12 van de wet van 10 juli 2006 en onderafdeling 7*bis* van de wet van 5 augustus 1992 op het politieambt.

Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 20, § 1, tweede lid, het volgende:

1° de identificatie van het OCAD en het openbaar of particulier orgaan die de persoonsgegevens uitwisselen;

2° de identificatie van de verwerkingsverantwoordelijken;

3° de contactgegevens van de betrokken functionarissen voor gegevensbescherming;

4° de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5° de wettelijke grondslag;

6° de beperkingen van de rechten van de betrokkene.

Het protocol draagt de markering “BEPERKTE VERSPREIDING” in de zin van het koninklijk besluit van 24 maart 2004 tot uitvoering van de wet van 11 december 1998, voor zover een classifcatie in de zin van de wet van 11 december 1998 niet gerechtvaardigd is.

CHAPITRE IX

Communication et transfert de données à caractère personnel

Section 1re

Communication de données à caractère personnel avec le secteur public et le secteur privé

Art. 158

Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d’impact relative à la protection des données et l’avis résultant de la consultation de l’autorité de contrôle compétente ne peuvent pas être exigés comme préalable à la communication de données à caractère personnel entre l’OCAM et tout organisme public ou privé dans l’intérêt de l’exercice des missions de l’OCAM.

Cette communication se déroule conformément aux articles 8, 9, 10, 11 et 12 de la loi du 10 juillet 2006 et à la sous-section 7*bis* de la loi du 5 août 1992 sur la fonction de la police.

Par dérogation à l’article 20, § 1er, alinéa 2, lorsque les parties décident de conclure un protocole, celui-ci porte notamment sur:

1° l’identification de l’OCAM et de l’organisme public ou privé qui échangent les données à caractère personnel;

2° l’identification des responsables du traitement;

3° les coordonnées des délégués à la protection des données concernés;

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° la base légale;

6° les restrictions aux droits de la personne concernée.

Le protocole porte le marquage “DIFFUSION RESTREINTE” au sens de l’arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998, à moins qu’une classification au sens de la loi du 11 décembre 1998 ne se justifie.

Afdeling 2

Doorgifte van persoonsgegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties

Art. 159

Persoonsgegevens mogen slechts worden doorgegeven aan een land dat geen lid is van de Europese Unie of een internationale organisatie, indien dat land of die organisatie een passend beschermingsniveau en de naleving van de andere bepalingen van deze ondertitel waarborgt.

De vraag of het beschermingsniveau passend is, wordt beoordeeld met inachtneming van alle omstandigheden die betrekking hebben op de doorgifte van persoonsgegevens of op een categorie van doorgiften van persoonsgegevens. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen of organisaties worden nageleefd.

Het passende beschermingsniveau kan verzekerd worden door veiligheidsclausules tussen de verwerkingsverantwoordelijke en de ontvanger van de persoonsgegevens.

Art. 160

In afwijking van artikel 159 mag een doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie, hetwelke geen waarborgen biedt voor een passend beschermingsniveau, slechts plaatsvinden wanneer:

1° de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven voor de beoogde doorgifte; of

2° de doorgifte verplicht is in het kader van de internationale betrekkingen; of

3° de doorgifte noodzakelijk is ter vrijwaring van het vitaal belang van de personen; of

4° de doorgifte noodzakelijk of wettelijk verplicht is ter vrijwaring van een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

Section 2

Transfert des données à caractère personnel vers des pays non membres de l'Union européenne ou à des organisations internationales

Art. 159

Le transfert de données à caractère personnel vers un pays non membres de l'Union européenne ou vers une organisation internationale ne peut avoir lieu que si le pays ou l'organisation en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions du présent sous-titre.

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données à caractère personnel ou à une catégorie de transferts de données à caractère personnel. Il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays ou l'organisation en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

Le niveau de protection adéquat peut être assuré par des clauses de sécurité entre le responsable du traitement et le destinataire des données à caractère personnel.

Art. 160

Par dérogation à l'article 159, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale n'assurant pas un niveau de protection adéquat, peut être effectué lorsque:

1° la personne concernée a indubitablement donné son consentement au transfert envisagé; ou

2° le transfert est obligatoire dans le cadre des relations internationales; ou

3° le transfert est nécessaire à la sauvegarde de l'intérêt vital des personnes; ou

4° le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

HOOFDSTUK X

Toezichthoudende autoriteit

Art. 161

Overeenkomstig artikel 10 van de wet van 10 juli 2006 worden het Vast Comité I, in zijn hoedanigheid van onafhankelijke publieke autoriteit, en het Vast Comité van Toezicht op de politiediensten, aangeduid als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens door het OCAD en zijn verwerkers volgens de nadere regels vastgelegd in de wet van 18 juli 1991.

HOOFDSTUK XI

Verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden

Art. 162

In afwijking van titel 4, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens van het OCAD en van hun personeel toegestaan door het OCAD indien dit geen afbreuk doet aan zijn opdrachten bedoeld in de wet van 10 juli 2006, aan een lopend opsporings- of gerechtelijk onderzoek, of aan de betrekkingen die België met vreemde staten of internationale organisaties onderhoudt en overeenkomstig de wet van 10 juli 2006.

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens van het OCAD en van hun personeel voor overige doelen dan die bedoeld in het eerste lid wordt geweigerd voor zover het doel legitiem is en het OCAD meent dat de verwerking geen afbreuk kan doen aan de belangen bedoeld in het voorgaande lid.

Art. 163

Vóór hun raadpleging bedoeld in artikel 162 moeten de persoonsgegevens voorzien worden van de vermelding “Bescherming van persoonsgegevens – hoofdstuk XI, ondertitel 4 van titel 3”.

CHAPITRE X

Autorité de contrôle

Art. 161

Conformément à l’article 10 de la loi du 10 juillet 2006, le Comité permanent R, en sa qualité d’autorité publique indépendante, et le Comité permanent de Contrôle des Services de police, sont désignés comme autorités de protection des données chargée du contrôle du traitement des données à caractère personnel par l’OCAM et par ses sous-traitants selon les modalités fixées par la loi du 18 juillet 1991.

CHAPITRE XI

Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques

Art. 162

Par dérogation au titre 4, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel de l’OCAM et de leur personnel par un responsable du traitement ultérieur est autorisée par l’OCAM si cela ne porte pas atteinte à ses missions visées dans la loi du 10 juillet 2006, à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des États étrangers ou des organisations internationales et conformément à la loi du 10 juillet 2006.

Toute demande adressée aux Archives de l’État de traitement ultérieur de données à carcatère personnel de l’OCAM et de son personnel à d’autres fins que celles visées à l’alinéa premier est refusée à moins que la finalité soit légitime et que l’OCAM estime que le traitement n’est pas susceptible de porter atteinte aux intérêts visés à l’alinéa précédent.

Art. 163

Avant leur consultation visée à l’article 162, les données à caractère personnel doivent être marquées de la mention “Protection des données à caractère personnel – chapitre XI, sous-titre 4 du titre 3”.

Art. 164

De persoonsgegevens bedoeld in artikel 162 worden voorafgaand aan hun raadpleging geanonimiseerd.

Indien een verdere verwerking van anonieme gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan het OCAD de raadpleging van gepseudonimiseerde gegevens toestaan.

Indien de anonimisering of pseudonimisering de identificatie van de gegevens niet onmogelijk maakt, weigert het OCAD de raadpleging indien dit een onevenredige afbreuk doet aan het privéleven.

Indien een verdere verwerking van gepseudonimiseerde gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan het OCADde raadpleging van niet-gepseudonimiseerde gegevens toestaan indien dit geen onevenredige afbreuk doet aan het privéleven.

Art. 165

In afwijking van titel 4, is een mededeling of publicatie van niet-geanonimiseerde of niet-gepseudonimiseerde persoonsgegevens bedoeld in artikel 162, geraadpleegd door de verdere verwerkingsverantwoordelijke, is enkel mogelijk met het akkoord van het OCAD en onder de voorwaarden die het vastlegt.

Art. 166

De verdere verwerkingsverantwoordelijke van persoonsgegevens bedoeld in artikel 162 houdt een logbestand van zijn verdere verwerkingsactiviteiten voor historische, wetenschappelijke of statistische doeleinden bij.

Dit logbestand is geclassificeerd in de zin van de wet van 11 december 1998 indien de verwerking betrekking heeft op geclassificeerde gegevens.

Dit logbestand bevat de volgende informatie:

1° de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming van deze laatste;

2° de doeleinden van de verdere verwerking;

Art. 164

Les données à caractère personnel visées à l'article 162 sont rendues anonymes préalablement à leur consultation.

Si un traitement ultérieur de données anonymes ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, l'OCAM peut autoriser la consultation de données pseudonymisées.

Si l'anonymisation ou la pseudonymisation ne rend pas l'identification des données impossible, l'OCAM refuse la consultation si cela constitue une atteinte disproportionnée à la vie privée.

Si un traitement ultérieur de données pseudonymisées ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, l'OCAM peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 165

Par dérogation au titre 4, une communication ou publication des données à caractère personnel visées à l'article 162 non anonymisées ou non pseudonymisées, consultées par le responsable du traitement ultérieur n'est possible qu'avec l'accord de l'OCAM et sous les conditions que celui-ci aura fixées.

Art. 166

Le responsable du traitement ultérieur des données à caractère personnel visées à l'article 162 tient un journal de ses activités de traitement ultérieur à des fins historiques, scientifiques ou statistiques.

Ce journal est classifié au sens de la loi du 11 décembre 1998 si le traitement porte sur des données classifiées.

Ce journal comporte les informations suivantes:

1° les coordonnées du responsable du traitement initial, du responsable du traitement ultérieur et du délégué à la protection des données de ce dernier;

2° les finalités du traitement ultérieur;

3° de gegevens die het voorwerp uitmaken van de verdere verwerking;

4° de eventuele voorwaarden voor de verdere verwerking vastgelegd door het OCAD;

5° de eventuele ontvangers toegestaan door het OCAD.

Art. 167

Elke overheidsinstantie of elke natuurlijke of rechtspersoon die persoonsgegevens bedoeld in artikel 162 verwerkt om historische, wetenschappelijke of statistische doeleinden is de verantwoordelijke van deze verwerking.

Hij mag geen handelingen verrichten die zijn gericht op de omzetting van anonieme of gepseudonimiseerde gegevens in persoonsgegevens.

ONDERTITEL 5

De bescherming van natuurlijke personen met betrekking tot bepaalde verwerkingen van persoonsgegevens door de passagiersinformatie-eenheid

HOOFDSTUK I

Definities

Art. 168

§ 1. De definities bedoeld in artikelen 26, 1° tot 3°, 8°, 10° en 11° en in artikel 72, § 2, 6° en 7° zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder:

1° "de wet van 25 december 2016": de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens;

2° "de PIE": de Passagiersinformatie-eenheid bedoeld in hoofdstuk 7 van de wet van 25 december 2016.

3° les données faisant l'objet du traitement ultérieur;

4° les éventuelles conditions du traitement ultérieur fixées par l'OCAM;

5° les éventuels destinataires autorisés par l'OCAM.

Art. 167

Toute autorité publique ou toute personne physique ou morale qui traite des données à caractère personnel visées à l'article 162 à des fins historiques, scientifiques ou statistiques est responsable dudit traitement.

Elle n'entreprendra aucune action pour convertir des données anonymes ou pseudonymisées en données à caractère personnel.

SOUS-TITRE 5

De la protection des personnes physiques a l'égard de certains traitements de données à caractère personnel par l'unité d'information des passagers

CHAPITRE I^ER

Définitions

Art. 168

§ 1er. Les définitions visées à l'article 26, 1° à 3°, 8°, 10° et 11° et à l'article 72, § 2, 6° et 7° sont applicables au présent sous-titre.

§ 2. Pour l'application du présent sous-titre, on entend par:

1° "la loi du 25 décembre 2016": la loi du 25 décembre 2016 relative au traitement des données des passagers;

2° "l'UIP": l'Unité d'information des passagers visée au chapitre 7 de la loi du 25 décembre 2016.

HOOFDSTUK II

Toepassingsgebied

Art. 169

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door de PIE in het kader van de finaliteiten bedoeld in artikel 8, § 1, 4°, van de wet van 25 december 2016.

Titels 1, 2, 4, 5 en 7 van deze wet zijn niet van toepassing op de verwerkingen bedoeld in het eerste lid. Enkel de artikelen 226 en 227 van titel 6 zijn van toepassing.

HOOFDSTUK III

Algemene verwerkingsvoorwaarden

Art. 170

Persoonsgegevens dienen:

1° eerlijk en rechtmatig te worden verwerkt;

2° voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden;

3° toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4° nauwkeurig te zijn en, zo nodig, te worden bijgewerkt. Alle redelijke maatregelen dienen te worden getroffen om de persoonsgegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, te wissen of te verbeteren.

HOOFDSTUK IV

Bewaring van persoonsgegevens

Art. 171

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de modaliteiten

CHAPITRE II

Champ d'application

Art. 169

Le présent sous-titre s'applique à tout traitement de données à caractère personnel par l'UIP effectué dans le cadre des finalités visées à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016.

Les titres 1, 2, 4, 5 et 7 de la présente loi ne s'appliquent pas aux traitements visés à l'alinéa premier. Dans le titre 6, seuls les articles 226 et 227 sont d'application.

CHAPITRE III

Conditions générales du traitement

Art. 170

Les données à caractère personnel doivent être:

1° traitées loyalement et licitement;

2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et réglementaires applicables;

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement;

4° exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

CHAPITRE IV

Conservation des données à caractère personnel

Art. 171

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon

bepaald in het kader van hoofdstuk 9 van de wet van 25 december 2016.

HOOFDSTUK V

Rechten van de betrokkene

Art. 172

Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op de bescherming van zijn persoonsgegevens.

Art. 173

De betrokkene heeft het recht te vragen:

1° om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen overeenkomstig artikel 174;

2° om de verificatie bij het vast Comite I van de naleving van de bepalingen van deze ondertitel overeenkomstig artikel 174.

Art. 174

De rechten, bedoeld in artikel 173 worden kosteloos uitgeoefend via het Vast Comité I op initiatief van de betrokkene die zijn identiteit bewijst.

Deze voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht.

De nadere regels voor de uitoefening van deze rechten worden bepaald in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

Art. 175

Het Vast Comite I en de Passagiersinformatie-eenheid houden een logbestand bij van alle aanvragen van betrokkenen tot uitoefening van hun rechten.

les modalités fixées dans le cadre du chapitre 9 de la loi du 25 décembre 2016.

CHAPITRE V

Droits de la personne concernée

Art. 172

Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de ses données à caractère personnel.

Art. 173

La personne concernée a le droit de demander:

1° la rectification ou la suppression de ses données à caractère personnel inexactes conformément à l'article 174;

2° la vérification auprès du Comité permanent R du respect des dispositions du présent sous-titre conformément à l'article 174.

Art. 174

Les droits visés à l'article 173 s'exercent, sans frais, par l'intermédiaire du Comité permanent R, à l'initiative de la personne concernée justifiant de son identité.

Celui-ci effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Les modalités d'exercice de ces droits sont déterminées par la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

Art. 175

Le Comité permanent R et l'Unité d'information des passagers tiennent un journal des demandes d'exercice des droits par les personnes concernées.

Art. 176

Een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn, mag niet louter worden genomen op grond van een geautomatiseerde persoonsgegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.

HOOFDSTUK VI

Verplichtingen van de verwerkingsverantwoordelijke

Afdeling 1

Algemene verplichtingen

Art. 177

De verwerkingsverantwoordelijke moet:

1° er nauwlettend over waken dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2° ervoor zorgen dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot wat nuttig is voor de uitoefening van hun taken of voor de behoeften van de dienst;

3° alle personen die onder zijn gezag handelen, informeren over de bepalingen van deze ondertitel en over alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer betreffende de verwerking van persoonsgegevens.

Art. 178

Eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verwerkingsverantwoordelijke verwerken, behoudens op grond van een verplichting door of krachtens een wet.

Art. 176

Une décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

CHAPITRE VI

Obligations du responsable du traitement

Section 1re

Obligations générales

Art. 177

Le responsable du traitement doit:

1° faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2° veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins du service;

3° informer les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 178

Toute personne agissant sous l'autorité du responsable du traitement qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi.

Afdeling 2

Beveiliging van persoonsgegevens

Art. 179

Om de veiligheid van de persoonsgegevens te waarborgen, treft de verwerkingsverantwoordelijke de passende technische en organisatorische maatregelen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen verzekeren een passend beveiligingsniveau, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen persoonsgegevens en de potentiële risico's.

Art. 180

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk binnen de kortste termijn aan het Vast Comité I en indien mogelijk, 72 uur nadat hij er kennis van heeft genomen.

§ 2. In de in paragraaf 1 bedoelde melding wordt, op zijn minst, het volgende omschreven of meegedeeld:

1° de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en de opgeslagen persoonsgegevens in kwestie;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt bij wie bijkomende informatie kan worden verkregen;

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder desgevallend maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Section 2

Sécurité des données à caractère personnel

Art. 179

Le responsable du traitement prend les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures assurent un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à caractère personnel à protéger et des risques potentiels.

Art. 180

§ 1er. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie au Comité permanent R dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance.

§ 2. La notification visée au paragraphe premier doit, à tout le moins:

1° décrire la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° décrire les conséquences probables de la brèche de sécurité;

4° décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Afdeling 3

Register

Art. 181

§ 1. De verwerkingsverantwoordelijke houdt een register bij van enerzijds de passgiersgegevensbank bedoeld in hoofdstuk 8 van de wet van 25 december 2016 en anderzijds van de gegevensbanken die aan haar ter beschikking worden gesteld.

Dit register bevat de volgende gegevens:

1° Voor de voormelde passagiersgegevensbank:

a) de contactgegevens van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;

a) de verwerkingsdoeleinden;

b) de categorieën van ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

c) indien mogelijk, de beoogde termijnen voor het verwijderen van de persoonsgegevens;

d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 179.

2° Voor gegevensbanken die aan de PIE ter beschikking gesteld worden:

a) de contactgegevens van de verwerkingsverantwoordelijke en, indien mogelijk voor de landen buiten de Europese Unie de dienst die de gegevensbank beheert en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken en van de functionaris voor gegevensbescherming;

a) de verwerkingsdoeleinden van de PIE.

§ 2. Het in de eerste paragraaf bedoelde register wordt in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 3. De verwerkingsverantwoordelijke stelt het register ter beschikking van het Vast Comité I op diens vraag.

Section 3

Registre

Art. 181

§ 1er. Le responsable du traitement tient un registre de la banque de données des passagers visée au chapitre 8 de la loi du 25 décembre 2016 d'une part et des banques de données mises à sa disposition d'autre part.

Ce registre comporte les informations suivantes:

1° pour la banque de données des passagers précitée:

a) les coordonnées du responsable du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) les catégories de destinataires auxquels des données à caractère personnel peuvent être communiquées;

d) dans la mesure du possible, les délais prévus pour l'effacement des données à caractère personnel;

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 179.

2° pour les banques de données mises à la disposition de l'UIP:

a) les coordonnées du responsable du traitement et, si possible pour les pays hors de l'Union européenne le service gestionnaire de la banque de données et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement par l'UIP.

§ 2. Le registre visé au paragraphe premier se présente sous une forme écrite y compris la forme électronique.

§ 3. Le responsable du traitement met le registre à la disposition du Comité permanent R à sa demande.

HOOFDSTUK VII

Mededeling en doorgifte van persoonsgegevens

Art. 182

Persoonsgegevens mogen slechts worden doorgegeven aan een land dat geen lid is van de Europese Unie of een internationale organisatie, indien dat land of die organisatie een passend beschermingsniveau en de naleving van de andere bepalingen van deze ondertitel en van de bepalingen van hoofdstuk 12 van de wet van 25 december 2016 waarborgt.

De vraag of het beschermingsniveau passend is, wordt beoordeeld met inachtneming van alle omstandigheden die betrekking hebben op de doorgifte van persoonsgegevens of op een categorie van doorgiften van persoonsgegevens. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen of organisaties worden nageleefd.

Het passende beschermingsniveau kan verzekerd worden door veiligheidsclausules tussen de verwerkingsverantwoordelijke en de ontvanger van de persoonsgegevens.

Art. 183

In afwijking van artikel 182 mag een doorgifte van persoonsgegevens aan een land dat geen lid is van de Europese Unie of aan een internationale organisatie, hetwelke geen waarborgen biedt voor een passend beschermingsniveau, slechts plaatsvinden wanneer:

1° de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven; of

2° de doorgifte verplicht is in het kader van de internationale betrekkingen; of

3° de doorgifte noodzakelijk is ter vrijwaring van het vitaal belang van de personen; of

4° de doorgifte noodzakelijk of wettelijk verplicht is ter vrijwaring van een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

CHAPITRE VII

Communication et transfert de données à caractère personnel

Art. 182

Le transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale ne peut avoir lieu que si le pays ou l'organisation en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions du présent sous-titre et des dispositions du chapitre 12 de la loi du 25 décembre 2016..

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données à caractère personnel ou à une catégorie de transferts de données à caractère personnel. Il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays ou l'organisation en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

Le niveau de protection adéquat peut être assuré par des clauses de sécurité entre le responsable du traitement et le destinataire des données à caractère personnel.

Art. 183

Par dérogation à l'article 182, un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou vers une organisation internationale n'assurant pas un niveau de protection adéquat, peut être effectué lorsque:

1° la personne concernée a indubitablement donné son consentement au transfert envisagé; ou

2° le transfert est obligatoire dans le cadre des relations internationales; ou

3° le transfert est nécessaire à la sauvegarde de l'intérêt vital des personnes; ou

4° le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

HOOFDSTUK VIII

Toezichthoudende autoriteit

Art. 184

De verwerkingen van persoonsgegevens zoals bedoeld in deze ondertitel zijn onderworpen aan het toezicht van de toezichthoudende autoriteit bedoeld in artikel 95.

ONDERTITEL 6

Bijzondere bepalingen

Art. 185

§ 1. De volgende publieke overheden verwerken, voor zover noodzakelijk voor de uitoefening van hun opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of de seksuele gerichtheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen:

1° de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van haar opdrachten bedoeld in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en in bijzondere wetten;

3° het Vast Comité van Toezicht op de politiediensten in het kader van haar opdrachten bedoeld in artikel 1, 2° en 3° en hoofdstuk IV van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

4° Het Controleorgaan op de politionele informatie in het kader van haar opdrachten bedoeld in artikel 71, § 1.

CHAPITRE VIII

Autorité de contrôle

Art. 184

Les traitements de données à caractère personnel tels que visés dans ce sous-titre sont soumis au contrôle de l'autorité de contrôle visée à l'article 95.

SOUS-TITRE 6

Dispositions particulières

Art. 185

§ 1er. Dans la mesure nécessaire à l'exercice de leurs missions, les autorités publiques suivantes traitent des données à caractère personnel de toute nature, en ce comprises celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes:

1° la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité dans le cadre de ses missions visées dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° le Comité permanent R dans le cadre de ses missions visées dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et dans des lois particulières;

3° le Comité permanent P dans le cadre de ses missions visées dans l'article 1er, 2° et 3° et le chapitre IV de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

4° L'Organe de contrôle de l'information policière dans le cadre de ses missions visées dans l'article 71, § 1er.

§ 2. Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van de opdrachten hierboven bedoeld, te verzekeren, is de toegang van de betrokkene tot zijn persoonsgegevens beperkt tot wat voorzien is in de bijzondere wetten.

§ 3. De betrokkene heeft het recht te vragen om zijn onjuiste persoonsgegevens, verwerkt door de in de eerste paragraaf vermelde overheden, te laten verbeteren of verwijderen.

§ 4. De verwerking van persoonsgegevens door de overheden bedoeld in de eerste paragraaf in het kader van de opdrachten bedoeld in dezelfde paragraaf is niet onderworpen aan het toezicht van de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit

TITEL 4

Verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden ter uitvoering van artikel 89 paragrafen 2 en 3 van de verordening

HOOFDSTUK I

Algemene bepalingen

Art. 186

Deze titel bepaalt het uitzonderingsregime ten aanzien van de rechten van betrokkenen bedoeld in artikel 89, paragrafen 2 en 3 van de Verordening.

Voor zover de uitoefening van de in artikel 89, paragrafen 2 en 3 van de Verordening bedoelde rechten de verwezenlijking van de verwerkingen met het oog op archivering in het algemeen belang, het wetenschappelijk of historisch onderzoek of statistische doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en afwijkingen noodzakelijk zijn om die doeleinden te bereiken, worden deze afwijkingen toegepast onder de voorwaarden bepaald door deze titel.

Art. 187

De artikelen 190 tot 203 zijn niet van toepassing mits naleving van een overeenkomstig artikel 40 van de Verordening goedgekeurde gedragscode.

§ 2. Afin de garantir la confidentialité et l'efficacité de l'exécution des missions visées ci-dessus, l'accès par la personne concernée à ses données à caractère personnel est limité à celui qui est prévu dans les lois particulières.

§ 3. La personne concernée a le droit de demander la rectification ou la suppression de ses données à caractère personnel inexactes traitées par les autorités visées au paragraphe premier.

§ 4. Le traitement de données à caractère personnel par les autorités visées au premier paragraphe dans le cadre des missions visées dans le même paragraphe n'est pas soumis au contrôle de l'Autorité de protection des données visée dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

TITRE 4

Traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques en exécution de l'article 89 2 et 3 du règlement

CHAPITRE IER

Dispositions générales

Art. 186

Le présent titre détermine le régime dérogatoire aux droits des personnes concernées visés à l'article 89, paragraphes 2 et 3 du Règlement.

Dans la mesure où l'exercice des droits visés à l'article 89, paragraphes 2 et 3 du Règlement risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques et où des dérogations sont nécessaires pour atteindre ces finalités, ces dérogations sont appliquées dans les conditions déterminées par ce titre.

Art. 187

Les articles 190 à 203 ne s'appliquent pas à condition de respecter un code de conduite approuvé conformément à l'article 40 du Règlement.

Art. 188

Voor de toepassing van deze titel wordt verstaan onder:

1° “derde vertrouwenspersoon”: de natuurlijke persoon of rechtspersoon, de feitelijke vereniging of de overheidsadministratie, niet zijnde de verantwoordelijke voor de verwerking met het oog op archivering of onderzoek of statistische doeleinden, die de gegevens pseudonimiseert;

2° “mededeling van gegevens”: mededeling van gegevens aan geïdentificeerde derde;

3°”verspreiding van gegevens”: bekendmaking van de gegevens, zonder identificatie van de derde;

Art. 189

Deze titel is niet van toepassing op de verwerkingen verricht door de overheden bedoeld in titel 3 van deze wet.

HOOFDSTUK II

Algemene waarborgen

Art. 190

De verwerkingsverantwoordelijke wijst een functionaris voor gegevensbescherming aan indien de verwerking van de persoonsgegevens een hoog risico kan inhouden zoals bedoeld in artikel 35 van de Verordening.

Art. 191

Voorafgaand aan de verzameling, en onverminderd de artikelen 24 en 30 van de Verordening, voegt de verantwoordelijke voor de verwerking met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden volgende elementen toe aan het register van de verwerkingsactiviteiten:

1° de verantwoording van het gebruik van de al dan niet gepseudonimiseerde gegevens;

2° de redenen volgens dewelke de uitoefening van de rechten van de betrokkene de verwezenlijking van de doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren;

Art. 188

Pour l’application du présent titre, on entend par:

1° “tiers de confiance”: la personne physique ou morale, l’association de fait ou l’administration publique autre que le responsable du traitement à des fins d’archive ou de recherche ou statistique, qui pseudonymise les données;

2° “communication des données”: communication des données à des tiers identifiés.

3° “diffusion des données”: publication des données, sans identification des tiers;

Art. 189

Le présent titre ne s’applique pas aux traitements effectués par les autorités visés dans le titre 3 de la présente loi.

CHAPITRE II

Garanties générales

Art. 190

Le responsable du traitement désigne un délégué à la protection des données lorsque le traitement des données à caractère personnel peut engendrer un risque élevé tel que visé par l’article 35 du Règlement.

Art. 191

Préalablement à la collecte, et sans préjudice des articles 24 et 30 du Règlement, le responsable du traitement à des fins de recherche scientifique ou historique ou à des fins statistiques inclut dans le registre des activités de traitement les éléments suivants:

1° la justification de l’utilisation des données pseudonymisées ou non;

2° les motifs selon lesquels l’exercice des droits de la personne concernée risque de rendre impossible ou d’entraver sérieusement la réalisation de la finalité;

3° desgevallend, de gegevensbeschermingseffectbeoordeling wanneer de verwerkingsverantwoordelijke met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden niet geanonimiseerde of niet gepseudonimiseerde gevoelige gegevens, in de zin van artikel 9.1 van de Verordening, verwerkt.

Art. 192

Voorafgaand aan de verzameling, en onverminderd de artikelen 24 en 30 van de Verordening, voegt de verwerkingsverantwoordelijke met het oog op archivering in het algemeen belang volgende elementen toe aan het register van de verwerkingsactiviteiten:

1° de verantwoording van het algemeen belang van de bewaarde archieven;

2° de redenen volgens dewelke de uitoefening van de rechten van de betrokkene de verwezenlijking van de doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren.

HOOFDSTUK III

Gegevensverzameling

Afdeling 1

Gegevensverzameling bij de betrokkene

Art. 193

Onverminderd artikel 13 van de Verordening informeert de verwerkingsverantwoordelijke die persoonsgegevens verzamelt bij de betrokkene hem over:

1° het feit dat de gegevens al dan niet worden geanonimiseerd;

2° de redenen volgens dewelke de uitoefening van de rechten van de betrokkene de verwezenlijking van de doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren.

Afdeling 2

Verdere verwerking van gegevens

Art. 194

Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, sluit de verwerkingsverantwoordelijke

3° le cas échéant, l'analyse d'impact relatif à la protection des données lorsque le responsable du traitement à des fins de recherche scientifique ou historique ou à des fins statistiques traite des données sensibles, dans le sens de l'article 9.1 du Règlement, non anonymisées ou non pseudonymisées .

Art. 192

Préalablement à la collecte, et sans préjudice des articles 24 et 30 du Règlement, le responsable du traitement à des fins archivistiques dans l'intérêt public inclut dans le registre des activités de traitement les éléments suivants:

1° la justification de l'intérêt public des archives conservées;

2° les motifs selon lesquels l'exercice des droits de la personne concernée risque de rendre impossible ou d'entraver sérieusement la réalisation de la finalité.

CHAPITRE III

Collecte de données

Section 1re

Collecte de données auprès de la personne concernée

Art. 193

Sans préjudice de l'article 13 du Règlement, le responsable du traitement qui collecte des données à caractère personnel auprès de la personne concernée, informe celle-ci:

1° du fait que les données seront anonymisées ou non;

2° des motifs selon lesquels l'exercice des droits de la personne concernée risque de rendre impossible ou d'entraver sérieusement la réalisation de la finalité.

Section 2

Traitement ultérieur de données

Art. 194

Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le

een overeenkomst met de verantwoordelijke voor de oorspronkelijke verwerking af.

Lid 1 is niet van toepassing wanneer:

1° de oorspronkelijke verwerking een openbare verwerking van gegevens inhoudt;

2° wanneer de Europese regelgeving, een wet, decreet of ordonnantie:

a) mandaat geeft aan de verwerkingsverantwoordelijke om persoonsgegevens te verwerken met het oog op archivering in het algemeen belang, het wetenschappelijk of historisch onderzoek of statistische doeleinden; en

b) het hergebruik van de verzamelde gegevens voor andere doeleinden verbiedt.

In geval van vrijstelling van het afsluiten van een overeenkomst, informeert de verwerkingsverantwoordelijke de verantwoordelijke van de oorspronkelijke verwerking over de gegevensverzameling.

Art. 195

De overeenkomst of de kennisgeving bedoeld in artikel 194 bepaalt de volgende elementen:

1° in geval van een overeenkomst, de contactgegevens van de verantwoordelijke voor de oorspronkelijke verwerking en van de verantwoordelijke voor de verdere verwerking;

2° de redenen volgens dewelke de uitoefening van de rechten van de betrokkene de verwezenlijking van de doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren.

Art. 196

De overeenkomst of de kennisgeving betreffende de gegevensverzameling worden bij het register van de verwerkingsactiviteiten gevoegd.

Afdeling 3

Anonimisering of pseudonimisering van de gegevens verwerkt met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden

Art. 197

responsable du traitement conclut une convention avec le responsable du traitement initial.

L'alinéa premier ne s'applique pas lorsque:

1° le traitement initial est un traitement public de données;

2° le droit de l'Union européenne, une loi, un décret ou une ordonnance:

a) donne pour mandat au responsable du traitement de traiter des données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques; et

b) interdit la réutilisation des données collectées à d'autres fins.

En cas d'exemption de la conclusion d'une convention, le responsable du traitement informe le responsable du traitement initial de la collecte de données.

Art. 195

La convention ou l'information visée à l'article 194 stipule les éléments suivants:

1° en cas de convention: les coordonnées du responsable du traitement initial et du responsable du traitement ultérieur;

2° les motifs selon lesquels l'exercice des droits de la personne concernée risque de rendre impossible ou d'entraver sérieusement la réalisation de la finalité du traitement ultérieur.

Art. 196

La convention ou l'information sur la collecte de données sont annexés au registre des activités de traitement.

Section 3

Anonymisation ou pseudonymisation des données traitées à des fins de recherche scientifique ou historique ou à des fins statistiques

Art. 197

In het kader van een verwerking van gegevens met het oog op archivering in het algemeen belang of met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden, gebaseerd op een gegevensverzameling bij de betrokkene, gaat de verwerkingsverantwoordelijke over tot de anonimisering of pseudonimisering van de gegevens na de verzameling ervan.

Art. 198

In het kader van een verwerking van gegevens met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden door een verantwoordelijke voor een latere verwerking die dezelfde is als de verantwoordelijke voor de oorspronkelijke verwerking anonimiseert of pseudonimiseert de verwerkingsverantwoordelijke de gegevens voorafgaandelijk aan hun verdere verwerking.

Art. 199

De verwerkingsverantwoordelijke mag de gegevens slechts depseudonimiseren indien dat noodzakelijk is voor het onderzoek of de statistische doeleinden, en desgevallend na advies van de functionaris voor gegevensbescherming.

Art. 200

Onverminderd bijzondere bepalingen, in het kader van een verwerking van gegevens met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden door een verwerkingsverantwoordelijke die verschillend is van de verantwoordelijke voor de oorspronkelijke verwerking, pseudonimiseert of anonimiseert de verantwoordelijke voor de oorspronkelijke verwerking de gegevens voorafgaandelijk aan de mededeling ervan aan de verantwoordelijke voor de verdere verwerking.

De verantwoordelijke voor de verdere verwerking heeft geen toegang tot de sleutels van de pseudonimisering.

Art. 201

§ 1. Onverminderd bijzondere bepalingen, in geval van een verwerking van gegevens met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden waarbij meerdere oorspronkelijke verwerkingen worden gekoppeld, laten de verantwoordelijken voor de initiële verwerkingen voorafgaandelijk aan de mededeling van de gegevens aan de verantwoordelijke

Lors d'un traitement de données à des fins archivistiques dans l'intérêt public ou à des fins de recherche scientifique ou historique ou à des fins statistiques basé sur une collecte de données auprès de la personne concernée, le responsable du traitement anonymise ou pseudonymise les données après leur collecte.

Art. 198

Lors d'un traitement de données à des fins de recherche scientifique ou historique ou à des fins statistiques par un responsable du traitement ultérieur identique au responsable du traitement initial, le responsable du traitement anonymise ou pseudonymise les données préalablement à leur traitement ultérieur.

Art. 199

Le responsable du traitement ne peut dépseudonymiser les données que pour les nécessités de la recherche ou des fins statistiques et, le cas échéant, après avis du délégué à la protection des données.

Art. 200

Sans préjudice de dispositions particulières, lors d'un traitement de données à des fins de recherche scientifique ou historique ou à des fins statistiques par un responsable du traitement distinct du responsable du traitement initial, le responsable du traitement initial anonymise ou pseudonymise les données préalablement à leur communication au responsable du traitement ultérieur.

Le responsable du traitement ultérieur n'a pas accès aux clés de la pseudonymisation.

Art. 201

§ 1er. Sans préjudice de dispositions particulières, lors d'un traitement de données à des fins de recherche scientifique ou historique ou à des fins statistiques couplant plusieurs traitement initiaux, les responsables des traitements initiaux font, préalablement à la communication des données au responsable du traitement ultérieur, anonymiser ou pseudonymiser les données

voor de verdere verwerking, de gegevens anonimiseren of pseudonimiseren door een verantwoordelijke voor de oorspronkelijke verwerking of door een derde vertrouwenspersoon.

§ 2. Onverminderd bijzondere bepalingen, in het kader van een verwerking van gepseudonimiseerde gegevens met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden die verschillende oorspronkelijke verwerkingen, waarvan tenminste één van gevoelige gegevens, aan elkaar koppelt, laten de verantwoordelijken voor de oorspronkelijke verwerkingen voorafgaandelijk aan de mededeling van de gegevens aan de verantwoordelijke voor de verdere verwerking, de gegevens anonimiseren of pseudonimiseren door de verantwoordelijke voor de oorspronkelijke verwerking van gevoelige gegevens of door een derde vertrouwenspersoon.

Enkel de verantwoordelijke voor de oorspronkelijke verwerking die de gegevens heeft gepseudonimiseerd of de derde vertrouwenspersoon heeft toegang tot de pseudonimiseringssleutels.

Art. 202

De derde vertrouwenspersoon mag geen belangenconflict hebben met de verantwoordelijke voor de verdere verwerking.

Art. 203

Indien een functionaris voor gegevensbescherming overeenkomstig artikel 190 werd aangeduid, beveelt deze het gebruik van de pseudonimiseringssleutels aan.

Afdeling 4

Verspreiding van gegevens verwerkt met het oog op archivering in het algemeen belang, het wetenschappelijk of historisch onderzoek of statistische doeleinden

Art. 204

Onverminderd de Europese regelgeving, bijzondere wetten, ordonnanties en decreten die strengere voorwaarden opleggen voor de verspreiding van de gegevens die verwerkt zijn met het oog op archivering in het algemeen belang, het wetenschappelijk of historisch onderzoek of statistische doeleinden, verspreidt de verwerkingsverantwoordelijke geen niet-gepseudonimiseerde gegevens, tenzij:

par l'un des responsables du traitement initial ou par un tiers de confiance.

§ 2. Sans préjudice de dispositions particulières, lors d'un traitement de données à des fins de recherche scientifique ou historique ou à des fins statistiques couplant plusieurs traitements initiaux dont l'un au moins de données sensibles, les responsables des traitements initiaux font, préalablement à la communication des données au responsable du traitement ultérieur, anonymiser ou pseudonymiser les données par le responsable du traitement initial de données sensibles ou par un tiers de confiance.

Seul le responsable du traitement originel qui a pseudonymisé les données ou le tiers de confiance a accès aux clés de pseudonymisation.

Art. 202

Le tiers de confiance ne peut avoir de conflit d'intérêt avec le responsable du traitement ultérieur.

Art. 203

Lorsqu'un délégué à la protection des données a été désigné conformément à l'article 190, celui-ci conseille l'utilisation des clés de pseudonymisation.

Section 4

Diffusion des données traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

Art. 204

Sans préjudice du droit de l'Union européenne, des lois particulières, ordonnances et décrets prévoyant des conditions plus strictes de diffusion pour la diffusion des données traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques le responsable du traitement ne diffuse pas les données non-pseudonymisées sauf lorsque:

1° de betrokkene zijn toestemming heeft verleend; of

1. de gegevens door de betrokkene zelf openbaar zijn gemaakt; of

2° de gegevens nauw samenhangen met het openbare of historische karakter van de betrokkene; of

3° de gegevens nauw samenhangen met het openbare of historische karakter van feiten waarbij de betrokkene betrokken was.

Art. 205

Onverminderd de Europese regelgeving, bijzondere wetten, ordonnanties en decreten die strengere voorwaarden opleggen voor de verspreiding van de gegevens die verwerkt zijn met het oog op archivering in het algemeen belang, het wetenschappelijk of historisch onderzoek of statistische doeleinden, mag de verwerkingsverantwoordelijke gepseudonimiseerde persoonsgegevens verspreiden, uitgezonderd wat betreft de persoonsgegevens bedoeld in artikel 9.1 van de Verordening.

Afdeling 5

Mededeling van de gegevens verwerkt met het oog op archivering in het algemeen belang, het wetenschappelijk of historisch onderzoek of statistische doeleinden

Art. 206

Onverminderd de Europese regelgeving, bijzondere wetten, ordonnanties en decreten die strengere voorwaarden opleggen voor de mededeling, ziet de verwerkingsverantwoordelijke erop toe dat de meegedeelde niet-gepseudonimiseerde gegevens niet gereproduceerd worden wanneer:

1° het om persoonsgegevens gaat in de zin van artikel 9.1 van de Verordening; of

2° de overeenkomst tussen de verantwoordelijke voor de oorspronkelijke verwerking en de verantwoordelijke voor de verdere verwerking zulks verbiedt; of

3° die reproductie de veiligheid van de betrokkene in het gedrang kan brengen.

1° la personne concernée a donné son consentement; ou

2° les données ont été rendues publiques par la personne concernée elle-même; ou

3° les données ont une relation étroite avec le caractère public ou historique de la personne concernée; ou

4° les données ont une relation étroite avec le caractère public ou historique de faits dans lesquelles la personne concernée a été impliquée.

Art. 205

Sans préjudice du droit de l'Union européenne, des lois particulières, ordonnances et décrets prévoyant des conditions plus strictes pour la diffusion des données traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, le responsable du traitement peut diffuser des données à caractère personnel pseudonymisées, à l'exception des données visées à l'article 9.1 du Règlement.

Section 5

Communication des données traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

Art. 206

Sans préjudice du droit de l'Union européenne, des lois particulières, ordonnances et décrets prévoyant des conditions plus strictes pour la communication, le responsable du traitement veille à ce que les données communiquées non-pseudonymisées ne soient pas reproduites lorsque :

1° il s'agit de données à caractère personnel dans le sens de l'article 9.1 du Règlement; ou

2° la convention entre le responsable du traitement initial et le responsable du traitement ultérieur l'interdit; ou

3° cette reproduction risque de nuire à la sécurité de la personne concernée.

Art. 207

De verplichting bedoeld in artikel 206 is niet van toepassing indien:

1° de betrokkene zijn toestemming heeft verleend; of

2° de gegevens door de betrokkene zelf openbaar zijn gemaakt; of

3° de gegevens nauw samenhangen met het openbare of historische karakter van de betrokkene; of

4° de gegevens nauw samenhangen met het openbare of historische karakter van feiten waarbij de betrokkene betrokken was.

TITEL 5

Rechtsmiddelen en vertegenwoordiging van de betrokkenen

HOOFDSTUK I

Vordering tot staking

Art. 208

Onverminderd andere mogelijkheden tot rechterlijk, administratief of buitengerechtelijk beroep, stelt de voorzitter van de rechtbank van eerste aanleg, zitting houdende zoals in kort geding, het bestaan vast van een verwerking die een inbreuk uitmaakt op een wettelijke en reglementaire bepaling betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en beveelt er de staking van.

De voorzitter van de rechtbank van eerste aanleg, zitting houdende zoals in kort geding, neemt kennis van de vorderingen betreffende het door of krachtens de wet verleende recht om kennis te krijgen van persoonsgegevens, alsook van de vorderingen tot rectificatie, tot verwijdering of tot het verbieden van de aanwending van onjuiste persoonsgegevens of die gelet op het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel waarvan de registratie de mededeling of de bewaring verboden is, tegen de verwerking waarvan de betrokkene zich heeft verzet of die langer bewaard werden dan de toegestane duur.

Art. 207

L'obligation visée à l'article 206 n'est pas applicable si:

1° la personne concernée a donné son consentement; ou

2° les données ont été rendues publiques par la personne concernée elle-même; ou

3° les données ont une relation étroite avec le caractère public ou historique de la personne concernée; ou

4° les données ont une relation étroite avec le caractère public ou historique de faits dans lesquelles la personne concernée a été impliquée.

TITRE 5

Voies de recours et représentation des personnes concernées

CHAPITRE I^ER

Action en cessation

Art. 208

Sans préjudice de tout autre recours juridictionnel, administratif ou extrajudiciaire, le président du tribunal de première instance, siégeant comme en référé, constate l'existence d'un traitement constituant une violation aux dispositions légales ou réglementaires concernant la protection des personnes physiques à l'égard du traitement de leur données à caractère personnel et en ordonne la cessation.

Le président du tribunal de première instance, siégeant comme en référé, connaît de toute demande relative au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel, et de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne concernée s'est opposée ou encore qui a été conservée au-delà de la période autorisée.

Art. 209

Vanaf het moment dat de verwerking bedoeld in artikel 208, persoonsgegevens betreft die worden verwerkt in de loop van een opsporingsonderzoek, van een gerechtelijk onderzoek, een strafrechtelijke procedure voor de bodemrechter of een procedure voor de uitvoering van een strafrechtelijk vonnis, behoort de beslissing over de rectificatie, de wissing of het verbod op gebruik van de persoonsgegevens, of de beperking van de verwerking, echter uitsluitend, naar gelang de fase van de procedure, tot het openbaar ministerie of de bevoegde strafrechter.

Art. 210

§ 1. De vordering tot staking wordt ingediend bij verzoekschrift op tegenspraak, overeenkomstig de artikelen 1034*ter* tot 1034*sexies* van het Gerechtelijk wetboek.

§ 2. In afwijking van artikel 624 van het Gerechtelijk wetboek kan de vordering naar keuze van de eiser worden gebracht voor de voorzitter van de rechtbank van eerste aanleg van:

1° de woonplaats of verblijfplaats van de eiser, indien de eiser of minstens één van de eisers de betrokkene is;

2° de woonplaats, verblijfplaats, zetel of plaats van vestiging van de verweerders of één van de verweerders;

3° de plaats of één van de plaatsen waar een deel of het geheel van de verwerking gebeurt.

Indien de verweerder geen woonplaats, verblijfplaats, zetel of plaats van vestiging in België heeft, wordt de vordering gebracht voor de voorzitter van de rechtbank van eerste aanleg te Brussel.

§ 3. De vordering gegrond op artikel 208 wordt ingesteld door:

1° de betrokkene;

2° de bevoegde toezichthoudende autoriteit.

Art. 211

Behoudens de toepassing van andersluidende bepalingen in internationale verdragen die in België van kracht zijn of in het recht van de Europese Unie, en onverminderd hun internationale rechtsmacht op grond

Art. 209

A partir du moment où le traitement visé par l'article 208 concerne des données à caractère personnel traitées lors d'une information, d'une instruction, d'une procédure pénale devant le juge de fond ou d'une procédure d'exécution d'une peine pénale, la décision concernant la rectification, l'effacement ou , l'interdiction d'utiliser les données à caractère personnel, ou la limitation du traitement, appartient toutefois exclusivement, suivant la phase de la procédure, au ministère public ou au juge pénal compétent.

Art. 210

§ 1er. L'action en cessation est introduite par requête contradictoire conformément aux articles 1034*ter* à 1034*sexies* du Code judiciaire.

§ 2. Par dérogation à l'article 624 du Code judiciaire, l'action peut être portée, au choix du demandeur, devant le président du tribunal de première instance:

1° du domicile ou de la résidence du demandeur, si le demandeur, ou au moins un des demandeurs, est la personne concernée;

2° du domicile ou de la résidence, du siège social ou le lieu d'établissement du défendeur ou d'un des défendeurs;

3° du lieu ou d'un des lieux où une partie ou la totalité du traitement est accompli.

Lorsque le défendeur n'a ni domicile, ni résidence, ni siège social ou lieu d'établissement en Belgique, l'action peut être portée devant le président du Tribunal de première instance de Bruxelles.

§ 3. L'action fondée sur l'article 208 est formé à la demande:

1° de la personne concernée;

2° de l'autorité de contrôle compétente.

Art. 211

Sous réserve de l'application de dispositions contraires dans les traités internationaux en vigueur en Belgique ou dans le droit de l'Union européenne, et sans préjudice de leur compétence internationale en

van de bepalingen van het Wetboek van internationaal privaatrecht, hebben de Belgische hoven en rechtbanken in elk geval internationale rechtsmacht voor de in artikel 208 van deze wet bedoelde vorderingen tegen:

1° een verwerkingsverantwoordelijke of een verwerker die op Belgisch grondgebied gevestigd is of een vestiging heeft, wat betreft de verwerking van persoonsgegevens in het kader van de activiteiten van die vestiging, ongeacht de plaats waar de verwerking plaatsvindt;

2° een verwerkingsverantwoordelijke of verwerker die niet op Belgisch grondgebied gevestigd is of een vestiging heeft, wat betreft verwerkingen die gevolgen hebben voor of geheel of gedeeltelijk gericht zijn op betrokkenen die zich op het Belgisch grondgebied bevinden.

Art. 212

De beschikking wordt ter kennis gebracht aan de bevoegde toezichthoudende autoriteit binnen acht dagen na de uitspraak.

Bovendien is de griffier van de rechtbank waar een beroep is ingesteld tegen de in het eerste lid bedoelde beschikking verplicht om de bevoegde toezichthoudende autoriteit onverwijld in te lichten.

Art. 213

De voorzitter van de rechtbank van eerste aanleg kan een termijn toestaan om aan de inbreuk een einde te maken, wanneer de aard van de inbreuk dit nodig maakt. Hij kan de opheffing van het stakingsbevel toestaan wanneer een einde werd gemaakt aan de inbreuk.

Art. 214

§ 1. De voorzitter van de rechtbank van eerste aanleg kan toestaan dat zijn beslissing of de samenvatting die hij opstelt, wordt aangeplakt tijdens de door hem bepaalde termijn, zowel buiten als binnen de betrokken inrichtingen, en kan op de wijze die hij gepast acht bevelen dat zijn beschikking of de samenvatting ervan in kranten of op enige andere wijze wordt bekendgemaakt, dit alles op kosten van de in het ongelijk gestelde partij.

§ 2. De in de eerste paragraaf vermelde maatregelen van openbaarmaking mogen evenwel slechts toegestaan worden indien zij er toe kunnen bijdragen dat de gewraakte daad of de uitwerking ervan ophouden.

vertu des dispositions du Code de droit international privé, les cours et tribunaux belges ont la compétence internationale pour les affaires portées en vertu de l'article 208 de la présente loi contre:

1° un responsable du traitement ou un sous-traitant situé sur le territoire belge ou ayant un établissement, en ce qui concerne le traitement de données à caractère personnel en rapport avec les activités de cet établissement, quel que soit le lieu du traitement;

2° un responsable du traitement ou un sous-traitant qui n'est pas établi ou n'a pas un établissement sur le territoire belge, en ce qui concerne un traitement ayant des conséquences pour ou visant en tout ou en partie des personnes concernées résidant sur le territoire belge.

Art. 212

L'ordonnance est notifiée à l'autorité de contrôle compétente dans les huit jours de la prononciation.

En outre, le greffier de la juridiction devant laquelle un recours est introduit contre l'ordonnance visée à l'alinéa premier est tenu d'en informer sans délai l'autorité de contrôle compétente.

Art. 213

Le président du tribunal de première instance peut accorder un délai pour mettre fin à la violation, lorsque la nature de la violation le nécessite. Il peut accorder la levée de la cessation lorsqu'il a été mis fin à la violation.

Art. 214

§ 1er. Le président du tribunal de première instance peut autoriser l'affichage de sa décision ou du résumé qu'il en rédige, pendant le délai qu'il détermine, aussi bien à l'extérieur qu'à l'intérieur des établissements concernés et ordonner, selon la manière qu'il jugera appropriée, la publication de son ordonnance ou de son résumé par la voie de journaux ou de toute autre manière, le tout aux frais de la partie qui succombe.

§ 2. Les mesures de publicité mentionnées au paragraphe premier ne peuvent toutefois être autorisées que si elles sont de nature à contribuer à la cessation de l'acte incriminé ou de ses effets.

Art. 215

Volgend op de in artikel 208 bedoelde vordering kan de eiser een schadevergoeding vorderen overeenkomstig het contractuele of buitencontractuele aansprakelijkheidsrecht.

Art. 216

Indien onjuiste, onvolledige of niet ter zake dienende persoonsgegevens of persoonsgegevens waarvan de bewaring verboden is, aan derden zijn medegedeeld, of indien een mededeling van persoonsgegevens heeft plaatsgehad na verloop van de tijd waarin de verwerking van die persoonsgegevens toegelaten is, kan de voorzitter van de rechtbank van eerste aanleg gelasten dat de verwerkingsverantwoordelijke, de verwerker, de ontvanger of hun gedelegeerde aan die derden kennis geeft van de beperking van de verwerking of de rectificatie of verwijdering van die persoonsgegevens.

Art. 217

Indien dwingende redenen bestaan om te vrezen dat bewijselementen die kunnen worden aangevoerd ter ondersteuning van een vordering voorzien in dit hoofdstuk worden verheeld, verdwijnen of ontoegankelijk worden gemaakt, gelast de voorzitter van de rechtbank van eerste aanleg op eenzijdig verzoekschrift, in overeenstemming met de artikelen 1026, 5°, en 1027, eerste lid van het Gerechtelijk wetboek, elke maatregel ter voorkoming van die verheling, verdwijning of ontoegankelijkheid.

Art. 219

Onverminderd artikel 209 houden de bepalingen van dit hoofdstuk geen beperking in van de bevoegdheid van de rechtbank van eerste aanleg en van de voorzitter van de rechtbank van eerste aanleg zetelend in kort geding.

HOOFDSTUK II

Vertegenwoordiging van betrokkenen

Art. 220

§ 1. De betrokkene heeft het recht om een orgaan, een organisatie, of een vereniging zonder winstoogmerk de opdracht te geven een klacht namens hem in te dienen en namens hem de administratieve of gerechtelijke beroepen uit te oefenen, hetzij aan de

Art. 215

Suite à l'action visée à l'article 208, le demandeur peut réclamer la réparation de son dommage conformément à la responsabilité contractuelle ou extracontractuelle.

Art. 216

Lorsque des données à caractère personnel inexactes, incomplètes ou non pertinentes, ou des données à caractère personnel dont la conservation est interdite, ont été communiquées à des tiers, ou lorsque une communication de données à caractère personnel a eu lieu après l'expiration de la période durant laquelle la conservation de ces données était autorisée, le président du tribunal de première instance peut ordonner au responsable du traitement, au sous-traitant, au destinataire ou leur délégué d'informer ces tiers de la limitation du traitement, de la rectification ou de la suppression de ces données à caractère personnel.

Art. 217

Lorsqu'il existe des motifs sérieux de craindre la dissimulation, la disparition ou l'inaccessibilité des éléments de preuve qui peuvent être invoqués à l'appui d'une action prévue au présent chapitre, le président du tribunal de première instance, saisi par voie de requête unilatérale, conformément aux articles 1026, 5°, et 1027, alinéa premier du Code judiciaire, ordonne toute mesure de nature à éviter cette dissimulation, disparition ou inaccessibilité.

Art. 219

Sans préjudice de l'article 209, les dispositions du présent chapitre ne limitent pas la compétence du tribunal de première instance et du président du tribunal de première instance siégeant en référé.

CHAPITRE II

Représentation des personnes concernées

Art. 220

§ 1er. La personne concernée a le droit de mandater un organe, une organisation ou une association à but non lucratif, pour qu'il introduise une réclamation en son nom et exerce en son nom les recours administratifs ou juridictionnels soit auprès de l'autorité de contrôle

bevoegde toezichthoudende autoriteit, hetzij aan de rechterlijke macht als bepaald in de bijzondere wetten, het Gerechtelijk wetboek en het Wetboek van Strafvordering.

§ 2. Bij de geschillen voorzien in de eerste paragraaf, moet een orgaan, een organisatie of een vereniging zonder winstoogmerk:

1° op geldige wijze zijn opgericht in overeenstemming met de Belgische wetgeving;

2° rechtspersoonlijkheid bezitten;

3° statutaire doelstellingen van openbaar belang hebben;

4° actief zijn op het gebied van de bescherming van de rechten en vrijheden van de betrokkenen in verband met de bescherming van de persoonsgegevens en dit sedert ten minste drie jaar.

§ 3. Het orgaan, de organisatie of vereniging zonder winstoogmerk bewijst door de voorlegging van haar activiteitenverslagen of van enig ander stuk, dat zijn activiteit minstens drie jaar effectief is geweest, dat het overeenstemt met haar maatschappelijk doel en dat deze activiteit betrekking heeft op de bescherming van persoonsgegevens.

TITEL 6

Sancties

HOOFDSTUK I

Administratieve sancties

Art. 221

§ 1. De corrigerende bevoegdheden van de toezichthoudende autoriteit krachtens artikel 58.2 van de Verordening zijn tevens van toepassing op de artikelen 7, 8, 9, 10, 20, 21, 22, 23 en 24 van titel 1, op de artikelen 31 tot 70 van titel 2 en op titel 4 van deze wet.

Onverminderd bijzondere bepalingen, is het eerste lid niet van toepassing op de verwerkingen van door artikel 26, 7°, b), bedoelde bevoegde overheden in de uitoefening van hun rechterlijke taken.

§ 2. Het artikel 83 van de Verordening is niet van toepassing op de overheid en hun aangestelden of gemachtigden.

compétente soit auprès de l'ordre judiciaire tels que prévus par les lois particulières, le Code judiciaire et le Code d'Instruction criminelle.

§ 2. Dans les litiges prévus au paragraphe premier, un organe, une organisation ou une association sans but lucratif doit nécessairement:

1° être valablement constituée conformément au droit belge;

2° avoir la personnalité juridique;

3° avoir des objectifs statutaires d'intérêt public;

4° être actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel depuis au moins trois ans.

§ 3. L'organe, l'organisation ou l'association sans but lucratif fournit la preuve, par la présentation de ses rapports d'activités ou de toute autre pièce, que son activité est effective depuis au moins trois ans, qu'elle corresponde à son objet social et que cette activité est en relation avec la protection de données à caractère personnel.

TITRE 6

Sanctions

CHAPITRE I^ER

Sanctions administratives

Art. 221

§ 1^er. Les compétences correctrices de l'autorité de contrôle en vertu de l'article 58.2 du Règlement s'appliquent également aux articles 7, 8, 9, 10, 20, 21, 22, 23 et 24 du titre 1^er, aux articles 28 à 70 du titre 2 et au titre 4 de la présente loi.

Sans préjudice de dispositions particulières, l'alinéa premier ne s'applique pas aux traitements effectués par les autorités visées à l'article 26, 7°, b), dans l'exercice de leur fonction juridictionnelle.

§ 2. L'article 83 du Règlement ne s'applique pas aux autorités publiques et leurs préposés ou mandataires.

HOOFDSTUK II

Strafsancties

Art. 222

De verwerkingsverantwoordelijke of de verwerker, zijn aangestelde of gemachtigde, de bevoegde overheid, zoals bedoeld in titels 1 en 2, wordt gestraft met een geldboete van tweehonderdvijftig euro tot vijftienduizend euro wanneer:

1° de persoonsgegevens verwerkt worden zonder wettelijke basis in overeenstemming met artikel 6 van de Verordening en de artikelen 29, § 1, en 33, § 1, van deze wet, inbegrepen de voorwaarden voor de toestemming en verdere verwerking;

2° de persoonsgegevens verwerkt worden in overtreding van de voorwaarden opgelegd door artikel 5 van de Verordening en artikel 28 van deze wet, met enstige nalatigheid of kwaadwillig;

3° de verwerking waartegen ingevolge artikel 21.1 van de Verordening bezwaar is gemaakt, wordt gehandhaafd zonder dwingende wettige redenen;

4° de doorgifte van persoonsgegevens aan een ontvanger in een derde land of een internationale organisatie, gebeurt in overtreding van de waarborgen, voorwaarden of uitzonderingen voorzien in de artikelen 44 tot 49 van de Verordening of de artikelen 66 tot 70 van deze wet met ernstige nalatigheid of kwaadwillig;

5° de door de toezichthoudende autoriteit vastgestelde corrigerende maatregel voor de tijdelijke of definitieve beperking van stromen in overeenstemming met artikel 58.2.f) van de Verordening niet wordt gerespecteerd;

6° de door de toezichthoudende autoriteit vastgestelde corrigerende maatregel in de zin van artikel 58.2.d) van de Verordening niet wordt gerespecteerd;

7° de wettelijke verificatie- en controle-opdrachten van de bevoegde toezichthoudende overheid, haar leden of deskundigen werden belemmerd;

8° weerspannigheid, in de zin van artikel 269 van het Strafwetboek, werd gepleegd ten aanzien van de leden van de toezichthoudende autoriteit;

9° de certificering bedoeld in artikel 42 van de Verordening wordt opgeëist of certificeringszegels voor gegevensbescherming worden openbaar gebruikt, ook al zijn die certificeringen, zegels of merktekens niet afgeleverd door een geaccrediteerde entiteit of worden

CHAPITRE II

Sanctions pénales

Art. 222

Le responsable du traitement ou le sous-traitant, son préposé ou mandataire, l'autorité compétente, visés aux titres 1 et 2, est puni d'une amende de deux cent cinquante euros à quinze mille euros lorsque:

1° les données à caractère personnel sont traitées sans base juridique conformément à l'article 6 du Règlement et aux articles 29, § 1er, et 33, § 1er, de la présente loi, y compris les conditions relatives au consentement et au traitement ultérieur;

2° les données à caractère personnel sont traitées en violation des conditions imposées par l'article 5 du Règlement et à l'article 28 de la présente loi par négligence grave ou avec intention malveillante;

3° le traitement ayant fait l'objet d'une objection conformément à l'article 21.1 du Règlement est maintenu sans raisons juridiques impérieuses;

4° le transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, effectué en violation des garanties, conditions ou exceptions prévues dans les articles 44 à 49 du Règlement ou des articles 66 à 70 de la présente loi par négligence grave ou avec intention malveillante;

5° la mesure correctrice adoptée par l'autorité de contrôle visant la limitation temporaire ou définitive des flux conformément à l'article 58.2.f) du Règlement n'est pas respectée;

6° la mesure correctrice adoptée par l'autorité de contrôle au sens de l'article 58.2.d) du Règlement n'est pas respectée;

7° il a été fait obstacle aux missions légales de vérification et de contrôle de l'autorité de contrôle compétente, ses membres ou ses experts;

8° de la rébellion, dans le sens de l'article 269 du Code pénal, a été commise à l'encontre des membres de l'autorité de contrôle;

9° la certification visée à l'article 42 du Règlement est revendiquée ou des sceaux de certification en matière de protection des données sont utilisées publiquement alors que ces certifications, labels ou marques n'ont pas été délivrés par une entité accréditée ou ceux-ci

ze gebruikt nadat de geldigheid van de certificering, de zegel of het merkteken is verlopen;

10° de certificering bedoeld in artikel 42 van de Verordening is verkregen op basis van valse documenten of onjuiste documenten;

11° taken worden uitgevoerd als een certificeringsorgaan, ook al is deze niet geaccrediteerd door de bevoegde nationale accreditatie-instantie;

12° het certificeringsorgaan niet voldoet aan de beginselen en taken waaraan het onderworpen is, zoals bepaald in de artikelen 42 en 43 van de Verordening;

13° de taken van het in artikel 41 van de Verordening bedoelde orgaan worden uitgevoerd zonder accreditatie van de bevoegde toezichthoudende autoriteit;

14° het geaccrediteerde orgaan bedoeld in artikel 41 van de Verordening niet de passende maatregelen heeft genomen in geval van een inbreuk op de gedragscode zoals bedoeld in artikel 41.4 van de Verordening.

Art. 223

Met een geldboete van vijfhonderd euro tot dertigduizend euro wordt de verwerkingsverantwoordelijke bedoeld in titel 1, de verwerker of de persoon die handelt onder hun gezag gestraft die:

1° de betrokkene, als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, heeft ingelicht over het bestaan van een persoonsgegeven dat hem aangaat dat afkomstig is van een overheid bedoeld in de titel 3 van deze wet in overtreding van artikel 11, terwijl hij de oorsprong van het gegeven kende en hij zich niet bevond in één van de gevallen bedoeld in 11, § 2, 1° of 2°;

2° de betrokkene, als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, heeft ingelicht dat een overheid bedoeld in titel 3 de ontvanger is van één van zijn persoonsgegevens in overtreding van artikel 12.

Art. 224

Met een geldboete van tweehonderd tot tienduizend euro wordt gestraft elk lid of elk personeelslid van de bevoegde toezichthoudende autoriteit of elke deskundige die de verplichting tot vertrouwelijkheid waartoe hij is gehouden heeft geschonden.

sont utilisés après que la validité de la certification, du sceau ou de la marque a expiré;

10° la certification visée à l'article 42 du Règlement a été obtenue sur la base de faux documents ou documents erronés;

11° des tâches sont exécutées en tant qu'organisme de certification alors que celui-ci n'a pas été accrédité par l'organisme national d'accréditation compétent;

12° l'organisme de certification ne se conforme pas aux principes et aux tâches auxquels il est soumis tel que prévu aux articles 42 et 43 du Règlement;

13° les tâches de l'organisme visée à l'article 41 du Règlement sont exécutées sans agrément par l'autorité de contrôle compétente;

14° l'organisme agréé visé à l'article 41 du Règlement n'a pas pris les mesures appropriées en cas de violation du code de conduite tel que visé à l'article 41.4 du Règlement.

Art. 223

Est puni d'une amende de cinq cents euros à trente mille euros, le responsable du traitement visé au titre 1er, le sous-traitant ou la personne agissant sous leur autorité qui:

1° a, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, informé la personne concernée de l'existence d'une donnée à caractère personnel la concernant émanant d'une autorité visée au titre 3 de la présente loi en violation de l'article 11, alors qu'il connaissait l'origine de la donnée et qu'il ne se trouvait pas dans un des cas visés a l'article 11, § 2, 1° ou 2°;

2° a, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, informé la personne concernée qu'une autorité visée au titre 3 est destinataire d'une de ses données à caractère personnel en violation de l'article 12.

Art. 224

Est puni d'une amende de deux cents euros à dix mille euros, tout membre ou tout membre du personnel de l'autorité de contrôle compétente ou tout expert qui a violé l'obligation de confidentialité à laquelle il est astreint.

Art. 225

Bij veroordeling wegens een misdrijf omschreven in de artikelen 222 of 223, kan de rechtbank bevelen dat het vonnis in zijn geheel of bij uittreksel wordt opgenomen in een of meerdere dagbladen op de wijze die zij bepaalt, zulks op kosten van de veroordeelde.

Art. 226

De verwerkingsverantwoordelijke of de persoon die handelt onder het gezag van de overheid bedoeld in titel 3 of van diens verwerker, die als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, één van de verplichtingen van vertrouwelijkheid en veiligheid, bedoeld in de artikelen 83 tot 86, 116 tot 119, 149 tot 152 en 177 tot 178 niet heeft nageleefd, wordt gestraft met een geldboete van honderd euro tot tienduizend euro.

Art. 227

Met een geldboete van honderd euro tot twintigduizend euro wordt gestraft:

1° de verwerkingsverantwoordelijke, de verwerker, de persoon die handelt onder het gezag van de overheid bedoeld in titel 3 of van de verwerker of de aangestelde die, als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, de persoonsgegevens verwerkt buiten de gevallen bedoeld in artikelen 74, 108, 140 en 170;

2° de verwerkingsverantwoordelijke, de verwerker of de aangestelde die persoonsgegevens verwerkt met overtreding van de voorwaarden voor de verwerking opgelegd door artikelen 75, 109, 141 en 170 en de persoon die handelt onder het gezag van de overheid bedoeld in titel 3 of van diens verwerker, die als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, gegevens verwerkt in overtreding van de voorwaarden opgelegd door artikel 75, 109, 141 en 170;

3° hij die, om een persoon te dwingen hem zijn instemming te geven met de verwerking van de hem betreffende persoonsgegevens, jegens die persoon gebruik maakt van feitelijkheden, geweld, bedreigingen, giften of beloften;

4° hij die persoonsgegevens doorgeeft, doet of laat doorgeven, als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, naar een land dat geen lid is van de Europese Unie of een internationale

Art. 225

En condamnant du chef d'infraction aux articles 222 ou 223, le tribunal peut ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'il détermine, aux frais du condamné.

Art. 226

Est puni d'une amende de cent euros à dix mille euros, le responsable du traitement ou la personne agissant sous l'autorité d'une autorité visée au titre 3 ou de son sous-traitant qui, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, n'a pas respecté une des obligations de confidentialité et de sécurité visées aux articles 83 à 86, 116 à 119, 149 à 152 et 177 à 178.

Art. 227

Est puni d'une amende de cent euros à vingt mille euros:

1° le responsable du traitement, le sous-traitant, la personne agissant sous l'autorité de l'autorité visée au titre 3 ou du sous-traitant ou le mandataire qui, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, qui traite des données à caractère personnel en dehors des cas prévus aux articles 74, 108, 140 et 170;

2° le responsable du traitement, le sous-traitant ou le mandataire qui traite des données à caractère personnel en infraction aux conditions imposées par les articles 75, 109, 141 et 170 et la personne agissant sous l'autorité d'une autorité visée au titre 3 ou du sous-traitant qui, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, traite des données à caractère personnel en infraction aux conditions imposées par les articles 75, 109, 141 et 170;

3° quiconque qui, pour contraindre une personne à lui donner son autorisation au traitement de données à caractère personnel la concernant, a usé à son égard de voies de fait, de violence ou menaces, de dons ou de promesses;

4° quiconque a transféré, fait ou laissé transférer, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, des données à caractère personnel vers un pays non membre de l'Union

organisatie zonder dat is voldaan aan de vereisten opgelegd door artikelen 93, 94, 126, 127, 159, 160, 182 en 183;

5° elke persoon die als gevolg van zijn nalatigheid voor zover deze ernstig is, of kwaadwillig, toegang heeft tot persoonsgegevens bedoeld in artikelen 99, 132 en 162 voor historische, wetenschappelijke of statistische doeleinden, en die deze gegevens verwerkt in overtreding van de artikelen 102, 135, 165 of 104, 137, 167.

Art. 228

Onverminderd bijzondere bepalingen, is de verwerkingsverantwoordelijke, de verwerker, of zijn vertegenwoordiger in België burgerrechtelijk aansprakelijk voor de betaling van de boeten waartoe zijn aangestelde of gemachtigde is veroordeeld.

Art. 229

§ 1. Met betrekking tot de in artikelen 222 en 223 bedoelde inbreuken kunnen de bevoegde toezichthoudende autoriteit en het College van procureurs-generaal een protocol afsluiten voor het vastleggen van de werkafspraken tussen de toezichthoudende autoriteit en het openbaar ministerie in dossiers die betrekking hebben op feiten waarvoor de wetgeving zowel in de mogelijkheid van een administratieve geldboete als in de mogelijkheid van een strafsanctie voorziet.

De Koning legt, bij een in Ministerraad overlegd besluit, de nadere modaliteiten en het model vast van dit protocolakkoord.

Dit protocolakkoord leeft alle wettelijke bepalingen na die met name betrekking hebben op de procedures voorzien voor de overtreders en kan niet afwijken van de rechten van de overtreders.

Het protocolakkoord wordt in het *Belgisch Staatsblad* en op de internetsite van de bevoegde toezichthoudende autoriteit bekendgemaakt.

§ 2. Bij gebrek aan een protocolakkoord en voor de inbreuken bedoeld in artikelen 222 en 223 beschikt de procureur des Konings over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het origineel proces-verbaal, om aan de bevoegde toezichthoudende autoriteit mee te delen dat een opsporingsonderzoek of een gerechtelijk onderzoek werd opgestart of vervolging werd ingesteld. Deze mededeling doet de mogelijkheid vervallen voor de toezichthoudende autoriteit om haar corrigerende bevoegdheden uit te oefenen.

européenne ou vers une organisation internationale sans qu'il ait été satisfait aux exigences prévues aux articles 93, 94, 126, 127, 159, 160, 182 et 183;

5° toute personne qui, de sa propre négligence, pour autant qu'elle soit grave, ou avec une intention malveillante, a accès à des données à caractère personnel visées aux articles 99, 132 et 162 à des fins historiques, scientifiques ou statistiques, et qui traite ces données en violation des articles 102, 135, 165 ou 104, 137, 167.

Art. 228

Sans préjudice de dispositions particulières, le responsable du traitement, le sous-traitant, ou son représentant en Belgique est civilement responsable du paiement des amendes auxquelles son préposé ou mandataire a été condamné.

Art. 229

§ 1er. En ce qui concerne les infractions visées aux articles 222 et 223, l'autorité de contrôle compétente et le Collège des Procureurs généraux peuvent conclure un protocole régissant les accords de travail entre l'autorité de contrôle et le ministère public dans des dossiers portant sur des faits pour lesquels la législation prévoit aussi bien la possibilité d'une amende administrative que la possibilité d'une sanction pénale.

Le Roi fixe les modalités et le modèle de ce protocole par arrêté délibéré en Conseil des ministres.

Ce protocole d'accord respecte l'ensemble des dispositions légales concernant notamment les procédures prévues pour les contrevenants et ne peut déroger aux droits de ceux-ci.

Le protocole d'accord est publié au *Moniteur belge* et sur le site internet de l'autorité de contrôle compétente.

§ 2. A défaut de protocole d'accord et pour les infractions visées aux articles 222 et 223 le procureur du Roi dispose d'un délai de deux mois, à compter du jour de la réception de l'original du procès-verbal, pour communiquer à l'autorité de contrôle compétente qu'une information ou une instruction a été ouverte ou que des poursuites ont été entamées. Cette communication éteint la possibilité pour l'autorité de contrôle d'exercer ses mesures correctrices.

De bevoegde toezichthoudende autoriteit kan geen sanctie opleggen vóór het verstrijken van deze termijn. Bij gebrek aan een mededeling vanwege de procureur des Konings binnen twee maanden, kunnen de feiten enkel nog administratiefrechtelijk worden bestraft.

Art. 230

Alle bepalingen van Boek I van het Strafwetboek, met inbegrip van hoofdstuk VII en artikel 85, worden toegepast op de misdrijven, omschreven bij deze wet of bij de uitvoeringsbesluiten ervan.

TITEL 7

Het controleorgaan op de politionele informatie

HOOFDSTUK I

Samenstelling en statuut van de leden en van de dienst onderzoeken

Art. 231

§ 1. Het Controleorgaan op de politionele informatie, hierna aangeduid als "Controleorgaan" is samengesteld uit drie werkende leden, waaronder een voorzitter, die hun functies voltijds uitoefenen. De toezichthoudende autoriteit is naast de Voorzitter, die een magistraat moet zijn, samengesteld uit een magistraat van het openbaar ministerie en een expert.

Behoudens één van de leden die functioneel tweetalig dient te zijn, bestaat het Controleorgaan uit een gelijk aantal Nederlandstalige en Franstalige leden. De leden moeten een functionele kennis hebben van de tweede landstaal en van het Engels. Ten minste één lid moet ook een functionele kennis hebben van het Duits. Zij worden allen benoemd door de Kamer van volksvertegenwoordigers, die hen ook kan afzetten wanneer de in artikel 232 bepaalde voorwaarden in hun hoofde niet meer vervuld zijn of wegens ernstige redenen. Zij kunnen evenwel niet van hun mandaat worden ontheven voor meningen die zij uiten of daden die zij stellen bij het vervullen van hun functies.

§ 2. De leden van het Controleorgaan worden op grond van hun competentie, hun ervaring, hun onafhankelijkheid en hun moreel gezag door de Kamer van volksvertegenwoordigers voor een termijn van zes jaar, éénmaal hernieuwbaar, aangesteld.

L'autorité de contrôle compétente ne peut infliger une sanction avant l'échéance de ce délai. A défaut de communication du Procureur du Roi dans les deux mois, les faits ne peuvent être sanctionnés que de manière administrative.

Art. 230

Toutes les dispositions du livre 1er du Code pénal, y compris le chapitre VII et l'article 85, sont applicables aux infractions prévues par la présente loi ou par les arrêtés pris pour son exécution.

TITRE 7

L'organe de contrôle de l'information policière

CHAPITRE IER

Composition et statut des membres et du service d'enquête

Art. 231

§ 1er. L'Organe de contrôle de l'information policière, ci-après dénommé "Organe de contrôle", se compose de trois membres effectifs dont un président, lesquels exercent leurs fonctions à temps plein. Outre le président qui doit être un magistrat, l'Autorité de contrôle se compose d'un magistrat du ministère public, et d' un expert.

Un des membres qui doit être fonctionellement bilingue exclu, l'organe de contrôle comprend autant de membres d'expression française que de membres d'expression néerlandaise parmi ses membres. Les membres doivent avoir une connaissance fonctionnelle de la deuxième langue nationale et de l'anglais. Au moins un membre doit aussi posséder une connaissance fonctionnelle de l'allemand. Tous sont nommés par la Chambre des représentants qui ne peut les démettre de leurs fonctions que si les conditions prévues à l'article 232 ne sont plus rencontrées ou pour motifs graves. Ils ne peuvent être relevés de leurs fonctions en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent pour remplir leurs fonctions.

§ 2. Les membres de L'Organe de contrôle sont nommés, sur base de leur compétence, de leur expérience, de leur indépendance et de leur autorité morale par la Chambre des représentants pour un terme de six ans renouvelable une fois.

Deze termijn begint te lopen vanaf hun eedaflegging. Na afloop van deze termijn, blijven de leden hun functie uitoefenen tot de eedaflegging van hun opvolger.

De leden mogen geen bij verkiezing verleend openbaar mandaat uitoefenen. Zij mogen geen openbare of particuliere betrekking of activiteit uitoefenen die de onafhankelijkheid of de waardigheid van het ambt in gevaar zou kunnen brengen of die onverenigbaar is met hun taken.

§ 3. Alvorens hun ambt te aanvaarden leggen de leden van het Controleorgaan in handen van de Voorzitter van de Kamer van volksvertegenwoordigers de bij artikel 2 van het decreet van 20 juli 1831 voorgeschreven eed af.

§ 4. Het Controleorgaan is daarnaast samengesteld uit een Dienst Onderzoeken, hierna genoemd "de Dienst Onderzoeken", die bestaat uit drie werkende leden die hun functies voltijds uitoefenen, waaronder twee leden van de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus, en een expert.

De Dienst Onderzoeken hangt exclusief af van het Controleorgaan. Het Controleorgaan oefent het gezag uit over de Dienst Onderzoeken, vertrouwt hem opdrachten toe en ontvangt een verslag over alle opdrachten die worden uitgevoerd.

§ 5. De leden van de Dienst Onderzoeken worden benoemd door het Controleorgaan die hen ook kan afzetten wanneer de in artikel 232 bepaalde voorwaarden in hun hoofde niet meer vervuld zijn of wegens ernstige redenen. De leden van de Dienst Onderzoeken worden voor een mandaat met een vernieuwbare termijn van zes jaar benoemd, op grond van hun competentie.

§ 6. Alvorens hun ambt te aanvaarden, leggen de leden van de Dienst Onderzoeken in handen van de Voorzitter van het Controleorgaan de bij artikel 2 van het decreet van 20 juli 1831 voorgeschreven eed af.

Art. 232

§ 1. Op het ogenblik van hun benoeming moeten de leden van het Controleorgaan de volgende algemene voorwaarden vervullen:

1° Belg zijn;

Ce délai prend cours à partir de la prestation de serment. A l'issue de ce terme, les membres continuent à exercer leurs fonctions jusqu'à la prestation de serment de leur successeur.

Les membres ne peuvent occuper aucun mandat public conféré par élection. Ils ne peuvent exercer d'emploi ou d'activité public(que) ou privé(e) qui pourrait mettre en péril l'indépendance ou la dignité de la fonction ou qui est incompatible avec leur fonction.

§ 3. Avant d'entrer en fonction, les membres de l'Organe de contrôle prêtent, entre les mains du président de la Chambre des représentants, le serment prescrit par l'article 2 du décret du 20 juillet 1831.

§ 4. L'Organe de contrôle est, en outre, composé d'un service enquête ci-après dénommé "service d'enquête", lequel est composé de trois membres effectifs lesquels exercent leurs fonctions à temps plein, dont deux membres des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, et d'un expert.

Le service d'enquête relève de l'autorité exclusive de l'Organe de contrôle. L'Organe de controle exerce son autorité sur le service d'enquête, lui confie des missions et reçoit des rapports sur toutes les missions qui sont effectuées.

§ 5. Les membres du service d'enquête de l'Organe de contrôle sont nommés par l'Organe de contrôle, lequel peuvent également les démettre de leurs fonctions que si les conditions prévues à l'article 232 ne sont plus rencontrées ou pour motifs graves. Les membres du service d'enquête de l'Organe de contrôle sont nommés, sur base de leurs compétences, par l'Organe de contrôle pour un mandat renouvelable de six ans.

§ 6. Avant d'entrer en fonction, les membres du service d'enquête prêtent, entre les mains du président de l'Organe de contrôle, le serment prescrit par l'article 2 du décret du 20 juillet 1831.

Art. 232

§ 1er. Au moment de leur nomination, les membres de l'Organe de contrôle doivent remplir les conditions suivantes:

1° être belge;

2° genieten van de burgerlijke en politieke rechten;

3° van onberispelijk gedrag zijn;

4° het bewijs leveren van hun deskundigheid in het domein van de bescherming van persoonsgegevens en van de politionele informatiehuishouding;

5° houder zijn van een veiligheidsmachtiging van het niveau “zeer geheim” verleend overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

6° geen functie uitoefenen in een beleidscel van een federale of regionale minister.

§ 2. Op het ogenblik van hun benoeming moeten de Voorzitter en de magistraat van het openbaar ministerie een relevante ervaring of deskundigheid hebben van minstens tien jaar in het domein van de bescherming van persoonsgegevens en de politionele informatiehuishouding.

§ 3. Op het ogenblik van zijn benoeming moet het lid-expert van het Controleorgaan aan de volgende specifieke voorwaarden voldoen:

1° tien jaar ervaring hebben als deskundige in het domein van de bescherming van persoonsgegevens en de politionele informatiehuishouding;

2° houder zijn van een diploma licenciaat of master in de rechten dat toegang verleent tot de betrekkingen van niveau A in de Rijksbesturen.

§ 4. Ingeval een mandaat van lid van het Controleorgaan om welke reden ook openvalt, wordt overgegaan tot de vervanging ervan voor de nog resterende duur van het mandaat.

§ 5. Op het ogenblik van hun benoeming moeten de leden van de Dienst Onderzoeken de volgende algemene voorwaarden vervullen:

1° Belg zijn;

2°genieten van de burgerlijke en politieke rechten;

3° van onberispelijk gedrag zijn;

4° het bewijs leveren van hun deskundigheid in het domein van de bescherming van persoonsgegevens en van de politionele informatiehuishouding;

2° jouir des droits civils et politiques;

3° être de conduite irréprochable;

4° justifier d’une expertise en matière de protection des données à caractère personnel et en matière de gestion de l’information policière;

5° être titulaire d’une habilitation de sécurité du niveau “très secret” octroyée en vertu de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

6° ne pas exercer une fonction dans une cellule stratégique ministérielle fédérale ou régionale.

§ 2. Au moment de leur nomination, le président et le magistrat du ministère public doit justifier d’une expérience pertinente ou d’une expertise d’au moins dix ans en tant qu’expert en matière de protection des données à caractère personnel et de gestion de l’information policière.

§ 3. Au moment de sa nomination, l’expert de l’Organe de contrôle remplit, en outre, les conditions spécifiques suivantes:

1° justifier d’une expérience de dix ans en tant qu’expert en matière de protection des données à caractère personnel et de gestion de l’information policière;

2° être titulaire d’un diplôme de licencié ou de master en droit donnant accès aux emplois de niveau A dans les administrations de l’État.

§ 4. En cas de vacance d’un mandat de membre de l’Organe de contrôle, et ce, quelle qu’en soit la cause, il est procédé à son remplacement pour la durée du mandat restant à courir.

§ 5. Au moment de leur nomination, les membres du service d’enquête remplissent les conditions suivantes:

1° être belge;

2° jouir des droits civils et politiques;

3° être de conduite irréprochable;

4° justifier d’une expertise en matière de protection des données à caractère personnel et en matière de gestion de l’information policière;

5° houder zijn van een veiligheidsmachtiging van het niveau “zeer geheim” verleend overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

6° geen functie uitoefenen in een beleidscel van een federale of regionale minister.

§ 6. Op het ogenblik van hun benoeming moeten daarenboven, voor de personeelsleden van de politiediensten die lid zijn van de dienst onderzoeken, de volgende specifieke voorwaarden zijn vervuld:

1° ten minste tien jaar dienstanciënniteit hebben en ten minste bekleed zijn met de graad van commissaris van politie of van niveau A zijn indien het een personeelslid betreft van het administratief en logistiek kader;

2° geen eindevaluatie “onvoldoende” hebben gekregen tijdens de vijf jaar voorafgaand aan de indiening van de kandidaatstelling, noch een niet uitgewiste zware tuchtstraf hebben opgelopen;

3° een ervaring van minimum twee jaar bezitten inzake de verwerking van politionele informatie of de bescherming van persoonsgegevens.

§ 7. Op het ogenblik van hun benoeming moet de experten van de Dienst Onderzoeken bovendien aan de volgende specifieke voorwaarden voldoen:

1° vijf jaar ervaring hebben als deskundige in het domein van de bescherming van persoonsgegevens en de politionele informatiehuishouding;

2° houder zijn van een diploma licenciaat of master dat toegang verleent tot de betrekkingen van niveau A in de Rijksbesturen.

Art. 233

§ 1. Het Controleorgaan stelt zijn huishoudelijk reglement op en kan zijn interne organisatie bepalen. Het huishoudelijk reglement wordt goedgekeurd door de Kamer van volksvertegenwoordigers.

De voorzitter leidt, met inachtneming van de collegialiteit, de vergaderingen van het Controleorgaan en zorgt voor het dagelijks beheer van de werkzaamheden. Hij ziet toe op de goede werking van het Controleorgaan, op de goede uitvoering van de taken ervan, alsook op de toepassing van het huishoudelijk reglement. Het

5° être titulaire d’une habilitation de sécurité du niveau “très secret” octroyée en vertu de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

6° ne pas exercer une fonction dans une cellule stratégique ministérielle fédérale ou régionale.

§ 6. Au moment de leur nomination, les membres du personnel des services de police, qui sont membres du service d’enquête, remplissent, en outre, les conditions spécifiques suivantes:

1° compter au moins dix ans d’ancienneté de service et être au moins revêtu du grade de commissaire de police ou de niveau A lorsqu’ il s’agit d’un membre du personnel du cadre administratif et logistique;

2° ne pas avoir fait l’objet d’une évaluation finale qualifiée “insuffisante” au cours des cinq années qui ont précédées l’introduction de la candidature, ni avoir encouru une sanction disciplinaire lourde non effacée;

3° justifier d’une expérience d’au moins deux ans en matière de traitement de l’information policière ou de protection des données à caractère personnel.

§ 7. Au moment de leur nomination, les experts membres du service d’enquête doivent en outre remplir les conditions spécifiques suivantes:

1° justifier d’une expérience de cinq ans en tant qu’expert en matière de protection des données à caractère personnel et de gestion de l’information policière;

2° être titulaire d’un diplôme de licencié ou master donnant accès aux emplois de niveau A dans les administrations de l’État.

Art. 233

§ 1er. L’Organe de contrôle élabore son règlement d’ordre intérieur et peut définir sa propre organisation. Le règlement d’ordre intérieur est soumis à l’approbation de la Chambre des représentants.

Le président assure, dans le respect de la collégialité, la direction des réunions de L’Organe de contrôle et la gestion journalière des activités. Il veille au bon fonctionnement de l’Organe de contrôle, à la bonne exécution de ses missions ainsi qu’à l’application du règlement d’ordre intérieur. Le règlement d’ordre intérieur précité

voormelde huishoudelijk reglement bepaalt welk lid de taken van de voorzitter overneemt, wanneer hij afwezig of verhinderd is.

§ 2. De leden van het Controleorgaan krijgen noch vragen binnen de perken van hun bevoegdheden op directe of indirecte wijze van niemand instructies. Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarbij zij een persoonlijk of rechtstreeks belang hebben of waarbij hun bloed- of aanverwanten tot en met de vierde graad een persoonlijk of rechtstreeks belang hebben.

§ 3. De leden van het Controleorgaan en haar personeelsleden zijn niet burgerlijk aansprakelijk voor hun beslissingen, handelingen of gedragingen in de uitoefening van de wettelijke opdrachten van de toezichthoudende autoriteit behalve in geval van bedrog of zware fout.

§ 4. De leden van het Controleorgaan zijn, onverminderd hun wettelijk opdrachten en bevoegdheden, tijdens en na de uitoefening van hun respectieve mandaat, tot geheimhouding verplicht ten aanzien van de feiten, handelingen of inlichtingen waarvan zij uit hoofde van hun functie kennis hebben gehad. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Art. 234

§ 1. De leden van het Controleorgaan genieten hetzelfde statuut als de raadsheren van het Rekenhof. De wedderegeling van de raadsheren van het Rekenhof, vervat in de wet van 21 maart 1964 betreffende de wedden van de leden van het Rekenhof, zoals gewijzigd bij de wetten van 14 maart 1975 en 5 augustus 1992, is van toepassing op de leden van de toezichthoudende autoriteit. Hun reeds verworven geldelijke anciënniteit wordt in aanmerking genomen en zij hebben ook recht op de tussentijdse verhogingen in dit barema.

De leden van de Dienst Onderzoeken genieten een wedde zoals bepaald in barema A3 van het statuut van de ambtenaren van de Gegevensbeschermingsautoriteit opgericht door de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Hun reeds verworven geldelijke anciënniteit wordt in aanmerking genomen en zij hebben ook recht op de tussentijdse verhogingen in dit barema. Zij genieten alle geldelijke voordelen die voorzien zijn in het statuut van de ambtenaren en in de organieke teksten van de Gegevensbeschermingsautoriteit.

détermine quel membre assume les tâches du président en cas d'absence ou d'empêchement de ce dernier.

§ 2. Les membres de l'Organe de contrôle ne reçoivent ni cherchent dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne. Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au quatrième degré ont un intérêt personnel ou direct.

§ 3. Les membres de l'Organe de contrôle et les membres de son personnel n'encourent aucune responsabilité civile en raison de leurs décisions, actes ou comportements dans l'exercice des missions légales de l'autorité de contrôle sauf en cas de dol ou de faute lourde.

§ 4. Les membres de l'Organe de contrôle sont tenus, durant et après l'exercice de leur mandat et contrat respectifs, de garder le secret à égard des faits, actes ou renseignements dont ils ont eu connaissance en raison de leurs fonctions. Toute violation du secret professionnel est punie conformément à l'article 458 du Code pénal.

Art. 234

§ 1er. Les membres de l'Organe de contrôle jouissent d'un statut identique à celui des conseillers de la Cour des comptes. Les règles régissant le statut pécuniaire des conseillers de la Cour des comptes, contenues dans la loi du 21 mars 1964 relative aux traitements des membres de la Cour des comptes, telle qu'elle a été modifiée par les lois des 14 mars 1975 et 5 août 1992, sont applicables aux membres de l'autorité de contrôle. Leur ancienneté pécuniaire déjà acquise est prise en considération et ils ont également droit aux augmentations intercalaires dans ce barème.

Les membres du service d'enquête de l'Organe de contrôle bénéficient d'un traitement tel que défini dans le barème A3 du statut des agents de l'autorité de protection de données crée par la loi du 3 décembre 2017 portant la création de l'Autorité de protection de données. Leur ancienneté pécuniaire déjà acquise est prise en considération et ils ont également droit aux augmentations intercalaires dans ce barème. Tous les avantages pécuniaires du statut des agents de l'Autorité de protection de données s'appliquent à eux.

De leden van het Controleorgaan en de leden van de Dienst Onderzoeken genieten de pensioenregeling die van toepassing is op de ambtenaren van het algemeen bestuur. Deze pensioenen zijn ten laste van de Staatskas. Het mandaat van de leden van het Controleorgaan en van de leden van de Dienst Onderzoeken wordt inzake pensioenen gelijkgesteld met een vaste benoeming.

§ 2. De leden van de Dienst Onderzoeken die lid zijn van de politiediensten kunnen na de beëindiging van hun mandaat in de toezichthoudende autoriteit terugkeren naar hun korps van oorsprong in het statuut dat zij hadden op het moment van hun benoeming in het Controleorgaan. Zij behouden niettemin tijdens hun mandaat , in de dienst of het bestuur waaruit zij afkomstig zijn, hun rechten op bevordering en op weddeverhoging. Het personeelslid van de politiediensten dat lid is van de Dienst Onderzoeken en dat voor een betrekking in de politiediensten geschikt wordt bevonden, heeft voorrang op alle andere kandidaten met betrekking tot de toewijzing van de betrekking, zelfs indien deze laatsten over een voorrang beschikken krachtens de wet. Deze voorrang geldt gedurende het laatste jaar van de zes jaren in dienst van het Controleorgaan.

Onder dezelfde voorwaarden wordt een voorrangstermijn van twee jaar toegekend bij de aanvang van het tiende jaar dat men in dienst is bij het Controleorgaan.

§ 3. Aan het lid van het Controleorgaan die magistraat in de rechterlijke orde, ambtenaar van het openbaar ambt of lid van de politiediensten is wordt een verlof voor opdracht van algemeen belang verleend voor de duur van het mandaat. Zij behouden, tijdens hun mandaat in het Controleorgaan of de Dienst Onderzoeken, in de dienst of het bestuur waaruit zij afkomstig zijn hun rechten op bevordering en op weddeverhoging.

Art. 235

§ 1. Het Controleorgaan beschikt over een secretariaat bestaande uit een directie-assistent, een jurist en een informaticus. Deze personeelsleden genieten de hiernavolgende wedde zoals voorzien in het statuut van de ambtenaren van het federaal openbaar ambt:

— Directie-assistent: barema A1

— Jurist: barema A3

— Informaticus: barema A3

Les membres de l'Organe de contrôle et les membres du service d'enquête bénéficient du régime de pension applicable aux fonctionnaires de l'administration générale. Ces pensions sont à charge du Trésor public. Le mandat des membres de l'Organe de contrôle et du service enquête sont assimilés, en matière de pensions, à une nomination à titre définitif.

§ 2. Les membres du service d'enquête qui sont membres des services de police peuvent, après la fin de leur mandat, réintégrer leur corps de police d'origine, dans le statut qu'ils avaient au moment de leur nomination à l'Organe de contrôle. Ils conservent néanmoins pendant leur mandat, dans le service ou dans l'administration dont ils sont originaires, leurs droits à la promotion et aux augmentations de traitement. Le membre du personnel des services de police, membre du service d'enquête, candidat pour une fonction au sein des services de police et reconnu apte pour celle-ci, bénéficie de la priorité sur tous les autres candidats à cette fonction, même si ces derniers disposent d'une priorité accordée en vertu de la loi. Cette priorité vaut pendant la dernière année des six années prestées au sein de l'Organe de contrôle.

Une période de priorité de deux années est accordée sous les mêmes conditions à partir du début de la dixième année prestée au sein de l'Organe de contrôle.

§ 3. Un congé pour mission d'intérêt général est octroyé au magistrat de l'ordre judiciaire, au fonctionnaire de la fonction publique ou membre des services de police pour la durée de leur mandat. Ils conservent, pendant leur mandat à l'Organe de contrôle ou le service d'enquête, dans le service ou dans l'administration dont ils sont originaires, leurs droits à la promotion et aux augmentations de traitement.

Art. 235

§ 1er. L'Organe de contrôle dispose d'un secrétariat composé d'un assistant de direction, un juriste et un informaticien. Ces membres du personnel jouissent du traitement prévu dans le statut des fonctionnaires de la fonction publique fédérale, soit:

— Assistant de direction: barème A1

— Juriste: barème A3

— Informaticien: barème A3

Zij worden aangeworven door het Controleorgaan die daarvoor een beroep kan doen op een deskundige in human resources.

§ 2. Het secretariaat en zijn personeelsleden staan onder het gezag van de leden van het Controleorgaan en de dagelijkse leiding van de voorzitter van het Controleorgaan.

HOOFDSTUK II

De opdrachten

Art. 236

§ 1. Het Controleorgaan is belast met de opdrachten voorzien in artikel 71, § 1, 1° tot 3°.

§ 2. Het Controleorgaan dient van advies, hetzij uit eigen beweging, hetzij op verzoek van de regering of van de Kamer van volksvertegenwoordigers, van een bestuurlijke of gerechtelijke overheid dan wel een politiedienst, omtrent iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer, zoals onder meer bepaald in afdeling 12 van hoofdstuk 4 van de wet op het politieambt.

Het Controleorgaan brengt advies uit binnen zestig dagen nadat alle daartoe noodzakelijke gegevens aan de toezichthoudende autoriteit zijn medegedeeld. De adviezen van het Controleorgaan zijn met redenen omkleed. Het Controleorgaan deelt zijn advies aan de betrokken overheid mede.

In de gevallen waar het advies van het Controleorgaan vereist is krachtens een bepaling van deze wet, wordt de termijn bedoeld in het tweede lid in speciaal gemotiveerde dringende gevallen verminderd tot ten minste vijftien dagen.

§ 3. In het kader van de opdracht voorzien in artikel 71, § 1, 3°, is het Controleorgaan in het bijzonder belast met de naleving van de regels inzake de mededeling van de informatie en persoonsgegevens uit de politionele gegevensbanken, de rechtstreekse toegang tot de A.N.G. en de technische gegevensbanken en de rechtstreekse bevraging ervan, alsook van de naleving van de in artikel 44/7, derde lid, van de wet op het politieambt bedoelde verplichting, voor alle leden van de politiediensten, tot voeding van deze gegevensbank.

Ils sont recrutés par l'Organe de contrôle qui peut se faire assister par un expert en ressources humaines.

§ 2. Le secrétariat et les membres du personnel sont placés sous l'autorité exclusive des membres de l'Organe de contrôle et sont au quotidien sous la direction du président de l'Organe de contrôle.

CHAPITRE II

Les missions

Art. 236

§ 1er. L'Organe de contrôle est chargé des missions prévues à l'article 71, § 1er, 1° à 3°.

§ 2. L'Organe de contrôle émet soit d'initiative soit sur demande du gouvernement ou de la Chambre des représentants, d'une autorité administrative ou judiciaire ou d'un service de police, des avis sur toute question relative à la gestion de l'information policière, comme prévu notamment dans la section 12 du chapitre 4 de la loi sur la fonction de police.

L'Organe de contrôle émet ses avis dans les soixante jours après la communication de toutes les données nécessaires à cet effet. Les avis de l'Organe de contrôle sont motivés. L'Organe de contrôle communique son avis à l'autorité concernée.

