*Mr. dr. ing. N.J. Margetson**

De Algemene verordening gegevensbescherming[1]

De Algemene verordening gegevensbescherming (AVG) is medio mei 2016 in werking getreden en is vanaf 25 mei 2018 van toepassing. Zij zal in Nederland worden uitgevoerd door een uitvoeringswet (UAVG). Hoewel er een overgangsperiode van twee jaar is geweest vanaf de datum van inwerkingtreding van de AVG tot de dag dat zij van kracht is, voldoen veel ondernemingen nog niet aan haar eisen. Met name kleine ondernemingen en zzp'ers zullen nog maatregelen moeten nemen om (U)AVG-compliant te worden. Deze bijdrage is een bespreking van de voor verwerkingsverantwoordelijken belangrijkste bepalingen van de AVG.

1. INLEIDENDE OPMERKINGEN

Op 25 mei 2018 wordt de Wet bescherming persoonsgegevens (Wbp) vervangen door de Algemene verordening gegevensbescherming[2] (AVG) en de Uitvoeringswet AVG (UAVG). De UAVG was op het moment van schrijven van dit artikel (medio april 2018) nog in behandeling bij de Eerste Kamer.[3]

De Wbp werd ingevoerd naar aanleiding van de Europese Richtlijn 95/46/EG. Die richtlijn had tot doel de bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met verwerkingsactiviteiten te harmoniseren en het vrije verkeer van persoonsgegevens binnen de Unie te waarborgen.[4]

De AVG bevat regels betreffende de bescherming van natuurlijke personen in verband met de *verwerking van persoonsgegevens* en betreffende het vrije verkeer van persoonsgegevens (art. 1 lid 1 AVG). Onder de AVG kunnen hoge boetes worden opgelegd. De hoogste boetes zijn maximaal 4% van de wereldwijde jaaromzet of € 20 miljoen (het hoogste bedrag geldt als maximum; zie art. 83 lid 5 AVG).

In dit artikel zullen, na deze inleidende opmerkingen, een aantal belangrijke definities en bepalingen uit de AVG worden besproken, waaronder het toepassingsgebied van de AVG (par. 2, 3 en 4), de beginselen inzake de verwerking van persoonsgegevens (par. 5), de rechten van de betrokkene (par. 6), de verantwoordelijkheden van de verwerkingsverantwoordelijke en de verwerker (par. 7), de functionaris voor gegevensbescherming (par. 8) en doorgiften van persoonsgegevens naar derde landen (par. 9). In par. 10 volgen enkele afsluitende opmerkingen.

2. PERSOONSGEGEVENS

Art. 4 sub 1 AVG definieert 'persoonsgegevens' als:

'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;' (curs. NJM).

De gegevens moeten iets over een specifieke persoon zeggen. Wanneer de gegevens niet iets zeggen over een specifieke persoon, dan zijn het geen persoonsgegevens. Een persoon is geïdentificeerd wanneer deze binnen een groep te onderscheiden is.

Indentificatoren (dit woord staat niet in *Van Dale* maar de betekenis volgt uit art. 4 sub 1 AVG) zijn gegevens die worden gebruikt om de identiteit van een persoon vast te stellen. Het zijn gegevens die specifiek op die persoon van toepassing zijn. Bijvoorbeeld: naam, adres en geboortedatum. Dat zijn directe identificatietekens. In combinatie met elkaar maken dergelijke gegevens het

* **Mr. dr. ing. N.J. Margetson** (nick@margetsonlaw.nl) is advocaat te Rotterdam, onderzoeker bij het Amsterdam Centre for Insurance Studies en redacteur van dit tijdschrift.

1. Voor het schrijven van deze publicatie is gebruikgemaakt van Bart W. Schermer, Dominique Hagenauw & Nathalie Falot, *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming* van 8 januari 2018, geschreven in opdracht van het Ministerie van Justitie en Veiligheid, online te vinden op: www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming. Voorts is gebruikgemaakt van Arnoud Engelfriet, Lisette Chew-Meij & Peter Kager, *De Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar*, Amsterdam: Ius Mentis 2017 (Engelfriet, Chew-Meij & Kager 2017). Ook raadpleegde ik de overwegingen voor de verordening.
2. 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 intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming).
3. *Kamerstukken I* 2017/18, 34851, C (10 april 2018).
4. Op grond van art. 8 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en art. 10 Grondwet is het recht op 'privacy' een grondrecht.

mogelijk dat een bepaalde persoon met een grote mate van zekerheid kan worden geïdentificeerd.

Ook uiterlijke kenmerken, sociale en economische kenmerken (zoals bijv. beroep, inkomen, opleiding) en online kenmerken zoals bijvoorbeeld een IP-adres kunnen iemand identificeren als zij worden gekoppeld met andere gegevens. Dit zijn daarom indirecte identificatiegegevens. Een persoon is identificeerbaar indien zijn identiteit nog niet is vastgesteld, maar dit redelijkerwijs, zonder onevenredige inspanning, wel kan gebeuren. Dit kan bijvoorbeeld door gegevens te koppelen aan direct identificerende gegevens of doordat gegevens door hun onderlinge combinatie dusdanig uniek zijn dat ze maar op één persoon betrekking kunnen hebben. Bijvoorbeeld een telefoonnummer (een indirecte indentificator) dat via een telefoonboek is te koppelen aan een naam.

Bijzondere categorieën van persoonsgegevens

Naast gewone persoonsgegevens, onderscheidt de AVG bijzondere categorieën van persoonsgegevens (art. 9 AVG) en persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (art. 10 AVG).[5]

Op grond van art. 87 AVG kunnen de lidstaten de specifieke voorwaarden voor de verwerking van een nationaal identificatienummer of enige andere identificator van algemene aard nader vaststellen. Art. 46 lid 1 UAVG bepaalt dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts wordt gebruikt ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald.

