



## Problematiek bij het versturen van procedurestukken via e-mail in plaats van met DPA-/e-Deposit

De dwingende richtlijnen van het College van Hoven en Rechtbanken van 18 maart 2020 bepalen dat voortaan “alle procedurestukken (eenzijdige verzoekschriften, verzoekschriften hoger beroep, dag-vaardingen, enz.) uitzonderlijk **per e-mail** of [DPA-/]e-Deposit mogen worden toegezonden.”

Hoewel de meeste hoven en rechtbanken vereisen dat DPA-/e-Deposit wordt gebruikt voor de neerlegging van verzoekschriften en andere procedurestukken, zijn er ook die nu toelaten dat dit per e-mail gebeurt.

Een neerlegging van procedurestukken staat echter gelijk aan een **verwerking van persoonsgegevens** onder de Algemene Verordening Gegevensbescherming (AVG). Dat moet onder meer voldoen aan het integriteits- en vertrouwelijkheidsbeginsel, zoals vervat in artikel 5, lid 1, f) AVG.<sup>1</sup>

Dat beginsel wordt concreet vertaald in artikel 32 AVG omtrent de **beveiliging** van de verwerking van persoonsgegevens:

“1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoelinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker **passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen**, die, waar passend, onder meer het volgende omvatten:

- a) de pseudonimisering en versleuteling van persoonsgegevens;
- b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

<sup>1</sup> “Persoonsgegevens moeten [...] door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid”).”

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name **rekening gehouden met de verwerkingsrisico's**, vooral **als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden**, opgeslagen of anderszins **verwerkte gegevens**, hetzij per ongeluk hetzij onrechtmatig." [...]²

**Maar e-mail is een onveilig communicatiemedium.**³ De Orde van Vlaamse Balies raadt advocaten af om van e-mail gebruik te maken voor de neerlegging van procedurestukken waarin zich (gevoelige) persoonsgegevens bevinden. Indien u toch gebruik wil maken van e-mail, weet dan dat u optreedt als een verwerkingsverantwoordelijke onder de AVG en u dus een **adequaate beveiligingsniveau** moet waarborgen. Zo nodig, dient u zich te kunnen verantwoorden bij de Gegevensbeschermingsautoriteit.

Daarom is het voor de neerlegging van procedurestukken aangeraden om DPA/-e-Deposit te gebruiken. Het KB van 16 juni 2016 houdende de elektronische communicatie overeenkomstig artikel 32ter van het Gerechtelijk Wetboek, duidt de FOD Justitie immers aan als de verwerkingsverantwoordelijke. In dat geval is het niet meer de verantwoordelijkheid van de advocaat om de oorsprong, de integriteit en de vertrouwelijkheid van de inhoud van de zending te waarborgen, maar wel die van de FOD Justitie (zie artikelen 6 en 7 van het KB van 16 juni 2016).

Voor meer informatie over de AVG-gerelateerde aspecten in verband met de online communicatie met cliënten en confraters, verwijs ik u graag door naar onze **webinar**.⁴

**Ben Claes,**  
Jurist Studiedienst OVB  
Versie 2 - 8 april 2020

---

² Mijn nadruk

³ Zie RvS 9 februari 2016, nr. 233.777, randnummers 17 en zeker 24: "Het recht op eerbiediging van het privé- en gezinsleven wordt als grondrecht gewaarborgd in artikel 22 van de Grondwet, artikel 8 van het EVRM en artikel 17 van het BUPO-verdrag. Het houdt ook het recht op geheimhouding van informatie over het privé-leven in en de vertrouwelijkheid van die informatie dient door de overheid te worden gewaarborgd. Om een kans te maken op het welslagen van zijn beroep bij de Raad voor Vreemdelingenbetwistingen, des te meer wanneer het gaat om beroepen met hervormingsbevoegdheid tegen een beslissing van de commissaris-generaal voor de vluchtelingen en de staatlozen, is de vreemdeling vaak genoodzaakt gevoelige persoonlijke informatie mee te delen in zijn verzoekschrift of synthesesamenvatting. Bij het bepalen van de elektronische wijze waarop deze processtukken moeten worden bezorgd aan de griffie van de Raad voor Vreemdelingenbetwistingen dient de regelgever hiermee rekening te houden en derhalve te kiezen voor een veilig en betrouwbaar medium. [...] Er kan worden aanvaard dat in het bestreden besluit is gekozen voor het verplichte gebruik van een elektronisch medium [e-mail] dat geen enkele garantie biedt voor de vertrouwelijkheid van de gevoerde communicatie."

⁴ <https://privaatluik.advocaat.be/beroepsuitoefening/coronavirus-justitie/digitaal-communiceren-met-uw-confraters-clienten-en-andere>.