Dans les cas où l'avis de l'Organe de contrôle est requis par une disposition de la présente loi, le délai visé à l'alinéa 2 est réduit à quinze jours minimum dans des cas d'urgence spécialement motivés.

§ 3. Dans le cadre de la mission prévue à l'article 71, § 1er, 3°, l'Organe de contrôle est particulièrement chargé du respect de la communication des informations et données à caractère personnel des banques de données policières, de l'accès direct à la BNG et les banques de données techniques et de leur consultation directe, et également du respect de l'obligation prévue dans l'article 44/7, troisième alinéa, de la loi sur la fonction police, pour tous les membres de services de police, d'alimenter cette banque de données.

Art. 237

Het Controleorgaan treedt ambtshalve op, op verzoek van de Gegevensbeschermingsautoriteit bedoeld in artikel 2, 1°, van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, van de gerechtelijke of bestuurlijke overheden, van de minister van Justitie, van de minister van Binnenlandse Zaken, van de minister die de privacy in zijn bevoegdheden heeft of van de Kamer van volksvertegenwoordigers.

Wanneer het Controleorgaan ambtshalve optreedt, brengt het de Kamer van volksvertegenwoordigers daarvan dadelijk op de hoogte.

Wanneer de controle heeft plaatsgevonden binnen een lokale politie, informeert het Controleorgaan daar de burgemeester of het politiecollege van en zendt hem zijn verslag.

Wanneer de controle informatie en gegevens betreft die verband houden met de uitoefening van opdrachten van gerechtelijke politie, wordt het verslag dat dienaangaande door het Controleorgaan wordt opgesteld, ook aan de bevoegde magistraat van het openbaar ministerie toegezonden.

Art. 238

Het Controleorgaan doet verslag aan de Kamer van volksvertegenwoordigers in de volgende gevallen:

1° jaarlijks, door een algemeen activiteitenverslag dat, indien nodig, algemene conclusies en voorstellen bevat en dat de periode betreft gaande van 1 januari tot 31 december van het voorgaande jaar. Dat verslag wordt uiterlijk op 1 juni overgezonden aan de voorzitter van de Kamer van volksvertegenwoordigers alsmede aan de bevoegde ministers bedoeld in artikel 237, eerste lid;

2° telkens wanneer het dit nuttig acht of op verzoek van de Kamer van volksvertegenwoordigers, door een tussentijds activiteitenverslag met betrekking tot een welbepaald onderzoeksdossier dat, indien nodig, algemene conclusies en voorstellen kan bevatten. Dat verslag wordt overgezonden aan de voorzitter van de Kamer van volksvertegenwoordigers alsmede aan de bevoegde ministers bedoeld in artikel 237, eerste lid;

3° wanneer door de Kamer van volksvertegenwoordigers een verzoek werd geuit om op te treden;

4° wanneer het vaststelt dat, bij het verstrijken van een termijn die het redelijk acht, geen gevolg werd gegeven

Art. 237

L'Organe de contrôle agit d'initiative, à la demande de l'Autorité de protection des données visée à l'article 2, 1°, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, des autorités judiciaires ou administratives, du ministre de la Justice ou du ministre de l'Intérieur, du ministre responsable pour la protection de la vie privée ou de la Chambre des représentants.

Lorsque l'Organe de contrôle agit d'initiative, il en informe immédiatement la Chambre des représentants.

Lorsque le contrôle a eu lieu au sein d'un corps de la police locale, l'Organe de contrôle en informe le bourgmestre ou le collège de police et lui adresse son rapport.

Lorsque le contrôle concerne des informations et des données à caractère personnel concernant l'exécution des missions de police judiciaire, le rapport y relatif qui est établi par l'Organe de contrôle est également transmis selon le cas au magistrat du ministère public compétent.

Art. 238

L'Organe de contrôle fait rapport à la Chambre des représentants dans les cas suivants:

1° annuellement, par un rapport général d'activités qui comprend, le cas échéant, des conclusions et des propositions d'ordre général et qui couvre la période allant du 1er janvier au 31 décembre de l'année précédente. Ce rapport est transmis au plus tard le 1er juin au président de la Chambre des représentants ainsi qu'aux ministres compétents visés à l'article 237, alinea premier;

2° chaque fois qu'il l'estime utile ou à la demande de la Chambre des représentants, par un rapport d'activités intermédiaire, qui peut comprendre, le cas échéant, des conclusions et des propositions d'ordre général relatives à un dossier d'enquête déterminé. Ce rapport est transmis au président de la Chambre des représentants ainsi qu'aux ministres compétents visés à l'article 237, alinea premier;

3° lorsque la Chambre des représentants lui a confié une mission;

4° lorsqu'au terme d'un délai qu'il estime raisonnable, il constate qu'aucune suite n'a été réservée à ses

aan zijn besluiten of dat de genomen maatregelen niet passend of ontoereikend zijn. Die termijn mag niet minder dan zestig dagen bedragen.

Art. 239

§ 1. Het Controleorgaan gaat door middel van onderzoek naar de werking na of de inhoud van de A.N.G., de basisgegevensbanken, de bijzondere gegevensbanken en de technische gegevensbanken, alsook de procedure voor de verwerking van de daarin bewaarde gegevens en informatie overeenkomen met het bepaalde in de artikelen 44/1 tot en met 44/11/13 van de wet op het politieambt en met hun uitvoeringsmaatregelen.

§ 2. Het Controleorgaan controleert in het bijzonder de regelmatigheid van de volgende verwerkingen in de algemene nationale gegevensbank, de basisgegevensbanken, de bijzondere gegevensbanken en de technische gegevensbanken:

1° de evaluatie van de gegevens en informatie;

2° de registratie van de verzamelde gegevens en informatie;

3° de validatie van de gegevens en informatie door de daartoe bevoegde organen;

4° de vatting van de geregistreerde gegevens en informatie op grond van de concrete aard of van de betrouwbaarheid ervan;

5° de wissing en de archivering van de gegevens en informatie nadat de termijn voor bewaring ervan is verstreken.

§ 3. Het Controleorgaan controleert in het bijzonder de werkelijke aard van de volgende, door de bevoegde politieoverheden voorgeschreven functiemogelijkheden en verwerkingen:

1° de relaties tussen de categorieën van gegevens en informatie geregistreerd op het tijdstip waarop zij zijn gevat;

2° de ontvangst van de gegevens en informatie door de autoriteiten en diensten die krachtens de wet tot raadpleging gemachtigd zijn;

3° de mededeling van de gegevens en de informatie aan de wettelijk gemachtigde autoriteiten en diensten;

conclusions, ou que les mesures prises sont inappropriées ou insuffisantes. Ce délai ne peut être inférieur à soixante jours.

Art. 239

§ 1er. L'Organe de contrôle veille, par le biais d'enquêtes de fonctionnement, à ce que le contenu de la B.N.G., les banques de données de base, les banques de données particulièreset les banques de données techniques, ainsi que la procédure de traitement des données et informations qui y sont conservées, soient conformes aux règles prescrites par les articles 44/1 à 44/11/13 de la loi sur la fonction de police et à leurs mesures d'exécution.

§ 2. L'Organe de contrôle vérifie en particulier la régularité des opérations de traitement suivantes au sein de la banque de données générale, les banques de données de base, les banques de données particulières et les banques de données techniques:

1° l'évaluation des données et informations;

2° l'enregistrement des données et informations collectées;

3° la validation des données et informations par les organes compétents à cet effet;

4° la saisie des données et informations enregistrées en fonction du caractère concret ou de la fiabilité de celles-ci;

5° l'effacement et l'archivage des données et informations à l'échéance de leur délai de conservation.

§ 3. L'Organe de contrôle vérifie en particulier le caractère effectif des fonctionnalités et opérations de traitement suivantes, prescrites par les autorités de police compétentes:

1° les relations entre les catégories de données et informations enregistrées au moment de leur saisie;

2° la réception des données et informations par les autorités et services légalement habilités à les consulter;

3° la communication des données et informations vers les autorités et services légalement habilités;

4° de verbinding met andere systemen voor informatieverwerking;

5° de bijzondere regels houdende vatting van de gegevens en de informatie op grond van hun adequaat, pertinent en niet overmatig karakter en de concrete betrouwbaarheid ervan.

Art. 240

Het Controleorgaan:

1° maakt het brede publiek beter bekend met en verschaft meer inzicht in de risico's, de regels, de waarborgen en de rechten in verband met verwerking van persoonsgegevens door de diensten voorzien in artikel 26, 7°, a), d), f);

2° maakt de verwerkingsverantwoordelijken en de verwerkers beter bekend met hun wettelijke verplichtingen in verband met de verwerking van persoonsgegevens;

3° verstrekt desgevraagd informatie aan iedere betrokkene over de uitoefening van zijn rechten uit hoofde van deze wet en, in voorkomend geval, werkt daartoe samen met de toezichthoudende autoriteiten in andere lidstaten. Een verzoek van een andere toezichthoudende autoriteit wordt zonder onnodige vertraging en in ieder geval binnen één maand na de ontvangst ervan beantwoord;

4° behandelt klachten, onderzoekt de inhoud van de klacht in de mate waarin dat nodig is en stelt de klager binnen een redelijke termijn in kennis van de vooruitgang en het resultaat van het onderzoek, met name indien verder onderzoek of coördinatie met een andere toezichthoudende autoriteit nodig is. Het Controleorgaan kan besluiten geen gevolg te geven aan een klacht of een aangifte die kennelijk niet gegrond is.

5° zij stelt een lijst op met betrekking tot het vereiste inzake een gegevensbeschermingseffectbeoordeling overeenkomstig artikel 35.4 van de Verordening, en houdt deze lijst bij;

6° zij bevordert de opstelling van gedragscodes uit hoofde van artikel 40.1, van de Verordening, geeft advies en keurt, overeenkomstig artikel 40.5, ven de Verordening, gedragscodes goed die voldoende waarborgen leveren;

7° zij bevordert de invoering van certificeringsmechanismen voor gegevensbescherming en van

4° la connexion avec d'autres systèmes de traitement de l'information;

5° les règles particulières de saisie des données et informations en fonction de leur caractères adéquat, pertinent et non excessif et de la fiabilité de celles-ci.

Art. 240

L'Organe de contrôle:

1° favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement des données à caractère personnel effectués par les services prévus à l'article 26, 7°, a), d), f);

2° encourage la sensibilisation des responsables du traitement et des sous-traitants aux obligations légales à l'égard des traitements de données à caractère personnel;

3° fournit, sur demande, à toute personne concernée, des informations sur l'exercice de ses droits découlant la présente loi, et, le cas échéant, coopère à cette fin avec les autorités de contrôle d'autres États membres. La demande d'une autre autorité de contrôle reçoit réponse le plus vite possible et en tout cas dans les trente jours après la réception de la demande;

4° traite des réclamations, enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire. L'organe de Contrôle peut décider de ne pas donner suite à une plainte ou à une réclamation qui est manifestement non fondée.

5° établit et tient à jour une liste en lien avec l'obligation d'effectuer une analyse d'impact relative à la protection des données en application de l'article 35.4 du Règlement;

6° encourage l'élaboration de codes de conduite en application de l'article 40.1, du Règlement, rend un avis et approuve les codes de conduite qui fournissent des garanties suffisantes, en application de l'article 40.5 du Règlement;

7° encourage la mise en place de mécanismes de certification ainsi que de labels et de marques en

gegevensbeschermingszegels en -merktekens, en keurt de criteria voor certificering uit hoofde van artikel 42, van de Verordening, goed;

8° waar van toepassing verricht zij een periodieke toetsing van de afgegeven certificeringen;

9° zij zorgt voor het opstellen en het bekendmaken van de criteria voor de accreditatie van een orgaan voor het toezicht op gedragscodes op grond van artikel 41 van de Verordening, en van een certificeringsorgaan op grond van artikel 43 van de Verordening;

10° zij zorgt voor de accreditatie van een orgaan voor het toezicht op gedragscodes en van een certificeringsorgaan.

Art. 241

Het Controleorgaan kan aan één of meer van haar leden, leden van de Dienst Onderzoeken of haar personeel de bevoegdheid opdragen om het Controleorgaan te vertegenwoordigen binnen comités of groepen waaraan het als toezichthoudende autoriteit in de politiesector verplicht deelneemt of kiest aan deel te nemen.

Art. 242

Het Controleorgaan kan overgaan tot een breed openbaar onderzoek of een brede openbare raadpleging of tot een meer gericht onderzoek of een meer gerichte raadpleging van de vertegenwoordigers van de politiesector.

Art. 243

§ 1. Het Controleorgaan dient de internationale verplichtingen uit te voeren die voortvloeien uit de taken en bevoegdheden die deze wet haar toebedeelt. Deze verplichtingen kunnen de samenwerking inhouden van het Controleorgaan met enige instantie of andere gegevensbeschermingsautoriteit van een andere staat door gebruik te maken van de bevoegdheden die haar zijn toegekend krachtens de van toepassing zijnde wetgeving.

Deze samenwerking kan betrekking hebben op:

1° de invoering van deskundigheidspools;

2° de uitwisseling van informatie;

matière de protection des données, et approuve les critères de certification en application de l'article 42, du Règlement;

8° procède, le cas échéant, à l'examen périodique des certifications délivrées;

9° rédige et publie les critères d'agrément d'un organisme chargé du suivi des codes de conduite en application de l'article 41 du Règlement et d'un organisme de certification en application de l'article 43 du Règlement;

10° procède à l'agrément d'un organisme chargé du suivi des codes de conduite et d'un organisme de certification.

Art. 241

L'Organe de contrôle peut déléguer à un ou plusieurs de ses membres, membres du service d'enquête ou son personnel le pouvoir de le représenter au sein de comités ou groupes auxquels il est tenu ou choisit de participer en tant qu'Autorité de contrôle dans le secteur police.

Art. 242

L'Organe de contrôle peut procéder à une enquête ou à une large consultation publique ou à une enquête ou consultation plus ciblée des représentants du secteur police.

Art. 243

§ 1er. L'Organe de contrôle exécute les obligations internationales liées aux tâches et compétences attribuées par la présente loi. Ces obligations peuvent consister dans la collaboration de l'Organe de contrôle avec toute instance ou autre autorité de protection des données d'un autre État en faisant usage des pouvoirs qui lui sont conférés soit en vertu de la législation en vigueur.

Cette collaboration peut porter sur:

1° la création de pôles d'expertise;

2° l'échange d'informations;

3° de wederzijdse bijstand in het kader van controlemaatregelen;

4° het delen van personele en financiële middelen.

De samenwerking kan aan de hand van samenwerkingsakkoorden worden geconcretiseerd.

§ 2. Het Controleorgaan is gemachtigd om in dit verband bepaalde van haar leden, leden van de Dienst Onderzoeken of personeelsleden aan te wijzen als vertegenwoordigers bij internationale autoriteiten.

HOOFDSTUK III

Bevoegdheden van het Controleorgaan, van haar leden en van de leden van de Dienst Onderzoeken

Art. 244

§ 1. Het Controleorgaan, zijn leden of de leden van de Dienst Onderzoeken hebben een onbeperkt recht op toegang tot alle informatie en gegevens verwerkt door de diensten voorzien in artikel 26, 7°, a), d), f), en in het bijzonder de politiediensten overeenkomstig artikel 44/1 tot en met 44/11/13 van de wet van 5 augustus 1992 op het politieambt, hierin begrepen deze die bewaard worden in de A.N.G., in de basisgegevensbanken, in de bijzondere gegevensbanken, in de technische gegevensbanken en in de internationale gegevensbanken die door de Belgische politiediensten worden gevoed.

De politiediensten zenden uit eigen beweging aan het Controleorgaan reglementen en interne richtlijnen over, betreffende de verwerking van persoonsgegevens en de politionele informatie die zij noodzakelijk achten voor het vervullen van hun opdracht. Het Controleorgaan en de Dienst Onderzoeken zijn ertoe gerechtigd alle teksten die zij noodzakelijk achten voor het vervullen van hun opdracht te laten overleggen.

Het Controleorgaan, zijn leden of de leden van de Dienst Onderzoeken kunnen een onderzoek ter plaatse doen. Te dien einde, beschikken zij over een onbeperkt recht op toegang tot de lokalen waarin en gedurende de tijd dat de in het eerste lid bedoelde informatie en gegevens verwerkt worden.

§ 2. Zij kunnen in deze plaatsen alle voorwerpen, documenten en gegevens van een informaticasysteem die nuttig zijn voor hun onderzoek in beslag nemen, behalve indien ze betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek.

3° l'assistance mutuelle dans le cadre de mesures de contrôle;

4° le partage de ressources humaines et financières.

La collaboration peut se concrétiser par le biais d'accords de coopération.

§ 2. L'Organe de contrôle est habilité à désigner à cet égard certains de ses membres, membres du service d'enquête ou membres du personnel en tant que représentants auprès d'autorités internationales.

CHAPITRE III

Compétences de l'Organe de contrôle, ses membres et des membres du service d'enquête

Art. 244

§ 1er. L'Organe de contrôle, ses membres et les membres du service d'enquête ont un accès illimité à toutes informations ou données traitées par les services visés par l'article 26, 7°, a), d), f), et en particulier, les services de police conformément aux articles 44/1 jusqu'au 44/11/13 de la loi du 5 août 1992 sur la fonction de police, en ce compris celles contenues dans la B.N.G., dans les banques de données de base, dans les banques de données particulières, les banques de données techniques et dans les bases de données internationales alimentées par les services de police belges.

Les services de police transmettent d'initiative à l'Organe de contrôle les règlements et les directives internes relatifs au traitement des données à caractère personnel et de l'information policière nécessaires à l'accomplissement de ses missions. L'Organe de contrôle et le service d'enquête ont le droit de se faire communiquer tous les textes qu'ils estiment nécessaires à l'accomplissement de leur mission.

L'Organe de contrôle, ses membres et les membres du service d'enquête peuvent effectuer des enquêtes sur place. A cette fin, ils ont un droit d'accès illimité aux locaux dans lesquels et pendant le temps où les informations et données visées à l'alinéa premier sont traitées.

§ 2. Ils peuvent saisir dans ces lieux tous les objets, documents et données d'un système informatique utiles pour leur enquête, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours.

Indien de korpschef of zijn plaatsvervanger van oordeel is dat door het beslag een persoon fysiek gevaar kan lopen, wordt de kwestie voorgelegd aan de voorzitter van het Controleorgaan of de magistraat die hem vervangt die uitspraak doet. De in beslag genomen voorwerpen en documenten worden vermeld in een daartoe speciaal bij te houden register.

§ 3. De leden van het Controleorgaan en de Dienst Onderzoeken doen, waar ook, alle nuttige vaststellingen.

Het Controleorgaan of zijn leden kunnen, voor het uitoefenen van haar opdrachten, de bijstand vorderen van de openbare macht.

§ 4. Het Controleorgaan, zijn leden of de leden van de Dienst Onderzoeken kunnen dwingende antwoordtermijnen opleggen aan de leden van de federale of van de lokale politie, waaraan ze vragen richten in de uitvoering van hun opdrachten.

§ 5. Het Controleorgaan heeft, voor de uitoefening van het toezicht dat door deze wet wordt georganiseerd, toegang tot de gegevens van artikel 3, eerste lid, 1° tot 6°, 9°, 9°/1 en tweede lid, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen.

Met het oog op de uitoefening van dit toezicht mag zij gebruikmaken van het rijksregisternummer.

Art. 245

§ 1. Onverminderd de wettelijke bepalingen betreffende de onschendbaarheid en het voorrecht van rechtsmacht, kunnen de leden van het Controleorgaan en van de Dienst Onderzoeken elke persoon van wie zij het verhoor noodzakelijk achten, uitnodigen om hem te horen. De leden of gewezen leden van de politiediensten zijn gehouden gevolg te geven aan elke schriftelijke oproeping.

De leden of gewezen leden van de politiediensten mogen verklaringen afleggen over feiten die worden gedekt door het beroepsgeheim.

§ 2. De voorzitter van het Controleorgaan kan de leden of gewezen leden van de politiediensten dagvaarden door tussenkomst van een gerechtsdeurwaarder. Deze leden of gewezen leden moeten getuigen na de eed te hebben afgelegd die is bepaald in artikel 934, tweede lid, van het Gerechtelijk Wetboek.

Si le chef de corps ou son remplaçant estime que la saisie risque de faire courir un danger physique à une personne, la question est soumise au président de l'Organe de contrôle ou le magistrat qui le remplace lequel statue. Les objets et documents saisis sont mentionnés dans un registre spécial tenu à cet effet.

§ 3. Les membres de l'Organe de contrôle et les membres du service d'enquête font, en tout lieu, les constatations qui s'imposent.

L'Organe de contrôle ou ses membres peuvent, dans l'exercice de leurs missions, requérir l'assistance de la force publique.

§ 4. L'Organe de contrôle, ses membres et les membres du service d'enquête peuvent imposer des délais de réponse contraignants aux membres de la police fédérale ou de la police locale auxquels ils adressent des questions dans l'exécution de leurs missions.

§ 5. L'Organe de contrôle a accès, pour l'exercice du contrôle organisé par la présente loi, aux données de l'article 3, premier alinéa, 1° à 6°, 9°, 9°/1 et second alinéa de la loi du 8 aout 1983 instituant un registre national des personnes physiques.

En vue de l'exercice de ce contrôle, elle peut utiliser le numéro de registre national.

Art. 245

§ 1er. Sans préjudice des dispositions légales relatives aux immunités et aux privilèges de juridiction, les membres de l'Organe de contrôle et les membres du service d'enquête peuvent inviter, afin de l'entendre, toute personne dont ils estiment l'audition nécessaire. Les membres ou anciens membres des services de police sont tenus de donner suite à toute convocation écrite.

Les membres ou anciens membres des services de police peuvent faire une déclaration sur des faits couverts par le secret professionnel.

§ 2. Le président de l'Organe de contrôle peut faire citer des membres ou anciens membres des services de police par huissier de justice. Les membres ou anciens membres des services de police sont tenus de déposer après avoir prêté le serment prévu à l'article 934, alinéa 2 du Code judiciaire.

De leden of gewezen leden van de politiediensten zijn verplicht geheimen waarvan zij kennis dragen, aan het Controleorgaan bekend te maken, behalve indien ze betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek.

Als het lid of gewezen lid van de politiedienst van oordeel is dat hij het geheim waarvan hij kennis draagt, moet bewaren omdat een persoon door de bekendmaking ervan fysiek gevaar zou kunnen lopen, wordt de kwestie voorgelegd aan de voorzitter van het Controleorgaan of de magistraat die hem vervangt, die uitspraak doet.

Als het lid of gewezen lid van de politiedienst van oordeel is dat hij het geheim waarvan hij kennis draagt, moet bewaren, wordt de kwestie voorgelegd aan de Commissaris-generaal of de korpschef in functie van de politiedienst waartoe de betrokkene behoort, die uitspraak doet.

§ 3. Het Controleorgaan kan de medewerking van deskundigen en tolken vorderen. Zij leggen de eed af volgens de formule als gebruikt voor het Hof van Assisen. De hen verschuldigde vergoedingen worden uitgekeerd overeenkomstig het tarief van de gerechtskosten in strafzaken.

§ 4. Artikel 9 van de wet van 3 mei 1880 op het parlementair onderzoek is van toepassing op de leden of gewezen leden van de politiediensten die als getuige worden gehoord of gedagvaard door het Controleorgaan en op de deskundigen en tolken die worden gevorderd.

De processen-verbaal die gepleegde inbreuken vaststellen, worden opgesteld door een lid van het Controleorgaan of een lid van de Dienst Onderzoeken en worden overgezonden aan de procureur des Konings in wiens ambtsgebied ze zijn begaan.

De leden of gewezen leden van de politiediensten die weigeren te getuigen voor het Controleorgaan en de deskundigen en de tolken die weigeren hun medewerking te verlenen, worden gestraft met een gevangenisstraf van één maand tot twee jaar en een geldboete van 100 tot 1 000 euro of met één van die straffen alleen.

Art. 246

Onverminderd artikel 44/1 van de wet op het politieambt, zijn alle diensten van de Staat, met inbegrip van de parketten en de griffies van de hoven en van alle rechtscolleges, de provincies, de gemeenten, de verenigingen waartoe zij behoren, de overheidsinstellingen die ervan afhangen, gehouden aan het Controleorgaan,

Les membres ou anciens membres des services de police sont tenus de révéler à l'Organe de contrôle les secrets dont ils sont dépositaires, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours.

Si le membre ou l'ancien membre du service de police estime devoir garder le secret dont il est dépositaire parce que sa révélation risquerait de faire courir un danger physique à une personne, la question est soumise au président de l'Organe de contrôle ou le magistrat qui le remplace qui statue.

Si le membre ou l'ancien membre du service de police estime devoir garder le secret dont il est dépositaire, la question est soumise au Commissaire général ou au chef de corps en fonction du service de police auquel l'intéressé appartient qui le remplace qui statue.

§ 3. L'Organe de contrôle peut requérir la collaboration d'interprètes et d'experts. Ils prêtent serment d'après la formule utilisée devant la Cour d'Assises. Les indemnités qui leurs sont dues sont réglées conformément au tarif des frais en matières pénales.

§ 4. L'article 9 de la loi du 3 mai 1880 sur les enquêtes parlementaires est d'application aux membres ou anciens membres des services de police qui sont entendus ou cités par l'Organe de contrôle à titre de témoins et aux experts et interprètes qui sont requis.

Les procès-verbaux constatant les infractions commises sont établis par un membre de l'Organe de contrôle ou un membre du service d'enquête et sont transmis au procureur du Roi dans le ressort duquel elles sont commises.

Les membres ou anciens membres des services de police qui refusent de témoigner devant l'Organe de contrôle et les experts et interprètes qui refusent leur collaboration sont punis d'un emprisonnement de un mois à deux ans et une amende de 100 euros à 1 000 euros ou une de ces peines.

Art. 246

Sans préjudice de l'article 44/1 de la loi sur la fonction de police, tous les services de l'État, y compris les parquets et les greffes des cours et de toutes les juridictions, des provinces, des communes, des associations dont elles font partie, des institutions publiques qui en dépendent, sont tenus, vis-à-vis de l'Organe

haar leden of de leden van de Dienst Onderzoeken, op haar of hun verzoek, alle inlichtingen te geven die laatstgenoemden nuttig acht voor het toezicht op de naleving van de wetgeving waarmee zij belast zijn, alsmede gelijk welke informatiedragers ter inzage over te leggen en kopieën ervan te verstrekken onder gelijk welke vorm.

Indien deze inlichtingen deel uitmaken van een lopend opsporings- of gerechtelijk onderzoek worden ze slechts mits voorafgaande goedkeuring van het bevoegde openbaar ministerie verstrekt.

Art. 247

Het Controleorgaan beslist over de opvolging die het aan een klacht in de zin van artikel 240, 4°, geeft en heeft de bevoegdheid om:

1° te besluiten dat de verwerking is uitgevoerd in overeenstemming met de bepalingen van de reglementering inzake de verwerking van persoonsgegevens;

2° de diensten voorzien in artikel 26, 7°, a), d)en f) of diens verwerker te waarschuwen dat een voorgenomen verwerking van persoonsgegevens de reglementering inzake de verwerking van persoonsgegevens kan schenden;

3° de diensten voorzien in artikel 26, 7°, a), d) en f) of diens verwerker te berispen wanneer een verwerking geresulteerd heeft in een schending van een bepaling van de reglementering inzake de verwerking van persoonsgegevens;

4° de diensten voorzien in artikel 26, 7°, a), d) en f) of diens verwerker te gelasten om een verwerking in overeenstemming te brengen met de bepalingen van de reglementering inzake de verwerking van persoonsgegevens, in voorkomend geval, op een nader bepaalde manier en binnen een nader bepaalde termijn;

5° een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, op te leggen;

6° het rectificeren of wissen van persoonsgegevens te gelasten;

7° het dossier over te maken aan het bevoegde openbaar ministerie, die het informeert van het gevolg dat aan het dossier gegeven wordt.

8° een certificering bedoeld in artikel 240 intrekken of het certificeringsorgaan gelasten een afgegeven

de contrôle, ses membres ou les membres du service d'enquête et à leur demande, de leur fournir tous les renseignements que ces derniers estiment utiles au contrôle du respect de la législation dont ils sont chargés, ainsi que de leur produire, pour en prendre connaissance, tous les supports d'information et de leur en fournir des copies sous n'importe quelle forme.

Si ces renseignements font partie d'une enquête judiciaire en cours, ils ne seront transmis que moyennant l'autorisation préalable du ministère public compétent.

Art. 247

L'Organe de contrôle décide du suivi qu'il donne à une plainte au sens de l'article 240, 4°, et a le pouvoir de:

1° conclure que le traitement est effectué en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel;

2° avertir les services visés à l'article 26, 7°, a), d) et f) ou son sous-traitant du fait qu'un traitement envisagé de données à caractère personnel est susceptible de violer la règlementation relative aux traitements des données à caractère personnel;

3° rappeler à l'ordre les services visés à l'article 26, 7°, a), d) et f) ou son sous-traitant lorsqu'un traitement a entraîné une violation d'une disposition de la règlementation relative aux traitements des données à caractère personnel;

4° ordonner aux services visés à l'article 26, 7°, a), d) et f) ou à son sous-traitant de mettre un traitement en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel, le cas échéant, de manière spécifique et dans un délai déterminé;

5° imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;

6° ordonner la rectification ou l'effacement de données à caractère personnel;

7° transmettre le dossier au ministère public compétent qui l'informe des suites données au dossier;

8° retirer une certification visée à l'article 240, délivrée ou ordonner à l'organisme de certification de retirer

certificering in te trekken, of het certificeringsorgaan te gelasten geen certificering af te geven.

9° de diensten voorzien in artikel 26, 7°, a), d) en f) of diens verwerker te gelasten een inbreuk in verband met persoonsgegevens aan de betrokkene mee te delen;

Art. 248

Het Controleorgaan informeert de dienst voorzien in artikel 26, 7°, a), d) en f) van de uitgevoerde onderzoeken naar de verwerking van persoonsgegevens van diens verwerkers en hun resultaten.

Wanneer het er kennis van neemt, informeert het Controleorgaan eveneens de diensten voorzien in artikel 26, 7°, a), d) en f) van de schendingen van de reglementering inzake de verwerking van persoonsgegevens door andere verwerkingsverantwoordelijken.

Art. 249

§ 1. Uiterlijk één maand na ontvangst van het verzoek brengt het Controleorgaan ten behoeve van de bevoegde overheid, een omstandig advies uit over de aanwijzing, de bevordering, de benoeming of de mutatie van de personeelseden van de politiediensten belast met het beheer van de A.N.G.

§ 2. Binnen de maand na ontvangst van het verzoek brengt het Controleorgaan ten behoeve van de bevoegde minister, een omstandig advies uit over de wenselijkheid van een tuchtrechtelijke procedure ten aanzien van het hoofd van de dienst die de A.N.G. beheert, of ten aanzien van zijn adjunct.

HOOFDSTUK IV

Financiering

Art. 250

Voor de werking van het Controleorgaan wordt een dotatie uitgetrokken op de algemene uitgavenbegroting van het Rijk.

Het Controleorgaan stelt jaarlijks een ontwerp van begroting op voor zijn werking. Bijgestaan door het Rekenhof, onderzoekt de Kamer van volksvertegenwoordigers de gedetailleerde begrotingsvoorstellen van het Controleorgaan, keurt ze goed en controleert

la certification ou ordonner à l'organisme de certification de ne pas délivrer de certification.

9° ordonner aux services visés à l'article 26, 7°, a), d) et f) ou à son sous-traitant de communiquer à la personne concernée une brèche de sécurité en violation de données à caractère personnel;

Art. 248

L'Organe de contrôle informe le service visé à l'article 26, 7°, a), d) et f) des enquêtes effectuées sur le traitement de données à caractère personnel par ses sous-traitants et de leurs résultats.

Lorsqu'il en prend connaissance, l'Organe de contrôle informe également les services visés à l'article 26, 7°, a), d) et f) des violations de la règlementation relative aux traitements de ses données à caractère personnel par d'autres responsables du traitement.

Art. 249

§ 1er. L'Organe de contrôle émet, à l'adresse de l'autorité compétente, dans les deux semaines de la réception de la demande, un avis circonstancié sur la désignation, la promotion, la nomination ou la mutation des membres du personnel des services de police chargés de la gestion de la B.N.G.

§ 2. L'Organe de contrôle émet, à l'adresse du ministre compétent, dans les deux semaines à dater de la réception de la demande, un avis circonstancié sur l'opportunité d'entamer une procédure disciplinaire à l'égard du chef du service gérant la B.N.G. ou de l'adjoint de celui-ci.

CHAPITRE IV

Financement

Art. 250

Une dotation est inscrite au budget général des dépenses de l'État pour financer le fonctionnement de l'Organe de contrôle.

L'Organe de contrôle établit annuellement un projet de budget pour son fonctionnement. Assistée par la Cour des comptes, la Chambre des représentants examine les propositions budgétaires détaillées de l'Organe de contrôle, elle les approuve et contrôle l'exécution

de uitvoering van zijn begroting, onderzoekt en keurt daarenboven de gedetailleerde rekeningen goed.

Het Controleorgaan voegt bij haar jaarlijks begrotingsvoorstel een strategisch plan.

Het Controleorgaan hanteert voor zijn begroting en rekeningen een schema dat vergelijkbaar is met het schema van de begroting en rekeningen van de Kamer van volksvertegenwoordigers.

TITEL 8

Slotbepalingen

Art. 251

In geval van verwerking van persoonsgegevens voor meerdere doeleinden, door eenzelfde verwerkingsverantwoordelijke of verwerker, of bedoeld in verschillende regelgevingen, zijn deze verschillende regelgevingen tegelijkertijd van toepassing. In geval van conflict tussen sommige van hun bepalingen, worden de regels van deze wet toegepast.

Art. 252

De Koning kan, bij een in Ministerraad overlegd besluit na advies van de bevoegde toezichthoudende autoriteit, bijkomende voorwaarden bepalen teneinde deze wet uit te voeren.

HOOFDSTUK I

Wijzigingsbepalingen

Art. 253

De bestaande wetten, koninklijke besluiten en elke andere reglementering die verwijzen naar de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, worden geacht te verwijzen naar deze wet of desgevallend de Verordening.

De Koning kan de verwijzingen in bestaande wetten en koninklijke besluiten naar de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens vervangen door verwijzingen naar de ermee overeenstemmende bepalingen in deze wet en de Verordening.

de son budget, elle examine et approuve en outre les comptes détaillés.

L'Organe de contrôle joint à sa proposition de budget annuel un plan stratégique.

Pour son budget et ses comptes, l'Organe de contrôle utilise un schéma budgétaire et des comptes comparable à celui qui est utilisé par la Chambre des représentants.

TITRE 8

Dispositions finales

Art. 251

En cas de traitement de données à caractère personnel pour plusieurs finalités par un même responsable du traitement ou sous-traitant, ou visées par différentes législations, ces différentes législations s'appliquent de manière simultanée. En cas de conflit entre certaines de leurs dispositions, les règles de la présente loi sont appliquées.

Art. 252

Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres après avis de l'autorité de contrôle compétente, des conditions supplémentaires afin d'exécuter la présente loi.

CHAPITRE I^ER

Dispositions modificatives

Art. 253

Les lois, les arrêtés royaux et toute autre règlementation existants qui font référence à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel sont présumés faire référence à la présente loi ou, le cas échéant, au Règlement.

Le Roi peut remplacer les références dans les lois ou arrêtés existants aux dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel par des références aux dispositions équivalentes de la présente loi ou du Règlement.

Art. 254

In wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit wordt een artikel 56*bis* ingevoegd luidende:

"In uitvoering van artikel 51 van de Verordening 2016/679 en overeenkomstig artikel 41.4 van de Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, vertegenwoordigt de Gegevensbeschermingsautoriteit de verschillende toezichtautoriteiten in het Europees Comité voor gegevensbescherming bedoeld in artikel 68 van de Verordening."

Art. 255

In de artikelen 3, 31 en 35 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, worden de woorden "Algemene Dienst Inlichtingen en Veiligheid" vervangen door de woorden "Algemene Dienst Inlichting en Veiligheid".

Art. 256

§ 1. In de Franse tekst van het opschrift van Hoofdstuk III en de afdelingen 1 en 2 van hetzelfde hoofdstuk, in het opschrift van Hoofdstuk IV evenals in de artikelen 2, 3, 2°, 28, 33, 38, 39, 40, 48, 53 en 65 van dezelfde wet worden de woorden "services de renseignements" vervangen door de woorden "services de renseignement".

§ 2. In de Franse tekst van de artikelen 28, 40, 41, 48, 50, 61 en 67 worden de woorden "service de renseignements" vervangen door de woorden "service de renseignement".

§ 3. In de Franse tekst van de artikelen 41 en 44 worden de woorden "des services de police ou de renseignements" vervangen door de woorden "des services de police ou de renseignement".

§ 4. In de Franse tekst van het artikel 44 worden de woorden "d'un service de police ou de renseignements" vervangen door de woorden "d'un service de police ou de renseignement".

Art. 254

Dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, il est inséré un article 56*bis* rédigé comme suit:

"En exécution de l'article 51 du Règlement 2016/679 et conformément à l'article 41.4 de la directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, l'Autorité de protection des données représente les différentes autorités de contrôle au Comité européen de la protection des données visé à l'article 68 du Règlement."

Art. 255

Aux articles 3, 31 et 35 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, les mots "Service général du renseignement et de la sécurité" sont remplacés par les mots "Service Général du Renseignement et de la Sécurité".

Art. 256

§ 1er. Dans l'intitulé du Chapitre III et des sections 1 et 2 de ce même chapitre, dans l'intitulé du Chapitre IV ainsi qu'aux articles 2, 3, 2°, 28, 33, 38, 39, 40, 48, 53 et 65 de la même loi, les mots "services de renseignements" sont remplacés par les mots "services de renseignement".

§ 2. Aux articles 28, 40, 41, 48, 50, 61 et 67, les mots "service de renseignements" sont remplacés par les mots "service de renseignement".

§ 3. Aux articles 41 et 44, les mots "des services de police ou de renseignements" sont remplacés par les mots "des services de police ou de renseignement".

§ 4. A l'article 44, les mots "d'un service de police ou de renseignements" sont remplacés par les mots "d'un service de police ou de renseignement".

§ 5. In de Franse tekst van het artikel 53 worden de woorden “des missions de renseignements” vervangen door de woorden “des missions de renseignement”.

Art. 257

In artikel 3 van dezelfde wet, worden een 7° en een 8° ingevoegd, luidende:

“7° “de gegevensbeschermingswet”: de wet van xx/xx/2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

8° “een gegevensbeschermingsautoriteit”: een autoriteit die toezicht houdt op verwerkingen van persoonsgegevens.”

Art. 258

§ 1. In artikel 28 van dezelfde wet, derde lid, 5°, worden de volgende wijzigingen aangebracht:

1° de woorden “de inlichtingen,” worden ingevoegd tussen de woorden “domein van” en “het strafrecht”;

2° de woorden “het recht van de bescherming van persoonsgegevens” worden ingevoegd tussen de woorden “het publiek recht,” en de woorden “of technieken inzake management”.

§ 2. In hetzelfde artikel wordt het vierde lid aangevuld met de woorden “, noch van een andere gegevensbeschermingsautoriteit, noch van de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten”.

Art. 259

Artikel 29, eerste lid, 8°, van dezelfde wet wordt aangevuld met de woorden “, veiligheidsattesten en veiligheidsadviezen”.

Art. 260

In artikel 31 van dezelfde wet worden de woorden “, alsook voor de organisatie en het bestuur van de Veiligheid van de Staat wanneer die organisatie en

§ 5. A l’article 53, les mots “des missions de renseignements” sont remplacés par les mots “des missions de renseignement”.

Art. 257

A l’article 3 de la même loi, sont insérés un 7° et un 8° rédigés comme suit:

“7° “la loi protection des données”: la loi du xx/xx/2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel;

8° “une autorité de protection des données”: une autorité de contrôle des traitements de données à caractère personnel.”

Art. 258

§ 1er. Dans l’article 28 de la même loi, alinéa 3, 5°, les modifications suivantes sont apportées:

1° les mots “du renseignement,” sont insérés entre les mots “le domaine” et les mots “du droit pénal”;

2° les mots “du droit de la protection des données à caractère personnel,” sont insérés entre les mots “du droit public,” et les mots “ou de techniques de gestion”.

§ 2. Dans ce même article, l’alinéa 4 est complété par les mots “, ni d’une autre autorité de protection des données, ni de la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité”.

Art. 259

A l’article 29 de la même loi, le 8° est complété par les mots “, attestations et avis de sécurité”.

Art. 260

A l’article 31 de la même loi, les mots “, ainsi que l’organisation et l’administration de la Sûreté de l’État lorsque celles-ci ont une influence directe sur l’exécution

dat bestuur een rechtstreekse invloed hebben op de uitvoering van de opdrachten inzake de handhaving van de openbare orde en de persoonsbescherming" opgeheven.

Art. 261

§ 1. In artikel 32, eerste lid van dezelfde wet, wordt het woord "of" vervangen door",".

§ 2. Het eerste lid van hetzelfde artikel wordt aangevuld met de woorden "of op vraag van een andere gegevensbeschermingsautoriteit".

§ 3. In het tweede lid van hetzelfde artikel worden de woorden "in het kader van de activiteiten en methodes bedoeld in artikel 33, eerste lid" ingevoegd tussen de woorden "beweging optreedt" en ", brengt het".

Art. 262

§ 1. In artikel 33 van dezelfde wet wordt na het eerste lid een nieuw lid ingevoegd, luidende:

"Het Vast Comité I onderzoekt eveneens de verwerkingen van persoonsgegevens door de inlichtingendiensten en hun verwerkers."

§ 2. In het vierde lid, dat het vijfde lid wordt, van hetzelfde artikel worden de volgende wijzigingen aangebracht:

1° het woord "of" wordt vervangen door ",";

2° de woorden "of de verwerkingen van persoonsgegevens" worden ingevoegd tussen de woorden "de werkwijzen" en de woorden "die de".

§ 3. In het zevende lid, dat het achtste lid wordt, van hetzelfde artikel worden de woorden "Het Vast Comité I mag enkel" vervangen door de woorden "Behalve als de wet zijn advies oplegt, mag het Vast Comité I enkel".

Art. 263

§ 1. In artikel 34 van dezelfde wet wordt tussen het eerste en het tweede lid een lid ingevoegd, luidende:

"Het Vast Comité I behandelt eveneens de verzoeken met betrekking tot de verwerkingen van

des missions de maintien de l'ordre public et de protection des personnes" sont supprimés.

Art. 261

§ 1er. A l'article 32, alinéa premier de la même loi, le mot "ou" est remplacé par ",".

§ 2. L'alinéa premier de ce même article est complété par les mots "ou à la demande d'une autre autorité de protection des données".

§ 3. A l'alinéa 2 de ce même article, les mots "dans le cadre des activités et méthodes visées à l'article 33, alinéa 1er" sont insérés entre les mots "d'initiative" et les mots ", il en informe".

Art. 262

§ 1er. Dans l'article 33 de la même loi, il est inséré après le premier alinéa un nouvel alinéa rédigé comme suit:

"Le Comité permanent R enquête également sur les traitements de données à caractère personnel par les services de renseignement et leurs sous-traitants."

§ 2. A l'alinéa 4, qui devient l'alinéa 5, de ce même article, les modifications suivantes sont apportées:

1° le mot "ou" est remplacé par ",";

2° les mots "ou les traitements des données à caractère personnel" sont insérés entre les mots "les méthodes" et les mots "qui seraient".

§ 3. A l'alinéa 7, qui devient l'alinéa 8, de ce même article, les mots "Le Comité permanent R peut seulement" sont remplacés par "Sauf si la loi impose son avis, le Comité permanent R peut seulement" sont insérés au début de l'alinéa.

Art. 263

§ 1er. Dans l'article 34 de la même loi, il est inséré après le premier alinéa un nouvel alinéa rédigé comme suit:

"Le Comité permanent R traite également des requêtes en matière de traitements des données à

persoonsgegevens door de inlichtingendiensten en hun verwerkers."

§ 2. In het derde lid, dat het vierde lid wordt, van hetzelfde artikel, worden de volgende wijzigingen aangebracht:

1° het woord "of" wordt vervangen door ",";

2° de woorden "of een verzoek" worden ingevoegd tussen de woorden "een aangifte" en de woorden "die kennelijk".

§ 3. In het vierde lid, dat het vijfde lid wordt, van hetzelfde artikel worden de volgende wijzigingen aangebracht:

1° het woord "of" wordt vervangen door ",";

2° de woorden "of een verzoek" worden ingevoegd tussen de woorden "klacht, aangifte" en de woorden "en om het";

3° de woorden "of het verzoek" worden ingevoegd tussen de woorden "die de klacht" en de woorden "heeft ingediend".

§ 4. Het vijfde lid, dat het zesde lid wordt, wordt aangevuld met de woorden:

"behalve voor onderzoeken met betrekking tot de verwerking van persoonsgegevens door de inlichtingendiensten en hun verwerkers, waar het Vast Comité I enkel antwoordt dat de nodige verificaties werden verricht".

Art. 264

Artikel 35 van dezelfde wet wordt aangevuld met een paragraaf 3, luidende:

"§ 3. Het Vast Comité I brengt jaarlijks verslag uit bij de Kamer van volksvertegenwoordigers omtrent de gegeven adviezen in zijn hoedanigheid van gegevensbeschermingsautoriteit, omtrent de onderzoeken die werden uitgevoerd en de maatregelen die werden genomen in dezelfde hoedanigheid alsook omtrent haar samenwerking met de andere gegevensbeschermingsautoriteiten. Een kopij van dit verslag wordt eveneens gericht aan de bevoegde ministers, alsook aan de Veiligheid van de Staat en aan de Algemene Dienst Inlichting en Veiligheid, die over de mogelijkheid beschikken om het Vast Comité I attent te maken op hun bemerkingen."

caractère personnel par les services de renseignement et leurs sous-traitants."

§ 2. A l'alinéa 3, qui devient l'alinéa 4, du même article, les modifications suivantes sont apportées:

1° les mots "ou à" sont remplacés par ",";

2° les mots "ou une requête" sont insérés entre le mot "dénonciation" et les mots "manifestement".

§ 3. A l'alinéa 5 (ancien alinéa 4) du même article, les modifications suivantes sont apportées:

1° les mots "ou à" sont remplacés par ",";

2° les mots "ou une requête" sont insérés entre le mot "dénonciation" et les mots "et de clôturer";

3° le mot "ou" est remplacé par "," et les mots "ou introduit la requête" complètent l'alinéa.

§ 4. L'alinéa 5, qui devient l'alinéa 6, du même article est complété par les mots:

", sauf en matière d'enquêtes portant sur le traitement des données à caractère personnel par les services de renseignement et leurs sous-traitants où le Comité permanent R répond uniquement que les vérifications nécessaires ont été effectuées".

Art. 264

L'article 35 de la même loi est complété par un paragraphe 3 rédigé comme suit:

"§ 3. Le Comité permanent R fait rapport annuellement à la Chambre des représentants sur les avis rendus en sa qualité d'autorité de protection des données, sur les enquêtes effectuées et mesures prises en cette même qualité ainsi que sur sa collaboration avec les autres autorités de protection des données. Copie de ce rapport est également adressé aux ministres compétents, ainsi qu'à la Sûreté de l'État et au Service Général du Renseignement et de la Sécurité, qui ont la faculté d'attirer l'attention du Comité permanent R sur leurs observations."

Art. 265

In artikel 38, tweede lid, van dezelfde wet wordt het woord “Vast” ingevoegd tussen de woorden “het” en “Comité”.

Art. 265

A l’article 38, alinéa 2, de la même loi, le mot “permanent” est inséré entre les mots “le Comité” et le mot “R”.

Art. 266

In artikel 40, tweede lid, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° de woorden “de klachten en aangiften” worden vervangen door de woorden “de klachten, aangiften en verzoeken”;

2° in de Franse tekst worden de woorden “ce d’appui” opgeheven;

3° de woorden “of handelingen” worden vervangen door de woorden “, handelingen of verwerkingen van persoonsgegevens”.

Art. 266

Dans l’article 40, alinéa 2, de la même loi, les modifications suivantes sont apportées:

1° les mots “les plaintes et dénonciations” sont remplacés par les mots “les plaintes, dénonciations et requêtes”;

2° les mots “ce d’appui” sont supprimés;

3° les mots “ou des actions” sont remplacés par les mots “, des actions ou des traitements de données à caractère personnel”.

Art. 267

In artikel 44 van dezelfde wet, wordt het eerste lid aangevuld met de woorden:

“of in het verwerken van persoonsgegevens of in de informatieveiligheid.”

Art. 267

A l’article 44 de la même loi, l’alinéa premier est complété par les mots:

“dans le traitement des données à caractère personnel ou dans la sécurité de l’information.”

Art. 268

Het tweede lid van artikel 45 van dezelfde wet wordt aangevuld met de woorden “, veiligheidsattesten en veiligheidsadviezen”.

Art. 268

L’alinéa 2 de l’article 45 de la même loi est complété par les mots “, attestations et avis de sécurité”.

Art. 269

In artikel 46 van dezelfde wet worden de woorden “buiten de gevallen bepaald in artikel 13/1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en die bepaald in de artikelen 226 en 227 van de gegevensbeschermingswet” ingevoegd tussen de woorden “een wanbedrijf” en de woorden “, maakt hij”.

Dit artikel wordt aangevuld met een lid, luidende:

“Wanneer een lid van de Dienst Enquêtes I kennis heeft van een wanbedrijf zoals bedoeld in de artikelen 226 en 227 van de gegevensbeschermingswet,

Art. 269

A l’article 46 de la même loi, les mots “en dehors des cas prévus à l’article 13/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et de ceux visés aux articles 226 et 227 de la loi protection des données” sont insérés entre les mots “d’un délit” et les mots “, il en dresse”.

Ce même article est complété par un aliéna rédigé comme suit:

“Lorsqu’un membre du Service d’enquêtes R a connaissance d’un délit visé aux articles 226 et 227 de la loi protection des données, il en informe le Comité

informeert hij zo snel mogelijk het Vast Comité I hierover. Deze laatste verzekert de opvolging volgens de nadere regels bepaald in artikel 54 van deze wet.”.

Art. 270

In hoofdstuk III van dezelfde wet, wordt een afdeling 4 ingevoegd, die de artikelen 51/1 tot 51/4 bevat, luidende: “Afdeling 4. Bevoegdheden van het Vast Comité I als gegevensbeschermingsautoriteit”.

Art. 271

In de nieuwe afdeling van hoofdstuk III van dezelfde wet, worden de artikelen 51/1 tot 51/4 ingevoegd, luidende:

“Art. 51/1. In zijn hoedanigheid van gegevensbeschermingsautoriteit voor de gegevens verwerkt door de inlichtingendiensten en hun verwerkers aangewezen door artikel 95 van de gegevensbeschermingswet, treedt het Vast Comité I ofwel op uit eigen beweging, ofwel op verzoek van een andere gegevensbeschermingsautoriteit, ofwel op verzoek van elke betrokkene.

Art. 51/2. Om ontvankelijk te zijn, moet het verzoek geschreven, gedateerd, ondertekend en gemotiveerd zijn en de identiteit van de betrokkene rechtvaardigen.

Art. 51/3. Het Vast Comité I beslist over de opvolging die het aan het dossier geeft en heeft de bevoegdheid om:

1° te besluiten dat de verwerking is uitgevoerd in overeenstemming met de bepalingen van de reglementering inzake de verwerking van persoonsgegevens;

2° de betrokken inlichtingendienst of diens verwerker te waarschuwen dat een voorgenomen verwerking van persoonsgegevens de reglementering inzake de verwerking van persoonsgegevens kan schenden;

3° de betrokken inlichtingendienst of diens verwerker te berispen wanneer een verwerking geresulteerd heeft in een schending van een bepaling van de reglementering inzake de verwerking van persoonsgegevens;

4° de betrokken inlichtingendienst of diens verwerker te gelasten om een verwerking in overeenstemming te brengen met de bepalingen van de reglementering inzake de verwerking van persoonsgegevens, in

permanent R dans les meilleurs délais. Celui-ci assure le suivi selon les modalités fixées à l’article 54 de la présente loi.”.

Art. 270

Dans le chapitre III de la même loi, est insérée une section 4, comprenant les articles 51/1 à 51/4, intitulée: “Section 4. Pouvoirs du Comité permanent R en tant qu’autorité de protection des données”.

Art. 271

Dans la nouvelle section 4 du chapitre III de la même loi, sont insérés les articles 51/1 à 51/4 rédigés comme suit:

“Art. 51/1. En sa qualité d’autorité de protection des données traitées par les services de renseignement et leurs sous-traitants désignée par l’article 95 de la loi protection des données, le Comité permanent R agit soit d’initiative, soit à la demande d’une autre autorité de protection de données, soit à la requête de toute personne concernée.

Art. 51/2. Pour être recevable, la requête doit être écrite, datée, signée, motivée et justifier de l’identité de la personne concernée.

Art. 51/3. Le Comité permanent R décide du suivi qu’il donne au dossier et a le pouvoir de:

1° conclure que le traitement est effectué en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel;

2° avertir le service de renseignement concerné ou son sous-traitant du fait qu’un traitement envisagé de données à caractère personnel est susceptible de violer la règlementation relative aux traitements des données à caractère personnel;

3° rappeler à l’ordre le service de renseignement concerné ou son sous-traitant lorsqu’un traitement a entraîné une violation d’une disposition de la règlementation relative aux traitements des données à caractère personnel;

4° ordonner au service de renseignement concerné ou à son sous-traitant de mettre un traitement en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel, le

voorkomend geval, op een nader bepaalde manier en binnen een nader bepaalde termijn;

5° een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, op te leggen;

6° het rectificeren of wissen van persoonsgegevens te gelasten;

7° het dossier over te maken aan de procureur des Konings van Brussel, die het informeert van het gevolg dat aan het dossier gegeven wordt.

Art. 51/4. Het Vast Comité I informeert de betrokken inlichtingendienst van de uitgevoerde onderzoeken naar de verwerking van persoonsgegevens van diens verwerkers en hun resultaten.

Wanneer het er kennis van neemt, informeert het Vast Comité I eveneens de betrokken inlichtingendienst van de schendingen van de reglementering inzake de verwerking van persoonsgegevens door andere verwerkingsverantwoordelijken."

Art. 272

In artikel 4, § 2, van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, wordt het tweede lid vervangen als volgt:

"De Gegevensbeschermingsautoriteit is de bevoegde toezichthoudende autoriteit wanneer geen andere wet anders bepaalt."

Art. 273

Artikel 18 van dezelfde wet wordt aangevuld met een tweede lid, luidende:

"De beslissing om op te treden in rechte namens de Gegevensbeschermingsautoriteit wordt genomen door het directiecomité.".

cas échéant, de manière spécifique et dans un délai déterminé;

5° imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;

6° ordonner la rectification ou l'effacement de données à caractère personnel;

7° transmettre le dossier au parquet du procureur du Roi de Bruxelles, qui l'informe des suites données au dossier.

Art. 51/4. Le Comité permanent R informe le service de renseignement concerné des enquêtes effectuées sur le traitement de données à caractère personnel par ses sous-traitants et de leurs résultats.

Lorsqu'il en prend connaissance, le Comité permanent R informe également le service de renseignement concerné des violations de la règlementation relative aux traitements de ses données à caractère personnel par d'autres responsables du traitement."

Art. 272

Dans l'article 4, § 2, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, l'alinéa 2 est remplacé par ce qui suit:

"L'Autorité de protection des données est l'autorité de contrôle compétente lorsqu'aucune autre loi en dispose autrement."

Art. 273

L'article 18 de la même loi est complété par un deuxième aliéna rédigé comme suit:

"La décision d'agir en droit au nom de l'Autorité de protection des données est prise par le comité de direction.".

Art. 274

In dezelfde wet wordt een artikel 54/1 ingevoegd, luidende:

“Art. 54/1

§ 1. Met het oog op de consequente toepassing van de nationale, Europese en internationale regelgeving inzake de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens werken de Gegevensbeschermingsautoriteit en de bevoegde toezichthoudende autoriteiten waarnaar wordt verwezen in de titels 2 en 3 van de wet van XXX betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens nauw samen, voor wat betreft de verwerking van klachten, adviezen en aanbevelingen die raken aan de bevoegdheden van twee of meerdere toezichthoudende autoriteiten.

Onverminderd bijzondere bepalingen, dient de gezamenlijke behandeling van klachten, adviezen en aanbevelingen te gebeuren aan de hand van het “één loket principe” dat zal worden waargenomen door de Gegevensbeschermingsautoriteit.

§ 2. Teneinde de in de eerste paragraaf beoogde samenwerking te verwezenlijken sluiten de toezichthoudende autoriteiten een samenwerkingsprotocol af.”.

HOOFDSTUK II

Opheffingsbepalingen

Art. 275

De wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens, gewijzigd bij de wet van 11 december 1998, en voor de laatste keer bij de wet van 3 december 2017, wordt opgeheven.

Het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens wordt opgeheven.

Het koninklijk besluit van 17 december 2003 tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van bepaalde sectorale comités opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer wordt opgeheven.

Art. 274

Il est inséré dans la même loi un article 54/1 rédigé comme suit:

“Art. 54/1

§ 1er. En vue de l’application cohérente des réglementations nationales, européennes et internationales relatives à la protection des personnes physiques à l’égard du traitement des données à caractère personnel, l’Autorité de protection des données et les autorités de contrôle compétentes visées aux titres 2 et 3 de la loi du XXX relative à la protection des personnes physiques à l’égard des traitements des données à caractère personnel, collaborent ensemble, en ce qui concerne le traitement des plaintes, les avis et les recommandations qui affectent les pouvoirs de deux ou plusieurs autorités de contrôle.

Sans préjudice de dispositions particulières, le traitement conjoint des plaintes, des avis et des recommandations doit se faire sur la base du “principe du guichet unique” qui sera assumé par l’Autorité de protection des données.

§ 2. Afin de réaliser la coopération visée au premier paragraphe, les autorités de contrôle concluent un protocole de coopération.”.

CHAPITRE II

Dispositions abrogatoires

Art. 275

La loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel, modifiée par la loi du 11 décembre 1998, et pour la dernière fois par la loi du 3 décembre 2017, est abrogée.

L’arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel est abrogé.

L’arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée est abrogé.

Artikel 15, § 3, van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens wordt opgeheven.

HOOFDSTUK III

Inwerkingtreding en overgangsbepalingen

Art. 276

Deze wet treedt in werking de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

In afwijking van de eerste lid treedt artikel 20 in werking op de eerste dag van de maand die volgt op het verstrijken van een termijn van zes maanden die ingaat de dag na de bekendmaking ervan in het *Belgisch Staatsblad*.

Art. 277

De wettelijke verplichtingen zoals vastgelegd in de Verordening en in deze wet doen geen afbreuk aan de rechtsgeldigheid van de handelingen die de verwerkingsverantwoordelijke of de verwerker heeft verricht vóór de inwerkingtreding van voormelde verplichtingen.

Art. 278

De internationale overeenkomsten betreffende de doorgifte van persoonsgegevens aan derde landen of internationale organisaties die zijn gesloten vóór 6 mei 2016 en die in overeenstemming zijn met de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens en het vóór die datum van toepassing zijnde Unierecht, blijven van kracht totdat zij worden gewijzigd, vervangen of herroepen.

Art. 279

In afwijking van artikel 276, worden de geautomatiseerde verwerkingssystemen die vóór 6 mei 2016 door de bevoegde autoriteiten bedoeld in titel 2 van deze wet werden opgezet, uiterlijk op 6 mei 2023 in overeenstemming gebracht met artikel 56, eerste paragraaf.

L'article 15, § 3, de la loi du 25 décembre 2016 relative au traitement des données des passagers est abrogé.

CHAPITRE III

Entrée en vigueur et dispositions transitoires

Art. 276

La présente loi entre en vigueur le jour de sa publication au *Moniteur belge*.

Par dérogation à l'alinéa premier, l'article 20 entre en vigueur le premier jour du mois qui suit l'expiration d'un délai de six mois prenant cours le jour suivant sa publication au *Moniteur belge*.

Art. 277

Les obligations légales telles que prévues dans le Règlement et la présente loi ne portent pas préjudice à la légalité des traitements de données à caractère personnel réalisés par le responsable du traitement ou le sous-traitant avant l'entrée en vigueur desdites obligations.

Art. 278

Les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales conclus avant le 6 mai 2016 et qui respectent la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le droit de l'Union tel qu'il est applicable avant cette date restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.

Art. 279

Par dérogation à l'article 276, les systèmes de traitement automatisé installés avant le 6 mai 2016 par les autorités compétentes visées au titre 2 de la présente loi sont mis en conformité avec l'article 56, paragraphe premier, au plus tard le 6 mai 2023.

Art. 280

§ 1. In afwijking van artikel 276, blijven de leden van het Controleorgaan die de eed hebben afgelegd, en daadwerkelijk in functie zijn op het moment van de inwerkingtreding van deze wet en die benoemd werden overeenkomstig artikel 36*ter*/1 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals ingevoegd bij artikel 42 van de wet van 18 maart 2014 betreffende het politionele informatiebeheer en tot wijziging van de wet op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering, van rechtswege aangesteld overeenkomstig de paragrafen 2, 3 en 4 als lid van het Controleorgaan of als lid van de Dienst Onderzoeken in de zin van deze wet tot op het einde van hun sedert 1 september 2015 lopende mandaat van zes jaar. Zij worden vanaf de inwerkingtreding van deze wet en voor de duur van voormeld mandaat geacht van rechtswege te voldoen aan de artikelen 231 en 232 van deze wet.

§ 2. De huidige leden worden van rechtswege aangesteld als lid van het Controleorgaan of van de Dienst Onderzoeken overeenkomstig de nieuwe benoemingsvereisten zoals voorzien door deze wet en overeenkomstig de paragrafen 3 en 4.

§ 3. De Voorzitter van het Controleorgaan blijft van rechtswege aangesteld als voorzitter van het Controleorgaan in de zin van deze wet. Het lid van de Commissie voor de bescherming van de persoonlijke levenssfeer wordt van rechtswege aangesteld als het lid van het Controleorgaan afkomstig uit het openbaar ministerie in de zin van deze wet en de huidige nederlandstalige expert-jurist wordt van rechtswege in de hoedanigheid van expert in de zin van deze wet aangesteld als lid van het Controleorgaan.

§ 4. De drie huidige andere leden, waarvan twee afkomstig uit de politiediensten en één franstalige expert niet-jurist worden van rechtswege aangesteld als lid van de dienst onderzoeken in de zin van deze wet in hun respectievelijke hoedanigheid van lid van de politiediensten en van expert.

§ 5. In afwijking van artikel 231, § 1, van deze wet kan het lid van het Controleorgaan, dat benoemd werd in zijn hoedanigheid van lid van de Commissie voor de bescherming van de persoonlijke levenssfeer, opgeheven door artikel 114 van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, vanaf de inwerkingtreding van deze wet tot het einde van zijn sedert 1 september 2015 lopende mandaat, zijn

Art. 280

§ 1er. Par dérogation à l'article 276, les membres de l'Organe de contrôle qui ont prêté serment, qui sont effectivement en fonction au moment d'entrée en vigueur de cette loi et qui ont été nommés conformément à l'article 36*ter*/1 de la loi du 8 décembre 1992 de la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, comme introduit par l'article 42 de la loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, restent de par la loi désignés conformément aux paragraphes 2, 3 et 4 comme membres de l'Organe de contrôle ou comme membre du service d'enquête dans le sens de cette loi jusqu'à la fin de leur mandat de six ans courant depuis le 1 septembre 2015. Au moment de l'entrée en vigueur de la présente loi et pour la durée de leur mandat précité, ils sont de par la loi réputé de répondre d'office aux articles 231 et 232 de la présente loi.

§ 2. Les membres actuels sont désignés de par la loi comme membre de l'Organe de Contrôle ou du service d'enquêtes en fonction des nouvelles exigences de nomination établies dans la présente loi et conformément aux paragraphes 3 et 4.

§ 3. Le président de l'Organe de Contrôle reste de par la loi désigné comme président de l'Organe de Contrôle au sens de la présente loi. Le membre de la Commission de la protection de la vie privée est désigné de par la loi comme membre de l'Organe de Contrôle venant du ministère public au sens de la présente loi et l'actuelle expert juriste néérlandophone est désigné de par la loi dans la capacité d'expert au sens de la présente loi comme membre de l'Organe de Contrôle.

§ 4. Les trois autres membres actuels, dont deux issus des services de police et un expert non juriste Francophone sont de par la loi désignés comme membre du service d'enquête au sens de la présente loi dans leurs capacité respective de membre des services de police et expert.

§ 5. Par dérogation à l'article 231, § 1er, de la présente loi, le membre de l'Organe de contrôle qui a été nommé en sa qualité de membre de la Commission de la protection de la vie privée, abrogé par l'article 114 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données peut, à partir de l'entrée en vigueur de la présente loi jusqu'à la fin de son mandat qui court depuis le 1er septembre 2015, continuer à

functie hetzij voltijds, hetzij deeltijds blijven uitoefenen. Bij een deeltijdse uitoefening van de functie geniet hij van een wedde gelijk aan 20 % van de wedde voorzien voor de andere leden zoals vermeld in artikel 234.

Gegeven te Brussel, 11 juni 2018

FILIP

VAN KONINGSWEGE:

De minister van Sociale Zaken en Volksgezondheid,

Maggie DE BLOCK

De minister van Justitie,

Koen GEENS

De vice-eersteminister bevoegd voor Binnenlandse Zaken,

Jan JAMBON

De minister van Defensie,

Steven VANDEPUT

De staatssecretaris voor Privacy,

Philippe DE BACKER

excercer la fonction soit à temps plein soit à temps partiel. Lorsqu'il exerce sa fonction à temps partiel, il bénéficie d'un traitement correspondant à 20 % du traitement fixé pour les autres membres par l'article 234.

Donné à Bruxelles, le 11 juin 2018

PHILIPPE

PAR LE ROI:

La ministre des Affaires sociales et de la Santé publique,

Maggie DE BLOCK

Le ministre de la Justice,

Koen GEENS

Le vice-premier ministre en charge de l'Intérieur,

Jan JAMBON

Le ministre de la Défense,

Steven VANDEPUT

Le secrétaire d'État à la Protection de la vie privée,

Philippe DE BACKER

Advies nr. 33/2018 van 11 april 2018

Betreft: Voorontwerp van wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (CO-A-2018-026)

De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna de Commissie);

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna AVG);

Gelet op Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad* (hierna Richtlijn);

Gelet op het verzoek om advies van de heer Philippe De Backer, staatssecretaris voor bestrijding van de sociale fraude, privacy en Noordzee, ontvangen op 20 maart 2018;

Gelet op het verslag van de voorzitter;

Brengt op 11 april 2018 het volgend advies uit:

INHOUDSOPGAVE

BEGRIPPENLIJST

GBA	De Gegevensbeschermingsautoriteit, opgericht door de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*
Commissie	De Commissie voor de bescherming van de persoonlijke levenssfeer
EHRM	Het Europese Hof voor de rechten van de mens
EVRM	Het Europees Verdrag voor de rechten van de mens
BUPO	Het internationaal verdrag inzake burgerrechten en politieke rechten
HvJ	Het Hof van Justitie van de Europese Unie
C.O.C.	Het Controleorgaan op de politionele informatie
Comité P	Het Vast Comité van toezicht op de politiediensten
Comité I	Het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
WVP	Wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*
GBAW	De wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*
AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG*
Richtlijn	Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad*
Ontwerp	Het voorliggende wetsontwerp
Advies	Het voorliggende advies van de Commissie voor de bescherming van de persoonlijke levenssfeer
DPIA	De gegevensbeschermingseffectbeoordeling in de zin van artikel 35 AVG – in het Engels ook wel Data Protection Impact Assessment (DPIA) genoemd.
DPO	De functionaris voor gegevensbescherming in de zin van artikel 37 AVG – in het Engels ook wel Data Protection Officer (DPO) genoemd.
Groep artikel 29	De Groep Gegevensbescherming artikel 29. De groep omvat de nationale toezichthouders, waaronder de Commissie, en geeft advies over de toepassing van de Europese privacywetgeving. Vanaf 25 mei 2018 vervangt het Europees Comité voor gegevensbescherming de Groep Gegevensbescherming artikel 29.

1. INLEIDING

1. Le Dit advies handelt over een voorontwerp van wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna het Ontwerp).

2. Het werd op 20 maart 2018 officieel voor advies voorgelegd aan de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna de Commissie).

3. Het Ontwerp kadert binnen de hervorming van de regelgeving inzake bescherming van persoonsgegevens en volgt op de goedkeuring op 27 april 2016 van de *Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG") en de *Richtlijn 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad* (hierna "Richtlijn").

4. Beide teksten die respectievelijk van kracht zijn geworden op 24 mei 2016 en 5 mei 2016 voorzien elk in een overgangsperiode van 2 jaar.

5. Zo wordt de AVG van toepassing binnen enkele weken, met name op 25 mei 2018. De Richtlijn moet daarentegen omgezet zijn tegen 6 mei 2018.

6. Het Secretariaat van de Commissie heeft tijdens de voorbereidingsfase van het Ontwerp de gelegenheid gekregen om bepaalde suggesties te doen. Maar de Commissie betreurt het dat zij binnen een uiterst korte termijn haar advies moet geven over een tekst van dergelijke omvang die toch van enorm belang is voor de omkadering van persoonsgegevens.

7. De Commissie drukt de wenst uit dat dit advies, hoe kritisch het ook is, zal leiden tot een betere tekst en ze blijft ter beschikking van de aanvrager om mee te helpen dit doel te verwezenlijken.

8. De AVG voorziet - niettegenstaande het bindend karakter ervan - in een aantal gevallen waarin de nationale wetgever naargelang het geval, moet of kan tussenkomen en als het geval zich voordoet, mag dit uitsluitend gebeuren binnen de toegelaten grenzen van de openstellingsbepaling.

9. Deze openstellingsbepalingen zijn zeer uiteenlopend. Bepaalde ervan machtigen de wetgever om de toepassing van de AVG gedetailleerd te omschrijven, andere dienen om te voorzien in uitvoeringsmaatregelen binnen de voorziene opties, nog andere om te voorzien in uitvoeringsmaatregelen die tot doel hebben de AVG verder aan te vullen. In al deze gevallen kunnen deze maatregelen niet ingaan tegen de AVG. Zij moeten worden betekend aan de Europese Commissie, meestal tegen 25 mei 2018.

10. De Richtlijn daarentegen moet binnen de voorziene wettelijke termijn worden omgezet en dit, zoals al vermeld, tegen 6 mei 2018. In het algemeen benadrukt de Commissie dat de tekst van de Richtlijn voor een zeer groot deel in overeenstemming is gebracht met de AVG waarbij rekening is gehouden met de specificiteiten die verband houden met het toepassingsgebied dat eigen is aan de Richtlijn, namelijk de gegevensverwerkingen die worden verricht met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties.

11. De wetgever moet bij zijn voorbereidende werkzaamheden van de uitvoeringsmaatregelen en de omzetting van deze beide Europese teksten de filosofie eerbiedigen waarop zij gebaseerd zijn, de richting die door de Europese omkadering is gewild en natuurlijk ook de letter van deze teksten die gelet op de hiërarchie van de normen, voorrang heeft en eveneens de algemene beginsels inzake gegevensbescherming en inzake de rechtsstaat.

12. De wetgever geeft aan dat hij zich niet beperkt tot het voorstellen van uitvoeringsmaatregelen of omzetting van de hierboven bedoelde Europese teksten, maar dat hij er ook "bijzondere bepalingen" aan toevoegt.

13. Niettemin moet de omkadering van de gegevensbescherming in België de Europese teksten eerbiedigen en een coherente geheel vormen en tevens een daadwerkelijke bescherming van het fundamenteel recht op gegevensbescherming garanderen.

Krachtlijnen van de AVG en de Richtlijn

14. De krachtlijnen van de EU hervorming van het gegevensbeschermingskader worden hierna herhaald: Het is dan ook in het licht van deze krachtlijnen dat de Commissie in voorliggend advies de bepalingen van het Ontwerp heeft onderzocht en uitgeschreven:

- Harmonisering: voor de AVG koos de Europese wetgever voor het juridische instrument waarmee de grootste harmonisering mogelijk is, namelijk een Verordening (AVG) en niet langer een richtlijn zoals dit het geval was in 1995. In diezelfde optiek, opteerde hij voor een lange lijst met geharmoniseerde definities. Tot slot opteert de Europese wetgever voor een gemeenschappelijk beschermingsstelsel voor de private- en overheidssector, waarbij hij aan de nationale wetgever de

mogelijkheid laat om voor de overheidssector de toepassing van de tekst gedetailleerd te omschrijven en dit binnen de beperkingen van de AVG.

- De versterkte rechten voor de betrokkenen staan in deze hervorming centraal. Met deze rechten krijgen de betrokkenen een reële controle over hun gegevens en een daadwerkelijke bescherming zodra zijn gegevens worden verwerkt. Het recht op informatie van de betrokkene, dat voorafgaand noodzakelijk is voor de uitoefening van zijn andere rechten, is versterkt. De versterking van dit recht draagt bij aan het algemeen doel van grotere transparantie wat ook verankerd zit in de tekst. Het recht op uitwissing is verder uitgewerkt evenals het recht op beperking van verwerking. Vanuit diezelfde optiek zijn ook de vereisten ter omkadering van de toestemming als rechtmatigheidsgrond voor de gegevensverwerking, versterkt. Bovendien vloeien deze versterkte rechten ook voort uit bepaalde verplichtingen die de AVG invoert, zoals bijvoorbeeld de bescherming van de gegevens van bij het ontwerp en bescherming van gegevens door standaardinstellingen (artikel 25 AVG). Tot slot biedt de AVG aan de betrokkenen nieuwe instrumenten om een proces te voeren - zoals de collectieve vertegenwoordiging als bedoeld in artikel 80 AVG - met de bedoeling de juridische bescherming van de burgers te versterken en de eerbiediging van hun rechten te doen gelden voor hoven en rechtbanken.

- Schrapping van bepaalde voorafgaande formaliteiten - Accountability: De schrapping van de voorafgaande formaliteiten ten aanzien van de gegevenbeschermingsautoriteit gaat samen met het principe van de verantwoordingsplicht (accountabilty) dat in deze teksten werd uitgewerkt. De verwerkingsverantwoordelijke moet de AVG naleven en moet in staat zijn die naleving aan te tonen. De schrapping van de voorafgaande aangifte van verwerking is symbolisch voor deze paradigmeverschuiving. Dit werd niet lichtzinnig geschrapt maar wel omdat dit in de praktijk niet tegemoetkwam aan de doelen inzake transparantie, reflectie en responsabilisering die in 1995 werden vooropgesteld.

- De nieuwe verplichtingen voor de verwerkingsverantwoordelijken en de verwerkers - risicogebaseerde aanpak: nieuwe verplichtingen zijn opgelegd aan de verwerkingsverantwoordelijken en de verwerkers zoals het houden van een Register van de verwerkingsactiviteiten (art. 30 AVG), een striktere omkadering van het gebruik van verwerkers en verdere verwerking (art. 28 van de AVG), de aanduiding van een functionaris voor gegevensbescherming (art 37 van de AVG), het verrichten van een gegevensbeschermingseffectbeoordeling (art. 35 van de AVG - DPIA) of de kennisgeving van de inbreuken op gegevens aan de gegevensbeschermingsautoriteit en de kennisgeving aan de betrokkene (art.33 en 34 van de AVG). Bepaalde van deze verplichtingen zijn slechts van toepassing als een verhoogd risico verband houdt met de verwerking of het incident. Deze verplichtingen zijn ook ontworpen om de verwerkingsverantwoordelijken en de verwerkers te helpen zich in overeenstemming te brengen met die teksten.

- Versterkte bevoegdheden voor de gegevensbeschermingsautoriteit: het achterwege laten van de meeste voorafgaande formaliteiten bij de toezichthoudende autoriteit en het accountabilitybeginsel gaan samen met grotere bevoegdheden voor de toezichthoudende autoriteit, vooral de corrigerende bevoegdheden, waaronder de mogelijkheid de opschorting of het verbod te eisen van gegevensverwerkingen en de bevoegdheid om afschrikwekkende administratieve boetes op te leggen. Er wordt van de toezichthoudende autoriteit een optreden verwacht dat resoluut gericht is op een *a posteriori* controle. Zijn rol in de bewustmaking van het publiek in het algemeen en informatieverstrekking aan de verwerkingsverantwoordelijken en verwerkers over hun verplichtingen zijn evenzeer van wezenlijk belang.

- Versterkte internationale samenwerking In een gemondialiseerde context worden de gegevensverwerkingen van multinationals, die in meerdere Lidstaten van de unie gevestigd zijn, steeds talrijker. Gezamenlijke onderzoeken, wederzijdse bijstand tussen de gegevensbeschermingsautoriteiten van de Europese Unie worden door de AVG omkaderd, zodat er doeltreffender kan worden opgetreden tegen deze actoren. De keuze voor een verordening die in de praktijk een geharmoniseerde bescherming garandeert, gaat bovendien samen met het opzetten van een zogenaamd "coherentiemechanisme" waarmee de gegevensbeschermingsautoriteiten een overeenkomst kunnen sluiten volgens de procedures als vastgesteld in de AVG over een geharmoniseerde interpretatie en toepassing van de bepalingen van de AVG. Deze samenwerking krijgt uitvoering vanaf 25 mei 2018 binnen het Europees Comité voor Gegevensbescherming (ECG) waarbinnen een nationale toezichthoudende autoriteit die hiertoe werd aangeduid, moet zetelen.

15. De krachtlijnen van de Richtlijn zijn verwant met deze van de AVG waarbij zoals eerder al gemeld, rekening wordt gehouden met de specificiteiten van haar toepassingsgebied.

Veiligheids- en inlichtingendiensten

16. Het Ontwerp ambieert de omkadering van alle verrichte gegevensverwerkingen, met inbegrip van deze die niet vallen onder het toepassingsgebied van het recht van de Europese Unie. Dit is met name het geval voor de verwerkingen die "de inlichtingen- en veiligheidsdiensten" verrichten, hetzij de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid. Die omkadering is voorzien onder Titel III van het Ontwerp. Ook in deze domeinen bestaat er een internationale consensus om de omkadering van de gegevensbescherming te versterken. Een moderniseringsontwerp van het Verdrag van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (STE 108) ligt op tafel van het Comité van Ministers van de Raad van Europa. Zonder vandaag formeel te zijn aangenomen door de deelnemende staten, stemmen de meesten in met de inhoud van deze tekst. Hij integreert op zijn manier (het gaat om een internationaal verdrag en niet om een rechtstreekse toepasbare verordening) de hierboven herhaalde krachtlijnen die terug te vinden zijn in de AVG en Richtlijn.

Methodologie van het advies

17. Als methodologie volgt dit advies over het algemeen de structuur van dit Ontwerp, Titel per Titel. Gelet op deze Titels wordt de analyse aangeboden volgens de behoeften van het advies en de opmerkingen die het Ontwerp aan de Commissie ontlokken worden artikel per artikel zeer gedetailleerd of meer in het algemeen besproken. Zo nodig sluit de Commissie de analyse van elke Titel af met een algemene beoordeling van deze Titel en een lijst met opmerkingen en verzoeken bestemd voor de wetgever. De analyse van Titel 7 bevat eveneens andere artikels die overigens verspreid staan in het Ontwerp.

18. De opmerkingen met betrekking tot Titel 7 zijn essentieel omdat ze betrekking hebben op de doeltreffendheid van het toezicht door de gegevensbeschermingsautoriteiten, waaronder de toekomstige Gegevensbeschermingsautoriteit, die de rechtsopvolger is van de Commissie.

2. ALGEMENE SYNTHESE

Voorafgaande opmerking

19. Deze synthese beperkt zich tot het oplijsten van de grootste bekommernissen van de Commissie, haar belangrijkste aandachtspunten. Ook al bevat deze een aantal verwijzingen, toch moet voor een algemene beoordeling van het Ontwerp de lezing ervan samengaan met een lezing ten gronde van het integrale advies.

Doel van het Ontwerp

20. Het Ontwerp is een ambitieuze tekst dat tegelijkertijd de AVG wil uitvoeren (Titel I), de Richtlijn wil omzetten (Titel II), de gegevensverwerkingen wil omkaderen die niet gedekt zijn door de EU-kaderregeling inzake gegevensbescherming (Titel III) en wil voorzien in bijzondere bepalingen. Aangezien het hier gaat over een Verordening, merkt de Commissie op dat alleen die bepalingen waarvoor de Europese wetgever een opening heeft gelaten voor de nationale wetgever, aangevuld mogen worden met de bepalingen van voorliggend ontwerp en als dit het geval is, binnen de grenzen van de AVG. De Commissie heeft daar bijzondere aandacht aan besteed in haar analyse.

21. Zoals gezegd heeft de wetgever ook de bedoeling om bijzondere bepalingen toe te voegen. De Commissie is evenwel van mening dat niet alle hun plaats hebben in het Ontwerp. Zij moeten in ieder geval, als zij steunen op de concepten van de AVG, de aard en de doelstelling ervan eerbiedigen.

Toepassingsgebied en definities

22. Uit de analyse van de verschillende Titels blijkt duidelijk dat het noodzakelijk is om het precieze toepassingsgebied op te helderen.

23. De Commissie staat positief tegenover de poging van de wetgever om in de Ontwerptekst te voorzien in een oplossing voor conflictsituaties van mogelijke toepasselijke wetten (artikel 4 van het Ontwerp). Aangezien de AVG in meerdere artikels de nationale wetgever de mogelijkheid biedt om het voorgestelde Europees reglementair kader nader te omschrijven of aan te vullen, moet op de vraag welk nationaal recht van toepassing zal zijn, inderdaad een antwoord worden gevonden dat rechtszekerheid garandeert. De Commissie is echter van mening dat de oplossing die het Ontwerp aanbeveelt, niet solide genoeg is en geen reële oplossing biedt. De Commissie doet in dit advies hiertoe een alternatief voorstel.

24. Aangaande de definities, die bijdragen aan de opbouw van een coherente kaderregeling, bepaalt het Ontwerp dat de definities van de AVG van toepassing zijn *«onverminderd de definities bepaald in deze wet »* (art. 5). Dit ingelaste zinnetje zaait verwarring om ze tegenspraak lijkt te zijn met de voorrang van het internationaal recht voor de titels waarop de AVG en de Richtlijn moeten worden toegepast. In dit verband, benadrukt het advies dat Titel 4 die gewijd is aan de verwerkingen met het oog op archivering in algemeen belang, voor wetenschappelijk, historisch of statistisch onderzoek, een reeks definities invoert waarvan sommige afwijken van de AVG. De Commissie verzoekt de schrapping van die definities. In het algemeen moet een globale coherentie bewaard worden in de definities (en in de mate van het mogelijke, ook voor de verwerkingen bedoeld onder Titel III, die niet gedekt zijn door het Unierecht).

    Daarentegen heeft de Commissie geen bezwaar tegen nieuwe definities die een begrip ophelderen dat niet in de AVG is gedefinieerd en waarvoor wordt verwezen naar het nationaal recht of tegen definities van ongedefinieerde woorden die ontegensprekelijk de rechtszekerheid verhogen.

25. Met betrekking tot de oprichting van verschillende "toezichthoudende autoriteiten", is de Commissie van mening dat hun respectievelijke bevoegdheden duidelijk en juridisch coherent moeten worden afgebakend zodat zij hun opdrachten daadwerkelijk en doeltreffend kunnen uitvoeren.

<u>Beperkingen van de rechten van de betrokken personen die ongegrond of in tegenspraak zijn met de AVG</u>

26. De Commissie stelt vast dat het Ontwerp talrijke beperkingen bevat op de rechten van betrokkenen waaronder een groot aantal die haar ongegrond lijkt en in tegenspraak met de AVG. De Commissie herhaalt, net zoals ze dat in de inleiding al deed , dat een van de belangrijkste krachtlijnen van de Europese hervorming precies de versterking van die rechten behelst.

27. Artikel 85.2 van de AVG «Verwerking en vrijheid van meningsuiting en van informatie » machtigt de nationale wetgever om te voorzien in uitzonderingen of afwijkingen op/aan Hoofdstuk III van de AVG, dat gewijd is aan de rechten van de betrokkenen *indien deze noodzakelijk zijn om* het *recht op bescherming van persoonsgegevens in overeenstemming te brengen met de vrijheid van meningsuiting en van informatie.* De Commissie is van mening dat de beperkingen als voorzien in de artikels 18 (recht op beperking van de verwerking) en 21 (recht van bezwaar) van de AVG ongegrond zijn aangezien de afweging van het recht op gegevensbescherming en de vrijheid van meningsuiting en informatie geen afwijking vereisen op het beginsel van de uitoefening van die rechten. Betreffende het recht op gegevenswissing is de Commissie gekant tegen de verklaring als opgenomen in de Memorie van toelichting volgens dewelke dit recht niet van toepassing zou zijn op de verwerkingen met vrije menings- en informatiedoeleinden.

28. Artikel 89 van de AVG "Waarborgen en afwijkingen in verband met verwerkingen met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden", staat de Lidstaten ook toe om te voorzien in afwijkingen op de rechten bedoeld in de artikelen 15, 16, 18 en 21, behoudens de voorwaarden en waarborgen bedoeld onder artikel 89.1. *voor zover* die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, *en dergelijke afwijkingen noodzakelijk zijn om die doeleinden* te bereiken. De Commissie is ook hier van mening dat de afwijkingen op de rechten van de betrokkenen onder Titel 4 die het Ontwerp invoert, in tegenspraak zijn met de AVG.

29. Naast de bovenvermelde artikelen en de eventuele voorziene afwijkingen ten aanzien van elk van de rechten in het artikel dat eraan is gewijd, machtigt artikel 23 van de AVG de Lidstaten om via wetgevende weg de rechten in te perken bedoeld onder de artikelen 12 tot 22 van de AVG. Een dergelijke beperking moet de essentie van de fundamentele rechten en vrijheden eerbiedigen en het moet gaan om een noodzakelijke en proportionele maatregel in een democratische samenleving om een van de redenen als opgesomd in dit artikel, zoals de nationale veiligheid of nationale defensie, om twee van de tien weerhouden redenen te citeren. Een dergelijke maatregel moet minstens de elementen bevatten die opgesomd zijn onder artikel 23.2 AVG (hetzij de identificering van de doeleinden van de verwerking, de categorieën persoonsgegevens, de waarborgen ter voorkoming van misbruik, etc.). In het Ontwerp ontbreken deze elementen in de bepalingen die zich baseren op artikel 23.1. van de AVG. Dientengevolge is de Commissie van oordeel dat deze afwijkingen de vereisten van artikel 23.2 van de AVG niet eerbiedigen voor wat de kwaliteit betreft van de wetgevende maatregel die de afwijking toestaat.

30. De Commissie betreurt dat het Ontwerp zich voor de gezondheids-, genetische en biometrische gegevens niet baseert op artikel 9.4. van de AVG zodat de bijkomende omkaderingsgaranties behouden blijven als voorzien in het bestaande Belgische wetgevend kader en een gelijkwaardig beschermingsniveau behouden blijft met wat vandaag van toepassing is ten gunste van de bescherming van de betrokkenen.

31. *Betreffende de beroepsmogelijkheden* (Hoofdstuk VIII van de AVG), die de rechten van de betrokkenen verder aanvullen, betreurt de Commissie dat de wetgever de onrechtstreekse, werkzame rechtsmiddelen niet toekent aan de betrokken personen, die de AVG nochtans toestaat in uitvoering van artikel 80.2. van *de AVG.*

32. Deze bepaling geeft immers aan de Lidstaten de mogelijkheid erin te voorzien dat elk orgaan, elke instelling of vereniging als bedoeld in artikel 80.1. los van elk mandaat toegekend door de betrokken persoon, in de Lidstaat waarvan sprake, het recht heeft klacht in te dienen bij de toezichthoudende autoriteit die bevoegd is krachtens artikel 77 en om de rechten uit te oefenen bedoeld onder de

artikelen 78 en 79 als zij menen dat de rechten van een betrokkene als bedoeld in deze verordening werden geschonden met het feit van de verwerking.

33. In toepassing van artikel 58.5 van de AVG, bepaalt iedere Lidstaat bij wet dat zijn toezichthoudende autoriteit de bevoegdheid heeft om elke schending van de verordening ter kennis te brengen van de gerechtelijke autoriteiten en eventueel een zaak aanhangig te maken voor het gerecht met de bedoeling de verordening te laten toepassen. Opdat het indienen van dergelijke beroepen rechtsgeldig zou zijn, is de Commissie van mening dat het absoluut noodzakelijk is dat de wetgever de wet van 3 december aanvult met een bepaling waarin nader wordt omschreven dat het aan het Directiecomité van de GBA is om te beslissen over dergelijke beroepsmiddelen. Zo niet, bestaat het gevaar dat elke vordering bij de GBA op ontvankelijkheid gecontesteerd wordt. Onrechtstreeks zouden de betrokkenen op die manier nog een ander beschermingsmiddel voor justitie worden ontzegd.

34. In diezelfde gedachte, verzoekt de Commissie dat een duidelijk juridisch onderscheid wordt gemaakt tussen de partij die in beroep gaat (hetzij GBA) en de vertegenwoordigingsbevoegdheid ervan.

35. Nog altijd met de bedoeling een daadwerkelijke bescherming van de betrokkenen toe te laten, verzoekt de Commissie de wetgever te voorzien in de mogelijkheid een beroep in te dienen om te vermijden dat zich een ernstig gebrek voordoet op het beroepsmodel als bedoeld in artikel 1 van de wet van 12 januari 1993 betreffende een vorderingsrecht inzake bescherming van het leefmilieu.

36. En tot slot, het gebrek aan toepasselijke administratieve boetes voor de overheidssector ook al machtigt artikel 83.7 van de AVG de wetgever om *«regels vast (te) stellen betreffende de vraag of en in hoeverre administratieve geldboeten kunnen worden opgelegd aan in die lidstaat gevestigde overheidsinstanties en overheidsorganen »*, gecombineerd met de strafrechtelijke immuniteit van sommige rechtspersonen van publiek recht (art. 84 van de AVG) en met de afwijkingen - waarvan sommige in dit advies bekritiseerd worden (zie met name artikel 3 van het Ontwerp) - plaatst de overheidssector in een geprivilegieerde positie, in afwijking van het gelijkheidsprincipe met de andere verwerkingsverantwoordelijken en verwerkers van de "privésector. Hoewel het klopt dat de Commissie beschikt over andere vormen van corrigerende bevoegdheden ten aanzien van de overheidssector, neemt dit niet weg dat de doeltreffendheid van haar vordering onvermijdelijk wordt afgezwakt.

<u>Eerbiediging van de artikelen 5.2 en 24 van de AVG</u>

37. Het principe van de verantwoordingsplicht staat in de AVG centraal. Het wordt in de volgende bewoordingen omschreven onder artikel 5.2.: De verwerkingsverantwoordelijke is verantwoordelijk

voor de naleving van lid 1 (van de principes met betrekking tot persoonsgegevensverwerkingen) en kan deze aantonen (verantwoordingsplicht).

38. Artikel 24 bepaalt dan weer dat rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treft om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.

39. Op meerdere plaatsen in het Ontwerp zijn er bepalingen die ingaan tegen dit artikel 24 van de AVG (artikel 3 van het Ontwerp is in dit verband bijzonder problematisch). Daarentegen staat de Commissie positief tegen de invoering van een omkaderingssysteem voor de doorzending van persoonsgegevens door « *de federale overheidsinstanties en de federale openbare organen*» met behulp van af te sluiten protocolakkoorden door de betrokken verwerkingsverantwoordelijken, na advies van hun respectievelijke functionarissen voor gegevensbescherming (DPO). Dit zou een goed accountability-instrument kunnen zijn voor de betrokken verwerkingsverantwoordelijken. De Commissie is echter van mening dat het systeem verplicht zou moeten worden maar dan enkel voor de verwerkingen die een risico vormen, en dit aansluitend op de op risico gebaseerde aanpak die de basis vormt van bepaalde verplichtingen van de AVG. Naast sommige voorgestelde verbeteringen, moeten die protocolakkoorden overigens bekend worden gemaakt.

<u>Ongegronde beperkingen op de verplichtingen van de verwerkingsverantwoordelijken</u>

40. Het Ontwerp voorziet in het Hoofdstuk dat gewijd is aan de verwerkingen voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen, in uitzonderingen op de naleving van bepaalde door de AVG opgelegde verplichtingen ten gunste van de verwerkingsverantwoordelijken en verwerkers (ter terbeschikkingstelling aan de gegevensbeschermingsautoriteit van het Register van de gegevensverwerkingen, de verplichte samenwerking met haar, de verplichte kennisgeving van gegevenslekken, verplichte raadpleging van de AVG over de voorafgaande gegevensbeschermingseffectbeoordelingen die zijn verricht en waaruit blijkt dat het restrisico van de bedoelde verwerking hoog blijft, afwijkingen van het hoofdstuk over het grensoverschrijdend gegevensverkeer).

41. Aangaande de uitzondering op de verplichte terbeschikkingstelling van het Register van verwerkingsactiviteiten op verzoek van de GBA (artikel 30.4 van de AVG), meent de Commissie dat dit niet noodzakelijk is en dus ingaat tegen de AVG; immers, de AVG vereist niet van het Register dat het de identiteit bevat van de personen van wie de gegevens worden verwerkt. De afweging van beide voormelde fundamentele rechten rechtvaardigt dus deze uitzondering niet. Hetzelfde geldt voor de artikelen 33 (kennisgeving van inbreuken (lekken) op gegevens en 36 (voorafgaande

raadpleging van de GBA voor de DPIA). In geen van deze gevallen zal de uitvoering van deze verplichtingen ertoe leiden dat de inhoud van een te publiceren persartikel aan de gegevensbeschermingsautoriteit wordt onthuld.

Verplichtingen die deze van de AVG aanvullen, opgelegd aan de verwerkingsverantwoordelijken en verwerkers en die in tegenspraak zijn met het onderliggend doel van deze verplichtingen in de AVG

42. *Functionaris voor gegevensbescherming* - Artikel 37.4. van de AVG laat aan de nationale wetgever de mogelijkheid om gevallen toe te voegen waarin een aanduiding van een functionaris voor gegevensbescherming (DPO) verplicht is. Artikel 37.1. van de AVG somt drie gevallen op waarin deze aanduiding - in toepassing van de AVG - verplicht is. Deze 3 gevallen kunnen naargelang de wensen van de nationale wetgever verder worden aangevuld. De Commissie merkt op dat de twee bijkomende gevallen waarbij het verplicht is een functionaris voor gegevensbescherming aan te duiden, als bedoeld in de artikelen 25 en *91* van het Ontwerp, afwijken van de filosofie achter de risicogebaseerde aanpak van de AVG. Inderdaad, de gevallen van een verplichte aanstelling van een functionaris voor gegevensbescherming in artikel 37.1 - wat zeker bijdraagt aan een daadwerkelijk uitvoering van de AVG - zijn verbonden met een risicofactor (verwerking van gevoelige gegevens, volgen van gedrag van personen, grote schaal, basisactiviteiten). Daarentegen worden de nieuwe gevallen gerechtvaardigd met het simpele feit van het doeleinde voor de verwezenlijking van verwerkingen voor archivering in algemeen belang, onderzoek of statistiek (artikel 191 van het Ontwerp) of het feit dat de overheden beroep doen op een verwerker (artikel 25 van het Ontwerp beoogt alle rechtspersonen van privaat recht die tussenkomen als verwerker in de bovenbedoelde federale openbare organen of particuliere organen en/of bij hen persoonsgegevens inzamelen), zelfs al zijn zij zelf verplicht een functionaris voor gegevensbescherming aan te duiden. Deze laatste voorwaarde sluit niet uit dat ook de verwerker hiertoe verplicht is als hij valt binnen de gevallen bedoeld onder artikel 37.1. van de AVG. Maar daarvan een algemene verplichting maken is evenwel bovenmatig, zo meent de Commissie.

43. *Register van de verwerkingsactiviteiten* - De Commissie vestigt er ook de aandacht op - tenminste dat is wat zij meent te begrijpen uit de bepalingen van Titel I - dat de verplichting om deel te nemen aan een centraal Register van verrichte verwerkingen in de overheidssector en toegankelijk wordt voor de betrokkenen, niet echt kan gezien worden als een uitvoeringsmaatregel van de AVG. Het streven naar transparantie is prijzenswaardig als principe maar kan niet worden verward met het verplicht bijhouden van een intern Register van verwerkingsactiviteiten als bedoeld in artikel 30 van de AVG. Deze bijkomende verplichting waarin het Ontwerp voorziet wijkt af van het doel van het Register dat niet dient om de betrokkenen rechtstreeks te informeren en geeft aan de Commissie het gevoel dat de verplichting van de voorafgaande aangifte van gegevensverwerkingen bij de toezichthoudende autoriteit in zekere zin opnieuw wordt ingevoerd terwijl er unanimiteit was over de schrapping ervan omdat dit niet langer strookt met het accountabilitybeginsel dat de AVG

aanhangt. Iedereen was het erover eens dat deze verplichte voorafgaande aangifte niet tegemoetkwam aan het transparantiedoel ten aanzien van de betrokkenen noch aan de bewustmaking van de verwerkingsverantwoordelijken en de omzetting hiervan in concrete maatregelen om in overeenstemming te zijn met de regels inzake gegevensbescherming. Het vormde een zware administratieve last waarbij de doelen niet werden bereikt. Het is ten aanzien van de administratieve transparantie dat een actief bekendmakingssysteem zou moeten worden ingevoerd zodat de ondoorgrondelijkheid van de doorgiftes van persoonsgegevens tussen administraties kleiner wordt. Er wordt in dit verband een voorstel gedaan.

Betreffende Titel IV gewijd aan verwerkingen, met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden

44. De Commissie beoordeelt Titel IV in zijn geheel ongunstig. De Commissie is immers van mening dat de ingevoerde bepalingen in tegenspraak zijn met de AVG. Zij beperken bovendien de onderzoeks- en statistische activiteiten die niet uitsluitend voorbehouden zijn voor universiteiten of andere onderzoekscentra maar worden meer in het algemeen verricht door elke type structuur, ongeacht de omvang of basisactiviteit.

Nationale toezichthoudende autoriteit

- ✓ De oprichting van drie bijkomende Belgische DPA's

45. De Commissie stelt vast dat in het Ontwerp drie nieuwe DPA's worden opgericht: het C.O.C., het Comité I en het Comité P. Dit evident bovenop de reeds door de GBAW opgerichte DPA, met name de GBA (en ook bovenop een apart toezicht op de gerechten in het kader van hun gerechtelijke taken[1]). In totaal zou de federale wetgever dus vier DPA's creëren (en wellicht nog een apart toezichtsorgaan voor de gerechten).