3. VERWERKING EN TOEPASSINGSGEBIED AVG

Art. 4 sub 2 AVG definieert 'verwerking' als:

'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, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen* van gegevens;' (curs. NJM).

Deze definitie toont aan dat er snel sprake is van 'verwerking'. Reeds het opslaan van persoonsgegevens wordt aangemerkt als verwerking van persoonsgegevens. Gezien de ruime definities zal er snel sprake zijn van verwerking van persoonsgegevens. Of een dergelijke verwerking onder de AVG valt, zal afhangen van het toepassingsbereik van de AVG.

Toepassingsbereik AVG

Om te bepalen of een verwerking van persoonsgegevens onder de AVG valt, dient eerst te worden vastgesteld of deze valt binnen het materiële (art. 2 AVG) en territoriale toepassingsbereik (art. 3 AVG).

Het materiële toepassingsbereik betreft de vraag waarop de verordening van toepassing is. Art. 2 lid 1 AVG 'Materieel toepassingsgebied' luidt:

'Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.'

De verordening is dus alleen van toepassing wanneer er sprake is van een geheel of gedeeltelijk geautomatiseerde[6] verwerking van persoonsgegevens of wanneer persoonsgegevens zijn opgenomen in een bestand of daartoe bestemd zijn. Ex art. 4 sub 6 AVG is een bestand een gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn. Een voorbeeld daarvan is een archiefkast waarin gegevens door middel van een kaartenbak kunnen worden gevonden.

Dossiers of een verzameling dossiers en de omslagen ervan, die niet volgens specifieke criteria zijn gestructureerd, mogen niet onder het toepassingsgebied van de AVG vallen (overweging 15 AVG).

Art. 2 lid 2, 3 en 4 AVG bevatten uitzonderingen op het materiële toepassingsgebied. De belangrijkste uitzonderingen zijn:

- verwerking in het kader van de nationale veiligheid;
- verwerking door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;
- verwerking door de 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.

Het territoriale toepassingsbereik betreft de vraag waar de verordening van toepassing is (binnen het grondgebied van de Europese Unie en in bepaalde situaties daarbuiten). De AVG is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een verwerkingsverantwoordelijke[7] of een verwerker[8] in de Unie, ongeacht of de verwerking in de Unie plaatsvindt (art. 3 AVG). Bijvoorbeeld de verwerking van gegevens door een Amerikaans bedrijf zoals Google. Google heeft een vestiging in Nederland. Daarom is de AVG op de verwerkingen van Google van toepassing.

5. Zie par. 5.
6. Geautomatiseerde verwerking is verwerking met computers.
7. De verwerkingsverantwoordelijke is, kort gezegd, diegene die het doel en de middelen van de verwerking van persoonsgegevens vaststelt (zie hierna en art. 4 sub 7 AVG).
8. De verwerker is, kort gezegd, diegene die ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt (zie hierna en art. 4 lid 8 AVG).

De AVG is ook van toepassing op de verwerking van betrokkenen die zich in de Unie bevinden door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker wanneer de verwerking verband houdt met:
– het aanbieden van goederen of diensten aan deze betrokkenen in de Unie ongeacht of daarvoor moet worden betaald of niet;
– het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.[9]

Een voorbeeld van het monitoren van gedrag in de Unie is het monitoren van het gedrag van websitebezoekers. Ik vraag mij af hoe de toezichthoudende autoriteiten denken te kunnen handhaven tegen zulke monitorwerkzaamheden die plaatsvinden buiten de jurisdictie van de Europese Unie.
Ten slotte is de AVG ook van toepassing op de verwerking door een verwerkingsverantwoordelijke die buiten de Unie is gevestigd op een plaats waar krachtens internationaal publiekrecht het recht van een lidstaat van toepassing is.[10] Bijvoorbeeld een consulaat of een ambassade van een EU-lidstaat.

Wanneer een verwerkingsverantwoordelijke niet gevestigd is in een lidstaat van de Europese Unie, maar op grond van de bovenstaande regels wel onder het toepassingsbereik van de verordening valt, dan is deze verplicht om schriftelijk een vertegenwoordiger aan te stellen (art. 27 lid 1 AVG). De vertegenwoordiger vertegenwoordigt de verwerkingsverantwoordelijke in verband met de verplichtingen krachtens de verordening en vormt het aanspreekpunt voor de toezichthouder.

4. VERWERKINGSVERANTWOORDELIJKE EN VERWERKER

Art. 4 sub 7 AVG definieert 'verwerkingsverantwoordelijke' als:

'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; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;'.

Degene die bepaalt welke persoonsgegevens worden verzameld, voor welk doel dit gebeurt en de manier waarop dit plaatsvindt (met welke middelen), is de verwerkingsverantwoordelijke. Een entiteit die een verwerking uitvoert binnen het doel en de middelen gesteld door een verwerkingsverantwoordelijke heet een verwerker (zie art. 4 sub 8 AVG). In de praktijk zal de verwerker echter de middelen voor de verwerking al hebben (bijvoorbeeld een salarisadministratiekantoor). Dit betekent echter niet dat de verwerker daarmee verwerkingsverantwoordelijke is geworden. De verwerkingsverantwoordelijke is diegene die besluit hoever de opdracht aan de verwerker gaat.

Op grond van art. 24 AVG treft de verwerkingsverantwoordelijke de technische en organisatorische maatregelen die nodig zijn om aan te kunnen tonen dat de verwerking in overeenstemming met de AVG geschiedt (zie art. 5 lid 2 AVG 'omkering bewijslast').

De verwerker heeft een uitvoerende taak en geen zeggenschap over de wijze van verwerken. Een verwerker is echter niet aan het gezag van de verwerkingsverantwoordelijke onderworpen. Een verwerker is bijvoorbeeld een administratiekantoor dat salarisadministratie voor een bedrijf uitvoert. Een secretaresse die gegevens van de cliënt van een advocaat verwerkt bijvoorbeeld, is geen verwerker. Zij is namelijk aan het gezag van de advocaat onderworpen.

