Orde van Vlaamse Balies

www.advocaat.be

Staatsbladsstraat 8
B – 1000 Brussel
T +32 (0)2 227 54 70
F +32 (0)2 227 54 79
info@advocaat.be
ondernemingsnummer 0267.393.267

NOTA

Veilig thuiswerken tijdens corona: videoconferenties en de AVG

8 april 2020

Auteur: Anke Verpoorte

1) Inleiding

Digitale communicatie is in deze tijd meer dan ooit noodzakelijk: videoconferenties met cliënten, online vergaderingen met de Algemene Vergadering, bestanden opslagen in de cloud, VPN-verbindingen vanop afstand, enz.

De Orde van Vlaamse Balies adviseert u de **nodige voorzorgsmaatregelen** te nemen als u en uw personeelsleden grotendeels thuis gaan werken vanwege COVID-19. Het is dan belangrijk om aandacht te hebben voor onderstaande punten en eventueel aanvullende maatregelen te treffen.

Aangezien veel advocaten nood hebben aan aanbeveling betreffende het organiseren van videoconferenties met hun cliënten, zullen onze aandachtspunten voornamelijk hierop gericht zijn.

In een digitale omgeving gesprekken voeren met uw cliënt brengt veel nieuwe uitdagingen met zich mee, waaronder het **veilig communiceren en delen van persoonsgegevens**.

Het toenemende gebruik en de waarde van persoonlijke informatie, het delen van persoonlijke informatie tussen diensten en de toenemende complexiteit van ICT-systemen kunnen het voor een advocatenkantoor moeilijk maken om gegevensbescherming te waarborgen en de naleving van de verschillende toepasselijke wetten (waaronder hoofdzakelijk de Algemene Verordening Gegevensbescherming) na te leven.

Advocaten zijn om verschillende redenen **verplicht om persoonlijke gegevens te beschermen**: om te voldoen aan wettelijke en reglementaire vereisten, om bedrijfsverantwoordelijkheid uit te oefenen, om boetes te vermijden, om het vertrouwen van de client te vergroten, om reputatie- en imagoschade te vermijden maar ook om een intern overzicht te hebben waar persoonlijke gegevens worden opgeslagen en aan wie ze worden doorgegeven. Op deze manier kan men proactief handelen en vermijden dat er persoonsgegevens verloren gaan of de schade minimaliseren als er een datalek zou voorvallen.

Bij de term '**persoonsgegevens**' wordt er vaak enkel gedacht aan de klassieke persoonsgegevens zoals naam, e-mailadres en adresgegevens, maar ook digitale of technische gegevens zoals

gebruikersnamen, netwerkadressen, IP-adressen, sociale media accounts en zelfs tweets die gelinkt kunnen worden aan een individuele natuurlijke persoon worden beschouwd als persoonsgegevens volgens de AVG. Als u dus een videoconferentie wil starten met uw client, dient u zich ervan bewust te zijn dat de aanbieder niet enkel zal beschikken over uw persoonsgegevens, maar ook die van uw cliënt aangezien zijn of haar IP-adres altijd beschikbaar zal zijn. Het is dus aan te raden om dit duidelijk in uw privacy policy op te nemen en op voorhand aan uw cliënt mee te delen.

Advocaten dienen te worden gestimuleerd om in het vroegste stadium van de verwerkingsactiviteiten technische en organisatorische maatregelen te treffen die nodig zijn om de beginselen inzake gegevensbescherming vanaf het begin te waarborgen. Standaard moeten advocaten ervoor zorgen dat persoonsgegevens worden verwerkt met het hoogste niveau van bescherming als het gaat om de opslag of het delen van gevoelige gesprekken met hun cliënt.

Hoewel dit document de meest courante problemen in verband met digitale communicatie behandelt, mogen de hier geïdentificeerde risico's niet als volledig worden beschouwd. Dit document omvat slechts een summiere samenvatting van vereisten om te voldoen aan gegevensbescherming zoals vooropgesteld door de AVG. Dit document geeft geen interpretatie weer van de AVG maar biedt enkel praktische beveiligingsmaatregelen aan om gegevensbescherming te garanderen. De principes van de AVG die niet aan bod zijn gekomen, blijven uiteraard ook van toepassing net zoals alle andere wetten, regelgevingen en globale beveiligingsmaatregelen die van toepassing zijn tijdens de uitoefening van uw beroep.