46. De Commissie neemt akte van deze beleidskeuzes en gaat in dit advies wel na in welke mate de concretisering van deze politieke keuzes in de tekst van het Ontwerp: (1) leidt tot een duidelijke/coherente/efficiënte bevoegdheidsverdeling tussen de DPA's[2] en (2) strookt met alle regels die in de AVG en in de Richtlijn aan DPA's worden opgelegd en coherent is met de GBAW.

47. De Commissie is van oordeel dat het uittekenen van een sluitende bevoegdheidsverdeling tussen de verschillende Belgische DPA's cruciaal is. Gezamenlijke/overlappende bevoegdheden moeten

[1] Cf artikel 4, §2, eerste lid GBAW en overweging 20 AVG.
[2] De Commissie heeft er evident alle belang bij dat er een duidelijke regeling wordt voorzien, aangezien haar rechtsopvolger – de GBA – vanaf 25 mei 2018 in dit landschap een centrale rol zal moeten opnemen.

hierbij zoveel mogelijk vermeden worden omdat dit tot rechtsonzekerheid leidt en omdat dit ook hoogst inefficiënt is.

48. De Commissie stelt vast dat de bevoegdheidsverdeling die in het Ontwerp voorzien wordt bijzonder complex is.

49. De Commissie dringt er dan ook op aan dat het Ontwerp op dit punt herzien wordt.

50. De Commissie vestigt de aandacht erop dat zowel het C.O.C. als het Comité P en het Comité I als toezichthoudende autoriteit gekwalificeerd worden. Het C.O.C. beschikt evenwel niet over alle bevoegdheden als vereist in de AVG, in toepassing van de artikels 57 en 58. Voor het Comité P en Comité R, wordt verwezen naar Titel 7.

51. De hiernavolgende opmerking houdt rechtstreeks verband met de voorgaande opmerking betreffende de oprichting van meerdere toezichthoudende autoriteiten.

52. Noch de wet GBA noch het Ontwerp bevatten bepalingen betreffende de internationale samenwerking die, nochtans zoals gezegd in de inleiding, centraal zal staan binnen de GBA vanaf 25 mei 2018. In toepassing van artikel 51.3 van de AVG *«Wanneer er in een lidstaat meer dan één toezichthoudende autoriteit is gevestigd, wijst die lidstaat de toezichthoudende autoriteit aan die die autoriteiten in het Comité moet vertegenwoordigen en stelt hij de procedure vast om ervoor te zorgen dat de andere autoriteiten de regels in verband met het in artikel 68 bedoelde coherentiemechanisme naleven».*

53. De Commissie meent dat voor deze kwestie absoluut een werkbare en doeltreffende oplossing moet worden gevonden. Wanneer de wetgever daarin niet voorziet, bestaat het risico op een "lege stoel". Als voorbeeld, de Commissie ontvangt vandaag al aanvragen voor goedkeuring van sectorale gedragscodes die een Europese bestemming hebben waarover zij na 25 mei niet langer alleen zal kunnen beslissen. Dergelijke verzoeken zullen moeten passeren via het coherentiemechanisme in toepassing van artikel 64.1.b. van de AVG. Maar welke DPA zal voor België aan de werkzaamheden deelnemen?

54. Als conclusie van haar analyse, verleent de Commissie een **ongunstig advies** op de bepalingen van het Ontwerp die betrekking hebben op de drie nieuwe DPA's[3], gelet op het feit dat: (1) de bevoegdheidsverdeling tussen de 4 federale DPA's complex is , (2) de hervorming van het C.O.C. niet ver genoeg gaat en op sommige punten niet conform is aan de Europese regels.

[3] Zie in hoofdzaak artikelen 73, 97 t.e.m. 100, 107.8, 130 t.e.m. 133, 163, 186 & Titel 7 van het Ontwerp.

55. De Commissie schuift **twee alternatieve pistes** naar voor om toch tot een Belgisch dataprotectie-landschap te kunnen komen dat logisch en efficiënt geordend is.

Ongegronde beperkingen van de bevoegdheden van de Toezichthoudende autoriteit en eerbiediging van haar onafhankelijkheid

56. Het Ontwerp voorziet in het Hoofdstuk dat gewijd is aan de verwerkingen voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen in afwijkingen op de uitoefening van bevoegdheden van de toekomstige gegevensbeschermingsautoriteit (GBA).

57. Wat de uitzondering betreft op de verplichte samenwerking van de verwerkingsverantwoordelijke met de Gegevensbeschermingsautoriteit (artikel 31 van de AVG) voorzien in artikel 29, § 9 van het ontwerp en de beperking van alle bevoegdheden van de Gegevensbeschermingsautoriteit ten opzichte van deze verwerkingen wanneer hun toepassing "aanwijzingen zou verschaffen over de bronnen van *informatie of wanneer de toepassing ervan een controlemaatregel voorafgaandelijk aan de publicatie van een artikel zou uitmaken" bedoeld in artikel* 29, § 11 van het ontwerp, stelt de Commissie het overmatig karakter hiervan vast. De afwijking op artikel 31 van de AVG is niet noodzakelijk aangezien de toepassing ervan geen verplichting inhoudt tot het onthullen van de informatiebronnen.

58. Anderzijds bepaalt het Ontwerp dat het Register van de verwerkingen van de "openbare sector" (waarvan sprake in de artikelen 23-24 van het Ontwerp) bij de toezichthoudende autoriteit wordt bijgehouden. De Commissie is van mening dat dit Register (wanneer het wordt behouden ondanks de opmerkingen van de Commissie in voorliggende advies), niet kan worden bijgehouden bij de toezichthoudende autoriteit, met name omwille van de budgettaire kost die het hosten van dit Register zou betekenen. Anderzijds, nog fundamenteler, meent de Commissie dat deze hosting bij de toezichthoudende autoriteit onverenigbaar zou zijn met het accountability- en onafhankelijkheidsbeginsel die de toezichthoudende autoriteit ook ogenschijnlijk, moet garanderen.

Overeenstemming van de Memorie van toelichting met de AVG - Correcties

59. Op meerdere plaatsen in het Ontwerp is een op elkaar afstemmen van de AVG en de Memorie van Toelichting noodzakelijk.

Legistiek

60. Een zuiver legistieke opmerking betreft het feit dat het Ontwerp op meerdere plaatsen bepalingen van de AVG onnodig herhaalt.

3. VOORAFGAANDE TITEL (art. 1 – 5)

3.1. Materieel toepassingsgebied van het ontwerp

Artikel 2

61. De WVP is van toepassing op "*elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op elke niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen*" en dit ongeacht de sector waarin de verantwoordelijke voor de verwerking actief is.

62. De bedoeling van de wetgever is deze lijn door te trekken "*teneinde ervoor te zorgen dat geen enkel domein buiten de regelgeving valt, wat rechtsonzekerheid zou creëren en een juridisch vacuüm ten opzichte van de situatie van vandaag alsook onze verplichtingen krachtens het Verdrag 108.*"

63. De Commissie onderschrijft dit opzet volledig.

64. De noodzaak om in artikel 2 van het ontwerp een uitzondering op te nemen voor de Krijgsmacht is onduidelijk. Een expliciete afwijking van het tweede lid (dat de AVG overeenkomstig van toepassing verklaart) is overbodig, daar het derde lid titels 2 en 3 (waarin de Krijgsmacht is opgenomen) hieraan al onttrekt. Bepalen dat "onverminderd artikel 107 deze wet niet van toepassing [is]" is eveneens overbodig, daar de structuur van het ontwerp reeds tot gevolg heeft dat enkel artikel 107 de beoogde verwerkingen door de Krijgsmacht regelt. De Commissie is van oordeel dat het laatste lid van artikel 2 van het ontwerp geschrapt dient te worden.

Artikel 3

65. Artikel 3, eerste lid van het ontwerp herhaalt artikel 1.3 AVG met toevoeging van 'vrij verkeer op het Belgisch grondgebied': "*Het vrije verkeer van persoonsgegevens* ***op het Belgische grondgebied*** *wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens*". De Memorie van toelichting licht toe "*Dit betekent dat een verwerkingsverantwoordelijke een gegevensstroom niet kan blokkeren onder het voorwendsel van het garanderen van de bescherming van persoonsgegevens.*"

66. Artikel 3 tweede lid van het ontwerp vervolgt:

67. *"In het bijzonder kan de uitwisseling van persoonsgegevens tussen de verwerkingsverantwoordelijken, de bevoegde overheden, de diensten, organen en de ontvangers die zich in de titels 1 tot 3 van deze wet bevinden et (sic) die binnen het kader van de doelstellingen*

bedoeld in artikel 23.1.a) tot h) van de Verordening werken niet worden beperkt noch verboden omwille van dergelijke redenen, onverminderd de bevoegdheden van de bevoegde toezichthoudende autoriteit."

68. Deze ontwerp-bepaling is om verschillende redenen hoogst problematisch.

69. Het eerste lid van deze bepaling overtreedt het overschrijfverbod zonder dat hiervoor een verantwoording gegeven wordt. De Commissie ziet overigens geen reden om de doelstelling van de AVG te kopiëren.

70. Wat de toevoeging van het 'Belgisch grondgebied' betreft, merkt de Commissie op dat artikel 1 AVG geen nationale specificatieclausule bevat die een afwijking toelaat. De verenigbaarheid van deze bepaling het de hogere rechtsnorm moet daarom zorgvuldig onderzocht worden.

71. Aldus de Memorie van toelichting betekent deze bepaling "*dat een verwerkingsverantwoordelijke een gegevensstroom niet kan blokkeren onder het voorwendsel van het garanderen van de bescherming van persoonsgegevens.*" Deze zienswijze is manifest in strijd met de verantwoordingsplicht vervat in de artikelen 5.2 en 24 AVG. Een verwerkingsverantwoordelijke die weet dat een ontvanger het gegevensbeschermingsrecht met de voeten treedt moet uiteraard de mededeling van persoonsgegevens stopzetten. Overigens lijkt deze bepaling de verwerkingsverantwoordelijke elke keuzevrijheid te ontnemen, telkens een derde hem vraagt om persoonsgegevens mee te delen moet hij dit doen[4], hetgeen manifest in strijd is met onder meer het doelbindingsbeginsel vervat in art. 5.1.b AVG.

72. Uit de Memorie van toelichting blijkt dat het tweede lid ingegeven is om te garanderen dat de overheid zijn missies kan volbrengen (continuïteit van de publieke dienstverlening)[5]. Dit is een belangrijke bezorgdheid, maar de Commissie meent dat het ontwerp onbedoeld ernstige gevolgen heeft voor de rechten en vrijheden van betrokkenen. Elke uitwisseling van persoonsgegevens moet conform de geldende regels gebeuren. Net zoals hierboven gesteld, kan niet aan de verwerkingsverantwoordelijke opgelegd worden om in te gaan op elk verzoek tot mededeling van persoonsgegevens.

73. De verwijzing naar artikel 23 AVG voldoet niet aan de daarin gestelde voorwaarden. Het volstaat niet om te verwijzen naar de doelstellingen opgesomd in art. 23.1.a-h AVG. De wetgeving moet de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laten (art. 23.1 AVG)

---

[4] Behoudens eventueel gevallen waar redenen buiten het gegevensbeschermingsrecht de mededeling verbieden.
[5] *"Een overheidsdienst mag vooral dus nooit tekort komen aan het volbrengen van zijn opdrachten om een reden gelinkt aan de gegevensbescherming. Elke overheidsdienst moet dus zijn opdrachten volbrengen met respect van het wettelijk kader inzake de gegevensbescherming. Het is van essentieel belang dat de nodige gegevensstromen en proportioneel aan het volbrengen van zijn openbare opdrachten gebeuren in naleving van de Verordening en de huidige wet."*

en de garanties vermeld in artikel 23.2 AVG vervullen. Overigens laat artikel 23 AVG de wetgever niet toe om instanties geheel te onttrekken aan de AVG, maar enkel om bepaalde rechten te beperken.

74. Een verwerkingsverantwoordelijke die persoonsgegevens meedeelt op vraag van de overheid kan deze ontwerp-bepaling niet inroepen om in alle omstandigheden te ontsnappen aan de toezichtsbevoegdheden van de GBA geregeld in de artikelen 58.2 AVG en 83 AVG, of aan het rechterlijk toezicht bepaald in artikel 79 AVG. Ondenkbaar is dat de verwerkingsverantwoordelijke zou moeten wachten op het ingrijpen van de GBA of een rechter vooraleer een onrechtmatige mededeling te mogen stopzetten. Het signaal geven aan overheden die doelstellingen van artikel 23.1.a-h AVG nastreven dat zij zich geen zorgen hoeven te maken om gegevensbeschermingsregels zolang de bevoegde autoriteit niet tussenkomt, is geheel onaanvaardbaar. Dit signaal staat in schril contrast trouwens met het belang dat de Memorie van toelichting zegt te hechten aan gegevensbescherming.[6]

75. De Commissie is van oordeel dat dit artikel geschrapt moet worden. Overigens bevat het ontwerp elders reeds bepalingen die toepassing maken van artikel 23 AVG (zie verder).

3.2. Territoriaal toepassingsgebied van het ontwerp

Artikel 4

76. Artikel 4 van het ontwerp omschrijft het territoriaal toepassingsgebied en volgt hierbij de krijtlijnen van artikel 3 AVG.

77. De Commissie merkt op dat de Memorie van toelichting niet overeenstemt met de inhoud van de ontwerpbepaling, noch met artikel 3 AVG. De Memorie luidt als volgt:

78. *"Het gaat om een bepaling waarin het territoriale toepassingsgebied wordt bepaald, waarin enerzijds de vestiging van de verwerkingsverantwoordelijke of de verwerker wordt opgenomen en anderzijds het gegeven zich op het Belgische grondgebied te bevinden voor de betrokkene teneinde de toepassing van het recht en de procedures te vergemakkelijken. Gelet op de uniforme regels in de Europese Unie zal in beginsel een zekere samenhang worden behouden. In de gevallen waarin beoordelingsruimte voor de lidstaten van de Europese Unie bestaat, zou een dergelijke territoriale regeling tot een wetsconflict kunnen leiden. Het criterium van de verblijfplaats/het gegeven dat de betrokkene zich op het Belgische grondgebied bevindt, moet evenwel tevens behouden blijven*

[6] *"Elke overheidsdienst moet dus zijn opdrachten volbrengen met respect van het wettelijk kader inzake de gegevensbescherming. Het is van essentieel belang dat de nodige gegevensstromen en proportioneel aan het volbrengen van zijn openbare opdrachten gebeuren in naleving van de Verordening en de huidige wet."*

teneinde de betrokkene eventueel tegen minder bindende regels te beschermen. Hierbij kan worden gedacht aan de leeftijd van het kind of de toestemming om gevoelige gegevens te verwerken, terwijl dat in België niet mogelijk is."

79. Het criterium dat de betrokkene zich op het Belgische grondgebied bevindt is enkel relevant voor niet in de EU gevestigde verwerkingsverantwoordelijken en verwerkers, maar speelt in het ontwerp geen zinvolle rol in de oplossing van wetsconflicten tussen lidstaten onderling daar waar de AVG beoordelingsruimte laat aan de nationale wetgever om de AVG verder in te vullen.

Het ontwerp is van toepassing op de activiteiten van de verwerkingsverantwoordelijke of een verwerker op het Belgische grondgebied. Verwerkingsverantwoordelijken gevestigd in een andere lidstaat kunnen de persoonsgegevens van betrokkenen die in België verblijven verwerken volgens de regels die gelden in hun eigen lidstaat – voor zover ze geen in België gevestigde verwerker onder de arm nemen. Strengere Belgische regels rond de verwerking van gevoelige gegevens zouden dus niet gelden, in tegenstelling tot hetgeen de Memorie van Toelichting impliceert.

80. Onduidelijk is de situatie van de verwerkingsverantwoordelijke gevestigd in een andere lidstaat die een Belgische verwerker inschakelt. Het ontwerp creëert een wetsconflict maar regelt de oplossing ervan niet. De verwerkingsverantwoordelijke is gebonden door de wetgeving van diens lidstaat bij het formuleren van instructies aan de Belgische verwerker, die op zijn beurt gebonden is door Belgische wetgeving die de AVG implementeert. Rechtsonzekerheid over welke Belgische bepalingen van toepassing zijn op de verwerker en doorwerken op de activiteiten van de verwerkingsverantwoordelijke is een concurrentieel nadeel voor Belgische verwerkers. Het probleem stelt zich overigens ongeacht of er Belgische betrokkenen gemoeid zijn bij de verwerking in kwestie.

81. Een piste van hoe het wetsconflict inzake verwerkers gevestigd in België geregeld kan worden is te vinden in de geldende Oostenrijkse wetgeving. De basisregel is daar dat de wet van toepassing is op elke verwerking van persoonsgegevens die in Oostenrijk ondernomen wordt of aangestuurd door een in Oostenrijk gevestigde verwerkingsverantwoordelijke. Voor verwerkers is volgende afwijking pertinent:

82. *"[] het recht van het land waarin de verwerkingsverantwoordelijke is gevestigd, is van toepassing op een verwerking van persoonsgegevens in [Oostenrijk], voor zover een verwerkingsverantwoordelijke uit de private sector […] met vestiging in een andere lidstaat van de EU persoonsgegevens verwerkt in Oostenrijk voor een doeleinde dat geen in Oostenrijk gelegen filiaal toegerekend moet worden."*[7]

[7] Vrije vertaling van "*(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck*

83. De Commissie dringt aan op een verduidelijking van de ontwerp-bepaling.

Definities

84. Artikel 5 van het ontwerp luidt als volgt:

"Onverminderd de definities bepaald in deze wet, zijn de definities van de Verordening van toepassing."

85. Voor de toegankelijkheid van de regelgeving is het inderdaad wenselijk expliciet te verwijzen naar de vindplaats van de definities in de AVG. De toevoeging "*Onverminderd de definities bepaald in deze wet*" is een formulering die tot verwarring leidt. Het woord "onverminderd" wordt vaak begrepen als een voorbehoud, hetgeen zou inhouden dat aan de definities opgenomen in de nationale wet voorrang wordt gegeven boven deze van de AVG, die een hogere rechtsnorm is. Dit is problematisch met name in titel 4 waar een aantal kernbegrippen uit de AVG opnieuw gedefiniëerd worden (zie verder). De Raad van State, afdeling wetgeving, beveelt aan het woord 'onverminderd' te vermijden en in de plaats 'los van' te gebruiken (Beginselen van de wetgevingstechniek, nr. 3.2).

86. De Commissie meent dat deze zinssnede geschrapt of aangepast moet worden.

CONCLUSIE van de Commissie over de voorafgaande titel van het ontwerp

87. Het advies van de Commissie met betrekking tot deze voorafgaande titel is dan ook globaal genomen ongunstig. Artikel 3 moeten geschrapt worden voor de hierboven aangehaalde redenen. De artikelen 2, 4 en 5 moet de aanvrager grondig aanpassen en verduidelijken om te voldoen aan de opmerkingen van de Commissie.

verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist." - §2, 2de lid van de Oostenrijkse Datenschutzgesetz 2000, https://www.dsb.gv.at/gesetze-in-osterreich .

4. TITEL 1: DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS

4.1. Hoofdstuk I – Algemene bepalingen

Uitvoering van de AVG

88. Artikel 6 van het ontwerp bepaalt "Met uitzondering van de verwerkingen bedoeld in de titels 2 en 3, en onverminderd bijzondere bepalingen, geeft deze titel uitvoering aan de Verordening".

89. Voor alle duidelijkheid en rechtszekerheid zou het aangewezen zijn het materieel toepassingsgebied van titel 1 van het ontwerp af te bakenen door bijvoorbeeld te verduidelijken dat dit van toepassing is op alle in artikel 2, 1ste lid bedoelde gegevensverwerkingen, met uitzondering van deze bedoeld in de titels 2 en 3.

4.2. Hoofdstuk II – Beginselen van verwerking

Uitvoering van artikel 8.1 AVG

90. Betreffende artikel 7 van het ontwerp, dat de leeftijd verlaagt vanaf welke minderjarigen alleen toestemming kunnen verlenen voor de verwerking van hun gegevens bedoeld in artikel 8.1 van de AVG, verwijst de Commissie naar het persbericht dat zij hierover uitbracht: «*De Privacycommissie ondersteunt de keuze van de Belgische wetgever om de leeftijd voor ouderlijke toestemming krachtens [artikel 8 van][8] de AVG te verlagen tot 13 jaar. Deze leeftijd sluit beter aan bij de dagdagelijkse praktijk waarbij heel wat jongeren zich reeds vanaf jonge leeftijd online begeven. We mogen hen hierbij geen kansen ontnemen om zich digitaal te ontwikkelen. Maar omdat kinderen zich ook bewust moeten zijn van hun privacy moet de keuze voor 13 jaar gepaard gaan met extra inspanningen om kinderen van jongs af mediawijs gedrag aan te leren.*»

91. Omwille van de duidelijkheid dient artikel 7 te preciseren dat het artikel 8.1. van de AVG uitvoert. Dit artikel van de AVG heeft immers een beperkte draagwijdte aangezien het enkel de verwerkingen beoogt uitgevoerd door de aanbieders van online informatiediensten die zich rechtstreeks tot de kinderen wenden (art. 8.1. van de AVG). En artikel 8.3 AVG blijft overigens van toepassing, de geldigheid van de verleende toestemming doet geen afbreuk aan het algemene overeenkomstenrecht van de lidstaten. Bijgevolg, bij gebrek aan verduidelijking dat artikel 7 enkel paragraaf 1 van artikel 8 uitvoert, geeft de tekst van het voorontwerp de indruk artikel 8.3 te overschrijden.

[8] Deze termen tussen […] werden toegevoegd ten opzichte van het vermelde persbericht.

Uitvoering van artikel 9.2.g) AVG

92. Artikel 8 van het voorontwerp stelt artikel 9.2.g van de AVG uit te voeren en herneemt de verwerkingen bedoeld in artikel 3 § 6 van de huidige Privacywet (child focus), in artikel 6, §1, k van dezelfde wet (verwerking van gevoelige gegevens door de vzw voor de verdediging van de rechten van de mens) en in artikel 6, § 3, steeds van de Privacywet (begeleiding en behandeling van daders van seksuele misdrijven), door deze te beschouwen als verwerkingen die noodzakelijk zijn om gewichtige redenen van algemeen belang.

93. Bij het lezen vormt artikel 8 van het ontwerp geen uitvoeringsmaatregel van artikel 9.2.g van de AVG krachtens hetwelk de wettelijke bepaling ter omkadering van de verwerking van gevoelige gegevens in de zin van artikel 9.2.g van de AVG niet alleen dient te beantwoorden aan gewichtige redenen van algemeen belang, maar eveneens de bedoelde verwerkingen zodanig dient te omkaderen dat het proportionaliteitsbeginsel wordt gerespecteerd (bepaling van de categorieën verwerkte gegevens, precieze bepaling van de bestemmelingen en de personen die over een recht op raadpleging beschikken, omstandigheden die de verschillende soorten verwerkingen rechtvaardigen, bewaringstermijn...) en voorzien in gepaste en specifieke maatregelen voor het vrijwaren van de fundamentele rechten en belangen van de betrokkenen. Welnu, artikel 8 van het ontwerp beperkt er zich toe een lijst op te stellen van redenen die bestempeld worden als gewichtige redenen van algemeen belang. Aangezien het gaat om een afwijking op het principiële verbod op de verwerking van gevoelige gegevens, zijn deze waarborgen bijzonder essentieel en onontbeerlijk.

94. Wat de verwerkingen van gevoelige gegevens door child focus betreft (momenteel bedoeld in artikel 8, 1ste lid, 2° van het ontwerp) zijn de garanties die momenteel voorkomen in artikel 3 van de Privacywet - namelijk (i) het verbod voor het Centrum om een bestand te houden betreffende personen die ervan verdacht worden een misdaad of wanbedrijf te hebben begaan of van veroordeelde personen, (ii) de verplichting om te beschikken over een DPO, (iii) de onderwerping van de personeelsleden aan de geheimhouding in de zin van artikel 458 van het Strafwetboek, (iv) het verbod op het opnemen van telefoongesprekken zonder voorafgaande kennisgeving aan de oproeper en voor zover hij zich daartegen niet heeft verzet - verdwenen. Er wordt aanbevolen dat een wettelijke bepaling die conform artikel 9.2.g van de AVG is, wordt opgenomen in een autonome wettekst.

95. Vervolgens meent de Commissie dat artikel 8, 1ste lid, 1° van het ontwerp onnodig is aangezien artikel 9.2.d van de AVG reeds het verbod op de verwerking van gevoelige gegevens in de zin van artikel 9 van de AVG opheft te voordele van "*een stichting, een vereniging (...) zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband*

met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt".

96. Zo wordt de hypothese bedoeld in artikel 8, 1ste lid, 3° van het ontwerp reeds omkaderd door artikel 9.2.h van de AVG. In dat geval dient de verwerking te worden uitgevoerd door een beroepsbeoefenaar in de gezondheidszorg die tot geheimhouding is gehouden of door een derde die eveneens tot een wettelijke of deontologische geheimhouding is gehouden (art. 9.3 AVG)

97. Tenslotte, indien de auteur van het ontwerp een wettelijke basis wil behouden voor eventuele koninklijke besluiten die werden goedgekeurd ter uitvoering van artikel 6 van de huidige Privacywet, dient hiertoe een specifieke wettelijke bepaling te worden opgenomen in de slotbepalingen van onderhavig ontwerp.

98. La Commissie stelt vast dat de wetgever geen gebruik heeft gemaakt van de mogelijkheid die hem wordt geboden door artikel 9.4 AVG om bijkomende voorwaarden met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid te handhaven of in te voeren. Aangezien het KB van 13 februari 2001 ter uitvoering van de Privacywet zal worden opgeheven, zullen de bijzondere waarborgen die in artikel 25 ervan waren opgenomen, worden geschrapt. Teneinde het beschermingsniveau ter zake niet te verlagen dient de auteur van het ontwerp deze waarborgen opnieuw op te nemen in de wet ter uitvoering van de AVG en voor deze gegevensverwerkingen te voorzien in:

- de verplichting van het aanwijzen van de categorieën van personen die de persoonsgegevens kunnen raadplegen, waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig moet worden omschreven;

- het bijhouden van een nominatieve lijst van deze personen die ter beschikking moet gesteld worden van de GBA zodra zij daarom verzoekt;

- de onderwerping van de aangewezen personen aan een wettelijke of statutaire of contractuele verplichting tot het bewaren van het vertrouwelijke karakter van de betrokken gegevens.

Uitvoering van artikel 10 AVG

99. Artikel 9 van het ontwerp voert artikel 10 AVG uit en bepaalt de categorieën verwerkingsverantwoordelijken andere dan de openbare overheden die gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen[9] verwerken.

[9] De formulering van het begin van § 1 van artikel 9 van het wetsontwerp verdient op dit punt te worden aangepast en te verduidelijken dat het de lijst omvat van personen die gemachtigd zijn om de bedoelde gegevens te verwerken.

100. Eerst en vooral merkt de Commissie op dat, in tegenstelling tot wat de Memorie van Toelichting stelt, artikel 9 van het ontwerp de toegangen tot het Strafregister niet omkadert. Het Strafregister en de limitatieve lijst van personen die er toegang toe hebben worden geregeld door het Wetboek van Strafvordering. De Memorie van Toelichting moet op dit punt gecorrigeerd worden

101. Betreffende de categorieën personen die gemachtigd zijn om gerechtelijke gegevens in de zin van artikel 10 AVG te verwerken, meent de Commissie dat de formulering van de 3de categorie van personen die gemachtigd zijn om gerechtelijke gegevens in de zin van artikel 10 AVG te verwerken, moet worden herzien om uitdrukkelijk enkel de personen te beogen die aangeduid zijn door een wet, een decreet of een ordonnantie, goedgekeurd wegens gewichtige redenen van algemeen belang voor het vervullen van taken van algemeen belang die hen zijn toevertrouwd door of krachtens een wet, een decreet of een ordonnantie.

102. Betreffende de 4de hypothese voor machtiging tot verwerking van gerechtelijke gegevens, merkt de Commissie op dat het begrip wetenschappelijk onderzoek te restrictief is aangezien het niet noodzakelijk het historisch onderzoek omvat. Het begrip historisch onderzoek dient dus in artikel 9, § 1, 4° van het ontwerp te worden toegevoegd. Opdat de onderzoekers toegang zouden krijgen tot de gegevens die zij nodig hebben voor hun onderzoek, dienen eveneens de verwerkingsverantwoordelijken bedoeld te worden die door de wetgever werden belast met opdrachten van openbare dienst bestaande uit archivering in het algemeen belang op voorwaarde dat de toegankelijkheid tot de in het algemeen belang gearchiveerde gegevens beperkt wordt tot de onderzoekers. Dit alles in naleving van artikel 4 van het ontwerp waarvoor de Commissie verwijst naar haar opmerkingen (cf. infra).

103. Artikel 9, §1, 5° voegt een nieuwe categorie personen toe die gemachtigd worden om deze gegevens te verwerken (child focus). In de ogen van de Commissie dient deze te worden geschrapt daar ze niet relevant, noch noodzakelijk is. Eerst en vooral zal Child focus op die basis geen toegang krijgen tot het Strafregister, in tegenstelling tot wat de Memorie van Toelichting stelt (zie punt XX hierboven). Bovendien wordt de verwerking door Child focus van dergelijke gegevens reeds gedekt door artikel 9, § 1, 3° van het ontwerp in het licht van artikel 383bis/1 van het Strafwetboek en het Koninklijk besluit van 15 november 2016 houdende de erkenning van Child Focus als organisatie bedoeld in artikel 383bis/1 van het Strafwetboek en dus gemachtigd om signalementen te ontvangen betreffende afbeeldingen die mogelijk bedoeld worden in artikel 383bis (kinderporno), om de inhoud en de oorsprong te analyseren, en deze door te spelen aan de politiediensten en gerechtelijke autoriteiten.

104. Tot slot merkt de Commissie op dat de definitie van gerechtelijke gegevens in de zin van artikel 10 AVG restrictiever is dan deze van artikel 8 van de huidige Privacywet die eveneens de verdenking van inbreuken dekt. Vanaf 25 mei eerstkomend zullen de verwerkingen van gerechtelijke gegevens enkel bestaan uit de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen

en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. De Commissie vraagt zich af of in de Nederlandse versie van artikel 9 van het ontwerp de woorden « infractions pénales » niet zouden moeten vertaald worden door « strafrechtelijke inbreuken » in de plaats van « strafbare feiten », zelfs indien deze vertaling overeenstemt met de officiële vertaling van artikel 10 AVG.

4.3. Hoofdstuk III – Rechten van de betrokkene

105. Als inleidende opmerking beveelt de Commissie aan om de titel van dit hoofdstuk te veranderen naar "*Beperkingen aan de rechten van de betrokkene*" aangezien de huidige titel niet overeenstemt met het eigenlijke opzet van dit hoofdstuk. In dit hoofdstuk wil de aanvrager uitvoering geven aan artikel 23 AVG dat de Lidstaten toelaat om binnen welbepaalde grenzen en voor specifieke doeleinden te voorzien in uitzonderingen op de rechten van de betrokkene.

De basisprincipes die de wetgever in acht moet nemen bij de uitvoering van artikel 23 AVG

106. Om de draagwijdte van de beoordelingsmarge die de wetgever hierbij geniet in kaart te brengen, is het van belang om te herinneren aan de rechtspraak van het Hof van Justitie over artikel 13 van Richtlijn 95/46/EG dat voorzag in een gelijkaardige uitzonderingsgrond. In het arrest *Smaranda Bara* bevestigde het Hof dat deze uitzonderingen alleen door "*wetgevende maatregelen*" kunnen ingevoerd worden[10]. Eerder preciseerde het Hof al dat de Lidstaten deze uitzonderingen slechts kunnen aannemen voor zover deze "*noodzakelijk*" zijn[11]. Gelet op het onveranderde streven van de Europese wetgever naar een hoog beschermingsniveau[12] betekent dit dat de uitzonderingen op de rechten van de betrokkenen moeten blijven binnen de grenzen van het strikt noodzakelijke[13]. De noodzaak en de evenredigheid van de betrokken maatregelen moeten dus beperkend geïnterpreteerd worden.

107. Artikel 23 AVG laat toe om door middel van een punctuele wetgevende interventie te voorzien in wettelijk omkaderde uitzonderingen waarvan de noodzaak voor één van de doeleinden van artikel 23.1 AVG duidelijk is aangetoond. In de Belgische rechtsorde vormen de artikelen 64 en 65 van de Wet van 18 september 2017 een goed voorbeeld van gemotiveerde sectorspecifieke uitzonderingen die beantwoorden aan de onderliggende filosofie van artikel 23 AVG[14]. De Commissie stelt vast dat de aanvrager dit vertrekpunt erkent in haar memorie van toelichting waar zij onder meer aangeeft dat deze uitzonderingen moeten worden neergelegd in "*een wettelijke bepaling*" die "*zo nauwkeurig*

[10] Hof van Justitie 1 oktober 2015 (C-201/14), *Smaranda Bara e.a.*, §39; Hof van Justitie 27 september 2017 (C-73/16), *Puškár*, §96.
[11] Hof van Justitie 7 november 2013 (C-473/12), *BIV v. Englebert*, §32.
[12] Overweging 10 AVG; Overweging 10 Richtlijn 95/46/EG.
[13] Ibid., §39.
[14] Wet 18 september 2017 *tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten*, *BS* 6 oktober 2017.

mogelijk" is[15]. De memorie van toelichting stelt zelfs dat een specifieke analyse moet plaatsvinden om de rechten van de betrokkene af te wegen aan de werkbaarheid voor de betrokken diensten[16].

108. Tot slot moet iedere wettelijke maatregel die voorziet in uitzonderingen op de rechten van de betrokkene, *ten minste* de elementen vernoemd in artikel 23.2 AVG bevatten.

109. De wetsartikelen in dit hoofdstuk worden dan ook getoetst aan deze basisprincipes.

Arikelen 10 en 11 van het ontwerp

110. Artikel 10 en 11 van het ontwerp voorzien in een zeer ruime en algemene uitzondering op *alle* rechten van de betrokkene waarop overheidsadministraties met bevoegdheden om strafbare feiten op te speuren, te onderzoeken en vervolgen, zich kunnen beroepen. De memorie van toelichting vermeldt op niet-exhaustieve wijze als voorbeelden: de sociale inspectiediensten, de economische inspectie, de inspectiedienstendiensten binnen de FOD Financiën, de gemeenten etc. Daarnaast zou deze uitzondering ook gelden voor "*andere openbare administraties […] die […] nood hebben aan een bijzondere regeling*"[17]. Die bijzondere regeling zou noodzakelijk zijn omdat er "*een algemeen geloof [circuleert] dat de GDPR te strikt zou zijn*" en om "*een bepaalde soepelheid te behouden voor de openbare sector*"[18]. De Commissie is van mening dat de aanvrager door dit 'algemeen geloof' de AVG met de voeten treedt. De artikelen 10 en 11 van het ontwerp doorstaan de toets van artikel 23.2 dan ook niet.

111. Volgens artikel 23.2.a) en 23.2.e) AVG moeten de wettelijke maatregelen de categorieën van verwerkingsverantwoordelijken en de doeleinden opsommen. De samenlezing van paragrafen 1, 2, 3 van artikel 10 van het ontwerp laat niet toe om de precieze verwerkingsverantwoordelijken te identificeren die zich op deze uitzonderingen kunnen beroepen. In het bijzonder artikel 10, §2 schendt deze vereiste door ruwweg te verwijzen naar elke instantie die een doelstelling in de zin van artikel 23.1.e) AVG nastreeft. Dit artikel voert de AVG niet uit, maar roept integendeel een misleidende norm in het leven die de indruk doet ontstaan dat elke overheidsinstantie artikel 23.1.e) AVG kan inroepen om de rechten van de betrokkene willekeurig in te perken. Artikel 10 preciseert evenmin de nagestreefde doeleinden doordat het ontwerp eenvoudigweg terugverwijst naar artikel 23.1 AVG, zonder de wettelijke opdrachten en taken van de betrokken diensten te omschrijven.

112. In dit verband verwijst de Commissie naar de mededeling van de Europese Commissie van 24 januari 2018 die uitdrukkelijk stelt: "*Reproducing the text of the Regulation word for word in national*

[15] Memorie van toelichting, blz. 21.
[16] Ibid.
[17] Memorie van toelichting, blz. 19.
[18] Memorie van toelichting, blz. 19.

specification law should be exceptional and justified, and cannot be used to add additional conditions or interpretations to the text of the regulation."[19]

113. De aanvrager voorziet zelfs niet in een verwijzing naar een Koninklijk Besluit om de diensten aan te wijzen die zich zouden kunnen beroepen op deze uitzonderingen, zoals dit momenteel het geval is voor artikel 3,§5 WVP[20]. Bovendien zou ook deze oplossing ontoereikend zijn omdat de filosofie van artikel 23 GDPR in samenlezing met artikel 22 van de Grondwet vereist dat deze uitzonderingen op de rechten van de betrokkenen bij formele wet ("*door de wet*") worden vastgesteld. Een willekeurige uitbreiding bij Koninklijk Besluit van de draagwijdte *ratione personae* van een ruime en algemene uitzondering als artikel 10 van het ontwerp, is in dit opzicht onaanvaardbaar. Zoals hierboven aangegeven vereist een goede uitvoering van artikel 23 AVG een aanpassing van de toepasselijke sectorale wetgeving zodat de uitzonderingen op maat zijn van de noden, taken en opdrachten van de betrokken diensten, zonder de rechten van de betrokkene overmatig te beperken.

114. De Commissie stelt vast dat de memorie van toelichting het gebrek aan afbakening van het personele toepassingsgebied van artikel 10 van het ontwerp bevestigt. De memorie stelt immers dat: "*Het toepassingsgebied van artikel 10 voldoende breed [is] om het geheel van de diensten te dekken die betrokken zouden kunnen zijn*". Het toepassingsgebied van artikel 10 van het ontwerp is dus volstrekt onduidelijk, terwijl dit een uitdrukkelijke vereiste is van artikel 23.2.c) AVG.

115. Volgens artikel 23.2.d) AVG moeten de wettelijke maatregelen waarborgen bevatten ter voorkoming van misbruik. Artikel 11 van het ontwerp doet hiertoe een poging door te voorzien in een systeem van minimumgaranties. Uit de memorie van toelichting blijkt dat de aanvrager zich liet inspireren door artikel 3,§7 WVP[21]. Artikel 11 van het ontwerp herneemt artikel 3, §7 WVP helaas op selectieve wijze en laat belangrijke waarborgen vallen waardoor het broze evenwicht dat deze wetsbepaling belichaamt, na meerdere adviezen van de Commissie[22] en een arrest van het Grondwettelijk Hof[23], breekt. Het ontwerp schiet tekort op de volgende vlakken:

---

[19]EC, "Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018", 24 januari 2018, blz. 9, te raadplegen via deze link.
[20]Zie bijvoorbeeld voor de sociale inspecteurs: *Koninklijk besluit van 11 maart 2015 ter uitvoering van artikel 3,§5,3° van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*, *BS* 25 maart 2015; Advies 09/2010 van de Commissie van 17 maart 2010, te raadplegen via deze link; Advies 34/2016 van de Commissie van 29 juni 2016, te raadplegen via deze link.
[21] Memorie van toelichting, blz. 24.
[22] Advies 11/2012 van de Commissie van 11 april 2012, te raadplegen via deze link; Advies 32/2012 van de Commissie van 17 oktober 2012, te raadplegen via deze link.
[23] Grondwettelijk Hof 27 maart 2014, Arrest nr. 51/2014.

- *beperking in de tijd*: destijds vernietigde het Grondwettelijk Hof een eerdere versie van artikel 3,§7 WVP net omdat de bestreden wetsbepaling niet preciseerde hoe lang de voorbereidende werkzaamheden die de schorsing van de rechten verantwoorden, konden duren[24]. De aanvrager laat deze maximale termijn vallen. Bijgevolg ontneemt artikel 11 niet alleen een waarborg aan de betrokkene, maar treedt het zelfs de rechtspraak van het Grondwettelijk Hof met de voeten. Tot slot leidt artikel 11, §3, tweede lid ertoe dat een openbare administratie voor "*belangrijke doelstellingen van algemeen belang*" *de facto* voor onbeperkte tijd de rechten van betrokkenen buiten werking kan stellen. Het ontwerp reikt geen enkel criterium aan om het begin- en eindpunt van deze periode vast te stellen waarvoor 'doelstellingen van algemeen belang' kunnen ingeroepen worden om de rechten van de betrokkene te schorsen. Dit is niet in overeenstemming met het arrest van het Grondwettelijk hof[25] en disproportioneel in het licht van artikel 23.1 AVG;

- *relevante gegevens*: in haar arrest benadrukt het Grondwettelijk Hof dat deze uitzondering zich niet mag uitstrekken tot gegevens die losstaan van het doel van het onderzoek of de controle. De bewoordingen "*voor zover*" van artikel 11 moeten dan ook op grondwetsconforme wijze geïnterpreteerd worden in deze zin. Toch verdient het aanbeveling om in dit soort uitzonderingsbepalingen ook uitdrukkelijk te bepalen dat voor alle andere persoonsgegevens die de betrokken dienst verwerkt voor andere doeleinden, de rechten van de betrokkene onaangetast blijven;

- *meedelen van motivering*: volgens artikel 3, §7 WVP deelt de verwerkingsverantwoordelijke na afloop van de schorsing de volledige motivering mee van de genomen beslissing. De zinssnede werd opgenomen in het huidige artikel 3, §7 WVP op advies van de Commissie[26] om af te wijken van de gemeenrechtelijke motiveringsplicht van de wet van 29 juli 1991[27] en te voorzien in een *a posteriori* controle van de motieven van de administratie. Artikel 11, §1, tweede lid van het ontwerp volstaat niet om van de motiveringsplicht van de wet van 29 juli 1991 af te wijken en ontneemt de betrokkene bovendien de waarborg om automatisch op de hoogte te worden gesteld van de motieven van de betrokken dienst na afloop van de controle of het onderzoek.

116. Tot slot moeten de artikelen 10 en 11 van het ontwerp in hun totaliteit ook de evenredigheids- en noodzakelijkheidstoets van artikel 23.1 AVG doorstaan. In het licht van de hierboven beschreven opmerkingen valt deze balans negatief uit. Bovendien roept artikel 10 een schorsing van *alle rechten* van de betrokkenen in het leven zonder na te gaan of de uitsluiting van bepaalde rechten wel noodzakelijk is in het licht van de wettelijke opdrachten en taken van de betrokken dienst. Zo merkte

[24]Grondwettelijk Hof 27 maart 2014, Arrest nr. 51/2014, B.8.5.
[25]Grondwettelijk Hof 27 maart 2014, Arrest nr. 51/2014, B.7.3.
[26] Stukken, *Kamer*, 2012-2013, nr. 2756/001, blz. 161-164; Advies 32/2012 van de Commissie van 17 oktober 2012, te raadplegen via deze link, randnummers 15-19.
[27] Wet van 29 juli 1991 *betreffende de uitdrukkelijke motivering van de bestuurshandelingen*, *BS* 12 september 1991.

de Commissie op in haar advies over artikel 3,§7 WVP dat de uitsluiting van het recht op verbetering of verwijdering tot gevolg zou kunnen hebben dat de fiscus een aanslag vestigt op foutieve gegevens of gegevens waarvan de verwerking verboden is[28]. De wetgever moet in het kader van de toepasselijke sectorale wetgeving gelijkaardige afwegingen maken waarbij aan de hand van de opdrachten van de betrokken dienst de noodzaak tot schorsing van ieder van de rechten afzonderlijk kan gerechtvaardigd worden. Zo ziet de Commissie bijvoorbeeld niet in waarom noodzakelijk zou zijn om systematisch te voorzien in een uitzondering op artikel 34 AVG[29].

117. De Commissie is dan ook van mening dat de artikelen 10 en 11 van het ontwerp in essentie een uitgeholde versie van huidig artikel 3, §7 WVP belichamen waarop bovendien een onbepaald aantal ongeïdentificeerde overheidsdiensten – mogelijks zelfs voor onbepaalde duur – beroep zouden kunnen doen. De poging om een zo groot mogelijk aantal openbare administraties onder te brengen in één uitzondering, heeft onverbiddelijk tot gevolg dat de aanvrager niet de noodzakelijke belangenafweging kon maken tussen de specifieke noden van elke dienst enerzijds, en de rechten van de betrokkene anderzijds. In tegenstelling tot wat artikel 11, §4 van het ontwerp suggereert komt het in de eerste plaats toe aan de wetgever om in haar uitvoeringsbepalingen van de AVG een juist evenwicht tussen deze conflicterende belangen vast te leggen. Deze paragraaf heeft dan ook geen enkele toegevoegde waarde[30].

Artikel 12 van het ontwerp

118. Artikel 12 van het ontwerp voorziet in een uitzondering op de rechten van de betrokkene voor de verwerkingsverantwoordelijken die over informatie beschikken die afkomstig is van de veiligheids- en inlichtingendiensten. De Commissie verwelkomt deze aanpassing die verhelpt aan een lacune die de rechtsleer al twintig jaar geleden identificeerde[31]. De bepaling wil voorkomen dat vertrouwelijke informatie zou kunnen 'lekken' via actoren in zowel de privé- als de publieke sector

[28] Advies 32/2012 van de Commissie van 17 oktober 2012, te raadplegen via deze link, randnummer 9.
[29] Zie in gelijkaardige zin advies 24/2017 van de Commissie van 24 mei 2017, te raadplegen via deze link, randnummer 36.
[30] Hetzelfde geldt voor artikel 11, §1, derde lid: de verwerkingsverantwoordelijke moet immers *altijd* zijn beleid omtrent de rechten van de betrokkene verantwoorden op verzoek van de Gegevensbeschermingsautoriteit. Dit vloeit op natuurlijke wijze voort uit de controleopdracht van de Gegevensbeschermingsautoriteit en behoeft geen overbodige en mogelijks verwarrende herhaling in uitzonderingsbepalingen.
[31] Y. POULLET EN B. HAVELANGE, "Secret d'Etat et Vie Privée: ou comment concilier l'inconciliable?", *Cahiers du Crids* n° 16, te consulteren via deze link, pagina 233-234: "*Comme il a été souligné, l'article 13 de la directive autorise des exceptions pour des responsables de traitement en communication avec la sûreté de l'État et les services de renseignements. […] La directive permet dans de tels cas des dérogations à l'application de ses prescrits. Une dérogation est-elle possible en droit belge? C'est discutable mais en tout cas certainement pas sur base de la nouvelle version de l'article 3.*"

die op basis van de artikelen 14 en 16 van de wet van 30 november 1998[32] in aanraking komen met de veiligheids- en inlichtingendiensten.

119. Het ontwerp zou uitdrukkelijk moeten verwijzen naar deze artikelen als de rechtsgrond voor deze informatie-uitwisseling in de plaats van de zeer algemene verwijzing naar de wetten van 30 november 1998 en 10 juli 2006[33] in de memorie van toelichting[34]. De uitzonderingen op de rechten van de betrokkene kunnen en mogen immers niet geïnterpreteerd worden als een wetsbepaling die impliciet deze informatie-uitwisseling toestaat bij gebreke aan een wetsbepaling die deze praktijk uitdrukkelijk in het leven roept. In dit opzicht merkt de Commissie op dat de betrokken wet van 10 juli 2006 geen gelijkaardige bepalingen bevat als de artikelen 14 en 16 van de wet van 30 november 1998.

120. Hoewel uit de memorie van toelichting blijkt dat met name de inlichtingen- en veiligheidsdiensten zich op deze uitzondering kunnen beroepen, veroorzaakt de Nederlandse formulering in artikel 12, eerste lid van het ontwerp verwarring over het personele toepassingsgebied. In plaats van te verwijzen naar "*persoonsgegevens […] die afkomstig zijn van andere overheden bedoeld in artikel (sic) 3 van deze wet*", zou de aanvrager beter eenvoudigweg verwijzen naar de overheden in titel 3 van het ontwerp. De Franstalige versie van het ontwerp is wel aangepast op dit punt.

121. De uitzondering heeft betrekking op de gegevens die afkomstig zijn van de instanties van titel 3 van het ontwerp, de instanties in artikel 10 van de wet van 10 juli 2006 en artikel 44/11/3ter, §2 en 3 van de *wet op het politieambt*. Ten eerste vraagt de Commissie zich af of het wel noodzakelijk is om in deze twee laatstgenoemde situaties een exceptie voor de doorgifte naar zowel de privé- als de publieke sector in het leven te roepen, terwijl deze twee wetten zelf op exhaustieve wijze opsommen wie de evaluatierapporten van het OCAD mag ontvangen en welke actoren toegang hebben tot de gemeenschappelijke databanken. Noch het ontwerp zelf, noch de memorie van toelichting duidt de wettelijke basis aan die verdere doorgifte van deze informatie mogelijk maakt. De Commissie maakt opnieuw het voorbehoud dat de uitzondering op de rechten van de betrokkene geen indirecte legitimering kan vormen van een praktijk die niet steunt op een expliciete wetsbasis.

122. Op redactioneel vlak ziet de Commissie niet de juridisch toegevoegde waarde in om doorheen artikel 12 van het ontwerp tot driemaal toe de uitsluiting van de rechten in de artikelen 12 tot 22

[32] Wet van 30 november 1998 *houdende regeling van de inlichtingen- en veiligheidsdiensten*, *BS* 18 december 1998.
[33] Wet van 10 juli 2006 *betreffende de analyse van de dreiging*, *BS* 20 juli 2006.
[34] Memorie van toelichting, blz. 26.

en 34 en het recht op transparantie te herhalen[35]. De rechten en de plichten die voortvloeien uit die artikelen zijn twee keerzijden van éénzelfde medaille en behoeven geen afzonderlijke uitzondering.

123. Artikel 12, §2 van het ontwerp voorziet in een gedifferentieerd 'beroepsrecht'. In dit verband wenst de Commissie meerdere opmerkingen te formuleren. Ten eerste zou het ontwerp, zowel in dit artikel als dooreen het gehele ontwerp, meteen moeten vastleggen wie de bevoegde toezichthoudende autoriteit is. Dit is des te belangrijker aangezien de aanvrager niet altijd duidelijk is in de afbakening van het toepassingsgebied tussen de AVG enerzijds en de Richtlijn[36] anderzijds.

124. Ten tweede stelt de Commissie zich vragen bij de toepassing van dit gedifferentieerde beroep. Sluiten de huidige bewoordingen voldoende uit dat een nietsvermoedende betrokkene een klacht zou neerleggen bij de Gegevensbeschermingsautoriteit en vervolgens antwoord krijgt van het Comité I dat "*de nodige verificaties werden verricht*" waardoor het onderzoeksgeheim breekt? Uit de bijkomende toelichting van de aanvrager blijkt evenwel dat de Gegevensbeschermingsautoriteit deze informatie zou meedelen. Het ontwerp spreekt echter van "de toezichthoudende autoriteit". Aangezien het Comité I de toezichthoudende autoriteit is van de inlichtingen- en veiligheidsdiensten (cfr. Artikel 97) sluit de huidige tekst van het ontwerp echter niet uit dat het Comité I deze informatie mee zou delen op basis van de tekst artikel 12, §2, laatste lid van het ontwerp.

125. Bovendien stelt zich de vraag onder welke omstandigheden een betrokkene een klacht kan neerleggen bij om het even welke toezichthoudende autoriteit die "*enkel betrekking heeft op persoonsgegevens afkomstig van een autoriteit bedoeld in titel 3*". Artikel 12 van het ontwerp wil immers net uitsluiten dat een betrokkene op de hoogte *kan* zijn van het feit dat de verwerkingsverantwoordelijke persoonsgegevens ontvangt van de veiligheids- en inlichtingendiensten.

126. Tot slot merkt de Commissie op dat haar rechtsopvolger geen kennis zal nemen van 'beroepen' die uitgaan van de betrokkene, maar wel van verzoeken en klachten. Het is dan ook onduidelijk

---

[35] Artikel 12, eerste lid: "*geniet de betrokkene met betrekking tot de verwerking van zijn persoonsgegevens die rechtstreeks of onrechtstreeks afkomstig zijn van andere overheden bedoeld in artikel 3 van deze wet, niet van de rechten bedoeld in de artikelen 12 tot 22 en 34 van de Verordening en ook niet van het recht op transparantie*"/ Artikel 12, tweede lid: "*zijn de verplichtingen bedoeld in artikelen 12 tot 22 en 34 van de Verordening niet van toepassing op instanties en personen die in het bezit zijn van deze gegevens*"/ Artikel 12, derde lid: "*De verwerkingsverantwoordelijke of de bevoegde overheid deelt niet mee dat hij in het bezit is van gegevens die van overheden bedoeld in titel 3 afkomstig zijn*."

[36] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad*.

waar de term 'beroep' op slaat en een doordachte harmonisatie met de bepalingen inzake indirecte toegang in de artikelen 80 t.e.m. 84 onder titel 3 van het ontwerp dringt zich op. Op die manier moet de wetgever het volledige proces dat de betrokkene doorloopt bij de uitoefening van zijn of haar rechten (en de eventuele beperkingen hierop) duidelijk en rechtlijnig in kaart brengen.

Artikel 13 van het ontwerp

127. Artikel 13 van het ontwerp vormt het logische spiegelbeeld van artikel 12. Terwijl artikel 12 van het ontwerp de veiligheids- en inlichtingendiensten wil beschermen als bron, wil dit artikel een gelijkaardige resultaat bereiken wanneer de veiligheids- en inlichtingendiensten ontvanger zijn. De Commissie stelt echter vast dat dit artikel overbodig is. De veiligheids- en inlichtingendiensten vallen immers niet onder het begrip "*ontvanger*" zoals gedefinieerd in artikel 4.9) AVG dat stelt: "*Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig […] het lidstatelijke recht gelden echter niet als ontvangers*". De veiligheids- en inlichtingendiensten vallen binnen deze uitzonderingscategorie. Uit de memorie van toelichting blijkt trouwens dat de aanvrager deze zienswijze weliswaar ook zelf aanhangt[37], maar vervolgens niet vertaalt naar het de tekst van het ontwerp zelf.

128. Artikel 13, tweede lid behoudt weliswaar haar bestaansreden voor structurele gegevensstromen met een specifieke wettelijke omkadering. De aanvrager moet zich echter buigen over de vraag of het verstrekken van algemene informatie over de samenwerking met veiligheids- en inlichtingendiensten het geheim van een punctueel onderzoek niet kan ondermijnen. Stel dat deze diensten samenwerken met een werkgever om personen met een risicoprofiel inzake terrorisme op te volgen, is het dan wenselijk dat de werkgever op algemene wijze haar personeel inlicht over deze contacten?

Artikel 14 van het ontwerp

129. Artikel 14 van het ontwerp wil de identiteit van de agenten van de veiligheids- en inlichtingendiensten beschermen wanneer zij gegevensbanken in de private of openbare sector rechtstreeks bevragen. Om het geheim van het onderzoek te verzekeren wil dit artikel door middel van technische en organisatorische beveiligingsmaatregelen de toegang tot de logs van deze gegevensbanken tot vier actoren beperken: de twee betrokken verwerkingsverantwoordelijken en hun respectievelijke functionarissen voor de gegevensbescherming. Uit de filosofie van de memorie blijkt dat het steeds om één persoon zou moeten gaan, zodat het aantal personen dat op de hoogte is van deze toegang

[37] Memorie van toelichting, blz. 22 en 23.

tot een strikt minimum – vier dus – beperkt blijft[38]. De tekst van het ontwerp zou zelf moeten specifiëren dat het steeds om één enkele natuurlijke persoon gaat.

130. De Commissie maakt voorbehoud bij de mogelijkheid om bij louter protocolakkoord tussen de betrokken verwerkingsverantwoordelijken niet alleen derden toegang te verlenen tot deze logs, maar deze toegang ook mogelijk te maken voor andere doeleinden. De Commissie begrijpt de noodzaak om voor technische ondersteuning beroep te doen op een derde persoon[39], maar de toegang door dergelijke derden moet dan duidelijk kaderen binnen de wettelijke toezichtsopdrachten van de functionarissen voor de gegevensbescherming en hun verwerkingsverantwoordelijken. Het ontwerp moet dit preciseren. Artikel 14, derde lid moet geschrapt worden wegens onaanvaard-baar vanuit het beginsel van doelbinding. Doeleinden moeten door de wet zelf bepaald worden.

131. Artikel 14, laatste lid van het ontwerp laat de overheden bedoeld in titel 3 van het ontwerp toe om dit artikel buiten werking te stellen "*wanneer hij van oordeel is dat de toepassing op een bepaalde gegevensbank niet relevant is*". De memorie van toelichting verklaart dat deze paragraaf doelt op de gemeenschappelijke gegevensbanken in de zin de artikelen 44/11/3*bis* tot *quinquies* van de wet op het politieambt. De buitenwerkingstelling voor deze specifieke databanken moet in de wet zelf opgenomen worden. De huidige bewoordingen van artikel 14, laatste lid maken de toepassing van de wet afhankelijk van een discretionaire bevoegdheid in hoofde van de overheden bedoeld in titel 3. Het principe van de rechtstaat vereist echter dat ook overheidsorganen gehouden zijn aan de naleving van de wet en niet willekeurig kunnen beslissen over de toepassing van deze wetten.

132. Tot slot dient het ontwerp ook te verwijzen naar de specifieke wetsbepalingen op basis waarvan deze bevraging van zowel private als publieke gegevensbanken mogelijk is.

Artikel 15 van het ontwerp

133. Artikel 15 van het ontwerp lijkt te voorzien in een vergelijkbare uitzondering als artikel 12, maar dan voor de politiediensten. De betrokkenen kunnen hun rechten niet in roepen ten aanzien van de "*ontvangers voorzien in de artikelen 44/1, §§ 3 en 4 alsook in de artikelen 44/11/7 tot 44/11/11 van de wet op het politieambt aan wie de politiediensten die gegevens bezorgd hebben*". Artikel 44/1, §§ 3 en 4 verwijst naar in essentie naar de politieoverheden in hun hoedanigheid van gerechtelijke als bestuurlijke politie. De verwijzing naar de artikelen 44/11/7 tot 44/11/11 omvat bovendien een groot aantal actoren die ofwel bevoegde overheid zijn in de zin van artikel 31.7 van het ontwerp ofwel vallen onder artikel 75 van het ontwerp. De definitie van de ontvangers is gedeeltelijk tautologisch en slaat dus ook op verwerkingen van persoonsgegevens die uitsluitend

[38] Memorie van toelichting, blz. 31.
[39] Memorie van toelichting, blz. 32.

onder het toepassingsgebied van de Richtlijn vallen[40]. Bovendien stelt de memorie van toelichting dat de exceptie voor andere actoren die in de opsomming van de artikelen 44/11/7 tot 44/11/11 voorkomen – bijvoorbeeld het Comité P – zelfs overbodig is[41]. Bijgevolg is de draagwijdte van deze uitzondering onduidelijk en de memorie van toelichting kan evenmin de exacte toedracht van dit artikel verklaren. Het ontwerp moet met precisie de actoren omschrijven die deze uitzondering kunnen inroepen.

134. De Commissie merkt ook op dat in tegenstelling tot wat artikel 15, vijfde lid van het ontwerp lijkt te suggereren, het in de eerste plaats aan de wetgever toekomt om te voorzien in de gepaste waarborgen in de zin van artikel 23.2 AVG. Een totaal gebrek aan de noodzakelijke wetgevende waarborgen kan niet geregulariseerd worden door de bal terug te kaatsen naar de verwerkings-verantwoordelijke zelf.

135. Artikel 15, laatste lid van het ontwerp bepaalt dat ieder verzoek tot uitoefening van de rechten van de betrokkene aan de bevoegde toezichthoudende autoriteit wordt bezorgd. Opnieuw benadrukt de Commissie de noodzaak om de toezichthoudende autoriteit te benoemen en deze wetsbepaling af te stemmen op, of ten minste verwijzen naar de bepalingen van hoofdstuk III onder titel 2 van het ontwerp. De huidige formulering en versnippering biedt geen duidelijk zicht op het volledige proces dat de betrokkene moet doorlopen bij de uitoefening van zijn of haar rechten en de controlemechanismen waarop hij of zij zich kan beroepen.

Artikel 16 van het ontwerp

136. Artikel 16 van het ontwerp voorziet in een bijna identieke kopie van artikel 15, maar ditmaal voor de ontvangers van informatie van de gerechtelijke overheden. Het enige verschil situeert zich in de bepaling dat deze ontvangers kunnen afwijken van de beperkingen op de rechten van de betrokkene indien de wet dit verplicht in het kader van een geschillenprocedure of de betrokken gerechtelijke overheid dit toestaat. De Commissie stelt zich de vraag waarom deze bepaling niet geldt voor artikel 15 van het ontwerp. Op die manier kon één geconsolideerde uitzonderingsbepaling opgesteld worden voor alle ontvangers van informatie die afkomstig is van de bevoegde overheden in de zin van titel 2 van het ontwerp.

137. Met betrekking tot de artikelen 12 tot 16 en 18 van het ontwerp merkt de Commissie tot slot op dat deze bepalingen niet thuishoren in titel 1 van het ontwerp. De organieke afbakening van de respectievelijke toepassingsgebieden van titels 1, 2 en 3 houdt onvoldoende rekening met de nagestreefde doeleinden van de verschillende actoren, waardoor veel onduidelijkheden ontstaan, bijvoorbeeld voor de aanduiding van de bevoegde toezichthoudende autoriteit.

[40] De memorie van toelichting lijkt dit trouwens zelf te bevestigen op bladzijde 35.
[41] Memorie van toelichting, blz. 36.

138. Voor de veiligheids- en inlichtingendiensten is artikel 4.9) van de AVG nochtans duidelijk: "*Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek […] gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn*". Hoewel deze bepaling zich beperkt tot het begrip ontvanger, biedt dit een stevig argument om de bepalingen die overheden zoals bedoeld in titel 3 van het ontwerp willen beschermen als bron, op te nemen in titel 3 van het ontwerp.

139. Een gelijkaardige opmerking dient zich aan voor de artikelen 15 en 16 van het ontwerp die uitdrukkelijk bepalen dat "*deze uitzonderingen slechts van toepassing [zijn] op de gegevens die aanvankelijk […] verwerkt worden voor de doeleinden in artikel 32 van de wet*". Deze zinssnede erkent dat de beoogde verwerkingen in het licht van de doeleinden die zij nastreven, in essentie vallen onder titel 2 van het ontwerp. De uitzonderingen op de rechten van betrokkenen ten aanzien van derden die samenwerken met de overheden vermeld in titel 2 of 3 van deze wet – en dus plaatsvindt voor de specifieke doeleinden die deze overheden nastreven – komen dus beter tot hun recht onder deze respectievelijke titels.

Artikel 17 van het ontwerp

140. Artikel 17 van het ontwerp bepaalt dat "*Wanneer de persoonsgegevens in een rechterlijke beslissing of een gerechtelijk dossier zijn opgenomen of in het kader van strafrechtelijke onderzoeken en procedures worden verwerkt, de in de artikelen 12 tot 22 en 34 van de Verordening bedoelde rechten [worden] uitgeoefend overeenkomstig het Gerechtelijk wetboek en het wetboek van Strafvordering.*" De Commissie merkt op dat strafrechtelijke onderzoeken en procedures vallen onder het toepassingsgebied van de Richtlijn en dus niet thuishoren in titel 1 van het ontwerp.

141. Met betrekking tot de procedures die vallen onder het *Gerechtelijk wetboek* kan de wetgever dan wel de intentie hebben om de uitoefening van de rechten van de betrokkene te moduleren, dit belet niet dat de AVG voorgaat op het nationale recht van de Lidstaten krachtens de primauteit van het unierecht[42]. Dit wetsartikel heeft bijgevolg geen enkele toegevoegde waarde en geeft de rechtsonderhorige de foutieve indruk dat het *Gerechtelijk Wetboek* afbreuk zou kunnen doen aan de AVG. In de mate dat het *Gerechtelijk Wetboek* wil afwijken van de rechten van de betrokkene, dient dit te gebeuren onder de voorwaarden van artikel 23 AVG. Een dergelijke generieke bepaling voldoet niet aan de vereisten van artikel 23 AVG. De bepalingen van de betrokken nationale wetgeving moet getoetst worden aan de voorwaarde die artikel 23 oplijst, luidens dewelke "*die*

[42] Hof van Justitie 9 maart 1978 (C-106/77), *Simmentahl*, §22 en 24. M.b.t. de rechtstreekse doorwerking van het internationaal recht in de Belgische rechtsorde zie: Hof van Cassatie 27 mei 1971, Franco-Suisse Le Ski, *Arr. Cass.* 1971, 959.

beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:… d) ter voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;… f) De bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures."

142. Een dergelijk onderzoek lijkt op het eerste zicht een titanenwerk maar zou normaliter geen bijzondere problemen mogen opleveren gelet op het feit dat sinds vele jaren nieuwe wetgeving wordt getoetst aan enerzijds het artikel acht van het EVRM enerzijds en aan de principes van het verdrag 108 van de raad van Europa van 28 januari 1981[43], het BUPO, de oude EU privacy richtlijn 95/46[44] en uiteraard ook de WVP. Men mag er dus geredelijk van uitgaan dat de bestaande wetgeving in overeenstemming is met de vereisten van artikel 23 AVG. Maar via een algemeen wetsartikel ontsnappen aan dit onderzoek is niet aanvaardbaar.

143. In dat onderzoek dient niet alleen het *Wetboek van Strafvordering* en het *Gerechtelijk Wetboek* betrokken te worden maar ook tal van andere wetten en regelgeving die, meestal op een gedetailleerde manier, de behandeling van persoonsgegevens en in het bijzonder de rechten van de betrokken burger legifereert. Louter bij wijze van voorbeeld: de huiszoekingswet van 7 juni 1969, DNA-wet van 22 maart 1999, de wet centraal staatregister van 31 juli 2009,… voor wat het strafrecht betreft. Daarnaast is er ook o.a. nog ook uitvoeringsregelgeving zoals het KB van 21 juni 2011 houdende het beheer van de centrale registers van testamenten en huwelijksovereenkomsten[45].

Artikel 18 van het ontwerp

144. Tot slot ziet de Commissie de toegevoegde waarde niet in van artikel 18 van het ontwerp. Een cumulatieve toepassing van de – grondig herschreven – artikelen 12, 15 en 16 van het ontwerp zou moeten leiden tot het gewenste resultaat. De memorie moet de noodzaak van deze bepaling duiden en verklaren hoe deze exceptie zich verhoudt ten opzichte van de andere uitzonderingen op de rechten van de betrokkene. Bovendien laat het ontwerp na om te definiëren wat begrepen moet worden onder "*een gemeenschappelijke behandeling*" terwijl het gaat om een constitutief element van deze wetsbepaling dat doorslaggevend is voor de bepaling van het toepassingsgebied. Uit de

[43] Council of Europe, Treaty n° 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981.
[44] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens*.
[45] Zie voor wetsverwijzingen: Larcier thema wetboeken "privacy-wetgeving 2015", Willem Debeuckelaere, Gert Vermeulen, III.2: strafwetgeving en III. Gerechtelijk en burgerlijk recht.

bijkomende toelichting verschaft door de aanvrager blijkt dat het ontwerp de gemeenschappelijke gegevensbanken in de zin van artikelen 44/11/3bis, 44/11/3ter, 44/11/3quater, 44/11/3quinquies van de *wet op het politieambt* bedoelt. Dit valt noch uit de tekst van het ontwerp, noch uit de memorie van toelichting op te maken. De aanvrager moet deze uitzondering dan ook uitwerken en verantwoorden in het licht van de specifieke noden die voortvloeien uit de gemeenschappelijke gegevensbanken in de *wet op het politieambt.*

Algemeen besluit voor hoofdstuk III van titel I

145. Samengevat worden alle uitzonderingen die hoofdstuk III van titel I opsomt gekenmerkt door grote onduidelijkheid over a) wie de uitzondering kan inroepen; b) voor welke doeleinden; c) m.b.t. welke gegevens; en d) voor welke duur. Bovendien ontbreekt het aan afdoende wettelijke waarborgen – of verwijzingen naar bestaande waarborgen – die bescherming moeten bieden tegen een willekeurige inperking van de rechten van de betrokkene. Wetsbepalingen waarvan de omvang zo onduidelijk is falen niet alleen om de vereisten van artikel 23 AVG te vervullen, maar zijn door hun dubbelzinnigheid voor de rechtsonderhorige evenmin redelijkerwijze voorzienbaar in de zin van artikel 8 EVRM. Om al deze redenen is het advies van de Commissie voor het volledige hoofdstuk III van titel I ongunstig.

Voorstel van amendement

146. De Commissie stelt de volgende structuur voor om helder geformuleerde uitzonderingen op te stellen die uitvoering geven aan artikel 23 AVG in de toepasselijke sectorale wetgeving:

1) Een inleidende bepaling die aangeeft van welk *specifieke* recht van de AVG de wetgever wenst af te wijken, voor welke doelstelling in de zin van artikel 23.1 AVG dit moet gebeuren en de concrete uitwerking van die doelstelling aan de hand de toepasselijke sectorale wetgeving. Ook de actoren die deze uitzondering kunnen inroepen moeten exhaustief opgesomd worden. Bijvoorbeeld:

"*In afwijking van artikel 15 van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), om [doelstelling artikel 23.1 AVG] te waarborgen, kan het recht op inzage van de hem betreffende persoonsgegevens geheel of gedeeltelijk worden uitgesteld en beperkt voor wat betreft verwerkingen van persoonsgegevens waarvan [de verwerkingsverantwoordelijken en de omschrijving van hun wettelijke taken en opdrachten die de uitzondering wettigen] verwerkingsverantwoordelijke zijn.*"

2) Een omschrijving van de verwerkingen waarvoor deze uitzondering geldt. Bijvoorbeeld:

"*De in het eerste lid bedoelde verwerkingen zijn deze die de voorbereiding, de organisatie, het beheer en de opvolging van de door de in het eerste lid bedoelde diensten gevoerde onderzoeken, met inbegrip van de procedures voor de eventuele toepassing van een administratieve geldboete of administratieve sanctie door de bevoegde diensten, tot doel hebben.*"

3) Een afbakening in de tijd van deze uitzondering – of indien dit niet mogelijk is een onderbouwde verantwoording in de memorie van toelichting die uitlegt waarom de uitzondering niet beperkt is in tijd (bv. voor de politie- en inlichtingendiensten waarbij een tijdelijke schorsing van de rechten ontoereikend zou kunnen zijn). Bijvoorbeeld:

"*Deze afwijkingen gelden gedurende de periode waarin de betrokkene het voorwerp uitmaakt van een controle of een onderzoek of de daarmee verband houdende voorbereidende werkzaamheden uitgevoerd door de voormelde inspectiediensten in het kader van de uitvoering van hun wettelijke opdrachten*

De duur van de voorbereidende werkzaamheden gedurende dewelke artikel 15 van de algemene verordening gegevensbescherming niet van toepassing is, mag niet meer bedragen dan één jaar vanaf de ontvangst van het verzoek dat is ingediend in toepassing van artikel 15.

Wanneer een dossier wordt overgemaakt aan het openbaar ministerie, worden de rechten pas hersteld nadat het openbaar ministerie aan de bevoegde dienst heeft bevestigd hetzij dat het afziet van het instellen van strafvervolging, hetzij van het voorstellen van een minnelijke schikking of een bemiddeling in de zin van artikel 216ter van het Wetboek van strafvordering, en nadat de bevoegde dienst voor administratieve geldboeten een beslissing heeft genomen.

Wanneer een dossier wordt overgemaakt aan de administratie waarvan de inspectiedienst afhangt, of aan de bevoegde instelling om over de bevindingen van het onderzoek te beslissen, worden de rechten pas hersteld nadat de bevoegde administratie of instelling heeft beslist over het resultaat van het onderzoek."

4) Een duidelijke afbakening van het materiële toepassingsgebied van deze uitzondering. Bijvoorbeeld:

"*Deze afwijkingen gelden voor zover de toepassing van dit recht nadelig zou zijn voor de controle, het onderzoek of de voorbereidende werkzaamheden of het geheim van het strafonderzoek dreigt te schenden.*

De beperking bedoeld in paragraaf 1, eerste lid, heeft geen betrekking op de gegevens die losstaan van het voorwerp van het onderzoek dat of van de controle die de weigering of beperking van inzage rechtvaardigt."

5) Een goed uitgewerkt mechanisme voor het behandelen van klachten of verzoeken van de betrokkene (rechtstreekse toegang), waarbij de rol van de functionaris van de gegevensbescherming omkaderd is door strikte deadlines. Bijvoorbeeld:

"*Bij ontvangst van een verzoek tot inzage bevestigt de functionaris voor de gegevensbescherming van de verwerkingsverantwoordelijke de ontvangst hiervan.*

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke informeert de betrokkene schriftelijk, onverwijld, en in ieder geval binnen één maand na de ontvangst van het verzoek, over iedere weigering of beperking van zijn recht op inzage van de hem betreffende gegevens alsook van de redenen voor deze weigering of beperking. Die informatie kan achterwege worden gelaten wanneer de verstrekking daarvan één van de doelstellingen genoemd in […] zou ondermijnen. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van deze verlenging en van de redenen van het uitstel."

6) Een consequente informatiestroom naar de betrokkene toe over de toepassing van deze uitzondering en de beschikbare controlemechanismen is ook noodzakelijk. Bijvoorbeeld:

"*De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke informeert de betrokkene over de mogelijkheden om een klacht in te dienen bij de Gegevensbeschermingsautoriteit of om een jurisdictioneel beroep in te stellen.*

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke vermeldt de feitelijke of juridische redenen waarop zijn beslissing steunt. Deze inlichtingen worden ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Wanneer één van de voormelde inspectiediensten gebruik heeft gemaakt van de uitzondering bepaald bij […] wordt de uitzonderingsregel onmiddellijk opgeheven na de afsluiting van de controle of van het onderzoek. De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke brengt de betrokkene hiervan onverwijld op de hoogte."

4.4. Hoofdstuk IV - Verwerkingsverantwoordelijke en verwerker

4.4.1. Sectie 1 – Algemene bepalingen

Ontvangstbevestiging bij vraag tot uitoefening van de rechten

147. Artikel 19 van het ontwerp legt aan de verwerkingsverantwoordelijken een maximumtermijn op van een maand voor het verzenden van een ontvangstbevestiging aan eenieder die zijn rechten uitoefent overeenkomstig de AVG. De Commissie meent dat deze termijn moet worden ingekort aangezien elke verwerkingsverantwoordelijke krachtens artikel 12.3 AVG onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens de artikelen 15 tot en met 22 aan de betrokkene de nodige informatie moet verstrekken.

4.4.2. Sectie 2 – Publieke sector

148. Afdeling 2 van Hoofdstuk III strekt ertoe specifiek de gegevensstromen te omkaderen die afkomstig zijn van de openbare sector.

Begrippen « overheidsorgaan en overheidsinstantie»

149. Vanuit algemeen oogpunt merkt de Commissie op dat het ontwerp, als wet ter uitvoering van de AVG, de door de AVG onder meer in haar artikel 37.1.a (die hen verplicht een functionaris voor gegevensbescherming aan te wijzen) gebruikte bewoordingen "overheidsinstantie en overheidsorgaan" zou moeten definiëren, en dit om een correct rechtszekerheidsniveau te bereiken. De Groep Artikel 29 heeft in zijn richtsnoeren over de DPO vooropgesteld dat deze begrippen moeten worden gedefinieerd in functie van het nationaal recht. Deze uitvoeringsmaatregel ontbreekt in onderhavig ontwerp aangezien de voorgestelde definities voor overheidsinstantie en overheidsorgaan enkel betrekking hebben op afdeling 2 van het ontwerp.

150. Artikel 21 van het ontwerp definieert de begrippen overheidsinstantie en overheidsorgaan bedoeld in afdeling 2 van het ontwerp als "de openbare instelling of privaatrechtelijke instelling of publiekrechtelijke instelling die een openbare dienst verleent". Het verduidelijkt dat afdeling 2 eveneens van toepassing is op de politiediensten.

151. Hoewel de Commissie de bedoeling van de wetgever begrijpt, gaat het erom dat elke publiekrechtelijke rechtspersoon en elke privaatrechtelijke rechtspersoon wordt bedoeld die werd opgericht of erkend door de openbare overheden of waarvan de werking wordt gecontroleerd door de openbare overheden, die door de wetgever werd belast met een opdracht van openbare dienst en beschikt over de bevoegdheid om dwingende beslissingen te nemen jegens derden.

152. Indien dit het geval is, is het belangrijk (i) dat de auteur van het ontwerp dit expliciet vermeldt in artikel 21 van het ontwerp, door toe te voegen dat hij "de publiekrechtelijke rechtspersonen en de privaatrechtelijke rechtspersonen" bedoelt "die werden opgericht of erkend door de openbare overheden of waarvan de werking wordt gecontroleerd door de openbare overheden, en die door de wetgever werden belast met een opdracht van openbare dienst en beschikken over de bevoegdheid om dwingende beslissingen te nemen jegens derden" en (ii) dat hij hen een gemeenschappelijk patronaat toekent zoals bijvoorbeeld "openbare of private instellingen". De thans in het ontwerp gebruikte benaming "openbaar orgaan" leidt tot verwarring. In het vervolg van haar advies gebruikt de Commissie de woorden "betrokken of bovenvermelde openbare en private instellingen".

Omkadering van gegevensdoorgiften door federale overheidsinstantie- of federale openbare organen (artikel 22 van het ontwerp)

153. Artikel 22 van het ontwerp voorziet in een facultatief systeem van omkadering van doorgiften van persoonsgegevens door de voormelde federale openbare en private instellingen, via door de verwerkingsverantwoordelijken goed te keuren protocolakkoorden na advies van hun respectievelijke functionarissen voor gegevensbescherming (DPO).

154. De Commissie benadrukt het belang van de naleving van het rechtmatigheidsbeginsel voor de gegevensverwerkingen in deze sector. Een uitwisselingsprotocol kan nooit een wettelijke basis vormen voor een gegevensverwerking. De authentieke bronnen van persoonsgegevens beschikken over een wettelijk kader dat de essentiële elementen bevat voor de verwerkingen die hiermee mogen worden uitgevoerd[46].

Verplicht en niet facultatief

155. Bijgevolg onderschrijft de Commissie de noodzaak tot invoering van een systematische routine die de DPO zal toelaten de invoering van een doorgifte van persoonsgegevens voor te bereiden en te analyseren voor de uitvoering van een opdracht van openbare dienst. Iedere gegevensuitwisseling in de schoot van de voormelde openbare of private instellingen mag slechts plaatsvinden nadat de betrokken verwerkingsverantwoordelijken de verenigbaarheid met de AVG hebben gecontroleerd en meer in het bijzonder of de mededeling kadert binnen de opdrachten van de betrokken openbare of private instelling die de gegevens meedeelt en dat de inzameling van gegevens kadert binnen de opdrachten van de voormelde openbare of private instelling die de gegevens raadpleegt/ontvangt. Bijgevolg oordeelt de Commissie dat dit systeem, dat bijdraagt aan

[46] Cf. de wet van 8/08/1983 tot regeling van een Rijksregister van de natuurlijke personen, wet van 19/05/2010 houdende oprichting van de Kruispuntbank van de voertuigen, ...

de toepassing van de "accountability" (Verantwoordingsplicht - artikel 5.2 AVG) van de verwerkingsverantwoordelijken, verplicht moet gesteld worden en niet facultatief mag blijven.

156. Het is anderzijds, in verband met de risicogebaseerde benadering die voortvloeit uit sommige bepalingen van de AVG voor de verwerkingsverantwoordelijken en verwerkers, aangewezen dit te beperken tot elektronische gegevensdoorgiften betreffende risicovolle verwerkingen (zoals het hergebruik van persoonsgegevens voor andere doeleinden dan waarvoor ze werden ingezameld, of de uitwisseling van gegevens tussen de voormelde openbare of private instellingen die opdrachten van openbare dienst van verschillende aard nastreven, of nog verwerkingen van gevoelige gegevens,...).

157. Het is eveneens denkbaar sommige verwerkingen, waarbij de risico's beperkt zijn, hiervan uit te sluiten (mededeling van gepseudonimiseerde gegevens voor wetenschappelijk onderzoek overeenkomstig de nadere regels bedoeld in het specifiek hieraan gewijd hoofdstuk in de wet ter uitvoering van de AVG,...). Bovendien is het wenselijk dit systeem van protocol voor gegevensuitwisseling te verzoenen met het *voorontwerp van wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG*. Hiertoe is het in voorkomend geval aangewezen de gegevensmededelingen door de Kruispuntbank van de Sociale Zekerheid, de instellingen van de sociale zekerheid of het eHealthplatform van dit systeem van protocol voor gegevensuitwisseling vrij te stellen aangezien hiervoor noodzakelijkerwijs een voorafgaande beraadslaging van dit informatieveiligheidscomité zal vereist zijn.

158. De Commissie stelt zich vragen bij de relevantie van de vermelding in artikel 22 van het ontwerp van de gegevensstromen naar private instellingen die geen opdrachten van openbare dienst uitvoeren. De elektronische mededelingen van gegevens, uitgaande van de voormelde openbare of private instellingen betreffen over het algemeen enkel gegevensstromen voor de vervulling van opdrachten van openbare dienst of voor de verwezenlijking van wetenschappelijk onderzoek.

159. Wat de formulering betreft van dit artikel 22, § 1, 1ste lid, verdient het begrip "verwerkingsverantwoordelijke bestemmeling van de gegevens" de voorkeur op "verdere gegevensverwerker" aangezien de bedoelde gegevensstromen niet systematisch bestaan uit een verdere gegevensverwerking.

Inhoud van het protocol

160. Wat de inhoud van het protocol betreft zoals artikel 22 van het ontwerp dit bepaalt; naast het feit dat de wetgever zijn elementen verplicht dient te stellen en niet facultatief ("kan" moet worden vervangen door "moet"), dringen de volgende opmerkingen zich op:

a. Punt 2 "identificatie van de verwerkingsverantwoordelijke" moet worden vervangen door "identificatie van de verwerkingsverantwoordelijken". Van nature heeft de gegevensuitwisseling bedoeld in het eerste lid van artikel 22, § 1 van het ontwerp ten minste twee verwerkingsverantwoordelijken;
b. Punt 5 dient niet alleen te slaan op de precieze categorieën gegevens maar conform het proportionaliteitsbeginsel eveneens op hun omvang[47];
c. Punt 7 zou moeten vervangen worden door "de wettelijke basis(sen) die zowel de mededeling als de inzameling van de gegevens wettigen";
d. Punt 9 zou moeten beperkt worden tot de maatregelen die eigen zijn aan de beveiliging van de gegevensuitwisseling aangezien het enkel deze verwerking van gegevensuitwisseling is die omkaderd wordt door het protocol. Bovendien dient de formulering van deze maatregelen functioneel te zijn teneinde te vermijden dat gevoelige details worden onthuld over de technische veiligheidsmaatregelen en dat de betrokkenen worden blootgesteld aan veiligheidsaanvallen;
e. Punt 10 moet worden geschrapt aangezien het strijdig is met artikel 28 van de AVG. Behoudens in de hypothese waar een gegevensverwerking wordt uitgevoerd door gezamenlijke verwerkingsverantwoordelijken die samen een beroep doen op een verwerker, is de verwerkingsverantwoordelijke die de bestemmeling is van de gegevens de enige verantwoordelijke voor de keuze van zijn eigen verwerker;
f. Punt 11 dient eveneens te worden geschrapt; enkel de wetgever is bevoegd om afwijkingen toe te staan op de rechten van de betrokkenen en dit volgens de voorwaarden vervat in artikel 23 van de AVG. In de plaats zou erin kunnen worden voorzien dat de verwerking geniet van wettelijke afwijkingen op sommige rechten van de betrokkenen alsook de rechtvaardiging van hun toepassing in voorkomend geval;
g. De nummering van de titel waarnaar punt 16 verwijst is foutief, het gaat om titel 6;
h. De volgende punten moeten worden toegevoegd vermits zij inherent zijn aan het onderzoek van de bedoelde gegevensuitwisselingen:
    i. De beschrijving van de precieze doeleinden waarvoor de gegevens oorspronkelijk werden ingezameld door de voormelde openbare of private instelling, beheerder van de geraadpleegde gegevensbron;

[47] Het proportionaliteitsbeginsel vereist dat niet alleen de gegevens worden beperkt tot het strikt noodzakelijke voor het verwezenlijken van de beoogde doeleinden maar ook hun formaat in die zin dat een formaat van het type "ja of neen" of "aantal personen waaruit het gezin bestaat" of nog "inkomstenniveau hoger of lager dan een bepaald bedrag" kan in sommige gevallen ruimschoots volstaan.

ii. Ingeval van latere verwerking[48] van de ingezamelde gegevens, vermelding van de verenigbaarheidsanalyse van de doeleinden van deze verwerking met het doeleinde waarvoor de gegevens aanvankelijk zijn verzameld overeenkomstig artikel 6.4 van de AVG;

iii. Controle op de naleving van het beginsel "inzameling bij de authentieke gegevensbron" die de kwaliteit van de gegevens garandeert alsook de eerbiediging van het wettelijk kader dat de toegang tot de authentieke bron regelt;

iv. Alle specifieke maatregelen die de gegevensflux omkaderen conform het proportionaliteitsbeginsel en de vereisten inzake gegevensbescherming by design en default (keuze van het formaat van de mededeling, logging van de toegangen zodat men kan controleren wie wanneer toegang had tot welke gegevens en waarom, invoering van een verwijzingsrepertorium ingeval van automatische mededeling van de wijzigingen aan de gegevens om zich ervan te verzekeren dat enkel de noodzakelijke gegevens worden bijgewerkt en dit voor de nodige termijn,...)

Adviezen van de functionarissen voor gegevensbescherming

161. Artikel 22, § 2 van het ontwerp dient te bepalen dat de adviezen van de DPO zullen aangehecht worden aan het protocol voor gegevensuitwisseling en dat de inleidende bepalingen van het protocol de rechtvaardiging zullen bevatten van de verwerkingsverantwoordelijke(n) wanneer hij/zij afwijken van het advies van de DPO.

Openbaarheid van het protocol

162. Teneinde de voorzienbaarheid van de bedoelde gegevensstromen te waarborgen zullen deze uitwisselingsprotocollen moeten bekend gemaakt worden in het Belgisch Staatsblad. Dit dient uitdrukkelijk te worden bepaald in artikel 22 van het ontwerp. Aangezien deze protocollen verwerkingen van gegevens van burgers zullen omkaderen, dienen zij te voldoen aan de criteria inzake voorzienbaarheid en toegankelijkheid[49].

Gewesten en Gemeenschappen

163. Tot slot, aangezien de elektronische gegevensuitwisselingen verbonden aan E-government - van nature - niet beperkt zijn tot de voormelde federale openbare of private instellingen, oordeelt de Commissie dat een specifieke omkadering zich dient uit te strekken tot de Gewesten en

[48] Gebruik van de gegevens voor (een) ander(e) doeleinde(n) dan waarvoor de gegevens oorspronkelijk werden ingezameld door de overheid of openbare instelling die de gegevens meedeelt.
[49] Zie hierover HvJEU, 1/10/2015, Zaak Smaranda Bara, ECLI :EU :C :2015 :638 ; EHRM, 4/12/2015, zaak Roman Zakarov v. Rusland https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160008%22]}

Gemeenschappen, wat kan worden verkregen door een samenwerkingsakkoord dat door de wetgevers zal worden goedgekeurd, zoals wordt voorzien in artikel 92bis, § 1 van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen[50].

Omkadering van de Registers van de gegevensverwerking (artikelen 23 en 24 van het ontwerp)

164. Met het oog op normalisering omkaderen de artikelen 23 en 24 van het ontwerp de registers van de verwerking van persoonsgegevens die gehouden worden door de voormelde openbare of private instellingen in toepassing van artikel 30 van de AVG[51].

165. In dit verband stelt de Commissie zich vragen bij de relevantie van een normalisering van de modaliteiten voor het beheer en het houden van het register gelet op de diversiteit van de verwerkingen van persoonsgegevens waarmee de verwerkingsverantwoordelijken en verwerkers van deze sector worden geconfronteerd. De centralisatie van de registers biedt in de ogen van de Commissie geen enkele meerwaarde voor de toekomstige gegevensbeschermingsautoriteit.

166. Bijgevolg dient artikel 24 van het ontwerp te worden geschrapt (de AVG voorziet reeds dat het register uit een elektronisch geschrift moet bestaan). Ten overvloede zouden overgangsmaatregelen moeten worden voorzien en tot slot lijkt § 1 van artikel 23 redundant met artikel 30 van de AVG dat reeds bepaalt dat de verwerkingsverantwoordelijke verplicht een register van de verwerkingsactiviteiten moet bijhouden.

Inhoud van het Register

167. Voor het overige erkent de Commissie het nut van het opleggen aan de betrokken openbare of private instellingen dat hun registers bijkomende elementen moeten bevatten bovenop deze bepaald in artikel 30 van de AVG waar specifieke kenmerken van hen worden vereist bij de verwerking van persoonsgegevens. Voor de leesbaarheid zou de formulering van artikel 23 in die zin moeten worden herzien. Na analyse denkt de auteur van het ontwerp aan de volgende aanvullende punten: een eventuele toevlucht tot profilering, de rechtsgrond, de categorieën externe bronnen, het protocol voor gegevensuitwisseling, het advies van de DPO en de motivering van de verwerkingsverantwoordelijke wanneer het advies van zijn DPO niet wordt gevolgd. Volgende opmerkingen kunnen dienaangaande worden gemaakt:

[50] Cf. hierover Elise Degrave, *L'e-gouvernement et la protection de la vie privée – Legalité, transparence et contrôle,* Collection du CRIDS, Larcier, 2014, p. 295 en v.

[51] *De Commissie vraagt zich af in hoeverre bepaalde delen van dit wetsontwerp nog actueel zijn aangezien dit niet overeenstemt met de uitleg die dienaangaande op 5 april 2018 werd verstrekt bij de FOD BOSA.*

i. De rubriek profilering zou facultatief moeten zijn en worden vervolledigd met " de verwijzing, in voorkomend geval, naar de wettelijke bepaling bedoeld in artikel 22 van de AVG".

j. De punten "rechtsgrond" en "categorieën van externe bronnen" zouden moeten worden gepreciseerd. Bedoelt men de wettelijke basis die de verwerking omkadert of de wettelijke basis die de opdracht van openbare dienst van de verwerkingsverantwoordelijke omkadert of allebei? Wat de categorieën externe bronnen betreft, bedoelt men de bron(nen) van persoonsgegevens waar de verwerkingsverantwoordelijke de gegevens onrechtstreeks inzamelt om zijn opdracht van openbare dienst te vervullen? Waarom enkel doelen op de categorieën van bronnen en niet de volledige bronnen als dusdanig?

k. De volgende bijkomende punten zouden kunnen worden toegevoegd[52]:
   i. De benaming van de verwerking (niet te verwarren met haar doeleinde);
   ii. De precisering met betrekking tot elk verwerkingsdoeleinde, indien bijzondere categorieën gegevens worden verwerkt in de zin van artikelen 9 en 11 van de AVG;
   iii. De aanduiding voor elk verwerkingsdoeleinde van de dienst bij wie de betrokkenen hun rechten kunnen uitoefenen;
   iv. Indien, met betrekking tot elk verwerkingsdoeleinde, de verwerking een gegevensbeschermingseffectbeoordeling vereiste en de verwijzingen naar het betrokken administratief document;
   v. In voorkomend geval, voor elk betrokken verwerkingsdoeleinde, de redenen waarop de verwerkingsverantwoordelijke zich baseert om te rechtvaardigen dat hij voldoet aan een van de wettelijke afwijkingen op de rechten van de betrokkenen;
   vi. Het overzicht van alle inbreuken in verband met persoonsgegevens zoals vereist in artikel 33.5 van de AVG.

Het Register mag niet worden gehouden bij de GBA

169. De § 4 en 5 van artikel 23 van het ontwerp bepalen dat het register van verwerkingsactiviteiten wordt bijgehouden door de Gegevensbeschermingsautoriteit (behalve dit van de politiediensten dat enkel ter beschikking van de van de Gegevensbeschermingsautoriteit wordt gesteld), wat strijdig is met de AVG aangezien het niet tot haar opdracht behoort het bijhouden van deze registers te verzekeren en het beheer van een dergelijk informaticasysteem haar begroting negatief zou beïnvloeden (terwijl het een regeringswens is om in de mate van het mogelijke een budgettair

[52] Cf. de Aanbeveling nr. 06/2017 van 14 juni 2017 van de Commissie betreffende het Register van de verwerkingsactiviteiten.

neutrale hervorming door te voeren[53]). Volgens de AVG blijft elke verwerkingsverantwoordelijke en verwerker verantwoordelijk voor het bijhouden van het Register van de verwerkingsactiviteiten. Aangezien de AVG reeds bepaalt dat het register op haar vraag ter beschikking moet gesteld worden van de toezichthoudende autoriteit, dienen deze twee paragrafen te worden geschrapt.

Openbaarheid van het register

170. Over de kwestie van de openbaarheid van het register, aangesneden in artikel 24 van het ontwerp, herinnert de Commissie eraan dat het Register van de verwerkingsactiviteiten in de eerste plaats een intern « accountability » instrument is voor de verwerkingsverantwoordelijke en de verwerker[54]. Voorzien (bij Koninklijk besluit) in het potentieel openbaar karakter van dit register (art. 24 van het ontwerp) is strijdig met de *ratio legis* van artikel 30 van de AVG.

171. Om te beantwoorden aan de problematiek van ondoorzichtigheid van de elektronische gegevensuitwisselingen door de betrokken openbare of private instellingen, dient te worden voorzien in een systeem van actieve openbaarheid dat kan worden gerealiseerd via een specifiek portaal dat ter beschikking wordt gesteld van de burgers die, mits voorafgaande authenticatie, kennis kunnen nemen van (i) de verschillende categorieën gegevensstromen in de betrokken openbare of private instellingen, met hun doeleinde(n), de verwijzing naar hun specifiek uitwisselingsprotocol en de datum van de publicatie in het Belgisch Staatsblad; (ii) het gebruik controleren dat zal worden gemaakt van hun persoonsgegevens ; (iii) de eventuele fouten in hun gegevens verbeteren[55] en, ten slotte, (iv) makkelijk in contact treden met de functionaris voor gegevensbescherming van de betrokken openbare of private instelling. Een dergelijk systeem zou het reeds bestaande recht op elektronische toegang dat reeds op verschillende niveaus is voorzien (Rijksregister….) op nuttige wijze vervolledigen. Gelet op artikel 2 van de wet van 11 april 1994 betreffende de openbaarheid van bestuur en het KB van 19 juli 2001 tot uitvoering van artikel 2, 1°, van de wet van 11 april 1994 betreffende de openbaarheid van bestuur, wordt misschien

[53] De Commissie onderschrijft niet de passage in de Memorie van toelichting met betrekking tot deze bepaling van het ontwerp (p. 45). Naast het feit dat een systeem van openbare registers die gecentraliseerd worden bij de CBPL deel uitmaakt van een logica die door de AVG bewust werd verlaten (Register van aangiften van verwerkingen) zou het houden van een dergelijk geïnformatiseerd systeem voor de GBA de ontwikkeling impliceren van specifieke IT middelen, wat een belangrijke kostprijs zou vertegenwoordigen. Hoewel het punt b (budgettaire impact) op pagina 3 van de Nota aan de Ministerraad van 9/03/2018 handelt over dit systeem, merkt de Commissie eveneens het foutieve karakter op van de 2de paragraaf. Geen enkele actuele technische infrastructuur zou hiertoe materieel kunnen worden gerecupereerd.

[54] Cf. de voormelde Aanbeveling 06/2017

[55] Cf. dienaangaande het advies CBPL 02/2018 van 17 januari 2018 over het ontwerp van KB tot vaststelling van de criteria op basis waarvan gegevens als authentiek gekwalificeerd worden en advies 08/2017 van de Europese toezichthouder voor gegevensbescherming over (vrije vertaling) het voorstel van Verordening tot oprichting van een uniek digitaal portaal en over het principe "voor eens en altijd".

geoordeeld dat de oprichting van dit portaal behoort tot de bevoegdheden van de FOD Kanselarij van de Eerste Minister.

Bijkomende hypothesen voor verplichte aanwijzing van een DPO (art.25 van het ontwerp)

172. Artikel 25 van het ontwerp voorziet in de gevallen waarin verplicht een DPO moet worden aangewezen, bovenop deze die reeds zijn voorzien in artikel 37.1 van de AVG. De Commissie is verwonderd over de reikwijdte van het toepassingsgebied van artikel 25 aangezien het alle privaatrechtelijke rechtspersonen[56] dekt die optreden als verwerker voor de voormelde federale openbare of private instellingen en/of bij hen persoonsgegevens inzamelen. Het is aangewezen om de voorkeur te geven aan de op het risico gebaseerde benadering van de AVG en enkel de verwerkingsverantwoordelijken en verwerkers aan deze verplichting te onderwerpen die verwerkingen uitvoeren die een zeker risico vormen (groot aantal bij de verwerkingen betrokken personen, verwezenlijking van opdrachten van openbare dienst (monopolie) die de verwerking vergen van de persoonsgegevens van de gebruikers van hun openbare diensten,...).

173. §2 van artikel 25 kan worden geschrapt aangezien de vertegenwoordiging reeds is voorzien in artikel 37.4 van de AVG.

Advies van de DPO (artikel 26 van het Ontwerp)

174. Artikel 26 verplicht de federale openbare of private instellingen om voorafgaand aan elke gegevensverwerking systematisch het advies van de DPO te vragen. Voor de gegevensuitwisselingen tussen deze instellingen verwijst de Commissie naar haar hogervermelde overwegingen. Voor het overige meent de Commissie dat verplichten om voor elke gegevensverwerking systematisch het advies van de DPO in te winnen niet strookt met de risicogebaseerde benadering van de AVG. Artikel 39 AVG omkadert reeds de taken van de DPO en bepaalt dat de verwerkingsverantwoordelijke en de verwerker er voor dienen te zorgen dat hij beschikt over de nodige middelen voor het vervullen van deze taken. Het bepaalt eveneens dat "*de functionaris voor gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.*" De Groep Artikel 29 heeft in zijn richtsnoeren hieruit afgeleid dat de DPO's prioriteiten zullen moeten bepalen onder hun activiteiten en hun inspanningen concentreren op de kwesties die een hoog risico vormen inzake gegevensbescherming[57].