De plichten van de verwerker staan in art. 28 AVG. Ex art. 28 lid 3 AVG geschiedt de verwerking door een verwerker onder een overeenkomst[11] met de verwerkingsverantwoordelijke.

5. BEGINSELEN INZAKE DE VERWERKING VAN PERSOONSGEGEVENS

De beginselen inzake de verwerking van persoonsgegevens staan in hoofdstuk II (art. 5-11 AVG). Art. 5 lid 1 AVG somt de beginselen inzake de verwerking van persoonsgegevens op. Daar staat (samengevat weergegeven) dat persoonsgegevens moeten:
a. worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig,[12] behoorlijk en transparant is;
b. worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en vervolgens niet verder op een met die doeleinden onverenigbare wijze mogen worden verwerkt ('doelbinding');[13]
c. zijn beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking');
d. juist zijn ('juistheid');
e. worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is ('opslagbeperking');
f. beveiligd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernieti-

9. Art. 3 lid 2 AVG.
10. Art. 3 lid 3 AVG.
11. Zie hierna voor meer over de verwerkingsovereenkomst.
12. In art. 6 AVG is de rechtmatigheid van de verwerking geregeld.
13. De verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig art. 89 lid 1 niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (art. 5 lid 1 sub b AVG).

ging of beschadiging ('integriteit en vertrouwelijkheid').

Op grond van art. 5 lid 2 AVG is de verwerkingsverantwoordelijke verantwoordelijk voor de naleving van art. 5 lid 1 AVG en moet hij kunnen aantonen dat hij aan de vereisten van art. 5 lid 1 AVG voldoet ('verantwoordingsplicht'). De bewijslast van naleving ligt dus bij de verwerkingsverantwoordelijke en niet bij de Autoriteit Persoonsgegevens.[14] Dit is, civielrechtelijk gezien, een omkering van de bewijslast.

De verwerking dient op grond van art. 5 lid 1 AVG rechtmatig te zijn. Art. 6 AVG bepaalt dat de verwerking alleen rechtmatig is indien aan ten minste een van de in art. 6 AVG genoemde voorwaarden is voldaan. Die voorwaarden zijn (samengevat weergegeven):

a. de betrokkene[15] heeft toestemming[16] gegeven voor de verwerking van zijn persoonsgegevens;
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;[17]
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;[18]
e. de verwerking is noodzakelijk 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;[19]
f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde.[20]

Hier is een belangenafweging vereist tussen het belang van de verwerkingsverantwoordelijke en de grondrechten van de betrokkene. Een voorbeeld is dat de betrokkene een klant is van de verwerkingsverantwoordelijke en de verwerking nodig is om fraude jegens de verwerkingsverantwoordelijke te voorkomen.

Op grond van art. 6 lid 4 AVG mogen persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verwerkt (zie ook art. 5 lid 1 sub b AVG 'doelbinding'). Echter, art. 6 lid 4 AVG bepaalt dat wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld en die verdere verwerking niet berusten op toestemming van de betrokkene of, kort gezegd, een wettelijke bepaling, dan houdt de verwerkingsverantwoordelijke onder meer rekening met:

a. ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;
Als kan worden vastgesteld dat er sprake is van een verenigbaar doel, is voor de verdere verwerking geen andere afzonderlijke rechtsgrond vereist dan die op grond waarvan de verzameling van de persoonsgegevens werd toegestaan. Hoe nauwer de doelen aan elkaar verwant zijn, hoe eerder zij als verenigbaar worden aangemerkt.
b. de verhouding tussen verantwoordelijke en betrokkene;
Bij persoonsgegevens die direct van de betrokkene zijn verkregen, zal eerder sprake zijn van verenigbaarheid dan bij gegevens die indirect zijn verkregen.
c. de aard van de persoonsgegevens;
Bij bijzondere persoonsgegevens (art. 9 AVG) zal er minder snel worden geoordeeld dat de verwerking verenigbaar met de AVG is.
d. de mogelijke gevolgen van de verdere verwerking;
Hoe kleiner de mogelijke gevolgen hoe eerder de verwerking als verenigbaar kan worden gezien.
e. het bestaan van passende waarborgen waaronder eventueel versleuteling of pseudonimisering.
Dit zijn beveiligingsmaatregelen die de risico's van oneigenlijk gebruik beperken (zie art. 32 lid 1 sub a AVG).

Als de verwerking berust op toestemming (art. 6 lid 1 sub a AVG) moet de verwerkingsverantwoordelijke kunnen aantonen dat die toestemming er is (art. 7 AVG). Art. 4 sub 11 AVG definieert toestemming van de betrokkene als:

'elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;'.

De betrokkene heeft het recht zijn eerder gegeven toestemming in te trekken.[21]

Wanneer een internetdienst, zoals bijvoorbeeld een sociaal netwerk, een dienst aanlevert en daarbij toestemming[22] voor verwerking nodig heeft van een kind dat jonger is dan 16 jaar, is zulke toestemming slechts geldig als het wordt gegeven door de wettelijke vertegenwoordiger van het kind.[23]

14. De Autoriteit Persoonsgegevens is de toezichthoudende autoriteit, bedoeld in art. 51 lid 1 AVG (art. 6 lid 2 UAVG).
15. 'De betrokkene' is de geïdentificeerde of identificeerbare natuurlijke persoon (art. 4 sub 1 AVG).
16. Art. 7 AVG regelt de voorwaarden voor toestemming.
17. Bijvoorbeeld het verstrekken van gegevens van werknemers aan de Belastingdienst.
18. Bijvoorbeeld het verstrekken van medische gegevens van een persoon die een ongeval heeft gehad.
19. Bijvoorbeeld gezondheidsdoeleinden zoals volksgezondheid.
20. Dit geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken. De overheid kan immers de rechtsgrond om persoonsgegevens te verwerken zelf creëren door middel van wet- en regelgeving.
21. Art. 7 lid 3 AVG.
22. Ex art. 6 lid 1 sub a AVG.
23. Art. 8 AVG.