2) Correct omgaan met persoonlijke gegevens in een digitale omgeving

Eerst en vooral dient te worden benadrukt dat elk advocatenkantoor verschillend is en dus ook de technische en organisatorische maatregelen per kantoor zullen variëren. Documenteer op voorhand welke digitale tools voor uw kantoor noodzakelijk zijn en voeg hierbij passende en met het risico evenredige technische en organisatorische maatregelen toe. **Hoe meer gevoelige gegevens u verwerkt, hoe meer maatregelen u dient te nemen om deze gegevens optimaal te beveiligen.** Als u bijvoorbeeld een online vergadering wil organiseren met uw medewerkers om de weekplanning te overlopen en taken te verdelen, zullen de technische en organisatorische maatregelen op een lagere schaal dienen te worden toegepast dan wanneer u een videoconferentie wil organiseren met uw cliënt waarbij u inhoudelijke en gevoelige materies bespreekt in verband met een procesvoering. **De keuze voor een applicatie of tool is dus afhankelijk van het doel van de online vergadering en welke soort (persoons)gegevens er worden gedeeld tijdens die vergadering.**

Onderzoek per applicatie of tool wat de gebruikersvoorwaarden, beveiligingsmaatregelen en functionaliteiten zijn. Beoordeel of deze factoren in voldoende mate overeenkomen met het interne gegevensbeschermingsbeleid. Als dit onvoldoende is, breng in kaart wat de afwijkingen zijn en neem compenserende maatregelen.

Hieronder geven we concreet enkele tips en aandachtspunten mee die u helpen om de juiste beoordeling te kunnen maken bij uw keuze rond een online tool of applicatie voor videoconferenties.

De beveiliging van netwerk- en informatiesystemen

Werk uitsluitend in een beveiligde thuiswerkomgeving, als dat mogelijk is. Dus log thuis in op de server van uw organisatie en gebruik liefst geen onbekende wifiverbinding. Gebruik hiervoor als dat mogelijk is apparatuur dat uw kantoor u heeft verschaft en gebruik zo min mogelijk een persoonlijke lap top of tablet, tenzij dit uitdrukkelijk wordt toegelaten en uw kantoor werkt met een bring your own device policy.

De technische en organisatorische maatregelen moeten een niveau van beveiliging van de netwerk- en informatiesystemen verzekeren dat is afgestemd op de risico's. Maak hierbij ook een **veiligheidspolicy** op voor de behandeling van incidenten indien er zich een lek voordoet zodat uw kantoor en al uw medewerkers volledig voorbereid zijn en weten welke stappen ze dienen te ondernemen en welke personen dienen te worden aangesproken.

Technische en organisatorische maatregelen om veilig aan videoconferenties te doen

Controleer of de aanbieder van videoconferenties onderstaande mogelijkheden aanbiedt en ga volgende aandachtspunten na:

- Wees voorzichtig met het gebruik van gratis tools of applicaties. Het is mogelijk dat zo'n dienst juist gratis is omdat de aanbieder uw persoonsgegevens en die van uw cliënt gebruikt voor andere doeleinden, zoals marketing of verkoop van gegevens aan derden. U bent op deze manier het beheer van uw persoonsgegevens kwijt;
- Indien mogelijk, kies bij videoconferenties voor een applicatie of een tool die een unieke ID genereert die maar voor 1 persoon te gebruiken is en kies voor een sterk meeting-paswoord zodat uw vergadering wordt afgeschermd voor derden.
- End-to-end encryptie.
- Mogelijkheid tot versleuteling van documenten;
- Two Factor Authentication;
- Hashing van wachtwoorden;
- Vermelding van ISO-normen en andere veiligheidscertificaten op website;
- Als u een videconferentie wil opnemen en opslagen, verkies dan de opslag op de eigen server in plaats van op een publieke cloud;
- Controleer of ook effectief aan bovenstaande beveiligingseisen wordt voldaan, bijvoorbeeld via de quickscan maar wees ook waakzaam over het feit dat er bepaalde zaken over het hoofd kunnen worden gezien en dat u of uw IT-expert op regelmatige basis ook zelf dienen te controleren dat er voldoende veiligheid en bescherming wordt geboden.

Controleer ook de AVG-compliancy

Ga na op de website of via de privacy policy of de beheerder van een digitale dienst voldoende garanties kan bieden met betrekking tot de AVG. Kies indien mogelijk voor een applicatie of tool waarbij het datacentrum in de Europese Unie ligt en dus de gegevens worden opgeslagen binnen Europa.

Als (een deel van) de opslag of andere verwerking van persoonsgegevens door de aanbieder toch buiten de EER plaatsvindt, controleer dan of er een adequaatsheidsbesluit is genomen door de Europese Commissie, of (bij Amerikaanse partijen) of er een Privacyshield certificaat is. Verifieer het certificaat op https://www.privacyshield.gov/list.