Expertengroep (artikel 27 van het ontwerp)

[56] De formulering "privaatrechtelijke rechtspersoon" verdient de voorkeur op het gebruikte "particulier orgaan";
[57] Richtsnoeren van de Groep van het Artikel 29 betreffende de DPO, goedgekeurd op 5 april 2017, blz. 22

175. Artikel 27 van het ontwerp voorziet in de mogelijkheid om een expertengroep op te richten, samengesteld uit verwerkingsverantwoordelijken om op te treden als overlegplatform in het raam van de ontwikkeling van het beleid inzake gegevensbescherming in de schoot van de voormelde openbare en private instellingen. Gelet op de overlegdoelstelling van deze expertengroep zou het nuttig en relevant zijn de DPO's hierbij te betrekken. Bovendien zou artikel 27 van het ontwerp de concrete opdrachten van deze expertengroep moeten preciseren.

176. Artikel 28 van het ontwerp kan worden geschrapt aangezien artikel 35.1 van de AVG reeds voorziet in de verplichting voor de verwerkingsverantwoordelijke om het advies in te winnen van de DPO in het raam van de uitvoering van de gegevensbeschermingseffectbeoordeling (DPIA). De Commissie is immers van mening dat de formulering van artikel 39.1.c. deze verplichting niet opnieuw in vraag stelt.

Toepassing van artikel 35.10

177. Artikel 28 § 2 van het ontwerp stelt dat een DPIA wordt verricht vóór de verwerkingsactiviteit, ook al werd reeds een algemene gegevensbeschermingseffectbeoordeling uitgevoerd "in het kader van de vaststelling van de rechtsgrond". Dit standpunt stemt overeen met dat wat de Commissie uitdrukkelijk formuleerde in haar aanbeveling 01/2018 van 28 februari 2018 met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging en de toepassing van artikel 35.10 van de AVG.

4.5. Hoofdstuk V - Verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen

Uitvoering van artikel 85 van de AVG

178. Artikel 85 AVG verplicht elke lidstaat om wettelijke bepalingen goed te keuren om de twee grondrechten, zijnde het recht op bescherming van persoonsgegevens en het recht op vrijheid van meningsuiting en van informatie, daaronder begrepen de verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen, in overeenstemming te brengen. Voor deze verwerkingen laat artikel 85.2 AVG de lidstaten toe uitzonderingen of afwijkingen vast te stellen op sommige hoofdstukken van de AVG indien deze noodzakelijk zijn om deze twee grondrechten in overeenstemming te brengen; wat het doel is van hoofdstuk V van het ontwerp.

Begrip verwerking van persoonsgegevens voor journalistieke doeleinden

179. Artikel 29 van het ontwerp geeft een duidelijke definitie van het begrip verwerking van persoonsgegevens voor journalistieke doeleinden, die de nadruk legt op de grond van de informatie

en niet op de vorm, conform de rechtspraak van het HvJEU[58]. Naar het voorbeeld van de huidige "Franse privacywet[59]", beveelt de Commissie aan om hieraan een begrip naleving van de journalistieke deontologische regels als volgt toe te voegen : "en waarbij de verwerkingsverantwoordelijke zich de naleving van de journalistieke deontologische regels tot taak stelt".

Wettelijke basis

180. De Memorie van toelichting vermeldt met betrekking tot artikel 29 van het ontwerp een passage op basis van de rechtmatigheid van journalistieke verwerkingen. Er wordt vermeldt dat deze rechtmatigheidsbasis gebaseerd is op artikel 6.1.f van de AVG (gerechtvaardigd belang van de verwerkingsverantwoordelijke). Deze bepaling kan niet de enige potentiële rechtmatigheidsbasis zijn aangezien in bepaalde omstandigheden verwerkingen van journalistieke gegevens de toestemming vergen van de persoon over wie een reportage wordt gemaakt. Bijgevolg dient de passage van de Memorie van toelichting in die zin te worden gematigd.

Afwijkingen

181. L§3 en volgende van artikel 29 bevatten:

(i) afwijkingen op **de rechten van de betrokkenen** (recht op uitoefening van rechten ingeval van heridentificatie van de betrokkene op basis van door hemzelf verstrekte informatie, recht op voorafgaande informatie, recht op toegang, recht op rectificatie, recht op beperking van de verwerking, recht van verzet),

(ii) afwijkingen **op sommige verplichtingen opgelegd door de AVG** ten gunste van de verwerkingsverantwoordelijken en verwerkers (terbeschikkingstelling van het register van verwerkingsactiviteiten aan de Gegevensbeschermingsautoriteit, verplichting om met haar samen te werken, verplichting tot het melden van gegevenslekken, verplichting tot raadpleging van de GBA voor de voorafgaande gegevensbeschermingseffectbeoordeling die werden uitgevoerd en waaruit blijkt dat het residuair risico van de betrokken verwerking hoog blijft, afwijkingen op het hoofdstuk grensoverschrijdende gegevensstromen),

(iii) (iii) Afwijkingen **op de uitoefening van bevoegdheden door de toekomstige Gegevensbeschermingsautoriteit (GBA).**

De hiernavolgende opmerkingen dringen zich op met betrekking tot deze afwijkingen.

[58] Cf. Arrest van 16 december 2008, Satamedia, C-73/07, EU:C:2008:727, punt 61.
[59] Art. 67 van de Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Recht op de beperking van de verwerking

182. § 3 van artikel 29 moet worden geschrapt. Het is onnodig een afwijking te voorzien op artikel 11.2 van de AVG aangezien, indien de hypothese bedoeld in artikel 11.2 van de AVG zich voordoet, de betrokkene slechts de rechten zal kunnen uitoefenen die hem door de AVG worden verleend binnen de strikte grenzen bepaald in de uitvoeringsreglementering van de AVG (die een optimaal evenwicht zal hebben bereikt voor de eerbiediging van zowel het recht op de vrije meningsuiting als dat van de gegevensbescherming.

183. § 7 van artikel 29 van het ontwerp stelt de betrokken verwerkingsverantwoordelijken vrij van het recht op beperking van de gegevensverwerking (art. 18 AVG) wanneer door de toepassing van dit recht een voorgenomen publicatie in het gedrang wordt gebracht. De toepassing van het recht op beperking van gegevensverwerking kan er in de praktijk in bestaan de gegevens tijdelijk over te brengen naar een ander informatiesysteem, de geselecteerde gegevens tijdelijk ontoegankelijk te maken, of nog om de op een website gepubliceerde gegevens tijdelijk te verwijderen[60].

184. De Commissie begrijpt de noodzaak om af te wijken van dit recht wanneer de betrokkene zijn recht van bezwaar, bedoeld in artikel 21.1 van de AVG (18.1.d van de AVG) uitoefent en wanneer de juistheid van de gegevens door de betrokkene wordt betwist (hypothese bedoeld in artikel 18.1.a van de AVG) hoewel het onderscheid dient gemaakt te worden tussen de onderwerping van een journalistieke opinie aan een waarheidstest - wat kan gebeuren zonder het recht op vrije meningsuiting en persvrijheid met voeten te treden - en de controle op de juistheid van de persoonsgegevens waarop een journalistieke opinie is gebaseerd.

185. De hypotheses bedoeld in artikel 18.1.b en c (de verwerking is onrechtmatig en de persoon eist de beperking in de plaats van de uitwissing, of de verwerkingsverantwoordelijke heeft de gegevens niet langer nodig maar de betrokkene heeft deze nog nodig voor een rechtsvordering) dienen niet te worden gedekt door de afwijking van het ontwerp voor het afwegen van het recht op de vrijheid van meningsuiting en het recht op gegevensbescherming. Artikel 29, §7 moet op dit punt worden gecorrigeerd .

Recht van bezwaar

186. Artikel 29, § 8 van het ontwerp stelt de verwerkingsverantwoordelijken vrij van de eerbiediging van het recht van bezwaar van de betrokkenen, voorzien in artikel 21.1 van de AVG. Het is overmatig hiervan onbeperkt af te wijken. In navolging van wat reeds is bepaald in de huidige Privacywet,

[60] Cf. overweging 67 van de AVG.

dient te worden verduidelijkt dat deze vrijstelling slechts geldt indien de uitoefening van het recht van bezwaar bedoeld in artikel 21.1 een voorgenomen publicatie in het gedrang dreigt te brengen.

Recht op gegevenswissing

187. Wat het recht op gegevenswissing betreft merkt de Commissie op dat het ontwerp in geen enkele afwijking voorziet. Zij deelt niet de interpretatie van artikel 17.3 die werd opgenomen in de Memorie van Toelichting volgens welke een afwijking niet noodzakelijk is omdat volgens artikel 17.3 het recht op uitwissing niet van toepassing zou zijn op gegevensverwerkingen voor informatiedoeleinden of doeleinden van vrijheid van meningsuiting.

188. Artikel 17.3 van de AVG bepaalt immers dat *"De leden 1 en 2 (van artikel 17) zijn niet van toepassing voor zover verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie*"; wat impliceert dat een afweging moet worden gemaakt tussen de fundamentele rechten wanneer het recht op gegevenswissing wordt uitgeoefend, opdat de beperking van het recht op gegevenswissing enkel zou toegepast worden wanneer strikt noodzakelijk voor het recht van vrijheid van meningsuiting. De Memorie van Toelichting moet op dit punt[61] gecorrigeerd worden en gelet op de ervaring van de Commissie ter zake, wordt daartoe een wetgevend initiatief aanbevolen. De Commissie stelt volgende formulering voor:

> Voorstel: *"Artikel 17 van de Verordening is van toepassing op verwerkingen van persoonsgegevens voor journalistieke doeleinden of ten behoeve van academische, artistieke en literaire uitdrukkingsvormen indien hun informatieve inhoud niet of niet langer relevant is voor het debat van het algemeen nut of indien hun bewaring in de originele toestand niet aangewezen is gelet op hun inhoud of hun vorm of wegens de omstandigheden en de repercussies van hun informatieve inhoud op de betrokkene(n). De neemt, rekening houdend met de stand van de technologie, een van de volgende vormen aan:*
>
> *a) anonimisering van de informatieve inhoud;*
>
> *b) goedkeuring van technische maatregelen die, zonder afbreuk te doen aan de mogelijkheid om kennis te nemen van de betwiste informatieve inhoud bij de verwerkingsverantwoordelijke, op z'n minst toelaten de verspreiding ervan te beperken. (De Memorie van Toelichting zal in dit verband nuttig verwijzen naar de wijzigingen van de gewoonlijke verwijzingen, naar de toevoeging van een label No index dat belet dat het artikel van een referentie wordt voorzien door de zoekmotoren of nog naar de terbeschikkingstelling van het publiek van een gepseudonimiseerde versie...)".*

[61] De verwijzing naar het arrest Google Spain van het HvJEU zou eveneens moeten worden geschrapt aangezien dit arrest handelt over de tussenpersonen dienstverleners die de informatie verspreiden en niet over de journalistieke bron die de informatie als eerste publiceert.

Afwijkingen op de verplichtingen als verwerkingsverantwoordelijke of verwerker

Terbeschikkingstelling van het register aan de GBA

Melding van inbreuken aan de GBA

Voorafgaande raadpleging van de GBA

189. Wat betreft de uitzondering op de terbeschikkingstelling van het register van verwerkingsactiviteiten op vraag van de GBA (artikel 30.4 van de AVG), oordeelt de Commissie dat deze niet noodzakelijk is en dus strijdig met de AVG; immers, de AVG vereist niet dat het register van verwerkingsactiviteiten de identiteit bevat van de bij de verwerking betrokken personen. De afweging van de twee voormelde fundamentele rechten rechtvaardigt dus niet deze uitzondering. Hetzelfde geldt voor de artikelen 33 (Melding van inbreuken (gegevenslekken)) en 36 (voorafgaande raadpleging van de GBA voor de DPIA). Artikel 29, § 8, van het ontwerp dient dus te worden geschrapt. In geen enkel geval mag/kan de uitvoering van deze bepalingen ertoe leiden dat de inhoud van een persartikel dat op het punt staat te worden gepubliceerd onthuld wordt aan de Gegevensbeschermingsautoriteit en potentieel leiden tot een censuurmaatregel.

Verplichting tot samenwerking met de GBA

190. Wat de uitzondering betreft op de verplichte samenwerking van de verwerkingsverantwoordelijke met de Gegevensbeschermingsautoriteit (artikel 31 van de AVG) voorzien in artikel 29, § 9 van het ontwerp en de beperking van alle bevoegdheden van de Gegevensbeschermingsautoriteit ten opzichte van deze verwerkingen wanneer hun toepassing "aanwijzingen zou verschaffen over de informatiebronnen of wanneer de toepassing ervan een controlemaatregel voorafgaandelijk aan de publicatie van een artikel zou vormen" bedoeld in artikel 29, § 11 van het ontwerp, stelt de Commissie het overmatig karakter hiervan vast. De afwijking op artikel 31 van de AVG is niet noodzakelijk aangezien de toepassing ervan geen verplichting inhoudt tot het onthullen van de informatiebronnen. Wat artikel 29, § 11 van het ontwerp betreft, dit dient als volgt opnieuw geformuleerd te worden

> Voorstel: *"De Gegevensbeschermingsautoriteit oefent ten opzichte van de verwerkingsverantwoordelijken en verwerkers die verwerkingen van persoonsgegevens uitvoeren voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen, haar bevoegdheden bedoeld in artikelen 58.1 en 2. van de Verordening uit zonder kennis te nemen van de journalistieke informatiebronnen en zonder over te gaan tot een evaluatie van een journalistieke, academische, artistieke of literaire opinie"*.

191. De Commissie merkt eveneens op dat artikel 64 van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (GBA) bepaalt dat de onderzoeken van de haar

toekomstige inspectiedienst geheim zijn tot het moment van de neerlegging van het rapport van de inspecteur-generaal bij de geschillenkamer. Artikel 48 van diezelfde wet bepaalt dat zowel de leden van de gegevensbeschermingsautoriteit als de personeelsleden ervan wettelijk verplicht zijn het vertrouwelijke karakter te bewaren van de feiten, handelingen of inlichtingen waarvan zij uit hoofde van hun functie kennis hebben gehad.

CONCLUSIE van de Commissie over titel 1 van het ontwerp

192. Het advies van de Commissie is ongunstig voor heel hoofdstuk III van titel I voor de redenen uiteengezet in randnummer 145 van dit advies en gunstig voor de overige bepalingen op voorwaarde dat ontwerp wordt aangepast aan de volgende opmerkingen:

1.1. Betreffende Hoofdstuk I

1.1.1. Aanpassing van artikel 6 van het ontwerp om hierin duidelijk het toepassingsgebied van Titel I af te bakenen;

1.2. Betreffende Hoofdstuk II

1.2.1. Verduidelijken dat artikel 7 van het ontwerp artikel 8.1. van de AVG uitvoert ;

1.2.2. Schrapping van artikel 8, eerste lid, 2° van het ontwerp - deze verwerking moet omkaderd worden door een autonome wettekst conform de vereisten van artikel 9. 2. g van de AVG en die op z'n minst de waarborgen herneemt waarin reeds werd voorzien in de alinea's 2 tot 6 van § 6 van artikel 3 van de huidige Privacywet;

1.2.3. Schrapping van de litera 1° en 3° van het eerste lid van artikel 8 van het ontwerp die reeds gedekt worden door de litera d. en h. van artikel 9.2 van de AVG:

1.2.4. Herziening van artikel 9, § 1, 4° zoals aanbevolen om rekening te houden met het historisch onderzoek en de verwerkingsverantwoordelijken die belast zijn met opdrachten van openbare dienst bestaande uit archivering in het algemeen belang;

1.2.5. Toevoeging van bijzondere waarborgen voor de verwerking van genetische, biometrische of gegevens betreffende de gezondheid teneinde het beschermingsniveau dat thans wordt bereikt door de actuele wetgeving niet te verlagen.

1.2.6. In de Nederlandstalige versie van de definitie van gerechtelijk gegeven de woorden « strafbare feiten » vervangen door « strafrechtelijke inbreuken » ; Te bespreken

1.3. Betreffende Hoofdstuk IV

1.3.1. Vermindering van de in artikel 19 van het ontwerp voorziene termijn voor het versturen van de ontvangstbevestiging aan de betrokkenen;

1.3.2. Definitie van de termen "overheidsinstantie" en "overheidsorgaan" die gebruikt worden door de AVG;

1.3.3. Verbetering van de definitie van overheidsinstantie en overheidsorgaan voorgesteld in artikel 21 van het ontwerp teneinde precies en duidelijk het toepassingsgebied af te bakenen van afdeling 2 van dit hoofdstuk;

1.3.4. Wijziging van het facultatief systeem van protocol voor gegevensuitwisseling bedoeld in artikel 22 van het ontwerp, in een verplicht systeem beperkt tot de bedoelde gegevensstromen die risico's inhouden voor de rechten en vrijheden van de betrokkenen;

1.3.5. Aanpassing van de inhoud van het protocol aan de opmerkingen van de Commissie;

1.3.6. In artikel 22 van het ontwerp uitdrukkelijk voorzien dat de adviezen van de DPO's zullen aangehecht worden aan de protocollen;

1.3.7. Vermelden in artikel 22 van het ontwerp dat de protocollen overeenkomstig de criteria inzake voorzienbaarheid en toegankelijkheid zullen worden bekendgemaakt in het Belgisch Staatsblad.

1.3.8. De omkadering van de bedoelde gegevensstromen op nationaal niveau via door de wetgevers goedgekeurde samenwerkingsakkoorden;

1.3.9. Schrapping van artikel 24 van het ontwerp (gecentraliseerd register van verwerkingen van de openbare sector en geharmoniseerd beheer);

1.3.10. Aanpassing van de inhoud van het register van de openbare sector (art. 23 van het ontwerp) aan de opmerkingen van de Commissie;

1.3.11. Schrapping van de § 4 en 5 van artikel 23 van het ontwerp wegens strijdig met de AVG (gecentraliseerd houden van registers bij de GBA) en potentieel zware budgettaire impact van deze maatregel zonder echte meerwaarde in het licht van de opdrachten van openbare dienst van de GBA;

1.3.12. Schrapping van artikel 24 van het ontwerp dat voorziet dat de Koning het publieke karakter van het register van de verwerkingen van de openbare sector bepaalt en vervanging door een systeem van actieve openbaarheid zoals aangeprezen door de Commissie;

1.3.13. Beperking van de verruiming van de verplichte aanwijzing van een DPO (Art. 25 van het ontwerp) overeenkomstig de risicogebaseerde benadering van sommige verplichtingen in de AVG);

1.3.14. Beperking van het verplichte karakter van de adviezen van de DPO (art. 26 van het ontwerp) overeenkomstig de risicogebaseerde benadering van sommige verplichtingen in de AVG en de richtsnoeren van de Groep van het Artikel 29;

1.3.15. Schrapping van artikel 28, §1 van het ontwerp wegens redundant ten opzichte van de AVG;

1.4. Betreffende Hoofdstuk V

1.4.1. Toevoeging van het begrip van eerbiediging van de journalistieke gedragscode aan de definitie van de verwerking van persoonsgegevens voor journalistieke doeleinden;

1.4.2. Aanpassing van de Memorie van toelichting met betrekking tot de rechtmatigheidsbasis van journalistieke verwerkingen;

1.4.3. Schrapping van artikel 29, §3 van het ontwerp;

1.4.4. Beperking van de afwijking op het recht van beperking van de verwerking voorzien in artikel 29, § 7 van het ontwerp tot de hypothesen bedoeld in artikel 18.1.a en d. van de AVG;

1.4.5. Beperking van de afwijking op het recht van bezwaar van de betrokkenen, bedoeld in artikel 21.1 van de AVG, voorzien in artikel 29, § 8 van het ontwerp, tot het geval waarin de uitoefening van dit recht een voorgenomen publicatie in het gedrang dreigt te brengen;

1.4.6. Toevoeging van een afwijking op het recht op gegevenswissing (art. 17 AVG) zoals door de Commissie voorgesteld en verbetering van de Memorie van Toelichting dienaangaande;

1.4.7. Schrapping van artikel 29, §8 van het ontwerp (afwijking van de verplichte terbeschikkingstelling van het register van verwerkingsactiviteiten op vraag van de GBA, op de verplichting tot het melden van gegevenslekken aan de GBA, op de verplichte samenwerking met de GBA, op de verplichting tot voorafgaande raadpleging van de GBA voor de DPIA);

1.4.8. Aanpassing van artikel 29, § 9 van het ontwerp (beperking van de bevoegdheden van de GBA tegenover de bedoelde verwerkingsverantwoordelijken tot het strikt noodzakelijke) zoals voorgesteld.

5. TITEL 2: DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR DE BEVOEGDE OVERHEDEN MET HET OOG OP DE VOORKOMING, HET ONDERZOEK, DE OPSPORING EN DE VERVOLGING VAN STRAFBARE FEITEN OF DE TENUITVOERLEGGING VAN STRAFFEN, MET INEBGRIP VAN DE BESCHERMING TEGEN EN DE VOORKOMING VAN GEVAREN VOOR DE OPENBARE VEILIGHEID

193. Titels Titels 2 en 3 van het Ontwerp hebben respectievelijk betrekking op de verwerking van persoonsgegevens in de politie- en strafrechtketen enerzijds en door de inlichtingen- en veiligheidsdiensten, de Krijgsmacht en het Coördinatieorgaan voor de Dreigingsanalyse anderzijds. Gelet op de korte tijdsspanne waarin het advies van de Commissie moet worden uitgebracht, volgt in onderhavige onderdeel slechts analyse van enkele in het oog springende knelpunten.

OPMERKINGEN TITEL 2

194. Door titel 2 wordt de Richtlijn Politie & Justitie in de Belgische rechtsorde omgezet. Het betreft de verwerking van persoonsgegevens "*door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid*" (artikel 1.1. Richtlijn Politie & Justitie).

195. De Richtlijn Politie & Justitie is niet van toepassing op de verwerkingsactiviteiten van persoonsgegevens die buiten het toepassingsgebied van het Unierecht vallen en op de verwerkingen door de instellingen, organen en instanties van de Unie (artikel 1.3. Richtlijn Politie & Justitie). Bijgevolg is deze Richtlijn niet van toepassing op de verwerking van persoonsgegevens in het kader van de bescherming van de nationale veiligheid en Defensie. Deze worden dan ook afzonderlijk geregeld in titel 3.

196. Het onderscheid tussen AVG en de Richtlijn Politie & Justitie is vooral gelegen in een beperking op de transparantieplichten en de rechten van de betrokkene, zoals de onrechtstreekse toegang tot de persoonsgegevens, geen recht van verzet of recht op vergetelheid en geen recht op overdraagbaarheid van de persoonsgegevens. Daarnaast wordt er ook geen dwingend systeem van administratieve sancties opgelegd.

Afbakening in het kader van de finaliteit: toepassingsgebied

197. Artikel 32 van het Ontwerp herneemt de finaliteit zoals omschreven in voornoemd artikel 1.1. van de Richtlijn Politie & Justitie. Zoals uit artikel 1.1. van de Richtlijn Politie & Justitie blijkt, is het personele toepassingsgebied beperkt tot "bevoegde autoriteiten". Volgens de Richtlijn Politie & Justitie betreft het, kort gezegd, "*iedere overheidsinstantie die bevoegd is* voor de in artikel 1.1. omschreven doestelling of "*ieder ander orgaan of iedere andere entiteit die krachtens het lidstatelijke recht gemachtigd is openbaar gezag en openbare bevoegdheden uit te* oefenen" met het oog op deze finaliteit. Artikel 31.7.a) tot en met g) van het Ontwerp viseert de volgende entiteiten:

a) de reguliere politiediensten;
b) de gerechtelijke overheden, te verstaan de hoven en rechtbanken en het openbaar ministerie;
c) de Dienst Enquêtes van het Comité P;
d) de Algemene Inspectie van de federale en lokale politie;
e) de Algemene administratie van de douane en accijnzen, in het kader van haar taak inzake opsporing, vaststelling en vervolging van de misdrijven;
f) de Passagiersinformatie-eenheid, en
g) de Cel voor Financiële Informatieverwerking

198. Wat betreft het materieel toepassingsgebied wordt in de memorie van toelichting benadrukt dat het Ontwerp restrictief moet toegepast worden zodat er zo nauw kan aangesloten worden bij het personele toepassingsgebied van de Richtlijn Politie & Justitie. Dat heeft volgens de memorie van toelichting tot gevolg dat andere "*administratieve*" overheden niet als een bevoegde overheden in de zin van deze titel worden beschouwd, ook al zijn zij "*bevoegd tot controle, inspectie, of vervolging van strafbare feiten*". Indien de verwerkingsactiviteiten van deze administratieve overheden niet onder de finaliteit van de Richtlijn Politie & Justitie vallen, is de AVG van toepassing.[62]

199. De Commissie stelt echter vast dat er geen eenduidige criteria of aanknopingspunten worden aangegeven op basis waarvan de bevoegde autoriteiten aangeduid worden.. Waar daarentegen wel aanknopingspunten worden gezocht met de finaliteit van de Richtlijn Politie & Justitie lijkt dat niet het geval te zijn voor alle aangeduide bevoegde autoriteiten. Zo wordt in artikel 31.7.c) van het Ontwerp de Dienst Enquêtes van het Comité P als een "bevoegde overheid" beschouwd "*in het kader van zijn gerechtelijke*" opdrachten. Het Comité P heeft inderdaad een dubbele opdracht, met name een administratieve opdracht en een gerechtelijke opdracht, zodat de administratieve opdracht niet onder het toepassingsgebied van titel 2 valt.[63] Dezelfde redenering wordt echter niet doorgetrokken voor de Algemene Inspectie van de federale en lokale politie (AI) en de

[62] MvT, p. 64 en 69.
[63] Art. 16, tweede en derde lid, van de wet van 18 juli 1991 *tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreingingsanalyse*.

Passagiersinformatie-eenheid (PIE). Ook de AI heeft een dubbele opdracht[64], maar de specifieke afbakening tot gerechtelijke opdrachten wordt niet uitdrukkelijk in artikel 31.7.d) vastgelegd. De Passagiersinformatie-eenheid is een administratief orgaan die in een eerste fase persoonsgegevens van luchtvaarmaatschappijen ontvangt in het kader van de toepassing van de AVG, maar in een tweede fase de persoonsgegevens koppelt aan politionele gegevens met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en zware criminaliteit.[65] Vervolgens wordt in art. 31.7.e) van het Ontwerp ook de "*Algemene administratie van de douane en accijnzen*" (AADA) als bevoegde overheid beschouwd wanneer de verwerkingen gebeuren met het oog op opsporing, vaststelling en vervolging van de misdrijven die onder haar bevoegdheid vallen. In dat verband brengt de Commissie haar het advies 13/2015 van 13 mei 2015 in herinnering waarin wordt opgemerkt dat, gelet op de verschillende opdrachten die aan de AADA werden toebedeeld, alleen de onderzoeks- en opsporingsdienst van de AADA als een actor van de straf- en veiligheidsketen kan beschouwd worden.[66] [67] Om deze onduidelijkheid op te heffen, beveelt de Commissie aan om in artikel 31.7.e van het Ontwerp expliciet te refereren naar artikel 44/11/9, § 1, 4° van de wet op het politieambt, met name de onderzoeks- en opsporingsdienst en de administratie toezicht, controle en vaststellingen van de Algemene Administratie der douane en accijnzen.

200. Hoewel de Commissie begrijpt dat de afbakening van het toepassingsgebied geen sinecure is, neemt dit niet weg dat de criteria minstens in de memorie van toelichting moeten aangegeven worden.. Als bijvoorbeeld AI en de AADA zo ruim worden opgevat dat zij als een "bevoegde overheid" moeten aangeduid worden, valt niet in te zien waarom dat ook niet het geval zou zijn voor, bijvoorbeeld, de inspectiediensten van Economie, Milieu en, *a fortiori*, de Sociale Inlichtingen en Opsporingsdienst (SIOD). Ook deze diensten verwerken persoonsgegevens met een gerechtelijke finaliteit. Maar indien de aanvrager alle inspectiediensten onder de toepassing van de Richtlijn Politie & Justitie zou brengen, zou tot gevolg hebben dat het toepassingsbied ruimer wordt opgevat dan wordt bedoeld.

201. Bij wijze van suggestie stelt de Commissie de volgende oplossing voor. Uit de samenlezing van de preambule en de bepalingen van de Richtlijn Politie & Politie kan afgeleid worden dat het Kaderbesluit 2008/977/JBZ van 27 november 2008 als aanknopingspunt wordt genomen.[68] Met het oog op de harmonisatie van de gegevensverwerking met politionele en gerechtelijke doeleinden

[64] Wet van 15 mei 2007 *op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten*.
[65] Wet van 26 december 2016 *betreffende de verwerking van passagiersgegevens*.
[66] Zie randnummers 61-65.
[67] MvT, p. 62-63.
[68] Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 *over de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële samenwerking in strafzaken*.

wordt het raamwerk van het Kaderbesluit 2008 uitgebreid tot de interne verwerkingsactiviteiten van de reeds onder het Kaderbesluit 2008 begrepen bevoegde autoriteiten, met name de reguliere politie, het parket en de douane.

202. Wat betreft de instanties en organen die niet onder onderhavige titel 2 worden begrepen, vallen de verwerkingsactiviteiten (met een gerechtelijke finaliteit) onder de uitzonderingen van artikel 23.1., d en h) van de AVG waarbij in hun sectorale wetgeving wordt rekening gehouden met de voorwaarden en waarborgen van artikel 23.2. AVG. Op die manier wordt beter aangesloten bij de doelstellingen van zowel de AVG als de Richtlijn Politie & Justitie.

Definities

203. In artikel 31 van het Ontwerp worden alle definities van de Richtlijn Politie & Justitie hernomen. Artikel 31.3 definieert de "verwerkingsbeperking". Daaronder wordt verstaan "*het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken*". In de memorie van toelichting wordt daarbij vermeld dat deze "*behandelingsbeperking als doel (heeft) om bijvoorbeeld metadata toe te voegen*".[69] De Commissie is van oordeel dat het hier een foute interpretatie van de term "markeren" betreft. Zoals uit de definitie zelf volgt, is het de bedoeling om de verwerking van de persoonsgegevens te beperken. Aldus moet de verwerkingsverantwoordelijke de gegevens als het ware 'bevriezen' (en mogen dus niet gewist worden):

- wanneer door de betrokkenen de juistheid van de persoonsgegevens wordt betwist en dat niet kan geverifieerd worden; of
- de persoonsgegevens moeten (langer) bewaard worden met oog op het gebruik als bewijsmateriaal (artikel 16.3. Richtlijn Politie & Justitie).

204. Hieruit volgt dat bij het inroepen van een verwerkingsbeperking geen persoonsgegevens, zoals metadata, aan de betreffende persoonsgegevens kunnen "toegevoegd" worden. De Commissie nodigt de aanvrager dan ook uit om dit voorbeeld in de memorie van toelichting te schrappen, teneinde geen verwarring in de hand te werken.

Verwijzingen naar "toezichthoudende autoriteit"

205. Artikel 31.15. van het Ontwerp herneemt de definitie van "toezichthoudende autoriteit" van de Richtlijn Politie & Justitie. De Commissie vraagt zich af waarom hier niet reeds de toezichthoudende autoriteit wordt aangeduid. Dit zou het begrip en de leesbaarheid van de overige bepalingen van

[69] MvT, p. 59.

deze titel ten goede komen. Nu wordt de toezichthoudende autoriteit, met name het Controleorgaan op de politionele informatie, pas op het einde van Titel 2, in artikel 73 van het Ontwerp, kenbaar gemaakt. Aangezien deze toezichthoudende autoriteit het aanspreekpunt is in het kader van een verzoek tot onrechtstreekse toegang (*infra*), is het van belang dat het voor de betrokkene bij de analyse van zijn rechten reeds duidelijk is wie precies dit aanspreekpunt is. De Commissie is dan ook van oordeel dat het Controleorgaan op de politionele informatie uitdrukkelijk in artikel 31.15. van het Ontwerp moet aangeduid worden.

Rechtmatigheid van de verwerking

206. Artikel 38 van het Ontwerp beoogt de omzetting van artikel 8 Richtlijn Politie & Justitie, dat uitvoering geeft aan de legaliteitsvereiste, en aldus als de kernbepaling van het Ontwerp kan beschouwd worden. De tweede paragraaf van artikel 38 vermeldt dat "*De wettelijke verplichting verduidelijkt ten minste de categorieën van persoonsgegevens die verwerkt moeten worden en doeleinden van de verwerking*". In het belang van een consequent gebruik van de juridische terminologie roept de Commissie de aanvrager op om het woord "verduidelijkt" te vervangen door "regelt", wat beter aansluit bij de legaliteitsvereiste. Dat de wetgeving bovendien "duidelijk" moet zijn, is op zichzelf reeds een aspect van de kwaliteitsvereisten waaraan de wettelijke basis voor de verwerking van persoonsgegevens moet voldoen.

Rechten van de betrokkene

207. Artikel 46 van het Ontwerp vormt de uitzondering op de rechten van de betrokken. Met deze bepaling wordt artikel 17 van de Richtlijn Politie & Justitie in het Ontwerp omgezet die beperkingen op het recht op informatie, recht op inzage, het recht op verbetering, wissen en het recht op verwerkingsbeperking mogelijk maakt. In die zin is artikel 46 van het Ontwerp een voorzetting van artikel 13 van de WVP, de zogenaamde onrechtstreekse toegang, waarbij de betrokkene zich tot de toezichthoudende autoriteit moet wenden zodat deze laatste in de plaats van de betrokkene een controle in de politiedatabanken kan uitvoeren.

208. Uit artikel 46 volgt dat een systeem van onrechtstreekse toegang niet door het Ontwerp wordt opgelegd, maar in sectorale wetgeving moet geregeld worden met dien verstande dat de verzoeken om onrechtstreekse toegang bij de toezichthoudende autoriteit moeten ingediend worden.

209. Wat betreft de Passagiersinformatie-eenheid is een regeling van rechtstreekse en onrechtstreekse toegang vastgelegd in artikel 15, § 3, van de wet van 25 december 2016 *betreffende de verwerking van passagiersgegevens*. Wat betreft de aangeleverde passagiersgegevens heeft de betrokkene rechtstreeks toegang tot zijn persoonsgegevens. Daarvoor wordt het verzoek ingediend bij de functionaris voor de gegevensbescherming van de Passagiersinformatie-eenheid. Het gaat hier dus om het recht van inzage zoals vastgelegd in de

AVG. Voor de toegang tot de persoonsgegevens waarop de Passagiersinformatie-eenheid de vereiste controles heeft uitgevoerd, is het systeem van onrechtstreekse toegang van toepassing waarbij het verzoek bij de Commissie/Gegevensbeschermingsautoriteit wordt ingediend. Hiermee komt opnieuw de complexiteit van de gegevensverwerking tot uiting. Zowel het toepassingsgebied van AVG als de Richtlijn Politie & Justitie komt in beeld (*supra*).

210. Wat de andere bevoegde overheden betreft, vestigt de Commissie er de aandacht op dat de WVP door het Ontwerp wordt opgeheven en bijgevolg ook artikel 3, § 5 van de WVP dat voor de politie, het de Dienst Enquêtes van het Comité P en de Algemene inspectie van de politie voorziet in een uitzondering op de rechten van de betrokkene. Aangezien het weinig waarschijnlijk is dat de sectorale wetgeving van deze bevoegde autoriteiten zal aangepast zijn wanneer het Ontwerp effecief van toepassing wordt, zal dit gevolgen hebben voor het systeem van onrechtstreekse toegang.

211. De Commissie begrijpt overigens niet waarom in de paragrafen 4 en 5 van artikel 46 van het Ontwerp opnieuw wordt vermeld dat de rechten van de betrokkene door de toezichthoudende autoriteit worden uitgeoefend, terwijl dat deze voorwaarde reeds in de tweede paragraaf van hetzelfde artikel wordt vastgelegd. Deze herhaling is niet zinvol en schept de foute indruk dat het ter zake een "bijzondere" afwijking betreft (of het geval zou kunnen zijn) op de "algemene" uitzondering op de rechten van de betrokkene zoals vastgelegd in artikel 46 van het Ontwerp. De Commissie is van oordeel dat de verwijzing naar de toezichthoudende autoriteit in deze paragrafen overbodig is, en bijgevolg dient geschrapt te worden.

212. Wanneer de betrokkene bij de toezichthoudende autoriteit een verzoek tot onrechtstreekse toegang indient voor zijn persoonsgegevens die door de politie, de douanediensten of de Cel Financiële Informatie worden verwerkt, wordt door de dezelfde paragrafen 4 en 5 van artikel 46 van het Ontwerp voorzien dat aan de betrokkene "*bepaalde contextuele informatie*" kan worden medegedeeld. Het is de bevoegde minister die, na advies van de toezichthoudende autoriteit, de richtlijnen vastlegt inzake de "*categorieën van contextuele informatie*" die aan de betrokkene kan worden verstrekt.

213. De Commissie is voorstander van een gelaagde transparantie naar gelang de context waarbij de onrechtstreekse toegang wordt verzocht. Het aantal politiedatabanken neemt sterk toe en worden door tal van niet-politionele doeleinden geraadpleegd of bevraagd. In specifieke situaties worden zelfs de politionele antecedenten van burgers (in abstracte vorm) aan private actoren doorgegeven terwijl deze actoren op zichzelf niet tot de strafrecht- en veiligheidsketen behoren. De

betrokkenen weten daarentegen doorgaans niet of, laat staan waarom, hun persoonsgegevens in een politionele databank worden verwerkt. De maatschappelijke realiteit leert dat de persoon van wie zijn gegevens in politiedatabanken zijn opgeslagen een reëel risico loopt op negatieve gevolgen voor zowel zijn professionele leven als zijn privéleven. Een gelaagde transparantie is dus onontbeerlijk en zal ertoe bijdragen dat de toegang tot de rechter wordt versterkt, wat een van de uitgangspunten is die met het nieuwe Europees kader inzake de persoonsgegevensbescherming wordt nagestreefd.[70]

214. In dat verband wijst de Commissie erop dat het verstrekken van contextuele informatie aan de betrokkene met zich meebrengt dat de betrokkene van zijn kant ook de relevante elementen en omstandigheden van het verzoek zal moeten meedelen opdat er kan worden onderzocht of en zo ja, welke informatie aan de betrokkene kan worden meegedeeld. De Commissie beveelt aan dat in de memorie van toelichting hierop wordt gewezen, met de aanbeveling dat de sectorale wetgeving in die zin wordt aangepast.

215. In artikel 47 van het Ontwerp wordt vastgelegd dat wanneer de persoonsgegevens van de betrokkene worden verwerkt in het kader van een strafrechtelijk onderzoek en strafrechtelijke procedures de rechten van de betrokkene worden uitgeoefend overeenkomstig het Gerechtelijk wet boek en het wetboek van Strafvordering. Deze mogelijk wordt voorzien in de Richtlijn Politie & Justitie. Hierbij heeft de Commissie geen bijzondere opmerkingen.

<u>Persoonsgegevens ontvangen van andere overheden uit Titel 3</u>

216. Artikelen 48 en 49 van het Ontwerp voorzien in een beperking op de rechten van de betrokkene in geval de bevoegde autoriteiten informatie ontvangen van de inlichtingen- en veiligheidsdiensten of het Coördinatieorgaan voor de dreigingsanalyse (OCAD).

217. De Commissie ziet evenwel niet in waarom deze bepaling in Titel 2 wordt opgenomen, nu ook in Titel 3 uitzonderingen op de rechten van de betrokkene worden voorzien voor de verwerkingsactiviteiten door de inlichtingen- en veiligheidsdiensten en het OCAD. Wanneer de bevoegde overheden van Titel 2 persoonsgegevens ontvangen met het oog op de uitoefeningen van de opdrachten van de inlichtingen- en veiligheidsdiensten en het OCAD, dan gelden de beperkingen op de rechten van de betrokkene uit hoofde van Titel 3 ook op doorgifte van de persoonsgegevens aan de bevoegde overheden van Titel 2 . Dat zal slechts anders zijn wanneer de deze overheden de persoonsgegevens voor hun eigen, en dus andere, doeleinden gebruiken. Maar

[70] Vgl. R. SAELENS, '*Profiling* for Tomorrowland: de screening van festivalgangers door de politie', *TPP* 2018, afl. 1, 20 – 27.

in dat geval zouden de uitzonderingen op de rechten van de betrokkene uit hoofde van Titel 2, met name via de toepassing van artikel 46 van het Ontwerp, moeten gelden.

218. Daarnaast, zoals in Titel 1 wordt opgemerkt, wijst de Commissie er op dat de definitie van ontvanger niet van toepassing is op overheden die de persoonsgegevens in het kader van hun bijzonder onderzoek conform het nationaal recht ontvangen. Het betekent dat, hoewel de mogelijkheid van gegevensuitwisseling tussen de overheden in Titel 2 en 3 in de sectorale wetgeving moet vastgelegd zijn, de betrokkene niet specifiek moet geïnformeerd worden wanneer een overheid bedoeld in Titel 3 persoonsgegevens van de betrokkene aan een bevoegde overheid in Titel 2 doorgeeft.

219. Het voorgaande geldt evenwel niet voor particulieren, die dus wel als "ontvanger" worden beschouwd wanneer zij informatie van overheden uit Titel 2 of 3 zouden ontvangen. De Commissie merkt in dat verband op dat de doorgifte van persoonsgegevens door de politiediensten aan de private sector in het kader van de opdrachten van bestuurlijke en gerechtelijke politie niet in de wet op het politieambt is geregeld. Aangezien in het kader van de integrale veiligheid ook de private sector als een belangrijke actor in de veiligheidsketen wordt beschouwd, leidt dat in de praktijk tot situaties waarbij de rechtspositie van zowel de politie als de betrokkene onduidelijk is. Naar analogie met het hierboven besproken systeem van onrechtstreekse toegang zou kunnen nagedacht worden aan de mate waarin (bij de toepassing van de onrechtstreekse toegang) door de *bevoegde autoriteit* aan de betrokkene die het voorwerp uitmaakt van een negatieve beslissing of een beslissing die hem in aanmerkelijke mate treft contextuele informatie kan worden verstrekt zodat hij de beslissing desgewenst aan de rechter kan voorleggen, zonder dat er de facto toegang wordt verleend tot de politiedatabanken.

220. In artikel 50 van het Ontwerp wordt gewag gemaakt van het "controlesysteem", zonder dat dit wordt gedefinieerd. Hoewel uit de memorie van toelichting kan opgemaakt worden dat het systeem betrekking heeft op de controle van het gebruik van en de toegang tot de gegevensbanken, is de Commissie van oordeel dat het controlesysteem in artikel 31 van het Ontwerp moet gedefinieerd worden.

221. De Commissie begrijpt niet wat de ratio is van artikel 51 van het Ontwerp. Deze bepaling lijkt een afspiegeling van artikel 18 van Titel 1, maar in de memorie van toelichting ontbreekt enige duiding. Het betreft de situatie waarbij de betrokkene het voorwerp uitmaakt van aan "gemeenschappelijke verwerking", met name de situatie waarbij verschillende actoren dezelfde persoonsgegevens verwerken, ieder binnen het kader van hun bevoegdheden en finaliteit waarop de hierboven besproken beperkingen op de rechten van de betrokkene van toepassing blijken te zijn. De Commissie ziet daarbij gelijkenissen met de verwerkingen die gebeuren in het kader van

de gemeenschappelijke gegevensbank (*Foreign) Terrorist Fighters* die krachtens artikel 44/11/3*bis* van de wet op het politieambt is opgericht.

222. De Commissie is van oordeel dat de term "gemeenschappelijke verwerking" in de definities van artikel 31 van het Ontwerp moet opgenomen worden. Indien het ook gaat om een gemeenschappelijk gegevensbanken zoals bedoeld in artikel 44/11/3*bis* van de wet op het politieambt moeten deze in het Ontwerp worden aangeduid. In dat verband verwijst de Commissie naar de opmerkingen over artikel 18 van Titel 1 van het Ontwerp.

223. Wat betreft § 6 van artikel 51 van het Ontwerp begrijpt de Commissie evenmin de verwijzing naar het "*beroep*" dat bij de toezichthoudende autoriteit aanhangig wordt gemaakt. Er kan immers geen "beroep" bij de toezichthoudende autoriteit aanhangig worden gemaakt.

De plichten van de verwerkingsverantwoordelijke

224. In artikel 52 van het Ontwerp heeft betrekking op verplichting om passende organisatorische en technische maatregelen te nemen. Het gebruik van de term "mogen" veronderstelt een vrijheid in hoofde van de verwerkingsverantwoordelijke die door de Richtlijn Politie & Justitie niet wordt gegund. In overweging 53 van de Richtlijn Politie & Justitie, die blijkbaar in artikel 52 van het Ontwerp wordt vastgelegd, wordt gezegd dat de verwerkingsverantwoordelijke intern beleid "*dient*" vast te stellen". Het betreft dus een *verplichting* en niet een keuzevrijheid in hoofde van de verwerkingsverantwoordelijke.

De functionaris gegevensbescherming

225. Artikel 60 van het Ontwerp heeft betrekking op de gegevensbeschermingseffectbeoordeling. De Commissie merkt op dat in de memorie van toelichting ten onrechte wordt aangenomen dat deze verplichting ook op de functionaris voor gegevensbescherming kan rusten.[71] Deze verplichting rust echter louter op de verwerkingsverantwoordelijke, die uiteraard kan worden bijgestaan door de functionaris voor gegevensbescherming. De Commissie nodigt de aanvrager de toelichting in die zin aan te passen.

CONCLUSIE van de Commissie over titel 2 van het ontwerp

226. De Commissie legt de nadruk op een duidelijke afbakening van het toepassingsgebied van de Richtlijn Politie & Justitie in het Ontwerp. De keuze om bepaalde overheidsorganen of

[71] MvT, p. 103.

overheidsdiensten al dan niet onder de toepassing van Titel 2 te plaatsen is niet gebaseerd op aangegeven criteria zodat deze niet kan afgetoetst worden aan het restrictief toepassingsgebied die door de aanvrager wordt vooropgesteld.

Daarnaast wordt een systeem van beperkingen op de rechten van de betrokkene uitgewerkt waarbij het voor de betrokkene moeilijk te vatten is ten opzichte van welke verwerkingen het onrechtstreekse toegang geldt, met name alleen de verwerkingsactiviteiten onder Titel 2 of tevens op, of voor zover, de persoonsgegevens ontvangen werden door overheden uit Titel 3. Daarnaast worden bepaalde concepten geïntroduceerd die naar het oordeel van de Commissie moeten gedefinieerd worden.

Daarom brengt de Commissie een **ongunstig** advies uit wat betreft de afbakening van het toepassingsgebied;
Voor het overige een **gunstig** advies uitbrengt, mits wordt voldaan aan de volgende opmerkingen:

- in toezichthoudende autoriteit het uitdrukkelijk in de definities benoemen;
- in artikel 38 van het Ontwerp het woord "verduidelijkt" vervangen door "regelt";
- de verwarring die door de paragrafen 4 en 5van artikel 46 van het Ontwerp ontstaat, wegwerken;
- onderzoeken of de opname van de artikelen 48 en 49 van het Ontwerp, waarin wordt voorzien in een beperking op de rechten van de betrokkene in geval de bevoegde autoriteiten informatie ontvangen van overheden uit Titel 3, wel zinvol is;
- de termen "controlesysteem" en "gemeenschappelijke verwerking" definiëren;
- in artikel 52 van het Ontwerp het woord "mogen" vervangen door "dient";
- schrappen van de verplichting voor de functionaris voor gegevensbescherming om een gegevensbeschermingseffectbeoordeling uit te voeren

6. TITEL 3 : DE BESCHERMING VAN NATUURLIJKE PERSONEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS DOOR ANDERE OVERHEDEN DAN DIE BEDOELD IN TITELS 1 EN 2

6.1. Ondertitels 1, 2, 3 en 4

227. Titel 3 heeft betrekking op de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten, de Krijgsmacht, OCAD en Passagiers-eenheid specifiek met betrekking tot de verwerkingsactiviteiten die onder de nationale veiligheid vallen. Zoals hierboven al uiteengezet, is in principe de AVG noch de Richtlijn Politie & Justitie van toepassing op de verwerking van persoonsgegevens door deze overheidsdiensten en de Defensie. Niettemin werd de verwerking van persoonsgegevens door deze diensten geregeld door de WVP. Daarnaast moet rekening worden gehouden met het Verdrag nr. 108 van 28 januari 1982 *tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens* (Verdrag nr. 108).

228. Met Titel 3 van het Ontwerp bevestigt de aanvrager de toepassing van de algemene principes voor de verwerking persoonsgegevens door deze entiteiten. Daarvoor wordt mutaties mutandis een afspiegeling gemaakt van de Richtlijn Politie en Justitie. In dat verband worden de definities van artikel 31 van het Ontwerp hernomen, met uitzondering van "bevoegde overheden", "verwerkingsverantwoordelijke", "ontvanger" en "toezichthoudende autoriteit". Behalve de "ontvanger" worden deze in artikel 74 van het Ontwerp opnieuw gedefinieerd.

Bijzondere categorieën persoonsgegevens

229. Artikel 77 van het Ontwerp herneemt de basisbeginselen, met name de vereisten van rechtmatigheid, doelbindingsprincipe, noodzakelijkheid, proportionaliteit en accuraatheid. Volgens artikel 78 van het Ontwerp verwerken de inlichtingen- en veiligheidsdiensten persoonsgegevens van alle aard verwerken, inbegrepen bijzondere categorieën van persoonsgegevens, waaronder genetische en biometrische gegevens, en strafrechtelijke gegevens.

230. De Commissie begrijpt dat de inlichtingen- en veiligheidsdiensten de mogelijkheid moeten hebben om elk type van persoonsgegeven te verwerken om te kunnen anticiperen op elke bedreiging van de nationale veiligheid.[72] De Commissie brengt evenwel in herinnering dat de bijzondere categorieën van persoonsgegevens slechts kunnen verwerkt worden wanneer de

[72] MvT, p. 143.

specifieke aard van het persoonsgegeven in verband staat met het te beschermen belang dat in de wet op de inlichtingen- en veiligheidsdiensten is vastgelegd.

231. De Commissie stelt vast dat de inlichtingen- en veiligheidsdiensten rechtstreeks door artikel 78 van het Ontwerp worden gemachtigd om bijzondere categorieën van persoonsgegevens te verwerken, zonder dat in de sectorale wetgeving de noodzaak en de proportionaliteit moeten uitgewerkt en gerechtvaardigd worden. De aanvrager verantwoordt deze machtiging om bijzondere categorieën van persoonsgegevens te verwerken door te verwijzen naar artikel 3, § 4 WVP en artikel 9, § 2 van het Verdrag nr. 108.[73] De Commissie verwijst in dat verband naar de bezwaren over de artikelen 10 en 11 van Titel 1. Zo rijst de vraag naar de noodzaak en de proportionaliteit voor het verwerken van, bijvoorbeeld, genetische persoonsgegevens.

Recht van toegang

232. In het licht van de opdrachten van de inlichtingen- en veiligheidsdiensten voorziet artikel 80 e.v. van het Ontwerp in beperkingen op de rechten van de betrokkene. Daarbij wordt verwezen naar de overeenstemmende bepalingen van de wet van 30 november 1998 *houdende regeling van de inlichtingen- en veiligheidsdiensten*. De Commissie merkt op dat artikel 82 van het Ontwerp voor verwarring zorgt door te suggereren dat artikel 2, § 3 van de wet van 30 november 1998 betrekking heeft op het recht van toegang. In dat laatste artikel gaat het, onder voorwaarden, echter om een notificatieplicht aan de betrokkene wanneer hij het voorwerp was van bepaalde onderzoeksmethoden. Het betreft dus een informatieplicht *a posteriori* die los staat van het "recht van toegang". In dat opzicht heeft artikel 82 geen enkele meerwaarde, tenzij deze bepaling een impact heeft op artikel 83 van het Ontwerp. Nu artikel 83 van het Ontwerp voorziet in een systeem van onrechtstreekse toegang zou het samenlezen van artikel 82 en 83 immers de indruk kunnen wekken dat zelfs de onrechtstreekse toegang kan beperkt worden. Maar hiervoor wordt geen enkele rechtvaardiging gegeven. De Commissie beveelt aan om artikel 82 van het Ontwerp te schrappen of de de eventuele weerslag op de onrechtstreekse toegang aan te geven en te rechtvaardigen.

Contactpunt gezamenlijke verwerkingsverantwoordelijken

233. De situatie kan zich voordoen dat er sprake is van gezamenlijke verwerkingsverantwoordelijken. In tegenstelling tot wat in Titel 2 van het Ontwerp wordt vereist, zijn de gezamenlijke verwerkingsverantwoordelijken volgens artikel 89 van het Ontwerp vrij om al dan niet in de onderlinge overeenkomst één contactpunt voor de betrokkene aan te wijzen. De Commissie is daarentegen van oordeel dat een contactpunt *moet* aangewezen worden. Dat is niet alleen van

[73] MvT, p. 136.

belang voor de betrokkene teneinde zijn rechten te kunnen afdwingen. Daarnaast is het aanwijzen van een aanspreekpunt ook van belang voor de contacten met de toezichthoudende autoriteit.

Inbreuk op de beveiliging

234. Wat betreft de melding van een inbreuk op de beveiliging van de persoonsgegevens voorziet artikel 90 van het Ontwerp niet een termijn. De Commissie roept de aanvrager op om dezelfde termijn vast teleggen als deze die is opgelegd in Titel 2 van het Ontwerp , met name 72 uur.

Register

235. De verwerkingsverantwoordelijken onder Titel 3 moeten ook een register bijhouden. De Commissie vindt het opmerkelijk dat volgens artikel 92 van het Ontwerp de inlichtingen en veiligheidsdiensten niet de categorieën van personen en de categorie van persoonsgegevens in het register moeten opnemen. Volgens de memorie van toelichting ligt de reden in het feit dat er eigenlijk alleen sprake is van "doelwitten".

236. De Commissie begrijpt dat de registratiegrond van persoonsgegevens door de veiligheids- en inlichtingendiensten gekoppeld is aan een activiteit die een dreiging vormt zoals vastgelegd in de wet van 30 november 1998 *houdende regeling van de inlichtingen en veiligheidsdiensten*. Maar die activiteit staat ontegensprekelijk in verband met een persoon waarbij diens handeling (activiteit) een dreiging vormt voor de nationale veiligheid. De Commissie is dan ook van oordeel dat wanneer de inlichtingen en veiligheidsdiensten de handel en wandel van (natuurlijke) personen of groeperingen nagaan daarbij identificatiegegevens en andere categorieën van persoonsgegevens worden verwerkt, zoals extreem rechts, extreem links, geradicaliseerd, salafist, enz. De Commissie ziet dan ook niet in waarom het register niet de categorieën van personen en categorieën van persoonsgegevens zou moeten vermelden.

237. Tot slot blijkt uit hetzelfde artikel 92 van het Ontwerp dat de inlichtingen en veiligheidsdiensten de contactgegevens van verwerkingsverantwoordelijke of beheerders van andere (buitenlandse) gegevensbanken waartoe zij toegang hebben slechts in het register moeten vermelden indien zij de contactgegevens van (de verwerkingsverantwoordelijke of de beheerder) kennen.[74] De Commissie acht het zeer merkwaardig dat de inlichtingen- en veiligheidsdiensten ook toegang zou hebben tot gegevensbanken waarvan zij de contactgegevens (van de beheerder) niet kennen. De (rechtmatigheid van de) toegang tot persoonsgegevens zal immers afhangen van de mate waarin voorafgaand met de bevoegde (buitenlandse) overheidsdienst is afgetoetst hoe de toegang tot deze gegevensbanken kan worden afgesproken binnen het kader van de wettelijke opdrachten van de

[74] MvT, p. 143.

inlichtingen- en veiligheidsdiensten. Er valt dan ook niet in te zien waarom de contactgegevens van (minstens) de beheerder van de gegevensbank niet in het register zou kunnen opgenomen worden.

Verwerken van bijzondere categorieën persoonsgegevens in het kader van veiligheidsmachtigingen, -attesten en –adviezen

238. Wat betreft de verwerkingen in het kader van de toepassing van de wet van 11 december 1998 *betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen* herhaalt de Commissie de noodzaak om reeds in de definitie van "toezichthoudende autoriteit" de toezichthoudende autoriteit uitdrukkelijk te benoemen (*supra*).

239. De Commissie stelt vast dat een resem overheden (kunnen) betrokken zijn bij de verwerking van persoonsgegevens in het kader van veiligheidsmachtigingen, -attesten en -adviezen (art. 109 van het Ontwerp). Problematisch is dat de overheden bedoeld in artikel 109 van het Ontwerp door artikel 112 van het Ontwerp rechtstreeks worden gemachtigd om bijzondere categorieën persoonsgegevens te verwerken zonder dat wordt onderzocht in welke mate dat noodzakelijk en proportioneel is, aangezien blijkbaar *alle* (mogelijks) betrokken overheden, ongeacht het gaat om veiligheidsmachtigingen, -attesten of –adviezen, *sommige of alle* bijzondere categorieën persoonsgegevens mogen verwerken. De Commissie verwijst naar de hierboven geformuleerde opmerkingen met betrekking tot het gelijkaardig artikel 78 van het Ontwerp. Net zoals dat het geval is voor artikel 78 van het Ontwerp, brengt de redactie van artikel 112 van het Ontwerp immers met zich mee dat de noodzaak en de proportionaliteit niet meer in de sectorale wetgeving moet onderzocht worden.

Overige opmerkingen

240. Artikel 187, § 4 van het Ontwerp bepaalt dat de Gegevensbeschermingsautoriteit (GBA) niet bevoegd is om toezicht uit te oefenen op de verwerking van persoonsgegevens door de bestuurlijke commissie in het kader van haar opdrachten.. Deze bestuurlijke commissie is belast met het toezicht op de specifieke en uitzonderlijke methoden van de inlichtingen- en veiligheidsdiensten. Daarnaast is de GBA ook niet bevoegd voor de verwerkingen in het kader van hun opdraxchten door het Comité I, het Comité P en het C.O.C. Volgens de memorie van toelichting behoeft dit artikel geen commentaar. De Commissie merkt toch volledigheidshalve op dat deze organen ook persoonsgegevens verwerken die onder de toepassing van de AVG vallen en daardoor onder het toezicht van de GBA vallen, tenzij ook het toezicht op deze verwerkingsactiviteiten uitdrukkelijk aan deze controleorganen is toegekend zoals het geval is voor alle verwerkingen van de politie die onder het toezicht van het C.O.C. zouden vallen. In het onderhavige advies wordt hierop nog teruggekomen bij de analyse over het landschap van de toezichthoudende autoriteiten.

241. In dat verband vraagt de Commissie zich overigens af wat precies de plaats is van de bestuurlijke commissie nu ook dit orgaan persoonsgegevens verwerkt in het kader van de controle op het gebruik van de bepaalde onderzoeksmethoden door de inlichtingen- en veiligheidsdiensten. Valt zij onder de controle van het Comité I als toezichthoudende autoriteit, geniet zij de uitzondering zoals voorzien voor gerechten in het kader van rechtszaken of wordt voorzien in een controle sui generis?

CONCLUSIE van de Commissie over de ondertitels 1 tot en met 4 van titel 3 van het ontwerp

242. Samenvattend neemt de Commissie akte van de bevestiging dat ook voor de verwerkingsactiviteiten die buiten het Unierecht vallen deze actoren onderworpen zijn aan de principes van het persoonsgegevensbeschermingsrecht. Niettemin heeft de Commissie enkele knelpunten opgemerkt waarmee in het Ontwerp moet rekening worden gehouden.

Wat betreft de verwerking van bijzondere categorieën persoonsgegevens zoals geregeld in de artikelen 78 en 112 van het Ontwerp brengt de Commissie **ongunstig** advies uit, gelet op de fundamentele opmerkingen ter zake.
Voor het overige brengt de Commissie een **gunstig** advies uit, mits wordt voldaan aan de volgende opmerkingen:

- uitdrukkelijk aanduiden van de toezichthoudende autoriteit;
- opnemen van de categorieën personen en categorieën persoonsgegevens in het register;
- opnemen van de contactgegevens van de gegevensbanken in het register;
- vastleggen van een termijn voor het melden van inbreuken op de beveiliging van persoonsgegevens;
- de noodzaak van artikel 82 onderzoeken en de eventuele impact ervan op artikel 83 van het Ontwerp rechtvaardigen;
- in geval van gezamenlijke verwerkingsverantwoordelijken de verplichting opleggen om een contactpunt in het register op te nemen.

6.2. Ondertitel 5. De bescherming van natuurlijke personen met betrekking tot bepaalde verwerkingen van persoonsgegeens door de passagiersinformatie-eenheid

243. Er is in een bijzonder beschermingsstelsel voorzien voor de verwerkingen van passagiersgegevens (PNR)[75] door de passagiersinformatie-eenheid (PIE) die worden verricht voor de doeleinden bedoeld onder artikel 8, §1, 4° van de wet van 25 december 2016 *betreffende de verwerking van passagiersgegevens*[76] (hierna de wet PNR), namelijk voor de opvolging door de inlichtingendiensten van activiteiten die de fundamentele belangen van de Staat kunnen bedreigen. Volgens de Memorie van Toelichting worden "*De verwerkingen in het kader van de finaliteit bedoeld in artikel 8, §1, 4° van voornoemde wet van 25 december 2016 ingedeeld onder Titel 3 daar dit verwerkingen betreffen van persoonsgegevens (passagiersgegevens), uitgevoerd in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten als bedoeld in artikelen 7 en 11 van de wet van 30 november 1998 (organieke wet inlichtingen- en veiligheidsdiensten)*". De Commissie noteert dat de activiteiten van de inlichtingendiensten inderdaad niet onder het toepassingsgebied vallen van de Unie en bijgevolg niet onderworpen zijn aan de AVG of de Richtlijn Politie & Justitie. Artikel 271, 2de lid van het Ontwerp bepaalt dat de andere titels van het Ontwerp niet van toepassing zijn op de betrokken verwerkingen afgezien van sommige bepalingen betreffende de strafrechtelijke straffen[77].

244. De concrete betrokken verwerkingen zijn hier:

- de correlatie tussen de passagiersgegevens die werden verstrekt door de vervoerder of reisoperatoren met de databanken van de inlichtingendiensten of met de criteria bestemd om individuen uit te steken tijdens de voorafgaande passagiersbeoordelingen in het kader van de opvolging door de inlichtingendiensten van activiteiten die de fundamentele belangen van de Staat kunnen bedreigen;
- gerichte opzoekingen in de passagiersgegevensbank voor inlichtingendoeleinden.

245. Ondertitel 5 van Titel 3 van dit Ontwerp bepaalt:

- de algemene verwerkingsvoorwaarden: beginsels inzake rechtmatigheid, doeleinde van de verwerkingen, proportionaliteit en kwaliteit van de gegevens;
- de bewaring van de gegevens;
- de rechten van de betrokkene;
- de verplichtingen van de verwerkingsverantwoordelijke inzake de beveiliging van de verwerkingen en betreffende het bijhouden van een register van gegevensbanken van de PIE en van deze die hen ter beschikking staan;
- de voorwaarden voor de internationale doorgifte van PNR-gegevens.

[75] Passenger Name Record.
[76] http://www.ejustice.just.fgov.be/eli/wet/2016/12/25/2017010166/justel.
[77] Te weten de artikelen 239 en 240 van het Ontwerp.

246. De Memorie van toelichting bepaalt hierover dat "*de wet van 25 december 2016 bevat reeds verscheidene bepalingen inzake gegevensbescherming zoals het aanstellen van een functionaris voor de gegevensbescherming, het voorzien van een manuele validatie of het verbod om gevoelige gegevens te verwerken. Bepaalde punten die reeds opgenomen zijn in de wet van 25 december 2016 dienen bijgevolg niet opgenomen te worden in de huidige wet*". De Commissie noteert ook dat het recht op informatie van de betrokkenen vastgesteld is in artikel 6 van de wet PNR die het volgende bepaalt: "*De vervoerders en de reisoperatoren informeren de betrokken personen dat hun gegevens worden doorgestuurd naar de PIE en achteraf kunnen worden verwerkt voor de in artikel 8 beoogde doelen*". Hetzelfde geldt voor het recht op toegang en het recht op verbetering.

247. Voor dit laatste, herinnert de Commissie er vooreerst aan dat het recht op toegang en verbetering van de betrokkenen tot/aan de hen betreffende PNR-gegevens principieel verloopt volgens een rechtstreekse toegang (art. 15 van de PNR wet). Een afwijkende procedure van onrechtstreekse toegang is uitsluitend voorzien voor de positieve overeenstemmingen[78] en de resultaten van de gerichte opzoekingen. De Commissie is er niet zeker van of dit Ontwerp deze binaire indeling en de mogelijkheid van rechtstreekse toegang voor de betrokkene naleeft aangezien het bepaalt dat de persoon het recht heeft om verbetering of verwijdering te vragen van zijn onjuiste gegevens bij de bevoegde toezichthoudende autoriteit (artikelen 175 en 177 van het Ontwerp). Daarom verzoekt zij de aanvrager om te preciseren dat er in het Ontwerp alleen sprake is van de onrechtstreekse toegang als bedoeld in artikel 15, §3, 2de lid van de wet PNR en om de procedure van de bestaande rechtstreekse toegang[79] toe te voegen aan de opsomming in de Memorie van Toelichting van de bepalingen van de wet PNR betreffende de bescherming van gegevens die niet in het Ontwerp moeten worden opgenomen.

248. De Commissie verwondert zich daarnaast over het generieke en het uit de context gehaalde karakter van sommige bepalingen terwijl er sprake is van zeer specifieke en afgebakende verwerkingen door de wet PNR en dat er overigens wordt verwezen naar de wet PNR voor de punten die niet in het Ontwerp zijn opgenomen.

249. Zo bepaalt artikel 176 van het Ontwerp in het kader van het recht op onrechtstreekse toegang van de betrokkene "*Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van de verwerkingen zoals hierboven bedoeld[80], is de toegang van de betrokkene tot zijn persoonsgegevens beperkt tot de toegang die expliciet voorzien is bij wet*". De Commissie vraagt zich af waarom hier niet gewoon wordt verwezen naar de wet PNR. Overigens nodigt zij de

[78] Uit de correlatie met de gegevensbanken van de bevoegde diensten of met de criteria bestemd om individuen uit te steken
[79] Bedoeld onder artikel 15, §3, 1ste lid van de wet PNR.
[80] het zou beter zijn te vermelden "de verwerkingen als bedoeld onder deze ondertitel".

aanvrager uit om gebruik te maken van de meer geschikte verwijzing "verwerkingen bedoeld in deze ondertitel" in plaats van naar de "verwerkingen zoals hierboven bedoeld".

250. Hetzelfde geldt voor artikel 177 van het Ontwerp. Dit artikel begint met de opsomming van de nadere regels voor de onrechtstreekse toegang en verificatie conform de verwerkingen die het Comité R verricht als volgt "*de betrokkene, die zijn identiteit bewijst, richt zich kosteloos tot de bevoegde toezichthoudende autoriteit. Deze voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht*", alvorens te besluiten: "*de nadere regels voor de uitoefening van dit beroep zijn bepaald in de wet*". De Commissie verzoekt de aanvrager - opdat het voor de betrokkene eenvoudig en transparant zou zijn - rechtstreeks te omschrijven dat de bevoegde toezichthoudende autoriteit het Comité R is (of anders te verwijzen naar artikel 97 van het Ontwerp) en de betrokken wet te vermelden, namelijk hetzij de organieke wet van de inlichtingendiensten hetzij de wet PNR, hetzij dit Ontwerp. De Commissie laat overigens opmerken dat artikel 177 van het Ontwerp verkeerdelijk verwijst naar de punten 2° en 3° van zijn artikel 175 terwijl dit artikel slechts twee punten bevat.

251. Ook artikel 178 dat het verbod eist van zuiver geautomatiseerde beslissingen, preciseert dat het verbod "*niet geldt indien het besluit zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet of wanneer het noodzakelijk is vanwege een zwaarwegend openbaar belang*". Zelfs al ziet de Commissie dat het bestaande kader - in overeenstemming met de richtlijn PNR - geen zuiver geautomatiseerde beslissingen toestaat aangezien het een validatie vereist van de PIE van de positieve overeenstemmingen uit de verrichte correlaties, wenst zij dat er wordt verwezen naar de wet PNR voor wat de eerste uitzondering betreft en dat de aanvrager op zijn minst de tweede uitzondering motiveert in de de Memorie van toelichting.

252. Hoofdstuk VI betreffende de verplichtingen van de verwerkingsverantwoordelijke bevat ook zeer algemene bepalingen over de verplichtingen van de verwerkingsverantwoordelijke zonder specificiteit met betrekking tot de verwerkingen van passagiersgegevens, buiten het register dat onderscheidt maakt tussen "de gegevensbanken van de PIE" en de "gegevensbanken die aan de PIE ter beschikking worden gesteld". Zo wordt in de verschillende bepalingen verwezen naar de "verwerkingsverantwoordelijke" terwijl de verwerkingsverantwoordelijke van de passagiersgegevens aangeduid wordt door de wet PNR als de leidende ambtenaar van de PIE. De Commissie vraagt zich af - nogmaals opdat het eenvoudig en transparant zou zijn voor de betrokkenen - waarom deze aangeduide verantwoordelijke niet als zodanig wordt vermeld. De Commissie begrijpt overigens niet waarom er sprake is van de gegevensbanken PIE terwijl de wet PNR terecht spreekt van één passagiersgegevensbank.

253. Over de internationale doorgifte van PNR-gegevens tot slot, merkt de Commissie op dat het beter zou zijn om nader te omschrijven dat de regels van de artikelen 184 en 185 de strikte regels van de wet PNR verder aanvullen, aangezien deze verwijst naar de artikelen 21 en 22 van de WVP die zal worden opgeheven.

CONCLUSIE van de Commissie over de ondertitel 5 van titel 3 van het ontwerp

254. De Commissie brengt een gunstig advies uit voor ondertitel 5 van titel 3 op voorwaarde dat rekening gehouden wordt met de volgende opmerkingen:

- de noodzaak te omschrijven dat het Ontwerp gaat over de onrechtstreekse toegang en verwijst naar de wet PNR voor wat de rechtstreekse toegang betreft als erkend door deze wet;
- het generieke en uit de context gehaalde karakter van sommige bepalingen;
- De noodzaak te omschrijven dat de regels betreffende de internationale doorgifte van PNR-gegevens de strikte regels van de wet PNR verder aanvullen.

7. TITEL 4: VERWERKING MET HET OOG OP ARCHIVERING IN HET ALGEMEEN BELANG, WETENSCHAPPELIJK OF HISTORISCH ONDERZOEK OF STATISTISCHE DOELEINDEN

Algemene opmerkingen

255. De AVG erkent het maatschappelijk belang van de wetenschap, net zoals Richtlijn 95/46/EG dit expliciet al deed. Overweging 113 van de Verordening stelt in dat verband dat, met betrekking tot verwerkingen "*met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden, rekening [dient] te worden gehouden met de gerechtvaardigde verwachting van de maatschappij dat er sprake is van kennisvermeerdering".* De AVG streeft naar een evenwicht vinden tussen de vrijheid van het onderzoek en de bescherming van de persoonlijke levenssfeer.

De vereiste van gepaste waarborgen

256. Klaar en duidelijk wijst artikel 89(1) AVG er op dat *"[de] verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met deze verordening voor de rechten en vrijheden van de betrokkene*". Onderzoekers, statistici en archivarissen moeten de Verordening naleven en net als elke andere verwerkingsverantwoordelijke de nodige waarborgen inbouwen. Artikel 89(1) AVG maant verwerkingsverantwoordelijken aan om bijzonder aandacht te schenken aan pseudonimisering en verdere verwerking van anoniem gemaakte gegevens – waar mogelijk.

Grenzen aan de beperkingen van de rechten van de betrokken persoon

257. Artikel 89(2)-(3) AVG laat de lidstaten toe afwijkingen van bepaalde rechten in te voeren in de context van de verwerking van persoonsgegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Deze wettelijke afwijkingen zijn toegelaten *"voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken*". De toevoeging "*behoudens de in lid 1 van dit artikel bedoelde voorwaarden en waarborgen*" herinnert opnieuw aan de principiële toepasselijkheid van de AVG.

258.

De Commissie leest in deze zinssnede geen toelating aan de wetgever om een omvattend afwijkend regime in te voeren, bij gebrek aan expliciete vermelding in artikel 89(1) AVG dat in het lidstatelijke recht kan worden voorzien in afwijkingen. Overweging 156 doet de Commissie evenmin besluiten tot het bestaan van een brede openingsclausule in weerwil van de tekst van artikel 89(1) AVG. De lidstaten moeten immers passende waarborgen bieden voor de verwerking van persoonsgegevens – in overeenstemming met de AVG – in alle regelgeving die zij uitvaardigen.

259. Titel 4 van het ontwerp voert een specifiek regime in voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden dat de grenzen van de openingsclausules gelaten door de AVG te buiten gaat. Zo verklaart artikel 190 van het ontwerp titel 4 van toepassing zelfs wanneer de verwerkingsverantwoordelijke zou beslissen om géén gebruik te maken van de afwijkingen toegelaten op grond van artikel 89(2) - (3) AVG.

260. Een sterk punt van de AVG is het opleggen van gelijke regels voor allerlei sectoren. Het kost de maatschappij dan ook minder om één gedeelde set spelregels te implementeren in de dagelijkse praktijk, dan een waaier aan verschillende spelregels die elk naargelang de omstandigheden gelden en dat binnen één en dezelfde organisatie voor activiteiten die verder nauw samenhangen (bijvoorbeeld beheren van het mobiliteitsbudget van individuele werknemers enerzijds en met statistische gegevens de mobiliteitsnoden van het bedrijf in kaart brengen anderzijds).

261. Titel 4 van het ontwerp doorkruist dit basisidee volledig. Activiteiten met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden overal ondernomen op grote of kleine schaal tot zeer kleine schaal. De impact van deze titel is dus niet beperkt tot universiteiten of welbepaalde innovatie-gerichte bedrijven, hetgeen de Memorie van toelichting ook erkent.[81]

262. Enkele voorbeelden van kleinschalige getroffen activiteiten:

- Een bedrijf nodigt een groep consumenten uit om te peilen of een nieuw ontwikkelde verpakking gebruikersvriendelijker is dan de huidige verpakking.
- Een vereniging schrijft voor het ledenblad een artikel over hun oprichting naar aanleiding van een jubileumjaar en interviewt de stichtende leden.
- Een heemkundige kring verzamelt getuigenissen van oudere inwoners over een lokale traditie.
- Voor een eindwerk in de menswetenschappen nemen studenten een enquête af bij ouders en buurtbewoners over mobiliteit om zich de beginselen van statistiek eigen te maken.
- Studenten geneeskunde, verpleegkunde en andere beroepen in de verzorging die in het kader van hun opleiding stageverslagen over de opgedane kennis opstellen.
- Een genealoog staat een familie bij in het opstellen van hun stamboom.

[81] "De verantwoordelijken voor verwerking met het oog op archivering, wetenschappelijk of historisch onderzoek of statistische doeleinden kunnen dus overheidsdepartementen zijn (de AD Statistiek bij de FOD Economie of het Algemeen Rijksarchief,…), private ondernemingen (farmaceuticabedrijven, universiteiten, private stichtingen, vzw's, centra voor private archieven...), enz."

Rekening houden met risico

263. Als uitgangspunt neemt het voorwerp blijkbaar de stelling in dat deze verwerkingen per definitie een hoog risico met zich meebrengen. Een uitgangspunt dat zonder meer haaks staat op de realiteit en niet onderbouwd wordt in de Memorie van toelichting. Het is opmerkelijk dat het ontwerp elke vorm van onderzoek strenger regelt dan verwerkingen gericht op direct marketing of deze verricht door werkgevers over hun werknemers. Met ander woorden, onderzoekers worden onderworpen aan een strenger regime dan degenen die naderhand de wetenschappelijke inzichten gebruiken voor het nemen van maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen.

De verplichte aanduiding van een DPO

264. De verplichting een functionaris voor gegevensbescherming aan te stellen - ongeacht het risicoprofiel van de verwerking - en vervolgens bij alle stappen van de verwerking in te schakelen getuigt van een verregaand formalisme. De steller van de tekst is zich daarvan trouwens bewust. Dit blijkt uit de suggestie in de Memorie van toelichting dat de functionaris voor gegevensbescherming generieke adviezen zou kunnen geven, voor meerdere onderzoeken met gelijkaardige doeleinden en methodologieën. Dit is een indicatie dat die tussenkomst verwordt tot niet meer dan een formaliteit.

Een gebrek aan aandacht voor de internationale context van wetenschappelijk onderzoek

265. Titel 4 van het ontwerp is voor een kennismaatschappij een belemmering – zonder duidelijke meerwaarde voor de bescherming van de rechten en vrijheden van betrokkenen. De gevolgen zullen zich niet alleen binnen de landsgrenzen maar ook daarbuiten laten voelen. De ontwerp-tekst is immers van toepassing van zodra een verwerker op het Belgische grondgebied een rol speelt in de verwerkingsactiviteiten (cf. artikel 4 §1 van het ontwerp). Hoe dit te rijmen valt met het vrije verkeer van persoonsgegevens in de Unie (artikel 1.3 AVG) is op zijn minst onduidelijk. De aanmaning in overweging 159 dat "de doelstelling van de Unie uit hoofde van artikel 179, lid 1, Verdrag betreffende de werking van de Europese Unie (hierna VWEU), te weten de totstandbrenging van een Europese onderzoeksruimte, in acht [moet] worden genomen"[82] heeft in het ontwerp geen

[82] Artikel 179, lid 1 en lid 2 VWEU luiden: "*1. De Unie heeft tot doel haar wetenschappelijke en technologische grondslagen te versterken door de totstandbrenging van een Europese onderzoeksruimte waarbinnen onderzoekers, wetenschappelijke kennis en technologieën vrij circuleren, tot de ontwikkeling van het concurrentievermogen van de Unie en van haar industrie bij te dragen en de onderzoeksactiviteiten te bevorderen die uit hoofde van andere hoofdstukken van de Verdragen nodig worden geacht.*
2. Te dien einde stimuleert zij in de gehele Unie de ondernemingen, met inbegrip van kleine en middelgrote ondernemingen, de onderzoekcentra en de universiteiten bij hun inspanningen op het gebied van hoogwaardig onderzoek en hoogwaardige technologische ontwikkeling; zij ondersteunt hun streven naar onderlinge samenwerking, waarbij het beleid er vooral op gericht is onderzoekers in staat te stellen vrijelijk samen te werken over de grenzen heen, en ondernemingen in staat te stellen de mogelijkheden van de interne markt ten volle te benutten, in het bijzonder door openstelling van de nationale overheidsopdrachten, vaststelling van

weerklank gevonden. Een groot aantal Belgische onderzoekers nemen deel aan projecten in Europese samenwerkingsverbanden. De Commissie vreest dat Belgische onderzoekers benadeeld zullen worden. Over intra-Europese grensoverschrijdende verwerkingen voor *wetenschappelijk of historisch onderzoek of statistische doeleinden* wordt met geen woord gerept in het ontwerp of in de Memorie van toelichting.

266. De Commissie is van oordeel dat de wetgever het territoriaal toepassingsgebied dient te heroverwegen. Minstens zou in titel 4 het oorsprongslandbeginsel[83] ingevoegd kunnen worden voor de afwijkingen die gelden voor verwerkingen in deze context, bijvoorbeeld in volgende bewoordingen:

> *"In afwijking van artikel 4, § 1 zijn van deze titel uitgezonderd de verwerkingen van persoonsgegevens die grensoverschrijdend zijn in de zin van artikel 4.23 AVG en die gebeuren in het kader van de activiteiten van een hoofdvestiging gevestigd buiten het Belgische grondgebied."*

***

267. Zoals hierna in de artikelsgewijze bespreking wordt toegelicht is de Commissie van oordeel dat titel 4 grotendeels in strijd is met de AVG. Wat de overige artikelen betreft, zijn een heel aantal overbodig of minstens onvoldoende gemotiveerd.

7.1. Hoofdstuk I - Algemene bepalingen

Artikel 188 Definities

268. Artikel 188 van het ontwerp definieert 12 begrippen voor gebruik in deze titel, waarbij legistieke vraagtekens geplaatst kunnen worden.

269. Zo krijgt het kernbegrip 'verwerkingsverantwoordelijke' een eigen invulling die enkel geldt voor Titel 4, hetgeen in de praktijk onvermijdelijk tot enorme begripsverwarring zal leiden en juridisch in strijd is met de definitie bepaald in artikel 4, 7° AVG. Deze definitie[84] is overbodig, daar uit artikel

---

gemeenschappelijke normen en opheffing van de wettelijke en fiscale belemmeringen welke die samenwerking in de weg staan."

[83] Naar het voorbeeld van hetgeen geregeld wordt in artikel 3 en 4 van de Richtlijn 2000/31/EG van het *Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt.* De geldende Oostenrijkse gegevensbeschermingswet huldigt binnen de EU reeds het oorsprongslandbeginsel (zie het tweede lid van § 3 'Räumlicher Anwendungsbereich', *Bundesgesetz über den Schutz personenbezogener Daten).*

[84] Art. 188, 5°: "verwerkingsverantwoordelijke": *verantwoordelijke voor de verwerking met het oog op archivering of onderzoek of statistische doeleinden*.

190 van het ontwerp al blijkt dat de bepalingen van titel 4 enkel gelden voor "*de verwerking met het oog op archivering of onderzoek of statistische doeleinden*".

270. Ook het begrip 'toestemming' krijgt een eigen invulling voor titel 4, namelijk "*toestemming in de zin van artikel 4, 11° en van overweging 33 van de Verordening*". Ook met deze definitie ligt begripsverwarring voor de hand en ook deze definitie is overbodig. Deze herdefiniëring is in strijd met artikel 4, 11° AVG en dient geschrapt te worden. Indien gewenst kan overweging 33 van de AVG in herinnering gebracht worden in de Memorie van toelichting bij titel 4.

271. Artikel 188, 3° definieert "*verwerking met het oog op onderzoek*" als "*verwerking van persoonsgegevens met het oog op wetenschappelijk of historisch onderzoek*". Deze definitie bespaart luttele woorden in de rest van de wettekst, maar de asymmetrie met de bepalingen van de AVG die telkens voluit "*wetenschappelijk of historisch onderzoek*" vermelden stelt de opmerkzaamheid van de lezer danig op de proef. Daar het ontwerp niet gericht is aan een kleine groep experten, maar aan iedereen die onderzoek verricht moet terminologische coherentie met de AVG bijzonder bewaakt worden.

272.

Wenst de wetgever de tekst in te korten, dan is het zinvoller één term te zoeken die lading "*wetenschappelijk of historisch onderzoek of statistische doeleinden*" geheel dekt. Geen van de bepalingen van het ontwerp maakt immers een onderscheid tussen "*verwerking met het oog op onderzoek*" (waaronder wetenschappelijk én historisch onderzoek valt) en "*verwerking met het oog op statistische doeleinden*". In hetgeen volgt worden voornoemde doelstellingen tezamen met de doelstelling 'archivering in het algemeen belang' aangeduid als 'kennisdoeleinden'.

273. Artikel 188, 1° definieert "*verwerking met het oog op archivering*" als "*verwerking van persoonsgegevens met het oog op archivering in het algemeen belang*". Ook deze definitie heeft tot gevolg dat de daaropvolgende bepalingen van het ontwerp de lezer op het verkeerde been zetten. De expert gegevensbeschermingsrecht uitgezonderd, zal alleen de meest opmerkzame lezer zich realiseren dat het ontwerp net als artikel 89 AVG alléén voor archivering *in het algemeen belang* een bijzondere regeling treft. De leesbaarheid die de Memorie van toelichting hiermee zegt na te streven wordt niet vergroot, daar het toepassingsgebied van de regels aan het oog onttrokken wordt. Coherentie met de AVG en duidelijkheid moeten ook hier zonder enige twijfel voorrang krijgen.

274. Artikel 188, 2° definieert verder "*archivering in het algemeen belang*" als "*statische archieven, gesorteerd omwille van hun permanente waarde en bewaard voor onbepaalde duur teneinde ze toegankelijk te maken in het algemeen belang*;". Deze definitie belicht één aspect van overweging 158 bij de AVG, namelijk de activiteiten van instanties belast met de opdracht om door hen geselecteerde gegevens van blijvende waarde voor het algemeen belang te beheren en

toegankelijk te maken. Een tweede en minstens even belangrijk aspect vermeld in overweging 158 wordt evenwel verzwegen in deze definitie: "*de lidstaten moeten tevens worden gemachtigd om te bepalen dat persoonsgegevens voor archiveringsdoeleinden verder mogen worden verwerkt*"

De Memorie van toelichting stelt:

> "*Voor documenten bestaan er twee opvattingen omtrent de term archief: volgens de eerste opvatting bestaat het archief uit alle administratieve documenten, volgens de tweede opvatting uit de documenten die de eindfase van hun administratieve levensduur bereikt hebben.*
>
> *Artikel 89 van de Verordening heeft enkel betrekking op de documenten in hun eindfase. Er is immers geen enkele reden om te voorzien in uitzonderingen op de rechten van de betrokkenen voor de documenten die nog in de fase van de administratieve levensduur verkeren*"

275. Het standpunt ingenomen in het ontwerp en in de memorie miskent de archiefreglementering die benadrukt dat archiefbeheer start van het ogenblik waarop de stukken gecreëerd worden én vindt verder geen steun in de AVG.[85] Door in overweging 158 precies te erkennen dat de verdere verwerking voor archiveringsdoeleinden ook door deze verwerkingsverantwoordelijken ingeroepen mag worden, vermijdt men dat na afloop van de operationele doeleinden alles vernietigd wordt, nog voor de bevoegde archiefinstantie tot selectie en inbewaringneming kon overgaan. Door ook in deze fase al een aantal uitzonderingen op de rechten van betrokkenen strikt ter vrijwaring van archieven in het algemeen belang te regelen, vermijdt men dat de geschiedenis probleemloos herschreven wordt zolang dit maar wordt doorgevoerd vóór de overdracht aan de archiefinstelling. De AVG bepaalt trouwens zelf expliciet een uitzondering op het recht op wissing van persoonsgegevens ter vrijwaring van archivering in het algemeen belang (art. 17(3)(d) AVG).

---

[85] Het K.B. van 18 augustus 2010 definieert in artikel 1, 2° archieven als "*alle documenten die ongeacht hun datum, materiële vorm, ontwikkelingsstadium of drager naar hun aard bestemd zijn om te berusten onder een overheid of een privaat persoon, een vennootschap of een vereniging van privaat recht die ze heeft ontvangen of opgemaakt uit hoofde van zijn of haar activiteiten, zijn of haar taken of tot vastlegging van zijn of haar rechten en plichten*;". Artikel 3, 2° van het Vlaams Archiefdecreet van 9 juli 2010 definieert archiefdocumenten als "*alle documenten die ongeacht hun datum, vorm, ontwikkelingsstadium of drager naar hun aard bestemd zijn om te berusten onder de zorgdrager die ze heeft ontvangen, verworven of opgemaakt uit hoofde van zijn activiteiten of taken of ter handhaving van zijn rechten;*" en vervolgt in artikel 5, §2 als volgt "*Elke zorgdrager brengt en bewaart de onder hem berustende archiefdocumenten in goede, geordende en toegankelijke staat gedurende de volledige levenscyclus, van de creatie, verwerving of ontvangst tot aan de eventuele vernietiging.*" Art. 1 van het Waals decreet van 6 december 2001 betreffende overheidsarchieven definieert archieven als "*alle documenten die ongeacht hun datum, vorm of drager opgemaakt of ontvangen uit hoofde van zijn activiteiten door enig archiefvormer bedoeld in artikel 2"*.

276. De Commissie is van oordeel dat de definitie van artikel 188, 2° van het ontwerp geschrapt moet worden. Overweging 158 van de AVG, waarnaar in de memorie verwezen wordt, licht voldoende toe wat bedoeld wordt met archivering in het algemeen belang.

277. Indien deze definitie niet geschrapt wordt, dient ze aangepast te worden om beide aspecten van archivering te omvatten. Bijkomend dient de term 'toegankelijk te maken' gehanteerd in de Nederlandse tekst vertaald te worden door 'donner accès' (zoals het geval is in overweging 158 AVG). De notie 'rendre publique' impliceert een veel verdergaande toegang tot archiefstukken dan de huidige archiefpraktijk toepast.

278. De in deze context gangbare term 'geselecteerd' dient ingevoegd te worden in plaats van 'gesorteerd' in de Nederlandse tekst.

Artikelen 189-190

Gepaste waarborgen

279. Artikel 189 van het ontwerp luidt: "*Dit hoofdstuk bepaalt de passende waarborgen die vereist zijn op grond van artikel 89 van de Verordening.*"

280. Artikel 190 van het ontwerp luidt: "*Dit hoofdstuk is van toepassing op de verwerking met het oog op archivering of onderzoek of statistische doeleinden, met uitzondering van de verwerkingen verricht door de diensten bedoeld in titel 3 van deze wet.*"

281. Beide artikelen spreken over "dit hoofdstuk", terwijl ongetwijfeld bedoeld wordt "deze titel".

282. De Commissie verwijst naar de opmerkingen gemaakt hierboven in nrs. 256 - 264 en is van oordeel dat beide bepalingen geschrapt moeten worden wegens in strijd met de AVG.

7.2. Hoofdstuk II - Algemene waarborgen

Artikel 191

Functionaris voor de gegevensbescherming

283. Artikel 191 van het ontwerp verplicht elke verwerkingsverantwoordelijke die zich waagt aan een verwerking voor kennisdoeleinden een functionaris voor gegevensbescherming aan te stellen. Zoals hierboven toegelicht geldt deze plicht ongeacht hoe bescheiden de verwerking, ongeacht het risico dat ermee gepaard gaat en ongeacht of de onderzoeker uitsluitend gepseudonimiseerde gegevens in handen krijgt. Enige verantwoording voor het uitbreiden van de plicht tot aanstellen van een functionaris voor gegevensbescherming ontbreekt in de Memorie van toelichting. Ten onrechte stelt

de Memorie van toelichting dat voor het merendeel van verwerkingen voor kennisdoeleinden de plicht tot aanstelling van een functionaris voor gegevensbescherming toch al zou gelden op grond van artikel 37 AVG. De hierboven gegeven voorbeelden illustreren dit (zie nr. 262).

284. De Commissie is van oordeel dat deze bepaling overmatig is en geschrapt moet worden. Vroeg of laat gaat elke verwerkingsverantwoordelijke over tot een verwerking voor kennisdoeleinden, zodat virtueel elke verwerkingsverantwoordelijke ook een functionaris voor gegevensbescherming zou moeten aanstellen. Gelet op het ruim omschreven territoriaal toepassingsgebied van het ontwerp, stelt de problematiek zich ook voor verwerkingen voor kennisdoeleinden aangestuurd vanuit een andere EU-lidstaat (zie nr. 265 e.v.).

285. Als er al nood zou zijn aan het uitbreiden van de plicht tot aanstellen van een functionaris voor gegevensbescherming, dan mag dit enkel opgelegd worden voor verwerkingen die een bijzonder risico met zich meebrengen. Zo'n bijzonder risico kan bestaan bij bepaalde – maar niet noodzakelijk alle - verwerkingen met het oog op pseudonimisering of anonimisering van gegevens (zie de kanttekening gemaakt in nr. 299) – in het bijzonder indien er sprake zal zijn van publicatie van de geanonimiseerde of gepseudonimiseerde gegevens samen met de resultaten van het onderzoek in kwestie. Evenwel is de Commissie van oordeel dat de gegevensbeschermingseffectbeoordeling een geschikter instrument is om deze risico's te ondervangen in functie van de aard, de omvang, de context en de doeleinden.

Artikel 192

Register van de verwerkingsactiviteiten

286. Artikel 192 van het ontwerp verplicht elke verwerkingsverantwoordelijke die een verwerking voor kennisdoeleinden uitvoert om een register van de verwerkingsactiviteiten bij te houden. De beperkte vrijstelling vervat in artikel 30(5) AVG – incidentele verwerkingen verricht door kleinschalige verwerkingsverantwoordelijken - wordt bijgevolg geschrapt binnen de context van titel 4. Enige verantwoording voor deze schrapping ontbreekt in de Memorie van toelichting, nochtans mogen de gevolgen hiervan op het terrein niet onderschat worden.

287. Een redelijke veronderstelling is dat vrijwel elke verwerkingsverantwoordelijke vroeg of laat een verwerking voor kennisdoeleinden onderneemt. De draagwijdte van artikel 30(5) AVG is op zich al moeilijk uit te leggen aan alle kleine entiteiten die er menen gebruik van te kunnen maken. Artikel 192 § 1 van het ontwerp voegt hier – zonder duidelijke reden – de onnodige complicatie aan toe dat de vrijstelling voor incidentele verwerkingen soms vervalt én bovendien aangevuld wordt met bijkomende verplichtingen (zie verder). Dat deze verplichting door de GBA in de praktijk handhaafbaar zou zijn, is vrijwel ondenkbaar.

Transparantie

288. Artikel 192 § 2 van het ontwerp luidt als volgt: *"In het kader van een verdere verwerking van verdere persoonsgegevens maakt de verwerkingsverantwoordelijke de naam van de verwerkingsverantwoordelijke, de naam en de contactgegevens van de functionaris voor gegevensbescherming en het doel van de verwerking openbaar."*

289. De Memorie van toelichting stelt dat bijkomende transparantie nodig is als "*een passende maatregel als tegengewicht voor de beperking van de rechten van de betrokkenen en omdat de voorkeur wordt gegeven aan verdere verwerking*" en verwijst verderop naar de mogelijkheden die artikel 89 AVG aan de wetgever geeft. (Over de draagwijdte van de term 'verdere verwerking' in het ontwerp, zie nr. 344.)

290. Transparantieverplichtingen worden geregeld in artikelen 13 en 14 AVG:

- Artikel 13 AVG regelt de transparantieverplichting in die gevallen waarin een verwerkingsverantwoordelijke persoonsgegevens rechtstreeks bij de betrokkene heeft ingezameld en vervolgens verder wil verwerken voor een nieuwe doelstelling. Art. 13(3) AVG bepaalt dat "*de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2*" verstrekt. Artikel 13 AVG bevat geen uitzonderingen voor verwerkingen voor kennisdoeleinden.

- Artikel 14 AVG regelt de transparantieverplichting in die gevallen waarin een verwerkingsverantwoordelijke persoonsgegevens niet rechtstreeks bij de betrokkene heeft ingezameld en vervolgens verder wil verwerken voor een nieuwe doelstelling. In beginsel moet de verwerkingsverantwoordelijke de betrokkene informeren vooraleer over te gaan tot verdere verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen (art. 14(4) AVG). Artikel 14(5)(b) AVG bevat een beperking van de informatieverplichting – onder voorwaarden – voor verwerkingen voor kennisdoeleinden in het bijzonder. In dit laatste geval moet de verwerkingsverantwoordelijke passende maatregelen nemen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie.

291. Het ontwerp legt met artikel 192 § 2 de lat globaal genomen lager voor transparantie dan artikelen 13 en 14 AVG. De verwerkingsverantwoordelijke die enkel de publiciteitsplicht vervat in artikel 192 §2 van het ontwerp naleeft komt bedrogen uit. Daar artikel 89(2)-(3) AVG de wetgever niet toelaat een beperking in te voeren op de daarin vervatte informatieverplichtingen naar

betrokkenen toe[86], kan er alvast geen sprake zijn van een 'tegengewicht' voor de beperking van deze rechten.

292. Zelfs indien de plicht van artikel 192 § 2 van het ontwerp gelezen moet worden als een aanvullende plicht die geldt "*onverminderd artikelen 13 en 14 AVG*" stellen zich nog ernstige vragen over de verenigbaarheid met de AVG.
De Memorie van toelichting omschrijft deze bepaling als een gedeeltelijke plicht tot publicatie van het register van de verwerkingsactiviteiten. Artikel 30 AVG bevat geen marge voor nationale afwijkingen.
Wat de verplichting tot bekendmaking van de naam van de functionaris voor gegevensbescherming betreft, gaat het ontwerp in tegen artikel 37(7) AVG dat enkel de bekendmaking van contactgegevens oplegt.

293. De Memorie van toelichting geeft als verantwoording enkel het volgende mee: "*Niettemin hebben de lidstaten op grond van artikel 89 van de Verordening de mogelijkheid om verder te gaan dan de passende waarborgen, en dus het register openbaar te maken.*" Hiermee toont de wetgever in het geheel niet aan dat de grenzen voor nationale afwijkingen gerespecteerd worden.

294. De Commissie meent dat de publicatie van bepaalde informatie een passende waarborg is in die gevallen waar het rechtstreeks informeren van betrokkenen uitblijft, waar artikel 14(5)(d) AVG dit toelaat. Hieruit kan evenwel niet zomaar afgeleid worden dat publicatie van bepaalde informatie moet opgelegd worden bij élke 'verdere verwerking' voor kennisdoeleinden. De maatschappelijke kosten voor de toepassing en de handhaving kunnen niet anders dan zeer hoog ingeschat worden, terwijl er nauwelijks baten te verwachten zijn boven de regeling van de AVG. Het ontwerp verwacht van elke verwerkingsverantwoordelijke om zorgvuldig te bewaken wanneer er een verdere verwerking voor kennisdoeleinden – hoe bescheiden ook – voorgenomen wordt en te investeren in een interne procedure die ervoor zorgt dat een publicatie conform artikel 192 § 2 van het ontwerp gebeurt. De gevraagde inspanning weegt het zwaarst door op kleine entiteiten, zoals bijvoorbeeld innovatieve KMO's of individuele onderzoekers, daar zij in de regel geen gespecialiseerde juridische hulp onmiddellijk ter beschikking hebben.

295. Ervaring met het openbaar register van verwerkingen leert dat algemene publicatieverplichtingen een eerder bescheiden rol spelen als waarborg van transparantie naar individuele betrokkenen toe.

296. De Commissie is van oordeel dat artikel 192 in zijn geheel geschrapt dient te worden. De verplichting tot het houden van een register zoals bepaald in artikel 30 AVG volstaat ook voor de

[86] Hoewel artikel 14(5)(b) AVG verwijst naar "*de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen*", leest de Commissie hierin geen impliciete toelating aan de wetgever om een afwijkende regeling in te voeren, bij gebrek aan vermelding in artikel 89(1) AVG dat "*in het lidstatelijke recht [kan] worden voorzien in afwijkingen*".

context van titel 4, daarnaast regelen artikel 13 en 14 AVG reeds een hoger transparantieniveau ten aanzien van de betrokkene ingeval van hergebruik van persoonsgegevens (zowel intern als extern).

297. Indien de wetgever vasthoudt aan artikel 192 § 2 van het ontwerp, dan moeten de bedoeling en draagwijdte van de bepaling verduidelijkt worden én minstens ingeperkt tot verwerking door een andere verwerkingsverantwoordelijke dan degene die instond voor de oorspronkelijke verwerking. Overigens stelt de Commissie vast dat de Nederlandstalige en de Franstalige versie niet overeenstemmen.