Art. 9 lid 1 AVG definieert een aantal categorieën bijzondere persoonsgegevens zoals bijvoorbeeld ras, etnische afkomst, politieke opvattingen etc. Verwerking van dergelijke gegevens mag alleen als aan een van de volgende voorwaarden is voldaan (samengevat weergegeven):

a. de betrokkene heeft toestemming gegeven;
b. de verwerking is noodzakelijk in verband met verplichtingen of rechten op het gebied van arbeids- of sociaal recht;
c. de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon;
d. de verwerking wordt verricht door politieke, religieuze en levensbeschouwelijke organisaties en vakbonden;
e. de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
f. de verwerking is noodzakelijk in verband met een rechtsvordering;[24]
g. de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang;
h. de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer etc.;
i. de verwerking is noodzakelijk in verband met de volksgezondheid;
j. de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.[25]

Op grond van art. 10 AVG mogen persoonsgegevens betreffende strafrechtelijke veroordelingen alleen worden verwerkt onder toezicht van de overheid of als verwerking wettelijk toegestaan is.

6. RECHTEN VAN DE BETROKKENE

De verwerkingsverantwoordelijke neemt passende maatregelen om ervoor te zorgen dat de betrokkene de in art. 13 en 14 AVG bedoelde informatie in korte, eenvoudige en makkelijk toegankelijke vorm kan verkrijgen.[26] Ook neemt hij passende maatregelen om te zorgen dat hij gehoor kan geven aan de hierna te bespreken rechten van de betrokkene. De verwerkingsverantwoordelijke dient onverwijld, maar in elk geval binnen een maand na een verzoek op grond van art. 15-22 AVG (zie hierna), informatie over de verwerking van dat verzoek te geven. De verzochte informatie dient kosteloos te worden verstrekt tenzij de verzoeken buitensporig zijn (art. 12 lid 5 AVG).

Wanneer persoonsgegevens betreffende een betrokkene bij die persoon worden verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens al de volgende informatie (art. 13 lid 1 AVG):

a. de gegevens van de verwerkingsverantwoordelijke;
b. de gegevens van de eventuele functionaris voor gegevensbescherming;[27]
c. de verwerkingsdoeleinden en de rechtsgrond voor de verwerking;
d. indien van toepassing: de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde op grond waarvan de persoonsgegevens worden verwerkt;
d. de eventuele ontvangers van de persoonsgegevens;[28]
e. in geval van verstrekking aan derde landen:[29]
  – of er een adequaatheidsbesluit[30] van de Commissie bestaat,
  – of passende waarborgen zijn getroffen en zo ja, welke.

Naast deze gegevens dient informatie te worden verstrekt over de bewaartermijn van de persoonsgegevens en de rechten van de betrokkene.

Als persoonsgegevens niet van de betrokkene zelf zijn verkregen, dienen dezelfde gegevens als onder art. 13 genoemd te worden verstrekt alsmede de bron van de persoonsgegevens.[31]

De betrokkene heeft het recht om te weten welke persoonsgegevens van hem worden verwerkt. De volgende informatie dient op zijn verzoek aan hem te worden verstrekt (samengevat weergegeven):[32]

a. de verwerkingsdoeleinden;
b. de betrokken categorieën van persoonsgegevens;
c. de ontvangers van de persoonsgegevens;
d. de bewaartermijn;
e. de rechten van de betrokkene;
f. het recht van de betrokkene om te mogen klagen bij de Autoriteit Persoonsgegevens;
g. als het persoonsgegevens zijn die van derden zijn verkregen, de bron van die persoonsgegevens;
h. informatie over het eventuele bestaan van geautomatiseerde besluitvorming.[33]

Wanneer de persoonsgegevens worden doorgezonden naar een land zonder passend beschermingsniveau (zie art. 46 AVG), dan is de verwerkingsverantwoordelijke verplicht om informatie te verstrekken over de door hem

24. Bijvoorbeeld het overleggen van een bewijsstuk waarin bijzondere persoonsgegevens staan.
25. Zie art. 89 lid 1 AVG.
26. Art. 12 lid 1 AVG.
27. Hierna wordt de functionaris voor gegevensbescherming uitgebreid besproken.
28. In de AVG is per abuis art. 13 lid 1 sub d tweemaal gebruikt.
29. Zie par. 9 over de voorwaarden voor de verstrekking van persoonsgegevens aan ontvangers in derde landen.
30. Zie par. 9.
31. Art. 14 AVG.
32. Art. 15 AVG.
33. Hierna (par. 6) wordt uitgebreider ingegaan op geautomatiseerde besluitvorming.

gebruikte passende waarborgen[34] om de gegevensexport te legitimeren.

Indien daarom gevraagd, dient de verwerkingsverantwoordelijke een kopie van de verwerkte persoonsgegevens te verstrekken.

De betrokkene heeft recht op verbetering van onjuiste persoonsgegevens.[35] Ook heeft hij recht op 'wissing'[36] van zijn gegevens:

a. als ze niet langer nodig zijn;
b. als hij zijn toestemming intrekt;
c. als hij bezwaar maakt tegen de verwerking (zie art. 21 AVG);
d. in geval van onrechtmatige verwerking;
e. in geval van een wettelijke verplichting om te wissen;
f. als de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij (bijvoorbeeld mobiele telefonie of internet) aan een kind.[37]

Als de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt, dan neemt hij de nodige maatregelen om voor wissing te zorgen (art. 17 lid 2 AVG).
Art. 17 lid 3AVG bevat uitzonderingen op de verplichtingen uit art. 17 lid 1 en 2 AVG. Het betreft, kort gezegd, de volgende uitzonderingen:

a. de gegevens zijn nodig voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
b. de gegevens zijn nodig voor het nakomen van een wettelijke plicht;
c. de gegevens zijn nodig om redenen van algemeen belang op het gebied van volksgezondheid;
d. de gegevens zijn nodig in verband met archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig art. 89 lid 1 AVG;
e. de gegevens zijn nodig in verband met een rechtsvordering.