U kan bij een applicatie of tool nagaan of er privacyvriendelijke instellingen aanwezig zijn die u zelf kan aanpassen, zoals de keuze om persoonsgegevens alleen op te slaan in de EU of een optie om een adresboek van de organisatie niet te uploaden naar de cloud. Zorg ervoor dat de omgang met en inrichting van de tool zoveel mogelijk privacyvriendelijk gebeurt: zet (attention)trackingfuncties uit en neem het gesprek niet op indien dit niet noodzakelijk is. Het is bijvoorbeeld vaak ook mogelijk dat u in uw instellingen kan aangeven dat niet elke deelnemer de chatgesprekken kan downloaden. Zet ook de functie "Auto saving chats uit", tenzij u de chat wil opslagen voor bijvoorbeeld het uitwerken van uw notulen maar dan dient u hiervoor eerst de cliënt van op de hoogte te brengen.

Indien je bepaalde functionaliteiten toch wil inschakelen, zoals het opnemen van de meeting, opslaan van de chat of "Attention Tracking" wil gebruiken, **zal u de cliënt hierover voorafgaandelijk dienen te informeren en de toestemming te vragen.** De host (of de organisator van een videoconferentie) wordt meestal aanzien als de Verwerkingsverantwoordelijke en is gehouden aan deze verplichtingen te voldoen.

Sluit met de beheerder een verwerkersovereenkomst af waarin de verplichtingen worden vastgelegd met betrekking tot de correcte naleving van de AVG. Een aanbieder van videoconferenties zal meestal als een verwerker worden beschouwd. **Een advocaat die zich registreert bij de beheerder en een online vergadering wil opstarten is de verwerkingsverantwoordelijke en draagt dus ook de eindverantwoordelijkheid bij de verwerking van persoonsgegevens.** Deze dient aan te tonen dat zijn verwerkers voldoende garanties hebben aangeboden om de naleving van de AVG te verzekeren.

De menselijke factor

Deze aanbeveling gaat voornamelijk in op technische en juridische maatregelen, maar een menselijke tekortkoming is echter ook vaak de oorzaak van beveiligingslekken. Zeker in deze periode van thuiswerken is videoconferenties een vaak gebruikt hulpmiddel. Geef hiervoor duidelijke richtlijnen mee aan de cliënt zoals bijvoorbeeld dat hij, indien mogelijk, in een afgesloten ruimte een gesprek via videoconferentie voert. Verifieer ook altijd eerst de identiteit van uw cliënt via een verificatieprocedure zodat u zeker bent dat u geen persoonsgegevens uitwisselt met een onbevoegde persoon. Breng uw cliënt op de hoogte van de privacyrisico's tijdens het bespreken van persoonsgegevens via videoconferenties.

Het is aan te raden om dit via een privacy policy te plaatsen en duidelijk op uw website mee te delen of op voorhand aan uw cliënt te overhandigen. Vraag indien nodig de voorafgaandelijke toestemming aan uw cliënt, bijvoorbeeld als u een gesprek wil opslagen om later opnieuw te bekijken.

Besef ook steeds wat voor informatie u wil delen met uw cliënt. **Gevoelige persoonsgegevens kunnen best niet via gratis digitale tools worden gedeeld, omdat in het merendeel van de gevallen betalende versies van applicaties en tools meer veiligheidsnormen en beveiligingsmaatregelen aanbieden.**

Maak ten slotte ook al uw confraters en medewerkers bewust van deze aandachtspunten als u een tool gebruikt voor een online omgeving. Creëer een bewustwording zodat enkele evidente zaken worden nagegaan: controleer of er niemand meeluistert tijdens een videoconferenties, ga na of uw applicatie of tool geschikt is om gevoelige persoonsgegevens mee te delen en sluit de

videoconferentie volledig af na afronding van het gesprek. Als de host een vergadering verlaat, zou het kunnen voorkomen dat het scherm, camera en audio gedeeld blijven worden met de deelnemers. Bij sommige applicaties of tools heb je dan bijvoorbeeld de mogelijk om volgende functionaliteit aan te zetten: "*stop my video and audio when my display is off or screen saver begins*" dan zal de sessie automatisch worden gestopt als de laptop wordt toegedaan of in slaapstand gaat.

Het is aan te raden om bovenvermelde zaken aan uw kantoorgenoten bewust te maken via een **interne company policy, of een veiligheidsbeleid.**