7.3. Hoofdstuk III - Minimale gegevensverwerking

Artikel 193

298. Artikel 193 van het ontwerp herneemt het beginsel "minimale gegevensverwerking" vervat in artikel 5(1)(c) AVG en artikel 89(1) AVG en giet het samen met artikel 195 van het ontwerp in een strakker keurslijf (zie verder nrs. 309-313).

299. Het koninklijk besluit van 13 februari 2001 bevat in de artikelen 3-5 inderdaad een cascadesysteem voor latere verwerkingen voor historische, statistische of wetenschappelijke doeleinden (bij voorkeur anonieme gegevens, zoniet gecodeerde gegevens, zoniet niet-gecodeerde gegevens). Artikel 193 van het ontwerp heeft als doel de verwerkingsverantwoordelijken "*aan te sporen om de verschillende mogelijkheden die hij heeft om zijn doeleinden te bereiken te onderzoeken om zijn doeleinden te bereiken*" (aldus de Memorie van toelichting). Voor zover deze bepaling louter gelezen moet worden als een artikel van pedagogische aard, heeft de Commissie geen principieel bezwaar tegen de herneming van de regeling uit artikelen 3-5 van het K.B. Volgende kanttekening moet hierbij wel gemaakt worden: persoonsgegevens deugdelijk anonimiseren zodat heridentificering praktisch wordt uitgesloten, blijkt zéér moeilijk te zijn.[87] Ook deugdelijk pseudonimiseren is geen evidentie. De meerwaarde die deze bepaling kan bieden voor de bescherming van betrokkenen is op zijn minst relatief te noemen.

300. De Commissie heeft zich in het verleden – behoudens marginale toetsing – niet geroepen gevoeld zich systematisch in te mengen in de wijze waarop onderzoek gevoerd werd. De Commissie beveelt haar opvolger aan deze lijn aan te houden, zeker nu het ontwerp zowel verdere verwerking als oorspronkelijke verwerking voor kennisdoeleinden omvat. Dit om een ontradingseffect op onderzoek dat - geheel volgens de regels van de kunst – bouwt op rechtstreeks contact met betrokkenen te vermijden.

[87] Zie bv. Paul Ohm, "*Broken Promises of Privacy: Responding to the Suprising Failure of Anonymization*", UCLA Law Review, 2010, p. 1701 e.v.

301. De Commissie is van oordeel dat artikel 193 van het ontwerp minstens dient beperkt te worden tot hergebruik van persoonsgegevens. Zie ook verder – afdeling 3 'Anonimisering of pseudonimisering van de gegevens verwerkt met het oog op onderzoek of statistische doeleinden' (zie nr. 358 e.v.).

Artikel 194

302. Artikel 194 van het ontwerp luidt als volgt:

"*Eerder dan de gegevens te verzamelen bij de betrokkene hanteert de verwerkingsverantwoordelijke met het oog op onderzoek of statistische doeleinden bij voorkeur de verdere verwerking.*

Wanneer het niet mogelijk is om met een verdere verwerking het onderzoeksdoel of het statistische doel te bereiken, gaat hij over tot een nieuwe verzameling van gegevens bij de betrokkenen."

303. Uit de Memorie van toelichting blijkt dat de voorkeur voor hergebruik algemeen moet gelden, ook wanneer er sprake is van een mededeling van persoonsgegevens door "*de verantwoordelijke voor de oorspronkelijke verwerking*" aan de "*verantwoordelijke voor de verdere verwerking*". De Commissie licht verder bij Afdeling 2 'Gegevensverzameling via verdere verwerking van gegevens' toe waarom de term 'verdere verwerking' ongeschikt is en hanteert hierna de term 'hergebruik' (zie nr. 344).

304. De invoering van een algemene geldende voorkeur voor hergebruik is een inperking van de vrijheid om onderzoek te doen. Historici die hedendaagse geschiedenis beschrijven en getuigen wensen te interviewen zullen eerst afdoende moeten verantwoorden dat het bestuderen van bestaande geschreven bronnen het onmogelijk maakt hun onderzoeksdoel te bereiken. Wetenschappers uit allerlei humane disciplines zullen de keuze voor kwalitatieve onderzoek in rechtstreeks contact met betrokkenen moeten verdedigen, net als klinische studies in het medisch domein.

305. Deze inperking is niet terug te voeren op één van de beginselen van de AVG. Rechtstreeks een aantal vragen stellen aan de betrokkene voor een onderzoek zal in heel wat omstandigheden net beter stroken met de beginselen van transparantie, doelbinding en proportionaliteit (minimale gegevensverwerking) dan dezelfde informatie inzamelen uit andere bronnen met het oog op hergebruik.

De Memorie van toelichting erkent uitdrukkelijk dat het ontwerp een gebrek aan transparantie veroorzaakt, maar voert aan dat het dit gebrek compenseert via artikel 192 §2 en artikel 202 en volgende van het ontwerp. De deugdelijkheid van deze compensaties wordt elders besproken (zie hiervoor en hierna).

306. De verwijzingen in de Memorie van toelichting naar artikel 5(1)(b), artikel 89(1) AVG, overweging 162 en advies nr. 11/2003 van de Commissie overtuigen niet als verantwoording. Artikel 5(1)(b) verduidelijkt dat het doelbindingsbeginsel verdere verwerking voor kennisdoeleinden niet in de weg staat, het poneert evenwel geen algemene voorkeur voor hergebruik.
Artikel 89(1) AVG herinnert onderzoekers aan het beginsel van minimale gegevensverwerking als volgt: "*Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt.*" Uit deze zin kan geen algemene voorrang afgeleid worden voor verdere verwerking of hergebruik daar waar anonieme gegevens niet volstaan.
Overweging 162 stelt inderdaad "*dat statistische resultaten ook voor andere doeleinden [kunnen] worden gebruikt, onder meer voor wetenschappelijke onderzoeksdoeleinden*", maar er kan geen voorkeur voor hergebruik in gelezen worden.[88]

307. Advies nr. 11/2003 van de Commissie[89] zegt uitdrukkelijk dat een voorkeur voor hergebruik geen operationele vertaling is van het proportionaliteitsprincipe, maar erkent inderdaad de waarde ervan binnen de specifieke context van de wet van 4 juli 1962 betreffende de openbare statistiek.

308. De Commissie acht artikel 194 van het ontwerp in strijd met artikel 6(4) AVG dat de verdere verwerking voor andere doelstellingen regelt en behoudens toepassing van artikel 23 AVG geen ruimte laat voor nationale afwijkingen. Verder strookt dit artikel ook niet met artikel 5 AVG, met name de beginselen transparantie, doelbinding en proportionaliteit (minimale gegevensverwerking) en de verantwoordingsplicht.

Artikel 195

309. Artikel 195 verplicht de verwerkingsverantwoordelijke in bijlage bij diens register van de verwerkingsactiviteiten bij te houden welke toepassing hij maakt van artikelen 193 en 194 van het ontwerp. Daarenboven moet de verwerkingsverantwoordelijke steeds het advies inwinnen van zijn functionaris voor gegevensbescherming en dit eveneens toevoegen aan het register.

310. De Commissie stelt vast dat waar de Europese regelgever komaf maakt met tal van formalistische bepalingen, de Belgische wetgever tegen deze tendens ingaat in de context van titel 4. Nochtans is er geen reden om aan te nemen dat meer formalisme ook leidt tot een betere naleving van de gegevensbeschermingsregels.

311. De AVG huldigt de verantwoordingsplicht (artikel 5(2) AVG) dat de verwerkingsverantwoordelijke opdraagt de AVG na te leven en dit te kunnen aantonen. In het licht

[88] "… Onder statistische doeleinden wordt verstaan het verzamelen en verwerken van persoonsgegevens die nodig zijn voor statistische onderzoeken en voor het produceren van statistische resultaten. …"
[89] Advies nr. 11/2003 van de Commissie van 27 februari 2003 *betreffende een voorontwerp van wet tot wijziging van de wet van 4 juli 1962 betreffende de openbare statistiek.*

hiervan is het dan ook zonder meer aan te bevelen dat de verwerkingsverantwoordelijke documenteert welke keuzes hij maakt inzake de verwerking van persoonsgegevens. De flexibiliteit waarmee artikel 24(1) AVG dit invult – rekening houdend met de aard, de omvang, de context en het doel van de verwerking en de eraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen, ontbreekt in het ontwerp.

312. Zoals eerder toegelicht is dit strikte regime virtueel op elke verwerkingsverantwoordelijke van toepassing en kan de maatschappelijke kost ervan – niet in het minst voor KMO's en individuele onderzoekers – enkel als zeer hoog ingeschat worden.
De Commissie herhaalt dat het inschakelen van een functionaris voor gegevensbescherming voor élke verwerking voor kennisdoeleinden manifest overmatig is (zie nr. 283-285).

313. De Commissie ziet geen meerwaarde in artikel 195 van het ontwerp en is van oordeel dat het geschrapt moet worden wegens in strijd met artikel 24 AVG.

Artikel 196

314. Artikel 196 van het ontwerp luidt als volgt:

"Voorafgaand aan de verzameling verantwoordt de verantwoordelijke voor de verwerking met het oog op archivering het algemeen belang van de bewaarde archieven.

De verantwoording wordt bij het register van de verwerkingsactiviteiten gevoegd."

315. Uit de Memorie van toelichting blijkt dat ook deze bepaling enkel geschreven is met de activiteiten van publieke archiefinstanties in gedachten. De volgorde van de acties – verantwoording van het algemeen belang voorafgaand aan de verzameling van archieven – wijst hier eveneens op. De Commissie verwijst naar de hierboven gemaakte opmerkingen hierover (zie nr. 274).

316. In het licht van de verantwoordingsplicht (artikel 5(2) AVG) is het zonder meer aan te bevelen dat de verwerkingsverantwoordelijke de verwerking voor archiefdoeleinden in het algemeen belang goed documenteert. Het formalisme van artikel 196 doorkruist de flexibele regeling van artikel 24(1) AVG.

317. De Commissie ziet geen meerwaarde in artikel 196 van het ontwerp en is van oordeel dat het geschrapt moet worden wegens in strijd met artikel 24 AVG.

7.4. Hoofdstuk IV - Gegevensverzameling

7.4.1. Afdeling 1 - Gegevensverzameling bij de betrokkene

Artikel 197

Rechtstreekse gegevensverzameling

318. Artikel 197 van het ontwerp bepaalt dat de verwerkingsverantwoordelijke die gegevens verzamelt bij de betrokkene hem hiervan op de hoogte stelt – een verplichting die reeds volgt uit artikel 13 AVG.

319. Betreft het een inzameling van gevoelige gegevens dan moet de verwerkingsverantwoordelijke in beginsel verplicht de toestemming van de betrokkene verkrijgen. De vereiste van toestemming is volgens de Memorie van toelichting een passende en specifieke maatregel bij wet te treffen ter bescherming van de grondrechten en de belangen van de betrokkene zoals vereist door artikel 9.2.j AVG.

320. Evenwel komt de vereiste van toestemming neer op het schrappen van artikel 9.2.j AVG als uitzonderingsgrond die de verwerking van gevoelige gegevens toelaat. Geen soelaas bieden de uitzonderingen op de toestemmingsvereiste vervat in artikel 197, 2e lid van het ontwerp voor de gevallen waarin:

1. de gegevens door de betrokkene zelf openbaar zijn gemaakt; of

2. de verzameling door een wet of een openbaar belang verplicht is geworden; of

3. de verzameling wordt verricht in het vitaal belang van de betrokkene.

321. De oplettende lezer stelt vast dat deze opsomming deels - maar allerminst volledig - bewoordingen herneemt van artikel 9.2 AVG, zonder hiermee een uitweg te vinden uit de kringredenering gecreëerd door artikel 197 van het ontwerp. Het probleem wordt treffend geïllustreerd door hetgeen de Memorie van toelichting stelt over de gevolgen te geven aan de intrekking van de toestemming in deze context. Omdat de toestemming hier geldt als waarborg en niet als rechtsgrondslag, heeft intrekking geen gevolgen:

"Wanneer de persoon zijn toestemming intrekt behoudt de verwerking met het oog op archivering, onderzoek en statistische doeleinden zijn rechtsgrond : de wet aangenomen krachtens artikel 9.2 j) van de Verordening.

In dit geval bepaalt artikel 17.3 .d) van de Verordening uitdrukkelijk dat het recht op vergetelheid niet van toepassing is "voor zover die verwerking noodzakelijk is (…) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, voor zover het in lid 1 bedoelde recht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen".

322. Hoe verwerkingsverantwoordelijken de draagwijdte van deze toestemmings-als-waarborg op een begrijpelijke manier zullen kunnen uitleggen aan betrokkenen is een groot vraagteken. Ook handhaving van deze verplichting door de GBA zal geen sinecure zijn.

323. Het ontwerp beperkt de gevallen opgesomd in artikel 9.2 AVG waarin de verwerking van gevoelige gegevens is toegelaten en gaat hiermee verder dan de openingsclausule opgenomen in artikel 9.4 AVG die toelaat dat lidstaten "*bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren*" en niet voor andere types gevoelige gegevens.

324. De Commissie is van oordeel dat artikel 197 van het ontwerp minstens strijdig is met artikel 9 AVG, en voor het overige onnodig artikel 13 AVG herneemt, en geschrapt moet worden.

Artikel 198

325. Artikel 198 van het ontwerp verplicht tot enkele aanvullingen op artikel 13 AVG.

326. Wat betreft de kennisgeving van "*het algemene belang van de verzamelde gegevens, voor de verwerkingen met het oog op archivering*" herneemt de Commissie de opmerking dat de rechtstreekse inzameling van persoonsgegevens slechts één geval is waarin archivering in het algemeen belang aan de orde is (zie nr. 274).

327. Wat betreft een kennisgeving van de nadere regels inzake de uitoefening van de rechten van de betrokkene, volgt deze verplichting reeds uit artikel 12.2 AVG.

328. De Commissie raakt elders in het advies de overige elementen van de kennisgeving aan:

- de anonimisering of eventuele pseudonimisering van de gegevens na verzameling ervan, voor de verwerking met het oog op onderzoek of statistische doeleinden (nr. 299-301);
- de beperkingen inzake de verspreiding en de mededeling van de gegevens (nr. 377-388);
- de beperkingen van de rechten van de betrokkene (nr. 332 e.v., nr. 355 e.v., nr. 373 e.v.);

329. De Commissie is van oordeel dat dit artikel naar aanleiding van de opmerkingen waarnaar hierboven verwezen dient geschrapt of minstens herschreven te worden.

Artikelen 199 en 200

330. Het ontwerp verplicht de verwerkingsverantwoordelijke ertoe zijn kennisgeving ter advies voor te leggen aan de functionaris voor gegevensbescherming, en vervolgens de kennisgeving, het advies én eventuele motivering voor het niet volgen van dat advies in bijlage bij het register van de verwerkingsactiviteiten te voegen.

331. Deze bepaling is in grote mate overlappend met artikel 195 van het ontwerp. De Commissie herneemt haar opmerkingen bij die bepalingen (zie nrs. 309-313). De Commissie ziet geen

meerwaarde in de artikelen 199 en 200 van het ontwerp en is van oordeel dat ze geschrapt moeten worden wegens in strijd is met artikel 24 AVG.

Artikel 201

332. Artikel 201, §1 van het ontwerp maakt toepassing van artikel 89(2)-(3) AVG en bepaalt dat de artikelen 15 en 16 AVG niet van toepassing zijn op verwerkingen voor kennisdoeleinden in twee gevallen.

333. Het eerste geval is wanneer "*de verwerkingsverantwoordelijke motiveert dat de uitoefening van die rechten de verwezenlijking van die archiverings-, onderzoeks- of statistische doeleinden onmogelijk dreigt te maken of ernstig te belemmeren*". In dat geval moet *"[de] verantwoording, het advies van de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke en de verantwoording van de verwerkingsverantwoordelijke wanneer hij het advies van de functionaris voor gegevensbescherming niet volgt, worden [gevoegd] bij het register van de verwerkingsactiviteiten*". Deze formalistische insteek is in grote mate overlappend met de artikelen 195, 199 en 200 van het ontwerp, de Commissie herneemt haar opmerkingen bij die bepalingen en meent dat de tweede zin geschrapt moet worden wegens in strijd met artikel 24 AVG.

334. Het tweede geval is wanneer er een wettelijke basis te vinden is voor de verwerking in Europese regelgeving, een wet, decreet of ordonnantie die:

- *de verwerkingsverantwoordelijke een mandaat geeft om gegevens te verwerken met het oog op archivering, onderzoek of statische doeleinden, en*
- *regels inzake veiligheid en vertrouwelijkheid oplegt aan de personen die werken onder de verantwoordelijkheid of voor rekening van de verwerkingsverantwoordelijke, en*
- *het hergebruik van de gegevens voor andere doeleinden verbiedt.*

335. Met opzet is in dit tweede geval geen sprake van een afwijking "voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren" (art. 89(2)-(3) AVG), immers het "wetsontwerp gaat ervan uit dat de uitoefening van die rechten op inzage en op rectificatie de verwerking met het oog op archivering of statistische doeleinden ernstig belemmert" aldus de Memorie van toelichting. Deze bepaling is om deze reden alleen al problematisch.

336. Veiligheid en vertrouwelijkheid worden reeds opgelegd door artikel 32.4 AVG dat expliciet verwijst naar "*iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker*". In artikelen 28.3.b en 29 AVG komt dit eveneens aan bod. Het tweede verplicht element is overbodig.
Overigens voldoet de Archiefwet van 24 juni 1955 – in de Memorie van toelichting vermeld als voorbeeld – niet aan deze vereiste.

337. Hoogst opmerkelijk is het laatste element – het verbod op hergebruik van de gegevens voor andere doeleinden. De stelling in de Memorie van toelichting dat de persoonsgegevens kunnen "*hergebruikt worden door andere verwerkingsverantwoordelijken met het oog op historisch of sociologisch onderzoek of statistische doeleinden*" – verwijzend naar overweging 158 – stemt niet overeen met de ontwerptekst.
De Archiefwet van 24 juni 1955 vervult deze voorwaarde niet. Volgens de definitie van 'archivering in het algemeen belang' opgenomen in het ontwerp is de bedoeling hiervan precies om bronnen toegankelijk te maken in het algemeen belang, hetgeen minstens een hergebruik laat veronderstellen voor andere doeleinden dan deze die het Rijksarchief als wettelijke opdracht heeft. Ook de wet van 4 juli 1962 betreffende de openbare statistiek organiseert zelf hergebruik voor andere doeleinden dan deze die het Nationaal Instituut voor de Statistiek als wettelijke opdracht heeft. Minstens zal de onderzoeker die gegevens verkrijgt uit het Rijksarchief of vanwege het Nationaal Instituut voor de Statistiek twijfelen over de toepassing van de uitzondering.

338. Artikel 201, § 2 bepaalt: "*De artikelen 17, 18 en 21 van de Verordening zijn niet van toepassing op verwerkingen met het oog op onderzoek of statistische doeleinden die vervat zijn in de kennisgeving opgelegd in artikel 14 van de Verordening*."

339. Artikel 201, § 3 bepaalt: "*De artikelen 17, 18, 20 en 21 van de Verordening zijn niet van toepassing op verwerkingen met het oog op archivering die vervat zijn in de kennisgeving betreffende de gegevensverzameling, opgelegd in artikel 14 van de Verordening.*"

340. De vermelding van een afwijking op artikel 17 AVG is in strijd met de AVG daar dit artikel niet vermeld wordt in de openingsclausules van artikel 89(2)-(3) AVG. Artikel 17 AVG bevat reeds een uitzondering voor kennisdoeleinden (in 17.3.d AVG) zodat een afwijking niet nodig is.

341. Artikel 201, §2-3 van het ontwerp staat in de afdeling gewijd aan 'gegevensverzameling bij de betrokkene', maar is van toepassing op verwerkingen "*die vervat zijn in de kennisgeving betreffende de gegevensverzameling opgelegd in artikel 14 van de Verordening"*, dat geldt in geval van onrechtstreekse verzameling. De Memorie van Toelichting zwijgt over deze zinssnede zodat de Commissie in het duister tast over de achterliggende bedoeling.

342. Het ontwerp schrapt de rechten van de betrokkene binnen deze context, hetgeen verder gaat dan een afwijking invoeren "*voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren*" (art. 89(2)-(3) AVG).

343. De Commissie is van oordeel dat artikel 201 van het ontwerp in strijd is met de AVG en herwerkt dient te worden. De Commissie beveelt de ontwerp-steller aan aansluiting te zoeken bij de regeling

die reeds uitgevaardigd werd in andere Europese lidstaten, bijvoorbeeld de Duitse of Oostenrijkse regeling.[90]

7.4.2. Afdeling 2 - Gegevensverzameling via verdere verwerking van gegevens

344. Het opschrift van afdeling 2 'Gegevensverzameling via verdere verwerking van gegevens' is intern contradictorisch. De term 'verdere verwerking'[91] moet in het licht van de AVG als een verwijzing naar artikel 6.4 AVG begrepen worden – dat slaat op verwerking voor een ander doel door één en dezelfde verwerkingsverantwoordelijke. De Memorie van toelichting gaat daarentegen uit van onderscheiden verwerkingsverantwoordelijken: een "*verantwoordelijke voor de verdere verwerking*" die met "*de verantwoordelijke voor de oorspronkelijke verwerking*" verplicht een overeenkomst moet afsluiten. In termen van de AVG is er in dit geval sprake van onrechtstreekse inzameling (hergebruik) van persoonsgegevens zoals bedoeld in artikel 14 AVG.

345. Gelet op het hoogst problematisch karakter van het door artikel 194 van het ontwerp ingevoerd beginsel van voorkeur voor hergebruik van persoonsgegevens, is de Commissie van oordeel dat Afdeling 2 geschrapt dient te worden.

Artikel 202

346. Artikel 202 van het ontwerp verplicht tot het afsluiten van een overeenkomst tussen de "verantwoordelijke voor de oorspronkelijke verwerking" en de hergebruiker ("verantwoordelijke voor de verdere verwerking").

347. De Memorie van toelichting motiveert niet welke bepaling van de AVG toelaat dergelijke verplichting op te leggen. De Commissie meent dat dit artikel overbodig is en geschrapt moet worden.

Artikel 203

348. Artikel 203 van het ontwerp voert het begrip 'openbare verwerking van gegevens' ten tonele om een vrijstelling van de verplichting tot afsluiten van een overeenkomst te kunnen verlenen. De Memorie van toelichting blijft vaag over de invulling van dit begrip en omschrijft het enerzijds als elke "verwerking zonder beperking tot toegang, noch voor de betrokken personen, noch voor derden" en vult anderzijds aan met de semi-publieke plaatsen beschreven in een arrest van het Hof van Cassatie van 28 maart 2017.

---

[90] Zie § 26 en § 27 van de Duitse Datenschutz-Anpassungs- und –Umsetzungsgesetz, gebpubliceerd in het BGB I NR. 44/2017; § 7 van de Oostenrijkse *Bundesgesetz über den Schutz personenbezogener Daten* zoals aangepast door de *Datenschutz-Anpassungsgesetz 2018*, gepubliceerd in het BGBl. I Nr. 120/2017.

[91] Deze terminologie werd vermoedelijk overgenomen uit het K.B. van 13 februari 2001 dat spreekt over 'latere verwerking' net als Richtlijn 1995/46/EC in de context van kennisdoeleinden.

349. De Commissie meent dat dit artikel onnodige complicaties met zich meebrengt en net als het voorgaande geschrapt moet worden.

Artikel 204

350. Artikel 204 van het ontwerp bevat een tweede vrijstelling van de verplichting tot afsluiten van een overeenkomst in dezelfde bewoordingen als artikel 201, §1, b van het ontwerp.

351. De Commissie verwijst naar de opmerkingen hierboven gemaakt bij artikel 201, §1, b en 203 van het ontwerp en is van oordeel dat deze bepaling geschrapt moet worden.

Artikelen 205-207

352. Gelet op de opmerkingen hierboven geformuleerd is de Commissie van oordeel dat de artikelen 205 tot en met 207 die de inhoud van de overeenkomst of kennisgeving opgelegd bij artikelen 202 en 204 van het ontwerp geschrapt dienen te worden.

353. In het bijzonder moeten de bepalingen geschrapt worden die de verantwoordelijke voor de oorspronkelijke verwerking een zekere zeggenschap geven over de activiteiten van 3de verantwoordelijke voor de verdere verwerking". Van de eerstgenoemde moet voorafgaand akkoord gevraagd worden bij de inschakeling van een verwerker door de hergebruiker en voor een nieuwe verdere verwerking. Hiermee mengt het ontwerp zich verregaand in met het opzet en de uitvoering van onderzoek, zonder hiervoor enige rechtvaardiging te bieden.

354. De verantwoordingsplicht verwoord in de artikelen 5.2 en 24 AVG zal de verwerkingsverantwoordelijke ertoe brengen een overeenkomst af te sluiten met de bron van de onderzoeksgegevens, met een inhoud gepast voor de aard, de omvang, de context en het doel van de verwerking. Het keurslijf opgelegd door artikelen 205-207 van het ontwerp is overbodig en de Commissie is van oordeel dat het geschrapt moet worden.

Artikel 208

355. Artikel 208 van het ontwerp herneemt de inhoud van artikel 201 §1 van het ontwerp dat geldt voor rechtstreekse inzameling van persoonsgegevens voor kennisdoeleinden, met toevoeging van artikel 14 AVG in de opsomming. De vermelding van een afwijking op artikel 14 AVG is in strijd met de AVG daar dit artikel niet vermeld wordt in de openingsclausules van artikel 89(2)-(3) AVG. Artikel 14 AVG bevat reeds een uitzondering voor kennisdoeleinden (in 14.5.b AVG) zodat een afwijking niet nodig is.

356. De Commissie verwijst voor het overige naar de opmerkingen gemaakt hierboven bij artikel 201, §1 van het ontwerp en afdeling 2 'Gegevensverzameling via verdere verwerking van gegevens' en is van oordeel dat deze bepaling herschreven moet worden.

Artikel 209

357. Artikel 209 van het ontwerp herneemt grotendeels de inhoud van artikel 201, §2 en §3 van het ontwerp dat geldt voor rechtstreekse inzameling van persoonsgegevens voor kennisdoeleinden. De Commissie verwijst naar de opmerkingen gemaakt hierboven bij artikel 201, §2 van het ontwerp en afdeling 2 'Gegevensverzameling via verdere verwerking van gegevens' en is van oordeel dat deze bepaling herschreven moet worden.

7.4.3. Afdeling 3 - Anonimisering of pseudonimisering van de gegevens verwerkt met het oog op onderzoek of statistische doeleinden

358. De Memorie van toelichting geeft volgende bestaansreden voor afdeling 3 van het ontwerp:

Artikel 89 van de Verordening bepaalt dat de passende waarborgen:

- *pseudonomisering inhouden;*
- *de voorkeur geven aan verdere verwerkingen die de identificatie van betrokkenen niet of niet langer toelaten.*

[Deze] afdeling brengt die principes ten uitvoer.

359. De gebruikte bewoordingen verwijzen naar artikel 89(1) AVG, zoals hierboven toegelicht leest de Commissie hierin slechts een herinnering aan de toepasselijkheid van de AVG in deze context en geen toelating aan de wetgever om een omvattend afwijkend regime in te voeren (zie nrs. 256, 257 e.v.).
De Memorie van toelichting motiveert niet welke bepaling(en) van de AVG toelaat (toelaten) de in afdeling 3 opgenomen verplichting op te leggen.

360. De Commissie meent dat deze afdeling geschrapt moet worden gelet op het problematisch karakter van de erin opgenomen bepalingen.

Artikelen 210, 211, 213 en 214

361. Artikelen 210, 211, 213 en 214 van het ontwerp bepalen dat de allereerste stap in elke verwerking voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden moet bestaan in de anonimisering of pseudonimisering van persoonsgegevens. Artikel 210 van het ontwerp regelt dit voor het geval van rechtstreekse inzameling, artikel 211 van het ontwerp voor verwerkingen "*door een verantwoordelijke voor een latere verwerking die dezelfde is als de verantwoordelijke voor de oorspronkelijke verwerking*".

362. De verwerkingsverantwoordelijke die via onrechtstreekse inzameling (hergebruik) persoonsgegevens bekomt voor deze doeleinden komt aan bod in artikel 213 van het ontwerp. De

verwerkingsverantwoordelijke die via onrechtstreekse inzameling (hergebruik) persoonsgegevens bekomt uit verschillende bronnen is onderworpen aan artikel 214 van het ontwerp.

363. Het ligt voor de hand dat persoonsgegevens zo vroeg mogelijk gepseudonimeerd moeten worden – waar mogelijk – om in overeenstemming te zijn met de bepalingen van de AVG. Dermate gedetailleerde regels over wie dit wanneer moet doen zijn evenwel overbodig. De betrokken partijken zijn het best geplaatst om te bepalen hoe de lasten die pseudonimisering met zich meebrengt te verdelen.

364. De Memorie van toelichting stelt dat deze bepalingen "*niet van toepassing [zijn] op de verwerkingen voor historische, statistische of wetenschappelijke doeleinden waarvan de verwerkingsverantwoordelijke, overeenkomstig artikel 100 van dit ontwerp, aantoont dat hij de doeleinden van de verwerking niet kan verwezenlijken met enkel beroep te hebben op niet gepseudonymiseerde of niet geanonymiseerde persoonsgegevens*."[92]
Dit stemt niet overeen met de tekst van deze bepalingen die geen enkele uitzondering bevatten[93], hetgeen vanzelfsprekend voor historisch onderzoek - maar even goed in andere gevallen – neerkomt op een verbod van bepaalde gangbare onderzoeksmethoden.

365. In heel wat gevallen is voor de praktische organisatie van het onderzoek de identificatie van de betrokkenen op welbepaalde momenten nodig is: bijvoorbeeld om respondenten voor interviews te contacteren, opvolgingsenquêtes te doen, een panel samen te stellen voor onderzoeken of om kandidaten voor klinische proeven te werven en te selecteren. Een voorzichtige onderzoeker zal identificatiegegevens – waar mogelijk – afzonderlijk bewaren van de overige gegevens om te voldoen aan de vereisten van de AVG, ook zonder expliciete bepaling in het nationale recht.

366. De Commissie herneemt de kanttekening die eerder gemaakt werd over anonimisering en pseudonimisering (zie nr. 299). De Commissie meent dat de inmenging in de wijze waarop verwerkingsverantwoordelijken hun onderzoeksactiviteiten vorm geven – en het gedeeltelijk verbod op onderzoeksmethoden - niet gerechtvaardigd wordt door de Memorie van toelichting en daarenboven ingaat tegen het basisbeginsel verwoord door artikelen 5.2 en 24 AVG. De verantwoordingsplicht houdt immers in dat de verwerkingsverantwoordelijke effectief verantwoordelijk is voor de naleving van de AVG en dit kan aantonen. Bijgevolg is de Commissie van oordeel dat deze bepalingen geschrapt moeten worden.

Artikel 212

[92] De verwijzing naar artikel 100 moet hier vermoedelijk als artikel 193 gelezen worden.
[93] Artikel 213 en 214 bevatten wel de zinsnede "[onverminderd] bijzondere bepalingen" maar dit kan moeilijk als een uitzondering geduid worden.

367. Artikel 212 van het ontwerp bepaalt dat de verwerkingsverantwoordelijke de gegevens slechts mag depseudonimiseren indien dat noodzakelijk is voor het onderzoek of de statistische doeleinden en na advies van de functionaris voor gegevensbescherming.

368. De Commissie herneemt haar opmerking hierboven gemaakt bij artikel 195 van het ontwerp en is van oordeel dat het artikel 212 geschrapt moet worden (zie nrs. 309-313).

Artikel 215

369. Artikel 215 van het ontwerp luidt als volgt :

"De derde vertrouwenspersoon mag geen belangenconflict hebben met de verantwoordelijke voor de verdere verwerking.

De derde vertrouwenspersoon is verwerker van de oorspronkelijke verwerkingsverantwoordelijken."

370. Het eerste lid volgt reeds uit de definitie van "derde vertrouwenspersoon". Het tweede lid geeft een bepaalde invulling aan het begrip 'verwerker' die niet noodzakelijk overeenstemt is met de criteria bepaald door artikel 4.8 AVG, zodat dit lid hiermee in strijd is. De Commissie meent dat dit artikel geschrapt moet worden.

Artikel 216

371. Volgens artikel 216 van het ontwerp controleert de functionaris voor gegevensbescherming het gebruik van de pseudonimiseringssleutels.

372. De Commissie herneemt de eerder gemaakte opmerkingen over de verplichte inschakeling van een functionaris voor gegevensbescherming en is van oordeel dat dit artikel geschrapt moet worden (zie nrs. 283-285).

Artikel 217

373. Artikel 217 van het ontwerp bevat net als artikelen 201, 208 en 209 afwijkingen op bepaalde rechten van de betrokkene wanneer de gegevens geanonimiseerd of gepseudonimiseerd zijn.

374. Eens gegevens deugdelijk geanonimiseerd zijn is de AVG niet langer van toepassing, zodat een afwijking overbodig is.
Eens gegevens gepseudonimiseerd zijn, geldt de beperking van artikel 11 AVG op de rechten vervat in artikelen 15 tot en met 20 AVG, behalve wanneer de betrokkene aanvullende gegevens verstrekt die het mogelijk maken hem te identificeren. Artikel 217 beperkt de rechten van betrokkenen ook in deze gevallen.

375. De vermelding van een afwijking op artikel 14 AVG is in strijd met de AVG daar dit artikel niet vermeld wordt in de openingsclausules van artikel 89(2)-(3) AVG. Artikel 14 AVG bevat reeds een uitzondering voor kennisdoeleinden (in 14.5.b AVG) zodat een afwijking niet nodig is.

376. De Commissie verwijst voor het overige naar de opmerkingen gemaakt hierboven bij artikel 201 van het ontwerp en meent dat artikel 217 geschrapt moet worden

7.4.4. Afdeling 4 - Verspreiding van gegevens verwerkt met het oog op archivering, onderzoek of statistische doeleinden

377. De Memorie van toelichting bevat geen verwijzing naar bepalingen van de AVG die door deze afdeling geïmplementeerd zouden worden, maar verwijst naar twee overwegingen die verband houden met artikel 89 AVG. Zoals hierboven toegelicht bevat artikel 89(1) AVG geen openingsclausule voor de lidstaten (zie nrs. 256, 257 e.v.). Deze afdeling voert een afwijkend regime in voor de verwerking van niet-gepseudonimiseerde persoonsgegevens voor kennisdoeleinden – meer bepaald de verspreiding ervan – en is bij gebrek aan rechtvaardiging strijdig met de AVG.

378. Overigens regelt Hoofdstuk V van titel 1 de verwerking van persoonsgegevens ten behoeve van academische uitdrukkingsvormen reeds, zonder dat in deze afdeling het verband daarmee gelegd wordt. De Commissie is van oordeel dat de regeling die geldt voor de publicatie van onderzoeksresultaten parallel moet lopen met de regeling die geldt voor de publicatie van journalistieke artikelen, omdat het onderscheid tussen beide activiteiten maken in de praktijk vrijwel onmogelijk is.

379. De Commissie herhaalt nogmaals dat de draagwijdte van de artikelen 218 en 219 van het ontwerp moeilijk te doorgronden is door het dubbel onderscheid dat gemaakt wordt in toepassingsgebied.

380. Artikel 218 van het ontwerp regelt de publicatie van persoonsgegevens in niet-gepseudonimiseerde vorm – zowel voor gevoelige als niet-gevoelige gegevens. Dit is toegelaten onder bepaalde voorwaarden geïnspireerd op de huidige regeling[94]:

a) de betrokkene zijn toestemming heeft verleend; of
b) de gegevens door de betrokkene zelf openbaar zijn gemaakt; of
c) de gegevens nauw samenhangen met het openbare of historische karakter van de betrokkene; of

[94] Art. 23 van het K.B. van 13 februari 2001.

d) de gegevens nauw samenhangen met het openbare of historische karakter van feiten waarbij de betrokkene betrokken was.

381. Artikel 219 van het ontwerp bepaalt dat voor zover het gaat om niet-gevoelige gegevens, de publicatie in gepseudonimiseerde vorm toegelaten is. Aan te nemen is dat voor gevoelige gegevens de publicatiemogelijkheid geregeld in artikel 218 van het ontwerp alsnog van toepassing is.

382. De Commissie dringt er op aan dat deze artikelen geschrapt worden.

7.4.5. Afdeling 5 - Mededeling van de gegevens verwerkt met het oog op archivering, onderzoek of statistische doeleinden

383. De Memorie van toelichting bevat geen verwijzing naar bepalingen van de AVG die door deze afdeling geïmplementeerd zouden worden. Zoals hierboven toegelicht bevat artikel 89(1) AVG geen openingsclausule voor de lidstaten (zie nrs. 256, 257 e.v.). Deze afdeling voert een afwijkend regime in voor de verwerking van niet-gepseudonimiseerde persoonsgegevens voor kennisdoeleinden – meer bepaald voor de mededeling ervan aan een derde - en is hierdoor strijdig met de AVG.

384. Ten overvloede stelt de Commissie vast dat de draagwijdte van artikel 220 van het ontwerp – een verbod op het reproduceren van niet-gepseudonimiseerde gegevens – in die mate vaag gesteld wordt zodat de handhaving ervan problematisch is. Zeker is dat reproductie van gegevens een onontkoombare noodzaak is in elk informaticasysteem, al was het maar om gegevens van het opslagmedium op een scherm te kunnen tonen. Het verbod niet-gepseudonimiseerde gegevens te reproduceren komt in elk geval neer op een algeheel verbod op het gebruik van geautomatiseerde middelen voor de verwerking – zelfs indien deze middelen net dienen om de persoonsgegevens te pseudonimiseren.

385. Verder stelt de Commissie vast dat deze bepaling niet verenigbaar is met artikel 214 van het ontwerp dat ingeval van koppeling van verschillende initiële verwerkingen regelt wie tot pseudonimisering moet over gaan – hetgeen moeilijk te realiseren is zonder reproductie van de persoonsgegevens.

386. De Memorie van toelichting stelt dat het de bedoeling is "safe rooms" te verplichten, waar de onderzoeker geen foto's of scans mag nemen, maar wel notities mag nemen. Dit strookt niet met de inhoud van de ontwerp-tekst, daar handgeschreven notities wel degelijk ook 'reproducties' zijn.

387. Het verbod geldt weliswaar niet voor elke verwerking voor kennisdoeleinden, het geldt van zodra er sprake is van "mededeling van de gegevens", waarmee onrechtstreekse inzameling van persoonsgegevens bedoeld wordt ogenschijnlijk[95] en het één van drie criteria vervuld zijn:

a) het om gevoelige gegevens gaat; of

b) de overeenkomst tussen de verantwoordelijke voor de oorspronkelijke verwerking en de verantwoordelijke voor de verdere verwerking zulks verbiedt; of

c) die reproductie de veiligheid van de betrokkene in het gedrang kan brengen.

388. De drempel voor toepasselijkheid van deze ontwerp-bepaling is zodanig laag, dat een onvoorstelbaar groot aantal verwerkingen voor kennisdoeleinden hierdoor getroffen worden, ongeacht hoe hoog of hoe laag het risico ook is die deze met zich meebrengen voor betrokkenen. Een systeem van "safe rooms" opleggen als algemeen geldende verplichting is vanzelfsprekend overmatig. De uitzonderingen vermeld in artikel 221 zijn niet meer dan een doekje voor het bloeden.

De Commissie dringt aan op de schrapping van deze artikelen.

CONCLUSIE van de Commissie over titel 4 van het ontwerp

389. In het licht van de bovenstaande bemerkingen is advies van de Commissie ongunstig voor de totaliteit van titel 4 van het ontwerp.

[95] Het ontwerp definieert "mededeling van gegevens" als "mededeling van gegevens aan geïdentificeerde derde" (artikel 188, 10° van het ontwerp).

8. TITEL 5 : RECHTSMIDDELEN EN VERTEGENWOORDIGING VAN DE BETROKKENEN

8.1. Hoofdstuk I - Vordering tot staking

Bevoegdheidsregeling (art. 222)

390. Art. 222 regelt de bevoegdheid van de voorzitter van de rechtbank van eerste aanleg, zitting houdende zoals in kortgeding, wanneer een verwerking inbreuk maakt op een wettelijke of reglementaire bepaling betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens[96].

391. De Commissie verwelkomt de keuze van de wetgever om in een doeltreffende voorziening in rechte te voorzien via een procedure zoals in kortgeding. De bevoegdheid van de voorzitter van de rechtbank van eerste aanleg wordt algemeen omschreven. Bijgevolg is de voorzitter van de rechtbank van eerste aanleg op grond van deze bepaling bevoegd om kennis te nemen van vorderingen ingesteld door de GBA ingevolge art. 6 GBAW.[97] Dit wordt overigens uitdrukkelijk bevestigd door art. 224.3.2.

392. De Memorie van toelichting verwijst enkel naar de vordering tot staking zoals thans voorzien in art. 14 WVP (dat vanaf 25 mei 2018 wordt opgeheven). Om de lezer een beter begrip te geven van de werkelijke draagwijdte van deze bepaling, raadt de Commissie de wetgever aan om uitdrukkelijk toe te lichten dat art. 222 de voorzitter van de rechtbank van eerste aanleg bevoegd maakt om kennis te nemen van vorderingen ingesteld door de GBA ingevolge art. 6 GBAW.

393. Ook verdient het aanbeveling om in de Memorie van Toelichting te preciseren dat de voorzitter van de rechtbank van eerste aanleg via art. 222 ook kan worden gevat om, overeenkomstig art. 267 VWEU, een prejudiciële vraag te stellen aan het Hof van Justitie. Overeenkomstig het Schrems arrest (C-362/14), moet de nationale wetgever immers beroepsgangen voorzien waarmee de bevoegde autoriteit grieven omtrent de geldigheid van een handeling van de Unie aan de nationale rechter kan voorleggen, zodat die laatste, wanneer hij twijfelt ten aanzien van de geldigheid van de handeling, de vraag naar de geldigheid ervan prejudicieel kan verwijzen.[98]

---

[96] De Commissie merkt op dat de Franstalige versie spreekt van "*dispositions légales **ou** réglementaires*", terwijl de Nederlandstalige versie spreekt van "*wettelijke **en** reglementaire bepaling*". De Nederlandstalige versie dient te worden aangepast door het woord "of" te gebruiken, aangezien hier geen cumulatieve voorwaarde kan worden gesteld.

[97] De lidstaten zijn op grond van artikel 58(5) AVG verplicht om bij wet te bepalen dat hun toezichthoudende autoriteit bevoegd is om "*inbreuken op deze verordening ter kennis te brengen van de gerechtelijke autoriteiten en, waar passend, daartegen een rechtsvordering in te stellen of anderszins in rechte op te treden, teneinde de bepalingen van deze verordening te doen naleven*".

[98] HVJEU, Maximillian Schrems t. Data Protection Commissioner, Zaak C-362/14, paragraaf 65.

Lacune: dreiging van ernstige inbreuk

394. Indien het waarschijnlijk is dat een voorgenomen verwerking, die op punt staat om te gebeuren, een ernstige inbreuk zal maken op een wettelijke of reglementaire bepaling betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens, moet men de (verdere) uitvoering van die verwerking kunnen voorkomen.

395. Een gelijkaardige mogelijkheid wordt voorzien in art. 1 van de Wet van 12 januari 1993 betreffende een vorderingsrecht inzake bescherming van het leefmilieu[99], welk bepaalt dat:

"*Onverminderd de bevoegdheid van andere rechtscolleges op basis van andere wetsbepalingen, stelt de voorzitter van de rechtbank van eerste aanleg, op verzoek van de procureur des Konings, van een administratieve overheid of van een rechtspersoon zoals omschreven in artikel 2, het bestaan vast van een zelfs onder het strafrecht vallende handeling, die een kennelijke inbreuk is of een ernstige dreiging vormt voor een inbreuk op één of meer bepalingen van wetten, decreten, ordonnanties, verordeningen of besluiten betreffende de bescherming van het leefmilieu. Hij kan de staking bevelen van handelingen waarvan de uitvoering reeds is begonnen of maatregelen opleggen ter preventie van de uitvoering ervan of ter voorkoming van schade aan het leefmilieu. Voor elk debat over de grond van de zaak moet een verzoeningspoging plaatshebben. De voorzitter kan aan de overtreder een termijn toestaan om aan de opgelegde maatregelen te voldoen.*"

396. Art. 222 regelt enkel de bevoegdheid van de voorzitter van de rechtbank van eerste aanleg indien er sprake is van een verwerking. Strikt genomen zou de voorzitter van de rechtbank dan ook niet bevoegd zijn om uitspraak te doen wanneer de verwerking als zodanig nog niet is aangevangen, zelfs wanneer het waarschijnlijk is dat een voorgenomen verwerking een ernstige inbreuk zal maken op een wettelijke of reglementaire bepaling betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens.

397. De Commissie raadt aan om, naar analogie van voornoemde bepaling van de Wet betreffende een vorderingsrecht inzake bescherming van het leefmilieu, een bepaling toe te voegen die luidt als volgt:

"*De voorzitter van de rechtbank van eerste aanleg kan de staking bevelen van verwerkingen waarvan de uitvoering reeds is begonnen of maatregelen opleggen ter preventie van de uitvoering ervan of ter voorkoming van een ernstige inbreuk op een wettelijke of reglementaire bepaling betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens."*

De territoriaal bevoegde rechter (art. 224.2)

[99] B.S., 19 februari 1993.

398. Art. 224.2 regelt de territoriale bevoegdheid van de voorzitter van de rechtbank van eerste aanleg. Het betreft een gespecialiseerde bevoegdheid die om kwaliteitsredenen best ook wordt toegekend aan gespecialiseerde magistraten. De territoriale versnippering van de bevoegdheid voor de voorzitter van de rechtbank van eerste aanleg zal bovendien leiden tot disparate rechtspraak; immers zijn er kortgedingprocedures in alle 27 afdelingen van de gerechtelijke arrondissementen.

399. Het lijkt de Commissie aangewezen om deze procedures zo veel mogelijk te concentreren in Brussel, wat de Nederlandstalige zaken betreft bij de voorzitter van de Nederlandstalige rechtbank van eerste aanleg te Brussel en wat de Franstalige zaken betreft bij de voorzitter van de Franstalige rechtbank van eerste aanleg te Brussel (en wat de Duitstalige zaken betreft bij de voorzitter van de rechtbank van eerste aanleg te Eupen).

400. In het licht van het voorgaande raadt de Commissie de wetgever aan om ontwerp art. 224.2 als volgt te herformuleren:
"§ 2. In afwijking van artikel 624 van het Gerechtelijk wetboek wordt de vordering gebracht : wat de Nederlandstalige zaken betreft voor de voorzitter van de Nederlandstalige rechtbank van eerste aanleg te Brussel, wat de Franstalige zaken betreft voor de voorzitter van de Franstalige rechtbank van eerste aanleg te Brussel en wat de Duitstalige zaken betreft voor de voorzitter van de rechtbank van eerste aanleg te Eupen." [100]

Wie stelt de vordering in? (art. 224.3)

401. Art. 224.3 van het voorontwerp bepaalt dat de vordering gegrond op art. 222 ingesteld kan worden door de betrokkene of door de "*voorzitter van de bevoegde toezichthoudende autoriteit*".

402. De Commissie merkt op dat deze bepaling ogenschijnlijk een vorderingsrecht toekent aan iedere bevoegde toezichthoudende autoriteit die door het voorontwerp wordt beoogd (handelend in het kader van haar resp. bevoegdheden) en dus niet enkel aan de GBA. Het Controleorgaan, het Comité I en het Comité P vallen hier bijgevolg ook onder. De Commissie verwijst in dit verband naar haar opmerkingen wat betreft het gebruik van de aanduiding "bevoegde toezichthoudende autoriteit".

403. Wat het vorderingsrecht van de GBA betreft, merkt de Commissie op dat de GBA ingevolge art. 3 GBAW over rechtspersoonlijkheid beschikt. Aangezien de GBA over rechtspersoonlijkheid zal beschikken, dienen de woorden "de voorzitter van" te worden geschrapt (althans wat de GBA

[100] Zie ook naar analogie artikel 627, 11°, 16° en 17° Ger.W. wat betreft de territoriale bevoegdheid van de Nederlandstalige respectievelijk Franstalige rechtbanken te Brussel. Zie ook naar analogie de artikelen 632, 632*bis*, 633*sexies* en 633*septies* Ger. W. wat betreft de territoriale bevoegdheid van de rechtbank van eerste aanleg te Eupen wanneer de procedure in het Duits wordt gevoerd.

betreft).[101] Art. 18 GBAW bepaalt immers reeds dat het de voorzitter is die de GBA vertegenwoordigt in rechte. Bovendien moet er procesrechtelijk een onderscheid gemaakt worden tussen enerzijds de procespartij en anderzijds het orgaan van de procespartij dat de procespartij vertegenwoordigt in rechte. De procespartij zal de GBA zijn, en het orgaan dat de GBA vertegenwoordigt, zal de voorzitter ervan zijn. Het zou merkwaardig zijn dat 224.3 zou bepalen dat de procespartij niet de GBA maar de vertegenwoordiger van de GBA is.

Lacune: administratiefrechtelijke bevoegdheid voor de beslissing om in rechte op te treden

404. Zowel in de GBAW als in het voorontwerp ontbreekt een bepaling die stipuleert welk orgaan van de GBA bevoegd is om de beslissing te nemen om in rechte op te treden. Het is niet omdat art. 18 GBAW bepaalt dat de voorzitter of het oudste lid van het directiecomité procesrechtelijk de GBA vertegenwoordigt in rechte, dat hij meteen ook administratiefrechtelijk bevoegd is om de beslissing te nemen om in rechte op te treden. Dat zijn twee onderscheiden zaken. Het kan immers zijn dat orgaan X van een overheidsinstelling bevoegd is om de beslissing te nemen in rechte op te treden maar dat de instelling dan in rechte wordt vertegenwoordigd door orgaan Y.

405. Wie de bevoegdheid heeft om die beslissing te nemen, kan ook niet louter in het reglement van interne orde worden geregeld, omdat dit louter intern geldt en geen juridische werking heeft ten aanzien van derden. Dit moet dus bij wet worden geregeld. Een wet die een staatsinstelling opricht, moet een bepaling bevatten die stelt welk orgaan van die instelling bevoegd is om te beslissen om in rechte op te treden (los van wie de instelling in rechte vertegenwoordigt).

406. Zo bepaalt art. 193 § 1 van het Gemeentedecreet bijvoorbeeld :

"*Het college van burgemeester en schepenen vertegenwoordigt de gemeente in gerechtelijke en buitengerechtelijke gevallen **en** beslist om op te treden in rechte namens de gemeente.*"

407. Uit deze bepaling blijkt dat de beslissing om in rechte op te treden, moet worden genomen door het college, en dat het daarnaast ook het college is dat de gemeente vervolgens vertegenwoordigt bij dat optreden in rechte.

408. Als de wetgever niet duidelijk bepaalt welk orgaan van de GBA de bevoegdheid heeft om te beslissen om in rechte op te treden, bestaat er het risico dat iedere partij die door de GBA wordt gedagvaard, vraagt om de vordering onontvankelijk te verklaren (omdat niet geldig is beslist om

[101] De situatie is anders onder artikel 32, §3 WVP, dat sprak van "de voorzitter van" en niet "de Commissie" omdat de Commissie geen rechtspersoonlijkheid heeft.

tot dagvaarding over te gaan). De Belgische wetgever zou daarmee tekortkomen aan haar verplichtingen ingevolge art. 58.5 AVG. Om hieraan te verhelpen, raadt de Commissie aan om aan het voorontwerp een bepaling toe te voegen dat art. 18 van de GBAW vervolledigt met de volgende toevoeging (naar analogie van de desbetreffende bepaling in het Gemeentedecreet) :

"*De voorzitter van het directiecomité en, in diens afwezigheid, het oudste aanwezige lid van het directiecomité, met uitzondering van de voorzitter van de geschillenkamer, vertegenwoordigt de Gegevensbeschermingsautoriteit in rechte. De beslissing om op te treden in rechte namens de Gegevensbeschermingsautoriteit wordt genomen door het directiecomité*."

Beslissingen over de rectificatie, schrapping of beperking in geval van een strafonderzoek of -procedure (art. 223)

409. Art. 223 voorziet in een uitzondering op de algemene bevoegdheid van de voorzitter van de rechtbank van eerste aanleg om kennis te nemen van verwerkingen die inbreuk maken op een wettelijke of reglementaire bepaling betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens, toch minstens wat betreft vorderingen met betrekking tot de rectificatie, schrapping, beperking van de behandeling, het verbod op gebruik of verwijdering van persoonsgegevens. De uitzondering zal van toepassing zijn "vanaf het moment" dat de gegevens worden verwerkt "in de loop van een opsporingsonderzoek, van een gerechtelijk onderzoek, een strafrechtelijke procedure voor de bodemrechter of een procedure voor de uitvoering van een strafrechtelijk vonnis".[102] Vanaf dat ogenblik zou de bevoegdheid om te beslissen over de rectificatie, schrapping, beperking van de behandeling, het verbod op gebruik of verwijdering van persoonsgegevens echter uitsluitend, volgens de fase van de procedure, aan het openbaar ministerie of de bevoegde strafrechter toebehoren.

410. De Commissie heeft hierbij twee bedenkingen. Ten eerste ziet de Commissie niet in hoe de behandeling van de vordering door het openbaar ministerie een doeltreffende voorziening in rechte uitmaakt in de zin van art. 79 AVG, te meer wanneer het opsporingsonderzoek onder de verantwoordelijkheid van het openbaar ministerie zelf zou plaatsvinden. Ten tweede meent de Commissie dat deze bepaling bijzonder onduidelijk is opgesteld.

411. In het licht van het voorgaande raadt de Commissie aan om art. 223 als volgt te herformuleren:
"*In afwijking van artikel 222, is de strafrechter, in zoverre deze reeds is gevat, bevoegd om uitspraak te doen over een vordering betreffende de rectificatie, schrapping, beperking van de verwerking, het verbod op gebruik of de verwijdering van persoonsgegevens.*"

[102] De Commissie merkt op dat de Franse term "traitement" in art. 223 telkens zou moeten worden vertaald met het Nederlandse woord "verwerking".

412. Art. 224-232 vereisen geen bijzondere opmerkingen.

8.2. Hoofdstuk II - Vertegenwoordiging van betrokkenen

413. Art. 233 regelt de mogelijkheid tot vertegenwoordiging van betrokkenen in rechte. De Commissie betreurt dat het voorontwerp daarbij geen gebruik maakt van de mogelijkheid voorzien in art. 80.2 AVG, dat toelaat om te bepalen dat een orgaan, organisatie of vereniging als bedoeld in art. 80.1 AVG, over het recht beschikt om *onafhankelijk van de opdracht* van een betrokkene, klacht in te dienen of een vordering in rechte in te stellen, indien het/zij van mening is dat de rechten van een betrokkene uit hoofde van deze verordening zijn geschonden ten gevolge van de verwerking. De Commissie raadt aan om van deze mogelijkheid alsnog gebruik te maken.

CONCLUSIE van de Commissie over titel 5 van het ontwerp

414. De Commissie brengt een gunstig advies uit over Titel 5 van het wetsontwerp wat betreft de bevoegdheidsregeling , mits rekening wordt gehouden met zowel de algemene opmerkingen als de opmerkingen die artikelsgewijs zijn geformuleerd, meer bepaald wat betreft de art. 222, art. 223 en art. 224 en brengt een ongunstig advies uit over Titel 5 van het wetsontwerp wat betreft de lacunes in geval van dreiging van ernstige inbreuk en wat betreft de administratiefrechtelijke bevoegdheid voor de beslissing om in rechte op te treden.

9. TITEL 6 : SANCTIES

Algemene opmerkingen

Afwijking voor de publieke sector

415. Artikel 83.7 AVG noopt de lidstaten ertoe om expliciet te bepalen of en in hoeverre administratieve geldboeten kunnen worden opgelegd aan overheidsinstanties en overheidsorganen.

416. Art. 234, § 2 van het ontwerp luidt "*Het artikel 83 van de Verordening is niet van toepassing op de overheidsinstanties en openbare organen.*" De Memorie van toelichting geeft geen verantwoording voor de gemaakte keuze, maar stelt enkel het volgende:

> *"Het is duidelijk dat de publieke sector niet uitgesloten is van de verplichtingen voorzien in de Verordening en dit wetsontwerp. Er is echter voor geopteerd om geen administratieve geldboetes op te leggen aan de publieke sector."*

417. Wat de opening betreft die de AVG aan de nationale wetgever laat, is de Commissie er in beginsel voorstander van om de private en de publieke sector gelijk te behandelen op vlak van handhaving. Het is moeilijk te verdedigen dat de GBA minder handhavingsmogelijkheden heeft ten aanzien van de publieke sector, zeker wanneer het gaat om overheden die dwingende beslissingen kunnen nemen ten aanzien van rechtsonderhorigen of wanneer de betrokkenen geen keuze hebben op wie ze beroep doen voor de verstrekking van een openbare dienst. .

418. Dat het de bedoeling zou zijn van de wetgever om een verwerkingsverbod of –beperking te beschouwen als ultieme handhavingsmogelijkheid voor de GBA ten aanzien van de publieke sector, valt niet uit de Memorie van toelichting af te leiden. Evenmin voor de hand liggend is dat het vrijwaren van de continuïteit van de publieke dienstverlening hiermee het best gediend is. Enerzijds dient de verwerkingsbeperking om de schending van de rechten van de betrokkene inzake gegevensbescherming te doen ophouden, anderzijds is kan diezelfde verwerkingsbeperking de betrokkene raken in zijn belangen – zodat moet vastgesteld worden dat de betrokkene riskeert tweemaal de dupe te zijn.

419. Indien de wetgever meent een afwijking te moeten invoeren voor 'overheidsinstanties en openbare organen' is de Commissie van oordeel dat het toepassingsgebied van deze afwijking zorgvuldig moet afgepakend worden in het belang van de rechtszekerheid (zie ook de opmerkingen gemaakt bij titel 1, hoofdstuk IV, afdeling 2, randnummers 149-152). Bij gebrek aan enige definitie van 'overheidsinstanties en openbare organen' in het ontwerp moet de Commissie vaststellen dat een grote grijze zone ontstaat die effectieve handhaving in de weg staat.

420. Op basis van het ontwerp valt geen antwoord te geven op de vraag of de uitzondering geldt voor openbare diensten verricht door privaatrechtelijke entiteiten (bv. vzw's en stichtingen belast door of krachtens de wet met taken van algemeen belang) of voor de autonome overheidsbedrijven zoals geregeld in de wet van 21 maart 1991. [103] Nochtans ligt voor de hand dat organisaties die in essentie dezelfde activiteiten hebben op gelijke wijze behandeld worden. Een louter organiek criterium kan bijvoorbeeld niet verantwoorden dat een OCMW-ziekenhuis geen administratieve boete kan opgelegd worden, terwijl dit wel kan ten aanzien ziekenhuizen die opgericht zijn in de vorm van een vzw.

421. De wijze waarop het ontwerp gebruik maakt van de openingsclausule vervat in artikel 83.7 AVG is in strijd met het AVG en het legaliteitsbeginsel. In haar richtlijnen over de functionaris voor gegevensbescherming, heeft de Werkgroep artikel 29 gesteld dat deze notie in het nationaal recht moet bepaald worden.[104]

422. De Commissie dringt aan op een heroverweging van deze bepaling. Indien de afwijking gehandhaafd wordt dient dit uitvoeriger toegelicht te worden en stelt de Commissie voor de afwijking af te bakenen door te verwijzen naar artikel 5, 4e lid van het Strafwetboek dat een opsomming bevat van een aantal instanties[105].

Strafsancties in de publieke sector

423. Daar het ontwerp ervoor opteert om administratieve geldboeten uit te sluiten voor de publieke sector, moet artikel 84.1 AVG des te zorgvuldiger nageleefd worden[106]. Er moet een systeem van sancties bestaan dat doeltreffend, evenredig en afschrikkend is. De artikelen 235-242 van het ontwerp dienen om uitvoering hieraan te geven door bepaalde inbreuken te beteugelen met strafsancties.

424. Wat het afschrikkend karakter betreft, stelt de Memorie van toelichting het volgende over het vastgestelde maximumniveau van de strafrechtelijke boetes als volgt:

---

[103] Wet van 21 maart 1991 *betreffende de hervorming van sommige economische overheidsbedrijven.* .
[104] Werkgroep artikel 29, "Guidelines on Data Protection Officers ('DPOs')", WP243 rev. 01, p. 6.
[105] Het gaat om de federale staat, de gewesten, de gemeenschappen, de provincies, de hulpverleningszones, de prezones, de Brusselse agglomeratie, de gemeenten, de meergemeentezones, de binnengemeentelijke territoriale organen, de Franse Gemeenschapscommissie, de Vlaamse Gemeenschapscommissie, de gemeenschappelijke Gemeenschapscommissie en de openbare centra voor maatschappelijk welzijn. .
[106]Artikel 84.1 AVG luidt als volgt "De lidstaten stellen de regels inzake andere sancties vast die van toepassing zijn op inbreuken op deze verordening, in het bijzonder op inbreuken die niet aan administratieve geldboeten onderworpen zijn overeenkomstig artikel 83, en treffen alle nodige maatregelen om ervoor te zorgen dat zij worden toegepast. Die sancties zijn doeltreffend, evenredig en afschrikkend."

"Om de strafsancties te versterken en ze afschrikkend te maken in het licht van de administratieve sancties worden de bedragen als dusdanig behouden, zulks op grond van artikel 2 van de wet van 26 juni 2000 betreffende de invoering van de euro in de wetgeving die betrekking heeft op aangelegenheden als bedoeld in artikel 78 van de Grondwet: de bedragen uitgedrukt in BEF worden geacht te zijn uitgedrukt in euro, zonder omrekening. Er wordt tevens op gewezen dat de bedragen sedert 1 januari 2017 worden vermenigvuldigd met 8 ingevolge artikel 1, eerste en tweede lid, van de wet van 5 maart 1952 betreffende de opdeciemen op de strafrechtelijke geldboeten, gewijzigd door artikel 59 van de wet van 25 december 2016."

425. Ondanks het voorgaande kan de Commissie enkel vaststellen dat het maximumniveau van de strafrechtelijke boetes markant lager is dan de administratieve geldboeten. De wetgever is er niet toe gehouden een identiek maximumniveau vast te stellen, zolang het vastgelegd niveau toelaat doeltreffend, evenredig en afschrikkend te reageren. De Memorie van toelichting is onvoldoende om tot deze conclusie te komen. In andere domeinen is overigens gebruikelijk dat het niveau van administratieve boetes lager ligt dan de strafrechtelijke boetes, die als ultieme remedie gelden. De Commissie is van oordeel dat het ontwerp op dit punt herzien moet worden.

426. Het inperken van administratieve geldboeten ten aanzien van de publieke sector wordt in erg beperkte mate ondervangen door de strafbepalingen. Volgens artikel 5, 4e lid van het Strafwetboek gelden een belangrijk aantal instanties niet als strafrechtelijk verantwoordelijke rechtspersoon.[107]

427. Het ontwerp legt een verband tussen de corrigerende maatregelen die de toezichthoudende autoriteit kan opleggen en de strafbepalingen. Artikel 235, e) van het ontwerp beteugelt het niet respecteren van de door de toezichthoudende autoriteit vastgestelde corrigerende maatregel voor de definitieve beperking van stromen in overeenstemming met artikel 58.2.f) AVG strafbaar te stellen. De schending van een tijdelijke beperking van gegevensstromen kan dan weer niet bestraft worden, hetgeen de effectiviteit van deze maatregel ten aanzien van de publieke sector verder ondermijnt. De Commissie meent dat het ontwerp op dit punt moet herzien worden.

428. De Commissie meent verder dat hieraan minstens toegevoegd moet worden het negeren van een corrigerende maatregel in de zin van artikel 58.2.d) AVG (de verwerkingsverantwoordelijke of de verwerker gelasten op een nader bepaalde manier en binnen een nader bepaalde termijn, verwerkingen in overeenstemming te brengen met de bepalingen van de AVG).

[107] Het gaat om de federale staat, de gewesten, de gemeenschappen, de provincies, de hulpverleningszones, de prezones, de Brusselse agglomeratie, de gemeenten, de meergemeentezones, de binnengemeentelijke territoriale organen, de Franse Gemeenschapscommissie, de Vlaamse Gemeenschapscommissie, de gemeenschappelijke Gemeenschapscommissie en de openbare centra voor maatschappelijk welzijn.

429. Op grond van het voorgaande is de Commissie van oordeel dat niet aan de plicht is voldaan om te zorgen voor sancties die doeltreffend, evenredig en afschrikkend in de publieke sector. De Commissie meent dat het ontwerp op dit punt moet herzien worden, bijvoorbeeld door één van volgende pistes op te nemen.

430. De Europese Commissie heeft een regeling voorgesteld waarbij de instellingen of organen van de Europese Unie onderworpen zouden kunnen worden aan administratieve geldboeten tot 50 000 EUR per inbreuk en tot een totaal van 500 000 EUR per jaar voor bepaalde inbreuken.[108]

431. Naast het vastleggen van een ander plafond, zou de wetgever de toezichthoudende autoriteit de bevoegdheid kunnen geven om overheidsinstanties en openbare organen op te leggen hetzij een som, hetzij een aandeel van hun budget voor één of meerdere daaropvolgende periodes aan te wenden voor de uitvoering van de corrigerende maatregel die zij uitspreekt of heeft uitgesproken. Als stok achter de deur zou niet-naleving van deze maatregel als gevolg kunnen hebben hetzij omzetting ervan in een administratieve geldboete hetzij de gedwongen uitvoering door of in opdracht van de toezichthoudende autoriteit.

Artikelsgewijze opmerkingen

Artikel 234

432. De corrigerende bevoegdheden van de toezichthoudende autoriteit krachtens artikel 58.2 van de Verordening zijn tevens van toepassing op volgende bepalingen:

- op de artikelen 7, 8, 9, 19, 23, 25, 26, 28 en 29 van titel 1;
- op de artikelen 33 tot 72 van titel 2;
- op titel 4.

433. Wat de verwijzing betreft naar artikelen van titel 1 betreft het een gevolgtrekking van hetgeen artikel 2, 2e lid van het ontwerp bepaalt over de uitbreiding van het toepassingsgebied van de Verordening naar de verwerkingen bedoeld in de artikelen 2.2.a) en 2.2.b) van de AVG.

434. De Commissie is van oordeel dat artikel 22 van het ontwerp dient opgenomen te worden, zie opmerkingen hierboven over het verplicht karakter van het protocol voor de mededeling van persoonsgegevens door overheidsinstanties (nr. 159).

---

[108] Voorstel van een Verordening van het Europese Parlement en de Raad *en betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG*, COM(2017)8.

Artikel 235

435. De strafbepaling vervat in artikel 235 van het ontwerp viseert onder andere de 'vertegenwoordiger in België' van de verwerkingsverantwoordelijke of de verwerker.

436. De vraag stelt zich in welke mate de vermelding van de vertegenwoordiger werkzaam kan zijn, daar de vertegenwoordiger in de AVG als contactpersoon fungeert maar geen op zichzelf staande verplichtingen heeft. De gevallen waarin een vertegenwoordiger in de praktijk strafbare feiten zal aangewreven kunnen worden mogen dan al zeldzaam lijken, het signaal dat de wetgever geeft is dat de rol van vertegenwoordiger opnemen in België dit risico met zich meebrengt.

437. De Memorie van toelichting verheldert de beweegreden niet voor deze vermelding. De Commissie is van oordeel dat de wetgever dit dient te heroverwegen.

Artikel 238

438. Artikel 238 luidt: "*Bij veroordeling wegens een misdrijf omschreven in de artikelen 236 of 237, kan de rechtbank bevelen dat het vonnis in zijn geheel of bij uittreksel wordt opgenomen in een of meerdere dagbladen op de wijze die zij bepaalt, zulks op kosten van de veroordeelde.*"

439. Deze bepaling is een overname van artikel 40 WVP aldus de Memorie van toelichting. De Commissie stelt vast dat in dat geval verwezen moet worden naar de artikelen 235 en 236 van het ontwerp. Artikel 237 van het ontwerp is een herneming van artikel 37 WVP, waarnaar niet verwezen wordt door artikel 40 WVP. De Commissie is van oordeel dat deze materiële fout dient rechtgezet te worden.

Artikelen 239 - 240

440. De artikelen 239 en 240 van het ontwerp straffen bepaalde inbreuken op de gegevensverwerkingen geregeld in titel 3.

441. De Commissie stelt vast dat de straffen vermeld in de artikelen 239 en 240, 1° en 2° van het ontwerp inbreuken begaan door de verwerker, door personen die handelen onder het gezag van de overheid bedoeld in titel 3 of van diens verwerker beteugelen. Opvallende afwezige is de verwerkingsverantwoordelijke zelf, die per slot van rekening verantwoordelijk is voor de verwerking van persoonsgegevens conform de geldende regels. De Memorie van toelichting stelt in dit verband: "*De strafbepaling is niet van toepassing op de verwerkingsverantwoordelijke, aangezien een overheidsinstantie zonder rechtspersoonlijkheid niet strafrechtelijk veroordeeld kan worden.*"[109] De Commissie meent dat de verwerkingsverantwoordelijke vermeld dient te worden.

[109] Zoals hierboven toegelicht sluit artikel 5, 4e lid van het Strafwetboek de strafrechtelijke aansprakelijkheid van een aantal benoemde overheidsinstanties uit.

442. Artikel 240, 4° van het ontwerp viseert bepaalde inbreuken begaan door "*hij die persoonsgegevens doorgeeft*". Artikel 240, 5° van het ontwerp richt zich op "*elke persoon die toegang heeft tot persoonsgegevens bedoeld in artikelen 101, 134 en 164*". De Commissie stelt vast dat niet duidelijk is of deze bepalingen een andere personele scope hebben dan artikel 240, 1° en 2° van het ontwerp.

Artikel 242

443. Artikel 242 van het ontwerp regelt de samenloop tussen administratieve en strafrechtelijke procedures. Bij gebrek aan protocolakkoord beschikt de procureur des Konings over een termijn van twee maanden om te beslissen welk vervolg zij geeft aan een proces-verbaal. Tijdens deze termijn én indien de procureur het dossier effectief opneemt is "de mogelijkheid vervallen voor de toezichthoudende autoriteit om haar corrigerende bevoegdheden uit te oefenen".

444. De Commissie is van oordeel dat een dergelijk verval van corrigerende bevoegdheden – zelfs tijdelijk – in strijd is met artikel 58.2 AVG en bijgevolg geschrapt dient te worden.

CONCLUSIE van de Commissie over titel 6 van het ontwerp

445. In het licht van de bovenstaande bemerkingen is advies van de Commissie ongunstig voor de totaliteit van titel 6 van het ontwerp.

10. TITEL 7 : HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

De oprichting van drie bijkomende Belgische DPA's[110]

A. Algemeen

446. De Commissie stelt vast dat in het Ontwerp drie nieuwe DPA's worden opgericht: het C.O.C., het Comité I en het Comité P. Dit evident bovenop de reeds door de GBAW opgerichte DPA, met name de GBA (en ook bovenop een apart toezicht op de gerechten in het kader van hun gerechtelijke taken[111]). **In totaal zou de federale wetgever dus vier DPA's creëren** (en wellicht nog een apart toezichtsorgaan voor de gerechten).

447. De Commissie wees er in haar advies nr. 45/2016 van 31 augustus 2016 reeds op dat het bestaande Controleorgaan op de Politionele Informatie (hierna "C.O.C.") een hybride statuut heeft: enerzijds lijkt het C.O.C. op een DPA specifiek voor de politie-sector en anderzijds oefent het C.O.C. niet alle bevoegdheden uit die krachtens de Richtlijn aan een DPA worden opgelegd. De Commissie drong er toen op aan dat er in de toekomst een duidelijk keuze zou gemaakt worden: ofwel wordt het C.O.C. een volwaardige DPA voor alle politionele gegevensverwerkingen, ofwel wordt het aspect gegevensbescherming in de politionele sector volledig behandeld door de Commissie[112]. Het was de Commissie toen ook reeds duidelijk dat de huidige situatie van het C.O.C. ongunstig/onlogisch is – in die zin dat het qua taken en bevoegdheden 'gewrongen' zit tussen de taken en bevoegdheden van de Commissie en het Comité P – en dat een hervorming zich hoe dan ook opdringt. Het C.O.C. gaf in 2016 overigens ook zelf aan dat het wenste te evolueren in de richting van een volwaardige DPA, en dat het deze hervorming budgetneutraal kon doorvoeren[113]. Het lag dan ook reeds in de lijn der verwachtingen dat het C.O.C. zou gereorganiseerd worden.

---

[110] Zie in hoofdzaak de artikelen 73, 97 t.e.m. 100, 107.8, 130 t.e.m. 133, 163, 186 & Titel 7 & Titel 8 van het Ontwerp.

[111] Cf artikel 4, §2, eerste lid GBAW en overweging 20 AVG.

[112] Zie randnummers 6 tot en met 13 van advies nr. 45/2016.

[113] Zie advies nr. 01/2016 van het C.O.C. van 15 september 2016 (randnummer 8): "*Om volledig als een TA in de zin van de Richtlijn te worden beschouwd, ontbreekt enkel nog de mogelijkheid voor het C.O.C. om klachten te behandelen, waaronder de behandeling van de verzoeken tot al dan niet rechtstreekse toegang, en de mogelijkheid om dwingende maatregelen op te leggen. (…) Dit kan daarenboven budgetneutraal gebeuren, aangezien het C.O.C. van oordeel is deze bijkomende werkzaamheden binnen het huidige budget te kunnen uitoefenen*"

448. De Commissie stelt tegelijk vast dat krachtens het Ontwerp niet alleen het C.O.C. DPA zou worden, maar dat dit ook het geval zou zijn voor het Comité I en voor het Comité P.

De Commissie neemt akte van deze beleidskeuzes, die op zich stroken met het principe dat er in een lidstaat meerdere DPA's kunnen aangeduid worden (Cf art. 51.1, AVG en art. 41.1, Richtlijn). De Commissie gaat hierna wel na in welke mate de concretisering van deze politieke keuzes in de tekst van het Ontwerp

- leidt tot een duidelijke/coherente/efficiënte bevoegdheidsverdeling tussen de DPA's[114];
- strookt met alle regels die in de AVG en in de Richtlijn aan DPA's worden opgelegd en coherent is met de GBAW.

B. <u>De bevoegdheidsverdeling tussen de DPA's</u>

449. De Commissie is van oordeel dat het uittekenen van een sluitende bevoegdheidsverdeling tussen de verschillende Belgische DPA's cruciaal is. Gezamenlijke/overlappende bevoegdheden moeten hierbij zoveel mogelijk vermeden worden omdat dit tot rechtsonzekerheid leidt en omdat dit ook hoogst inefficiënt is: indien twee DPA's gezamenlijk moeten optreden – bv. naar aanleiding van een adviesaanvraag/klacht/onderzoek – impliceert dit immers dat er achterliggend twee verschillende diensten het dossier moeten analyseren en ook onderling moeten overleggen om zoveel mogelijk tot een coherent standpunt te komen. In het bijzonder in tijden van budgettaire restricties zou het de bedoeling moeten zijn om efficiëntiewinsten te realiseren en om zeker geen nieuwe inefficiënties, zoals dubbele dossiers bij verschillende diensten, te creëren. De Commissie acht het dan ook vanzelfsprekend dat aan elk van de DPA's een homogeen bevoegdheidspakket zou toebedeeld worden.

450. Indien de Commissie het Ontwerp goed begrepen heeft – wat absoluut geen evidentie is aangezien de bepalingen over de bevoegde DPA verspreid zitten over de hele tekst van het Ontwerp (en van de GBAW)– zou de bevoegdheidsverdeling tussen de vier DPA's er als volgt uit zien:

- C.O.C. wordt DPA voor[115]
  - de politiediensten;
  - de Dienst Enquêtes van het Comité P;
  - de Algemene Inspectie van de federale en lokale politie;
  - de Passagiersinformatie-eenheid,

[114] De Commissie heeft er evident alle belang bij dat er een duidelijke regeling wordt voorzien, aangezien haar rechtsopvolger – de GBA – vanaf 25 mei 2018 in dit landschap een centrale rol zal moeten opnemen.
[115] Cf artikel 31, punt 7, artikel 73, §1, artikel 248, §1, artikel 280 van het Ontwerp & Artikel 4, §2, derde lid, van de GBAW.

en dit voor verwerkingen van deze vier diensten die vallen onder Titel 2 en/of onder Afdeling 2 van Hoofdstuk IV van Titel 1 van het Ontwerp. Voor de drie eerst geciteerde diensten komen hier ook nog de verwerkingen bij die onder de AVG en de uitvoeringswetten bij de AVG vallen. Voor verwerkingen die onder de AVG vallen en die uitgevoerd worden door de Passagiersinformatie-eenheid, is dus niet het C.O.C. maar de GBA bevoegd.

- Comité I[116] wordt DPA voor
  - de inlichtingen –en veiligheidsdiensten, voor zover het verwerkingen betreft die onder Ondertitel 1 van Titel 3 van het Ontwerp vallen;
  - verwerkingen van persoonsgegevens in het kader van veiligheidsmachtigingen, attesten en adviezen (bedoeld in de wet van 11 december 1998) door vijf instanties/personen die in artikel 109 van het Ontwerp worden opgesomd;
  - De Passagiersinformatie-eenheid, voor zover het verwerkingen betreft die onder Ondertitel 5 van Titel 3 van het Ontwerp vallen.
- Comité P wordt samen met het Comité I DPA voor het OCAD[117], voor zover het verwerkingen van het OCAD betreft die onder Ondertitel 4 van Titel 3 van het Ontwerp vallen (en dit terwijl het Comité P zelf – zoals hoger aangehaald – gedeeltelijk onder het toezicht van C.O.C. valt).
- GBA[118] is DPA voor alle andere gegevensverwerkingen die niet onder de bevoegdheid van C.O.C. of Comité I of Comité P vallen (*de facto* krijgt GBA dus een residuaire bevoegdheid).

451. De Commissie is van oordeel dat deze bevoegdheidsverdeling bijzonder complex is en bovendien niet op basis van logische/objectieve criteria is uitgewerkt[119]. De regeling voor het OCAD en voor de Passagiersinformatie-eenheid vormt hier een mooie illustratie van. Het Comité I en het Comité P[120] worden met name gezamenlijk bevoegd verklaard als zijnde DPA van het OCAD en dit enkel voor de verwerkingen van het OCAD die onder Ondertitel 4 van Titel 3 van het Ontwerp vallen[121].

---

[116] Cf. artikel 97, artikel 109, artikel 130, §1, artikel 186, van het Ontwerp.
[117] Cf. artikel 163 van het Ontwerp.
[118] Cf. Artikel 4 GBAW.
[119] Hierbij worden soms zelfs argumenten gebruikt om bepaalde bevoegdheden aan een orgaan toe te wijzen, terwijl diezelfde argumenten genegeerd worden om andere bevoegdheden juist niet aan datzelfde orgaan toe te bedelen. Het C.O.C is voor de politiediensten bijvoorbeeld bevoegd voor verwerkingen die onder de Richtlijn vallen én voor de verwerkingen die onder de AVG en de uitvoeringswetten bij de AVG vallen. Op p. 129 van de Memorie wordt dit als volgt gemotiveerd: *"(…) het Controleorgaan eveneens bevoegd te maken als GBA onder meer uit eenvoud en efficiëntie naar de politiediensten toe. Zo kan vermeden worden dat deze laatste te maken zouden krijgen met twee toezichtautoriteiten (…)"* Nochtans zou het argument dat een instantie beter onder één DPA valt even goed kunnen gebruikt worden voor andere instanties die onder toezicht van het C.O.C. vallen (zoals de Passagiersinformatie-eenheid), maar voor hen geldt dit argument blijkbaar niet.
[120] En dit terwijl de Dienst Enquêtes van het Comité P zelf onder het C.O.C. valt.
[121] Artikel 163 van het Ontwerp.

Voor andere verwerkingen (bv. verwerkingen in het kader van het personeelsbeleid) van het OCAD is de GBA bevoegd[122]. Ook voor de Passagiersinformatie-eenheid zijn er potentieel drie DPA's bevoegd.

452. **Het hoeft hoe dan ook weinig betoog dat de bevoegdheidsregeling tussen de vier DPA's complex is en tot discussies tussen de DPA's zal leiden. De Commissie dringt er dan ook ten stelligste op aan dat het Ontwerp op dit punt volledig herzien zou worden.**

453. De Commissie stelt overigens vast dat de stellers van het Ontwerp kennelijk ook inzien dat een dergelijke regeling onvermijdelijk tot discussies zal leiden, aangezien pogingen worden ondernomen – zoals het afsluiten van overeenkomsten tussen de verschillende DPA's[123] – om tot werkbare oplossingen te komen. Artikel 281 van het Ontwerp bevat bijvoorbeeld ook de volgende regeling: met het oog op de consequente toepassing van de regelgeving inzake dataprotectie worden de vier DPA's uitgenodigd om nauw samen te werken wanneer dossiers overlappen en wordt ook verzocht om in een 'één loket principe' te voorzien. De Commissie gelooft niet dat dergelijke maatregelen op zich een degelijke oplossing zullen bieden en herhaalt haar pleidooi om in de eerste plaats in een duidelijke wettelijke bevoegdheidsregeling te voorzien, in het bijzonder voor de Passagiersinformatie-eenheid en voor het OCAD. Een belangrijk deel van de oplossing zou er overigens kunnen in bestaan om het aantal DPA's te reduceren (zie ook infra punt E). Een reductie tot drie DPA's zou alvast eenvoudig gerealiseerd kunnen worden door het Comité P te ontlasten van zijn slechts kleine rol van DPA (enkel voor het OCAD). De DPA-functie voor het OCAD zou immers gezamenlijk kunnen worden uitgeoefend door het Comité I en het C.O.C[124].

454. In ondergeschikte orde dringt de Commissie er ook op aan om de bevoegde DPA in het Ontwerp telkens nominatief te benoemen en om te vermijden om de algemene term "toezichthoudende autoriteit" te gebruiken (waaraan dan ook nog een vage definitie wordt gegeven[125]). Ter illustratie kan verwezen worden naar artikel 107.8 van het Ontwerp, waar de verwerkingen van persoonsgegevens door de Krijgsmacht onderworpen worden aan het toezicht van de "toezichthoudende autoriteit". Wellicht wordt hiermee de GBA geviseerd, maar om dat te weten te

[122] Artikel 280 Ontwerp.
[123] Zie bv bovenaan p. 107 van de Memorie: *"(…) Overeenkomsten tussen de verschillende toezichthoudende autoriteiten moeten worden afgesloten als het dossier wordt ingediend bij verschillende bevoegde toezichthoudende autoriteiten (…)"*
[124] Nu reeds zorgen deze twee instellingen immers voor de controle op de gemeenschappelijke gegevensbanken terrorisme en extremisme dat tot terrorisme kan leiden – waarvan het OCAD de beheerder is – en werd recent een eerste controle beëindigd.
[125] Zie bv artikel 31, punt 15 & artikel 108 in fine van het Ontwerp.

komen is een analyse nodig van minstens artikel 31, artikel 73, §1, artikel 97, artikel 109, artikel 130, §1, artikel 163 en artikel 248, §1, van het Ontwerp, wat evident niet de bedoeling kan zijn.

C. <u>De conformiteit met de DPA-vereisten in de Europese regelgeving & de coherentie met de GBAW</u>

a. <u>Het C.O.C</u>

455. De Commissie stelt vast dat de wijze waarop de hervorming van het C.O.C. in het Ontwerp is uitgewerkt, positieve elementen bevat:

- Er wordt eindelijk een duidelijke keuze gemaakt (cf. supra punt A): het C.O.C wordt DPA;
- Binnen het C.O.C. werd de voorbije jaren een zekere dataprotectie-expertise opgebouwd en in die zin is de keuze om het C.O.C. tot een volwaardige DPA om te vormen ook een begrijpelijke nieuwe stap in het hervormingstraject dat al sinds 2014 aan de gang is;
- Er wordt een eigen secretariaat opgericht, waardoor een einde zou komen aan de huidige, onlogische/moeilijk werkbare situatie waarbij het C.O.C. deels gebruik maakt van het secretariaat van de Commissie[126] [127];
- De onafhankelijkheid wordt versterkt, aangezien de leden die afkomstig zijn van de politie onder het gezag van de andere leden worden geplaatst en aangezien die leden ook slechts een minderheid (2/6) van het totaal aantal leden uitmaken.

456. **Tegelijk constateert de Commissie ook nog tal van hiaten/knelpunten/onlogische elementen in de geplande hervorming (en dit bovenop de hoger besproken problematische bevoegdheidsverdeling):**

- Het C.O.C. dient – specifiek ten aanzien van de politie – niet alleen toe te zien op de naleving van de Richtlijn, maar ook op de naleving van de AVG[128]. Dit heeft twee belangrijke implicaties waarmee in het Ontwerp geen rekening wordt gehouden:
    - Conform de artikelen 57 en 58 van de AVG dient een DPA <u>alle</u> taken en bevoegdheden te kunnen uitoefenen die in deze twee artikels worden opgesomd, wat niet het geval is voor het C.O.C. De volgende taken en bevoegdheden werden bijvoorbeeld niet in het Ontwerp voorzien[129]:

[126] Zie randnummers 11 & 12 van advies nr. 30/2015.
[127] Dit strookt overigens ook met artikel 52.5 AVG.
[128] Artikel 4, §2, derde lid, GBAW.
[129] Cf. artikel 57.1. k), m), n), o), p), q) AVG.

- Verplichte opstelling van een lijst van verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling vereist is;
- Bevorderen, adviseren en goedkeuren van gedragscodes;
- Bevorderen van certificeringsmechanismen;
- Opstellen en bekendmaken van criteria voor de accreditatie van toezichtsorganen op gedragscodes;
- Toetsing van afgegeven certificeringen;
- De corrigerende maatregelen als bedoeld in artikel 58.2. AVG.

De Commissie merkt op dat omwille van deze zware AVG-vereisten alleen al, het absurd is om het C.O.C. bevoegd te verklaren voor gegevensverwerkingen die onder de AVG vallen. Dit type van verwerkingen (het betreft bv. het HR-beheer bij politiediensten) vormt immers maar een fractie van alle verwerkingen bij de politie. De operationele verwerkingen van bv politiediensten vallen allen onder de Richtlijn en voor die verwerkingen is het daarentegen wel enigszins logisch dat het C.O.C. de bevoegde toezichthouder wordt (zie in dit verband ook infra punt E).

Maar als artikel 4, §2, derde lid GBAW, artikel 73, §1, punt 2, en artikel 280 van het Ontwerp ongewijzigd zouden blijven, dan moet het C.O.C. dus alle taken en bevoegdheden kunnen uitoefenen die in de artikelen 57 en 58 van de AVG worden opgesomd. Idealiter worden deze taken en bevoegdheden ook in de tekst van het Ontwerp opgenomen (zoals dit ook het geval is voor de GBA in de GBAW).

- Artikel 51.3. AVG schrijft voor dat – wanneer er in een lidstaat meer dan één DPA gevestigd is – de nationale wetgever moet aanduiden welke DPA in het Europees Comité voor Gegevensbescherming zetelt. Uit het Ontwerp kan echter niet worden afgeleid of de GBA dan wel het C.O.C. in dit Comité zullen zetelen. Artikel 41.4. van de Richtlijn bevat overigens een gelijkaardige bepaling als artikel 51.3. AVG, en deze wordt dus evenmin in het Ontwerp geïmplementeerd.

- De Richtlijn schrijft in haar artikelen 46 en 47 voor welke taken en bevoegdheden aan een DPA dienen toebedeeld te worden. Voor het C.O.C. werden de bevoegdheden tot het treffen van corrigerende maatregelen (Artikel 47.2. Richtlijn) vergeten[130], en wordt de Richtlijn op dit vlak aldus niet correct in nationaal recht omgezet;

[130] In artikel 279 van het Ontwerp lijken deze bevoegdheden nochtans wel aan het Comité I toebedeeld te worden.

- De Commissie neemt er akte van dat het C.O.C. verzoeken tot onrechtstreekse toegang zal behandelen op basis van artikel 46 Ontwerp en dat het tegelijk ook tot opdracht heeft om alle internationale verplichtingen uit te voeren die voortvloeien uit de taken en bevoegdheden die haar in het Ontwerp worden toebedeeld[131]. De Commissie stelt zich de vraag wat dit exact impliceert voor verzoeken tot onrechtstreekse toegang die betrekking hebben op SIS II[132]-seiningen (bv de zogenaamde artikel 24-seiningen[133]). Hetzelfde geldt voor de zgn. Schengen-evaluatie. Het lijkt logisch dat het C.O.C. hiervoor bevoegd wordt en de Commissie adviseert om deze aspecten expliciet in het Ontwerp te regelen.

- De Commissie heeft ernstige bedenkingen aangaande bepaalde voorwaarden waaraan sommige leden van het C.O.C. dienen te voldoen.

  Noch de AVG, noch de Richtlijn leggen de voorwaarde op dat DPA-leden magistraat zouden moeten zijn. Het Ontwerp legt deze vereiste nochtans wel op voor wat twee leden (waaronder de voorzitter) van het C.O.C betreft[134]. De magistraat-voorwaarde wordt naar aanleiding van onderhavige hervorming wel wat versoepeld voor wat de Voorzitter van het C.O.C. betreft, aangezien er voor deze functie geen onderscheid meer wordt gemaakt tussen zittende en staande magistratuur en dit *"teneinde het potentieel aantal kandidaten voor de functie te verhogen"*[135]. De Commissie meent dat deze redenering nog verder zou moeten doorgetrokken worden: teneinde het aantal potentiële kandidaten nog te verhogen zouden deze twee functies perfect kunnen opengesteld worden voor niet-magistraten.

  Samengevat voorzien de Europese regels voor DPA-leden twee grote voorwaarden: kennis inzake dataprotectie en onafhankelijkheid. Wat de expertise inzake dataprotectie betreft, kan worden opgemerkt dat dit een vakgebied betreft dat geen bijzondere aandacht krijgt in de opleiding tot magistraat en er zijn dan ook geen objectieve argumenten om aan te nemen dat magistraten over een grotere expertise in dit domein zouden beschikken dan personen die niet onder dit statuut vallen. Ook het feit dat de Europese regels de nadruk leggen op de onafhankelijkheid van DPA-leden, verantwoordt niet dat deze functies enkel door magistraten zouden kunnen uitgeoefend

[131] Artikel 255 van het Ontwerp.
[132] Cf. Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II).
[133] Dit artikel bevat de voorwaarden voor signaleringen met het oog op weigering van toegang of verblijf.
[134] Artikel 243, §1.
[135] P. 251 Memorie.

worden. Een expert dataprotectie kan de functie van DPA-lid in alle onafhankelijkheid uitoefenen, ongeacht of hij al dan niet het statuut van magistraat geniet. De assumptie dat een magistraat meer waarborgen zou bieden qua onafhankelijkheid, weegt in elk geval niet op tegen het feit dat dit criterium het aantal potentiële kandidaten sterk doet dalen en dat deze daling van het aantal kandidaten het andere essentiële criterium – met name expertise inzake dataprotectie – *de facto* teveel onder druk dreigt te zetten.

Ook het argument dat C.O.C.-leden quasi jurisdictionele bevoegdheden zouden hebben[136], overtuigt de Commissie overigens niet. De taken van de C.O.C.-leden zijn immers niet sterk verschillend van die van de GBA-leden en voor laatstgenoemden geldt de magistraat-vereiste niet.

Daarom is de Commissie van oordeel dat de toegang tot de functies van DPA-leden niet beperkt zouden mogen worden tot magistraten. Dit criterium verengt onnodig de groep van potentiële kandidaten en houdt het risico in dat niet de meest geschikte, onafhankelijke dataprotectie-experts toegang krijgen tot deze functie.

- De Commissie stelt vast dat het hervormde C.O.C. ook opdrachten zal vervullen die geen DPA-taken zijn, maar die eerder te maken hebben met de efficiëntie/effectiviteit van gegevensverwerkingen. In dit verband waarschuwt zij er voor dat dit risico's inhoudt: de meest efficiënte/effectieve oplossing voor een gegevensverwerking is niet noodzakelijk de meest privacy-vriendelijke en het C.O.C. zal aldus steeds moeten proberen om tot evenwichtige oplossingen te komen waarin dataprotectie centraal staat.

  En aansluitend hierbij, wijst de Commissie er ook op dat in artikel 259 van het Ontwerp – dat handelt over de aanstelling van personeelsleden die belast zijn met het beheer van de AVG – aan het C.O.C. taken worden toebedeeld die in essentie aan een verwerkingsverantwoordelijke en zijn functionaris voor gegevensbescherming zouden moeten toekomen en niet aan een DPA.

- Het aantal voltijdse mandaten bij het C.O.C. en haar Dienst Onderzoeken wordt weliswaar teruggebracht van acht naar zes, maar dat is nog altijd één voltijds mandaat meer dan bij de GBA. Het is aldus de Commissie onlogisch dat het C.O.C. meer voltijdse mandaathouders zal tellen dan de GBA, aangezien het takenpakket van het C.O.C. maar een fractie omvat van de taken van de GBA[137]. Bovendien is het aantal mandaatsfuncties (zes) in deze structuur groter dan het aantal secretariaatsmedewerkers (drie).

[136] P. 251 Memorie.

[137] Het feit dat er een opdeling wordt gemaakt tussen de leden van het C.O.C. en de leden van de Dienst Onderzoeken binnen het C.O.C. doet overigens geen afbreuk aan het feit dat het in totaal om zes voltijdse mandaten gaat.

- Het statuut van de leden van het C.O.C. wordt in het Ontwerp logischerwijze gealigneerd op dat van de GBA[138], aangezien de rol van beide instanties sterk gelijkaardig zal zijn. Deze alineëring is echter slechts partieel (functionele drietaligheid wordt bijvoorbeeld niet voorzien voor de leden van het C.O.C.). De Commissie adviseert aldus om het statuut in al zijn aspecten maximaal op dat van de GBA te aligneren.

b. Het Comité P en het Comité I

457. De Commissie constateert dat het Comité P en het Comité I tot DPA worden omgevormd[139]. Onverminderd de in punt B uiteengezette fundamentele bezwaren tegen de complexe bevoegdheidsverdeling tussen alle Belgische DPA's (zie in het bijzonder randnummer 454), heeft de Commissie hieromtrent een stuk minder inhoudelijke opmerkingen dan bij het C.O.C. en dit heeft onder andere te maken met het feit dat de toezichtsrol van beide Comités –op basis van de huidige tekst van het Ontwerp –los staat van de AVG en van de Richtlijn en dat het Verdrag nr. 108 aldus de enig toetssteen betreft. Onderhavig standpunt kan dus wijzigen, mocht in de toekomst beslist worden om aan deze organen ook een toezichtsrol toe te bedelen die betrekking heeft op gegevensverwerkingen die onder de Richtlijn of onder de AVG vallen.

458. De Commissie stelt vast dat beide Comités vandaag reeds over bevoegdheden beschikken die in lijn liggen met die van een DPA (bv onderzoeksbevoegdheden, bevoegdheid om advies te verlenen op ontwerpen van regelgeving[140]). In het Ontwerp worden daar een aantal typische DPA-taken aan toegevoegd, zoals de behandeling van verzoeken tot onrechtstreekse toegang[141] en van andere "*verzoeken*"[142]. Ook wordt expertise inzake dataprotectie een vereiste om aangesteld te kunnen worden als lid van de Comités P & I[143].

459. Verder vestigt de Commissie er de aandacht op dat de bevoegdheid van het Comité I in artikel 130, §1, eerste lid, van het Ontwerp potentieel bijzonder ruim kan geïnterpreteerd worden. Het Comité I zou met name moeten instaan voor *"(…) de controle van de verwerking van*

[138] Hierdoor zal ook terecht een einde komen aan de actuele, incoherente statutaire situatie van de leden. (Zie p. 257 Memorie en zie ook advies nr. 30/2015).
[139] Cf. supra punt B.
[140] Artikelen 9 & 33 van de wet van 18 juli 1991 *tot regeling van het toezicht op politie –en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.*
[141] Cf. Artikelen 83 & 149 van het Ontwerp.
[142] Artikel 271, tweede lid van het Ontwerp. De Commissie adviseert om het vage woord "verzoeken" te vervangen door een meer duidelijke term zoals "vragen om informatie".
[143] Artikel 266.2. van het Ontwerp.

persoonsgegevens uitgevoerd door de overheden en personen bedoeld in artikel 109, eerste lid". In artikel 109, eerste lid, van het Ontwerp worden overheden opgesomd die betrokken zijn bij de toekenning/intrekking van veiligheidsmachtigingen, attesten en adviezen zoals bedoel in de wet van 11 december 1998[144]. Deze overheden verrichten daarnaast nog andere gegevensverwerkingen en om te vermijden dat het Comité I ook voor deze verwerkingen als de bevoegde DPA wordt aanzien, kan overwogen worden om artikel 130, §1, eerste lid, van het Ontwerp als volgt te formuleren: *"(…) de controle van de verwerking van persoonsgegevens in het kader van artikel 109, eerste lid, door de overheden en personen bedoeld in hetzelfde artikel".*

D. Besluit: ongunstig advies

1. Gelet op de hoger geschetste problemen, verleent de Commissie een **ongunstig advies** op de bepalingen van het Ontwerp die betrekking hebben op de drie nieuwe DPA's[145], gelet op het feit dat:

- de bevoegdheidsverdeling tussen de 4 federale DPA's chaotisch en volstrekt onlogisch geregeld is (cf. supra punt B);
- de hervorming van het C.O.C. niet ver genoeg gaat en op sommige punten niet conform is aan de Europese regels (cf. supra punt C.a. en infra punt E);

460. Infra onder punt E schuift de Commissie twee alternatieve pistes naar voor om toch tot een Belgisch dataprotectie-landschap te kunnen komen dat logisch en efficiënt geordend is.

E. Voorstellen van oplossing

461. De Commissie maakt zoals – hoger aangehaald – evident geen beleidskeuzes, maar zij ziet het wel als haar plicht om de aanvrager zo goed mogelijk te adviseren over alle voor –en nadelen die aan bepaalde beleidsopties verbonden zijn. Na analyse van de bepalingen in het Ontwerp betreffende de hervorming van het C.O.C, het Comité P & het Comité I, en de bevoegdheidsverdeling tussen de vier DPA's, maakt zij zich – zoals hoger aangehaald – grote zorgen over de werkbaarheid van deze voorgestelde regeling en over haar conformiteit met de Europese rechtsnormen. Aangezien het Ontwerp de grootste hervorming van het privacy-landschap in jaren omvat (die bovendien tegen 25 mei 2018 een feit zou moeten zijn) en aangezien haar

[144] Wet van 11 december 1998 *betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.*
[145] Zie in hoofdzaak artikelen 73, 97 t.e.m. 100, 107.8, 130 t.e.m. 133, 163, 186 & Titel 7 & Titel 8 van het Ontwerp.

rechtsopvolger – met name de GBA – een centrale rol zal opnemen in dit landschap, neemt zij zich de vrijheid om twee alternatieve oplossingen voor te stellen.