De betrokkene heeft in de volgende gevallen recht op beperking van de verwerking:[38]

– bij betwisting van de juistheid van de persoonsgegevens;
– bij onrechtmatige verwerking;
– als de persoonsgegevens niet meer nodig zijn;
– als hij bezwaar maakt tegen de verwerking.

Op grond van art. 19 AVG dient de verwerkingsverantwoordelijke iedere ontvanger van persoonsgegevens te informeren over de rectificatie, 'wissing' (verwijdering) of beperking van verwerking van de persoonsgegevens.

De betrokkene heeft het recht om zijn persoonsgegevens in een gestructureerde, gangbare vorm te verkrijgen en het recht om ze over te dragen aan een andere verwerkingsverantwoordelijke.[39] Ook heeft hij het recht om bezwaar te maken tegen de verwerking van zijn persoonsgegevens ingeval de grondslag voor die verwerking berust op noodzaak (art. 6 lid 1 sub e en f AVG) en als de persoonsgegevens worden gebruikt voor *direct marketing*.[40]

De betrokkene heeft ook het recht niet te worden onderworpen aan een besluit dat tot stand is gekomen door middel van geautomatiseerde individuele besluitvorming, waaronder profilering.[41] Geautomatiseerde individuele besluitvorming is het gebruik van persoonsgegevens om tot een bepaalde beslissing te komen waarbij die beslissing uitsluitend gebaseerd is op geautomatiseerde verwerking. Profilering (*profiling*) is het indelen van personen in categorieën (profielen) op basis van hun persoonsgegevens. Op basis van deze profielen kunnen vervolgens (geautomatiseerde) individuele besluiten worden genomen, zoals bijvoorbeeld het verlenen van krediet door een financiële instelling.
Een voorbeeld van een verboden geautomatiseerde individuele besluitvorming met een rechtsgevolg is de opzegging van een arbeidscontract omdat de computer aangeeft dat de werknemer een risico vormt voor de organisatie. Een vorm van profilering die mensen in aanzienlijke mate treft, is het opstellen van bijvoorbeeld een kredietwaardigheidsprofiel en enkel op basis van dit profiel geautomatiseerd besluiten om iemand geen lening te geven.

De volgende uitzonderingen bestaan op het verbod van art. 22 lid 1 AVG:

a. als het besluit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
b. als het besluit bij wet is toegestaan;
c. als het besluit berust op toestemming van de betrokkene.[42]

Gepersonaliseerde internetadvertenties (*online behavioral advertising*) zullen naar mijn mening niet snel onder die uitzonderingen vallen.

Op grond van art. 23 AVG wordt de reikwijdte van de verplichtingen en rechten beperkt als het een noodzakelijke en evenredige maatregel is ter waarborging van de nationale veiligheid, opsporing en vervolging van strafbare feiten en dat soort zaken.

34. In par. 9 komt doorgifte van persoonsgegevens naar derde landen uitgebreid aan de orde.
35. Art. 16 AVG.
36. Ook dit woord staat niet in *Van Dale*. Bedoeld zal zijn 'verwijdering'.
37. Art. 17 lid 1 AVG.
38. Art. 18 AVG.
39. Art. 20 AVG.
40. Art. 21 AVG.
41. Art. 22 lid 1 AVG.
42. Art. 22 lid 2 AVG.

7. VERANTWOORDELIJKHEDEN VAN DE VERWERKINGSVERANTWOORDELIJKE EN DE VERWERKER

Ex art. 4 sub 7 AVG stelt de verwerkingsverantwoordelijke het doel van en de middelen voor de verwerking vast. De verwerkingsverantwoordelijke dient persoonsgegevens te verwerken volgens de in art. 5 AVG genoemde beginselen. Hij moet kunnen bewijzen dat hij volgens deze beginselen verwerkt (art. 5 lid 2 AVG). Daartoe dient hij passende technische en organisatorische maatregelen te treffen en deze te evalueren en zo nodig tijdig te actualiseren. Dit is de algemene verplichting (art. 24 AVG). Daarbij dient rekening te worden gehouden met zogenoemde *privacy by design* en *privacy by default* (art. 25 lid 1 AVG). *Privacy by design* betekent dat de voor de verwerking gebruikte mechanismen zo zijn ingericht dat zij zo veel mogelijk rekening houden met de vereisten uit de AVG. *Privacy by default* betekent dat de standaardinstellingen van het systeem van gegevensverwerking aldus zijn dat privacy maximaal wordt gewaarborgd.

Art. 25 lid 2 AVG is een uitwerking van het beginsel van minimale gegevensverwerking (art. 5 lid 1 sub c AVG).

Om aan de eisen van art. 25 AVG te voldoen kan gebruik worden gemaakt van goedgekeurde certificeringsmechanismen[43] om aan te tonen dat aan de vereisten van art. 25 AVG is voldaan (art. 25 lid 3 AVG).

Als een verwerkingsverantwoordelijke buiten de Unie gevestigd is, dan dient hij een vertegenwoordiger in de Unie aan te wijzen (art. 26 AVG).

De verwerking door een verwerker wordt geregeld in een overeenkomst tussen de verwerker en de verwerkingsverantwoordelijke (art. 28 lid 3 AVG). De inhoud van die overeenkomst moet voldoen aan de eisen van art. 28 lid 3 sub a-h AVG. Daar staat, samengevat weergegeven, dat de verwerkingsovereenkomst minimaal bepaalt dat de verwerker:

a. uitsluitend verwerkt op instructie van de verwerkingsverantwoordelijke;
b. de vertrouwelijkheid van de te verwerken gegevens waarborgt;
c. de maatregelen ex art. 32 AVG[44] zal nemen;
d. voorwaarden in acht zal nemen voor het in dienst nemen van een andere verwerker;
e. -*f.* bijstand zal verlenen aan het nakomen van de verplichtingen met betrekking tot de rechten van de betrokkene;
g. na afloop van de verwerking voor wissing of opslag van de gegevens zal zorgen;
h. de verwerkingsverantwoordelijke zal voorzien van de nodige informatie.

De verwerker kan met toestemming van de verwerkingsverantwoordelijke een andere verwerker in dienst nemen (art. 28 lid 2 AVG). De verwerker moet met die andere verwerker wel een overeenkomst aangaan (art. 28 lid 4 AVG).

De verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden (art. 30 AVG). Het bijhouden van zo een register is om aan te tonen (ex art. 5 lid 2 AVG) dat aan de eisen van de AVG is voldaan. Dat register bevat de volgende gegevens (art. 30 AVG):

a. de naam en contactgegevens van de verwerkingsverantwoordelijke;
b. de verwerkingsdoeleinden; de grondslag hoeft niet te worden genoemd maar het is aan te bevelen die wel te noemen;
c. een beschrijving van de categorieën van de betrokkenen en van de categorieën van persoonsgegevens;
d. de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
e. indien van toepassing, doorgiften van persoonsgegevens aan een ontvanger in een 'derde land' of aan een internationale organisatie;
f. indien mogelijk, de beoogde termijnen waarbinnen de gegevens worden gewist;
g. indien mogelijk, een algemene beschrijving van de beveiligingsmaatregelen (ex art. 32).

Ook de verwerker dient een register bij te houden van de verwerkingsactiviteiten. Dat register bevat de volgende gegevens:

a. de naam en contactgegevens van de verwerker en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt;
b. de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke worden uitgevoerd;
c. indien van toepassing: doorgiften van persoonsgegevens naar een derde land of internationale organisatie;
d. indien mogelijk, een algemene beschrijving van de beveiligingsmaatregelen bedoeld in art. 32 lid 1 AVG.

Op grond van art. 30 lid 5 AVG hoeft geen register te worden bijgehouden voor ondernemingen die minder dan 250 personen in dienst hebben, tenzij:

– het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen (in te schatten door de verwerkingsverantwoordelijke ex art. 24 AVG); of
– de verwerking niet incidenteel is; of
– de verwerking betreft bijzondere categorieën van gegevens, als bedoeld in art. 9 lid 1 AVG; of
– de verwerking betreft persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in art. 10 AVG.

Omdat de verwerking al snel structureel is, zal naar mijn mening niet snel aan een van de uitzonderingen zijn voldaan.

43. Voor zover ik heb kunnen nagaan bestaan er (nog) geen goedgekeurde certificeringsmechanismen.
44. Art. 32 AVG regelt de beveiliging van de verwerking.

Beveiliging

Op grond van art. 32 lid 1 AVG dienen maatregelen te worden genomen om de persoonsgegevens te beveiligen door middel van onder meer:

a. pseudonimisering[45] en versleuteling;
b. het vermogen om altijd de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;[46]
c. het vermogen om bij een technisch incident de beschikbaarheid en toegang tot de persoonsgegevens tijdig te herstellen;[47]
d. een procedure om de doeltreffendheid van de technische maatregelen te testen.

Melding van een inbreuk aan de toezichthoudende autoriteit

Art. 33 AVG gaat over de situatie dat er een inbreuk op persoonsgegevens heeft plaatsgevonden. Dit wordt ook wel aangeduid als een 'datalek'. Te denken valt aan een verloren of gehackte laptop of USB-stick met persoonsgegevens. Ook het verzenden van een e-mail aan een groep personen met zichtbare e-mailadressen kan onder omstandigheden een datalek opleveren.
Art. 4 sub 12 AVG definieert 'inbreuk in verband met persoonsgegevens' als:
'een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;'.

De verwerkingsverantwoordelijke moet een datalek zonder onredelijke vertraging, indien mogelijk uiterlijk binnen 72 uur melden aan de toezichthouder.[48] De toezichthouder is in Nederland de Autoriteit Persoonsgegevens (art. 6 lid 2 UAVG). Melden kan online via het meldpunt datalekken.[49]

De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging over een datalek.[50] Bij een hoog risico voor de rechten en vrijheden van natuurlijke personen dient de verwerkingsverantwoordelijke het lek ook te melden aan de betrokkene.[51] Melding aan betrokkene is niet nodig als het datalek versleutelde gegevens betreft, maatregelen zijn genomen om te zorgen dat het risico zich niet zal voordoen of indien de mededeling onevenredige inspanning zou vergen. In het laatste geval volstaat een openbare melding.[52]

Gegevensbeschermingseffectbeoordeling

Een gegevensbeschermingseffectbeoordeling wordt ook wel een *Privacy Impact Assessment* (PIA) genoemd.
Wanneer een soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.[53] Een PIA is met name vereist in de volgende gevallen:[54]

a. geautomatiseerde verwerking, waaronder *profiling*, leidend tot besluiten;[55]
b. grootschalige[56] verwerking van bijzondere categorieën van persoonsgegevens;
c. stelselmatige/grootschalige monitoring openbare ruimten.

De toezichthouder (in Nederland is dat de Autoriteit Persoonsgegevens) dient ex art. 35 lid 4 AVG een lijst op te stellen van het soort verwerkingen waarvoor een PIA verplicht is (de zogenoemde 'zwarte lijst'). Ook kan de toezichthouder een lijst opstellen van verwerkingen waarvoor geen PIA verplicht is (art. 35 lid 5 AVG, de zogenoemde 'witte lijst').

Op grond van art. 35 lid 7 AVG dient de PIA minimaal te bevatten (samengevat weergegeven):

a. een beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
b. een beoordeling van de noodzaak van de verwerkingen;
c. een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen;
d. de beoogde maatregelen om de risico's aan te pakken.