462. Het eerste voorstel van de Commissie is meteen het meest eenvoudige en het meest efficiënte. Het is ook de oplossing die in quasi alle andere Europese landen wordt gekozen. Er zou met name kunnen voor geopteerd worden om geen bijkomende DPA's op te richten en de GBA aldus de volheid van bevoegdheid te verlenen. Hiermee zouden de hoger geschetste knelpunten volledig worden vermeden. Dit voorstel zou ook als voordeel hebben dat de toezichtstaken – en dus ook de expertise – inzake dataprotectie binnen één organisatie gecentraliseerd zouden worden. In deze hypothese dient wel nog een gepaste oplossing gevonden te worden voor het bestaande C.O.C, dat zoals hoger gezegd hoe dan ook 'gewrongen' zit tussen de taken en bevoegdheden van de Commissie en van het Comité P.

463. De Commissie ziet ook een tweede mogelijke oplossing, die volgens haar eveneens werkbaar kan zijn, op voorwaarde dat ze goed is uitgewerkt: de GBA enkel laten toezien op verwerkingen die onder de AVG (en de nationale uitvoeringsbepalingen bij de AVG) vallen en een tweede DPA oprichten die bevoegd is voor alle andere gegevensverwerkingen, met name (in hoofdzaak) de verwerkingen die in artikel 2, tweede lid, en in Titels 2 & 3 van het Ontwerp geviseerd worden, behalve de verwerkingen bij de gerechtelijke overheden. Op die manier wordt de Europese logica (opdeling AVG - Richtlijn) gerespecteerd, wordt expertise op een meer logische/efficiënte manier gecentraliseerd dan vandaag in het Ontwerp het geval is, dient ook niet noodzakelijk aan de regelgeving op het Comités P & I geraakt te worden, en kunnen de bevoegdheidsdiscussies tussen Belgische DPA's tot een minimum beperkt worden[146].

464. Laatstgenoemd voorstel zou ook als voordeel hebben dat er tegelijk een oplossing wordt gevonden voor het C.O.C. Het C.O.C. heeft immers een plaats verworven in het nationale institutionele landschap en het heeft ook een zekere dataprotectie-expertise opgebouwd. Maar het mist vandaag een homogeen/logisch takenpakket, gelet op de overlappende bevoegdheden met het Comité P en met de Commissie (toekomstige GBA). Na een nog meer doorgedreven hervorming dan wat in het Ontwerp wordt voorgesteld[147] — zou het C.O.C. de taak van de tweede Belgische DPA kunnen opnemen. Deze hervorming van het C.O.C. zou aldus de Commissie kunnen gerealiseerd worden door:

[146] In deze constellatie zullen er wel nog bevoegdheidsproblemen blijven opduiken, maar de omvang ervan zal veel beperkter zijn dan het kluwen dat in de huidige tekst van het Ontwerp gecreëerd wordt.
[147] Zoals dat overigens ook in de GBAW gebeurde voor de Commissie.

- Artikel 73 en Titel 7 van het Ontwerp als vertrekbasis te nemen en
- de bevoegdheden van het C.O.C te herijken – wat zowel een uitbreiding als een kleine beperking van haar geplande bevoegdheden impliceert[148] - tot alle verwerkingen die in artikel 2, tweede lid, en in Titels 2 & 3 van het Ontwerp geviseerd worden, behalve de verwerkingen bij de gerechtelijke overheden, en
- de opmerkingen te implementeren die hoger in punt C.a. gemaakt worden, en
- erover te waken dat deze DPA ook de nodige expertise in huis heeft om eveneens te kunnen toezien op de gegevensverwerkingen door de inlichtingendiensten (en door meer reguliere overheidsdiensten, zoals de Douane[149]).

465. De Commissie is er overigens van overtuigd dat dit de enige twee valabele pistes zijn om tot een Belgisch data-protectie-landschap te komen dat logisch en efficiënt geordend is. Alle andere scenario's – zoals bijvoorbeeld de regeling die wordt voorzien in het Ontwerp – zullen onherroepelijk leiden tot

- bevoegdheidsproblemen;
- een versplintering van expertise;
- complexe dossierbehandeling;
- divergenties in de rechtspraak.

CONCLUSIE van de Commissie over titel 7 van het ontwerp

466. De Commissie een ongunstig advies op de bepalingen van het ontwerp die betrekking hebben op de drie nieuwe DPA's omwille van de hierboven aangehaalde redenen en in het bijzonder gelet op het feit dat:

- de bevoegdheidsverdeling tussen de 4 federale DPA's chaotisch en volstrekt onlogisch geregeld is;
- de hervorming van het C.O.C. niet ver genoeg gaat en op sommige punten niet conform is aan de Europese regels;

De Commissie nodigt de aanvrager uit om de twee alternatieve pistes die zij naar voor schuift ernstig te overwegen om toch tot een Belgisch dataprotectie-landschap te kunnen komen dat logisch en efficiënt geordend is.

[148] De enige beperking van de bevoegdheden van het C.O.C., betreft de schrapping van artikel 4, §2, derde lid, van de GBAW en van de artikelen 73, §1, punt 2, en 280, van het Ontwerp, aangezien het C.O.C. AVG-bevoegdheden toebedeeld kreeg en dit enkel voor vier instanties. Deze bevoegdheid zou moeten geschrapt worden en deze diensten zouden – enkel voor wat de verwerkingen betreft die onder de AVG vallen (bv voor HR-verwerking, wat slechts een fractie vormt van alle gegevensverwerkingen door deze diensten) – voor dat luik aldus onder toezicht van de GBA komen te vallen (cf. supra punt C.a.).
[149] Cf. artikel 31, punt 7, punt e), van het Ontwerp.

11. BESLUIT

OM DEZE REDENEN,

Brengt de Commissie een advies uit in overeenstemming met haar afzonderlijke eindconclusies voor elkeen van de titels van het voorliggende ontwerp. Dit houdt in:

- M.b.t. de voorafgaande titel van het ontwerp een **ongunstig** advies omwille van de redenen uiteengezet in randnummer 87;
- M.b.t. titel 1 van het ontwerp een **ongunstig** advies voor hoofdstuk drie en een **gunstig** advies voor de overige hoofdstukken op voorwaarde dat de opmerkingen vermeld in randnummer 192 integraal worden opgenomen;
- M.b.t. titel 2 van het ontwerp een **ongunstig** advies voor de afbakening van het toepassingsgebied en een **gunstig** advies voor de overige bepalingen op voorwaarde dat de opmerkingen vermeld in randnummer 226 integraal worden opgenomen;
- M.b.t. titel 3 van het ontwerp een **ongunstig** advies over de artikelen 78 en 112 van het ontwerp en een **gunstig** advies voor de overige bepalingen op voorwaarde dat de opmerkingen vermeld in randnummers 242 en 254 integraal worden opgenomen;
- M.b.t. titel 4 een **ongunstig** advies over de hele lijn (zie randnummer 389);
- M.b.t. titel 5 een **ongunstig** advies over de lacunes in geval van dreiging van ernstige inbreuk en wat betreft de administratiefrechtelijke bevoegdheid voor de beslissing om in rechte op te treden en een **gunstig** advies voor de overige bepalingen op voorwaarde dat de opmerkingen vermeld in randnummer 414 integraal worden opgenomen;
- M.b.t. titel 6 een **ongunstig** advies over de hele lijn (zie randnummer 445);
- M.b.t. titel 7 een **ongunstig** advies over de hele lijn (zie randnummer 466).

Gelet op het grotendeels ongunstige karakter van haar advies herhaalt de Commissie dat zij zich ter beschikking houdt van de aanvrager om dit ontwerp grondig bij te sturen om te komen tot een kaderwet die de *ratio legis* van de AVG en de Richtlijn respecteert en bijdraagt tot een transparant, coherent en daadkrachtig privacyregime in België.

De Wnd. Administrateur, De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere

Avis n° 33/2018 du 11 avril 2018

Objet: Avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (CO-A-2018-026)

La Commission de la protection de la vie privée (ci-après la Commission) ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après RGPD) ;

Vu la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après la Directive) ;

Vu la demande d'avis de monsieur Philippe De Backer, secrétaire d'Etat à la Lutte contre la fraude sociale, à la Protection de la vie privée et à la Mer du Nord, reçue le 20 mars 2018;

Vu le rapport du Président ;

Émet, le 11 avril 2018, l'avis suivant

SOMMAIRE

LEXIQUE

APD	L'Autorité de protection des données, instituée par la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*
Commission	La Commission de la protection de la vie privée
CEDH	La Convention européenne des droits de l'homme
Cour EDH	La Cour européenne des droits de l'homme
PIDCP	Le Pacte international relatif aux droits civils et politiques
CJUE	La Cour de Justice de l'Union Européenne
C.O.C.	L'Organe de contrôle de l'information policière
Comité P	Le Comité permanent de contrôle des services de police
Comité R	Le Comité permanent de contrôle des services de renseignements et de sécurité
LVP	Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel
LAPD	La loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*
RGPD	Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE
Richtlijn	La Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil
Projet	Le présent projet de loi soumis à la Commission
Avis	Le présent avis rendu par la Commission
DPIA	L'analyse d'impact relative à la protection des données dans le sens de l'article 35 RGPD - appelée en anglais Data Protection Impact Assessment (DPIA).
DPO	Le délégué à la protection des données dans le sens de l'article 37 RGPD – aussi appelé en anglais Data protection Officer (DPO).
Le Groupe 29	Le Groupe de travail de l'Article 29 sur la protection des données. Le groupe comprend les contrôleurs nationaux des Etats membres de l'Union Européenne et émet des avis sur l'application de législation européenne en matière de protection de la vie privée. Le 25 mai 2018, le Comité européen de la protection des données remplacera le Groupe 29.

1. INTRODUCTION

1. Le présent avis porte sur l'avant - projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après le Projet).

2. Il a été soumis officiellement pour avis à la Commission de la protection de la vie privée (ci-après, la Commission) le 20 mars 2018.

3. Le Projet s'inscrit dans la réforme de la règlementation de la protection des données à caractère personnel consécutive à l'adoption, le 27 avril 2016, du *Règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après le RGPD) et de la *Directive (UE) 2016/680/UE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil* (ci-après la Directive) .

4. Ces deux textes entrés en vigueur respectivement les 24 mai 2016 et 5 mai 2016 prévoient chacun une période de transitoire de 2 ans.

5. Ainsi le RGPD sera d'application dans quelques semaines, soit le 25 mai 2018. La Directive doit quant à elle être transposée d'ici au 6 mai 2018.

6. Le Secrétariat de la Commission a eu l'occasion de formuler certaines suggestions dans la phase préliminaire de la préparation du Projet.

La Commission n'en regrette pas moins de devoir donner son avis sur un texte d'une telle ampleur et importance pour l'encadrement des données à caractère personnel dans un délai extrêmement court.

7. La Commission forme le vœu que cet avis, aussi critique soit-il, permette une amélioration du texte et demeure à la disposition du demandeur pour collaborer à la réalisation de cet objectif.

8. S'agissant du RGPD, nonobstant sa nature de règlement, il prévoit un certain nombre d'hypothèses dans lesquelles le législateur national doit ou peut, selon le cas, intervenir, le cas échéant dans les seules limites autorisées par la clause d'ouverture.

9. Ces clauses d'ouverture sont de plusieurs ordres. Certaines d'entre-elles autorisent le législateur à spécifier l'application du RGPD, d'autres à prévoir des mesures d'exécution dans les limites des options qu'elles prévoient, d'autres encore à prévoir des mesures d'exécution visant à compléter le RGPD. Dans chacun des cas ces mesures ne peuvent contrevenir au RGPD. Elles doivent être notifiées à la Commission européenne, pour la plupart d'ici au 25 mai 2018.

10. Quant à la Directive, elle doit être transposée dans le délai légal prévu, soit pour le 6 mai 2018 déjà mentionné. De manière générale, la Commission souligne que dans une très grande proportion, le texte de la Directive est aligné sur celui du RGPD tout en tenant compte des spécificités liées au champ d'application propre à la Directive, soit les traitements de données opérés à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales par les autorités compétentes.

11. Dans son travail de proposition et d'adoption des mesures d'exécution et de transposition de ces deux textes européens, le législateur est tenu de respecter la philosophie qui les sous-tend, l'orientation voulue par l'encadrement européen et, bien entendu, la lettre de ces textes qui priment du point de vue de la hiérarchie des normes ainsi que les principes généraux de la protection des données et ceux de l'état de droit.

12. Le législateur indique qu'il ne se limite pas à proposer des mesures d'exécution ou de transposition des textes européens susvisés, mais qu'il y ajoute également des « dispositions particulières ».

13. Il n'en demeure pas moins que l'encadrement de la protection des données en Belgique doit s'inscrire dans le respect des textes européens et former un tout cohérent et à même de garantir une protection effective du droit fondamental à la protection des données.

Lignes de forces du RGPD et de la directive

14. Les lignes de force de la réforme UE de l'encadrement de la protection des données sont rappelées ci-dessous. C'est aussi à l'aune de celles-ci que la Commission a examiné les dispositions prévues par le Projet et formulé le présent avis:

- Harmonisation : s'agissant du RGPD, le législateur européen a choisi l'instrument juridique qui permet l'harmonisation la plus forte, soit un Règlement (RGPD) et non plus une directive comme il l'avait fait en 1995. Dans cette même optique, il opte aussi pour une longue liste de définitions harmonisées. Enfin, le législateur européen opte pour un régime de protection commun au secteur privé et au secteur public tout en laissant au législateur national la possibilité de spécifier l'application du texte pour le secteur public, et ce, dans les limites du RGPD.

- Le renforcement des droits des personnes concernées est central dans la réforme. Ces droits doivent permettre aux personnes concernées une réelle maîtrise informationnelle et une protection effective dès que des traitements de données les concernant sont opérés. Le droit à l'information de la personne concernée, préalable indispensable à l'exercice de ses autres droits, est renforcé. Le renforcement de ce droit participe à l'objectif général de transparence accrue également ancré dans le texte. Le droit à l'effacement est développé de même que le droit à la limitation du traitement. Dans le même esprit, les exigences entourant le recours au consentement en tant que base de licéité du traitement de données sont également renforcées. En outre, ce renforcement des droits découle également de certaines nouvelles obligations introduites par le RGPD comme la protection des données dès la conception et protection des données par défaut (article 25 RGPD). Finalement le RGPD offre aux personnes concernées de nouvels instruments pour agir en justice – comme la représentation collective au sens de l'article 80 RGPD – dans le but de renforcer la protection juridique des citoyens et faire valoir le respect de leur droits devant les cours et tribunaux.

- Suppression de certaines formalités préalables – Accountability : la suppression des formalités préalables vis-à-vis de l'autorité de protection des données va de pair avec le principe de responsabilité (accountability) développé dans les textes. Le responsable de traitement est tenu de respecter le RGPD et doit être en mesure de démontrer ce respect. La suppression de la déclaration préalable de traitement est emblématique de ce changement de paradigme. Elle n'a pas été supprimée à la légère mais bien parce qu'elle ne remplissait, en pratique, ni les objectifs de transparence, ni ceux de réflexion et de responsabilisation qui lui avaient été assignés en 1995.

- Des obligations nouvelles pour les responsables de traitement et les sous-traitants – Approche par le risque : de nouvelles obligations sont mises à charge des responsables de traitement et des sous-traitants telles que la tenue d'un Registre des activités de traitement (art. 30 du RGPD), un encadrement plus strict du recours à la sous-traitance et à la sous-traitance ultérieure (art. 28 du RGPD), la désignation d'un délégué à la protection des données (art. 37 du RGPD), la réalisation d'une analyse d'impact en matière de protection des données (art. 35 du RGPD - DPIA) ou encore la notification des violations de données à l'autorité et de protection des données et leur communication à la personne concernée (art. 33-34 du RGPD). Certaines de ces obligations ne s'appliquent que lorsque un risque (élevé) est lié au traitement ou à l'incident. Ces obligations sont également conçues pour aider les responsables de traitement et les sous-traitants à être en conformité avec les textes.

- Renforcement des pouvoirs de l'autorité de protection des données : l'abandon de la plupart des formalités préalables auprès de l'autorité de contrôle et le principe d'accountability s'accompagnent d'un renforcement des pouvoirs de l'autorité de contrôle, en particulier de ses

pouvoirs correctifs, parmi lesquels la possibilité d'exiger la suspension ou l'interdiction de traitements de données et celle d'imposer des amendes administratives dissuasives. Une action résolument tournée vers le contrôle *a posteriori* est attendue des autorités de contrôle. Son rôle de sensibilisation du public en général et celui d'information des responsables de traitement et sous-traitants quant à leurs obligations n'en demeurent pas moins essentiels.

- Renforcement de la coopération internationale : dans un contexte mondialisé, les traitements de données opérés par des entreprises multinationales notamment établies dans plusieurs Etats membres de l'Union sont toujours plus nombreux. Des investigations conjointes ainsi qu'une assistance mutuelle entre autorités de protection des données de l'Union européenne sont encadrées par le RGPD, pour une action plus efficace vis-à-vis de ces acteurs. Le choix d 'un règlement destiné à garantir une protection harmonisée en pratique s'accompagne en outre de la mise sur pied d'un mécanisme dit « de la Cohérence » aux termes duquel les autorités de protection des données doivent se mettre d'accord selon des procédures établies dans le RGPD sur une interprétation et une application harmonisées des dispositions du RGPD. Cette coopération s'opérera, à dater du 25 mai 2018 au sein du Comité Européen de la Protection des Données (CEPD) au sein duquel une autorité de contrôle nationale désignée à cet effet doit siéger.

15. Les lignes de force de la Directive s'apparentent à celles du RGPD, tenant compte, comme déjà indiqué, des spécificités de son champ d'application.

les services de renseignements et de sécurité

16. Le Projet ambitionne d'encadrer l'ensemble des traitements de données opérés, en ce compris ceux qui ne tombent pas dans le champ d'application du droit de l'Union européenne. C'est notamment le cas des traitements opérés par « les services de renseignements et de sécurité », soit par la Sûreté de l'Etat et le Service général du Renseignement et de la Sécurité . Cet encadrement est prévu au Titre III du Projet. Dans ces domaines également, il existe un consensus international pour renforcer l'encadrement de la protection des données. En effet, un projet de modernisation de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108) est sur la table du Comité des ministres du Conseil de l'Europe. Sans avoir été formellement adopté par les Etats Parties à ce jour , ce texte recueille quant au fond l'assentiment du plus grand nombre. Il intègre à sa manière (il s'agit d'une Convention internationale et non d'un règlement directement applicable) les lignes de force rappelées ci-dessus que l'on trouve dans le RGPD et la Directive.

Méthodologie de l'avis

17. D'un point de vue méthodologique , le présent avis suit généralement la structure du Projet, Titre par Titre. Au regard de chacun des Titres, l'analyse est présentée, selon les besoins de l'avis et

les préoccupations que soulève le Projet dans le chef de la Commission, article par article de manière détaillée ou de manière plus globale. Le cas échéant, l'analyse de chacun des Titres s'achève par une appréciation globale de la Commission sur le Titre et sur une liste de remarques et demandes adressées au législateur. L'analyse du Titre 7 couvre également d'autres articles dispersés ailleurs dans le projet.

18. Les remarques formulées au regard de ce Titre 7 sont essentielles en ce qu'elles portent sur l'effectivité du contrôle par les autorités de protection des données mises sur pied, dont la future Autorité de protection des données, successeur en droit de la Commission

2. SYNTHESE GENERALE

Remarque préalable

19. La présente synthèse se limite à lister les préoccupations majeures de la Commission, ses points d'alerte principaux. Même si elle comporte un certain nombre de renvois, la lecture de cette synthèse doit s'accompagner d'une lecture approfondie de l'avis dans son intégralité pour une appréciation globale du Projet.

Objectif du Projet

20. Le Projet est un texte ambitieux qui vise à la fois à exécuter le RGPD (Titre I), transposer la Directive (Titre II), encadrer les traitements de données non couverts par l'encadrement UE de la protection des données (Titre III) et prévoir des dispositions particulières. La Commission relève que s'agissant d'un Règlement, seules les dispositions pour lesquelles une ouverture a été laissée au législateur national par le législateur européen peuvent être complétées par des dispositions du présent projet et ce, dans les limites autorisées le cas échéant par le RGPD. Dans son analyse, la Commission y a été particulièrement attentive..

21. Comme mentionné, le législateur poursuit également l'objectif d'ajouter des dispositions particulières. La Commission est d'avis que toutes n'ont pas leur place dans le Projet. Elles doivent en tout état de cause, si elles s'appuient sur des concepts du RGPD, en respecter la nature et l'objectif.

Champ d'application et définitions

22. L'analyse des différents Titres met en évidence la nécessité d'en clarifier le champ d'application précis.

23. La Commission salue la tentative du législateur de tenter de prévoir dans le texte du Projet une solution aux situations de conflit de loi susceptibles de se présenter (article 4 du Projet). En effet, dès lors que le RGPD prévoit à plusieurs articles la possibilité pour le législateur national de venir spécifier ou compléter le cadre règlementaire européen qu'il propose, la question de savoir quel sera le droit national applicable doit trouver une réponse qui garantisse une sécurité juridique. La Commission est d'avis que la solution préconisée par le Projet n'est pas suffisamment solide et n'apporte pas de réelle solution. La Commission formule une suggestion alternative dans le présent avis.

24. Quant aux définitions, lesquelles participent à la construction d'un encadrement cohérent, le Projet prévoit que les définitions du RGPD sont d'application *« sans préjudice des définitions prévues dans la présente loi »* (art. 5). Cette incise porte à confusion dans la mésure ou elle semble être en contradiction avec la primauté du droit international pour les titres auxquels le RGPD et la Directive s'appliquent. A cet égard, l'avis souligne que le Titre 4 consacré aux traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques introduit une série de définitions dont certaines s'écartent de celles du RGPD. La Commission demande la suppression de ces définitions. De manière générale, une cohérence globale doit être préservée au regard des définitions (en ce compris, dabns la mesure du possible, pour les traitements visés au Titre III qui ne sont pas couverts par le droit de l'Union).

    La Commission ne s'oppose par contre pas à l'introduction de nouvelles définitions qui viennent éclairer une notion non définie par le RGPD et pour laquelle il est renvoyé au droit national ou lorsque la définition de termes non définis introduite est incontestable et de nature à augmenter la sécurité juridique.

25. Quant à la création de différentes « autorités de contrôle » la Commission est d'avis que leurs compétences respectives doivent être délimitées de manière claire et juridiquement cohérente de manière à leur permettre d'effectuer elurs missions de manière effective et efficace.

<u>Des restrictions, injustifiées ou contraires au RGPD, aux droits des personnes concernées</u>

26. La Commission fait le constat que le Projet contient de nombreuses restrictions aux droits des personnes concernées parmi lesquelles un grand nombre lui apparaissent injustifiées et contraires au RGPD. La Commission rappelle , comme elle l'a faut en introduction qu'un des axes majeur de la réforme européenne est précisément le renforcement de ces droits.

27. L'article 85.2. du RGPD « Traitement et liberté d'expression et d'information » autorise le législateur national à prévoir des exemptions ou des dérogations au Chapitre III du RGPD consacré aux droits des personnes concernées *si et dans la mesure où* celles-ci sont nécessaires pour *concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information*. La Commission est d'avis que les limitations prévues aux articles 18 (droit à la limitation du traitement) et 21 (droit d'opposition) du RGPD sont injustifiée dès lors que la mise en balance du droit à la protection des données et de la liberté d'expression et d'information ne requiert pas de dérogation de principe à l'exercice de ces droits. S'agissant du droit à l'effacement, la Commission est opposée à l'affirmation reprise dans l'exposé des motifs selon laquelle ce droit ne serait pas applicable aux traitements à des fins de liberté d'expression et d'information.

28. L'article 89 du RGPD « Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques » autorise également les Etats membres à prévoir des dérogations aux droits visés aux articles 15, 16, 18 et 21, sous réserve des conditions et garanties visées à l'article 89.1. *dans la mesure où* ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et *où de telles dérogations sont nécessaires pour atteindre ces finalités* d'archivage dans l'intérêt public, de recherche scientifique ou historique ou statistique. La Commission est ici aussi d'avis que les dérogations apportées par le Projet aux droits des personnes concernées au Titre 4 sont contraires au RGPD.

29. Outre les articles susvisés et les dérogations prévues le cas échéant au regard de chacun des droits dans l'article qui leur est consacré, l'article 23 du RGPD autorise les Etats membres à limiter, par la voie de mesures législatives, notamment la portée des droits prévus aux articles 12 à 22 du RGPD. Une telle limitation doit respecter l'essence des libertés et droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique pour un des motifs listés au dit article tel que la sécurité nationale ou la défense nationale pour ne citer que deux des dix motifs retenus. Telle mesure législative doit contenir au minimum les éléments listés à l'article 23.2. du RGPD (soit, notamment, l'identification des finalités du traitement, des catégories de données à caractère personnel les garanties destinées à prévenir les abus etc.). Ces éléments font défaut dans les dispositions qui s'appuient sur l'article 23.1. du RGPD dans le Projet. Partant, la Commission est d'avis que ces dérogations ne respectent pas les exigences de l'article 23.2. du RGPD quant à la qualité de la mesure législative autorisant la dérogation.

30. S'agissant du traitement des données relatives à la santé, génétiques et biométriques, la Commission regrette que le Projet ne s'appuie pas sur l'article 9.4. du RGPD pour conserver les garanties d'encadrement additionnelles prévues par le cadre légal belge actuel et conserver ainsi un niveau de protection équivalent à celui aujourd'hui en application au bénéfice de la protection des personnes concernées.

31. *Quant au voies de recours* (Chapitre VIII du RGPD), lesquelles viennent compléter les droits des personnes concernées, la Commission regrette que le législateur n'ait pas souhaité faire bénéficier les personnes concernées de moyens d'action indirects effectifs pourtant autorisés par le RGPD en exécutant l'article 80.2. du RGPD.

32. Cette disposition donne en effet aux Etats membres la possibilité de prévoir que tout organisme, organisation ou association visé à l'article 80.1. indépendamment de tout mandat confié par une personne concernée, a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle qui est compétente en vertu de l'article 77, et d'exercer les droits

visés aux articles 78 et 79 s'il considère que les droits d'une personne concernée prévus dans le présent règlement ont été violés du fait du traitement.

33. En application de l'article 58.5. du RGPD, chaque Etat membre prévoit par la loi que son autorité de contrôle a le pouvoir de porter toute violation du règlement à l'attention des autorités judiciaires et, le cas échéant d'ester en justice en vue de faire appliquer le règlement. Pour permettre une introduction juridiquement valable de tels recours, la Commission est d'avis qu'il est indispensable que le législateur complète la Loi du 3 décembre 2017 par une disposition précisant qu'il appartient au Comité de direction de l'APD de prendre la décision de tels recours. A défaut, toute action de l'APD risquerait d'être contestée quant à sa recevabilité. Indirectement, les personnes concernées se verraient ainsi privées d'un autre moyen de protection en justice.

34. Dans le même ordre d'idée, la Commission demande que la distinction juridique entre la partie au recours (soit l'APD) et le pouvoir de représentation de celle-ci soit clairement faite.

35. Toujours dans le but de permettre une protection effective des personnes concernées, la Commission demande au législateur de prévoir la possibilité de l'introduction d'un recours pour empêcher un manquement grave à la réglementation sur le point de se produire sur le modèle du recours prévu à l'article 1er de la loi du 12 janvier 1993 concernant un droit d'action en matière de protection de l'environnement.

36. Enfin, l'absence d'amendes administratives applicables au secteur public alors même que l'article 83.7. du RGPD autorise le législateur à *« établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire »* , combinée à l'immunité pénale de certaines personnes morale de droit public (art. 84 du RGPD) et à des dérogations – dont certaines sont critiquée dans le présent avis (voy. notamment l'article 3 du Projet) - place le secteur public dans une position privilégiée, en rupture avec le principe d'égalité avec les autres responsables de traitements et sous-traitants du « secteur privé ». S'il est vrai que la Commission dispose d'autres formes de pouvoirs correctifs à l'égard du dit secteur public, il n'en demeure pas moins que l'effectivité de son action s'en trouvera nécessairement déforcée.

Respect des articles 5.2 du RGPD et de l'article 24 du RGPD

37. Le principe de responsabilité est au cœur du RGPD. Il est énoncé à l'article 5.2. dans les termes suivants : le responsable de traitement est responsable du respect du paragraphe 1 (principes relatifs au traitement de données à caractère personnel) et est en mesure de démontrer que celui-ci est respecté (responsabilité).

38. L'article 24 dispose quant à lui que compte tenu d'un certain nombre de facteurs, dont la nature, la portée, la finalité du traitement mais aussi des risques pour les droits et libertés des personnes, le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD.

39. A plusieurs endroits du Projet, des dispositions contreviennent à cet article 24 du RGPD (l'article 3 du Projet est à cet égard particulièrement problématique). Par contre, la Commission salue la mise en place d'un système d'encadrement des transmissions de données à caractère personnel par les « *autorités publiques fédérales et les organismes public fédéraux* » , par le biais de protocoles d'accord à adopter par les responsables de traitement concernés, après avis de leurs délégués à la protection des données (DPO) respectifs. Cela pourrait constituer un bon outil d'accountability pour les responsables de traitement concernés. La Commission est toutefois d'avis que le système devrait être rendu obligatoire pour les seuls traitements présentant un risque, dans la lignée de l'approche par le risque qui sous-tend certaines obligations du RGPD. Outre certaines améliorations qui sont proposées, ces protocoles doivent par ailleurs être rendus publics.

<u>Des restrictions injustifiées aux obligations des responsables de traitement et sous-traitants</u>

40. Le Projet prévoit dans son Chapitre consacré aux traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire des exemptions au respect de certaines obligations imposées par le RGPD en faveur des responsables de traitements et des sous-traitants (mise à disposition du Registre des traitements de données à l'autorité de protection des données, obligation de collaborer avec elle, obligation de notification des fuites de données, obligation de consultation de l'APD pour les études préalables d'impact sur la protection des données réalisées dont il ressort que le risque résiduaire du traitement concernés reste élevé, dérogations au chapitre sur les flux transfrontaliers de données).

41. En ce qui concerne l'exemption à l'obligation de mise à disposition du Registre des activités de traitement sur demande de l'APD (article 30.4 du RGDP), la Commission ne l'estime pas nécessaire et donc contraire au RGPD ; en effet, le RGDP ne requiert pas du Registre qu'il contienne l'identité des personnes concernées par le traitement des données. La mise en balance des deux droits fondamentaux précités ne justifie donc pas cette exemption. Il en est de même pour les articles 33 (notification des violations (fuites) de données) et 36 (consultation préalable de l'APD pour les DPIA). En aucun cas, l'exécution de ces obligations ne doit amener à dévoiler à l'autorité de protection des données le contenu d'un article de presse en cours de publication.

Des obligations complémentaires à celles du RGPD pour les responsables de traitement et les sous-traitants en contradiction avec l'objectif sous-jacent de ces obligations dans le RGPD

42. *Délégué à la protection des données* - L'article 37.4. du RGPD permet au législateur national d'ajouter des cas dans lesquels la désignation d'un délégué à la protection des données (DPO) est obligatoire. L'article 37.1. du RGPD liste trois hypothèses dans lesquelles cette désignation est obligatoire en application du RGPD. Ces 3 cas peuvent donc être complétés selon la volonté du législateur national. La Commission relève que les deux hypothèses complémentaires de désignation obligatoire d'un délégué à la protection des données prévues aux articles 25 et 191 du Projet s'écartent de la philosophie de l'approche par le risque du RGPD. En effet, les hypothèses de désignation obligatoire d'un délégué à la protection des données à l'article 37.1. – dont l'action contribue assurément à la mise en oeuvre effective du RGPD - sont liées à un facteur de risque (traitement de données sensibles, de suivi du comportement des personnes, grande échelle, activités de base). Par contre, les hypothèses nouvelles prévues dans le Projet sont justifiées par le simple fait de la finalité de la réalisation de traitements à des fins d'archives dans l'intérêt public, ou de recherche ou de statistique quelle qu'elle soit (art. 191 du Projet) ou du recours à un sous-traitant pour les autorités publiques (l'article 25 du Projet vise toutes les personnes morales de droit privé intervenant comme sous-traitant des organismes fédéraux publics ou privés susvisés et/ou collectant auprès d'eux des données à caractère personnel) alors même qu'elles-mêmes sont tenues à la désignation obligatoire d'un délégué à la protection des données. Cette dernière circonstance n'exclut pas, que le sous-traitant doive l'être également s'il tombe dans les cas visés à l'article 37.1. du RGPD. La Commission est toutefois d'avis qu'en faire une obligation généralisée est excessif.

43. *Registre des activités de traitement* - La Commission relève aussi que l'obligation – c'est à tout le moins sa compréhension des dispositions du Titre I à cet égard - de participation à un Registre centralisé des traitements opérés dans le secteur public et rendu accessible à la personne concernée ne constitue pas à proprement parler une mesure d'exécution du RGPD. L'objectif de transparence est louable sur le plan du principe mais ne peut se confondre avec l'obligation de tenir un Registre interne des activités de traitement prévu à l'article 30 du RGPD. Cette obligation additionnelle prévue par le Projet s'écarte de l'objectif du Registre qui n'est pas destiné à informer directement les personnes concernées et crée dans le chef de la Commission le sentiment que l'obligation de déclaration préalable des traitements de données auprès de l'autorité de contrôle est en quelque sorte réintroduite alors même que sa suppression a fait l'unanimité et ne cadre plus avec le principe d'accountability consacré dans le RGPD. En effet, cette obligation de déclaration préalable ne remplissait, de l'avis de tous, ni son objectif de transparence à l'égard des personnes concernées, ni celui de la prise de conscience et sa traduction par des mesures concrètes pour se conformer aux règles de protection des données auprès des responsables de

traitement. Elle constituait une charge administrative lourde sans rencontrer ses objectifs. C'est au regard de la transparence administrative qu'un système de publicité active devrait être mis en place pour réduire l'opacité des transmissions de données à caractère personnel entre administrations. Une proposition est faite à ce sujet.

Quant au Titre IV consacré aux traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

44. L'appréciation de la Commission sur le Titre IV est défavorable pour l'entièreté de ce titre. La Commission est en effet d'avis que les dispositions qui y sont prévues sont contraires au RGPD. Elles sont de surcroît de nature à restreindre les activités de recherche et de statistique qui ne sont pas réservées aux seules universités ou autres centres de recherche mais sont plus généralement opérés par tout type de structure, quelle qu'en soit la taille ou l'activité de base.

Autorités de contrôle nationales

- ✓ De oprichting van drie bijkomende Belgische DPA's

45. La Commission constate que dans le Projet, trois nouvelles DPA sont créées : le C.O.C., le Comité R et le Comité P, ce en plus évidemment de la DPA déjà créée par la LAPD, à savoir l'APD (et en plus aussi d'un contrôle distinct des juridictions dans le cadre de leur fonction juridictionnelle[1]). Au total, le législateur fédéral créerait donc quatre DPA (et peut-être encore un organe de contrôle distinct pour les juridictions).

46. La Commission prend acte de ces choix politiques, qui correspondent en soi au principe selon lequel plusieurs DPA peuvent être désignées dans un État membre (cf. art. 51.1 du RGPD et art. 41.1 de la Directive). La Commission examine toutefois ci-après dans quelle mesure la concrétisation de ces choix politiques dans le texte du Projet : (1) donne lieu à une répartition de compétences claire/cohérente/efficace entre les DPA[2] et (2) respecte toutes les règles imposées aux DPA par le RGPD et la Directive et est cohérente avec la LAPD.

47. La Commission estime qu'il est crucial de définir une répartition de compétences convaincante entre les différentes DPA belges. Il convient à cet égard d'éviter autant que faire se peut des compétences communes ou qui se chevauchent en raison de l'insécurité juridique qui en découle et de leur caractère extrêmement inefficace.

---

[1] Cf. article 4, § 2, premier alinéa de la LAPD et considérant 20 du RGPD.

[2] La Commission a évidemment tout intérêt à ce qu'un règlement clair soit prévu, étant donné que son successeur en droit – l'APD – devra jouer un rôle central dans ce paysage à partir du 25 mai 2018.

48. La Commission constate que la répartition des compétences est extrêmement complexe dans le projet.

49. La Commission insiste à ce que le projet soit revu sur ce point-là.

50. La Commission relève que tant le C.O.C que les Comité P. et Comité I. sont qualifiés d'autorités de contrôle. Le C.O.C ne dispose toutefois pas de l'ensemble des compétences exigées par le RGPD en application des articles 57 et 58. S'agissant du Comité P et du Comité, il est renvoyé au Titre 7 .

51. La remarque qui suit est directement liée à celles qui précèdent relativement à la création de plusieurs autorités de contrôle.

52. Ni la loi APD ni le Projet ne contiennent de dispositions relatives à la coopération internationale qui sera pourtant, comme rappelé en introduction, au cœur de l'activité de l'APD dès le 25 mai 2018. En application de l'article 51.3. du RGPD, *« lorsqu'un Etat membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité [lisez le CEDP] et définit le mécanisme permettant de s'assurer du respect par les autres autorités des règles relatives au mécanisme de contrôle de la cohérence visé à l'article 68 ».*

53. La Commission est d'avis que cette question doit impérativement trouver une solution praticable et efficace. A défaut pour le législateur de le prévoir, l'on court le risque de la « chaise vide ». A titre d'exemple, la Commission reçoit aujourd'hui déjà des demandes d'approbation de codes de conduite sectoriels à vocation européenne sur lesquels elle ne pourra, après le 25 mai, se prononcer seule. De telles demandes devront passer par le mécanisme de contrôle de la cohérence en application de l'article 64.1.b. du RGPD. Mais quelle DPA va participer aux travaux pour la Belgique ?

54. En conclusion la Commission émet un avis défavorable quant aux dispositions du projet portant sur les trois nouvelles DPA[3] en raison des motifs évoqués ci-avant et en particulier eu égard au fait que : (1) la répartition de compétences entre les 4 DPA fédérales a été régie de manière chaotique et tout à fait illogique et (2) la réforme du C.O.C. ne va pas assez loin et n'est, en certains points, pas conforme aux règles européennes.

[3] Voir principalement les articles 73, 97 à 100 inclus, 107.8, 130 à 133 inclus, 163, 186 & Titre 7 & Titre 8 du Projet.

55. La Commission avance deux pistes alternatives afin de parvenir quand même à la création en Belgique d'un paysage de protection des données logique et organisé de manière efficace.

Restrictions indues aux pouvoirs de l'Autorité de contrôle et respect de son indépendance

56. Le Projet prévoit dans son Chapitre consacré aux traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire des dérogations à l'exercice des pouvoirs de la future autorité de protection des données (APD).

57. En ce qui concerne l'exemption à l'obligation de coopération du responsable de traitement avec l'autorité de protection des données (article 31 du RGPD) prévue à l'article 29, §9 du Projet et la limitation de tous les pouvoirs de l'autorité de protection des données vis-à-vis de ces traitements lorsque leur exercice *« fournirait des indications sur les sources d'information ou constituerait une mesure de contrôle préalable à la publication d'un article »* visée à l'article 29, §11 en projet, la Commission en constate le caractère disproportionné. La dérogation à l'article 31 du RGPD n'est pas nécessaire dans la mesure où sa mise en œuvre n'implique pas une obligation de divulgation des sources d'information.

58. D'autre part, le Projet prévoit que le Registre des traitements du « secteur public » (dont question aux articles 23-24 du Projet) est tenu auprès de l'autorité de contrôle. La Commission est d'avis que ce Registre (s'il est conservé malgré les remarques exprimées par la Commission dans le présent avis par ailleurs), ne peut être tenu auprès de l'autorité de contrôle notamment en raison du coût budgétaire que l'hébergement de ce Registre représenterai. D'autre part, plus fondamentalement encore, la Commission est d'avis que cet hébergement auprès de l'autorité de contrôle est incompatible avec le principe d'accountability et l'indépendance que se doit de garantir, en ce compris en apparence, l'autorité de contrôle.

Alignement de l'Exposé des motifs avec le RGPD – Corrections

59. A plusieurs endroits du Projet, un alignement du RGPD et de son Exposé des motifs est nécessaire.

Légistique

60. Au titre de remarque plus strictement légistique, le Projet reproduit inutilement des dispositions du RGPD à plusieurs endroits.

3. TITRE PRÉLIMINAIRE (art. 1 – 5)

3.1. Champ d'application matériel du Projet

Article 2

61. La LVP s'applique "*à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*", et ce quel que soit le secteur dans lequel le responsable du traitement est actif.

62. L'intention du législateur est de continuer sur cette voie "*afin de ne pas laisser de domaine hors réglementation, ce qui engendrerait de l'insécurité juridique et des vides juridiques face à la situation d'aujourd'hui ainsi qu'à nos obligations en vertu de la Convention 108.*"

63. La Commission souscrit entièrement à cette intention.

64. La nécessité de reprendre à l'article 2 du Projet une exception pour les forces armées n'est pas claire. Une dérogation explicite à l'alinéa 2 (qui déclare le RGPD applicable) est superflue, étant donné que le troisième alinéa soustrait déjà les titres 2 et 3 (qui reprennent les forces armées) à l'application de la présente loi. Stipuler que "*sans préjudice de l'article 107, la présente loi n'est pas applicable*" est également superflu, vu que la structure du Projet a déjà pour conséquence que seul l'article 107 régit les traitements poursuivis par les forces armées. La Commission estime que le dernier alinéa de l'article 2 du Projet doit être supprimé.

Article 3

65. L'article 3, premier alinéa du Projet rappelle l'article 1.3 du RGPD en ajoutant 'la libre circulation sur le territoire belge' : "*La libre circulation des données à caractère personnel (...)* ***sur le territoire belge*** *n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*". L'Exposé des motifs explique "*Cela signifie qu'un responsable de traitement ne peut faire obstacle à un flux de données sous prétexte de garantir la protection des données à caractère personnel.*"

66. L'article 3, deuxième alinéa du Projet poursuit :

67. *"En particulier, le partage des données à caractère personnel entre les responsables du traitement, les autorités compétentes, les services, organes et les destinataires, qui se situent dans les titres 1 à 3 de la présente loi et qui travaillent dans le cadre des finalités visées à l'article 23.1.a) à h) du Règlement ne peut être ni limité ni interdit pour de tels motifs, sans préjudice des compétences de l'autorité de contrôle compétente."*

68. Cette disposition du Projet est extrêmement problématique pour différentes raisons.

69. Le premier alinéa de cette disposition transgresse l'interdiction de copie sans qu'une justification ne soit fournie à cet effet. La Commission ne voit d'ailleurs aucune raison de copier la finalité du RGPD.

70. En ce qui concerne l'ajout du 'territoire belge', la Commission fait remarquer que l'article premier du RGPD ne contient aucune clause de spécification nationale qui autorise une dérogation. La compatibilité de cette disposition avec la norme juridique supérieure doit dès lors être examinée scrupuleusement.

71. Selon l'Exposé des motifs, cette disposition signifie "*qu'un responsable de traitement ne peut faire obstacle à un flux de données sous prétexte de garantir la protection des données à caractère personnel*". Cette vision est manifestement contraire à la responsabilité reprise aux articles 5.2 et 24 du RGPD. Un responsable du traitement qui sait qu'un destinataire bafoue le droit à la protection des données doit naturellement cesser la communication de données à caractère personnel. Par ailleurs, cette disposition semble priver le responsable du traitement de toute liberté de choix, chaque fois qu'un tiers lui demande de communiquer des données à caractère personnel, il doit le faire[4], ce qui est manifestement contraire notamment au principe de finalité repris à l'article 5.1.b du RGPD.

72. Il ressort de l'Exposé des motifs que le deuxième alinéa est dicté par la volonté de garantir que l'autorité puisse remplir ses missions (continuité du service public)[5]. Il s'agit d'une préoccupation importante, mais la Commission pense que le Projet a des conséquences graves non souhaitées pour les droits et libertés des personnes concernées. Chaque échange de données à caractère personnel doit se faire conformément aux règles en vigueur. Tout comme indiqué ci-dessus, on ne peut pas imposer au responsable du traitement d'accéder à chaque demande de communication de données à caractère personnel.

73. Le renvoi à l'article 23 du RGPD ne répond pas aux conditions qui y sont posées. Il ne suffit pas de faire référence aux objectifs énumérés à l'article 23.1.a-h du RGPD. La législation doit respecter l'essence des libertés et droits fondamentaux (art. 23.1 du RGPD) et remplir les garanties mentionnées à l'article 23.2 du RGPD. En outre, l'article 23 du RGPD n'autorise pas le législateur à soustraire totalement des instances au RGPD, mais uniquement à limiter certains droits.

---

[4] Sauf éventuellement dans les cas où des motifs en dehors du droit à la protection des données interdisent la communication.

[5] *"Il ne peut donc jamais être question notamment pour un service public de ne pas exercer ses missions pour des raisons liées à la protection des données. Il s'agira cependant pour chaque autorité publique de remplir ses missions en respectant le cadre législatif relatif à la protection des données. Il est crucial que les flux de données nécessaires et proportionnel (NdT : lisez "proportionnels") à l'exécution des missions public (Ndt : lisez "publiques") aient lieu, dans le respect du Règlement et de la présente loi."*

74. Un responsable du traitement qui communique des données à caractère personnel à la demande de l'autorité ne peut pas invoquer cette disposition du Projet pour échapper en toutes circonstances aux pouvoirs de contrôle de l'APD régis aux articles 58.2 et 83 du RGPD ou au contrôle judiciaire défini à l'article 79 du RGPD. Il est inconcevable que le responsable du traitement doive attendre l'intervention de l'APD ou d'un juge avant de pouvoir mettre fin à une communication illicite. Donner le signal aux autorités qui poursuivent des objectifs de l'article 23.1.a-h du RGPD qu'elles ne doivent pas se faire du souci concernant les règles de protection des données tant que l'autorité compétente n'intervient pas est tout à fait inadmissible. D'ailleurs, ce signal contraste fortement avec l'importance que l'Exposé des motifs prétend accorder à la protection des données[6].

75. La Commission estime que cet article doit être supprimé. De plus, le Projet contient déjà ailleurs des dispositions qui appliquent l'article 23 du RGPD (voir plus loin).

3.2. Champ d'application territorial du Projet

Article 4

76. L'article 4 du Projet définit le champ d'application territorial et suit ainsi les lignes directrices de l'article 3 du RGPD.

77. La Commission fait remarquer que l'Exposé des motifs ne concorde pas avec le contenu de la disposition du Projet, ni avec l'article 3 du RGPD. L'Exposé des motifs est rédigé comme suit :

78. "*Il s'agit d'une disposition déterminant le champ d'application territorial, lequel reprend d'une part l'établissement du responsable du traitement ou du sous-traitant, et d'autre part, le fait de se trouver sur le territoire belge pour la personne concernée afin de faciliter l'application du droit et des procédures. En principe, vu les règles uniformes dans l'Union européenne, il sera maintenu une certaine cohérence. Dans les cas où il existe une marge d'appréciation pour les États membres de l'Union européenne, un tel régime territorial pourrait aboutir à un conflit de loi. Mais il est nécessaire de maintenir également le critère de résidence/se trouvant sur le territoire belge de la personne concernée afin de la protéger éventuellement contre des règles moins contraignantes. On peut penser à l'âge de l'enfant ou l'autorisation de traiter des données sensibles, alors que cela n'est pas possible en Belgique.*"

---

[6] *"Il s'agira cependant pour chaque autorité publique de remplir ses missions en respectant le cadre législatif relatif à la protection des données. Il est crucial que les flux de données nécessaires et proportionnel (NdT : lisez "proportionnels") à l'exécution des missions public (Ndt : lisez "publiques") aient lieu, dans le respect du Règlement et de la présente loi."*

79. Le critère selon lequel la personne concernée se trouve sur le territoire belge n'est pertinent que pour les responsables du traitement et les sous-traitants qui ne sont pas établis sur le territoire de l'Union européenne mais ce critère ne joue aucun rôle significatif dans la résolution de conflits de lois entre États membres dans les situations où le RGPD laisse au législateur national une marge d'appréciation dans l'exécution du RGPD. Le Projet s'applique aux activités du responsable du traitement ou d'un sous-traitant sur le territoire belge.
Les responsables du traitement établis dans un autre État membre peuvent traiter les données à caractère personnel des personnes concernées qui séjournent en Belgique selon les règles en vigueur dans leur propre État membre - à condition qu'ils ne recourent pas à un sous-traitant établi en Belgique. Des règles belges plus strictes concernant le traitement de données sensibles ne s'appliqueraient donc pas, contrairement à ce qu'implique l'Exposé des motifs.

80. La situation du responsable du traitement établi dans un autre État membre qui fait appel à un sous-traitant belge n'est pas claire. Le Projet crée un conflit de lois mais n'y apporte pas de solution. Le responsable du traitement est tenu par la législation de cet État membre lors de la formulation d'instructions au sous-traitant belge, qui est à son tour lié par la législation belge qui met en œuvre le RGPD. L'insécurité juridique quant à savoir quelles dispositions belges s'appliquent au sous-traitant et se répercutent sur les activités du responsable du traitement constitue un désavantage concurrentiel pour les sous-traitants belges. D'ailleurs, le problème se pose, que des personnes concernées belges soient impliquées ou non dans le traitement en question.

81. Une piste pour régler le conflit de lois concernant les sous-traitants établis en Belgique se trouve dans la législation autrichienne en vigueur. La règle de base est que la loi s'applique à chaque traitement de données à caractère personnel qui est entrepris en Autriche ou géré par un responsable du traitement établi en Autriche. Pour les sous-traitants, la dérogation suivante est pertinente :

82. "*[] le droit du pays où le responsable du traitement est établi s'applique à un traitement de données à caractère personnel en [Autriche] pour autant qu'un responsable du traitement du secteur privé [...] avec un établissement dans un autre État membre de l'Union européenne traite des données à caractère personnel en Autriche pour une finalité qui ne doit pas être attribuée à une filiale située en Autriche.*"[7]

---

[7] Traduction libre de "*(1) Abweichend von Abs. 3 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.*" - § 2, 2e alinéa de la Datenschutzgesetz autrichienne (loi sur la protection des données) 2000, https://www.dsb.gv.at/gesetze-in-osterreich.

83. La Commission insiste pour que la disposition du Projet soit précisée.

Définitions

84. L'article 5 du Projet est libellé comme suit :

"*Sans préjudice des définitions prévues dans la présente loi, les définitions prévues dans le Règlement s'appliquent.*"

85. Pour l'accessibilité de la réglementation, il est effectivement souhaitable de renvoyer explicitement à l'endroit où se trouvent les définitions dans le RGPD.
L'ajout du passage "*Sans préjudice des définitions prévues dans la présente loi*" constitue une formulation qui crée la confusion. L'expression "sans préjudice de" est souvent comprise comme une réserve, ce qui impliquerait que la priorité est donnée aux définitions reprises dans la loi nationale plutôt qu'au RGPD, qui est une norme juridique supérieure. Ceci est problématique, notamment au titre 4 où plusieurs notions clés du RGPD sont redéfinies (voir plus loin). Le Conseil d'État, Section Législation, recommande d'éviter l'expression 'sans préjudice de' et d'utiliser à la place 'indépendamment de" (Principes de technique législative, point 3.2).

86. La Commission estime que cet élément de la phrase doit être supprimé ou adapté.

CONCLUSION de la Commission sur le titre préliminaire du Projet

87. L'avis de la Commission concernant ce titre préliminaire est dès lors globalement défavorable. L'article 3 doit être supprimé pour les motifs invoqués ci-dessus. Le demandeur doit adapter en profondeur les articles 2, 4 et 5 et les préciser pour tenir compte des remarques de la Commission.

4. TITRE 1 : DE LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE

4.1. Chapitre I – Dispositions générales

Exécution du RGPD

88. L'article 6 en projet prévoit qu' « A l'exception des traitements visés aux titres 2 et 3, et sous réserve de dispositions particulières, le présent titre exécute le Règlement ».

89. Par souci de clarté et de sécurité juridique, il conviendrait de délimiter le champ d'application matériel du titre 1 du projet en précisant par exemple qu'il s'applique à tous les traitements de données visés à l'article 2 al. 1, à l'exception de ceux visés aux titres 2 et 3.

4.2. Chapitre II – Principes de traitement

Exécution de l'article 8.1. du RGPD

90. Concernant l'article 7 en projet, qui abaisse l'âge à partir duquel les mineurs pourront consentir seuls aux traitements de leurs données visés à l'article 8.1 du RGPD, la Commission renvoie au communiqué de presse qu'elle a émis à ce sujet : « *La Commission vie privée soutient le choix du législateur belge d'abaisser à 13 ans l'âge pour le consentement parental en vertu [de l'article 8][8] du RGPD. Cet âge correspond mieux à la réalité quotidienne de très nombreux jeunes qui surfent déjà sur Internet à un jeune âge. Nous ne pouvons pas les priver d'opportunités de s'épanouir numériquement. Mais vu que les enfants doivent aussi prendre conscience de leur vie privée, le choix de 13 ans doit s'accompagner d'efforts supplémentaires pour leur apprendre dès l'enfance à adopter une attitude réfléchie à l'égard des médias* »

91. Par souci de clarté, l'article 7 en projet doit préciser qu'il exécute l'article 8.1. du RGPD. En effet, cet article du RGPD a une portée limitée dès lors qu'il ne vise que les traitements de données opérés par des services de la société de l'information s'adressant directement aux enfants (art. 8.1. du RGPD). Et l'article 8.3. du RGPD demeure par ailleurs d'application, la validité du consentement donné au regard des règles de protection des données ne porte pas atteinte au droit général des contrats des Etats membres. Partant, à défaut de préciser que l'article 7 exécute le seul paragraphe 1 de l'article 8, le texte du projet donne l'impression d'outrepasser l'article 8.3.

Exécution de l'article 9.2.g) du RGPD

[8] Ces termes entre […] sont ajoutés par rapport au communiqué de presse évoqué.

92. L'article 8 en projet prétend exécuter l'article 9.2.g du RGPD et reprend les traitements visés à l'article 3 § 6 de la loi vie privée actuelle (child focus), à l'article 6, §1, k de la même loi (traitements de données sensibles par ASBL pour la défense des droits de l'homme) et à l'article 6, § 3 toujours de la loi vie privée (traitements de guidance des personnes ayant un comportement sexuel infractionnel) en les considérant comme des traitements nécessaires pour des motifs d'intérêt public important.

93. A sa lecture, l'article 8 en projet ne constitue pas une mesure d'exécution de l'article 9.2.g du RGPD en vertu duquel la disposition légale encadrant le traitement des données sensibles au sens de l'article 9.2.g du RGPD doit, non seulement, répondre à des motifs d'intérêt public important, mais également, encadrer les traitements visés de manière telle que le principe de proportionnalité soit respecté (détermination des catégories de données traitées, des catégories de personnes concernées, détermination précise des destinataires et des personnes qui disposent d'un droit de consultation, circonstances justifiant les différents types de traitements, durée de conservation….) et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts des personnes concernées . Or, l'article 8 du projet se limite à établir une liste de motifs qualifiés d'intérêt publics importants. S'agissant d'une dérogation à l'interdiction de principe du traitement des données sensibles, ces garanties sont particulièrement essentielles et indispensables. Ces garanties font défaut dans le projet actuel.

94. En ce qui concerne les traitements de données sensibles réalisés par child focus (actuellement visé à l'article 8, al. 1, 2° en projet), les garanties qui figurent actuellement dans l'article 3 de la loi vie privée - à savoir (i) l'interdiction pour le Centre de tenir un fichier de personnes suspectées d'avoir commis un crime ou un délit ou de personnes condamnées, (ii) l'obligation de disposer d'un DPO, (iii) la soumission des membres du personnes au secret professionnel au sens de l'article 458 du code pénal, (iv) l'interdiction d'enregistrement des conversations téléphoniques sans information préalable de l'appelant et seule en cas de non exercice de son droit d'opposition – ont disparu. Il est recommandé qu'une disposition légale conforme à l'article 9.2.g du RGPD soit prévue dans un texte de loi autonome.

95. Ensuite, la Commission estime que l'article 8, alinéa 1, 1° en projet n'est pas nécessaire dans la mesure où l'article 9.2.d du RGPD prévoit déjà la levée de l'interdiction de traitement des données sensibles au sens de l'article 9 du RGPD au profit des « *fondations ou organisations (…) à but non lucratif poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées* ».

96. De même, l'hypothèse visée à l'article 8, alinéa 1, 3° en projet est déjà encadrée par l'article 9.2.h du RGPD. Dans ce cas, le traitement doit être réalisé par un professionnel de soins de santé soumis à une obligation de secret professionnel ou par un tiers agissant sous la responsabilité d'un tel professionnel ou par un tiers également soumis à une obligation légale ou déontologique de secret (art. 9.3 RGPD)

97. Enfin, si l'auteur du projet veut se préserver une base légale pour d'éventuels arrêtés royaux adoptés en exécution de l'article 6 de loi vie privée actuelle, il convient de prévoir à cet effet une disposition légale spécifique dans les dispositions finales du présent projet.

98. La Commission constate que le législateur n'a pas usé de la faculté qui lui est octroyée, en vertu de l'article 9.4 du RGPD, de maintenir ou d'introduire des conditions supplémentaires pour le traitements des données génétiques, des données biométriques ou des données concernant la santé. Dans la mesure où l'AR d'exécution de la loi vie privée du 13 février 2001 va être abrogé, les garanties particulières qui y étaient prévues, en son article 25, vont être supprimées. Afin de ne pas diminuer le niveau de protection en la matière, l'auteur du projet doit réintégrer ces garanties dans la loi d'exécution du RGPD et prévoir, pour ces traitements de données :

- L'obligation de désignation des catégories de personnes ayant accès à ces données avec la description précise de leur fonction par rapport au traitement de données visé ;
- La liste nominative des personnes visées tenue à la disposition de l'APD à 1ère demande ;
- La soumission des personnes visées à une obligation légale, statutaire ou contractuelle de respect du caractère confidentiel des données visées.

Exécution de l'article 10 du RGPD

99. L'article 9 du projet exécute l'article 10 du RGPD et détermine les catégories de responsables de traitement, autres que les autorités publiques, qui peuvent[9] traiter des données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes.

100. Tout d'abord, la Commission relève que, contrairement à ce qui est repris dans l'exposé des motifs, l'article 9 en projet n'encadre pas les accès au casier judiciaire. Le casier judiciaire et la liste limitative des personnes qui y ont accès sont réglementés par le Code d'instruction criminelle. L'exposé des motifs doit être corrigé sur ce point.

101. Concernant les catégories de personnes autorisées à traiter les données judiciaires au sens de l'article 10 du RGPD, la Commission considère que la formulation de la 3ème catégorie de personnes

[9] Le libellé du début du §1 de l'article 9 du projet de loi mérite sur ce point d'être adapté en précisant qu'il décrit la liste des personnes autorisées à traiter les données visées.

autorisées à traiter des données judiciaires au sens de l'article 10 du RGPD doit être revue pour viser explicitement les personnes déterminées par ou en vertu d'une loi, d'un décret ou d'une ordonnance adopté pour des motifs d'intérêt public important pour l'accomplissement de tâches d'intérêt général confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

102. Quant à la 4ème hypothèse d'autorisation de traitement des données judiciaires, la Commission relève que la notion de recherche scientifique est trop restrictive dans la mesure où elle n'inclut pas nécessairement la recherche historique. Il convient donc d'ajouter, à l'article 9, §1 er, 4° en projet, la notion de nécessité de la recherche historique. Afin que les chercheurs puissent accéder aux informations nécessaires à la réalisation de leur recherche, il convient également de viser les responsables de traitement chargés, par le législateur, de missions de service public consistant en des tâches d'archivage dans l'intérêt public général à la condition que l'accessibilité de ces données archivées dans l'intérêt public soit limitée aux chercheurs. Le tout, dans le respect du titre 4 du projet pour lequel la Commission renvoie à ses remarques (cf. infra).

103. L'article 9, §1, 5° ajoute une nouvelle catégorie de personnes autorisée à traiter ces données (child focus). Aux yeux de la Commission, il convient de la supprimer car elle n'est ni pertinente ni nécessaire. Tout d'abord, Child focus ne pourra pas sur cette base disposer d'un accès au casier judiciaire, contrairement à ce qui est explicité dans l'exposé des motifs. De plus, le traitement par Child focus de telles données est déjà couvert par l'article 9, § 1, 3° en projet au vu de l'article 383bis/1 du code pénal et de l'AR du 15 novembre 2016 portant agrément de Child Focus en tant qu'organisation visée à l'article 383bis/1 du Code pénal et donc habilitée à recevoir des signalements relatifs à des images susceptibles d'être visées à l'article 383bis (pédopornographie), à analyser leur contenu et leur origine, et à les transmettre aux services de police et autorités judiciaires.

104. Enfin, la Commission relève que la définition de données judiciaires au sens de l'article 10 du RGPD est plus restrictive que celle visée à l'article 8 actuel de la loi vie privée qui couvre aussi les suspicions d'infractions. A partir du 25 mai prochain, les traitements de données judiciaires consisteront uniquement en des traitement de données à caractère personnel relatives à des condamnations pénales et aux infractions pénales ou aux mesures de sûreté connexes. La Commission s'interroge si, dans la version néerlandaise du §1 de l'article 9 en projet, il ne convient pas de traduire les termes « infractions pénales » par « strafrechterlijke inbreuken » à la place de « strafbare feiten » et ce, même si cette traduction correspond à la traduction officielle de l'article 10 du RGPD.

4.3. Chapitre III – Droits de la personne concernée

105. Une remarque introductive pour commencer : la Commission recommande de changer le titre de ce chapitre et de le formuler comme suit "*Limitations des droits de la personne concernée*" étant donné que le titre actuel ne correspond pas à l'intention proprement dite de ce chapitre. Dans ce chapitre, le demandeur entend exécuter l'article 23 du RGPD qui permet aux États membres de prévoir, dans certaines limites et pour des finalités spécifiques, des exceptions aux droits de la personne concernée.

Les principes de base dont le législateur doit tenir compte lors de l'exécution de l'article 23 du RGPD

106. Pour cerner l'ampleur de la marge d'appréciation dont dispose le législateur à cet égard, il est important de rappeler la jurisprudence de la Cour de justice au sujet de l'article 13 de la Directive 95/46/CE qui prévoyait un motif d'exception similaire. Dans l'arrêt *Smaranda Bara*, la Cour a confirmé que ces exceptions ne pouvaient être introduites que par des "*mesures législatives*"[10]. La Cour avait déjà précisé auparavant que les États membres ne pouvaient adopter ces exceptions que pour autant qu'elles soient "*nécessaires* "[11]. Vu la volonté inchangée du législateur européen d'atteindre un niveau de protection élevé[12], il en résulte que les exceptions aux droits des personnes concernées doivent rester dans les limites de ce qui est strictement nécessaire[13]. La nécessité et la proportionnalité des mesures en question doivent donc être interprétées de manière limitative.

107. L'article 23 du RGPD permet de prévoir, par le biais d'une intervention législative ponctuelle, des exceptions encadrées légalement dont la nécessité pour une des finalités de l'article 23.1 du RGPD est clairement démontrée. Dans l'ordre juridique belge, les articles 64 et 65 de la loi du 18 septembre 2017[14] constituent un bon exemple d'exceptions motivées spécifiques à un secteur qui répondent à la philosophie sous-jacente de l'article 23 du RGPD. La Commission constate que le demandeur reconnaît ce point de départ dans son Exposé des motifs, indiquant notamment que ces exceptions doivent être reprises dans "*une disposition législative*" et "*qu'elles doivent être aussi précises que possible*"[15]. L'Exposé des motifs dispose même qu'une analyse spécifique doit

---

[10] Cour de justice, 1er octobre 2015 (C-201/14), *Smaranda Bara e.a.*, § 39 ; Cour de justice, 27 septembre 2017 (C-73/16), *Puškár*, § 96.

[11] Cour de justice, 7 novembre 2013 (C-473/12), *BIV v. Englebert*, § 32.

[12] Considérant 10 du RGPD. Considérant 10 de la Directive 95/46/CE.

[13] Ibid., § 39.

[14] Loi du 18 septembre 2017 *relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces*, M.B. 6 octobre 2017.

[15] Exposé des motifs, page 21.

avoir lieu pour mettre en balance les droits de la personne concernée et l'opérationnalité des services concernés[16].

108. Enfin, toute mesure légale prévoyant des exceptions aux droits de la personne concernée doit comporter *au moins* les éléments énoncés à l'article 23.2 du RGPD.

109. Les articles légaux de ce chapitre sont donc confrontés à ces principes de base.

Articles 10 et 11 du projet

110. Les articles 10 et 11 du projet prévoient une exception très large et générale à *tous* les droits de la personne concernée que peuvent invoquer les administrations publiques ayant des compétences pour détecter, poursuivre et enquêter sur des infractions pénales. L'Exposé des motifs mentionne plusieurs exemples non exhaustifs : les services d'inspection sociale, l'inspection économique, les services d'inspection au sein du SPF Finances, les communes, etc. Cette exceptions s'appliquerait par ailleurs aussi à "*d'autres administrations publiques […] qui ont […] besoin d'un régime particulier*"[17]. Ce régime spécial serait nécessaire parce que "*une croyance généralisée circule en ce que le [RGPD] serait trop strict*" et pour "*maintenir une certaine souplesse pour le secteur public*"[18]. La Commission estime que par cette "croyance généralisée", le demandeur bafoue le RGPD. Les articles 10 et 11 du projet ne passent dès lors pas le test de l'article 23.2 du RGPD.

111. D'après l'article 23.2.a) et 23.2.e) du RGPD, les mesures législatives doivent énoncer les catégories de responsables du traitement ainsi que les finalités. La lecture conjointe des paragraphes 1, 2 et 3 de l'article 10 du projet ne permet pas d'identifier avec précision les responsables du traitement qui peuvent invoquer ces exceptions. C'est en particulier l'article 10, § 2 qui enfreint cette exigence en se référant approximativement à toute instance qui poursuit un objectif au sens de l'article 23.1.e) du RGPD. Cet article n'exécute pas le RGPD, mais crée au contraire une norme trompeuse qui donne l'impression que toute instance publique peut invoquer l'article 23.1.e) du RGPD pour limiter arbitrairement les droits de la personne concernée. L'article 10 ne précise pas non plus les objectifs poursuivis du fait que le projet renvoie simplement à l'article 23.1 du RGPD, sans décrire les tâches et missions légales des services concernés.

[16] Ibid.

[17] Exposé des motifs, page 19.

[18] Exposé des motifs, page 19.

112. À cet égard la Commission se réfère à la communication de la Commission européenne du 24 janvier 2018 affirmant explicitement ce qui suit : "*La reproduction du texte du règlement mot pour mot dans la loi nationale visant à préciser le règlement devrait être exceptionnelle et justifiée et ne saurait servir à ajouter des conditions ou interprétations supplémentaires au texte du règlement*."[19]

113. Le demandeur ne prévoit même pas un renvoi à un arrêté royal pour désigner les services qui pourraient invoquer ces exceptions, comme c'est actuellement le cas pour l'article 3, § 5 de la LVP[20]. En outre, cette solution serait aussi insuffisante du fait que la philosophie de l'article 23 du RGPD, lu conjointement avec l'article 22 de la Constitution, requiert que ces exceptions aux droits des personnes concernées soient établies par une loi formelle ("*par la loi*"). Une extension arbitraire par arrêté royal de la portée *ratione personae* d'une exception large et générale comme dans l'article 10 du projet est en ce sens inacceptable. Comme indiqué ci-dessus, une bonne exécution de l'article 23 du RGPD requiert une adaptation de la législation sectorielle applicable de sorte que les exceptions soient établies sur mesure en fonction des besoins, tâches et missions des services concernés, sans limiter outre mesure les droits de la personne concernée.

114. La Commission constate que l'Exposé des motifs confirme le manque de délimitation du champ d'application personnel de l'article 10 du projet. L'Exposé des motifs dispose en effet que : "*Le champ d'application de l'article 10 est assez large afin de couvrir un ensemble de services qui se verraient concernés*." Le champ d'application de l'article 10 du projet manque donc totalement de clarté, alors que cela constitue une exigence expresse de l'article 23.2.c) du RGPD.

115. D'après l'article 23.2.d) du RGPD, les mesures légales doivent comporter des garanties destinées à prévenir les abus. L'article 11 du projet fait une tentative en ce sens en prévoyant un système de garanties minimales. Il ressort de l'Exposé des motifs que le demandeur s'est inspiré de l'article 3, § 7 de la LVP[21]. L'article 11 du projet reprend hélas l'article 3, § 7 de la LVP de manière sélective et laisse tomber des garanties importantes, rompant ainsi le fragile équilibre

---

[19] CE, " Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018", 24 janvier 2018, p. 10, disponible via ce lien.

[20] Voir par exemple pour les inspecteurs sociaux : Arrêté royal du 11 mars 2015 *portant exécution de l'article 3, § 5, 3, 5, 3° de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, M.B., 25 mars 2015. Avis n° 09/2010 de la Commission du 17 mars 2010, disponible via ce lien ; Avis n° 34/2016 de la Commission du 29 juin 2016, disponible via ce lien.

[21] Exposé des motifs, page 24.

incarné par cette disposition légale, après plusieurs avis de la Commission[22] et un arrêt de la Cour constitutionnelle[23]. Le projet fait défaut sur les points suivants :

- *Limitation dans le temps* : à l'époque, la Cour constitutionnelle avait annulé une autre version de l'article 3, § 7 de la LVP précisément parce que la disposition légale attaquée ne précisait pas combien de temps pouvaient durer les actes préparatoires justifiant la suspension des droits[24]. Le demandeur laisse tomber ce délai maximal. Dès lors, l'article 11 prive non seulement la personne concernée d'une garantie, mais il enfreint même la jurisprudence de la Cour constitutionnelle. Enfin, l'article 11, § 3, deuxième alinéa implique qu'une administration publique puisse *de facto* suspendre les droits de personnes concernées pour une durée illimitée pour des "*objectifs importants d'intérêt public*". Le projet ne donne aucun critère pour déterminer le point de commencement et de fin de cette période pendant laquelle les "objectifs d'intérêt public" peuvent être invoqués pour suspendre les droits de la personne concernée. Ce n'est pas conforme à l'arrêt de la Cour constitutionnelle[25] et est disproportionné à la lumière de l'article 23.1 du RGPD ;

- *données pertinentes* : dans son arrêt, la Cour constitutionnelle souligne que cette exception ne peut s'étendre aux données sans lien avec la finalité de l'enquête ou du contrôle. Les termes "*dans la mesure où* " de l'article 11 doivent donc être interprétés en ce sens, conformément à la Constitution. Il est quand même recommandé de préciser aussi explicitement dans ce type de dispositions d'exception que pour toutes les autres données à caractère personnel que le service concerné traite pour d'autres finalités, les droits de la personne concernée restent intacts ;

- *communication de la motivation* : d'après l'article 3, § 7 de la LVP, le responsable du traitement communique dans son entièreté la motivation de la décision prise, et ce au terme de la suspension. Ces termes ont été repris dans l'actuel article 3, § 7 de la LVP sur avis de la Commission[26] afin de déroger à l'obligation de motivation de droit commun de la loi du 29 juillet 1991[27] et de prévoir un contrôle *a posteriori* des motifs de l'administration. L'article 11, § 1, deuxième alinéa du projet ne suffit pas pour déroger à l'obligation de

---

[22] Avis n° 11/2012 de la Commission du 11 avril 2012, disponible via ce lien ; avis n° 32/2012 de la Commission du 17 octobre 2012, disponible via ce lien.

[23] Cour constitutionnelle, arrêt du 27 mars 2014, n° 51/2014.

[24] Cour constitutionnelle, arrêt du 27 mars 2014, n° 51/2014, B.8.5.

[25] Cour constitutionnelle, arrêt du 27 mars 2014, n° 51/2014, B.7.3.

[26] *Documents*, Chambre, 2012-2013, n° 2756/001, pp. 161-164 ; Avis n° 32/2012 de la Commission du 17 octobre 2012, disponible via ce lien, points 15-19.

[27] Loi du 29 juillet 1991 *relative à la motivation formelle des actes administratifs*, M.B. 12 septembre 1991.

motivation de la loi du 29 juillet 1991 et prive en outre la personne concernée de la garantie d'être informée automatiquement des motifs du service concerné au terme du contrôle ou de l'enquête.

116. Enfin, les articles 10 et 11 du projet doivent aussi passer dans leur intégralité le test de proportionnalité et de nécessité de l'article 23.1 du RGPD. À la lumière des remarques précitées, ce bilan est négatif. En outre, l'article 10 crée une suspension de *tous les droits des personnes concernées* sans vérifier si l'exclusion de certains droits est bien nécessaire au regard des missions et tâches légales du service concerné. Ainsi, la Commission a fait remarquer dans son avis sur l'article 3, § 7 de la LVP que l'exclusion du droit de rectification ou de suppression pourrait entraîner que le fisc établisse son imposition sur la base de données inexactes ou dont le traitement est interdit[28]. Le législateur doit, dans le cadre de la législation sectorielle applicable, procéder à des évaluations similaires permettant de justifier distinctement la nécessité de suspension de chacun des droits à l'aide des missions du service concerné. Ainsi, la Commission ne comprend pas pourquoi il serait nécessaire de prévoir systématiquement une exception à l'article 34 du RGPD[29].

117. La Commission estime dès lors que les articles 10 et 11 du projet incarnent en essence une version vidée de sens de l'actuel article 3, § 7 de la LVP auquel un nombre indéterminé de services publics non identifiés pourraient en outre recourir – probablement même pour une durée indéterminée. La tentative de réunir un nombre maximal d'administrations publiques sous une seule exception implique inexorablement que le demandeur n'a pas pu réaliser la nécessaire pondération d'intérêts entre les besoins spécifiques de chaque service d'une part et les droits de la personne concernée d'autre part. Contrairement à ce que suggère l'article 11, § 4 du projet, il appartient en premier lieu au législateur de créer dans ses dispositions d'exécution du RGPD un bon équilibre entre ces intérêts conflictuels. Ce paragraphe ne présente dès lors aucune valeur ajoutée[30].

Article 12 du projet

118. L'article 12 du projet prévoit une exception aux droits de la personne concernée pour les responsables du traitement qui disposent d'informations provenant des services de renseignement et de sécurité. La Commission salue cette adaptation qui comble une lacune que la doctrine a

---

[28] Avis n° 32/2012 de la Commission du 17 octobre 2012, disponible via ce lien, point 9.

[29] Voir dans le même sens l'avis n° 24/2017 de la Commission du 24 mai 2017, disponible via ce lien, point 36.

[30] Il en va de même pour l'article 11, § 1, troisième alinéa : le responsable du traitement doit en effet *toujours* justifier sa politique relative aux droits de la personne concernée sur demande de l'Autorité de protection des données. Cela découle naturellement de la mission de contrôle de l'Autorité de protection des données et ne nécessite pas de répétition inutile et potentiellement confuse dans des dispositions d'exception.

identifiée il y a vingt ans déjà[31]. La disposition entend éviter que des informations confidentielles puissent "fuir" via des acteurs tant du secteur privé que du secteur public qui entrent en contact avec les services de renseignement et de sécurité sur la base des articles 14 et 16 de la loi du 30 novembre 1998[32].

119. Le projet devrait se référer expressément à ces articles comme fondement juridique de cet échange d'informations au lieu de la référence très générale aux lois du 30 novembre 1998 et du 10 juillet 2006[33] dans l'Exposé des motifs[34]. Les exceptions aux droits de la personne concernée ne peuvent en effet pas être interprétées comme une disposition légale permettant implicitement cet échange d'informations à défaut d'une disposition légale qui crée expressément cette pratique. À cet égard, la Commission fait remarquer que la loi du 10 juillet 2006 en question ne comporte aucune disposition similaire aux articles 14 et 16 de la loi du 30 novembre 1998.

120. Bien qu'il ressorte de l'Exposé des motifs que notamment les services de renseignement et de sécurité peuvent invoquer cette exception, la formulation néerlandaise de l'article 12, premier alinéa du projet sème la confusion quant au champ d'application personnel. Au lieu de se référer aux "*persoonsgegevens die […] afkomstig zijn van andere overheden bedoeld in artikel (sic) 3 van deze wet*" (données à caractère personnel, émanant […] des autres autorités visées à l'article (sic) 3 de la présente loi), le demandeur devrait simplement se référer aux autorités du titre 3 du projet. La version en français du projet a bel et bien été adaptée sur ce point.

121. L'exception concerne les données provenant des instances du titre 3 du projet, des instances de l'article 10 de la loi du 10 juillet 2006 et de l'article 44/11/3*ter*, § 2 et 3 de la loi *sur la fonction de police*. Premièrement, la Commission se demande s'il est bien nécessaire de créer, dans ces deux dernières situations, une exception tant dans le secteur privé que dans le secteur public, alors que ces deux lois énoncent elles-mêmes de manière exhaustive qui peut recevoir les rapports d'évaluation de l'OCAM et quels acteurs ont accès aux banques de données communes. Ni le projet en lui-même, ni l'Exposé des motifs ne désignent la base légale permettant le transfert de ces informations. La Commission émet de nouveau la réserve suivante : l'exception aux droits de la

---

[31] Y. POULLET ET B. HAVELANGE, "Secret d'État et Vie Privée : ou comment concilier l'inconciliable ?", *Cahiers du Crids* n° 16, disponible via ce lien, pp. 233-234 : "*Comme il a été souligné, l'article 13 de la directive autorise des exceptions pour des responsables de traitement en communication avec la sûreté de l'État et les services de renseignements. […] La directive permet dans de tels cas des dérogations à l'application de ses prescrits. Une dérogation est-elle possible en droit belge ? C'est discutable mais en tout cas certainement pas sur base de la nouvelle version de l'article 3.*"

[32] Loi *organique des services de renseignement et de sécurité du 30* novembre 1998, M.B. 18 décembre 1998.

[33] Loi du 10 juillet 2006 *relative à l'analyse de la menace*, M.B. 20 juillet 2006.

[34] Exposé des motifs, page 26.

personne concernée ne peut constituer une légitimation indirecte d'une pratique qui ne repose pas sur une base légale explicite.

122. Sur le plan rédactionnel, la Commission ne voit pas quelle est la valeur juridique ajoutée de répéter jusqu'à trois reprises dans l'article 12 du projet l'exclusion des droits aux articles 12 à 22 et 34 ainsi que le droit à la transparence[35]. Les droits et obligations découlant de ces articles sont deux revers d'une même médaille et ne nécessitent pas une exception distincte.

123. L'article 12, § 2 du projet prévoit un "droit de recours" différencié. À cet égard, la Commission souhaite formuler plusieurs remarques. Premièrement, le projet devrait déterminer d'emblée, tant dans cet article que dans l'ensemble du projet, qui est l'autorité de contrôle compétente. C'est d'autant plus important que le demandeur n'est pas toujours clair dans la délimitation du champ d'application entre le RGPD d'une part et la Directive[36] d'autre part.

124. Deuxièmement, la Commission s'interroge quant à l'application de ce recours différencié. Les termes actuels excluent-ils suffisamment qu'une personne concernée qui ne se doute de rien porte plainte auprès de l'Autorité de protection des données et reçoive ensuite une réponse du Comité R selon laquelle "*les vérifications nécessaires ont été effectuées*", rompant ainsi le secret de l'enquête ? Il ressort des explications complémentaires du demandeur que l'Autorité de protection des données communiquerait cette information. Le projet parle toutefois de "l'autorité de contrôle". Étant donné que le Comité R est l'autorité de contrôle des services de renseignement et de sécurité (cf. article 97), le texte actuel du projet n'exclut pas que le Comité R communiquerait cette information sur la base du texte de l'article 12, § 2, dernier alinéa du projet.

125. Il se pose en outre la question de savoir dans quelles circonstances une personne concernée peut porter plainte auprès de n'importe quelle autorité de contrôle et que cette plainte "*ne porte que sur des données à caractère personnel émanant d'une autorité visée au titre 3*". En effet, l'article 12 du projet entend précisément exclure qu'une personne concernée *puisse* être au

---

[35]Article 12, premier alinéa : "*la personne concernée par le traitement de ses données à caractère personnel, émanant directement ou indirectement des autres autorités visées au titre 3 de la présente loi, ne bénéfice pas des droits visés aux articles 12 à 22 et 34 du Règlement, ainsi que du droit à la transparence*"/ Article 12, deuxième alinéa : "*les obligations visées aux articles 12 à 22 et 34 du Règlement ne s'appliquent pas aux autorités et personnes en possession de ces données*"/ Article 12, troisième alinéa : "*Le responsable du traitement ou l'autorité compétente ne fait aucune mention qu'il est en possession de données émanant des autorités visées au titre 3.*"

[36] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil.*

courant du fait que le responsable du traitement reçoit des données à caractère personnel des services de renseignement et de sécurité.

126. Enfin, la Commission fait remarquer que son successeur en droit ne prendra pas connaissance des "recours" émanant de la personne concernée, mais bien des requêtes et plaintes. On ne sait donc pas clairement sur quoi porte le terme "recours" et une harmonisation raisonnée s'impose avec les dispositions en matière d'accès indirect aux articles 80 à 84 inclus du titre 3 du projet. Ainsi, le législateur doit définir clairement et de manière linéaire l'ensemble du processus suivi par la personne concernée dans l'exercice de ses droits (et les éventuelles limitations de ceux-ci).

Article 13 du projet

127. L'article 13 du projet constitue le reflet logique de de l'article 12. Alors que l'article 12 du projet veut protéger les services de renseignement et de sécurité en tant que source, cet article entend atteindre un résultat similaire lorsque les services de renseignement et de sécurité sont destinataires. La Commission constate toutefois que cet article est superflu. Les services de renseignement et de sécurité ne relèvent en effet pas de la notion de "*destinataire*" telle que définie à l'article 4.9) du RGPD qui dispose que : "*Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément* […] *au droit d'un État membre ne sont pas considérées comme des destinataires*". Les services de renseignement et de sécurité font partie de cette catégorie d'exception. Il ressort d'ailleurs de l'Exposé des motifs que le demandeur adhère certes lui-même à ce point de vue[37], mais ne le répercute pas ensuite dans le texte du projet proprement dit.

128. L'article 13, deuxième alinéa conserve certes sa raison d'être pour les flux de données structurels ayant un encadrement légal spécifique. Le demandeur doit cependant se pencher sur la question de savoir si la communication d'informations générales au sujet de la collaboration avec les services de renseignement et de sécurité ne peut pas porter atteinte au secret d'une enquête ponctuelle. Imaginons que ces services collaborent avec un employeur pour suivre des personnes ayant un profil de risque en matière de terrorisme, est-il alors souhaitable que l'employeur informe de manière générale son personnel de ces contacts ?

Article 14 du projet

[37] Exposé des motifs, pp. 22 et 23.

129. L'article 14 du projet entend protéger l'identité des agents des services de renseignement et de sécurité lorsqu'ils consultent directement des banques de données dans le secteur privé ou public. Pour garantir le secret de cette enquête, cet article entend limiter, par des mesures de sécurité techniques et organisationnelles, l'accès aux loggings de ces banques de données à quatre acteurs : les deux responsables du traitement concernés et leurs délégués à la protection des données respectifs. Il ressort de la philosophie de l'Exposé des motifs qu'il devrait toujours s'agir d'une seule personne, permettant de limiter au strict minimum le nombre de personnes au courant de cet accès (quatre, donc)[38]. Le texte du projet proprement dit devrait spécifier qu'il ne s'agit toujours que d'une seule et même personne physique.

130. La Commission émet des réserves quant à la possibilité, créée par simple protocole d'accord entre les responsables du traitement concernés, non seulement de donner à des tiers un accès à ces loggings, mais aussi de permettre cet accès pour d'autres finalités. La Commission comprend la nécessité de faire appel à une tierce personne pour un support technique[39], mais l'accès par de tels tiers doit alors clairement s'inscrire dans le cadre des missions légales de contrôle des délégués à la protection des données et de leurs responsables du traitement. Le projet doit le préciser. L'article 14, troisième alinéa doit être supprimé car il est inacceptable du point de vue du principe de finalité. Les finalités doivent être déterminées par la loi elle-même.

131. L'article 14, dernier alinéa du projet permet à l'autorité visée au titre 3 du projet de déroger à cet article "*lorsqu'elle estime que son application à une banque de données déterminée n'est pas pertinente*". L'Exposé des motifs explique que ce paragraphe vise les banques de données communes au sens des articles 44/11/3*bis* à *quinquies* de la loi sur la fonction de police. Cette mise hors d'application pour ces banques de données spécifiques doit être reprise dans la loi elle-même. Les termes actuels de l'article 14, dernier alinéa conditionnent l'application de la loi à une compétence discrétionnaire dans le chef des autorités visée au titre 3. Le principe d'état de droit requiert toutefois que les organes publics soient également tenus au respect de la loi et ne puissent pas décider arbitrairement de l'application de ces lois.

132. Enfin, le projet doit aussi se référer aux dispositions légales spécifiques sur la base desquelles la consultation de banques de données tant publiques que privées est possible.

Article 15 du projet

[38] Exposé des motifs, page 31.

[39] Exposé des motifs, page 32.

133. L'article 15 du projet semble prévoir une exception similaire à celle de l'article 12, mais pour les services de police. Les personnes concernées ne peuvent pas opposer leurs droits à l'égard des "*destinataires prévus dans les articles 44/1, §§ 3 et 4 ainsi qu'aux articles 44/11/7 à 44/11/11 de la loi sur la fonction de police auxquelles* (sic) *ces données ont été transmises par les services de police*". Les §§ 3 et 4 de l'article 44/1 renvoient en essence aux autorités policières en leur qualité de police tant judiciaire qu'administrative. Le renvoi aux articles 44/11/7 à 44/11/11 comporte en outre un grand nombre d'acteurs qui sont soit une autorité compétente au sens de l'article 31.7 du projet, soit qui relèvent de l'article 75 du projet. La définition des destinataires est partiellement tautologique et concerne donc aussi les traitements de données à caractère personnel qui relèvent exclusivement du champ d'application de la Directive[40]. En outre, l'Exposé des motifs indique que l'exception pour d'autres acteurs énoncés dans l'énumération des articles 44/11/7 à 44/11/11 – par exemple le Comité P – est même superflue[41]. Dès lors, la portée de cette exception est obscure et l'Exposé des motifs ne peut pas non plus expliquer les circonstances exactes de cet article. Le projet doit définir avec précision les acteurs qui peuvent invoquer cette exception.

134. La Commission fait également remarquer que contrairement à ce que laisse suggérer l'article 15, cinquième alinéa du projet, il revient en premier lieu au législateur de prévoir les garanties appropriées au sens de l'article 23.2 du RGPD. Une absence totale de garanties législatives nécessaires ne peut être régularisée en renvoyant la balle au responsable du traitement lui-même.

135. L'article 15, dernier alinéa du projet dispose que toute demande d'exercice des droits de la personne concernée est transmise à l'autorité de contrôle compétente. De nouveau, la Commission souligne la nécessité de nommer l'autorité de contrôle et de mettre cette disposition légale en conformité avec les dispositions du chapitre III du titre 2 du projet, ou du moins de s'y référer. La formulation et la fragmentation actuelles n'offrent pas de vue claire sur l'ensemble du processus que la personne concernée doit parcourir dans l'exercice de ses droits et sur les mécanismes de contrôle dont elle peut se prévaloir.

Article 16 du projet

136. L'article 16 du projet prévoit une copie quasiment identique de l'article 15, mais cette fois pour les destinataires d'informations des autorités judiciaires. La seule différence se situe dans la disposition selon laquelle ces destinataires peuvent déroger aux limitations des droits de la personne concernée si la loi l'impose dans le cadre d'une procédure contentieuse ou si l'autorité

[40] L'Exposé des motifs semble d'ailleurs le confirmer lui-même à la page 35.

[41] Exposé des motifs, page 36.

judiciaire concernée l'autorise. La Commission se demande pourquoi cette disposition ne s'applique pas à l'article 15 du projet. On aurait pu ainsi rédiger une seule disposition d'exception consolidée pour tous les destinataires d'informations provenant des autorités compétentes au sens du titre 2 du projet.

137. En ce qui concerne les articles 12 à 16 et 18 du projet, la Commission remarque enfin que ces dispositions n'ont pas leur place dans le titre 1 du projet. La délimitation organique des champs d'application respectifs des titres 1, 2 et 3 ne tient pas assez compte des finalités poursuivies des différents acteurs, faisant apparaître de nombreuses imprécisions, par exemple pour la désignation de l'autorité de contrôle compétente.

138. Pour les services de renseignement et de sécurité, l'article 4.9) du RGPD est pourtant clair : "*les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière (...) ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.*" Bien que cette disposition se limite à la notion de destinataire, elle offre un argument de poids pour reprendre dans le titre 3 du projet les dispositions qui entendent protéger au titre de source les autorités telles que visées au titre 3 du projet.

139. Une remarque similaire s'applique aux articles 15 et 16 du projet qui disposent expressément que "*ces exceptions ne valent que pour les données traitées initialement […] pour les finalités visées à l'article 32 de la présente loi* ". Par ces termes, on reconnaît qu'à la lumière des finalités qu'il poursuit, les traitements envisagés relèvent essentiellement du titre 2 du projet. Les exceptions aux droits des personnes concernées à l'égard de tiers qui collaborent avec les autorités mentionnées dans le titre 2 ou 3 de cette loi – et donc pour des finalités spécifiques que poursuivent ces autorités – sont mieux mises en valeur dans ces titres respectifs.

Article 17 du projet

140. L'article 17 du projet dispose que "*Lorsque les données à caractère personnel figurent dans une décision judiciaire ou un dossier judiciaire, ou font l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale, les droits visés aux articles 12 à 22 et 34 du Règlement sont exercés conformément au Code judiciaire et au Code d'instruction criminelle.*" La Commission fait remarquer que les enquêtes judiciaires et procédures pénales relèvent du champ d'application de la Directive et n'ont donc pas leur place dans le titre 1 du projet.

141. En ce qui concerne les procédures qui relèvent du Code judiciaire, le législateur peut avoir l'intention illusoire de moduler l'exercice des droits de la personne concernée, mais cela n'empêche pas que le RGPD ait la priorité sur le droit national des États membres en vertu de la primauté du droit de l'Union[42]. Cet article de loi n'a dès lors aucune valeur ajoutée et donne au justiciable l'impression erronée que le Code judiciaire pourrait déroger au RGPD. Dans la mesure où le Code judiciaire veut déroger aux droits de la personne concernée, cela doit se faire aux conditions de l'article 23 du RGPD. Une telle disposition générique ne répond pas aux exigences de l'article 23 du RGPD. Les dispositions de la législation nationale en question doivent être confrontées à la condition énoncée à l'article 23, en vertu de laquelle : "*une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir :* (…) *d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;* (…) *f) la protection de l'indépendance de la justice et des procédures judiciaires*."

142. Un tel examen semble à première vue représenter un travail herculéen, mais ne devrait normalement pas poser de problème particulier étant donné que depuis de nombreuses années, la nouvelle législation est confrontée d'une part à l'article 8 de la CEDH et d'autre part aux principes de la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981[43], du Pacte international relatif aux droits civils et politiques, de l'ancienne directive européenne 95/46/CE[44] relative à la vie privée et bien entendu aussi de la LVP. On peut donc raisonnablement penser que la législation existante est conforme aux exigences de l'article 23 du RGPD. Mais échapper à cet examen via un article de loi général n'est pas acceptable.

143. Dans cet examen, il faut inclure non seulement le Code d'instruction criminelle et le Code judiciaire, mais aussi de nombreuses lois et réglementations qui légifèrent, généralement de manière plus détaillée, le traitement de données à caractère personnel et en particulier les droits du citoyen concerné. Pour donner un simple exemple : la loi relative aux perquisitions du 7 juin 1969, la loi ADN du 22 mars 1999, la loi concernant le Casier judiciaire central du 31 juillet 2009, … en ce qui concerne le droit pénal. On peut encore citer aussi notamment la

---

[42] Cour de justice, 9 mars 1978 (C-106/77), *Simmentahl*, §§ 22 et 24. En ce qui concerne l'application directe du droit international dans l'ordre juridique belge, voir : Cour de cassation, 27 mai 1971, Franco-Suisse Le Ski, *Arr. Cass.* 1971, 959.

[43] Conseil de l'Europe, Convention n° 108, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 janvier 1981.

[44] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*.

réglementation d'exécution comme l'arrêté royal du 21 juin 2011 *concernant la gestion des registres centraux des testaments et des contrats de mariage*[45].

Article 18 du projet

144. Enfin, la Commission ne voit pas quelle est la valeur ajoutée de l'article 18 du projet. Une application cumulative des articles 12, 15 et 16 du projet (réécrits en profondeur) devrait mener au résultat souhaité. L'Exposé des motifs doit expliquer la nécessité de cette disposition et expliquer comment cette exception intervient à l'égard des autres exceptions aux droits de la personne concernée. En outre, le projet omet de définir ce qu'il convient d'entendre par "*un traitement commun*" alors qu'il s'agit d'un élément constitutif de cette disposition légale qui est déterminant pour la définition du champ d'application. Il ressort des explications supplémentaires fournies par le demandeur que le projet vise les banques de données communes au sens des articles 44/11/3*bis*, 44/11/3*ter*, 44/11/3*quater* et 44/11/3*quinquies* de la loi *sur la fonction de police*. On ne peut le déduire ni du texte du projet, ni de l'Exposé des motifs. Le demandeur doit dès lors développer cette exception et la justifier à la lumière des besoins spécifiques découlant des banques de données communes dans la *loi sur la fonction de police.*

Conclusion générale pour le chapitre III du titre I

145. En résumé, toutes les exceptions qu'énumère le chapitre III du titre I sont caractérisées par une grande imprécision sur a) qui peut invoquer l'exception ; b) pour quelles finalités ; c) au sujet de quelles donnés ; et d) pour quelle durée. En outre, il manque des garanties légales suffisantes – ou des renvois à des garanties existantes – qui doivent offrir une protection contre une limitation arbitraire des droits de la personne concernée. Des dispositions légales dont l'ampleur est aussi imprécise ne respectent non seulement pas les exigences de l'article 23 du RGPD mais ne sont pas non plus raisonnablement prévisibles pour le justiciable au sens de l'article 8 de la CEDH en raison de leur ambigüité. Pour toutes ces raisons, l'avis de la Commission sur l'ensemble du chapitre III du titre I est défavorable.

Proposition d'amendement

146. La Commission propose la structure suivante pour établir des exceptions formulées plus clairement qui exécutent l'article 23 du RGPD dans la législation sectorielle applicable :

[45] Cf. pour les renvois légaux : Larcier thema wetboeken "privacy-wetgeving 2015", Willem Debeuckelaere, Gert Vermeulen, III.2: strafwetgeving en III. Gerechtelijk en burgerlijk recht.

1) Une disposition introductive qui indique le droit *spécifique* du RGPD auquel le législateur souhaite déroger, pour quelle finalité au sens de l'article 23.1 du RGPD cette dérogation a lieu d'être ainsi que l'exécution concrète de cette finalité à l'aide de la législation sectorielle applicable. Les acteurs qui peuvent invoquer cette exception doivent également être énumérés de manière exhaustive. Par exemple :

"*Par dérogation à l'article 15 du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), en vue de garantir [l'objectif de l'article 23.1 du RGPD], le droit d'accès aux données à caractère personnel la concernant peut être retardé, limité entièrement ou partiellement s'agissant des traitements de données à caractère personnel dont [les responsables du traitement et la description de leurs tâches et missions légales qui légitiment l'exception] sont le responsable du traitement."*

2) Une description des traitements pour lesquels cette exception s'applique. Par exemple :

"*Les traitements visés à l'alinéa 1er sont ceux dont la finalité est la préparation, l'organisation, la gestion et le suivi des enquêtes menées par les services visés à l'alinéa 1er, en ce compris les procédures visant à l'application éventuelle d'une amende administrative ou sanction administrative par les services compétents.*"

3) Une limitation dans le temps de cette exception – ou, si ce n'est pas possible, une justification étayée dans l'Exposé des motifs expliquant pourquoi l'exception n'a pas été imitée dans le temps (par exemple, pour les services de police et de renseignement, si une suspension temporaire des droits peut se révéler insuffisante). Par exemple :

"*Ces dérogations valent durant la période dans laquelle la personne concernée est l'objet d'un contrôle ou d'une enquête ou d'actes préparatoires à ceux-ci effectués par les services d'inspection précités dans le cadre de l'exécution de ses missions légales.*

La durée des actes préparatoires, pendant laquelle l'article 15 du règlement général sur la protection des données n'est pas applicable, ne peut excéder un an à partir de la réception de la demande introduite en application de l'article 15.

Lorsqu'un dossier est transmis au ministère public, les droits ne sont rétablis qu'après que le ministère public ait confirmé au service compétent soit qu'il renonce à engager des poursuites pénales, soit à

proposer une résolution à l'amiable ou une médiation au sens de l'article 216ter du Code d'instruction criminelle et que le service des amendes administratives compétent ait pris une décision.

Lorsqu'un dossier est transmis à l'administration dont dépend le service d'inspection ou à l'institution compétente pour statuer sur les conclusions de l'enquête, les droits ne sont rétablis qu'après que l'administration ou l'institution compétente ait statué sur le résultat de l'enquête."

4) Une délimitation claire du champ d'application matériel de cette exception. Par exemple :

"*Ces dérogations valent dans la mesure où l'application de ce droit nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires ou risque de violer le secret de l'enquête pénale.*

La restriction visée au paragraphe 1er, alinéa 1er, ne vise pas les données qui sont étrangères à l'objet de l'enquête ou du contrôle justifiant le refus ou la limitation d'accès."

5) Un mécanisme bien élaboré pour le traitement de plaintes ou de requêtes de la personne concernée (accès direct), le rôle du délégué à la protection des données étant assorti de délais stricts. Par exemple :

"*Dès réception d'une demande d'accès, le délégué à la protection des données du responsable du traitement en accuse réception.*

Le délégué à la protection des données du responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, de tout refus ou de toute limitation à son droit d'accès aux données la concernant ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des finalités énoncées au […]. Au besoin, ce délai peut être prolongé de deux mois, si cela est justifié par la complexité et le nombre de demandes. Lorsqu'il y a une prolongation du délai, le responsable du traitement doit informer la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande."