Wanneer uit een PIA blijkt dat de verwerking een hoog risico zou opleveren, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de Autoriteit Persoonsgegevens.[57] Als zij van mening is dat de voorgenomen verwerking een inbreuk op de AVG oplevert, dan

45. Bijvoorbeeld het gebruik van klantnummers in plaats van namen.
46. Dit vereist een goede inrichting van de gebruikte systemen.
47. Dit kan worden bereikt door het regelmatig maken van back-ups die offline worden opgeslagen om het gevaar van besmetting door een virus te voorkomen.
48. Art. 33 lid 1 AVG.
49. datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.
50. Art. 33 lid 2 AVG.
51. Art. 34 AVG.
52. Art. 34 lid 3 AVG.
53. Art. 35 lid 1 AVG.
54. Art. 35 lid 3 AVG.
55. Bijvoorbeeld een verzekeraar die claims automatisch laat beoordelen waarbij gebruik wordt gemaakt van analyses van Facebookprofielen (Engelfriet, Chew-Meij & Kager 2017, p. 150).
56. In overweging 91 AVG staat hierover onder meer: 'Dit dient met name te gelden voor grootschalige verwerkingen die bedoeld zijn voor de verwerking van een aanzienlijke hoeveelheid persoonsgegevens op regionaal, nationaal of supranationaal 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, (…)'.
57. Art. 36 lid 1 AVG.

informeert zij de verwerkingsverantwoordelijke binnen acht weken daarover. Ook mag zij de in art. 58 AVG genoemde (handhavings)bevoegdheden uitoefenen.

8. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

De functionaris voor gegevensbescherming wordt vaak afgekort tot FG. Ook ziet men de afkorting DPO, wat staat voor *Data Protection Officer.* Op grond van art. 37 lid 1 AVG wijzen de verwerkingsverantwoordelijke en de verwerker een functionaris voor gegevensbescherming (FG) aan in geval van:

a. verwerking door een overheidsinstantie met uitzondering van de rechterlijke macht;
b. regelmatige en stelselmatige observatie op grote schaal;[58]
c. grootschalige verwerking van bijzondere categorieën van persoonsgegevens.

De FG is geen toezichthouder en heeft geen corrigerende bevoegdheden. Zijn aanbevelingen zijn echter wel belangrijk bij de bepaling of de verwerking in overeenstemming met de AVG is. De FG moet een natuurlijk persoon zijn. Hij mag een personeelslid van de verwerkingsverantwoordelijke zijn (art. 37 lid 6 AVG). De FG dient deskundig te zijn op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en op het gebied van de in art. 39 bedoelde taken.[59] De verwerkingsverantwoordelijke en de verwerker mogen de FG geen instructies geven. Ook mag hij niet worden ontslagen of gestraft voor de uitvoering van zijn taken.[60]

Art. 39 lid 1 AVG bepaalt dat de FG ten minste de volgende taken vervult:

a. het informeren van de verwerkingsverantwoordelijke en de verwerker en werknemers over hun verplichtingen onder de AVG en andere wetgeving;
b. het toezien op naleving van de AVG en wetgeving;
c. adviseren over en toezien op uitvoering van de PIA;
d. samenwerking met de Autoriteit Persoonsgegevens;
e. optreden als contactpunt voor de Autoriteit Persoonsgegevens.

9. DOORGIFTEN VAN PERSOONSGEGEVENS AAN DERDE LANDEN OF INTERNATIONALE ORGANISATIES

Algemeen beginsel

Ex art. 44 AVG mogen persoonsgegevens slechts aan ontvangers in derde landen[61] worden doorgegeven indien de verwerkingsverantwoordelijke en de verwerker aan de voorwaarden in art. 45-50 AVG hebben voldaan.

Doorgiften op basis van adequaatheidsbesluiten

Doorgifte aan een derde land kan als de Commissie heeft besloten dat dat land een passend beschermingsniveau waarborgt.[62] De Commissie kan besluiten dat een derde land inderdaad het juiste beschermingsniveau waarborgt.[63] Op de website van de Autoriteit Persoonsgegevens staat de volgende lijst van derde landen waarvan de Europese Commissie heeft besloten dat zij een passend beschermingsniveau bieden: Andorra, Argentinië, Canada (let op de uitzonderingen!), Faeröer Eilanden, Guernsey, Isle of Man, Israël, Jersey, Uruguay, Zwitserland.

De Verenigde Staten

Op 12 juli 2016 heeft de Europese Commissie de overeenkomst *EU-US Privacy Shield* voor het uitwisselen van persoonsgegevens aangenomen. Deze overeenkomst is een vervanging van het Safe Harbor-verdrag dat op 6 oktober 2015 door het Europese Hof ongeldig was verklaard. Vanaf 1 augustus 2016 is het *Privacy Shield* geldig. Amerikaanse bedrijven kunnen een *privacy shield*-certificaat verkrijgen. Als zij dat hebben, dan is het niet nodig een Europees Modelcontract met ze aan te gaan.

Modelcontracten

De Europese Commissie (EC) heeft op dit moment de volgende drie modelcontracten (ook wel *standard contractual clauses* of SCC's genoemd) goedgekeurd:

– een modelcontract van de EC voor doorgifte tussen twee verantwoordelijken waarbij de een gevestigd is binnen de EU en de ander daarbuiten, zie: Beschikking van de Commissie van 15 juni 2001 (2001/497/EG);
– een door het bedrijfsleven opgesteld alternatief modelcontract voor de doorgifte tussen twee verantwoordelijken waarbij de een gevestigd is binnen de EU en de ander daarbuiten, zie: Beschikking van de Commissie van 27 december 2004 (2004/915/EG);
– een modelcontract voor doorgifte van een verantwoordelijke gevestigd binnen de EU naar een bewerker (degene die in opdracht van de verantwoordelijke persoonsgegevens verwerkt) in een derde land, zie Besluit van de Commissie van 5 februari 2010 (2010/87/EU).

Als er gebruik wordt gemaakt van een modelcontract zonder aanvullingen of wijzigingen, dan is geen vergunning van de Autoriteit Persoonsgegevens vereist voor de doorgifte van persoonsgegevens.

58. Bijvoorbeeld: recherchebureaus en internetbedrijven die diensten aanbieden om websitebezoek gedetailleerd te monitoren. Voorbeelden van 'op grote schaal' zijn ziekenhuizen, openbare vervoerders, verzekeringsmaatschappijen, banken, zoekmachines, telecom- en internetproviders. De voorbeelden zijn afkomstig uit Engelfriet, Chew-Meij & Kager 2017, p. 158-159.
59. Art. 37 lid 5 AVG.
60. Art. 38 lid 3 AVG.
61. Het begrip 'derde landen' wordt niet gedefinieerd in de AVG. Het wordt ook niet gedefinieerd in het Verdrag betreffende de Europese Unie en ook niet in het Verdrag betreffende de werking van de Europese Unie. Het is echter aannemelijk dat met 'derde landen' worden bedoeld landen buiten de Europese Unie, althans, niet-lidstaten.
62. Art. 45 lid 1 AVG.
63. Art. 45 lid 3 AVG.

Doorgiften op basis van passende waarborgen

Als er geen besluit van de Commissie is, dan mag een doorgifte alleen plaatsvinden als er passende waarborgen zijn.[64] Art. 46 lid 2 AVG bepaalt dat de in lid 1 bedoelde passende waarborgen kunnen worden geboden door de volgende instrumenten, zonder dat daarvoor specifieke toestemming van een toezichthoudende autoriteit is vereist:

a. een juridisch bindend en afdwingbaar instrument tussen overheidsinstanties of overheidsorganen;
b. bindende bedrijfsvoorschriften (ex art. 47 AVG);
c. en d. standaardbepalingen ex art. 93 lid 2 AVG;
e. een goedgekeurde gedragscode, samen met toezeggingen van de verwerkingsverantwoordelijke of verwerker in het derde land;
f. een goedgekeurd certificeringsmechanisme met toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land.

Art. 46 lid 3 AVG bepaalt dat, onder voorbehoud goedkeuring van de Autoriteit Persoonsgegevens, passende waarborgen ook kunnen worden geboden door, met name:

a. een overeenkomst tussen de verwerkingsverantwoordelijke/verwerker en de ontvanger van de persoonsgegevens in het derde land of de internationale organisatie; of
b. bepalingen die moeten worden opgenomen in administratieve regelingen tussen overheidsinstanties of overheidsorganen, waaronder afdwingbare en effectieve rechten van betrokkenen.

Op grond van art. 46 lid 2 sub b AVG kunnen ook bindende bedrijfsvoorschriften voldoende waarborgen bieden om doorgifte naar derde landen toelaatbaar te maken.

Art. 4 sub 20 AVG definieert 'bindende bedrijfsvoorschriften' als:

'beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;'.

Art. 47 AVG bevat een uitgebreide regeling over bindende bedrijfsvoorschriften die ik hier niet verder zal bespreken.

Afwijkingen voor specifieke situaties

Bij ontstentenis van een adequaatheidsbesluit ex art. 45 lid 1 AVG of aan passende waarborgen ex art. 46 kan doorgifte slechts plaatsvinden als aan een van de volgende voorwaarden (samengevat weergegeven) is voldaan:

a. de betrokkene heeft uitdrukkelijk met de voorgestelde doorgifte ingestemd;
b. de doorgifte is nodig voor uitvoering van een overeenkomst tussen de verwerkingsverantwoordelijke en de betrokkene;
c. de doorgifte is nodig voor uitvoering van een overeenkomst die in het belang van de betrokkene met een derde is afgesloten;
d. de doorgifte is nodig wegens gewichtige redenen van algemeen belang;
e. de doorgifte is nodig in verband met een rechtsvordering;
f. de doorgifte is nodig in verband met vitale belangen van de betrokkene of van andere personen;
g. de doorgifte is verricht vanuit een register dat bedoeld is om het publiek te informeren (bijv. een register van registeraccountants of advocaten).

Als aan geen van bovenstaande voorwaarden is voldaan kan onder omstandigheden doorgifte plaatsvinden. De verwerkingsverantwoordelijke dient dan wel de AP en de betrokkene te informeren.[65]

10. AFSLUITENDE OPMERKINGEN

Verwerkingsverantwoordelijken dienen ervoor te zorgen dat zij voor 25 mei 2018 voldoen aan de vereisten van de AVG waaronder het aangaan van verwerkingsovereenkomsten met diegenen die hun persoonsgegevens verwerken en, in de meeste gevallen, het opstellen van het in art. 30 AVG genoemde register van verwerkingsactiviteiten. Voorts dienen zij te zorgen dat hun data zijn beveiligd en dat er veilige back-ups worden gemaakt. Daarnaast dienen zij de hierboven besproken beginselen in acht te nemen en zich bewust te zijn van de rechten van de betrokkenen. Oude Elferink en Reus concluderen in hun gezamenlijke publicatie dat de Autoriteit Persoonsgegevens in de komende jaren haar nieuwe bevoegdheden op grote schaal en intensief zal inzetten.[66] Gezien de plafonds van de mogelijke boetes (ex art. 83 lid 5 AVG € 20 miljoen of 4% van de totale wereldwijde omzet) is het verwerkingsverantwoordelijken aan te bevelen om tijdig de nodige stappen te nemen.

64. Art. 46 lid 1 AVG.
65. Laatste alinea art. 19 lid 1 AVG.
66. E. Oude Elferink & J.G. Reus, 'Handhaving van de Algemene Verordening Gegevensbescherming vanuit Nederlands perspectief', *NtER* 2017, afl. 6, p. 157-164.