6) Un flux d'informations cohérent à l'égard de la personne concernée quant à l'application de cette exception et aux mécanismes de contrôle disponibles est également nécessaire. Par exemple :

"*Le délégué à la protection des données du responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'Autorité de protection des données ou de former un recours juridictionnel.*

Le délégué à la protection des données du responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition de l'autorité de contrôle compétente.

Lorsqu'un des services d'inspection précité a fait usage de l'exception telle que déterminée au […], la règle de l'exception est immédiatement levée après la clôture du contrôle ou de l'enquête. Le délégué à la protection des données du responsable du traitement en informe la personne concernée sans délai."

4.4. Chapitre IV - Responsable du traitement et sous-traitant

4.4.1. Section 1 - Dispositions générales

Accusé de réception des demandes d'exercice des droits

147. L'article 19 du projet impose un délai maximum d'un mois aux responsables de traitement pour l'envoi d'un accusé de réception à toute personne qui exerce ses droits en application du RGPD. La Commission considère que ce délai doit être réduit dans la mesure où, en vertu de l'article 12.3 du RGPD, tout responsable de traitement doit, en principe, endéans le mois suivant la réception de la demande, communiquer à la personne concernée les informations qu'il doit lui fournir en vertu des article 15 à 22 du RGPD.

4.4.2. Section 2 - Secteur public

148. La section 2 du chapitre III vise à encadrer spécifiquement les flux de données en provenance du secteur public.

Notions « d'autorité publique et d'organisme public »

149. D'un point de vue général, la Commission relève que le projet, en tant que la loi d'exécution du RGPD devrait définir les termes « autorités publiques ou organismes publics » utilisés par le RGDP, notamment à son article 37.1.a) (qui leur impose la désignation d'un délégué à la protection des données) et ce, afin d'atteindre un niveau de sécurité juridique correct. Dans ses lignes directrices sur le DPO, le Groupe de l'article 29 a mis en avant le fait que ces notions doivent être définies en fonction du droit national. Cette mesure d'exécution fait défaut dans le présent projet dans la mesure où les définitions proposées d'autorité publique et d'organisme public ne concernent que la section 2 du projet.

150. L'article 21 du projet définit les notions d'autorité publique et d'organisme public, visées par la section 2 du projet, comme « l'institution publique ou l'institution de droit privé ou de droit public qui fournit un service public ». Il précise que la section 2 est également applicable aux services de police.

151. Si la Commission comprend bien l'intention du législateur, il s'agit de viser toute personne morale de droit public et toute personne morale de droit privé créée ou agréée par les pouvoirs publics ou dont le fonctionnement est contrôlé par les pouvoirs publics, chargée par le législateur d'une mission de service public et disposant du pouvoir de prendre des décisions contraignantes vis-à-vis des tiers.

152. Si tel est le cas, il importe (i) que l'auteur du projet le précise explicitement, à l'article 21 en projet, en indiquant qu'il vise les « personnes morales de droit public et les personnes morales de droit privé créées ou agréées par les pouvoirs publics ou dont le fonctionnement est contrôlé par les pouvoirs publics , chargées par le législateur d'une mission de service public et disposant du pouvoir de prendre des décisions contraignantes vis-à-vis des tiers» et (ii) qu'il leur attribue un vocable commun tel que par exemple « organismes publics et privés ». Les termes « organisme public », actuellement utilisés dans le projet, prêtent à confusion. Dans la suite de son avis, la Commission fait usage des termes «organismes publics et privés concernés ou susvisés».

Encadrement des transmissions de données par les autorités publiques et organismes publics fédéraux (article 22 du Projet)

153. L'article 22 du projet prévoit un système optionnel d'encadrement des transmissions de données à caractère personnel par les organismes fédéraux publics et privés susvisés, par le biais de protocoles d'accord à adopter par les responsables de traitement concernés, après avis de leurs délégués à la protection des données (DPO) respectifs.

154. La Commission rappelle l'importance du respect du principe de légalité des traitements de données réalisés dans ce secteur. Un protocole d'échange ne pourra jamais constituer la base légale d'un traitement de données. Les sources authentiques de données à caractère personnel disposent d'un cadre légal précisant les éléments essentiels des traitements qui peuvent en être faits[46].

Obligatoire et non optionnel

[46] Cf loi du 8/08/1983 organisant un registre national des personnes physiques, loi du 19/05/2010 portant création de la Banque-carrefour des véhicules,…

155. Ceci étant, la Commission souscrit au besoin d'instaurer une routine systématique qui permettra aux DPO de préparer et d'analyser la mise en place d'un flux de données à caractère personnel pour la réalisation d'une mission de service public. Tout échange de données au sein des organismes publics et privés susvisés ne peut être réalisé qu'après que les responsables de traitement impliqués aient vérifié son caractère compatible avec les dispositions du RGPD et notamment, que la communication entre dans les missions de l'organisme public ou privé concerné qui communique les données et que la collecte de données entre dans les missions l'organisme public ou privé susvisé consultant/recevant les données. Par conséquent, la Commission considère que ce système qui participe à la mise en œuvre de l''accountability (responsabilité – article 5.2. du RGPD) des responsables de traitement doit être rendu obligatoire et non demeurer optionnel.

156. Il est en revanche, en lien avec l'approche par le risque qui sous-tend certaines des obligations découlant du RGPD pour les responsables de traitement et sous-traitants, indiqué de le limiter aux transmissions électroniques de données relevant de traitements à risque (tels que la réutilisation de données à caractère personnel pour des finalités différentes de celles pour lesquelles elles ont été collectées, ou l'échange de données entre des organismes publics ou privés susvisés poursuivant des missions de services public de nature différentes, ou encore des traitements portant sur des données sensibles, …).

157. Il est également envisageable d'en exclure certains traitements dont les risques sont limités (communication de données pseudonymisées à des fins de recherche scientifique conformément aux modalités visées par le chapitre spécifique y consacré dans la loi d'exécution du RGPD , ...). De plus, il est souhaitable de concilier ce système de protocole d'échange de données avec *l'avant-projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*[1]. A cet effet, il convient le cas échéant d'exempter de ce système de protocole d'échanges les communications de données par la Banque-carrefour de la sécurité sociale ou les institutions de sécurité sociale ou la plate-forme eHealth qui devront obligatoirement faire l'objet d'une délibération préalable de ce comité de sécurité de l'information.

158. La Commission s'interroge sur la pertinence de viser à l'article 22 en projet les flux de données vers des organismes privés qui ne poursuivent pas des missions de service public. Les communications électroniques de données émanant des organismes publics et privés susvisés ne

[1] Cf l'avis de la Commission sur cet avant-projet rendu en sa séance du 18 avril 2018.

concernent généralement que des flux de données pour la réalisation de missions de service public voire pour la réalisation de recherches scientifiques.

159. Quant au libellé de cet article 22, §1, alinéa 1er, la notion de « responsable de traitement destinataire des données » est à préférer à celle de « *responsable de traitement ultérieur* » étant donné que les flux visés ne consistent pas systématiquement en un traitement ultérieur de données.

Contenu du protocole

160. Quant au contenu du protocole, tel que l'article 22 en projet l'organise ; outre le fait que le législateur doit prévoir ses éléments obligatoires et non optionnels (« peut » doit être remplacé par « doit »), les remarques suivantes s'imposent :

a. Le point 2 « identification du responsable de traitement » doit être remplacé par « identification des responsables de traitement ». Par nature, l'échange de données visé à l'alinéa 1er de l'article 22, §1 en projet comporte au moins deux responsables de traitement ;
b. Le point 5 doit, non seulement, viser les catégories précises de données, mais également, leur format, conformément au principe de proportionnalité[47] ;
c. Le point 7 devrait être remplacé par « la ou les bases légales légitimant tant la communication que la collecte des données » ;
d. Le point 9 devrait être limité aux mesures de sécurité propres à sécuriser la transmission des données dans la mesure où c'est uniquement ce traitement d'échange de données qui est encadré par le protocole. De plus, la formulation de ces mesures doit être fonctionnelle afin d'éviter que ne soient dévoilés les détails sensibles des mesures techniques de sécurité et que les intéressés soient exposés à des attaques de sécurité ;
e. Le point 10 doit être supprimé car il est contraire à l'article 28 du RGPD. Sauf hypothèse d'un traitement de données réalisé par des responsables de traitement conjoints qui font ensemble appel à un sous-traitant, le responsable de traitement destinataire des données est seul responsable du choix de son propre sous-traitant.;
f. Le point 11 doit également être supprimé ; seul le législateur est compétent pour accorder des dérogations aux droits des personnes concernées et ce, dans les conditions prévues à l'article 23 du RGPD. Ce qui pourrait être prévu en lieu et place,

[47] Le principe de proportionnalité requiert que non seulement les données soient limitées au strict nécessaire pour la réalisation des finalités poursuivies mais leur format le soit également en ce sens qu'un format de type « oui ou non » ou « nombre de personnes composant un ménage » ou encore « niveau de revenu supérieur ou inférieur à tel montant » peut dans certains cas être amplement suffisant.

c'est que le traitement bénéficie de dérogations légales à certains droits des personnes concernées ainsi que la justification de leur application au cas d'espèce ;

g. La numérotation du titre auquel le point 16 renvoie est erronée, il devrait s'agir du titre 6;

h. Les points suivants doivent être ajoutés dans la mesure où ils sont inhérents à l'analyse des échanges de données visés:

   i. La description des finalités précises pour lesquelles les données ont été collectées à l'origine par l'organisme public ou privé susvisé, gestionnaire de la source de données accédée ;

   ii. En cas de traitement ultérieur[48] des données collectées, mention de l'analyse de compatibilité des finalités de ce traitement avec celle pour lesquelles les données ont été initialement collectées conformément à l'article 6.4 du RGPD ;

   iii. La vérification du respect du principe de « collecte auprès de la source authentique des données »qui garantit la qualité des données ainsi que le respect du cadre légal encadrant l'accès à la source authentique ;

   iv. Toutes mesures spécifiques encadrant le flux conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut (choix du format de la communication, journalisation des accès de manière telle que l'on puisse savoir qui a eu accès à quoi quand et pourquoi, mise en place d'un répertoire de références en cas de communication automatique des actualisations des données afin d'assurer que seules les données nécessaires soient actualisées et pour la durée nécessaire,…)

Avis des délégués à la protection des données

161. L'article 22, § 2 en projet doit prévoir que les avis des DPO seront annexés au protocole d'échange des données et que les dispositions préliminaires du protocole mentionneront, la justification du ou des responsable(s) de traitement lorsqu'il(s) s'écarte(nt) de l'avis du DPO.

Publicité du protocole

162. Afin d'assurer la prévisibilité des flux de données visés, ces protocoles d'échange devront faire l'objet d'une publication au Moniteur belge. Il convient de le prévoir explicitement à l'article 22 en

[48] Utilisation des données pour une ou des finalité(s) différente(s) de celle(s) pour la(les)quelle(s) elle(s) a(ont) été collectée(s) à l'origine par l'autorité ou l'organisme public qui communique les données.

projet. Dans la mesure où ces protocoles vont encadrer les traitements de données des citoyens, ils doivent répondre aux critères de prévisibilité et d'accessibilité[49].

Régions et Communautés

163. Enfin, dans la mesure où les échanges électroniques de données liés à l'E-gouvernement ne sont - par nature - pas limités aux flux entre les organismes fédéraux publics ou privés susvisés, la Commission considère qu'un encadrement spécifique doit s'étendre aux Régions et Communautés, ce qui peut être obtenu d'un accord de coopération auquel l'assentiment des législateurs sera accordé, ainsi que le prévoit l'article 92 bis, §1 de la loi spéciale de réformes institutionnelles du 8 août 1980[50].

Encadrement des Registres d'activités de traitement (articles 23 et 24 du Projet)

164. Dans un but d'uniformisation, les articles 23 et 24 du projet encadrent les registres de traitements de données à caractère personnel tenus par les organismes publics ou privés susvisés en application de l'article 30 du RGDP[51].

165. A ce sujet, la Commission s'interroge sur la pertinence d'uniformiser les modalités de gestion et de tenue du registre au vu des diversités de traitements de données à caractère personnel auxquels sont confrontés les responsables de traitement et sous-traitants de ce secteur. La centralisation des registres ne présente aux yeux de la Commission aucune plus-value pour la future autorité de protection des données.

166. Par conséquent, l'article 24 en projet doit être supprimé (le RGDP prévoyant aussi déjà que le registre doit avoir la forme d'un écrit électronique). Surabondamment, des mesures transitoires devraient être prévues et enfin, le §1 de l'article 23 apparait redondant avec l'article 30 du RGPD qui prévoit déjà l'obligation de tenue du Registre dans le chef des responsables de traitement visés.

Contenu du Registre

167. Pour le surplus, la Commission admet l'utilité d'imposer aux organismes publics et privés concernés que leurs registres contiennent des éléments complémentaires à ceux prévus à l'article

---

[49] Cf à ce sujet CJCE, 1/10/2015, Affaire Smaranda Bara, ECLI :EU :C :2015 :638 ; CEDH, 4/12/2015, allfaire Roman Zakarov c.Russie https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160008%22]}

[50] Cf à ce sujet Elise Degrave, *L'e-gouvernement et la protection de la vie privée – Legalité, transparence et contrôle,* Collection du CRIDS, Larcier, 2014, p. 295 et s.

[51] la Commission se demande dans quelle mesure certaines parties de ce projet de loi sont encore actuelles, vu que ça ne correspond pas avec l'explication donnée à ce sujet le 5avril 2018 chez le SPF BOSA.

30 du RGDP lorsque des spécificités s'imposent à eux en matière de traitement de données à caractère personnel. Par souci de lisibilité, la rédaction de l'article 23 devrait être revue en ce sens. A l'analyse, l'auteur du projet pense aux points complémentaires suivants : le recours éventuel au profilage, la base juridique, les catégories de sources externes, le protocole d'échange de données, l'avis du DPO et la motivation du responsable de traitement lorsque l'avis de son DPO n'est pas suivi. Les remarques suivantes peuvent être faites à ce sujet :

a. La rubrique profilage devrait être optionnelle et complétée par « la référence, le cas échéant, à la disposition légale visée à l'article 22 du RGPD ».
b. Les points « base juridique » et « catégories de sources externes » devraient être précisés. Vise-t-on la base légale encadrant le traitement de données ou la base légale encadrant la mission de service public du responsable de traitement ou les deux ? Quant aux catégories de sources externes, vise-t-on (la) ou les sources de données à caractère personnel auprès (de laquelle) desquelles le responsable de traitement collecte des données indirectement pour réaliser sa mission de service public ? Pourquoi viser uniquement les catégories de sources et pas les sources à part entière ?
c. Les points complémentaires suivants pourraient être ajoutés[52] :
    i. La dénomination du traitement (à ne pas confondre avec sa finalité) ;
    ii. La précision au regard de chaque finalité de traitement, si des catégories particulières de données au sens des articles 9 et 11 du RGDP sont traitées ;
    iii. La désignation, pour chaque finalité de traitement, du service auprès duquel les personnes concernées peuvent exercer leurs droits ;
    iv. Si, au regard de chaque finalité de traitement, le traitement a nécessité la réalisation d'une analyse d'impact à la protection des données et les références au document administratif la contenant ;
    v. Le cas échéant, pour chaque finalité de traitement concernée, des motifs sur lesquels le responsable de traitement se fonde pour justifier qu'il rentre dans une des dérogations légales aux droits des personnes concernées ;
    vi. Le relevé des violations de données à caractère personnel requis par l'article 33.5 du RGPD.

Le Registre ne peut être établi auprès de l'APD

169. Les § 4 et 5 de l'article 23 en projet prévoient que le registre de traitement est tenu auprès de l'autorité de protection des données (sauf celui de la Police qui est simplement mis à la disposition de l'autorité de protection des données), ce qui est contraire au RGDP dans la mesure où il n'entre pas dans ses missions d'assurer la tenue de ces registres et où la gestion d'un tel système informatique impacterait négativement son budget (alors que la volonté

[52] Cf la Recommandation 06/2017 de la CPVP du 14 juin 2017 relative au registre des activités de traitements

gouvernementale est de réaliser autant que faire se peut une réforme budgétairement neutre[53]). Selon le RGPD, la tenue du registre de traitement reste de la responsabilité de chaque responsable de traitement et sous-traitant. Dans la mesure où le RGDP prévoit déjà que le registre doit être mis à disposition de l'autorité de contrôle à sa demande, ces deux paragraphes doivent être supprimés.

Publicité du Registre

170. Sur la question de la publicité du registre abordée par l'article 24 en projet, la Commission rappelle que le registre des traitements est avant tout un outil d' « accountability » interne pour le responsable de traitement et le sous-traitant[54]. Prévoir potentiellement (par Arrêté royal) le caractère public de ce registre (art. 24 en projet) est contraire à la *ratio legis* de l'article 30 du RGDP.

171. Pour répondre à la problématique de l'opacité des échanges électroniques de données entre les organismes publics et privés concernés, il convient de prévoir un système de publicité active qui peut être réalisé par un portail spécifique à la disposition des citoyens qui pourront, moyennant authentification préalable, (i) voir les différentes catégories de flux de leurs données au sein des organismes publics ou privés concernés, avec leur(s) finalité(s), la référence à leur protocole d'échange spécifique et la date de leur publication au Moniteur belge ; (ii) contrôler l'utilisation qui sera faite de leurs données à caractère personnel ; (iii) corriger les éventuelles erreurs sur leurs données[55] et enfin, (iv) entrer facilement en contact avec le délégué à la protection des données de l'organisme public ou privé concerné. Un tel système complèterait utilement les droits d'accès électroniques déjà prévus à divers niveaux (Registre national…). Au vu de l'article 2 de la loi du 11 avril 1994 relative à la publicité de l'administration et de l'AR du 19 juillet 2001 portant exécution de l'article 2, 1°, de la loi du 11 avril 1994 relative à la publicité de l'administration, il est peut être considéré que la création de ce portail relève des compétences du SPF Chancellerie du Premier Ministre.

---

[53] La Commission ne souscrit pas au passage de l'exposé des motifs relatif à cette disposition en projet (p. 45). Outre le fait qu'un système de registres publics centralisés auprès de la CPVP s'inscrit dans une logique que le GDPR a sciemment abandonné (Registre des déclarations de traitements), La tenue d'un tel système informatique impliquerait pour l'APD le développement de ressources IT spécifiques allouées à ce système; ce qui représenterait un coût important. Si le point b (impact budgétaire) de la page 3 de la note au Conseil des Ministres du 9/03/2018 traite de ce système, la Commission relève également le caractère erroné de son 2nd paragraphe. Aucune infrastructure technique actuelle ne pourrait matériellement être récupérée pour ce faire.

[54] Cf la Recommandation 06/2017 précitée

[55] Cf à ce sujet l'avis CPVP 02/2018 du 17 janvier 2018 sur le projet d'AR déterminant les critères sur base desquels des données sont qualifiées d'authentiques et l'avis 8/2017 du contrôleur européen à la protection des données sur la proposition de Règlement établissant un portail numérique unique et sur le principe « une fois pour toutes ».

Hypothèses additionnelles de désignation obligatoire de DPO (art. 25 du Projet)

172. L'article 25 en projet prévoit les cas de désignation obligatoire de DPO supplémentaires à ceux prévus par l'article 37.1 du RGDP. La Commission s'étonne de l'ampleur du champ d'application de l'article 25 dans la mesure où il couvre toutes les personnes morales de droit privé[56] intervenant comme sous-traitant des organismes fédéraux publics ou privés susvisés et/ou collectant auprès d'eux des données à caractère personnel. Il est indiqué de privilégier l'approche par le risque choisie par le RGPD et de ne soumettre à cette obligation que les responsables de traitement ou sous-traitants qui réalisent des traitements impliquant un certain risque (ampleur du nombre de personnes concernées par leur traitements, réalisation de missions de service public (monopole) nécessitant le traitement de données à caractère personnel des usagers de leurs services publics,…).

173. Le §2 de l'article 25 peut être supprimé dans la mesure où la délégation est déjà prévue à l'article 37.4 du RGPD.

Avis du DPO (article 26 du Projet)

174. L'article 26 en projet impose au organismes fédéraux publics ou privés susvisés de solliciter systématiquement l'avis du DPO préalablement à chaque traitement de données. Pour les échanges de données entre ces organismes, la Commission renvoie à ses propos repris ci-dessus. Pour le surplus, la Commission considère qu'imposer un avis systématique du DPO pour chaque traitement de données ne cadre pas avec l'approche par le risque du RGDP. L'article 39 du RGDP encadre déjà les tâches du DPO et prévoit que le responsable de traitement et le sous-traitant sont tenus de faire en sorte qu'il dispose des ressources et moyens nécessaires pour réaliser sa mission. Il prévoit également que « *le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.*" Le Groupe de l'article 29 en a déduit, dans ses lignes directrices, que les DPO devront établir des priorités dans leurs activités et concentrer leurs efforts sur des questions qui présentent un risque élevé en matière de protection des données[57].

Groupe d'experts (article 27 du Projet)

175. L'article 27 en projet prévoit la possibilité de créer un groupe d'experts composé de responsables de traitement pour agir en tant que plateforme de concertation dans la cadre du développement de la politique relative à la protection des données au sein du organismes fédéraux

[56] La formulation "personne morale de droit privé" est préférable à celle utilisée d' «*organisme privé* ».

[57] Lignes directrices du Groupe de l'article 29 concernant le DPO adoptées le 5 avril 2017, p. 22

publics ou privés susvisés. Au vu de l'objet de la concertation de ce groupe d'expert, il serait utile et pertinent d'y associer les DPO. De plus, l'article 27 en projet devrait préciser les missions concrètes de ce groupe d'experts.

176. L'article 28 § 1 en projet peut être supprimé car l'article 35.1 du RGPD prévoit déjà l'obligation du responsable de traitement de demander conseil au DPO dans le cadre de la réalisation de l'analyse d'impact relative à la protection des données (DPIA). La Commission est en effet d'avis que le libellé de l'article 39.1.c. ne remet pas en cause cette obligation.

Application de l'article 35.10

177. L'article 28 § 2 en projet précise qu'une analyse DPIA doit être faite avant de réaliser un traitement, même si une analyse d'impact a été réalisée préalablement « dans le cadre de l'adoption d'une base juridique ». Cette position est conforme à celle que la Commission a explicitée dans sa recommandation 01/2018 du 28 février 2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable et l'application de l'article 35.10. du RGPD.

4.5. Chapitre V - Traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire

Exécution de l'article 85 du RGPD

178. L'article 85 du RGPD impose à chaque Etat membre d'adopter des dispositions légales en vue de concilier les deux droits fondamentaux que sont le droit la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, y compris les traitements à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire. Pour ces traitements, l'article 85.2 du RGPD permet aux Etats membres de prévoir des dérogations ou exemptions à certains chapitres du RGDP dans la stricte mesure nécessaire pour concilier ces deux droits fondamentaux ; ce qui est l'objet du chapitre V du projet.

Notion de traitement de données à caractère personnel à des fins journalistiques

179. L'article 29 en projet donne une définition claire de la notion de traitement de données à caractère personnel à des fins journalistiques, qui met l'accent sur le fond de l'information et non sur sa forme, conformément à la jurisprudence de la CJUE[58]. A l'instar de la « loi vie privée française » actuelle[59], la Commission recommande d'y ajouter un notion de respect des règles

[58] Cf Arrêt du 16 décembre 2008, Satamedia, C-73/07, EU:C:2008:727, point 61.

[59] Art 67 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

déontologiques du journalisme dans les termes suivants : « et dont le responsable de traitement s'impose le respect des règles déontologiques journalistiques ».

Base légale

180. L'exposé des motifs relatif à l'article 29 en projet contient un passage sur la base de licéité des traitements journalistiques. Il y est mentionné que cette base de licéité est l'article 6.1.f du RGDP (intérêt légitime du responsable de traitement). Cette disposition ne peut constituer l'unique base de licéité potentielle car, dans certaines circonstances, des traitements de données à caractère journalistique requièrent le consentement de la personne à propos de laquelle un reportage est réalisé. Il convient par conséquent de pondérer en ce sens ce passage de l'exposé des motifs.

Dérogations

181. Les § 3 et suivants de l'article 29 contiennent :

(i) des dérogations **aux droits des personnes concernées** (droit à l'exercice des droits en cas de ré-identification de la personne concernée sur base d'informations fournies par elle-même, droit d'information préalable, droit d'accès, droit de rectification, droit à la limitation du traitement, droit d'opposition),

(ii) des exemptions **au respect de certaines obligations imposées par le RGPD** en faveur des responsables de traitements et des sous-traitants (mise à disposition du Registre des traitements de données à l'autorité de protection des données, obligation de collaborer avec elle, obligation de notification des fuites de données, obligation de consultation de l'APD pour les études préalables d'impact sur la protection des données réalisées dont il ressort que le risque résiduaire du traitement concernés reste élevé, dérogations au chapitre sur les flux transfrontaliers de données),

(iii) (iii) des dérogations **à l'exercice des pouvoirs de la future autorité de protection des données (APD).**

Les remarques ci-dessous s'imposent au regard de ces dérogations.

Dérogations aux droits des personnes concernées

182. Le §3 de l'article 29 doit être supprimé. Il est inutile de prévoir une dérogation à l'article 11.2 du RGDP car, si l'hypothèse visée à l'article 11.2 du RGDP se réalise, la personne concernée ne pourra exercer les droits que lui confère le RGPD dans la stricte mesure prévue par la réglementation d'exécution du RGPD (qui aura atteint un équilibre optimal pour le respect tant du droit à la liberté d'expression que de celui à la protection des données).

Droit à la limitation du traitement

183. Le §7 de l'article 29 en projet dispense les responsables de traitement concernés du respect du droit à la limitation de traitement (art. 18 RGDP) si l'exercice de ce droit peut compromettre une publication en projet. L'exercice du droit à la limitation du traitement pourra consister en pratique à déplacer temporairement les données vers un autre système d'information, à rendre les données sélectionnées temporairement inaccessibles ou encore à retirer temporairement de données publiées sur un site internet[60].

184. La Commission peut comprendre la nécessité de déroger à ce droit lorsque la personne concernée exerce son droit d'opposition visé à l'article 21.1 du RGPD (18.1.d du RGPD) et lorsque l'exactitude des données est contestée par la personne concernée (hypothèse visée à l'article 18.1.a du RGPD) bien qu'il convienne de faire la distinction entre la soumission de l'opinion journalistique à un test de vérité – ce qui ne peut être fait sans empiéter sur le droit à la liberté d'expression et à la liberté de la presse – et la vérification du caractère exact des données à caractère personnel sur lesquelles une opinion journalistique se base.

185. Les hypothèses visées à l'article 18.1.b et c (le traitement est illicite et la personne en exige la limitation au lieu de son effacement, ou bien le responsable de traitement n'a plus besoin des données mais elles sont encore nécessaires à la personne concernée pour sa défense en justice) ne doivent pas être couvertes par la dérogation en projet pour la mise en balance entre le droit à la liberté d'expression et le droit à la protection des données. L'article 29, §7 doit être corrigé sur ce point.

Droit d'opposition

186. L'article 29, §8 en projet dispense les responsables de traitement du respect du droit d'opposition des personnes concernées prévu à l'article 21.1 du RGPD. Il est disproportionné d'y déroger sans limite. A l'instar de ce qui déjà prévu dans la loi vie privée actuelle, il convient de préciser que cette dispense vaut uniquement si l'exercice du droit d'opposition visé à l'article 21.1 est susceptible de compromettre une publication en projet.

Droit à l'effacement

187. En qui concerne le droit à l'effacement, la Commission remarque que le projet n'y prévoit aucune dérogation. Elle ne partage pas l'interprétation de l'article 17.3 reprise dans l'exposé des motifs, selon laquelle une dérogation n'est pas nécessaire au motif que selon l'article 17.3., le

[60] Cf considérant 67 du RGDP.

droit à l'effacement ne serait pas applicable aux traitements à des fins de liberté d'expression et d'information.

188. L'article 17.3 du RGPD prévoit en effet que *« les paragraphe 1 et 2 (de l'article 17) ne s'appliquent pas dans la mesure où ce traitement est nécessaire à l'exercice du droit à l'exercice du droit à la liberté d'expression et d'information »* ; ce qui implique qu'une balance des intérêts doit être réalisée entre les deux droits fondamentaux lorsque le droit à l'effacement est exercé, pour que la limitation au droit à l'effacement ne soit imposée que dans la stricte mesure nécessaire au droit à la liberté d'expression. L'exposé des motifs doit être corrigé sur ce point[61] et au vu de l'expérience de la Commission en la matière, un intervention législative est préconisée à ce sujet. Elle propose la formulation suivante :

> Proposition : *« L'article 17 du Règlement est applicable aux traitements de données à caractère personnel à finalités journalistiques ou d'expression universitaire, artistique ou littéraire si leur contenu informatif ne présente pas ou plus de pertinence pour le débat d'intérêt général ou si leur préservation en l'état d'origine n'est pas indiquée au vu de leur contenu ou de leur forme ou des circonstances et des répercussions de leur contenu informatif sur la ou les personnes concernées. L'effacement revêt l'une des formes suivantes, tenant compte de l'évolution de l'état de la technique:*
> *a) l'anonymisation du contenu informatif ;*
> *b) l'adoption de mesures techniques qui, sans altérer la possibilité de prendre connaissance du contenu informatif litigieux auprès du responsable de traitement, permettent au minimum d'en limiter la diffusion. (L'exposé des motifs fera à ce sujet utilement référence aux modifications du référencement habituel, à la mise en place de balise No index qui empêche le référencement de l'article par les moteurs de recherche ou encore à la mise à disposition d'une version pseudonymisée au public …) ».*

Dérogations aux obligations en tant responsable de traitement ou sous-traitant
Mise à disposition du registre à l'APD
Notification des violations de données à l'APD
Consultation préalable de l'APD

189. En ce qui concerne l'exemption à la mise à disposition du registre de traitement sur demande de l'APD (article 30.4 du RGDP), la Commission ne l'estime pas nécessaire et donc contraire au RGPD ; en effet, le RGDP ne requiert pas du registre de traitement qu'il contienne l'identité des

[61] La référence à l'Arrêt Google Spain de la CJCE devait également être supprimée dans la mesure où dans la mesure que cet arrêt traite que des prestataires intermédiaires qui diffusent l'information et non pas sur la source journalistique qui publie les informations en tout premier lieu.

personnes concernées par le traitement des données. La mise en balance des deux droits fondamentaux précités ne justifie donc pas cette exemption. Il en est de même pour les articles 33 (notification des violations (fuites) de données) et 36 (consultation préalable de l'APD pour les DPIA). L'article 29, §8, en projet doit donc être supprimé. En aucun cas, l'exécution de ces dispositions ne peuvent/doivent amener à dévoiler à l'autorité de protection des données le contenu d'un article de presse en cours de publication et potentiellement mener à un acte de censure.

Obligation de coopération avec l'APD

190. En ce qui concerne l'exemption à l'obligation de coopération du responsable de traitement avec l'autorité de protection des données (article 31 du RGPD) prévue à l'article 29, §9 en projet et la limitation de tous les pouvoirs de l'autorité de protection des données vis-à-vis de ces traitements lorsque leur exercice « fournirait des indications sur les sources d'information ou constituerait une mesure de contrôle préalable à la publication d'un article » visée à l'article 29, §11 en projet, la Commission en constate le caractère disproportionné. La dérogation à l'article 31 du RGPD n'est pas nécessaire dans la mesure où sa mise en œuvre n'implique pas une obligation de divulgation des sources d'information. Quant à l'article 29, §11 en projet, il convient de le reformuler de la façon suivante

Proposition : *« L'autorité de protection des données exerce, vis-à-vis des responsables de traitement et sous-traitant réalisant des traitements de données à caractère personnel à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire, ses pouvoirs visés à l'article 58.1 et 2. du Règlement sans prendre connaissance des sources d'information journalistique et sans procéder à l'évaluation d'une opinion journalistique, universitaire, artistique ou littéraire »*.

191. La Commission relève également que l'article 64 de la loi du 3 décembre 2017 portant création de l'autorité de protection des données (APD) prévoit que les enquêtes de son futur service d'inspection seront secrètes, sauf exception légale, jusqu'au dépôt du rapport de l'inspecteur général auprès de la chambre contentieuse. L'article 48 de cette même loi prévoit que tant les membres de l'Autorité de protection des données que les membres de son personnel seront légalement tenus à une obligation de confidentialité quant aux faits, actes ou renseignement dont ils ont connaissance en raison de leurs fonctions.

CONCLUSION de la Commission sur le titre 1 du Projet

192. L'avis de la Commission est défavorable sur l'entièreté du chapitre III du titre I du projet pour les motifs résumés dans le numéro 145 du présent avis et favorable sur le reste des dispositions du projet à la condition de tenir compte des remarques suivantes :

1.1. Concernant le chapitre I

1.1.1. Adaptation de l'article 6 en projet pour y délimiter clairement le champ d'application du titre 1;

1.2. Concernant le chapitre II

1.2.1. Précision que l'article 7 en projet exécute l'article 8.1. du RGPD ;

1.2.2. Suppression de l'article 8, al. 1, 2° en projet – ce traitement doit être encadré par un texte de loi autonome conforme aux exigences de l'article 9.2.g du RGPD et qui reprend au moins les garanties pour les personnes concernées déjà prévues aux alinéas 2 à 6 du §6 de l'article 3 de la loi vie privée actuelle ;

1.2.3. Suppression des litera 1° et 3° de l'alinéa 1 de l'article 8 en projet déjà couverts par les litera d. et h. de l'article 9.2 du RGPD :

1.2.4. Révision de l'article 9,§1er, 4° comme recommandé pour prendre en compte la recherche historique et les responsables de traitement chargés de mission de service public d'archivage dans l'intérêt public général ;

1.2.5. Ajout de garanties particulières pour le traitement des données génétiques, biométriques ou des données relatives à la santé afin de pas diminuer le niveau de protection actuel atteint par la législation actuelle ;

1.2.6. Dans la version néerlandaise de la définition de la notion de donnée judiciaire, remplacement des termes « strafbare feiten » par « strafrechterlijke inbreuken » ;

1.3. Concernant le chapitre IV

1.3.1. Réduction du délai prévu pour l'envoi de l'accusé de réception aux personnes concernées visé à l'article 19 en projet ;

1.3.2. Définition des termes « autorités publiques et organismes publics » utilisés par le RGPD ;

1.3.3. Rectification de la définition de la notion d'autorité publique ou d'organisme public proposée à l'article 21 en projet afin de circonscrire avec précision et clarté le champ d'application de la section 2 de ce chapitre;

1.3.4. Modification du système optionnel de protocole d'échange de données, visé à l'article 22 en projet, en un système obligatoire limité aux flux de données visés à risque pour les droits et libertés des personnes concernées ;

1.3.5. Adaptation du contenu du protocole aux remarques de la Commission ;

1.3.6. Prévision explicite, dans l'article 22 en projet, que les avis des DPO seront annexés aux protocoles ;

1.3.7. Mention à l'article 22 en projet que les protocoles seront publiés au Moniteur belge conformément aux critères de prévisibilité et d'accessibilité ;

1.3.8. Encadrement des flux visé à un niveau national par le biais d'accords de coopération approuvés par les législateurs ;

1.3.9. Suppression de l'article 24 en projet (registre de traitement du secteur public centralisés et gestion harmonisée) ;

1.3.10. Adaptation du contenu du registre du secteur public (art. 23 en projet) aux remarques de la Commission ;

1.3.11. Suppression des § 4 et 5 de l'article 23 en projet car contraires au RGPD (tenue centralisée des registres auprès de l'APD) et impact budgétaire lourd potentiel de cette mesure sans réelle plus-value au regard des missions de service public de l'APD ;

1.3.12. Suppression de l'article 24 en projet prévoyant que le Roi peut décider du caractère public du registre de traitement du secteur public et remplacement par un système de publicité active tel que prôné par la Commission ;

1.3.13. Limitation de l'élargissement de l'obligation de désignation d'un DPO (art. 25 en projet) conformément à l'approche par le risque de certaines obligations dans le RGPD) ;

1.3.14. Limitation du caractère obligatoire des avis des DPO (art. 26 en projet) conformément à à l'approche par le risque de certaines obligations dans le RGPD et aux lignes directrices du Groupe de l'article 29 ;

1.3.15. Suppression de l'article 28, §1 en projet pour redondance par rapport au RGPD ;

1.4. Concernant le chapitre V

1.4.1. Ajout de la notion de respect du code de déontologie journalistique à la définition de traitement de données à caractère personnel à des fins journalistiques ;

1.4.2. Adaptation de l'exposé des motifs concernant la base de licéité des traitements de données à des fins journalistiques ;

1.4.3. Suppression de l'article 29, §3 en projet ;

1.4.4. Limitation de la dérogation au droit à limitation de traitement, prévue à l'article 29, §7 en projet, aux hypothèses visées à l'article 18.1.a et d. du RGPD ;

1.4.5. Limitation de la dérogation au droit d'opposition des personnes concernées, visée à l'article 21.1 du RGPD, prévue à l'article 29,§8 en projet, aux cas où l'exercice de ce droit compromettrait une publication en projet ;

1.4.6. Ajout d'une dérogation au droit à l'effacement des données (art.17 RGPD) comme proposé par la Commission et correction de l'exposé des motifs sur ce point ;

1.4.7. Suppression de l'article 29, §8 en projet (dérogation à l'obligation de mise à disposition de l'APD du registre sur demande, à l'obligation de notification des fuites de données à l'APD, à l'obligation de collaboration avec l'APD, à l'obligation de consultation préalable de l'APD pour les DPIA) ;

1.4.8. Adaptation de l'article 29, § 9 en projet (limitation des pouvoirs de l'APD vis-à-vis des responsables de traitements visés au strict nécessaire) tel que proposé.

5. TITRE 2 : DE LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR LES AUTORITÉS COMPÉTENTES À DES FINS DE PRÉVENTION ET DE DÉTECTION DES INFRACTIONS PÉNALES, D'ENQUÊTES ET DE POURSUITES EN LA MATIÈRE OU D'EXÉCUTION DE SANCTIONS PÉNALES, Y COMPRIS LA PROTECTION CONTRE LES MENACES POUR LA SÉCURITÉ PUBLIQUE ET LA PRÉVENTION DE TELLES MENACES

193. Les titres 2 en 3 du Projet concernent respectivement le traitement de données à caractère personnel dans la chaîne policière et pénale d'une part et par les services de renseignement et de sécurité, les forces armées et l'Organe de coordination pour l'analyse de la menace d'autre part. Vu le bref délai dans lequel l'avis de la Commission doit être rendu, cette partie ne comporte qu'une analyse de quelques problèmes marquants.

REMARQUES RELATIVES AU TITRE 2

194. Le titre 2 transpose en droit belge la Directive Police et Justice. Il s'agit du traitement de données à caractère personnel "*par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces*" (article 1.1. de la Directive Police et Justice).

195. La Directive Police et Justice ne s'applique pas aux activités de traitement de données à caractère personnel qui ne relèvent pas du champ d'application du droit de l'Union ni aux traitements réalisés par les institutions, organes et organismes de l'Union (article 1.3. de la Directive Police et Justice). Cette Directive ne s'applique par conséquent pas aux traitements de données à caractère personnel dans le cadre de la garantie de la sécurité nationale et de la défense, qui sont régis distinctement au titre 3.

196. La distinction entre le RGPD et la Directive Police et Justice se situe surtout dans une limitation des obligations de transparence et des droits de la personne concernée, comme l'accès indirect aux données à caractère personnel, une absence de droit d'opposition ou de droit à l'oubli et une absence de droit à la portabilité des données à caractère personnel. Par ailleurs, aucun système contraignant de sanctions administratives n'est imposé non plus.

Délimitation dans le cadre de la finalité : champ d'application

197. L'article 32 du Projet reprend la finalité telle que décrite à l'article 1.1. de la Directive Police et Justice. Comme il ressort de l'article 1.1. de la Directive Police et Justice, le champ d'application personnel est limité aux "autorités compétentes". D'après la Directive Police et Justice, il s'agit en bref de "*toute autorité publique compétente*" pour la finalité décrite à l'article 1.1. ou "*tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique*" en vue de cette finalité. L'article 31.7.a) à g) inclus du Projet vise les entités suivantes :

a) les services de police réguliers ;
b) les autorités judiciaires, entendues comme les cours et tribunaux et le ministère public ;
c) le service d'enquêtes du Comité P ;
d) l'Inspection générale de la police fédérale et de la police locale ;
e) l'Administration générale des douanes et accises, dans le cadre de sa mission relative à la recherche, la constatation et la poursuite des infractions ;
f) l'Unité d'information des passagers, et
g) la Cellule de Traitement des Informations Financières.

198. En ce qui concerne le champ d'application matériel, l'Exposé des motifs souligne que le Projet doit être appliqué de manière restrictive de manière à pouvoir suivre au mieux le champ d'application personnel de la Directive Police et Justice. D'après l'Exposé des motifs, cela implique que d'autres autorités "*administratives*" ne sont pas considérées comme une autorité compétente au sens de ce titre, même si elles sont "*compétentes pour le contrôle, l'inspection, ou la poursuite d'infractions pénales*". Si les activités de traitement de ces autorités administratives ne relèvent pas de la finalité de la Directive Police et Justice, le RGPD s'applique[62].

199. La Commission constate toutefois que l'on n'indique aucun critère ni point de rattachement univoque sur la base duquel les autorités compétentes sont désignées. Alors que l'on recherche pourtant bien des points de rattachement avec la finalité de la Directive Police et Justice, il ne semble pas que ce soit le cas pour toutes les autorités compétentes désignées. Ainsi, à l'article 31.7.c) du Projet, le Service d'enquêtes du Comité P est considéré comme une "autorité compétente", "*dans le cadre de ses missions judiciaires*". Le Comité P a en effet une double mission, à savoir une mission administrative et une mission judiciaire, de sorte que la mission

[62] Exposé des motifs, pages 64 et 69.

administrative ne relève pas du champ d'application du titre 2[63]. Ce même raisonnement n'est toutefois pas appliqué à l'Inspection générale de la police fédérale et de la police locale (IG) et à l'Unité d'information des passagers (UIP). L'IG a également une double mission[64], mais la délimitation spécifique pour les missions judiciaires n'est pas établie expressément à l'article 31.7.d). L'Unité d'information des passagers est un organe administratif qui reçoit, dans une première phase, des données à caractère personnel de compagnies aériennes dans le cadre de l'application du RGPD, mais couple, dans une deuxième phase, les données à caractère personnel à des données policières en vue de la prévention et la détection des infractions terroristes et des formes graves de criminalité ainsi que pour les enquêtes et les poursuites en la matière[65]. Ensuite, à l'article 31.7.e) du Projet, "*l'Administration générale des douanes et accises*" (AGDA) est également considérée comme autorité compétente lorsque les traitements ont lieu en vue de la détection, de la constatation et de la poursuite d'infractions qui relèvent de sa compétence. À cet égard, la Commission rappelle son avis n° 13/2015 du 13 mai 2015 dans lequel on fait remarquer que, vu les différentes missions qui ont été attribuées à l'AGDA, seul le service d'enquête et de recherche de l'AGDA peut être considéré comme un acteur de la chaîne pénale et de sécurité[66] [67]. Pour lever cette imprécision, la Commission recommande de se référer explicitement, dans l'article 31.7.e du Projet, à l'article 44/11/9, § 1, 4° de la loi sur la fonction de police, à savoir le service d'enquête et de recherche et l'administration surveillance, contrôle et constatation de l'Administration générale des douanes et accises.

200. Bien que la Commission comprenne que la délimitation du champ d'application ne soit pas une sinécure, il n'empêche que les critères doivent être indiqués au moins dans l'Exposé des motifs. Si par exemple l'IG et l'AGDA sont comprises de manière large en ce sens qu'elles doivent être désignées en tant qu' "autorité compétente", on ne comprend pas pourquoi ce ne serait par exemple pas non plus le cas pour les services d'inspection de l'Économie et de l'Environnement et, *a fortiori*, le Service d'information et de recherche sociale (SIRS). Ces services traitent également des données à caractère personnel avec une finalité judiciaire. Mais si le demandeur soumettait tous les services d'inspection à l'application de la Directive Police et Justice, cela impliquerait que le champ d'application soit interprété de manière plus large que ce qui est visé.

---

[63] Art. 16, deuxième et troisième alinéas de la loi organique du 18 juillet 1991 *du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace*.

[64] Loi du 15 mai 2007 *sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police*.

[65] Loi du 25 décembre 2016 *relative au traitement des données des passagers*.

[66] Voir les points 61 - 65.

[67] Exposé des motifs, pages 62-63.

201. En guise de suggestion, la Commission propose la solution suivante. On peut déduire de la lecture conjointe du préambule et des dispositions de la Directive Police et Justice que la Décision-cadre 2008/977/JAI du 27 novembre 2008 est prise comme point de départ[68]. En vue de l'harmonisation du traitement de données avec les finalités policières et judiciaires, le cadre de la Décision-cadre de 2008 est élargi aux activités de traitement internes des autorités compétentes déjà comprises dans la Décision-cadre de 2008, à savoir la police régulière, le parquet et les douanes.

202. En ce qui concerne les instances et organes qui ne sont pas compris dans le présent titre 2, les activités de traitement (avec une finalité judiciaire) relèvent des exceptions de l'article 23.1., d) et h) du RGPD, où il est tenu compte dans leur législation sectorielle des conditions et garanties de l'article 23.2. du RGPD. On suit ainsi mieux les finalités tant du RGPD que de la Directive Police et Justice.

Définitions

203. L'article 31 du Projet reprend toutes les définitions de la Directive Police et Justice. L'article 31.3 définit la "limitation du traitement". On entend par là "*le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur*". L'Exposé des motifs mentionne à cet égard que cette "*limitation de traitement (…) vise par exemple l'ajout de métadonnées*"[69]. La Commission estime qu'il s'agit ici d'une interprétation erronée du terme "marquage". Comme il ressort de la définition proprement dite, le but est de limiter le traitement de données à caractère personnel. Le responsable du traitement doit ainsi en quelque sorte "geler" les données (et elles ne peuvent donc pas être effacées) :

- lorsque les personnes concernées contestent l'exactitude des données à caractère personnel et qu'on ne peut le vérifier ; ou
- lorsque les données à caractère personnel doivent être conservées (plus longtemps) en vue d'une utilisation à des fins probatoires (article 16.3. de la Directive Police et Justice).

204. Il en résulte que lorsque l'on invoque une limitation de traitement, aucune donnée à caractère personnel, comme des métadonnées, ne peut être "ajoutée" aux données à caractère personnel

[68] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 *relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale*.

[69] Exposé des motifs, page 59.

en question. La Commission invite dès lors le demandeur à supprimer cet exemple dans l'Exposé des motifs afin de ne pas semer la confusion.

Renvois à l' "autorité de contrôle"

205. L'article 31.15. du Projet reprend la définition d' "autorité de contrôle" de la Directive Police et Justice. La Commission se demande pourquoi on ne désigne pas déjà ici l'autorité de contrôle. Cela serait bénéfique pour la notion ainsi que pour la lisibilité des autres dispositions de ce titre. L'autorité de contrôle, à savoir l'Organe de Contrôle de l'Information policière, n'est cependant révélée qu'à la fin du Titre 2, à l'article 73 du Projet. Étant donné que cette autorité de contrôle est l'interlocuteur dans le cadre d'une demande d'accès indirect (voir *infra*), il est important pour la personne concernée que lors de l'analyse de ses droits, elle sache déjà qui est précisément l'interlocuteur. La Commission estime donc que l'Organe de Contrôle de l'Information policière doit être désigné expressément à l'article 31.15. du Projet.

Licéité du traitement

206. L'article 38 du Projet vise la transposition de l'article 8 de la Directive Police et Justice, qui exécute l'exigence de légalité et qui peut donc être considéré comme la disposition centrale du Projet. Le deuxième paragraphe de l'article 38 mentionne que "*L'obligation légale précise au moins les catégories de données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement* ". Dans l'intérêt d'un usage logique de la terminologie juridique, la Commission appelle le demandeur à remplacer le terme "précise" par le terme "régit", ce qui correspond mieux à l'exigence de légalité. Le fait que la législation doive en outre être "claire" est déjà en soi un aspect des exigences de qualité auxquelles la base légale du traitement de données à caractère personnel doit répondre.

Droits de la personne concernée

207. L'article 46 du Projet constitue l'exception aux droits de la personne concernée. Cette disposition transpose l'article 17 de la Directive Police et Justice dans le Projet, permettant des limitations au droit à l'information, au droit d'accès, au droit de rectification, au droit d'effacement et au droit de limitation du traitement. En ce sens, l'article 46 du Projet est une poursuite de l'article 13 de la LVP, ce qu'on appelle l'accès indirect par lequel la personne concernée peut s'adresser à l'autorité de contrôle afin qu'elle puisse effectuer un contrôle, en lieu et place de la personne concernée, dans les banques de données policières.

208. Il découle de l'article 46 qu'un système d'accès indirect n'est pas imposé par le Projet, mais doit être réglé par une législation sectorielle étant entendu que les demandes d'accès indirect doivent être introduites auprès de l'autorité de contrôle.

209. En ce qui concerne l'Unité d'information des passagers, un règlement d'accès direct et indirect est établi à l'article 15, § 3 de la loi du 25 décembre 2016 *relative au traitement des données des passagers*. En ce qui concerne les données des passagers fournies, la personne concernée a un accès direct à ses données à caractère personnel. À cet effet, la demande est introduite auprès du délégué à la protection des données de l'Unité d'information des passagers. Il s'agit donc ici du droit d'accès tel qu'établi dans le RGPD. Pour l'accès aux données à caractère personnel pour lesquelles l'Unité d'information des passagers a réalisé les contrôles requis, on applique le système d'accès indirect où la demande est adressée à la Commission/l'Autorité de protection des données. C'est ainsi que se manifeste à nouveau la complexité du traitement de données. Le champ d'application tant du RGPD que de la Directive Police et Justice apparaît (cf. *supra*).

210. En ce qui concerne les autres autorités compétentes, la Commission attire l'attention sur le fait que la LVP est abrogée par le Projet et dès lors aussi l'article 3, § 5 de la LVP qui prévoit pour la police, le Service d'enquête du Comité P et l'Inspection générale de la police une exception aux droits de la personne concernée. Étant donné qu'il est peu probable que la législation sectorielle de ces autorités compétentes soit adaptée lorsque le Projet sera effectivement d'application, il y aura des conséquences au niveau du système d'accès indirect.

211. La Commission ne comprend d'ailleurs pas pourquoi aux paragraphes 4 et 5 de l'article 46 du Projet, on mentionne de nouveau que les droits de la personne concernée sont exercés par l'autorité de contrôle, alors que cette condition est déjà fixée au deuxième paragraphe du même article. Cette répétition n'a pas de sens et donne l'impression erronée qu'il s'agit d'une dérogation "particulière" (ou que ce pourrait être le cas) à l'exception "générale" aux droits de la personne concernée, comme établie à l'article 46 du Projet. La Commission estime que la référence à l'autorité de contrôle dans ces paragraphes est superflue et doit donc être supprimée.

212. Lorsque la personne concernée introduit auprès de l'autorité de contrôle une demande d'accès indirect pour ses données à caractère personnel qui sont traitées par la police, les services des douanes ou la Cellule de Traitement des Informations Financières, il est prévu, par ces mêmes paragraphes 4 et 5 de l'article 46 du Projet, que l'on puisse communiquer à la personne concernée "*certaines informations contextuelles*". C'est le ministre compétent qui, après avis de l'autorité de

contrôle, fixe les directives concernant les "*catégories d'informations contextuelles*" qui peuvent être communiquées à la personne concernée.

213. La Commission est favorable à une transparence par couches selon le contexte dans lequel l'accès indirect est demandé. Le nombre de banques de données policières augmente fortement et celles-ci sont consultées ou interrogées pour de nombreuses finalités non policières. Dans des situations spécifiques, les antécédents policiers de citoyens sont même transmis (sous forme abstraite) à des acteurs privés alors que ces acteurs ne font en soi pas partie de la chaîne pénale et de sécurité. Les personnes concernées ne savent par contre généralement pas si (et encore moins pourquoi) leurs données à caractère personnel sont traitées dans une banque de données policière. La réalité sociale nous apprend que la personne dont les données sont enregistrées dans des banques de données policières risque réellement des conséquences négatives pour sa vie tant professionnelle que privée. Une transparence par couches est donc indispensable et contribuera à renforcer l'accès au juge, ce qui est un des points de départ poursuivi par le nouveau cadre européen en matière de protection des données à caractère personnel[70].

214. À cet égard, la Commission indique que la communication d'informations contextuelles à la personne concernée implique que cette dernière devra aussi de son côté communiquer les éléments et circonstances pertinents de la requête afin de pouvoir déterminer si, et si oui quelles informations peuvent être communiquées à la personne concernée. La Commission recommande d'y faire référence dans l'Exposé des motifs, en recommandant que la législation sectorielle soit adaptée en ce sens.

215. L'article 47 du Projet dispose que lorsque les données à caractère personnel de la personne concernée font l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale, les droits de la personne concernée sont exercés conformément au Code judiciaire et au Code d'instruction criminelle. Cette possibilité est prévue dans la Directive Police et Justice. La Commission n'a pas de remarque particulière à cet égard.

<u>Données à caractère personnel reçues d'autres autorités du Titre 3</u>

216. Les articles 48 et 49 du Projet prévoient une limitation des droits de la personne concernée lorsque les autorités compétentes reçoivent des informations des services de renseignement et de sécurité ou de l'Organe de coordination pour l'analyse de la menace (OCAM).

---

[70] R. SAELENS, '*Profiling* for Tomorrowland : de screening van festivalgangers door de politie', *TPP* 2018, vol. 1, 20 – 27.

217. La Commission ne comprend toutefois pas pourquoi cette disposition est reprise au Titre 2, dès lors que le Titre 3 prévoit également des exceptions aux droits de la personne concernée pour les activités de traitement par les services de renseignement et de sécurité et l'OCAM. Lorsque les autorités compétentes du Titre 2 reçoivent des données à caractère personnel en vue de l'exercice des missions des services de renseignement et de sécurité et de l'OCAM, les limitations des droits de la personne concernée en vertu du Titre 3 s'appliquent également au transfert de données à caractère personnel aux autorités compétentes du Titre 2. Il n'en sera autrement que lorsque ces autorités utiliseront les données à caractère personnel pour leurs propres finalités qui seront donc différentes. Mais dans ce cas, les exceptions aux droits de la personne concernée en vertu du Titre 2, à savoir via l'application de l'article 46 du Projet, devraient s'appliquer.

218. Par ailleurs, comme remarqué dans le Titre 1, la Commission souligne que la définition de destinataire ne s'applique pas aux autorités qui reçoivent les données à caractère personnel dans le cadre de leur enquête particulière, conformément au droit national. Cela signifie que, bien que la possibilité d'échange de données entre les autorités du Titre 2 et du Titre 3 doive être établie dans la législation sectorielle, la personne concernée ne doit pas être informée spécifiquement lorsqu'une autorité visée au Titre 3 transmet ses données à caractère personnel à une autorité compétente du Titre 2.

219. Ce qui précède n'est toutefois pas valable pour les particuliers, qui sont donc bien considérés comme des "destinataires" lorsqu'ils reçoivent des informations d'autorités du Titre 2 ou du Titre 3. À cet égard, la Commission observe que le transfert de données à caractère personnel par les services de police au secteur privé dans le cadre des missions de police administrative et judiciaire n'a pas été réglé dans la loi sur la fonction de police. Étant donné que dans le cadre de la sécurité intégrale, le secteur privé est également considéré comme un acteur important dans la chaîne de sécurité, cela donne lieu en pratique à des situations où la position juridique tant de la police que de la personne concernée est imprécise. Par analogie au système d'accès indirect abordé ci-avant, on pourrait penser à la mesure dans laquelle (lors de l'application de l'accès indirect) des informations contextuelles peuvent être envoyées par l'autorité compétente à la personne concernée faisant l'objet d'une décision négative ou d'une décision l'affectant de manière significative afin qu'elle puisse, si elle le souhaite, soumettre la décision au juge, sans accorder *de facto* un accès aux banques de données policières.

220. À l'article 50 du Projet, on mentionne le "système de contrôle", sans le définir. Bien que l'on puisse déduire de l'Exposé des motifs que le système concerne le contrôle de l'utilisation des

banques de données et de l'accès à ces dernières, la Commission estime que le système de contrôle doit être défini à l'article 31 du Projet.

221. La Commission ne comprend pas quelle est la raison de l'article 51 du Projet. Cette disposition semble être un reflet de l'article 18 du Titre 1, mais l'Exposé des motifs ne contient aucune explication à cet égard. Il s'agit de la situation dans laquelle la personne concernée fait l'objet d'un "traitement commun", à savoir celle où différents acteurs traitent les mêmes données à caractère personnel, chacun dans le cadre de ses compétences et finalités, ce à quoi les limitations des droits de la personne concernée évoquées ci-avant s'appliquent. La Commission voit à cet égard des similitudes avec les traitements qui ont lieu dans le cadre de la banque de données commune (*Foreign) Terrorist Fighters* créée en vertu de l'article 44/11/3*bis* de la loi sur la fonction de police.

222. La Commission estime que les termes "traitement commun" doivent être repris dans les définitions de l'article 31 du Projet. S'il s'agit également de banques de données communes comme visé à l'article 44/11/3*bis* de la loi sur la fonction de police, elles doivent être désignées dans le Projet. À cet égard, la Commission renvoie aux remarques formulées au sujet de l'article 18 du Titre 1 du Projet.

223. En ce qui concerne le § 6 de l'article 51 du Projet, la Commission ne comprend pas non plus la référence au "*recours*" dont est saisie l'autorité de contrôle. On ne peut en effet saisir l'autorité de contrôle d'un "recours".

Les obligations du responsable du traitement

224. L'article 52 du Projet concerne l'obligation de prendre des mesures techniques et organisationnelles appropriées. L'utilisation du terme "peuvent" suppose une liberté dans le chef du responsable du traitement qui n'est pas accordée par la Directive Police et Justice. Dans le considérant 53 de la Directive Police et Justice, qui est manifestement consacré à l'article 52 du Projet, on précise que le responsable du traitement "[doit] *adopter des règles internes*". Il s'agit donc d'une *obligation* et non d'une liberté de choix dans le chef du responsable du traitement.

Le délégué à la protection des données

225. L'article 60 du Projet concerne l'analyse d'impact relative à la protection des données. La Commission fait remarquer que dans l'Exposé des motifs, on suppose à tort que cette obligation

peut aussi reposer sur le délégué à la protection des données[71]. Cette obligation n'incombe toutefois qu'au responsable du traitement, qui peut bien entendu être assisté par le délégué à la protection des données. La Commission invite le demandeur à adapter l'Exposé des motifs en ce sens.

CONCLUSION de la Commission sur le titre 2 du Projet

226. La Commission insiste sur une délimitation claire du champ d'application de la Directive Police et Justice dans le Projet. Le choix de soumettre ou non certains organismes publics ou services publics à l'application du Titre 2 n'est pas basé sur des critères énoncés, de sorte qu'on ne peut pas le confronter au champ d'application restrictif qui est avancé par le demandeur.

Par ailleurs, un système de limitation des droits de la personne concernée est développé mais il est difficile pour la personne concernée de déterminer à l'égard de quels traitements l'accès indirect est d'application, à savoir seulement les activités de traitement du Titre 2 ou également les données à caractère personnel reçues des autorités du Titre 3, ou pour autant qu'il s'agisse de celles-ci. On introduit en outre certains concepts qui, de l'avis de la Commission, doivent être définis.

La Commission émet dès lors un avis **défavorable** en ce qui concerne la délimitation du champ d'application. Pour le reste, elle émet un avis **favorable**, moyennant la prise en compte des remarques suivantes :

- citer explicitement l'autorité de contrôle dans les définitions ;
- à l'article 38 du Projet, remplacer le terme "précise" par le terme "régit" ;
- lever la confusion créée par les paragraphes 4 et 5 de l'article 46 du Projet ;
- vérifier si la reprise des articles 48 et 49 du Projet, qui prévoient une limitation des droits de la personne concernée lorsque des autorités compétentes reçoivent des informations d'autorités du Titre 3, a bien du sens ;
- définir les termes "système de contrôle" et "traitement commun" ;
- à l'article 52 du Projet, remplacer le verbe "peuvent" par "doivent" ;
- supprimer l'obligation pour le délégué à la protection des données de réaliser une analyse d'impact relative à la protection des données.

[71] Exposé des motifs, page 103.

6. TITRE 3 : DE LA PROTECTION DES PERSONNES PHYSIQUES A L'ÉGARD DU TRAITEMENT DES DONNÉES A CARACTÈRE PERSONNEL PAR D'AUTRES AUTORITÉS QUE CELLES VISÉES AUX TITRES 1 ET 2

6.1. Sous-titres 1, 2, 3 et 4

227. Le Titre 3 porte sur le traitement de données à caractère personnel par les services de renseignement et de sécurité, les forces armées, l'OCAM et l'Unité d'information des passagers, spécifiquement en ce qui concerne les activités de traitement relevant de la sécurité nationale. Comme déjà exposé ci-avant, ni le RGPD ni la Directive Police et Justice ne sont en principe d'application au traitement de données à caractère personnel par ces services publics et la Défense. Le traitement de données à caractère personnel par ces services avait néanmoins été régi par la LVP. Par ailleurs, il convient de tenir compte de la Convention n° 108 du 28 janvier 1981 *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (Convention n° 108).

228. Par le Titre 3 du Projet, le demandeur confirme l'application des principes généraux pour le traitement de données à caractère personnel par ces entités. À cet effet, on reflète *mutatis mutandis* la Directive Police et Justice. À cet égard, les définitions de l'article 31 du Projet sont reprises, à l'exception des "autorités compétentes", du "responsable du traitement", du "destinataire" et de l' "autorité de contrôle". Sauf pour le "destinataire", ceux-ci sont à nouveau définis à l'article 74 du Projet.

Catégories particulières de données à caractère personnel

229. L'article 77 du Projet reprend les principes de base, à savoir les exigences de licéité, le principe de finalité, de nécessité, de proportionnalité et de précision. D'après l'article 78 du Projet, les services de renseignement et de sécurité traitent des données à caractère personnel de toute nature, en ce compris les catégories particulières de données à caractère personnel, dont les données génétiques et biométriques et les données pénales.

230. La Commission comprend que les services de renseignement et de sécurité doivent avoir la possibilité de traiter chaque type de donnée à caractère personnel afin de pouvoir anticiper toute menace à la sécurité nationale[72]. La Commission rappelle toutefois que les catégories particulières de données à caractère personnel ne peuvent être traitées que lorsque la nature spécifique de la

[72] Exposé des motifs, page 143.

donnée à caractère personnel est en lien avec l'intérêt à protéger énoncé dans la loi relative aux services de renseignement et de sécurité.

231. La Commission constate que les services de renseignement et de sécurité sont autorisés directement par l'article 78 du Projet à traiter des catégories particulières de données à caractère personnel, sans devoir développer ni justifier dans la législation sectorielle la nécessité et la proportionnalité. Le demandeur justifie cette autorisation de traiter des catégories particulières de données à caractère personnel en se référant à l'article 3, § 4 de la LVP et à l'article 9, § 2 de la Convention n° 108[73]. La Commission renvoie à cet égard aux objections relatives aux articles 10 et 11 du Titre 1. Se pose ainsi la question de la nécessité et de la proportionnalité du traitement, par exemple, de données à caractère personnel génétiques.

Droit d'accès

232. À la lumière des missions des services de renseignement et de sécurité, les articles 80 e.s. du Projet prévoient des limitations aux droits de la personne concernée. À cet égard, on renvoie aux dispositions correspondantes de la loi du 30 novembre 1998 *organique des services de renseignement et de sécurité*. La Commission fait remarquer que l'article 82 du Projet sème la confusion en suggérant que l'article 2, § 3 de la loi du 30 novembre 1998 concerne le droit d'accès. Dans ce dernier article, il s'agit toutefois d'une obligation de notification, sous conditions, à la personne concernée lorsqu'elle a fait l'objet de certaines méthodes de recherche. Il s'agit donc d'une obligation d'information *a posteriori* indépendante du "droit d'accès". À cet égard, l'article 82 ne présente aucune plus-value, sauf si cette disposition a un impact sur l'article 83 du Projet. Dès lors que l'article 83 du Projet prévoit un système d'accès indirect, la lecture conjointe des articles 82 et 83 pourrait en effet donner l'impression que même l'accès indirect peut être limité. Mais aucune justification n'est donnée à ce sujet. La Commission recommande de supprimer l'article 82 du Projet ou d'indiquer et de justifier l'éventuel impact sur l'accès indirect.

Point de contact pour les responsables conjoints du traitement

233. La situation dans laquelle il y a des responsables conjoints du traitement peut se présenter. Contrairement à ce qui est exigé au Titre 2 du Projet, les responsables conjoints du traitement sont, d'après l'article 89 du Projet, libres de désigner ou non un seul point de contact pour la personne concernée dans l'accord. La Commission estime par contre qu'un point de contact *doit*

[73] Exposé des motifs, page 136.

être désigné. Ceci est important non seulement pour la personne concernée afin qu'elle puisse faire valoir ses droits mais aussi pour les contacts avec l'autorité de contrôle.

Brèche de sécurité

234. En ce qui concerne la notification d'une brèche de sécurité des données à caractère personnel, l'article 90 du Projet ne prévoit pas de délai. La Commission appelle le demandeur à définir le même délai que celui imposé au Titre 2 du Projet, à savoir 72 heures.

Registre

235. Les responsables du traitement relevant du Titre 3 doivent également tenir un registre. La Commission trouve qu'il est singulier que selon l'article 92 du Projet, les services de renseignement et de sécurité ne doivent pas reprendre dans le registre les catégories de personnes ni la catégorie de données à caractère personnel. D'après l'Exposé des motifs, la raison réside dans le fait qu'il n'y a en fait que des "cibles".

236. La Commission comprend que le motif d'enregistrement de données à caractère personnel par les services de renseignement et de sécurité soit lié à une activité qui constitue une menace telle qu'établie dans la loi du 30 novembre 1998 *organique des services de renseignement et de sécurité*. Mais cette activité est indéniablement en lien avec une personne dont les actes (l'activité) constituent une menace pour la sécurité nationale. La Commission estime dès lors que lorsque les services de renseignement et de sécurité vérifient les faits et gestes de personnes (physiques) ou de groupements, des données d'identification ainsi que d'autres catégories de données à caractère personnel sont traitées à cet égard, comme l'extrême droite, l'extrême gauche, la radicalisation, les salafistes, etc. La Commission ne comprend dès lors pas pourquoi le registre ne devrait pas mentionner les catégories de personnes ni les catégories de données à caractère personnel.

237. Enfin, il ressort du même article 92 du Projet que les services de renseignement et de sécurité ne doivent mentionner dans le registre les coordonnées du responsable du traitement ou de gestionnaires d'autres banques de données (étrangères) auxquelles ils ont accès que s'ils connaissent les coordonnées du responsable du traitement ou du gestionnaire[74]. La Commission estime très étrange que les services de renseignement et de sécurité aient également accès à des banques de données dont ils ne connaissent pas les coordonnées (du gestionnaire). (La licéité de)

[74] Exposé des motifs, page 143.

l'accès à des données à caractère personnel dépendra en effet de la mesure dans laquelle on aura préalablement vérifié avec le service public (étranger) compétent comment l'accès à ces banques de données peut être convenu dans le cadre des missions légales des services de renseignement et de sécurité. On ne comprend donc pas pourquoi les coordonnées (au moins) du gestionnaire de la banque de données ne pourraient pas être reprises dans le registre.

Traitement de catégories particulières de données à caractère personnel dans le cadre d'habilitations, attestations et avis de sécurité

238. En ce qui concerne les traitements dans le cadre de l'application de la loi du 11 décembre 1998 *relative à la classification et aux habilitations, attestations et avis de sécurité*, la Commission répète la nécessité de nommer expressément l'autorité de contrôle dès la définition de l' "autorité de contrôle" (cf. *supra*).

239. La Commission constate qu'une série d'autorités sont (peuvent être) impliquées dans le traitement de données à caractère personnel dans le cadre d'habilitations, attestations et avis de sécurité (art. 109 du Projet). Ce qui est problématique, c'est le fait que les autorités visées à l'article 109 du Projet sont autorisées directement par l'article 112 du Projet à traiter des catégories particulières de données à caractère personnel, sans vérifier dans quelle mesure cela est nécessaire ou proportionnel étant donné que, peu importe qu'il s'agisse d'habilitations, attestations ou avis de sécurité, manifestement *toutes* les autorités concernées (potentiellement) peuvent traiter *certaines ou toutes les* catégories particulières de données à caractère personnel. La Commission renvoie aux remarques formulées ci-avant concernant l'article 78 du Projet qui est similaire. Tout comme pour l'article 78 du Projet, la rédaction de l'article 112 du Projet implique que l'on ne doit plus examiner la nécessité et la proportionnalité dans la législation sectorielle.

Autres remarques

240. L'article 187, § 4 du Projet dispose que l'Autorité de protection des données (APD) n'est pas compétente pour exercer un contrôle du traitement de données à caractère personnel par la commission administrative dans le cadre de ses missions. Cette commission administrative est chargée de la surveillance des méthodes spécifiques et exceptionnelles des services de renseignement et de sécurité. Par ailleurs, l'APD n'est pas non plus compétente pour les traitements dans le cadre de leurs missions par le Comité R, le Comité P et le C.O.C. Selon l'Exposé des motifs, cet article n'appelle aucun commentaire. Par souci d'exhaustivité, la Commission fait quand même remarquer que ces organes traitent également des données à caractère personnel relevant de l'application du RGPD et sont ainsi soumis à la surveillance de l'APD, sauf si la

surveillance de ces activités de traitement a aussi été expressément confiée à ces organes de contrôle comme c'est le cas pour tous les traitements de la police qui relèveraient de la surveillance du C.O.C. On y reviendra encore dans le présent avis lors de l'analyse du paysage des autorités de contrôle.

241. À cet égard, la Commission se demande d'ailleurs quelle est la place précise de la commission administrative, dès lors que cet organe traite également des données à caractère personnel dans le cadre du contrôle de l'utilisation de certaines méthodes de recherche par les services de renseignement et de sécurité. Relève-t-elle du contrôle du Comité R en tant qu'autorité de contrôle, bénéficie-t-elle de l'exception telle que prévue pour les juridictions dans le cadre d'affaires judiciaires ou prévoit-on un contrôle *sui generis* ?

CONCLUSION de la Commission sur les sous-titres 1 à 4 inclus du Titre 3 du Projet

242. En résumé, la Commission prend acte de la confirmation du fait que pour les activités de traitement ne relevant pas du droit de l'Union, ces acteurs sont aussi soumis aux principes du droit de protection des données à caractère personnel. La Commission a néanmoins relevé quelques points problématiques dont on doit tenir compte dans le Projet.

En ce qui concerne le traitement de catégories particulières de données à caractère personnel, comme régi aux articles 78 et 112 du Projet, la Commission émet un avis **défavorable**, vu les remarques fondamentales à cet égard. Pour le reste, la Commission émet un avis **favorable**, moyennant la prise en compte des remarques suivantes :

- indiquer expressément l'autorité de contrôle ;
- reprendre les catégories de personnes et les catégories de données à caractère personnel dans le registre ;
- reprendre les coordonnées des banques de données dans le registre ;
- fixer un délai pour la notification de brèches de sécurité de données à caractère personnel ;
- examiner la nécessité de l'article 82 et justifier l'éventuel impact sur l'article 83 du Projet ;
- en cas de responsables conjoints du traitement, imposer l'obligation de reprendre un point de contact dans le registre.

6.2. Sous-titre 5. De la protection des personnes physiques à l'égard de certains traitements de données à caractère personnel par l'unité d'information des passagers

243. Un régime particulier de protection est prévu pour les traitements de données des passagers (PNR[75]) par l'Unité d'information des passagers (UIP) effectués dans le cadre des finalités visés à l'article 8, § 1er, 4° de la loi du 25 décembre 2016 *relative au traitement des données des passagers*[76] (ci-après la « loi PNR »), à savoir dans le cadre du suivi par les services de renseignement des activités pouvant menacer les intérêts fondamentaux de l'État. Suivant l'Exposé des motifs, « *Les traitements dans le cadre de la finalité visée à l'article 8, §1er, 4° de la loi précitée du 25 décembre 2016 sont classés sous le Titre 3 puisqu'il s'agit de traitements de données à caractère personnel (données des passagers) dans le cadre des missions des services de renseignement et de sécurité visés aux articles 7 et 11 de la loi du 30 novembre 1998 [organique des services de renseignement et de sécurité]* ». La Commission note en effet que les activités de renseignement ne relèvent pas du champ d'application du droit de l'Union et ne sont dès lors pas soumises au RGPD ou à la Directive Police & Justice. L'article 271, alinéa 2 du Projet précise que les autres titres du Projet ne sont pas applicables aux traitements concernés hormis certaines dispositions relatives aux sanctions pénales[77].

244. Les traitements concrets concernés sont en l'occurrence :

- la corrélation des données des passagers communiquées par les transporteurs ou les opérateurs de voyage avec les banques de données des services de renseignement ou avec les critères destinés à cibler des individus, lors des évaluations préalables des passagers dans le cadre du suivi par les services de renseignement des activités pouvant menacer les intérêts fondamentaux de l'État ;
- des recherches ponctuelles à des fins de renseignement dans la banque de données des passagers.

245. Le sous-titre 5 du Titre 3 du Projet détermine :

- les conditions générales des traitements : principes de légitimité et finalité des traitements, de proportionnalité et de qualité des données ;
- la conservation des données ;
- les droits de la personne concernée ;

---

[75] Passenger Name Record.

[76] http://www.ejustice.just.fgov.be/eli/loi/2016/12/25/2017010166/justel.

[77] A savoir les articles 239 et 240 du Projet.

- les obligations du responsable du traitement, en termes de sécurité des traitements et en ce qui concerne la tenue d'un registre des banques de données de l'UIP et de celles mises à sa disposition ;
- les conditions du transfert international des données PNR.

246. L'Exposé des motifs précise à cet égard que « *La loi du 25 décembre 2016 précitée contient plusieurs dispositions concernant la protection des données telles que la désignation d'un délégué à la protection des données, la prévision d'une validation manuelle ou encore l'interdiction de traiter des données sensibles. Certains points déjà repris dans la loi du 25 décembre 2016 ne doivent par conséquent plus être repris dans la présente loi* ». La Commission note également que le droit d'information de la personne concernée est prévu à l'article 6 de la loi PNR qui dispose que « *Les transporteurs et les opérateurs de voyage informent les personnes concernées que leurs données sont transmises à l'UIP et peuvent être traitées ultérieurement pour les finalités visées à l'article 8* ». Il en va de même des droits d'accès et de rectification.

247. A ce dernier égard, la Commission rappelle tout d'abord que les droits d'accès et de rectification des personnes concernées aux données PNR qui les concernent se déroulent au travers d'une procédure d'accès direct de principe (article 15 de la loi PNR). Une procédure dérogatoire d'accès indirect est uniquement prévue en ce qui concerne les correspondances positives[78] et les résultats des recherches ponctuelles. La Commission n'est pas certaine que le Projet respecte cette dichotomie et la possibilité d'accès direct de la personne concernée dès lors qu'il stipule que la personne a le droit de demander la rectification ou la suppression de ses données inexactes auprès de l'autorité de contrôle compétente (articles 175 et 177 du Projet). Elle invite dès lors le demandeur à préciser qu'il est question dans le Projet de la seule procédure d'accès indirect de l'article 15, § 3, alinéa 2 de la loi PNR et de rajouter la procédure d'accès direct existante[79] à l'énumération figurant dans l'Exposé des motifs des dispositions de la loi PNR concernant la protection des données qui ne doivent pas être reprises dans le Projet.

248. La Commission s'étonne ensuite du caractère générique et décontextualisé de certaines dispositions alors qu'il est question de traitements très spécifiques et circonscrits par la loi PNR et qu'il est renvoyé par ailleurs à la loi PNR pour les points non repris dans le Projet.

249. Ainsi dans le cadre du droit d'accès indirect de la personne concernée, l'article 176 du Projet dispose qu'« *Afin de garantir la confidentialité et l'efficacité de l'exécution des traitements visés*

[78] Issues de la corrélation avec les banques de données des services compétents ou avec les critères destinés à cibler des individus.

[79] Visée à l'article 15, § 3, alinéa 1er de la loi PNR.

ci-dessus[80]*, l'accès par la personne concernée à ses données à caractère personnel est limité à celui prévu expressément par une loi* ». La Commission se demande pourquoi il n'est pas tout simplement renvoyé à la loi PNR. Elle invite par ailleurs le demandeur à faire référence de manière plus appropriée aux « traitements visés au présent sous-titre » en lieu et place des « traitements visés ci-dessus ».

250. Il en va de même de l'article 177 du Projet. Cet article commence par énumérer certaines modalités de l'accès indirect et de la vérification de la conformité des traitements opérée par le Comité R en ces termes « *La personne concernée justifiant de son identité s'adresse, sans frais, à l'autorité de contrôle compétente. Celle-ci effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires* », avant de conclure que « *les modalités d'exercice de ce recours sont déterminées par la loi* ». La Commission invite le demandeur - par souci de simplicité et de transparence vis-à-vis des personnes concernées - à préciser directement que l'autorité de contrôle compétente est le Comité R (ou opérer un renvoi à l'article 97 du Projet) et à spécifier la loi concernée, à savoir soit la loi organique des services de renseignement soit la loi PNR soit encore le présent Projet. La commission fait par ailleurs remarquer que l'article 177 du Projet fait erronément référence aux points 2° et 3° de son article 175, alors que cet article ne comprend que deux points.

251. Pareillement l'article 178 qui postule l'interdiction des décisions purement automatisées précise que l'interdiction « *ne s'applique pas lorsque la décision est fondée sur une disposition prévue par ou en vertu d'une loi ou lorsqu'elle est nécessaire pour la sauvegarde d'un intérêt public important* ». Même si la Commission note que le cadre actuel - en conformité avec la directive PNR – ne permet pas les décisions purement automatisées dès lors qu'il postule une validation par l'UIP des correspondances positives issues des corrélations opérées, elle souhaiterait que la référence soit faite à la loi PNR en ce qui concerne la première exception et que le demandeur motive à tout le moins la seconde exception dans l'Exposé des motifs.

252. Le Chapitre VI relatif aux obligations du responsable du traitement contient également des dispositions très générales sur les obligations du responsable du traitement sans spécificité par rapport aux traitements des données des passagers hormis pour le registre qui distingue entre « les banques de données de l'UIP » et les « banques de données mises à la disposition de l'UIP ». Il est ainsi fait référence dans les différentes dispositions au « responsable du traitement » alors que le responsable du traitement des données des passagers est désigné par la loi PNR comme étant le fonctionnaire dirigeant de l'UIP. Le Commission se demande – à nouveau par souci de simplicité et de transparence vis-à-vis des personnes concernées – pourquoi ce responsable

[80] Il serait plus approprié de mentionner « les traitements visés au présent sous-titre ».

désigné n'est pas cité tel quel. Par ailleurs, la Commission ne comprend pas pourquoi il est question des banques de données de l'UIP alors que la loi PNR parle à juste titre de l'unique banque de données des passagers.

253. Enfin s'agissant des transferts internationaux des données PNR, la Commission fait remarquer qu'il serait utile de préciser que les règles des articles 184 et 185 viennent compléter les règles strictes de la loi PNR, dès lors que celle-ci fait notamment référence aux articles 21 et 22 de la LVP, en passe d'être abrogés.

CONCLUSIE van de Commissie over de ondertitel 5 van titel 3 van het ontwerp

254. En conclusion, la Commission émet un avis favorable concernant ce sous-titre à la condition qu'il soit tenu compte des remarques suivantes:

- la nécessité de préciser que le Projet concerne l'accès indirect et renvoie à la loi PNR en ce qui concerne l'accès direct reconnu par cette loi;
- le caractère générique et décontextualisé de certaines dispositions ;
- la nécessité de préciser que les règles relatives aux transferts internationaux des données PNR viennent compléter les règles strictes de la loi PNR.

7. TITRE 4 : TRAITEMENT À DES FINS ARCHIVISTIQUES DANS L'INTÉRÊT PUBLIC, À DES FINS DE RECHERCHE SCIENTIFIQUE OU HISTORIQUE OU À DES FINS STATISTIQUES

Remarques générales

255. Le RGPD reconnaît l'intérêt sociétal de la science, tout comme la Directive 95/46/CE le faisait déjà explicitement. Concernant les traitements, le considérant 113 du Règlement dispose qu' "*À des fins de recherche scientifique ou historique ou à des fins statistiques, il y a lieu de prendre en considération les attentes légitimes de la société en matière de progrès des connaissances".* Le RGPD vise un équilibre entre la liberté de la recherche et la protection de la vie privée.

L'exigence de garanties appropriées

256. L'article 89.1 du RGPD souligne très clairement que "*Le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est soumis, conformément au présent règlement, à des garanties appropriées pour les droits et libertés de la personne concernée*"". Les chercheurs, statisticiens et archivistes doivent respecter le Règlement et, tout comme chaque autre responsable du traitement, instaurer les garanties nécessaires. L'article 89.1 du RGPD incite les responsables du traitement à accorder une attention particulière à la pseudonymisation et au traitement ultérieur de données anonymisées - dans la mesure du possible.

Dérogations aux droits des personnes concernées : limites

257. L'article 89.2-3 du RGPD autorise les États membres à instaurer des dérogations à certains droits dans le contexte du traitement de données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Ces dérogations légales sont autorisées "*dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités*" L'ajout "*sous réserve des conditions et des garanties visées au paragraphe 1 du présent article*" rappelle à nouveau l'applicabilité de principe du RGPD.

258. La Commission ne voit dans cet élément de la phrase aucune autorisation pour le législateur d'instaurer un régime dérogatoire général, en l'absence d'une mention explicite à l'article 89.1 du RGPD selon laquelle des dérogations peuvent être prévues dans le droit d'un État membre. Le considérant 156 non plus ne permet pas à la Commission de conclure à l'existence d'une clause d'ouverture large en dépit du texte de l'article 89.1 du RGPD. Les États membres doivent en effet

offrir des garanties appropriées pour le traitement de données à caractère personnel - en vertu du RGPD - dans chaque réglementation qu'ils promulguent.

259. Le titre 4 du Projet instaure un régime spécifique pour des fins archivistiques dans l'intérêt public, des fins de recherche scientifique ou historique ou des fins statistiques qui dépasse les limites des clauses d'ouverture laissées par le RGPD. Ainsi, l'article 190 du Projet déclare que le titre 4 s'applique même si le responsable du traitement décidait de ne pas faire usage des dérogations autorisées en vertu de l'article 89.2-3 du RGPD.

260. Un point fort du RGPD est l'imposition de règles égales pour toutes sortes de secteurs. Dès lors, cela coûte moins cher à la société de mettre en œuvre dans la pratique quotidienne un seul ensemble partagé de règles qu'un éventail de règles différentes qui s'appliquent chacune selon les circonstances, et ce dans une seule organisation pour des activités qui sont étroitement liées (par exemple la gestion d'un budget de mobilité de travailleurs individuels d'une part et la cartographie des besoins de mobilité de la société au moyen de données statistiques d'autre part).

261. Le titre 4 du Projet va tout à fait à l'encontre de cette idée de base. Des activités à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sont entreprises partout à grande ou petite échelle jusqu'à une très petite échelle. L'impact de ce titre ne se limite donc pas aux universités ou à des sociétés déterminées axées sur l'innovation, ce que l'Exposé des motifs reconnaît également[81].

262. Voici quelques exemples d'activités à petite échelle :

- Une société invite un groupe de consommateurs afin de les soumettre à un sondage visant à savoir si un emballage nouvellement mis au point est plus pratique que l'emballage actuel.
- Une association rédige, pour la revue destinée à ses membres, un article sur sa création, à l'occasion d'un anniversaire, et interviewe les membres fondateurs.
- Un cercle d'histoire locale recueille les témoignages d'habitants plus âgés sur une tradition locale.

---

[81] "*Les responsables du traitement à des fins d'archives, de recherches et de statistiques peuvent donc être des départements publics (comme la DG statistique du SPF économie ou les Archives générales du Royaume), des entreprises privées (comme les sociétés pharmaceutiques, des universités, des fondations privées, des ASBL, des centres d'archives privés,) etc.*"

- Pour un travail de fin d'études en sciences humaines, des étudiants organisent une enquête auprès de leurs parents et d'habitants du quartier sur la mobilité afin de se familiariser avec les principes des statistiques.

- Des étudiants en médecine, en soins infirmiers et autres professions des soins de santé qui, dans le cadre de leur formation, rédigent des rapports de stage sur les connaissances acquises.

- Un généalogiste assiste une famille dans l'élaboration de leur arbre généalogique.

La prise en compte des risques

263. Le Projet adopte manifestement pour point de départ l'affirmation selon laquelle ces traitements impliquent par définition un risque élevé. Un point de départ qui est purement et simplement en contradiction flagrante avec la réalité et qui n'est pas étayé dans l'Exposé des motifs. Il est surprenant que le Projet régisse toute forme de recherche de manière plus stricte que les traitements axés sur le marketing direct ou ceux réalisés par des employeurs concernant leurs employés. En d'autres termes, les chercheurs sont soumis à un régime plus strict que ceux qui utilisent par la suite les constatations scientifiques pour adopter des mesures ou prendre des décisions qui affectent une personne physique déterminée.

La désignation obligatoire d'un délégué à la protection des données

264. L'obligation de désigner un délégué à la protection des données - quel que soit le profil de risque du traitement - et de recourir à lui par la suite lors de toutes les étapes du traitement témoigne d'un formalisme extrême. L'auteur du texte en est d'ailleurs bien conscient. Cela ressort de la suggestion dans l'Exposé des motifs que le délégué à la protection des données pourrait donner des avis génériques couvrant plusieurs recherches poursuivant des finalités et utilisant des méthodologies similaires. Cela constitue une indication que cette intervention en est réduite à une simple formalité.

L'absence de prise en compte du contexte international de la recherche

265. Le titre 4 du Projet constitue une entrave pour une société de la connaissance - sans plus-value claire pour la protection des droits et libertés des personnes concernées. Les conséquences seront non seulement ressenties au sein des frontières nationales mais également en dehors. Le texte du Projet s'applique en effet dès qu'un sous-traitant joue un rôle sur le territoire belge dans les activités de traitement (voir l'article 4, § 1er du Projet). La manière dont cela est conciliable avec la libre circulation des données à caractère personnel dans l'Union (article 1.3 du RGPD) n'est vraiment pas claire. L'injonction dans le considérant 159 qu' "*[il faut] tenir compte de l'objectif de l'Union mentionné à l'article 179, paragraphe 1, du traité sur le fonctionnement de l'Union*

européenne (ci-après TFUE)*, consistant à réaliser un espace européen de la recherche*"[82] est restée sans écho dans le Projet. Un grand nombre de chercheurs belges participent à des projets dans le cadre de partenariats européens. La Commission craint que les chercheurs belges soient lésés. Il n'est nulle part question dans le Projet ou dans l'Exposé des motifs de traitements transfrontaliers intereuropéens *à des fins de recherche scientifique ou historique ou à des fins statistiques*.

266. La Commission estime que le législateur doit reconsidérer le champ d'application territorial. Le titre 4 pourrait au moins insérer le principe du pays d'origine[83] pour les dérogations qui s'appliquent aux traitements dans ce contexte, par exemple sous la forme suivante :

> *"Par dérogation à l'article 4, § 1er, ce titre ne s'applique pas aux traitements de données à caractère personnel transfrontaliers au sens de l'article 4, 23) du RGPD et qui sont effectués dans le cadre des activités d'un établissement principal établi en dehors du territoire belge."*

***

267. Comme expliqué ci-après dans la discussion des articles, la Commission estime que le titre 4 est majoritairement contraire au RGPD. En ce qui concerne les autres articles, un grand nombre d'entre eux sont superflus ou du moins pas suffisamment motivés.

7.1. Chapitre I - Dispositions générales

Article 188 Définitions

268. L'article 188 du Projet définit 12 notions à utiliser dans ce titre, suscitant des questions légistiques.

---

[82] Les alinéas 1 et 2 de l'article 179 du TFUE sont libellés comme suit : "*1. L'Union a pour objectif de renforcer ses bases scientifiques et technologiques, par la réalisation d'un espace européen de la recherche dans lequel les chercheurs, les connaissances scientifiques et les technologies circulent librement, et de favoriser le développement de sa compétitivité, y compris celle de son industrie, ainsi que de promouvoir les actions de recherche jugées nécessaires au titre d'autres chapitres des traités.*

2. À ces fins, elle encourage dans l'ensemble de l'Union les entreprises, y compris les petites et moyennes entreprises, les centres de recherche et les universités dans leurs efforts de recherche et de développement technologique de haute qualité; elle soutient leurs efforts de coopération, en visant tout particulièrement à permettre aux chercheurs de coopérer librement au-delà des frontières et aux entreprises d'exploiter pleinement les potentialités du marché intérieur à la faveur, notamment, de l'ouverture des marchés publics nationaux, de la définition de normes communes et de l'élimination des obstacles juridiques et fiscaux à cette coopération."

[83] Comme ce qui est régi aux articles 3 et 4 de la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur*. La loi autrichienne en vigueur sur la protection des données souscrit déjà au principe du pays d'origine au sein de l'Union européenne (voir le deuxième alinéa du § 3 'Räumlicher Anwendungsbereich', *Bundesgesetz über den Schutz personenbezogen Daten*).

269. Ainsi, la notion clé de 'responsable du traitement' se voit attribuer une interprétation propre qui ne s'applique qu'au titre 4, ce qui engendrera inévitablement dans la pratique une énorme confusion et est juridiquement contraire à la définition reprise à l'article 4, 7) du RGPD. Cette définition[84] est superflue, étant donné qu'il ressort déjà de l'article 190 du Projet que les dispositions du titre 4 ne s'appliquent qu' "*au traitement à des fins d'archives ou de recherche ou statistiques*".

270. La notion de 'consentement' se voit aussi attribuer une interprétation propre pour le titre 4, à savoir "*consentement au sens de l'article 4, 11° et du considérant 33 du Règlement*". Cette définition crée aussi une confusion et est superflue. Cette redéfinition est contraire à l'article 4, 11) du RGPD et doit être supprimée. Si on le souhaite, on peut rappeler le considérant 33 du RGPD dans l'Exposé des motifs du titre 4.

271. L'article 188, 3° définit le "*traitement à des fins de recherche*" comme le "*traitement de données à caractère personnel à des fins de recherche scientifique ou historique*". Cette définition économise quelques mots dans le reste du texte légal mais l'asymétrie avec les dispositions du RGPD qui mentionnent systématiquement en entier "*recherche scientifique ou historique*" soumet l'attention du lecteur à rude épreuve. Étant donné que le Projet ne s'adresse pas à un petit groupe d'experts mais à toute personne qui fait de la recherche, il faut particulièrement veiller à assurer la cohérence terminologique avec le RGPD.

272. Si le législateur souhaite raccourcir le texte, il est plus judicieux de rechercher un seul terme qui couvre intégralement la portée "*recherche scientifique ou historique ou à des fins statistiques*". En effet, aucune des dispositions du Projet n'établit de distinction entre "*traitement à des fins de recherche*" (dont font partie la recherche scientifique et la recherche historique) et "*traitement à des fins statistiques*". Dans ce qui suit, les finalités susmentionnées sont désignées, conjointement avec la finalité 'archives dans l'intérêt public' comme 'finalités de connaissances'.

273. L'article 188, 1° définit "*traitement à des fins d'archives*" comme "*traitement de données à caractère personnel à des fins archivistiques dans l'intérêt public*". Cette définition a également pour conséquence que les dispositions suivantes du Projet sèment le trouble chez le lecteur. À l'exception de l'expert en droit de la protection des données, seul le lecteur le plus observateur se rendra compte que le Projet, tout comme l'article 89 du RGPD, prévoit un règlement spécial uniquement pour l'archivage *dans l'intérêt public*. La lisibilité que l'Exposé des motifs prétend poursuivre n'est pas accrue, étant donné que le champ d'application des règles est dissimulé. La cohérence avec le RGPD et la clarté doivent ici aussi être sans aucun doute prioritaires.

---

[84] Art. 188. 5°: "responsable du traitement" : *responsable du traitement à des fins d'archive ou de recherche ou statistiques.*

274. L'article 188, 2° définit ensuite les "*archives d'intérêt public*" comme les "*archives statiques, triées pour leur valeur permanente et conservée (NdT : lisez "conservées") pour une durée illimitée afin d'être rendue publique (NdT : lisez "rendues publiques") dans l'intérêt public général*". Cette définition met en lumière un seul aspect du considérant 158 du RGPD, à savoir les activités d'autorités chargées de la mission consistant à gérer des archives qu'elles ont elles-mêmes triées qui sont à conserver à titre définitif dans l'intérêt public et d'y donner accès. Un deuxième aspect au moins tout aussi important du considérant 158 est toutefois passé sous silence dans cette définition : "*les États membres devraient également être autorisés à prévoir un traitement ultérieur des données à caractère personnel à des fins archivistiques*".
L'Exposé des motifs dispose ce qui suit :

> "*Il existe deux conceptions du mot archive appliquées aux documents : selon la première, les archives sont tous documents administratifs ; selon la seconde les archives sont les documents en fin de vie administrative.*
>
> *L'article 89 du Règlement ne porte que sur les documents en fin de vie. Il n'y a en effet aucun motif de prévoir des exceptions aux droits des personnes concernées pour les documents en cours de vie administrative.*"

275. Le point de vue adopté dans le Projet et dans l'Exposé des motifs nie la réglementation en matière d'archivage qui souligne que la gestion des archives commence dès le moment où les documents sont créés et ce point de vue ne trouve pas un fondement dans le RGPD[85]. En reconnaissant précisément dans le considérant 158 que le traitement ultérieur à des fins archivistiques peut également être invoqué par ces responsables du traitement, on évite qu'après la réalisation des finalités opérationnelles, tout soit détruit, avant que l'autorité compétente en matière d'archivage puisse procéder au tri et à la conservation. En déterminant également déjà dans cette phase plusieurs exceptions aux droits des personnes concernées, strictement afin de préserver les archives dans l'intérêt public, on évite que l'histoire ne soit réécrite sans difficulté,

---

[85] L'arrêté royal du 18 août 2010 définit à l'article 1er, 2., les "Archives" comme "*tous les documents qui, quels que soient leur date, leur forme matérielle, leur stade d'élaboration ou leur support, sont destinés, par leur nature, à être conservés par une autorité publique ou par une personne privée, une société ou une association de droit privé, dans la mesure où ces documents ont été reçus ou produits dans l'exercice de ses activités, de ses fonctions ou pour maintenir ses droits et obligations*. L'article 3, 2° du décret flamand sur les archives du 9 juillet 2010 définit les documents d'archives comme "*tout document, quels que soient sa date, forme, stade de développement ou support, qui de part* [NdT : lisez "par"] *sa nature est destiné à être confié au garant qui l'a reçu, acquis ou établi du chef de ses activités ou tâches ou en vue du maintien de ses droits*, et poursuit à l'article 5, § 2 comme suit : "*Tout garant assure la mise et la conservation en état de bonne qualité, d'ordre et d'accessibilité des documents d'archives à lui confiés durant tout leur cycle de vie à partir de leur création ou réception jusqu'à l'éventuelle destruction*". L'article 1 du décret wallon du 6 décembre 2001 *relatif aux archives publiques* définit les archives comme "*l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits et reçus par tout producteur d'archives visé à l'article 2, dans l'exercice de son activité*".

dans la période précédant le transfert à l'organisme d'archivage. Le RGPD définit d'ailleurs lui-même explicitement une exception au droit à l'effacement de données à caractère personnel afin de préserver les archives dans l'intérêt public (art. 17.3, d) du RGPD).

276. La Commission estime que la définition de l'article 188, 2° du Projet doit être supprimée. Le considérant 158 du RGPD, auquel fait référence l'Exposé des motifs, explique suffisamment ce que vise l'archivage dans l'intérêt public.

277. Si cette définition n'est pas supprimée, elle doit être adaptée afin d'inclure les deux aspects de l'archivage. En outre, l'expression 'toegankelijk te maken' dans le texte néerlandais doit être traduite par 'donner accès' (comme c'est le cas dans le considérant 158 du RGPD). La notion de 'rendre public' implique un accès bien plus large aux documents d'archives que ce que ne prévoit l'actuelle pratique en matière d'archives.

278. Dans la version néerlandaise, le terme courant dans ce contexte 'geselecteerd' doit être inséré à la place de 'gesorteerd'.

Articles 189-190

Garanties appropriées

279. L'article 189 du Projet est libellé comme suit : "*Le présent chapitre détermine les garanties appropriées requises par l'article 89 du Règlement.*"

280. L'article 190 du Projet est libellé comme suit : "*Le présent chapitre s'applique au traitement à des fins d'archives ou de recherche ou statistiques, à l'exception des traitements effectués par les services visés dans le titre 3 de la présente loi.*"

281. Ces deux articles parlent du "présent chapitre" alors qu'on vise sûrement "le présent titre".

282. La Commission renvoie aux remarques formulées ci-dessus aux 256264264 et estime que les deux dispositions doivent être supprimées car elles sont contraires au RGPD.

7.2. Chapitre II - Garanties générales

Article 191

Délégué à la protection des données

283. L'article 191 du Projet oblige chaque responsable du traitement qui se risque à un traitement poursuivant des finalités de connaissances à désigner un délégué à la protection des données. Comme expliqué ci-dessus, cette obligation s'applique quelle que soit la taille du traitement, quel que soit le risque qui l'accompagne et que le chercheur reçoive ou non exclusivement des données pseudonymisées. L'Exposé des motifs ne contient aucune justification de l'extension de l'obligation

de désigner un délégué à la protection des données. À tort, l'Exposé des motifs affirme que pour la majorité des traitements poursuivant des finalités de connaissances, l'obligation de désigner un délégué à la protection des données s'appliquerait quand même en vertu de l'article 37 du RGPD. Les exemples mentionnés ci-dessus illustrent cette affirmation (voir le point 262

284. La Commission estime que cette disposition est excessive et doit être supprimée. Tôt ou tard, chaque responsable du traitement procédera à un traitement poursuivant des finalités de connaissances, de sorte que virtuellement, chaque responsable du traitement devrait désigner un délégué à la protection des données. Vu le champ d'application territorial largement défini du Projet, la problématique se pose également pour les traitements poursuivant des finalités de connaissances dirigés au départ d'un autre État membre de l'Union européenne (voir les points 265e.s.).

285. S'il était quand même nécessaire d'étendre l'obligation de désigner un délégué à la protection des données, cela ne peut être imposé que pour les traitements qui impliquent un risque particulier. Un tel risque particulier peut exister dans le cas de certains - mais pas nécessairement tous les - traitements en vue de la pseudonymisation ou de l'anonymisation de données (voir l'observation mentionnée au 299299) - en particulier s'il s'agit de la publication des données anonymisées ou pseudonymisées avec les résultats de la recherche en question. Toutefois, la Commission estime que l'analyse d'impact relative à la protection des données constitue un instrument plus approprié pour faire face aux risques en fonction de la nature, de la portée, du contexte et des finalités.

Article 192

Registre des activités de traitement

286. L'article 192 du Projet oblige chaque responsable du traitement qui effectue un traitement poursuivant des finalités de connaissances à tenir un registre des activités de traitement. La dispense limitée reprise à l'article 30.5 du RGPD - traitements occasionnels effectués par des responsables du traitement de petite taille - est dès lors supprimée dans le contexte du titre 4. L'Exposé des motifs ne contient aucune justification de cette suppression. Néanmoins, ses conséquences sur le terrain ne peuvent pas être sous-estimées.

287. On peut raisonnablement supposer que presque chaque responsable du traitement entreprend tôt ou tard un traitement poursuivant des finalités de connaissances. La portée de l'article 30.5 du RGPD est en soi déjà difficile à expliquer à toutes les petites entités qui pensent pouvoir l'invoquer. L'article 192, § 1er du Projet ajoute à cela - sans motif clair - la complication inutile que la dispense pour des traitements occasionnels est parfois supprimée et est en outre complétée par des obligations supplémentaires (voir plus loin). Il est quasiment inconcevable que cette obligation soit applicable par l'APD dans la pratique.

Transparence

288. L'article 192, § 2 du Projet est libellé comme suit : "*Lors d'un traitement ultérieur de données à caractère personnel, le responsable du traitement ultérieur rend public le nom du responsable du traitement, le nom et les coordonnées du délégué à la protection des données et la finalité du traitement.*"

289. L'Exposé des motifs dispose qu'une transparence plus grande est nécessaire en tant qu' "*une garantie appropriée en contrepartie de la restriction des droits des personnes concernées et du fait de privilégier les traitements ultérieurs*" et renvoie en outre aux possibilités offertes au législateur par l'article 89 du RGPD. (Concernant la portée des termes 'traitement ultérieur' dans le Projet, voir le point 344.)

290. Les obligations de transparence sont régies aux articles 13 et 14 du RGPD :

- L'article 13 régit l'obligation de transparence dans les cas où un responsable du traitement a collecté des données à caractère personnel directement auprès de la personne concernée et veut les traiter ultérieurement pour une nouvelle finalité. L'article 13.3 du RGPD dispose que "*le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2*". L'article 13 du RGPD ne contient pas d'exception pour les traitements poursuivant des finalités de connaissances.

- L'article 14 du RGPD régit l'obligation de transparence dans les cas où un responsable du traitement n'a pas collecté les données à caractère personnel directement auprès de la personne concernée et veut les traiter ultérieurement pour une nouvelle finalité. En principe, le responsable du traitement doit informer la personne concernée avant de procéder au traitement ultérieur pour une autre finalité que celle pour laquelle les données à caractère personnel ont été obtenues (art. 14.4 du RGPD). L'article 14.5, b) du RGPD contient une limitation de l'obligation d'information - sous conditions - pour les traitements poursuivant des finalités de connaissances en particulier. Dans ce dernier cas, le responsable du traitement doit prendre des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.

291. Avec l'article 192, § 2, le Projet place globalement la barre moins haut en matière de transparence que les articles 13 et 14 du RGPD. Le responsable du traitement qui respecte uniquement l'obligation de publicité contenue à l'article 192, § 2 du Projet déchante. Étant donné que l'article 89.2-3 du RGPD n'autorise pas le législateur à instaurer une limitation aux obligations

d'information qui y sont reprises à l'égard des personnes concernées[86], on ne peut d'emblée pas parler d'une 'contrepartie' de la restriction de ces droits.

292. Même si l'obligation de l'article 192, § 2 du Projet doit être lue comme une obligation complémentaire qui s'applique "*sans préjudice des articles 13 et 14 du RGPD*", de sérieuses questions se posent encore concernant la compatibilité avec le RGPD.
L'Exposé des motifs décrit cette disposition comme une obligation partielle de publier le registre des activités de traitement. L'article 30 du RGPD ne contient aucune marge pour des dérogations nationales.
En ce qui concerne l'obligation de publier le nom du délégué à la protection des données, le Projet va à l'encontre de l'article 37.7 du RGPD qui n'impose que la publication des coordonnées.

293. L'Exposé des motifs fournit comme seule justification ce qui suit : "*Néanmoins l'article 89 du Règlement autorise les États-membres à aller plus loin dans les garanties appropriées et donc à rendre le registre public.*" Ainsi, le législateur ne démontre en aucune façon que les limites pour des dérogations nationales sont respectées.

294. La Commission estime que la publication de certaines informations constitue une garantie appropriée dans les cas où l'information directe des personnes concernées n'a pas lieu, lorsque l'article 14.5, d) du RGPD l'autorise. On ne peut toutefois pas en déduire tout simplement que la publication de certaines informations doit être imposée lors de chaque 'traitement ultérieur' poursuivant des finalités de connaissances. Les coûts pour la société de l'application et de l'exécution ne peuvent être évalués que très haut alors qu'on peut à peine s'attendre à des bénéfices au-delà de ce que prévoient les règles du RGPD. Le Projet attend de chaque responsable du traitement, lorsqu'un traitement ultérieur poursuivant des finalités de connaissances - aussi petit soit-il - est envisagé, qu'il veille soigneusement et investisse dans une procédure interne qui fait en sorte qu'une publication ait lieu conformément à l'article 192, § 2 du Projet. Les efforts demandés sont les plus lourds pour les petites entités, comme par exemple des PME innovatrices ou des chercheurs individuels, étant donné qu'ils n'ont généralement pas d'aide juridique immédiatement à leur disposition.

295. L'expérience avec le registre public des traitements nous apprend que des obligations générales de publication jouent un rôle plutôt modeste en tant que garantie de la transparence à l'égard des personnes concernées individuelles.

---

[86] Bien que l'article 14.5, b) du RGPD renvoie aux "*conditions et garanties visées à l'article 89, paragraphe 1*", la Commission ne voit ici aucune autorisation implicite accordée au législateur d'instaurer un règlement dérogatoire, en l'absence d'une mention à l'article 89.1 du RGPD que "*le droit d'un État membre peut prévoir des dérogations*".

296. La Commission estime que l'article 192 doit être supprimé dans son intégralité. L'obligation de tenir un registre tel qu'il est défini à l'article 30 du RGPD suffit également pour le contexte du titre 4. En outre, les articles 13 et 14 du RGPD régissent déjà un niveau plus élevé de transparence à l'égard de la personne concernée dans le cas d'une réutilisation de données à caractère personnel (tant en interne qu'en externe).

297. Si le législateur persiste avec l'article 192, § 2 du Projet, la finalité et la portée de la disposition doivent être précisées et pour le moins se limiter au traitement effectué par un autre responsable du traitement que celui qui s'est chargé du traitement initial. Par ailleurs, la Commission constate que la version néerlandaise et la version française ne coïncident pas.

7.3. Chapitre III. - Minimisation des données

Article 193

298. L'article 193 du Projet reprend le principe de "minimisation des données" contenu à l'article 5.1, c) et à l'article 89.1 du RGPD et l'encorsète conjointement avec l'article 195 du Projet dans un carcan plus serré (voir plus loin les points 309-313).

299. L'arrêté royal du 13 février 2001 contient en effet dans ses articles 3-5 un système de cascade pour les traitements ultérieurs à des fins historiques, statistiques ou scientifiques (de préférence des données anonymes, sinon des données codées et sinon, des données non codées). L'article 193 du Projet a pour objectif "*d'inviter le[s] responsable[s] du traitement à examiner les différentes possibilités qui s'offrent à lui [eux] pour atteindre ses [leurs] finalités*" (selon l'Exposé des motifs). Dans la mesure où cette disposition doit être uniquement lue comme un article de nature pédagogique, la Commission n'a pas d'objection de principe à la reprise du règlement des articles 3-5 de l'arrêté royal. Toutefois, la remarque suivante doit être formulée à cet égard : anonymiser correctement des données à caractère personnel afin d'exclure dans la pratique la réidentification s'avère très difficile[87]. Une pseudonymisation correcte n'est pas non plus évidente. La plus-value que peut offrir cette disposition pour la protection des personnes concernées est pour le moins relative.

300. Par le passé, la Commission n'a pas eu envie de se mêler systématiquement de la manière dont la recherche était menée - à l'exception d'un contrôle marginal. La Commission recommande à son successeur de maintenir cette ligne de conduite, d'autant plus que le Projet englobe aussi bien le traitement ultérieur que le traitement initial poursuivant des finalités de connaissances, et ce afin d'éviter un effet dissuasif sur la recherche qui - tout à fait selon les règles de l'art - compte sur le contact direct avec les personnes concernées.

---

[87] Voir par ex. Paul Ohm, "*Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*", UCLA Law Review, 2010, p. 170 et suivantes.

301. La Commission estime que l'article 193 du Projet doit au moins se limiter à la réutilisation des données à caractère personnel. Voir également plus loin - section 3 'Anonymisation ou pseudonymisation des données traitées à des fins de recherche ou statistiques' (voir les points 358e.s.).

Article 194

302. L'article 194 du Projet est libellé comme suit :

"*Plutôt que de collecter des données auprès de la personne concernée, le responsable du traitement à des fins de recherche ou statistiques utilise de préférence des traitements ultérieurs.*

Lorsqu'un traitement ultérieur ne permet pas d'atteindre la finalité de la recherche ou de statistiques, il procède à une nouvelle collecte de données auprès des personnes concernées."

303. Il ressort de l'Exposé des motifs que la préférence doit aller de manière générale à la réutilisation, même lorsqu'il s'agit d'une communication de données à caractère personnel par "*le responsable du traitement originel*" au "*responsable du traitement ultérieur*". La Commission explique en outre dans la Section 2 'Collecte de données par traitement ultérieur de données' pour quelles raisons les termes 'traitement ultérieur' sont inappropriés et elle utilise ci-après le terme 'réutilisation' (voir le point 344).

304. L'introduction d'une préférence générale pour la réutilisation est une limitation de la liberté de faire de la recherche. Les historiens qui décrivent l'histoire contemporaine et souhaitent interviewer des témoins devront d'abord justifier de manière suffisante que l'étude de sources écrites existantes ne leur permet pas d'atteindre leur objectif de recherche. Les scientifiques de toutes sortes de disciplines humaines devront défendre le choix d'une recherche qualitative en contact direct avec les personnes concernées, tout comme les études cliniques dans le domaine médical.

305. Cette limitation ne trouve pas sa source dans un des principes du RGPD. Poser directement un certain nombre de questions à la personne concernée pour une recherche sera plus conforme aux principes de transparence, de limitation de la finalité et de proportionnalité (minimisation des données) dans de très nombreuses circonstances que collecter les mêmes informations dans d'autres sources en vue de les réutiliser.
L'Exposé des motifs reconnaît explicitement que le Projet engendre un manque de transparence mais ajoute qu'il compense ce manque via l'article 192, § 2 et les articles 202 et suivants du Projet. La validité de ces compensations est examinée ailleurs (voir ci-avant et ci-après).

306. Les renvois dans l'Exposé des motifs aux articles 5.1, b), 89.1 et considérant 162 du RGPD ainsi qu'à l'avis n° 11/2003 de la Commission ne convainquent pas en tant que justification.

L'article 5.1, b) du RGPD précise que le principe de limitation de la finalité n'empêche pas le traitement ultérieur poursuivant des finalités de connaissances, il n'exprime toutefois pas une préférence générale pour la réutilisation.
L'article 89.1 du RGPD rappelle aux chercheurs le principe de minimisation des données comme suit : "*Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière*." On ne peut pas déduire de cette phrase une priorité générale au traitement ultérieur ou à la réutilisation lorsque des données anonymes ne suffisent pas.
Le considérant 162 du RGPD affirme en effet que les "*résultats statistiques peuvent en outre être utilisés à différentes fins, notamment des fins de recherche scientifique*" mais on ne peut pas y lire une préférence pour la réutilisation[88].

307. L'avis n° 11/2003 de la Commission[89] précise explicitement qu'une préférence pour la réutilisation ne traduit pas de manière opérationnelle le principe de proportionnalité mais en reconnaît en effet la valeur dans le contexte spécifique de la loi du 4 juillet 1962 *relative à la statistique publique*.

308. La Commission estime que l'article 194 du Projet est contraire à l'article 6.4 du RGPD qui régit le traitement ultérieur pour d'autres finalités et, sauf application de l'article 23 du RGPD, qu'il ne laisse pas de marge pour des dérogations nationales. En outre, cet article n'est pas non plus conforme à l'article 5 du RGPD, notamment aux principes de transparence, de limitation de la finalité et de proportionnalité (minimisation des données) et à la responsabilité.

Article 195

309. L'article 195 oblige le responsable du traitement à conserver, en annexe du registre des activités de traitement, quelle application il fait des articles 193 e 194 du Projet. En outre, le responsable du traitement doit toujours recueillir l'avis du délégué à la protection des données et également annexer celui-ci au registre.

310. La Commission constate que là où le législateur européen en finit avec de nombreuses dispositions formalistes, le législateur belge va à l'encontre de cette tendance dans le contexte du titre 4. Néanmoins, il n'y a aucune raison de croire que plus de formalisme conduit également à un meilleur respect des règles de protection des données.

311. Le RGPD souscrit à la responsabilité (art. 5.2 du RGPD) qui charge le responsable du traitement de respecter le RGPD et de pouvoir démontrer ce respect. À la lumière de ces éléments,

---

[88] "*Par "fins statistiques", on entend toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes statistiques ou la production de résultats statistiques.*"

[89] Avis n° 11/2003 de la Commission du 27 février 2003 *relatif à un avant-projet de loi modifiant la loi du 4 juillet 1962 relative à la statistique publique*.

on recommande donc simplement que le responsable du traitement documente les choix qu'il fait en matière de traitement de données à caractère personnel. La flexibilité encadrant ce principe, telle que reprise à l'article 24.1 du RGPD, - compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques - fait défaut dans le Projet.

312. Comme cela a été expliqué précédemment, ce régime strict s'applique virtuellement à chaque responsable du traitement et les coûts qui y sont liés pour la société ne peuvent être évalués que très haut - surtout pour les PME et les chercheurs individuels.
La Commission rappelle que recourir à un délégué à la protection des données pour chaque traitement poursuivant des finalités de connaissances est de toute évidence excessif (voir les points 283-285).

313. La Commission ne voit aucune plus-value dans l'article 195 du Projet et estime qu'il doit être supprimé car il est contraire à l'article 24 du RGPD.

Article 196

314. L'article 196 du Projet est libellé comme suit :

"Préalablement à la collecte, le responsable du traitement à des fins d'archives justifie l'intérêt public des archives conservées.

La justification est annexée au registre des activités de traitement."

315. Il ressort de l'Exposé des motifs que cette disposition aussi n'a été rédigée qu'en pensant aux activités d'autorités d'archivage publiques. L'ordre des actions - justifier l'intérêt général avant de procéder à la collecte des archives - l'indique également. La Commission renvoie aux remarques susmentionnées formulées à ce sujet (voir le point 274).

316. À la lumière de la responsabilité (art. 5.2 du RGPD), on recommande simplement que le responsable du traitement documente correctement le traitement à des fins d'archives dans l'intérêt public. Le formalisme de l'article 196 va à l'encontre du règlement flexible de l'article 24.1 du RGPD.

317. La Commission ne voit aucune plus-value dans l'article 196 du Projet et estime qu'il doit être supprimé car il est contraire à l'article 24 du RGPD.

7.4. Chapitre IV - Collecte de données

7.4.1. Section 1 - Collecte de données auprès de la personne concernée

Article 197

Collecte directe

318. L'article 197 du Projet définit que le responsable du traitement qui collecte des données auprès de la personne concernée en informe celle-ci - une obligation qui découle déjà de l'article 13 du RGPD.

319. S'il s'agit d'une collecte de données sensibles, le responsable du traitement doit en principe obligatoirement recueillir le consentement de la personne concernée. L'exigence du consentement est, selon l'Exposé des motifs, une mesure appropriée et spécifique qui doit être prévue par la loi en vue de sauvegarder les droits fondamentaux et les intérêts de la personne concernée, comme le requiert l'article 9.2, j) du RGPD.

320. Toutefois, l'exigence du consentement revient à supprimer l'article 9.2, j) du RGPD en tant que motif d'exception qui autorise le traitement de données sensibles. Les exceptions à l'exigence du consentement prévues à l'article 197, 2e alinéa du Projet dans les cas suivants n'apportent pas une solution :

1. lorsque les données ont été rendues publiques par la personne concernée ; ou

2. lorsque la collecte est rendue obligatoire par une loi ou l'intérêt public ; ou

3. lorsque la collecte est faite dans l'intérêt vital de la personne concernée.

321. Le lecteur attentif constate que cette énumération reprend partiellement - mais pas du tout entièrement - la formulation de l'article 9.2 du RGPD, sans trouver ainsi une échappatoire au raisonnement circulaire créé par l'article 197 du Projet. Le problème est illustré de manière étonnante par ce que l'Exposé des motifs affirme sur les suites à réserver au retrait du consentement dans ce contexte. Parce que le consentement sert ici de garantie et pas de base légale, le retrait n'a pas de conséquence :

"Lorsque la personne concernée retire son consentement, le traitement à des fins d'archives, de recherches ou statistiques conserve donc sa base légale : la loi adoptée en vertu de l'article 9.2 j) du Règlement.

Dans ce cas, l'article 17.3 d) du Règlement prévoit explicitement que le droit à l'oubli n'est pas d'application "dans la mesure où ce traitement est nécessaire (…) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement"."

322. Comment les responsables du traitement pourront expliquer la portée de ce consentement en tant que garantie de manière compréhensible aux personnes concernées reste un grand point d'interrogation. Le contrôle du respect de cette obligation par l'APD ne sera pas non plus une sinécure.

323. Le Projet limite les cas énumérés à l'article 9.2 du RGPD dans lesquels le traitement de données sensibles est autorisé et va plus loin que la clause d'ouverture reprise à l'article 9.4 du RGPD qui autorise les États membres à "*maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé*" et pas pour d'autres types de données sensibles.

324. La Commission estime que l'article 197 du Projet est pour le moins contraire à l'article 9 du RGPD et pour le reste, reprend inutilement l'article 13 du RGPD, et doit être supprimé.

Article 198

325. L'article 198 du Projet rend obligatoires quelques ajouts à l'article 13 du RGPD.

326. Concernant la notification de "*l'intérêt public des données collectées, en ce qui concerne les traitements à des fins d'archives*", la Commission reprend la remarque selon laquelle la collecte directe de données à caractère personnel ne constitue qu'un cas dans lequel l'archivage dans l'intérêt public intervient (voir le point 274).

327. En ce qui concerne un communication des modalités d'exercice des droits de la personne concernée, cette obligation découle déjà de l'article 12.2 du RGPD.

328. La Commission aborde ailleurs dans le présent avis les autres éléments de la communication :

- l'anonymisation ou la pseudonymisation éventuelle des données après leur collecte, en ce qui concerne les traitements à des fins de recherche ou statistiques299301);
- les limitations à la diffusion et à la communication des données377388);
- les restrictions aux droits de la personne concernée332 e.s., points 355 e.s., points 373 e.s.).

329. La Commission estime qu'à la lumière des remarques auxquelles il est fait référence ci-dessus, cet article doit être supprimé ou au moins réécrit.

Articles 199 et 200

330. Le Projet oblige le responsable du traitement à soumettre son information à l'avis du délégué à la protection des données et ensuite, à annexer au registre des activités de traitement l'information, l'avis et la justification éventuelle lorsqu'il ne suit pas cet avis.

331. Cette disposition chevauche dans une large mesure l'article 195 du Projet. La Commission reprend ses remarques formulées concernant cette disposition (voir les points 309-313 La Commission ne voit aucune plus-value dans les articles 199 et 200 du Projet et estime qu'ils doivent être supprimés car ils sont contraires à l'article 24 du RGPD.

Article 201

332. L'article 201, § 1er du Projet applique l'article 89.2-3 du RGPD et établit que les articles 15 et 16 du RGPD ne s'appliquent pas aux traitements poursuivant des finalités de connaissances dans deux cas.

333. Le premier cas est lorsque "*le responsable du traitement justifie que l'exercice de ces droits risquent de rendre impossible ou entravent sérieusement la réalisation de ces finalités d'archives, de recherche ou statistiques*". Dans ce cas, "*la justification, l'avis du délégué à la protection des données du responsable du traitement et la justification du responsable du traitement lorsqu'il ne suit pas l'avis du délégué à la protection des données sont annexés au registre des activités de traitement*". Cette approche formaliste chevauche dans une large mesure les articles 195, 199 et 200 du Projet. La Commission reprend donc ses remarques relatives à ces dispositions et estime que la deuxième phrase doit être supprimée car elle est contraire à l'article 24 du RGPD.

334. Le deuxième cas est lorsqu'il y a une base légale pour le traitement dans le droit de l'Union européenne, une loi, un décret ou une ordonnance qui :

- *donne pour mandat au responsable du traitement de traiter des données à des fins d'archives, de recherche ou statistique, et*
- *impose des règles de sécurité et de confidentialité aux personnes travaillant sous la responsabilité ou pour le compte du responsable du traitement, et*
- *interdit la réutilisation des données à d'autres fins.*

335. À dessein, ce deuxième cas ne mentionne pas une dérogation "*dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques*" (art. 89.2-3 du RGPD). En effet, selon l'Exposé des motifs, le "*projet de loi considère que l'exercice de ces droits d'accès et de correction entrave sérieusement les traitements à des fins d'archives ou statistiques*". Rien que pour cette raison, cette disposition est déjà problématique.

336. La sécurité et la confidentialité sont déjà imposées par l'article 32.4 du RGPD qui renvoie explicitement à "*toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant*". Cela figure également aux articles 28.3, b) et 29 du RGPD. Le deuxième élément obligatoire est superflu.
Par ailleurs, la loi *relative aux archives* du 24 juin 1955 - mentionnée dans l'Exposé des motifs à titre d'exemple - ne satisfait pas cette exigence.

337. Le dernier élément - l'interdiction de réutiliser les données à d'autres fins - est très surprenant. L'affirmation dans l'Exposé des motifs selon laquelle les données à caractère personnel sont "*réutilisables par d'autres responsables du traitement à des fins de recherches historiques, sociologiques ou statistiques*" - en faisant référence au considérant 158 du RGPD - ne correspond pas au texte du Projet.
La loi *relative aux archives* du 24 juin 1955 ne remplit pas cette condition. Selon la définition d' 'archives d'intérêt public' reprise dans le Projet, le but est précisément de rendre publiques des sources dans l'intérêt général, ce qui laisse au moins supposer une réutilisation pour d'autres finalités que celles que les Archives de l'État ont pour mission légale. La loi du 4 juillet 1962 *relative à la statistique publique* organise aussi elle-même une réutilisation pour d'autres finalités que celles que l'Institut national de Statistique a pour mission légale. Le chercheur qui obtient des données des Archives de l'État ou de l'Institut national de Statistique doutera au moins de l'application de l'exception.

338. L'article 201, § 2 dispose que : "*Les articles 17, 18 et 21 du Règlement ne s'appliquent pas aux traitements à des fins de recherche ou statistique qui font l'objet de l'information imposée à l'article 14 du Règlement.*"

339. L'article 201, § 3 dispose que : "*Les articles 17, 18, 20 et 21 du Règlement ne s'appliquent pas aux traitements à des fins d'archives qui font l'objet de l'information sur la collecte de données imposée à l'article 14 du Règlement.*"

340. La mention d'une dérogation à l'article 17 du RGPD est contraire au RGPD étant donné que cet article n'est pas mentionné dans les clauses d'ouverture de l'article 89.2-3 du RGPD. L'article 17 du RGPD contient déjà une exception pour des finalités de connaissances (à l'article 17.3, d) du RGPD) de sorte qu'une dérogation n'est pas nécessaire.

341. L'article 201, § 2-3 du Projet figure dans la section consacrée à la 'collecte de données auprès de la personne concernée' mais s'applique aux traitements "*qui font l'objet de l'information sur la collecte de données imposée à l'article 14 du Règlement*", qui s'applique en cas de collecte indirecte. L'Exposé des motifs ne dit rien sur cette partie de la phrase, de sorte que la Commission n'a aucun indice quant à la finalité sous-jacente.

342. Le Projet supprime les droits de la personne concernée dans ce contexte, ce qui va plus loin qu'instaurer une dérogation "*dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques*" (art. 89.2-3 du RGPD).

343. La Commission estime que l'article 201 du Projet est contraire au RGPD et doit être retravaillé. La Commission recommande à l'auteur du Projet de se rallier au règlement qui a déjà été promulgué dans d'autres États membres, par exemple le règlement allemand ou autrichien[90].

7.4.2. Section 2 - Collecte de données par traitement ultérieur de données

344. Le titre de la Section 2 'Collecte de données par traitement ultérieur de données' est contradictoire dans les termes. À la lumière du RGPD, les termes 'traitement ultérieur'[91] doivent être compris comme une référence à l'article 6.4 du RGPD - qui concerne le traitement à une autre fin par un seul responsable du traitement. L'Exposé des motifs, au contraire, considère qu'il y a différents responsables du traitement : un "*responsable du traitement ultérieur*" qui doit obligatoirement passer une convention avec le "*responsable du traitement originel*". Selon les termes du RGPD, il s'agit dans ce cas d'une collecte indirecte (réutilisation) de données à caractère personnel, telle que visée à l'article 14 du RGPD.

345. Vu le caractère extrêmement problématique du principe de préférence pour la réutilisation de données à caractère personnel introduit par l'article 194 du Projet, la Commission estime que la Section 2 doit être supprimée.

Article 202

346. L'article 202 du Projet rend obligatoire la signature d'une convention entre le responsable du traitement initial et celui qui réutilise les données ("responsable du traitement ultérieur").

347. L'Exposé des motifs ne justifie pas quelle disposition du RGPD permet d'imposer une telle obligation. La Commission estime que cet article est superflu et doit être supprimé.

Article 203

348. L'article 203 du Projet fait entrer en scène la notion de 'traitement public de données' pour pouvoir accorder une dispense de l'obligation de passer une convention. L'Exposé des motifs reste vague quant au contenu de cette notion et la définit d'une part comme tout "*traitement sans limite*

---

[90] Voir le § 26 et le § 27 de la *Datenschutz-Anpassugs- und -Umsetzungsgesetz* allemande, publiée dans le BGBI. I N° 44/2017 ; §. 7 de la *Bundesgesetz über den Schutz personenbezogener Daten* autrichienne telle qu'adaptée par la *Datenschutz-Anpassungsgesetz 2018*, publiée dans le BGBI I N° 120/2017.

[91] Cette terminologie a probablement été reprise de l'arrêté royal du 13 février 2001 qui parle de 'traitement ultérieur', tout comme la Directive 1995/46/CE dans le contexte de finalités de connaissances.

d'accès ni pour les personnes concernées ni pour les tiers" et complète d'autre part avec les lieux semi-publics définis dans un arrêt de la Cour de Cassation du 28 mars 2017.

349. La Commission estime que cet article entraîne des complications inutiles et que, tout comme le précédent, il doit être supprimé.

Article 204

350. L'article 204 du Projet contient une deuxième dispense de l'obligation de conclure une convention en utilisant les mêmes termes que ceux de l'article 201, § 1er, b) du Projet.

351. La Commission renvoie aux remarques exprimées ci-dessus concernant l'article 201, § 1er, b) et l'article 203 du Projet et estime que cette disposition doit être supprimée.

Articles 205-207

352. Vu les remarques formulées ci-dessus, la Commission estime que les articles 205 à 207 inclus qui définissent le contenu de la convention ou de l'information imposées par les articles 202 et 204 du Projet doivent être supprimés.

353. Il faut en particulier supprimer les dispositions qui accordent au responsable du traitement initial une certaine autorité sur les activités du responsable du traitement ultérieur. Il faut demander l'accord préalable du premier cité lors du recours à un sous-traitant par le réutilisateur et pour un nouveau traitement ultérieur. Le Projet s'ingère ainsi de manière substantielle dans l'organisation et l'exécution de la recherche, sans fournir la moindre justification.

354. La responsabilité formulée aux articles 5.2 et 24 du RGPD incitera le responsable du traitement à conclure une convention avec la source des données de recherche, ayant un contenu adapté à la nature, à la portée, au contexte et aux finalités du traitement. Le carcan imposé par les articles 205-207 du Projet est inutile et la Commission estime qu'il doit être supprimé.

Article 208

355. L'article 208 du Projet reprend le contenu de l'article 201, § 1er du Projet qui s'applique à la collecte directe de données à caractère personnel poursuivant des finalités de connaissances, en ajoutant l'article 14 du RGPD dans l'énumération. La mention d'une dérogation à l'article 14 du RGPD est contraire au RGPD étant donné que cet article n'est pas mentionné dans les clauses d'ouverture de l'article 89.2-3 du RGPD. L'article 14 du RGPD contient déjà une exception pour des finalités de connaissances (à l'article 14.5, d) du RGPD) de sorte qu'une dérogation n'est pas nécessaire.

356. Pour le reste, la Commission renvoie aux remarques formulées ci-dessus concernant l'article 201, § 1er du Projet et la Section 2 'Collecte de données par traitement ultérieur de données' et estime que cette disposition doit être réécrite.

Article 209

357. L'article 209 du Projet reprend en grande partie le contenu de l'article 201, § 2 et § 3 du Projet qui s'applique à la collecte directe de données à caractère personnel pour des finalités de connaissances. La Commission renvoie aux remarques formulées ci-dessus concernant l'article 201, § 2 du Projet et la Section 2 'Collecte de données par traitement ultérieur de données' et estime que cette disposition doit être réécrite.

7.4.3. Section 3 - Anonymisation ou pseudonymisation des données traitées à des fins de recherche ou statistiques

358. L'Exposé des motifs donne la raison d'être suivante pour la section 3 du Projet :

"*L'article 89 du Règlement dispose que les garanties appropriées :*

- *comprennent la pseudonimysation* [NdT : lisez "pseudonymisation"] *;*
- *privilégient les traitements ultérieurs ne permettant pas ou plus l'identification des personnes concernées.*

Cette section met en œuvre ces principes."

359. Les termes utilisés renvoient à l'article 89.1 du RGPD, comme expliqué ci-dessus, la Commission n'y lit qu'un rappel de l'applicabilité du RGPD dans ce contexte et aucune autorisation pour le législateur d'instaurer un régime dérogatoire général (voir les points 256257e.s.).
L'Exposé des motifs ne justifie pas quelle(s) disposition(s) du RGPD autorise(nt) l'imposition de l'obligation reprise dans la section 3.

360. La Commission estime que cette section doit être supprimée, vu le caractère problématique des dispositions qui y sont reprises.

Articles 210. 211, 213 et 214

361. Les articles 210, 211, 213 et 214 du Projet établissent que la toute première étape dans chaque traitement à des fins de recherche scientifique ou historique ou à des fins statistiques consiste à anonymiser ou pseudonymiser les données à caractère personnel. L'article 210 du Projet régit cet aspect pour le cas d'une collecte directe, l'article 211 du Projet pour les traitements "*par un responsable du traitement ultérieur identique au responsable du traitement initial*".

362. Le responsable du traitement qui obtient des données à caractère personnel via une collecte indirecte (réutilisation) pour ces finalités figure à l'article 213 du Projet. Le responsable du traitement qui obtient des données à caractère personnel via une collecte indirecte (réutilisation) de différentes sources est soumis à l'article 214 du Projet.

363. Il va de soi que les données à caractère personnel doivent être pseudonymisées le plus tôt possible - dans la mesure du possible - pour se conformer aux dispositions du RGPD. Des règles si détaillées concernant qui doit le faire et quand sont toutefois inutiles. Les parties concernées sont les mieux placées pour établir comment répartir les charges engendrées par cette pseudonymisation.

364. L'Exposé des motifs dispose que ces dispositions "*ne sont pas (...) d'application pour les traitements à des fins historiques, statistiques ou scientifiques dont le responsable du traitement démontre, conformément à l'article 100 du présent projet, qu'il ne peut réaliser la finalité du traitement qu'en ayant recours à des données à caractère personnel non pseudonymisées ou non anonymisées.*"[92]
Cela ne correspond pas au texte de ces dispositions qui ne contiennent aucune exception[93], ce qui revient évidemment pour la recherche historique - mais tout aussi bien dans d'autres cas - à une interdiction de certaines méthodes courantes de recherche.

365. Dans de très nombreux cas, pour l'organisation pratique de la recherche, l'identification des personnes concernées est nécessaire à certains moments déterminés : par exemple pour contacter les personnes interrogées pour les interviews, réaliser les enquêtes de suivi, constituer un panel pour des recherches ou engager et sélectionner des candidats pour des essais cliniques. Un chercheur prudent conservera - dans la mesure du possible - les données d'identification séparément des autres données afin de satisfaire aux exigences du RGPD, même sans disposition explicite dans le droit national.

366. La Commission reprend la remarque qui a été formulée sur l'anonymisation et la pseudonymisation (voir le 299299). La Commission considère que l'ingérence dans la manière dont les responsables du traitement concrétisent leurs activités de recherche - et l'interdiction partielle de méthodes de recherche - ne sont pas justifiées dans l'Exposé des motifs et sont en outre contraires au principe de base formulé aux articles 5.2 et 24 du RGPD. La responsabilité implique en effet que le responsable du traitement est effectivement responsable du respect du

[92] Le renvoi à l'article 100 doit probablement être lu ici comme un renvoi à l'article 193.

[93] Les articles 213 et 214 contiennent toutefois l'élément de phrase "sauf dispositions particulières" mais cela peut difficilement être signalé comme une exception.

RGPD et qu'il peut démontrer ce respect. Dès lors, la Commission estime que ces dispositions doivent être supprimées.

Article 212

367. L'article 212 du Projet établit que le responsable du traitement ne peut dépseudonymiser les données que pour les nécessités de la recherche ou des fins statistiques et après avis du délégué à la protection des données.

368. La Commission reprend la remarque qu'elle a formulée ci-dessus concernant l'article 195 du Projet et estime que l'article 212 doit être supprimé (voir les points 309313).

Article 215

369. L'article 215 du Projet est libellé comme suit :

"*Le tiers de confiance ne peut avoir de conflit d'intérêt avec le responsable du traitement ultérieur.*

Le tiers de confiance est le sous-traitant des responsables des traitements initiaux."

370. Le premier alinéa découle déjà de la définition de "tiers de confiance". Le deuxième alinéa donne une interprétation déterminée de la notion de 'sous-traitant' qui ne correspond pas nécessairement aux critères définis par l'article 4, 8) du RGPD, de sorte que cet alinéa est contraire au RGPD. La Commission estime que cet article doit être supprimé.

Article 216

371. Selon l'article 216 du Projet, le délégué à la protection des données contrôle l'utilisation des clés de pseudonymisation.

372. La Commission reprend les remarques formulées précédemment concernant le recours obligatoire à un délégué à la protection des données et estime que cet article doit être supprimé (voir les points 283-285).

Article 217

373. L'article 217 du Projet contient, tout comme les articles 201, 208 et 209, des dérogations à certains droits de la personne concernée lorsque les données sont anonymisées ou pseudonymisées.

374. Une fois que les données ont été dûment anonymisées, le RGPD ne s'applique plus, de sorte qu'une dérogation est inutile.
Une fois que les données ont été pseudonymisées, la limitation de l'article 11 du RGPD aux droits

repris aux articles 15 à 20 inclus du RGPD s'applique, sauf lorsque la personne concernée fournit des informations complémentaires qui permettent de l'identifier. L'article 217 limite aussi les droits des personnes concernées dans ces cas.

375. La mention d'une dérogation à l'article 14 du RGPD est contraire au RGPD étant donné que cet article n'est pas mentionné dans les clauses d'ouverture de l'article 89.2-3 du RGPD. L'article 14 du RGPD contient déjà une exception pour des finalités de connaissances (à l'article 14.5, d) du RGPD) de sorte qu'une dérogation n'est pas nécessaire.

376. Pour le reste, la Commission renvoie aux remarques formulées ci-dessus concernant l'article 201 du Projet et estime que l'article 217 doit être supprimé.

7.4.4. Section 4 - Diffusion des données traitées à des fins d'archives, de recherche ou statistiques

377. L'Exposé des motifs ne contient aucune référence à des dispositions du RGPD qui seraient mises en œuvre par cette section, mais renvoie à deux considérants liés à l'article 89 du RGPD. Comme expliqué ci-dessus, l'article 89.1 du RGPD ne contient aucune clause d'ouverture pour les États membres (voir les points 256257e.s). Cette section instaure un régime dérogatoire pour le traitement de données à caractère personnel non-pseudonymisées poursuivant des finalités de connaissances - plus particulièrement la diffusion de ces données - et, à défaut d'une justification, est contraire au RGPD.

378. D'ailleurs, le Chapitre V du titre 1 règle déjà le traitement de données à caractère personnel à des fins d'expression universitaire, sans que le lien soit établi dans cette section. La Commission estime que le règlement qui s'applique à la publication de résultats de recherche doit être parallèle au règlement qui s'applique pour la publication d'articles journalistiques, car établir dans la pratique la distinction entre les deux activités est quasiment impossible.

379. La Commission rappelle une fois encore que la portée des articles 218 et 219 du Projet est difficile à comprendre en raison de la double distinction qui est faite dans le champ d'application.

380. L'article 218 du Projet régit la publication de données à caractère personnel sous une forme non-pseudonymisée - tant concernant des données sensibles que non-sensibles. Ceci est permis sous certaines conditions inspirées du règlement actuel[94]:

a) la personne concernée a donné son consentement ; ou

b) les données ont été rendues publiques par la personne concernée elle-même ; ou

[94] Article 23 de l'arrêté royal du 13 février 2001.

c) les données ont une relation étroite avec le caractère public ou historique de la personne concernée ; ou

d) les données ont une relation étroite avec le caractère public ou historique de faits dans lesquelles (NdT : lisez "lesquels") *la personne concernée a été impliquée.*

381. L'article 219 du Projet dispose que dans la mesure où il s'agit de données non-sensibles, la publication sous une forme pseudonymisée est autorisée. Il faut supposer que pour les données sensibles, la possibilité de publication régie à l'article 218 du Projet s'applique encore.

382. La Commission insiste pour que ces articles soient supprimés.

7.4.5. Section 5 - Communication des données traitées à des fins d'archives, de recherche ou statistiques

383. L'Exposé des motifs ne contient aucune référence à des dispositions du RGPD qui seraient mises en œuvre par cette section. Comme expliqué ci-dessus, l'article 89.1 du RGPD ne contient aucune clause d'ouverture pour les États membres (voir 256257257 e.s). Cette section instaure un régime dérogatoire pour le traitement de données à caractère personnel non-pseudonymisées poursuivant des finalités de connaissances - plus particulièrement la communication de ces données à un tiers - et est de ce fait contraire au RGPD.

384. De surcroît, la Commission constate que la portée de l'article 220 du Projet - une interdiction de reproduire des données non-pseudonymisées - est formulée si vaguement que le respect de cette interdiction est problématique. Il est certain que la reproduction de données constitue une nécessité inévitable dans chaque système informatique, même s'il ne s'agit que de pouvoir afficher des données d'un support de stockage sur un écran. L'interdiction de reproduire des données non-pseudonymisées revient en tout cas à une interdiction générale d'utiliser des moyens automatisés pour le traitement - même si ces moyens servent précisément à pseudonymiser les données à caractère personnel.

385. En outre, la Commission constate que cette disposition n'est pas compatible avec l'article 214 du Projet qui régit qui doit procéder à la pseudonymisation en cas de couplage de plusieurs traitements initiaux - ce qui est difficilement réalisable sans reproduction des données à caractère personnel.

386. L'Exposé des motifs dispose que le but est d'obliger l'institution de "safe rooms" dans lesquelles le chercheur ne peut pas prendre de photos ou de scan mais bien des notes. Cela n'est pas conforme au contenu du texte du Projet, étant donné que des notes manuscrites constituent bel et bien aussi des 'reproductions'.

387. L'interdiction ne s'applique certes pas à tout traitement poursuivant des finalités de connaissances, elle s'applique dès qu'il est question d'une "communication des données", visant ainsi apparemment une collecte indirecte de données à caractère personnel[95] et dès qu'un des trois critères est rempli :

a) les données sont sensibles ; ou
b) la convention entre le responsable du traitement initial et le responsable du traitement ultérieur l'interdit ; ou
c) cette reproduction risque de nuire à la sécurité de la personne concernée.

388. Le niveau d'applicabilité de cette disposition du Projet est si bas qu'un nombre incroyablement élevé de traitements poursuivant des finalités de connaissances sont ainsi concernés, que le risque impliqué par ces traitements pour les personnes concernées soit élevé ou bas. Imposer un système de "safe rooms" en tant qu'obligation générale est évidemment excessif. Les exceptions mentionnées à l'article 221 ne sont rien de plus qu'un faux-fuyant.

La Commission insiste pour que ces articles soient supprimés.

CONCLUSION de la Commission sur le titre 4 du Projet

389. L'avis de la Commission est négatif sur l'intégralité de ce titre 4 pour les motifs expliqués au regard de chacun des articles commentés.

[95] Le Projet définit "communication des données" comme étant une "communication des données à des tiers identifiés" (art. 188, 10° du Projet).

8. TITRE 5 : VOIES DE RECOURS ET REPRESENTATION DES PERSONNES CONCERNEES

8.1. Chapitre I - Recours en cassation

Règles de compétence (art. 222)

390. L'article 222 règle la compétence du président du tribunal de première instance, siégeant comme en référé, lorsqu'un traitement constitue une violation d'une disposition légale ou réglementaire relative à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel[96].

391. La Commission accueille favorablement le choix du législateur de prévoir un recours juridictionnel effectif via une procédure telle que le référé. La compétence du président du tribunal de première instance fait l'objet d'une description générale. En vertu de cette disposition, le président du tribunal de première instance est donc compétent pour connaître des actions menées par l'APD en vertu de l'article 6 de la loi APD[97]. Ceci est d'ailleurs explicitement confirmé par l'article 224.3.2.

392. L'Exposé des motifs renvoie uniquement au recours en cessation tel qu'il est actuellement prévu à l'article 14 de la LVP (lequel sera abrogé à partir du 25 mai 2018). Afin que le lecteur comprenne mieux la portée réelle de cette disposition, la Commission recommande au législateur d'expliquer clairement que l'article 222 habilite le président du tribunal de première instance à connaître des actions menées par l'APD en vertu de l'article 6 de la loi APD.

393. Il est aussi recommandé de préciser dans l'Exposé des motifs que le président du tribunal de première instance peut aussi être saisi, via l'article 222, afin de poser une question préjudicielle à la Cour de Justice, conformément à l'article 267 du TFUE. Conformément à l'arrêt Schrems (C-362/14), il incombe en effet au législateur national de prévoir des voies de recours permettant à l'autorité compétente de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles doutent de la validité de l'acte, à un renvoi préjudiciel aux fins de l'examen de la validité de cet acte[98].

---

[96] La Commission observe que dans la version française, il est question de "*dispositions légales **ou** réglementaires*", tandis que dans la version néerlandaise, on parle de "*wettelijke **en** reglementaire bepaling*". La version néerlandaise doit être adaptée en utilisant le mot "of" car ici, aucune condition cumulative ne peut être posée.

[97] En vertu de l'article 58(5) du RGPD, les États membres sont tenus de prévoir, par la loi, que leur autorité de contrôle a le pouvoir de " *porter toute violation du présent règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement*".

[98] HVJEU, Maximillian Schrems c. Data Protection Commissioner, Affaire C-362/14, paragraphe 65.

Lacune : risque de violation grave

394. S'il est probable qu'un traitement envisagé, qui est imminent, constituera une violation grave à une disposition légale ou réglementaire relative à la protection des personnes physiques à l'égard de leurs données à caractère personnel, il convient de pouvoir empêcher l'exécution (ultérieure) de ce traitement.

395. Une possibilité similaire est prévue à l'article 1er de la loi du 12 janvier 1993 *concernant un droit d'action en matière de protection de l'environnement*[99], qui dispose que :

> "*Sans préjudice des compétences d'autres juridictions en vertu d'autres dispositions légales, le président du tribunal de première instance, à la requête du procureur du Roi, d'une autorité administrative ou d'une personne morale telle que définie à l'article 2, constate l'existence d'un acte même pénalement réprimé, constituant une violation manifeste ou une menace grave de violation d'une ou de plusieurs dispositions des lois, décrets, ordonnances, règlements ou arrêtés relatifs à la protection de l'environnement.*
> *Il peut ordonner la cessation d'actes qui ont formé un commencement d'exécution ou imposer des mesures visant à prévenir l'exécution de ces actes ou à empêcher des dommages à l'environnement. Avant tout débat au fond, une tentative de conciliation aura lieu.*
> *Le président peut accorder au contrevenant un délai pour se conformer aux mesures ordonnées.*"

396. L'article 222 régit uniquement la compétence du président du tribunal de première instance s'il est question d'un traitement. Strictement parlant, le président du tribunal ne serait dès lors pas compétent pour statuer si le traitement en tant que tel n'a pas encore débuté, même s'il est probable qu'un traitement envisagé constituera une violation grave d'une disposition légale ou réglementaire relative à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel.

397. La Commission recommande dès lors, par analogie avec la disposition précitée de la loi concernant un droit d'action en matière de protection de l'environnement, d'ajouter une disposition libellée comme suit :

> "*Le président du tribunal de première instance peut ordonner la cessation de traitements qui ont formé un commencement d'exécution ou imposer des mesures visant à prévenir leur exécution ou à empêcher une violation grave d'une disposition légale ou réglementaire relative à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel.*"

Le juge territorialement compétent (article 224.2)

398. L'article 224.2 régit la compétence territoriale du président du tribunal de première instance. Il s'agit d'une compétence spécialisée qui, pour des raisons de qualité, est de préférence octroyée à des magistrats spécialisés. Le morcellement territorial de la compétence pour le président du

[99] M.B. du 19 février 1993.

tribunal de première instance engendrera en outre une jurisprudence disparate ; il y a en effet des procédures en référé dans l'ensemble des 27 divisions des arrondissements judiciaires.

399. Il paraît indiqué à la Commission de concentrer ces procédure autant que possible à Bruxelles ; en ce qui concerne les affaires néerlandophones auprès du président du tribunal de première instance néerlandophone de Bruxelles et en ce qui concerne les affaires francophones, auprès du président du tribunal de première instance francophone de Bruxelles (et en ce qui concerne les affaires germanophones, auprès du président du tribunal de première instance d'Eupen).

400. À la lumière de ce qui précède, la Commission recommande au législateur de reformuler le projet d'article 224.2 comme suit :

"§ 2. Par dérogation à l'article 624 du Code judiciaire, le recours est porté : en ce qui concerne les affaires néerlandophones devant le président du tribunal de première instance néerlandophone de Bruxelles, en ce qui concerne les affaires francophones, devant le président du tribunal de première instance francophone de Bruxelles et en ce qui concerne les affaires germanophones, devant le président du tribunal de première instance d'Eupen." [100]

Qui introduit le recours ? (art. 224.3)

401. L'article 224.3 de l'avant-projet dispose que le recours fondé sur l'article 222 peut être formé par la personne concernée ou par le "*président de l'autorité de contrôle compétente*".

402. La Commission observe que cette disposition accorde apparemment un droit de recours à toute autorité de contrôle compétente visée par l'avant-projet (agissant dans le cadre de ses compétences) et donc pas uniquement à l'APD. L'Organe de contrôle, le Comité R et le Comité P en bénéficient donc également. La Commission se réfère à cet égard à ses remarques concernant l'utilisation de la désignation "autorité de contrôle compétente".

403. En ce qui concerne le droit de recours de l'APD, la Commission fait remarquer qu'en vertu de l'article 3 de la loi APD, l'APD dispose de la personnalité juridique. Vu que l'APD disposera de la personnalité juridique, les mots "du président de" doivent être supprimés (du moins en ce qui concerne l'APD)[101]. L'article 18 de la loi APD prévoit en effet déjà que c'est le président qui représente l'APD en droit. En outre, du point de vue procédural, il convient de faire une distinction entre d'une part la partie au procès et d'autre part l'organe de la partie au procès qui représente la partie au procès en justice. La partie au procès sera l'APD et l'organe qui représente l'APD sera

[100] Voir également par analogie l'article 627, 11°, 16° et 17° du Code judiciaire en ce qui concerne la compétence territoriale des tribunaux francophones et néerlandophones de Bruxelles. Voir aussi par analogie les articles 632, 632*bis*, 633*sexies* et 633*septies* du Code judiciaire en ce qui concerne la compétence territoriale du tribunal de première instance d'Eupen lorsque la procédure est menée en allemand.

[101] La situation est autre en vertu de l'article 32, § 3 de la LVP, où il était question "du président de" et pas "de la Commission" car la Commission n'a pas la personnalité juridique.

son président. Il serait étrange que l'article 224.3 dispose que la partie au procès ne soit pas l'APD mais le représentant de l'APD.

Lacune : compétence administrative pour la décision d'agir en droit

404. Tant la loi APD que l'avant-projet sont dépourvus d'une disposition précisant quel organe de l'APD est compétent pour prendre la décision d'agir en droit. Ce n'est pas parce que l'article 18 de la loi APD dispose que le président ou le membre le plus âgé du comité de direction représente l'APD en justice que celui-ci jouit aussi d'emblée de la compétence administrative pour prendre la décision d'agir en droit. Il s'agit là de deux choses différentes. Il peut en effet arriver que l'organe X d'une autorité publique soit compétent pour prendre la décision d'agir en droit mais que l'autorité soit ensuite représentée en justice par l'organe Y.

405. La question de savoir qui a la compétence de prendre cette décision ne peut donc pas être simplement réglée dans le règlement d'ordre intérieur car celui-ci a une valeur purement interne et n'a aucun effet juridique vis-à-vis de tiers. Cette question doit donc être réglée par voie légale. Une loi qui crée un organisme d'État doit comporter une disposition qui précise quel organe de cet organisme est compétent pour prendre la décision d'agir en droit (indépendamment de qui représentera l'organisme en justice).

406. Ainsi par exemple, l'article 193, § 1 du Décret communal dispose ce qui suit :

> "*Le collège des bourgmestre et échevins représente la commune dans des cas judiciaires et extrajudiciaires **et** décide d'agir en droit au nom de la commune.*"

407. Il ressort de cette disposition que la décision d'agir en droit doit être prise par le collège et que c'est par ailleurs également le collège qui représente ensuite la commune lors de cette intervention en justice.

408. Si le législateur ne détermine pas précisément quel organe de l'APD est compétent pour décider d'agir en droit, le risque existe que chaque partie citée à comparaître par l'APD demande de déclarer l'irrecevabilité de l'action (au motif qu'il n'a pas été valablement décidé de procéder à la citation à comparaître). Le législateur manquerait ainsi à ses obligations en vertu de l'article 58.5 du RGPD. Afin d'y remédier, la Commission recommande d'ajouter à l'avant-projet une disposition qui complète l'article 18 de la loi APD (par analogie avec la disposition en question du Décret communal), libellée comme suit :

> "*Le président du comité de direction et, en son absence, le membre présent le plus âgé du comité de direction, à l'exception du président de la chambre contentieuse, représente l'Autorité de protection des données en justice. La décision d'agir en droit au nom de l'Autorité de protection des données est prise par le comité de direction.*"

Décisions concernant la rectification, la suppression ou la limitation en cas d'enquête ou de procédure pénale (article 223)

409. L'article 223 prévoit une exception à la compétence générale du président du tribunal de première instance de prendre connaissance des traitements constituant une violation d'une disposition légale ou réglementaire relative à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel, du moins en ce qui concerne les actions relatives à la rectification, la suppression, la limitation du traitement, l'interdiction d'utiliser ou l'effacement de données à caractère personnel. L'exception sera applicable "À partir du moment" où les données font l'objet d'un traitement "lors d'une information, d'une instruction, d'une procédure pénale devant le juge de fond ou d'une procédure d'exécution d'une peine pénale "[102]. À partir de ce moment, la compétence de décider de la rectification, de la suppression, de la limitation du traitement, de l'interdiction d'utiliser ou de l'effacement de données à caractère personnel appartiendrait toutefois exclusivement, suivant la phase de la procédure, au ministère public ou au juge pénal compétent.

410. La Commission a deux remarques à cet égard. Premièrement, la Commission ne voit pas en quoi le traitement de l'action par le ministère public constitue un recours juridictionnel effectif au sens de l'article 79 du RGPD, d'autant plus lorsque l'information a lieu sous la responsabilité du ministère public même. Deuxièmement, la Commission trouve que cette disposition est rédigée de manière particulièrement floue.

411. À la lumière de ce qui précède, la Commission recommande de reformuler l'article 223 comme suit :

"*Par dérogation à l'article 222, le juge pénal, pour autant qu'il ait déjà été saisi, est compétent pour statuer sur une action relative à la rectification, la suppression, la limitation du traitement, l'interdiction d'utiliser ou l'effacement de données à caractère personnel.*"

412. Les articles 224-232 n'appellent aucune remarque particulière.

8.2. Chapitre II - Représentation des personnes concernées

413. L'article 233 règle la possibilité de représentation en droit des personnes concernées La Commission déplore que l'avant-projet ne fasse pas usage à cet égard de la possibilité reprise à l'article 80.2 du RGPD, qui permet de prévoir que tout organisme, organisation ou association visé(e) à l'article 80.1 du RGPD, indépendamment de tout mandat confié par une personne concernée, a le droit d'introduire une réclamation ou d'agir en droit s'il (elle) considère que les

[102] La Commission observe que le terme "traitement" en français à l'article 223 devrait à chaque fois être traduit par le terme "verwerking" en néerlandais.

droits d'une personne concernée prévus dans ce règlement ont été violés du fait du traitement. La Commission recommande d'encore utiliser cette possibilité.

CONCLUSION de la Commission sur le titre 5 du Projet

414. En conclusion, la Commission émet un avis favorable sur le Titre V du projet de loi en ce qui concerne les règles de compétence, à condition qu'il soit tenu compte à la fois des remarques générales et des remarques formulées par article, plus précisément en ce qui concerne l'article 222, l'article 223 et l'article 224 et émet un avis défavorable sur le Titre V du projet de loi en ce qui concerne les lacunes en cas de risque de violation grave et en ce qui concerne la compétence administrative pour la décision d'agir en droit.

9. TITRE 6 : SANCTIONS

Remarques générales

Dérogation pour le secteur public

415. L'article 83.7 du RGPD oblige les États membres à définir explicitement si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics.

416. L'article 234, § 2 du projet est énoncé comme suit : "*L'article 83 du Règlement ne s'applique pas aux autorités publiques et organismes publics.*" L'Exposé des motifs ne justifie pas le choix retenu, mais affirme seulement ce qui suit :

> "*Il est naturellement clair que le secteur public n'est pas exempté des obligations prévues par le Règlement et ce projet de loi. Toutefois il est choisi de ne pas faire appliquer les amendes administratives au secteur public.*"

417. En ce qui concerne l'ouverture que le RGPD laisse au législateur national, la Commission est en principe favorable au fait de traiter le secteur public et le secteur privé de la même manière en ce qui concerne le contrôle de l'application des lois. On peut difficilement défendre la situation où l'APD a moins de possibilités à l'égard du secteur public, surtout s'il s'agit d'autorités qui peuvent prendre des décisions contraignantes à l'égard de justiciables ou lorsque les personnes concernées n'ont pas le choix de la personne à qui elles recourent pour la fourniture d'un service public.

418. On ne peut pas déduire de l'Exposé des motifs que l'objectif du législateur serait de considérer une interdiction ou une limitation de traitement comme moyen ultime de faire appliquer la loi à l'égard du secteur public. La sauvegarde de la continuité du service public n'est de toute évidence pas non plus favorisée de la sorte. D'une part, la limitation de traitement sert à faire cesser la violation des droits de la personne concernée en ce qui concerne la protection des données et d'autre part, cette même limitation de traitement peut impacter la personne concernée dans ses intérêts. Force est dès lors de constater que la personne concernée risque d'être le dindon de la farce à deux reprises.

419. Si le législateur estime devoir introduire une dérogation pour les "autorités publiques et organismes publics", la Commission est d'avis que le champ d'application de cette dérogation doit être délimité minutieusement dans l'intérêt de la sécurité juridique (voir également les remarques formulées au sujet du titre 1, chapitre IV, section 2, n° 149-152). À défaut d'une quelconque définition des autorités publiques et organismes publics dans le projet, la Commission ne peut que constater qu'une grande zone grise est créée, entravant une application effective de la loi.

420. Le projet ne répond pas à la question de savoir si l'exception s'applique aux services publics exécutés par des entités de droit privé (par exemple des ASBL et fondations chargées par ou en vertu de la loi de tâches d'intérêt général) ou aux entreprises publiques autonomes telles que régies par la loi du 21 mars 1991[103]. Il va toutefois de soi que des organismes qui ont essentiellement les mêmes activités soient traités de la même manière. Un simple critère organique ne peut par exemple pas justifier que l'hôpital d'un CPAS ne puisse pas se voir infliger d'amende administrative, alors que cela pourrait bien être le cas à l'égard d'hôpitaux créés sous la forme d'une ASBL.

421. La manière dont le projet utilise la clause d'ouverture contenue à l'article 83.7 du RGPD est contraire au RGPD et au principe de légalité. Dans ses lignes directrices concernant les délégués à la protection des données, le Groupe de travail Article 29 a affirmé que cette notion devait être définie dans le droit national[104].

422. La Commission insiste pour que l'on reconsidère cette disposition. Si la dérogation est maintenue, il convient de l'expliquer plus avant et la Commission propose alors de délimiter la dérogation en se référant à l'article 5, 4e alinéa du Code pénal qui comporte une énumération de plusieurs instances[105].

Sanctions pénales dans le secteur public

423. Du fait que le projet choisit d'exclure les amendes administratives pour le secteur public, l'article 84.1 du RGPD doit être respecté avec d'autant plus de minutie[106]. Un système de sanction effectif, proportionné et dissuasif doit exister. Les articles 235-242 du projet servent à exécuter cela, en réprimant certaines infractions par des sanctions pénales.

424. En ce qui concerne le caractère dissuasif, l'Exposé des motifs précise ce qui suit au sujet du niveau maximal établi pour les amendes pénales :

"Afin de renforcer les sanctions pénales, et les rendre dissuasives, au regard des sanctions administratives, les montants sont maintenus tels quels et ce, en vertu de l'article 2 de la loi du 26 juin 2000 relative à l'introduction de l'euro dans la législation concernant les matières visées à l'article 78 de la Constitution : les montants exprimés en BEF sont censés être exprimés en EUR sans

---

[103] Loi du 21 mars 1991 *portant réforme de certaines entreprises publiques économiques.*

[104] Groupe de travail Article 29, "Lignes directrices concernant les délégués à la protection des données (DPD), WP243 rev. 01, p. 6.

[105] Il s'agit des instances suivantes : l'État fédéral, les régions, les communautés, les provinces, les zones de secours, les prézones, l'agglomération bruxelloise, les communes, les zones pluricommunales, les organes territoriaux intra-communaux, la Commission communautaire française, la Commission communautaire flamande, la Commission communautaire commune et les centres publics d'aide sociale.

[106] L'article 84.1 du RGPD est énoncé comme suit : "*Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives.*"

conversion. Il est également rappelé que les montants sont, depuis le 1er janvier 2017, multipliés par 8, en vertu de l'article 1, alinéas 1 et 2 de la loi du 5 mars 1952 relative aux décimes additionnels sur les amendes pénales, modifiée par l'article 59 de la loi du 25 décembre 2016."

425. Malgré ce qui précède, la Commission ne peut que constater que le niveau maximal des amendes pénales est significativement inférieur à celui des amendes administratives. Le législateur n'est pas tenu de fixer un niveau maximal identique, tant que le niveau établi permet de réagir avec effectivité, proportionnalité et dissuasion. L'Exposé des motifs est manifestement insuffisant que pour en arriver à cette conclusion. Dans d'autres domaines, il est d'ailleurs d'usage que le niveau des amendes administratives soit inférieur à celui des amendes pénales, qui servent de remède ultime. La Commission estime que le projet doit être revu sur ce point.

426. La limitation des amendes administratives à l'égard du secteur public est compensée de manière très limitée par les dispositions pénales. D'après l'article 5, 4e alinéa du Code pénal, un nombre important d'instances ne sont pas considérées comme des personnes morales responsables pénalement[107].

427. Le projet fait un lien entre les mesures correctrices que l'autorité de contrôle peut infliger et les dispositions pénales. L'article 235, e) du projet sanctionne le non-respect de la mesure correctrice adoptée par l'autorité de contrôle visant la limitation définitive des flux conformément à l'article 58.2.f) du RGPD. La violation d'une limitation temporaire de flux de données ne peut de nouveau pas être sanctionnée, ce qui ébranle encore un peu plus l'effectivité de cette mesure à l'égard du secteur public. La Commission estime que le projet doit être revu sur ce point.

428. La Commission estime par ailleurs qu'il faut au moins y ajouter le non-respect d'une mesure correctrice au sens de l'article 58.2.d) du RGPD (ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du RGPD, de manière spécifique et dans un délai déterminé).

429. Se basant sur ce qui précède, la Commission estime que l'on ne respecte pas l'obligation de veiller à des sanctions effectives, proportionnées et dissuasives dans le secteur public. Elle estime que le projet doit être revu sur ce point, par exemple en reprenant une des pistes suivantes.

---

[107] Il s'agit des instances suivantes : l'État fédéral, les régions, les communautés, les provinces, les zones de secours, les prézones, l'agglomération bruxelloise, les communes, les zones pluricommunales, les organes territoriaux intra-communaux, la Commission communautaire française, la Commission communautaire flamande, la Commission communautaire commune et les centres publics d'aide sociale.

430. La Commission européenne a proposé un règlement dans lequel les institutions ou organes de l'Union européenne pourraient être soumis à des amendes administratives allant jusqu'à 50 000 EUR par violation et jusqu'à un total de 500 000 EUR par an pour certaines violations[108].

431. Outre l'établissement d'un autre plafond, le législateur pourrait donner à l'autorité de contrôle la compétence d'imposer aux autorités publiques et organismes publics de consacrer soit une somme, soit une part de leur budget pour une seule ou plusieurs périodes successives à l'exécution de la mesure correctrice qu'elle prononce ou qu'elle a prononcée. Pour faire planer l'ombre de la sanction, le non-respect de cette mesure pourrait engendrer soit sa conversion en une amende administrative, soit l'exécution forcée par ou pour le compte de l'autorité de contrôle.

Remarques par article

Article 234

432. Les compétences correctrices de l'autorité de contrôle en vertu de l'article 58.2 du Règlement s'appliquent également aux dispositions suivantes :

- les articles 7, 8, 9, 19, 23, 25, 26, 28 et 29 du titre 1 ;
- les articles 33 à 72 du titre 2 ;
- le titre 4.

433. En ce qui concerne le renvoi aux articles du titre 1, il s'agit d'une conséquence de ce que prévoit l'article 2, deuxième alinéa du projet sur l'extension du champ d'application du Règlement aux traitements visés aux articles 2.2.a) et 2.2.b) du RGPD.

434. La Commission estime que l'article 22 du projet doit être repris. Voir les remarques formulées ci-dessus au sujet du caractère obligatoire du protocole de communication de données à caractère personnel par des autorités publiques (n° 159).

Article 235

435. La disposition pénale de l'article 235 du projet vise notamment le "représentant en Belgique" du responsable du traitement ou du sous-traitant.

---

[108] Proposition de Règlement du Parlement européen et du Conseil *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE*, COM(2017)8.

436. La question se pose de savoir dans quelle mesure la mention du représentant peut être opérationnelle étant donné que dans le RGPD, le représentant fait office de personne de contact mais n'a aucune obligation à proprement parler. Les cas dans lesquels on pourra imputer dans la pratique des faits punissables à un représentant semblent rares et le signal que donne le législateur est que le fait de reprendre le rôle de représentant en Belgique implique ce risque.

437. L'Exposé des motifs ne clarifie en rien les motifs de cette mention. La Commission estime que le législateur doit reconsidérer ce point.

Article 238

438. L'article 238 est énoncé comme suit : "*En condamnant du chef d'infraction aux articles 236 ou 237, le tribunal peut ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'il détermine, aux frais du condamné.*"

439. D'après l'Exposé des motifs, cette disposition est une reprise de l'article 40 de la LVP. La Commission constate que dans ce cas, il faut se référer aux articles 235 et 236 du projet. L'article 237 du projet est une reprise de l'article 37 de la LVP, auquel l'article 40 de la LVP ne se réfère pas. La Commission estime que cette erreur matérielle doit être rectifiée.

Articles 239 - 240

440. Les articles 239 et 240 du projet sanctionnent certaines violations de traitements de données régis au titre 3.

441. La Commission constate que les sanctions mentionnées aux articles 239 et 240, 1° et 2° du projet visent les infractions commises par le sous-traitant, par des personnes agissant sous l'autorité de l'autorité visée au titre 3 ou de son sous-traitant. Il est frappant de constater qu'il y a ici un absent : le responsable du traitement lui-même, qui est en fin de compte responsable du traitement de données à caractère personnel, conformément aux règles en vigueur. L'Exposé des motifs dispose ce qui suit à cet égard : "*Le responsable du traitement n'est pas visé par la disposition pénale, étant donné qu'une autorité publique n'ayant pas la personnalité juridique ne peut pas être condamnée au pénal.*"[109] La Commission estime que le responsable du traitement doit être mentionné.

442. L'article 240, 4° du projet vise certaines infractions commises par "*quiconque a transféré* (…) *des données à caractère personnel*". L'article 240, 5° du projet vise "*toute personne qui a accès à des données à caractère personnel visées aux articles 101, 134 et 164*". La Commission constate qu'on ne

[109] Comme expliqué ci-avant, l'article 5, 4e alinéa du Code pénal exclut la responsabilité pénale de plusieurs autorités publiques citées.

sait pas clairement si ces dispositions ont une autre portée personnelle que celle de l'article 240, 1° et 2° du projet.

Article 242

443. L'article 242 du projet régit le concours entre procédures administratives et pénales. À défaut d'un protocole d'accord, le procureur du Roi dispose d'un délai de deux mois pour décider des suites qu'il donne à un procès-verbal. Pendant ce délai et si le procureur reprend effectivement le dossier, "*la possibilité pour l'autorité de contrôle d'exercer ses mesures correctrices [est éteinte]*".

444. La Commission estime qu'une telle extinction de compétences correctrices – même temporaire – est contraire à l'article 58.2 du RGPD et doit dès lors être supprimée.

CONCLUSION de la Commission au sujet du Titre 6 du projet

445. L'avis de la Commission est négatif sur l'intégralité de ce Titre 6 pour les motifs expliqués au regard de chacun des articles commentés.

10. TITRE 7 : L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

La création de trois DPA belges supplémentaires[110]

A. Généralités

446. La Commission constate que dans le Projet, trois nouvelles DPA sont créées : le C.O.C., le Comité R et le Comité P, ce en plus évidemment de la DPA déjà créée par la LAPD, à savoir l'APD (et en plus aussi d'un contrôle distinct des juridictions dans le cadre de leur fonction juridictionnelle[111]). **Au total, le législateur fédéral créerait donc quatre DPA** (et peut-être encore un organe de contrôle distinct pour les juridictions).

447. Dans son avis n° 45/2016 du 31 août 2016, la Commission avait déjà souligné le fait que l'Organe de contrôle de l'information policière existant (ci-après le "C.O.C.") avait un statut hybride : d'une part le C.O.C. ressemble à une DPA spécifique pour le secteur policier et d'autre part il n'exerce pas toutes les compétences imposées à une DPA en vertu de la Directive. La Commission avait insisté à l'époque pour que l'on opère à l'avenir un choix clair : soit le C.O.C. devient une DPA à part entière pour tous les traitements de données policiers, soit l'aspect protection des données dans le secteur policier est traité intégralement par la Commission[112]. La Commission avait déjà bien compris à l'époque que la situation actuelle du C.O.C. était défavorable/illogique – en ce sens qu'au niveau des tâches et compétences, il se retrouvait pris dans un étau entre les tâches et compétences de la Commission et celles du Comité P – et qu'une réforme s'imposait quoi qu'il en soit. Le C.O.C. a d'ailleurs lui-même indiqué en 2016 qu'il souhaitait évoluer vers une DPA à part entière et qu'il pouvait mener cette réforme sans impact budgétaire[113]. On s'attendait donc à ce que le C.O.C. soit réorganisé.

448. La Commission constate par ailleurs qu'en vertu du Projet, non seulement le C.O.C. deviendrait une DPA, mais qu'il en serait de même pour le Comité R et pour le Comité P.

---

[110] Voir principalement les articles 73, 97 à 100 inclus, 107.8, 130 à 133 inclus, 163, 186 & Titre 7 & Titre 8 du Projet.

[111] Cf. article 4, § 2, premier alinéa de la LAPD et considérant 20 du RGPD.

[112] Voir les points 6 à 13 inclus de l'avis n° 45/2016.

[113] Voir l'avis n° 01/2016 du C.O.C. du 15 septembre 2016 (point 8) : "Pour être pleinement considéré comme une autorité de contrôle au sens de la Directive, il ne manque que la possibilité pour le C.O.C. de traiter des plaintes, dont le traitement de requêtes d'accès direct ou non, et la possibilité d'imposer des mesures contraignantes. (…) Cela peut en outre se faire sans impact budgétaire, étant donné que le C.O.C. estime pouvoir exercer ces activités supplémentaires dans le cadre du budget actuel". [Traduction libre effectuée par le Secrétariat de la Commission vie privée, en l'absence de traduction officielle].

La Commission prend acte de ces choix politiques, qui correspondent en soi au principe selon lequel plusieurs DPA peuvent être désignées dans un État membre (cf. art. 51.1 du RGPD et art. 41.1 de la Directive). La Commission examine toutefois ci-après dans quelle mesure la concrétisation de ces choix politiques dans le texte du Projet :

- donne lieu à une répartition de compétences claire/cohérente/efficace entre les DPA[114] ;
- respecte toutes les règles imposées aux DPA par le RGPD et la Directive et est cohérente avec la LAPD.

B. La répartition de compétences entre les DPA

449. La Commission estime qu'il est crucial de définir une répartition de compétences convaincante entre les différentes DPA belges. Il convient à cet égard d'éviter autant que faire se peut des compétences communes ou qui se chevauchent en raison de l'insécurité juridique qui en découle et de leur caractère extrêmement inefficace : si deux DPA doivent intervenir conjointement – par exemple à l'occasion d'une demande d'avis/plainte/enquête – cela implique en effet que deux services différents doivent analyser le dossier et se concerter pour tenter au maximum de parvenir à un point de vue cohérent. Eu égard en particulier aux restrictions budgétaires actuelles, le but devrait être de gagner en efficacité et certainement pas de créer de nouvelles inefficacités, comme des dossiers doublons dans différents services. La Commission estime dès lors évident d'attribuer à chacune des DPA un ensemble homogène de compétences.

450. Si la Commission a bien compris le Projet – ce qui n'est absolument pas une évidence étant donné que les dispositions relatives à la DPA compétente sont dispersées dans l'ensemble du texte du Projet (et de la LAPD) – la répartition de compétences entre les quatre DPA serait établie comme suit :

- le C.O.C. devient la DPA pour [115] :
  - les services de police ;
  - le Service d'enquêtes du Comité P ;
  - l'Inspection générale de la police fédérale et locale ;
  - l'Unité d'information des passagers,

[114] La Commission a évidemment tout intérêt à ce qu'un règlement clair soit prévu, étant donné que son successeur en droit – l'APD – devra jouer un rôle central dans ce paysage à partir du 25 mai 2018.

[115] Cf. l'article 31, point 7, article 73, § 1, article 248, § 1, article 280 du Projet & Article 4, § 2, troisième alinéa de la LAPD.

et ce pour les traitements de ces quatre services qui relèvent du Titre 2 et/ou de la Section 2 du Chapitre IV du Titre 1 du Projet. Pour les trois premiers services cités, on y ajoute encore les traitements qui relèvent du RGPD et des lois d'exécution du RGPD. Pour les traitements qui relèvent du RGPD et qui sont réalisés par l'Unité d'information des passagers, ce n'est donc pas le C.O.C. mais l'APD qui est compétente.

- le Comité R[116] devient la DPA pour :
  - les services de renseignement et de sécurité, pour autant qu'il s'agisse de traitements relevant du Sous-titre 1 du Titre 3 du Projet ;
  - les traitements de données à caractère personnel dans le cadre d'habilitations, d'attestations et d'avis de sécurité (visés dans la loi du 11 décembre 1998) par cinq instances/personnes énoncées à l'article 109 du Projet ;
  - l'Unité d'information des passagers, pour autant qu'il s'agisse de traitements relevant du Sous-titre 5 du Titre 3 du Projet.
- le Comité P devient, avec le Comité R, la DPA pour l'OCAM[117], pour autant qu'il s'agisse de traitements de l'OCAM relevant du Sous-titre 4 du Titre 3 du Projet (et ce alors que – comme indiqué ci-dessus – le Comité P lui-même relève partiellement du contrôle du C.O.C.).
- l'APD[118] est la DPA pour tous les autres traitements de données qui ne relèvent pas de la compétence du C.O.C. ou du Comité R ou du Comité P (l'APD reçoit donc *de facto* une compétence résiduaire).

451. La Commission estime que cette répartition de compétences est particulièrement complexe et n'est en outre pas basée sur des critères logiques/objectifs[119]. Le règlement afférent à l'OCAM et à l'Unité d'information des passagers en constitue ici une belle illustration.

---

[116] Cf. article 97, article 109, article 130, § 1, et article 186 du Projet.

[117] Cf. article 163 du Projet.

[118] Cf. article 4 de la LAPD.

[119] On utilise même parfois à cet égard des arguments pour attribuer certaines compétences à un organe, alors que ces mêmes arguments sont ignorés précisément pour ne pas attribuer d'autres compétences à ce même organe. Pour les services de police, le C.O.C est par exemple compétent pour les traitements relevant de la Directive de même que pour les traitements relevant du RGPD et des lois d'exécution du RGPD. À la p. 129 de l'Exposé des motifs, ceci est motivé comme suit : "(…) *rendre le C.O.C. également compétent en tant que APD entre autres par souci de simplicité et d'efficacité vis-à-vis des services de police. Ainsi, on évite que ces derniers risquent d'être confrontés à deux autorités de contrôle* (…)". Toutefois l'argument selon lequel il est préférable qu'une instance relève d'une seule DPA pourrait tout aussi bien être utilisé pour d'autres instances relevant du contrôle du C.O.C. (comme l'Unité d'information des passagers), mais cet argument ne s'applique apparemment pas à celles-ci.

Le Comité R et le Comité P[120] sont en effet déclarés conjointement compétents pour être la DPA de l'OCAM et ce uniquement pour les traitements de l'OCAM relevant du Sous-titre 4 du Titre 3 du Projet[121]. Pour d'autres traitements (par exemple les traitements dans le cadre de la politique du personnel) de l'OCAM, c'est l'APD qui est compétente[122]. Pour l'Unité d'information des passagers aussi, on compte potentiellement trois DPA.

452. **Quoi qu'il en soit, nul besoin d'argumenter beaucoup sur le fait que le règlement des compétences entre les quatre DPA est complexe et donnera lieu à des discussions entre les DPA. La Commission insiste dès lors fortement pour que le Projet soit entièrement revu sur ce point.**

453. La Commission constate par ailleurs que les auteurs du Projet comprennent aussi manifestement qu'un tel règlement donnera inévitablement lieu à des discussions, étant donné que des tentatives sont entreprises – comme la conclusion d'accords entre les différentes DPA[123] – afin de parvenir à des solutions opérationnelles. L'article 281 du Projet comporte par exemple aussi le règlement suivant : en vue d'une application conséquente de la réglementation en matière de protection des données, les quatre DPA sont invitées à collaborer lorsque des dossiers se chevauchent et il est demandé de prévoir un "principe du guichet unique". La Commission ne croit pas que de telles mesures constitueront en soi une solution sérieuse et elle répète son plaidoyer pour que l'on prévoie en premier lieu un règlement légal clair des compétences, en particulier pour l'Unité d'information des passagers et pour l'OCAM. Une part importante de la solution pourrait d'ailleurs consister à réduire le nombre de DPA (voir également ci-après, point E). Une réduction à trois DPA pourrait déjà être réalisée simplement en déchargeant le Comité P de son rôle de DPA qui n'est que restreint (uniquement pour l'OCAM). La fonction de DPA pour l'OCAM pourrait en effet être exercée conjointement par le Comité R et par le C.O.C[124].

454. En ordre subsidiaire, la Commission insiste également pour que le Projet cite chaque fois nominativement la DPA compétente et que l'on évite d'utiliser l'expression générale

---

[120] Et ce alors que le Service d'Enquêtes du Comité P relève lui-même du C.O.C.

[121] Article 163 du Projet.

[122] Article 280 du Projet.

[123] Voir par exemple en haut de la p. 107 de l'Exposé des motifs : "(…) *Des accords devront être établit* (sic) *entre les différentes autorités de contrôle si le dossier est introduit par plusieurs autorités de contrôle compétentes* (…)".

[124] À l'heure actuelle, ces deux institutions veillent en effet déjà au contrôle des banques de données communes terrorisme et extrémisme pouvant mener au terrorisme – dont l'OCAM est le gestionnaire – un premier contrôle ayant récemment été clôturé.

"autorité de contrôle" (dont on donne aussi une définition vague[125]). À titre d'illustration, on peut se référer à l'article 107.8 du Projet, où les traitements de données à caractère personnel par les forces armées sont soumis à l' "autorité de contrôle". On vise probablement ici l'APD, mais pour le savoir, il faut analyser au moins l'article 31, l'article 73, § 1, l'article 97, l'article 109, l'article 130, § 1, l'article 163 et l'article 248, § 1 du Projet, ce qui ne peut évidemment pas être le but.

C. *La conformité avec les exigences d'une DPA dans la réglementation européenne & la cohérence avec la LAPD*

a. Le C.O.C

455. La Commission constate que la manière dont la réforme du C.O.C. est élaborée dans le Projet comporte des éléments positifs :

- Un choix clair est enfin opéré (cf. le point A ci-dessus) : le C.O.C devient une DPA ;
- Ces dernières années, une certaine expertise en matière de protection des données a été acquise au sein du C.O.C. et en ce sens, le choix de faire du C.O.C. une DPA à part entière constitue aussi une nouvelle étape logique dans le processus de réforme qui est déjà en cours depuis 2014 ;
- Un secrétariat propre est constitué, mettant fin à la situation actuelle qui est illogique/peu efficace où le C.O.C. recourt en partie au secrétariat de la Commission[126] [127] ;
- L'indépendance est renforcée, étant donné que les membres provenant de la police sont placés sous l'autorité des autres membres et que ces membres constituent aussi seulement une minorité (2/6) du nombre total de membres.

456. **Parallèlement, la Commission constate encore aussi de nombreux hiatus/problèmes/éléments illogiques dans la réforme envisagée (et ce en sus de la répartition de compétences problématique abordée ci-avant) :**

- Le C.O.C. doit – spécifiquement à l'égard de la police – non seulement veiller au respect de la Directive, mais aussi au respect du RGPD[128]. Cela implique deux choses importantes dont on ne tient pas compte dans le Projet :

[125] Voir par exemple l'article 31, point 15 & l'article 108 *in fine* du Projet.

[126] Voir les points 11 et 12 de l'avis n° 30/2015.

[127] Cela concorde d'ailleurs aussi avec l'article 52.5 du RGPD.

[128] Article 4, § 2, troisième alinéa de la LAPD.

- Conformément aux articles 57 et 58 du RGPD, une DPA doit pouvoir exercer toutes les tâches et compétences qui sont énoncées dans ces deux articles, ce qui n'est pas le cas pour le C.O.C. Les tâches et compétences suivantes n'ont par exemple pas été prévues dans le Projet[129] :
  - Établir obligatoirement une liste des traitements pour lesquels une analyse d'impact relative à la protection des données est requise ;
  - Favoriser, recommander et approuver des codes de conduite ;
  - Favoriser des mécanismes de certification ;
  - Établir et publier des critères pour l'accréditation d'organes de contrôle en matière de codes de conduite ;
  - Vérifier des certifications délivrées ;
  - Les mesures correctrices telles que visées à l'article 58.2. du RGPD.

  La Commission fait remarquer que rien qu'en raison de ces lourdes exigences du RGPD, il est absurde de déclarer le C.O.C. compétent pour les traitements de données relevant du RGPD. Ce type de traitements (il s'agit par exemple de la gestion RH des services de police) ne constitue en effet qu'une fraction de tous les traitements de la police. Les traitements opérationnels des services de police par exemple relèvent tous de la Directive et pour ces traitements, il est par contre bel et bien logique que le C.O.C. devienne le contrôleur compétent (à cet égard, voir aussi le point E ci-après).
  Mais si l'article 4, § 2, troisième alinéa de la LAPD, l'article 73, § 1, point 2, et l'article 280 du Projet restent inchangés, le C.O.C. devra alors pouvoir exercer toutes les tâches et compétences énoncées aux articles 57 et 58 du RGPD. Idéalement, ces tâches et compétences devraient également être reprises dans le texte du Projet (comme c'est le cas pour l'APD dans la LAPD).
- L'article 51.3. du RGPD prescrit que – lorsqu'un État membre institue plusieurs DPA – le législateur national doit désigner quelle DPA siège au Comité européen de la protection des données. Le Projet ne permet toutefois pas de déduire si c'est l'APD ou le C.O.C. qui siègera au sein de ce Comité. L'article 41.4. de la Directive contient d'ailleurs une disposition similaire à l'article 51.3. du RGPD, qui n'est pas non plus implémentée dans le Projet.

- La Directive prescrit en ses articles 46 et 47 quelles tâches et compétences doivent être attribuées à une DPA. Pour le C.O.C., on a oublié la compétence de prendre des mesures

[129] Cf. article 57.1. k), m), n), o), p), q) du RGPD.

correctrices (article 47.2. de la Directive)[130], et sur ce plan, la Directive n'est donc pas transposée correctement en droit national ;

- La Commission prend acte du fait que le C.O.C. traitera des demandes d'accès indirect sur la base de l'article 46 du Projet et qu'il a également pour mission d'exécuter toutes les obligations internationales découlant des tâches et compétences qui lui sont confiées par le Projet[131]. La Commission se demande ce que cela implique exactement pour les demandes d'accès indirect concernant les signalements SIS II[132] (par exemple ce qu'on appelle les signalements article 24[133]). Il en va de même pour ladite évaluation Schengen. Il semble logique que le C.O.C. soit compétent à cet égard et la Commission recommande de régler ces aspects dans le Projet.

- La Commission émet de sérieuses réserves quant à certaines conditions auxquelles quelques membres du C.O.C. doivent répondre :
    - Ni le RGPD, ni la Directive n'imposent la condition selon laquelle les membres d'une DPA doivent être magistrats. Le Projet impose toutefois quand même cette exigence pour deux membres (dont le président) du C.O.C.[134]. Dans le cadre de la présente réforme, cette exigence est quelque peu assouplie en ce qui concerne le président du C.O.C., étant donné que pour cette fonction, on ne fat plus de distinction entre la magistrature assise et debout, et ce "afin d'augmenter le nombre potentiel de candidats pour la fonction"[135]. La Commission considère que ce raisonnement devrait aller encore plus loin : afin d'accroître encore le nombre de candidats potentiels, ces deux fonctions pourraient tout à fait être accessibles à des non-magistrats.

      En résumé, les règles européennes prévoient deux grandes conditions pour les membres d'une DPA : les connaissances en matière de protection des données et l'indépendance. Pour ce qui est de l'expertise en matière de protection des données, on peut faire remarquer qu'il s'agit d'un domaine qui ne fait pas l'objet d'une attention particulière dans la formation de magistrat et il n'y a dès lors pas d'argument objectif de penser que dans ce domaine,

---

[130] À l'article 279 du Projet, ces compétences semblent toutefois bel et bien être confiées au Comité R.

[131] Article 255 du Projet.

[132] Cf. Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 *sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) ;*

[133] Cet article contient les conditions pour les signalements en vue du refus d'accès ou de séjour.

[134] Article 243, § 1.

[135] P. 251 de l'Exposé des motifs.

des magistrats auraient une plus grande expertise que des personnes qui ne relèvent pas de ce statut. Le fait même que les règles européennes insistent sur l'indépendance des membres d'une DPA ne justifie pas non plus que ces fonctions ne puissent être exercées que par des magistrats. Un expert en protection des données peut exercer la fonction de membre d'une DPA en toute indépendance, qu'il ait ou non le statut de magistrat. La supposition qu'un magistrat offrirait davantage de garanties en termes d'indépendance n'est quoi qu'il en soit pas prépondérante par rapport au fait que ce critère réduit fortement le nombre de candidats potentiels et que cette réduction risque de facto de mettre trop sous pression l'autre critère essentiel, à savoir l'expertise en matière de protection des données.

L'argument selon lequel les membres du C.O.C. disposeraient de compétences quasi juridictionnelles[136] ne convainc d'ailleurs pas non plus la Commission. Les tâches des membres du C.O.C. ne sont en effet pas fortement différentes de celles des membres de l'APD et pour ces derniers, l'exigence d'être magistrat ne s'applique pas.

C'est pourquoi la Commission estime que l'accès aux fonctions de membre d'une DPA ne devrait pas être limité aux magistrats. Ce critère restreint inutilement le groupe des candidats potentiels et implique le risque que ce ne soient pas les experts en protection des données les plus appropriés et les plus indépendants qui accèdent à cette fonction.

- La Commission constate que le C.O.C. réformé accomplira également des tâches qui ne sont pas des tâches de DPA mais qui ont plutôt trait à l'efficacité/effectivité de traitements de données. À cet égard, elle prévient des risques que cela implique : la solution la plus efficace/effective pour un traitement de données n'est pas nécessairement celle qui protège le plus la vie privée et le C.O.C. devra donc toujours tenter de dégager des solutions équilibrées dans lesquelles la protection des données occupe une place centrale. En parallèle, la Commission souligne également qu'à l'article 259 du Projet – qui traite de la désignation de membres du personnel chargés de la gestion du RGPD – on confie au C.O.C. des tâches qui devraient incomber en essence à un responsable du traitement et à son délégué à la protection des données et non à une DPA.
- Le nombre de mandats à temps plein au C.O.C. et à son Service d'enquête est certes réduit, passant de huit à six membres, mais il s'agit quand même encore d'un mandat à temps plein de plus qu'à l'APD. De l'avis de la Commission, il est illogique que le C.O.C. compte plus de mandataires à temps plein que l'APD, étant donné que l'ensemble des missions du

[136] P. 251 de l'Exposé des motifs.

C.O.C. ne comporte qu'une fraction des missions de l'APD[137]. En outre, le nombre de fonctions à mandat (six) dans cette structure est supérieur au nombre de collaborateurs de secrétariat (trois).

- Dans le Projet, le statut des membres du C.O.C. est logiquement aligné sur celui de l'APD[138], étant donné que le rôle des deux instances sera fortement similaire. Cet alignement n'est toutefois que partiel (le trilinguisme fonctionnel n'est par exemple pas prévu pour les membres du C.O.C.). La Commission recommande donc d'aligner au maximum le statut sur celui de l'APD, dans tous ses aspects.

b. Le Comité P et le Comité R

457. La Commission constate que le Comité P et le Comité R sont transformés en DPA[139]. Sans préjudice des objections fondamentales exposées au point B concernant la répartition de compétences complexe entre toutes les DPA belges (voir en particulier le point 454), la Commission a à cet égard un peu moins de remarques de fond que pour le C.O.C., ce qui est notamment dû au fait que le rôle de contrôle des deux Comités – sur la base du texte actuel du Projet – est indépendant du RGPD et de la Directive et que la Convention n° 108 ne constitue donc que la seule pierre de touche. Le présent point de vue peut donc changer s'il était décidé ultérieurement de confier à ces organes un rôle de contrôle portant sur des traitements de données relevant de la Directive ou du RGPD.

458. La Commission constate qu'à l'heure actuelle, les deux Comités disposent déjà de compétences correspondant à celles d'une DPA (par exemple des compétences d'enquête, une compétence d'émettre des avis sur des projets de réglementation[140]). Le Projet y ajoute plusieurs tâches typiques d'une DPA, comme le traitement de demandes d'accès indirect[141] et d'autres "*requêtes*" [142]. L'expertise en matière de protection des données devient également une exigence pour pouvoir être désigné en tant que membre des Comités P & R[143].

---

[137] Le fait de créer une subdivision entre les membres du C.O.C. et les membres du Service d'enquête au sein du C.O.C. ne porte d'ailleurs pas préjudice au fait qu'il s'agit au total de six mandats à temps plein.

[138] On mettra ainsi fin à juste titre à l'actuelle situation statutaire incohérente des membres (voir la p. 257 de l'Exposé des motifs ainsi que l'avis n° 30/2015).

[139] Cf. supra, point B.

[140] Articles 9 & 33 de la loi organique du 18 juillet 1991 *du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.*

[141] Cf. Articles 83 & 149 du Projet.

[142] Article 271, deuxième alinéa du Projet. La Commission recommande de remplacer le terme vague "requêtes" par des termes plus explicites tels que "demandes d'informations".

[143] Article 266.2 du Projet.

459. Par ailleurs, la Commission attire l'attention sur le fait que la compétence du Comité R à l'article 130, § 1, premier alinéa du Projet peut potentiellement être interprétée de manière particulièrement large. Le Comité R devrait en effet se charger *"(…) du contrôle du traitement des données à caractère personnel effectué par les autorités et personnes visées à l'article 109, alinéa premier".* L'article 109, premier alinéa du Projet énumère les autorités impliquées dans l'attribution/le retrait d'habilitations, attestations et avis de sécurité comme visé dans la loi du 11 décembre 1998[144]. Ces autorités effectuent en outre d'autres traitements de données et pour éviter que le Comité R soit également considéré comme DPA compétente pour ces traitements, on peut envisager de formuler l'article 130, § 1, premier alinéa du Projet comme suit : *"(…) du contrôle du traitement des données à caractère personnel dans le cadre de l'article 109, alinéa premier, effectué par les autorités et personnes visées dans ce même article".*

D. Conclusion : avis défavorable

Vu les problèmes énoncés ci-dessus, la Commission émet un avis **défavorable** quant aux dispositions du Projet concernant les trois nouvelles DPA[145], étant donné que :

- la répartition de compétences entre les 4 DPA fédérales est régie de manière chaotique et tout à fait illogique (cf. supra, point B) ;
- la réforme du C.O.C. ne va pas assez loin et n'est, en certains points, pas conforme aux règles européennes (cf. supra, point C.a. et infra, point E).

460. Au point E ci-dessous, la Commission avance deux pistes alternatives afin de parvenir quand même à la création en Belgique d'un paysage de protection des données logique et organisé de manière efficace.

E. Propositions de solution

461. Comme évoqué ci-avant, la Commission n'opère évidement aucun choix stratégique, mais elle estime qu'il est de son devoir de conseiller au mieux le demandeur sur les avantages et inconvénients liés à certaines options stratégiques. Après analyse des dispositions du Projet relatives à la réforme du C.O.C, du Comité P & du Comité R, et de la répartition de

[144] Loi du 11 décembre 1998 *relative à la classification et aux habilitations, attestations et avis de sécurité.*

[145] Voir principalement les articles 73, 97 à 100 inclus, 107.8, 130 à 133 inclus, 163, 186 & Titre 7 & Titre 8 du Projet.

compétences entre les quatre DPA, elle s'inquiète fortement – comme évoqué ci-dessus – de l'opérationnalité de ce règlement proposé et de sa conformité avec les normes juridiques européennes. Étant donné que le Projet constitue la plus grande réforme du paysage de la protection de la vie privée depuis des années (qui devrait en outre être un fait d'ici le 25 mai 2018) et vu que son successeur en droit – à savoir l'APD – jouera un rôle central dans ce paysage, elle prend la liberté de proposer deux solutions alternatives.

462. La première proposition de la Commission est d'emblée la plus simple et la plus efficace. Il s'agit également de la solution qui a été privilégiée dans quasiment tous les autres pays européens. On pourrait en effet choisir de ne pas créer de DPA supplémentaires et d'octroyer ainsi à l'APD la plénitude des compétences. On éviterait ainsi totalement les problèmes précités. Cette proposition présenterait aussi l'avantage que les tâches de contrôle – et donc aussi l'expertise – en matière de protection des données seraient centralisées au sein d'une seule organisation. Dans cette hypothèse, il faudrait toutefois encore trouver une solution appropriée pour le C.O.C. existant qui, comme indiqué plus haut, est quoi qu'il en soit pris dans un étau entre les tâches et compétences de la Commission et celles du Comité P.

463. La Commission voit également une deuxième solution possible, qui peut également être opérationnelle selon elle, à condition de bien la mettre en œuvre : ne confier à l'APD que le contrôle des traitements relevant du RGPD (et des dispositions d'exécution nationales du RGPD) et créer une deuxième DPA compétente pour tous les autres traitements de données, à savoir (principalement) les traitements visés à l'article 2, deuxième alinéa, et aux Titres 2 & 3 du Projet, à l'exception des traitements auprès des autorités judiciaires. On respecte ainsi la logique européenne (subdivision RGPD - Directive), l'expertise est centralisée de manière plus logique/efficace qu'à l'heure actuelle dans le Projet, on ne doit pas non plus nécessairement toucher à la réglementation s'appliquant aux Comités P & R, et les discussions relatives aux compétences entre les DPA belges peuvent être réduites à un minimum[146].

464. Cette dernière proposition présenterait également l'avantage de dégager simultanément une solution pour le C.O.C. Le C.O.C. a en effet acquis une place dans le paysage institutionnel national et s'est construit une certaine expertise en matière de protection des données. Mais il lui manque aujourd'hui un ensemble de tâches homogène/logique, vu le chevauchement de compétences avec le Comité P et la Commission (future APD). Après une réforme encore plus approfondie que celle proposée dans le Projet[147],

[146] Dans cette constellation, des problèmes de compétence surviendront encore bel et bien, mais leur ampleur sera bien plus limitée que dans l'embrouillamini créé par le texte actuel du Projet.

[147] Comme ce fut d'ailleurs le cas pour la Commission dans la LAPD.

le C.O.C. pourrait assurer la tâche de la deuxième DPA belge. D'après la Commission, cette réforme du C.O.C. pourrait être réalisée en :

- prenant comme point de départ l'article 73 et le Titre 7 du Projet, et
- en réévaluant les compétences du C.O.C – ce qui implique tant un élargissement qu'une petite limitation de ses compétences prévues[148] – pour tous les traitements visés à l'article 2, deuxième alinéa et aux Titres 2 & 3 du Projet, à l'exception des traitements auprès des autorités judiciaires, et
- en implémentant les remarques formulées ci-dessus au point C.a., et
- en veillant à ce que cette DPA dispose de l'expertise utile pour pouvoir contrôler aussi les traitements de données par les services de renseignement (et par des services publics plus réguliers, comme les Douanes[149]).

465. La Commission est d'ailleurs convaincue qu'il s'agit là des deux seules pistes valables pour parvenir en Belgique à un paysage de protection des données logique et organisé de manière efficace. Tous les autres scénarios – comme par exemple le règlement prévu dans le Projet – mèneront inéluctablement à :

a. Des problèmes de compétence ;
b. un éclatement de l'expertise ;
c. un traitement de dossiers complexe ;
d. des divergences de jurisprudence.

CONCLUSION de la Commission au sujet du Titre 7 du projet

466. La Commission émet un avis défavorable quant aux dispositions du projet portant sur les trois nouvelles DPA en raison des motifs évoqués ci-avant et en particulier eu égard au fait que :

- la répartition de compétences entre les 4 DPA fédérales a été régie de manière chaotique et tout à fait illogique ;

[148] La seule limitation des compétences du C.O.C. concerne la suppression de l'article 4, § 2, troisième alinéa de la LAPD et des articles 73, § 1, point 2, et 280 du Projet, étant donné que le C.O.C. a reçu des compétences liées au RGPD, et ce uniquement pour quatre instances. Cette compétence devrait être supprimée et ces services devraient – uniquement en ce qui concerne les traitements relevant du RGPD (par exemple pour le traitement RH, ce qui ne constitue qu'une fraction de tous les traitements de données par ces services) – relever pour ce volet du contrôle de l'APD (cf. supra, point C.a.).

[149] Cf. article 31, point 7, point e) du Projet.

- la réforme du C.O.C. ne va pas assez loin et n'est, en certains points, pas conforme aux règles européennes.

La Commission invite le demandeur à considérer sérieusement les deux pistes alternatives qu'elle a avancées afin de parvenir quand même à un dispositif de protection des données logique et organisé efficacement en Belgique.

11. CONCLUSION

PAR CES MOTIFS,

la Commission rend un avis conforme aux conclusions finales distinctes qu'elle a formulées pour chacun des titres du présent projet. Elle émet donc :

- au sujet du titre préliminaire du projet, un avis **défavorable** pour les motifs exposés au point 87 ;
- au sujet du titre 1 du projet, un avis **défavorable** pour le chapitre trois et un avis **favorable** pour les autres chapitres, à condition que les remarques mentionnées au point 192 soient reprises dans leur intégralité ;
- au sujet du titre 2 du projet, un avis **défavorable** pour la délimitation du champ d'application et un avis **favorable** pour les autres dispositions, à condition que les remarques formulées au point 226 soient reprises dans leur intégralité ;
- au sujet du titre 3 du projet, un avis **défavorable** pour les articles 78 et 112 du projet et un avis **favorable** pour les autres dispositions, à condition que les remarques formulées aux points 242 et 254 soient reprises dans leur intégralité ;
- au sujet du titre 4, un avis **défavorable** sur toute la ligne (voir le point 389) ;
- au sujet du titre 5, un avis **défavorable** au sujet des lacunes en cas de risque de violation grave ainsi qu'au sujet de la compétence administrative pour la décision d'agir en droit et un avis **favorable** pour les autres dispositions, à condition que les remarques formulées au point 414 soient reprises dans leur intégralité ;
- au sujet du titre 6, un avis **défavorable** sur toute la ligne (voir le point 445) ;
- au sujet du titre 7, un avis **défavorable** sur toute la ligne (voir le point 466).

Vu le caractère essentiellement défavorable de son avis, la Commission répète qu'elle se tient à la disposition du demandeur pour corriger ce projet en profondeur afin d'élaborer une loi-cadre qui respecte la *ratio legis* du RGPD et de la Directive et qui contribue à un régime transparent, cohérent et efficace pour la protection de la vie privée en Belgique.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere