G-J. Zwenne & L. Mommers, 'De tien belangrijkste veranderingen die de algemene verordening gegevensbescherming gaat brengen (in minder dan vijfduizend woorden)', *Tijdschrift voor Compliance*, 2016/4, p. 182-189

DE TIEN BELANGRIJKSTE VERANDERINGEN DIE DE ALGEMENE VERORDENING GEGEVENSBESCHERMING GAAT BRENGEN (IN MINDER DAN VIJFDUIZEND WOORDEN)

Prof. mr. Gerrit-Jan Zwenne & mr. Laurens Mommers*

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming in werking. Als het gaat om de verwerking van persoonsgegevens hebben we vanaf dat moment niet meer te maken met de Wet bescherming persoonsgegevens, maar met nieuwe regels die in de hele Europese Unie gelijk zijn. Wat betekent dat? In deze bijdrage gaan we in op de tien belangrijkste veranderingen die de verordening met zich brengt

0. Inleiding

De titel van deze bijdrage is misleidend. Althans, deze suggereert iets waarvan het maar de vraag is of we dat kunnen waarmaken. Want wat zijn de tien belangrijkste veranderingen die de Algemene Verordening Gegevensbescherming[1] (AVG) gaat brengen? De wijze waarop wij tot onze selectie gekomen zijn, is arbitrair. Althans: die is ingegeven door wat de auteurs van deze bijdrage denken dat de lezers van dit tijdschrift, belangrijk vinden.

---

* Prof. mr. Gerrit-Jan Zwenne is hoogleraar Recht en de informatiemaatschappij aan de Universiteit Leiden en advocaat bij Brinkhof in Amsterdam. Mr. Laurens Mommers is COO van PrivacyPerfect in Rotterdam. De auteurs danken mr. ir. Ard Jan Dunnik voor zijn waardevolle opmerkingen bij een eerder versie van deze bijdrage.

[1] Voluit: 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), *PbEG* L 119 van 04/05/2016, bldz. 1-88.

In deze bijdrage gaan wij in vogelvlucht door de verordening heen, zonder de pretentie om volledig te zijn. We willen op hoofdlijnen inzichtelijk maken wat er gaat veranderen en wat daarvan de betekenis kan zijn, zodat u zich daarop wellicht al enigszins kunt voorbereiden.

1. Een verordening, géén richtlijn

In Europa vinden we op dit moment de regels voor de verwerking van persoonsgegevens in de nationale privacywetten waarmee lidstaten de Privacyrichtlijn 95/46/EG van 24 oktober 1995 hebben omgezet. Deze Privacyrichtlijn verlangt van lidstaten dat zij ervoor zorgen dat hun wetgeving waarborgen bevat 'in verband met de verwerking van persoonsgegevens' en dat dit gebeurt 'overeenkomstig de bepalingen van de richtlijn'.

In Nederland is dat gebeurd in de Wet bescherming persoonsgegevens (Wbp) en ook wel in andere wetten, zoals de Wet basisregistratie personen. In België is dat gedaan in de Wet verwerking persoonsgegevens, in Frankrijk in de *Loi informatique et libertés*, in het Verenigd Koninkrijk in de *UK Data Protection Act 1998* en in Zweden in de *Personuppgiftslagen*, enzovoorts.

De richtlijn beoogt binnen een zekere bandbreedte te komen tot een harmonisatie van nationale privacyregels, maar leidt niet tot een volledige harmonisatie van de regels. Er is een zeker minimum en een maximum en binnen die kaders zijn de lidstaten vrij hun wetgeving naar eigen inzicht in te richten.[2] De richtlijn heeft daardoor niet kunnen voorkomen dat er in de Unie nog steeds verschillen zijn tussen de regels die in verschillende lidstaten gelden. Er is met andere woorden sprake van fragmentatie.

De verordening wil deze fragmentatie verminderen en zo bijdragen aan onder andere rechtszekerheid en een consistent en hoog beschermingsniveau voor de natuurlijke personen ('betrokkenen' of '*data subjects*') over wie er persoonsgegevens worden verwerkt (overw. 9-10 Preambule AVG). Dit doet de verordening doordat deze, anders dan de Privacyrichtlijn, niet behoeft te worden omgezet in nationale wetgeving, maar rechtstreeks verplichtingen oplegt aan degenen die persoonsgegevens verwerken en rechten toekent aan de betrokkenen.

Wat betekent dat? Doordat we in alle lidstaten te maken hebben met een en dezelfde verordening ligt het voor de hand dat er geen sprake meer gaat zijn van nationale afwijkingen. Iedere lidstaat werkt met de-

[2] *Kamerstukken II* 1997/98, 25 892, nr. 3, bldz. 5.

zelfde tekst, zij het dat die wel in alle officiële talen van de unie beschikbaar is.[3] En hoewel inmiddels wel al duidelijk is dat er bij de vertalingen onbedoeld allerlei oneffenheden zijn ingeslopen, kunnen we er vanuit gaan dat die zonder veel moeite kunnen worden gladgestreken. En toch moeten we er rekening mee houden dat de toepassing van de regels in verschillende lidstaten uiteen gaat lopen. Enerzijds doordat de verordening lidstaten op belangrijke beleidsterreinen, zoals sociale zekerheid, arbeid en zorg, de ruimte geeft om eigen regels vast te stellen. En anderzijds doordat de verordening, zoals alle privacywetgeving, zich kenmerkt door veel open begrippen en vage normen, die in de praktijk moeten worden ingevuld en geconcretiseerd. Ook doordat nationale toezichthouders en nationale rechters onverminderd bevoegd blijven over de toepassing van de verordening, leidt dit zonder twijfel tot verschillen in de uitleg en toepassing van de regels in de lidstaten.

> Een voorbeeld. Als het gaat om het openbaar maken van inkomensinformatie heeft men in Scandinavië heel andere opvattingen dan elders in Europa. In Finland zijn er bijvoorbeeld in termen van de privacywet weinig bezwaren tegen een sms-informatiedienst waarmee door iedereen het belastbaar inkomen van willekeurige burgers kan worden opgevraagd (€2,00 p.b.).[4] In Nederland zou zo een dienst waarschijnlijk niet voldoen aan de op grond van de privacyregels voorgeschreven proportionaliteitstoetsen.[5]

Wat betekent het nog meer dat we straks de regels niet meer in de Wbp maar in de verordening vinden? Voor de Nederlandse praktijkjurist of *compliance-officer* is wellicht het meest tastbare gevolg dat er straks geen of weinig parlementaire geschiedenis beschikbaar is om inzicht te geven in de bedoelingen van de wetgever. Wij moeten het doen met de 173 overwegingen in de preambule, die vaak alleen maar papagaaien wat in de bepalingen van de verordening ook al staat.

Voor die gevallen waarin gebruik wordt gemaakt van de Nederlandse versie van de verordening, past een waarschuwing. Aan die vertaling is helaas te weinig aandacht besteed en daardoor is deze bepaald niet foutloos. In enkele gevallen is de Nederlandse tekst volstrekt onbegrijpelijk

---

[3] Er zijn in de EU 24 officiële talen: Bulgaars, Deens, Duits, Engels, Ests, Fins, Frans, Grieks, Hongaars, Iers, Italiaans, Kroatisch, Lets, Litouws, Maltees, Nederlands, Pools, Portugees, Roemeens, Sloveens, Slowaaks, Spaans, Tsjechisch en natuurlijk Zweeds.

[4] Het voorbeeld is ontleend aan HJEU 16 december 2008, C-73/07 (Satakunnan Markkinapörssi / Satamedia).

[5] Een uitzondering geldt voor topinkomens bij semipublieke instellingen of bonussen van beursgenoteerde ondernemingen. Als het daarover gaat, vinden we in Nederland inkomenstransparantie vaak niet zo heel bezwaarlijk, misschien vooral omdat het onszelf meestal niet direct raakt.

zonder de Engelse. In geval van twijfel is dan ook verstandig uit te gaan van de Engelse tekst.[6]

2. Een handvol nieuwe begrippen

De verordening introduceert een handvol nieuwe begrippen. Enkele daarvan zijn nieuwe aanduidingen voor inhoudelijk ongewijzigde begrippen die ook al in de Privacyrichtlijn te vinden waren. Enkele andere begrippen waren nog niet in de richtlijn opgenomen, maar werden al wel gebruikt. En weer enkele andere begrippen zijn helemaal nieuw, in zoverre dat de verordening daarvoor een nieuwe begripsomschrijving geeft en een geheel nieuwe regeling.

Van de inhoudelijk ongewijzigde begrippen die een nieuwe aanduiding hebben gekregen, zijn de meest bekende die van de 'verwerkingsverantwoordelijke' en de 'verwerker' (art. 4(7) en (8) AVG). In de Wbp werd nog gesprokken van de 'verantwoordelijke' en 'bewerker' (art. 1(d) en (e) Wbp), in de richtlijn van de 'voor de verwerking verantwoordelijke' en de 'verwerker' (art. 2(d) en (e) richtlijn). Over deze twee nieuwe aanduidingen is meteen ook de meeste ergernis. Allereerst omdat de 'verwerkingsverantwoordelijke', vergeleken met de 'verantwoordelijke' meer dan een hele mond vol is (maar welbeschouwd niet meer dan 'voor de verwerking verantwoordelijke'). En verder omdat er de zorg is dat het begrip 'verwerker' meer dan het eerdere begrip 'bewerker' uit de Wbp gaat worden verward met de 'verantwoordelijke'. We zullen eraan moeten wennen.

Enkele voorbeelden van begrippen waarmee we al wel bekend zijn en waarvoor in de verordening nu begripsomschrijvingen worden gegeven, zijn de 'bindende bedrijfsvoorschriften' (art. 4(20) AVG) of de 'gegevensbeschermingseffectbeoordeling' (art. 35(1) AVG), wat enigszins Vlaams aandoende vertalingen zijn van respectievelijk de 'binding corporate rules' of 'BCRs' en de 'data protection impact assessments' of 'DPIAs'. Wat verder betrekkelijk nieuw is in de verordening, in die zin dat de richtlijn daarvoor niet in definities voorziet, zijn begrippen als 'profilering' (art. 4(4) AVG), 'pseudonimisering' (art. 4(5) AVG), 'inbreuk in verband met persoonsgegevens' (art. 4(12) AVG), alsmede 'genetische gegevens' en 'biometrische gegevens' (art. 4(12) en (13) AVG). Het zijn allemaal begrippen die in de verordening eigen specifieke regelingen hebben gekregen.

---

[6] Een treurig voorbeeld biedt de Nederlandse vertaling van artikel 23(1) AVG, dat volstrekt onbegrijpelijk is doordat de vertaler het hulpwerkwoord en een komma heeft misplaatst.

Wat betekent dit? Allereerst moeten we wennen aan de nieuwe begrippen en aanduidingen. En we moeten ons er maar bij neerleggen dat degenen die de verordening naar het Nederlands hebben vertaald waarschijnlijk een overwegend Vlaamse achtergrond hebben. Niks aan te doen en ook niet heel erg. Verder lijkt de betekenis van de nieuwe begrippen zich vooral te doen gelden in de nieuwe regelingen waarin de verordening voorziet, bijvoorbeeld waar het gaat om profilering (art. 21-22 AVG) of biometrische gegevens (art. 9(1) en (4) AVG) en genetische gegevens (art. 10 AVG).

3. Vergrote materiële werkingssfeer (?)

De materiële werkingssfeer van de verordening—waarop zijn de regels van toepassing en waarop niet?—komt overeen met die van de richtlijn. De verordening is, evenals de richtlijn, van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand ('een gestructureerd geheel een persoonsgegevens') zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (resp. art. 3(1) richtlijn en art. 2(2) AVG.

En net als in de richtlijn voorziet de verordening in een handvol uitzonderingen (art. 3(2) richtlijn en art. 2(2) AVG). De regels zijn niet van toepassing op de gegevensverwerkingen in het kader van activiteiten die buiten de werkingssfeer van het unierecht vallen. En evenmin op verwerkingen door lidstaten bij de uitvoering van activiteiten betreffende de openbare veiligheid, defensie, de staatsveiligheid en dergelijke. Ook niet op verwerkingen 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. En ten slotte ook niet op verwerkingen door natuurlijke personen bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit.

In zoverre niets nieuws dus. Echter, in het wetgevingsproces zijn wel op enig moment voorstellen gedaan die beoogden de materiele werkingssfeer van de regels vergaand op te rekken. Zo werd, toen het voorstel werd behandeld in het Europees Parlement, het voorstel gedaan om de begripsomschrijving van het begrip van persoonsgegevens op te rekken. In het voorstel van de Commissie werd, overeenkomstig de definitie die daarvoor werd gegeven in de richtlijn, het begrip omschreven als ieder gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 2(a) richtlijn). Van enkele privacybelangengroepen en de nationale privacytoezichthouders, verenigd in de Werkgroep Art. 29, meenden dat daarmee de reikwijdte van het persoonsgegevensbegrip te

beperkt was en deden het voorstel om onder het begrip ook de gegevens te brengen betreffende natuurlijke personen die kunnen worden onderscheiden van anderen; in het Engels: *singled-out*. De werkgroep deed daartoe het voorstel om uit te gaan van de volgende begripsomschrijving van het begrip 'data subject' wat in de indertijd gevolgde systematiek de definitie van het begrip persoonsgegevens aldus zou oprekken:

> *"'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, or singled out and treated differently, by means reasonably likely to be used by the controller or by any other natural or legal person…"* [de voorgestelde toevoeging is onderstreept].

Als dit voorstel was overgenomen, zouden veel meer gegevens kwalificeren als persoonsgegevens. En daarmee zou de materiële werkingssfeer van de verordening, vergeleken met die van de richtlijn, vergaand worden opgerekt. Uiteindelijk is het niet zo ver gekomen. In de finale tekst van de verordening wordt het 'singled-out'-criterium slechts eenmaal genoemd, en dan alleen in een overweging in de preambule, en het heeft daarin alleen betekenis als het erom gaat welke middelen kunnen worden gebruikt om de identiteit van een natuurlijke persoon vast te stellen (overw. 26 Preambule AVG). Er staat, in de Engelse versie van de verordening, dat…

> "*[t]he principles of data protection should apply to any information concerning an identified or identifiable natural person. […] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*." [onderstreping toegevoegd]

Daaruit kan, meen ik, worden opgemaakt dat singling-out weliswaar kan bijdragen aan de identificeerbaarheid en dus wel relevant kan zijn voor de kwalificatie van persoonsgegevens, maar op zichzelf géén zelfstandige betekenis heeft. Er is nog géén sprake van persoonsgegevens als het gaat om gegevens die betrekking hebben op iemand waarvan de identiteit niet zonder onevenredige inspanning kan worden achterhaald, ook niet als die persoon bijvoorbeeld met behulp van een IP-adres of andere apparaat-identifier (zoals een MAC-adres) kan worden onderscheiden van anderen.[7]

---

[7] Zie G-J. Zwenne, 'Nog enkele opmerkingen over IP-adressen en persoonsgegevens, identificeerbaarheid en «single out»', *P&I* 2015/6, bldz. 216-221, alsmede C.C.M. Kroeks-De Raaij, R.J.J. Westerdijk en G.J. Zwenne, 'De Algemene Verordening Gegevensbescherming', *Tijdschrift voor Internetrecht* 2016/2, bldz. 51-52.

Wat is daarvan de betekenis? Voor de praktijkjurist en *compliance officer* is waarschijnlijk vooral van belang dat de werkingssfeer van de gegevensbeschermingsregels niet verandert. Deze regels gaan over de verwerking van persoonsgegevens, en wat daaronder wél en niet valt, blijft ongewijzigd. En toch is van belang dat we er rekening mee houden dat er, ook onder de verordening, nog veel discussie gaat zijn over wat wél en wat niet als persoonsgegeven moet worden aangemerkt. Er is vooral bij privacytoezichthouders een sterke neiging om de reikwijdte van de wet op te rekken. Onder de verordening wordt dat niet anders. Integendeel misschien.

4. Uitbreiding territoriale werkingssfeer

Als we het gaat over de territoriale werkingssfeer van de richtlijn en verordening hebben we het over de vraag wanneer de regels uit de beide rechtsinstrumenten van toepassing zijn. Deze vraag komt vooral op als persoonsgegevens niet in de Unie worden verwerkt of als de verwerkingsverantwoordelijke niet in een van de lidstaten van de Unie is gevestigd.

Voor de richtlijn is de hoofdregel dat van toepassing is: de nationale privacywetgeving van de lidstaat waar zich een vestiging bevindt van de verantwoordelijke, voor zover er persoonsgegevens worden verwerkt in het kader van de activiteiten van die vestiging. Als er geen vestiging van de verantwoordelijke is in de Unie kan niettemin van toepassing zijn de nationale privacywet van de lidstaat waar gebruik wordt gemaakt van geautomatiseerde middelen om de gegevens te verwerken, tenzij die middelen alleen worden gebruikt voor de doorvoer ('transit') van de gegevens (art. 4(1)(a) en (c) richtlijn).

In de verordening verandert dit. De systematiek van de hoofdregel blijft dezelfde, maar de werking ervan wordt uitgebreid tot zogeheten 'verwerkers', dat wil zeggen: derde partijen die de persoonsgegevens verwerken namens de verwerkingsverantwoordelijken (art. 4(8) AVG), zoals een HR of CRM-systeem in de cloud (bijv. Oracle PeopleSoft of Salesforce) of een extern gehoste opslag- of e-mailoplossing (Dropbox, GoogleDocs, Gmail etc.). De verordening is van toepassing als er gegevens worden verwerkt in het kader van de activiteiten van een vestiging van verwerkingsverantwoordelijken of van verwerkers (art. 3(1)).

In aanvulling daarop geldt een heel nieuwe toepassingsregel. De verordening is ook van toepassing als er in de unie *geen* vestiging is van verwerkingsverantwoordelijke of verwerker, als de verwerking van persoonsgegevens verband houdt met (a) het aanbieden van goederen of diensten aan betrokkenen in de Unie, ongeacht of een betaling door deze

betrokkenen is vereist; of (b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt. Dit brengt talloze niet-Europese ondernemingen in het bereik van de verordening, alleen doordat ze erin hebben voorzien dat hun producten via een internationale vervoerder (zeg: UPS of DHL) ook in een van de lidstaten kunnen worden bezorgd. Ook het gebruik van cookies en andere technologie voor *behavourial targeting* leidt tot toepassing van de verordening, als er daarbij sprake is van de verwerking van persoonsgegevens.

Wat merkt de bedrijfsjurist of compliance officer in Nederland daarvan? Voor de organisatie waarvan hij of zij onderdeel uitmaakt misschien niet zoveel. Als er sprake is van een vestiging in Nederland, is de verordening sowieso van toepassing. Wél betekent het dat concurrenten van buiten de Unie in veel gevallen aan dezelfde privacyregels moeten voldoen. En als er gebruik wordt gemaakt van verwerkers zullen die, in de gevallen waarin die een vestiging hebben in de Unie, ook met dezelfde regels te maken hebben. Een nog onbeantwoorde vraag blijft natuurlijk of verwerkingsverantwoordelijken en verwerkers van buiten de Unie überhaupt bereid zijn zich te conformeren aan regels die, vanuit hun perspectief, maar weinig aanknopingspunten hebben met hun bedrijfsvoering. Een andere vraag is of toezichthouders daarop gaan handhaven. We gaan het zien - of niet.

5. Meer verplichtingen voor verwerkers

In de vorige paragraaf bleek dat de uniewetgever voor de territoriale werkingssfeer van de verordening ook uitgaat van de vestigingsplaats van de verwerker ('bewerker' in de Wbp). In het verlengde daarvan ligt dat in de verordening, veel meer dan in de richtlijn, zelfstandige verplichtingen oplegt aan de verwerker.

In de richtlijn wordt van de nationale wetgever alleen verlangd dat aan verwerkers de verplichting wordt opgelegd om persoonsgegevens uitsluitend in opdracht van de verantwoordelijke te verwerken (art. 16 richtlijn; art 12 Wbp). Verder wordt verlangd dat er in een bewerkersovereenkomst is voorzien dat de verwerker zich moeten houden een geheimhoudingsverplichtingen (art. 17 richtlijn, art. 14 Wbp).

In de verordening worden die verplichtingen aangevuld met een tiental nieuwe, rechtstreeks op de verwerker rustende verplichtingen. Het gaat (onder meer) om verplichtingen:

- met betrekking tot het gebruik maken van sub-verwerkers (art. 28(2) en (4) AVG);

- voor verwerkers buiten de unie om een vertegenwoordiger aan te wijzen (art. 27(1) AVG);
- om aan de verantwoordelijke melding te doen van beveiligingsinbreuken (art. 28(3)(h) en art. 33(2) AVG);
- om een register bij te houden van alle ten behoeve van een verwerkingsverantwoordelijke verrichte verwerkingen (art. 30(2) AVG);
- om mee te werken met een onderzoek en de uitvoering van andere taken van de toezichthouder (art. 31 AVG);
- om een functionaris voor de gegevensverwerking aan te stellen (art . 37(1) AVG);
- met betrekking tot gegevensdoorgiften naar landen buiten de unie (art. 44t/m 49 AVG).

Voor de hand ligt dat vrijwel al deze verplichtingen op dit moment worden geregeld in de bewerkersovereenkomst tussen verantwoordelijke en verwerker Voor deze overeenkomst voorziet de verordening overigens ook al in een opsomming van daarin te regelen onderwerpen (art. 28(3)(a) t/m (h) AVG). Maar toegegeven kan worden dat veel daarvan ook op dit moment wel in de overeenkomst wordt opgenomen. In zoverre is er misschien geen sprake van een heel grote verandering. Wat echter wel verandert, is dat betrokkenen in relatie tot deze verplichtingen rechtstreeks een beroep kunnen doen op de verwerker. Hetzelfde geldt voor toezichthouders. Waar zij onder de richtlijn niet gemakkelijk om de verantwoordelijke heen kunnen, maakt de verordening het mogelijk de verwerker rechtstreeks aan te spreken op de naleving van deze verplichtingen.

6. En meer rechten voor betrokkenen

Onder de richtlijn hebben betrokkenen allerlei rechten die zij tegenover de verantwoordelijke kunnen inroepen. Het gaat dan vooral om inzage en verbeterings- of verwijderingsrechten, en het daaruit afgeleide vergeetrecht,[8] alsmede verzetsrechten met betrekking tot geautomatiseerde besluitvorming of direct marketing (art. 12, 14, en 15 richtlijn).

In de verordening zien we al deze rechten in meer uitgewerkte en gedetailleerde vorm terug. In de richtlijn en in de wet geeft het inzagerecht de betrokkene aanspraak op informatie over de doeleinden van de verwerkingen, de categorieën van de verwerkte gegevens en de ontvangers

[8] HJEU 13 mei 2014, C-131/12 (Google/Costeja).

of categorieën ontvangers aan wie de gegevens worden verstrekt, alsmede de beschikbare informatie over de herkomst van de gegevens (resp. art. 12(1) richtlijn en art. 35(2) Wbp). Onder de verordening gaat het om al deze informatie, met in aanvulling daarop ook informatie over de bewaartermijnen, klachtrechten en -procedures, gegevensdoorgiften naar landen buiten de Unie en de in dat verband getroffen waarborgen, en het bestaan van de mogelijkheid dat er geautomatiseerde besluitvorming en profilering plaatsvindt (art. 15(1), (2) en (4) AVG).

Verder voorziet de verordening in een aantal heel nieuwe rechten voor betrokkenen. Wat daarvan vooral opvalt zijn het gegevenswissingsrecht, ook wel aangeduid als - het staat er echt - 'recht op vergetelheid' en het recht op gegevensoverdraagbaarheid (art. 17 en art. 20 AVG). Het gegevenswissingsrecht ziet erop dat de betrokkene van de verwerkingsverantwoordelijk kan verlangen dat zijn persoonsgegevens worden gewist als deze niet meer relevant zijn of onrechtmatig worden verwerkt. In het geval deze gegevens openbaar zijn gemaakt door de verwerkingsverantwoordelijke, moet deze ervoor zorgen dat degenen die daardoor over de gegevens beschikken worden geïnformeerd over het verwijderingsverzoek (art. 17(2) AVG). Het gegevensoverdraagbaarheidsrecht geeft de betrokkene het recht om in bepaalde gevallen de informatie die hij heeft verstrekt aan de éne verwerkingsverantwoordelijke te doen overdragen naar de andere (art. 20(1) AVG). Het is bedoeld voor sociale netwerken, maar de werking ervan is daartoe niet beperkt[9] (overw. 68 Preambule AVG).

Interessant is het 'recht op beperking' (art. 18 AVG). Op grond daarvan kan een betrokkene, die stelt dat gegevens onjuist zijn of onrechtmatig worden verwerkt, de verwerking daarvan laten opschorten zolang het onderzoek naar de onjuistheid of onrechtmatigheid nog loopt. Dit recht kan verstrekkende gevolgen hebben doordat betrokkenen daarmee een nauwelijks beperkt recht lijken te hebben om een hen onwelgevallige gegevensverwerking voor een bepaalde tijd te laten beëindigen, enkel door te stellen dat die verwerking onrechtmatig is. Daarmee lijkt het dan alsof gegevensbeschermingsrechten voorrang hebben op andere fundamentele rechten en vrijheden, zoals de informatievrijheid en de vrijheid van ondernemerschap, enz. En dat lijkt dan weer strijdig met de uitgangspunten van de verordening, namelijk dat gegevensbeschermingsrechten moeten worden beschouwd in relatie tot de functie ervan in de samenleving en worden afgewogen tegen andere rechten en vrijheden (overw. 4 Preambule AVG). De nationale wetgever kan hiervoor

[9] Interessant is dat Google al de mogelijkheid biedt om de door een accounthouder uitgevoerde zoekopdrachten te exporteren.

regels stellen (art. 23(1) AVG), sterker nog: voor zover het gaat om de informatievrijheid is de wetgever gehouden dat te doen (art. 85 AVG).

Wat is de betekenis hiervan? We kunnen ervan uitgaan dat de positie van betrokkenen aanmerkelijk wordt versterkt door de rechten die de verordening hen toekent. Echter, van alle hoofdstukken in de verordening blijkt vooral dit hoofdstuk op betrekkelijk inconsistente, om niet te zeggen slordige wijze te zijn opgeschreven. Het is te hopen dat de nationale wetgever de problemen als gevolg daarvan gaat oplossen.

7. Nogal wat formaliteiten

De verordening voorziet in nogal wat verplichtingen die we gemakshalve maar samenvatten onder de noemer 'formaliteiten', zonder dat we daarmee de suggestie willen wekken dat deze geen of weinig waarde hebben. Het zijn de verplichtingen die verband houden met wat we wel aanduiden als *accountability*, het kunnen aantonen dat er is voldaan aan de wettelijke vereisten. In zoverre hebben deze verplichtingen enige verwantschap met boekhoudverplichtingen, waaraan nogal eens wordt voldaan omdat het nou eenmaal moet.

We doelen dan allereerst op de informatieplichten waaraan vaak wordt voldaan door privacyverklaringen die vaak ongelezen blijven. In de verordening zijn deze informatieplichten veel gedetailleerder dan in de richtlijn en verlangen onder andere dat bewaartermijnen worden vermeld, evenals klachtenprocedures, doorgiften naar landen buiten de unie, enz. (art. 14(1)(a) t/m (e) en (2)(a) t/m (f) en 15(1)(a) t/m (f) en (2)(a) t/m (g) AVG).

Verder kan worden gedacht aan de verplichtingen om een register van verwerkingsactiviteiten bij te houden (art. 30 AVG) of om een gegevensbeschermingseffectbeoordeling te doen (art. 35 AVG). Ook de verplichting om een functionaris voor de gegevensbescherming aan te stellen, kent nogal wat formele vereisten, bijvoorbeeld met betrekking tot zijn of haar rechtspositie, takenpakket en verantwoording (art. 37-39 AVG).

Een risico van dit soort formaliteiten is dat deze bijdragen aan een bedrijfscultuur waarin erop wordt vertrouwd dat het met de gegevensbescherming wel goed zit als in de privacyverklaring alle verplichte onderwerpen zijn benoemd, zolang de vragenlijsten van de gegevensbeschermingseffectbeoordelingen netjes zijn ingevuld, zolang er iemand is met op haar visitekaartje de titel DPO, enz. Voor de *compliance officer* zijn dat misschien geen onbekende verschijnselen. Maar tegeljkertijd kunnen juist dit soort formele vereisten ook leiden tot meer aandacht voor en kennis van al datgene wat met persoonsgegevens in een organisatie gebeurt, en daarmee de kwaliteit van de gegevensbescherming

verhogen, net als een goede boekhouding de verantwoording van en de omgang met financiële verslaglegging ondersteunt.

8. Meer instrumenten voor internationale doorgifte

De verordening bevat, evenals de richtlijn, een verbod op de doorgifte van persoonsgegevens naar landen buiten de Europese Unie, of eigenlijk de Europese Economische Ruimte (EER),[10] die geen passend beschermingsniveau bieden (art. 44 AVG). Wat dat betreft verandert de verordening niet veel aan de situatie onder de richtlijn (art. 25-26 richtlijn).

De verordening voorziet wel in veel meer instrumenten die het mogelijk maken om persoonsgegevens door te geven naar landen die geen passend beschermingsniveau bieden. In de richtlijn, en in de wet, kenden we al de door de Commissie goedgekeurde modelcontracten, beter bekend onder de Engelse aanduiding '*standard contractual clauses*' of '*SCCs*' (art. 26(4) richtlijn, art. 77(1)(g) Wbp). In de verordening worden die ook genoemd (art. 46(2)(c) AVG), maar daarbij komen dan nog door nationale toezichthouders goedgekeurde modelcontracten, gedragscodes en certificeringsmechanismes (art. 46(2)(d), (e) en (f) AVG). Ook noemt de verordening de bindende bedrijfsvoorschriften, wat de vertaling blijkt te zijn van de welbekende 'binding corporate rules' (art. 46(2)(b) AVG), die ook onder de richtlijn al wijdverspreid zijn, hoewel ze daarin niet worden genoemd.

In aanvulling op deze doorgifte-instrumenten voorziet de verordening, net als de richtlijn, in een handvol uitzonderingen op grond waarvan persoonsgegevens toch wel mogen worden doorgegeven naar de derdelanden die geen passend beschermingsniveau bieden. Zo een doorgifte is toegestaan als de betrokkenen daarmee hebben ingestemd, als de doorgifte nodig is voor de uitvoering van een overeenkomst die is gesloten met, of in het belang van, de betrokkene, als de doorgifte nodig is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, ter bescherming van vitale belangen van de betrokkene of uit publieke registers (art. 26(1)(a) t/m (f) richtlijn, art. 49(1)(a) t/m (f) AVG).

In de verordening wordt vervolgens nog wel een extra uitzondering geïntroduceerd die we niet in de richtlijn zien. Als een doorgifte niet op een van voornoemde uitzonderingen kan worden gegrond, kan deze toch toegestaan zijn als is voldaan aan de volgende, tamelijk strenge voorwaarden: (i) de doorgifte mag niet repetitief zijn en (ii) het aantal betrokkenen moet beperkt zijn; (iii) de doorgifte moet nodig zijn voor dwingende gerechtvaardigde belangen van de verwerkingsverantwoor-

[10] Zie art. 76(2) Wbp.

delijke die niet ondergeschikt zijn aan de belangen of rechten en vrijheden van de betrokkene; (iv) en de verwerkingsverantwoordelijke moet alle omstandigheden in verband met de gegevensdoorgifte hebben beoordeeld en op basis daarvan passende waarborgen voor de bescherming van persoonsgegevens hebben geboden.

Als gebruik wordt gemaakt van deze uitzondering moet de verwerkingsverantwoordelijke ten slotte ook de nationale toezichthouder en de betrokkenen daarover informeren (art. 49(h), laatste alinea, AVG).[11]

Al met al gaat dit hoofdstuk van de verordening meer mogelijkheden bieden om oplossingen te vinden voor de problemen die kunnen ontstaan als gevolg van het verbod van internationale doorgifte van persoonsgegevens. Er is tot op zekere hoogte sprake van codificatie, in het bijzonder waar het gaat om de bindende bedrijfsvoorschriften, en dat zou op zichzelf moeten bijdragen aan de rechtszekerheid. We moeten afwachten wat de praktische betekenis gaat zijn van de nationale standaardcontracten, gedragscodes en certificeringsmechanismen.

9. Het Europees Comité voor Gegevensbescherming

We kennen de op artikel 29 van de richtlijn gebaseerde 'Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens', in het dagelijks taalgebruik aangeduid als de Art. 29 Werkgroep. Deze werkgroep bestaat uit vertegenwoordigers van de nationale toezichthouders in de verschillende lidstaten en van de Commissie en andere EU-instellingen. De werkgroep wordt geacht onafhankelijk te zijn en raadgevend van aard. In de praktijk zien we dat de werkgroep zich ook heel actief bemoeit met handhaving in individuele gevallen[12] en zich zeer intensief inlaat met wetgevingsprocessen in brede zin (zoals bij de totstandkoming van de verordening).[13]

---

[11] Het is ons onduidelijk waarom deze uitzondering geen eigen nummeraanduiding heeft gekregen.

[12] Zie bijv. Letter from the Article 29 Working Party to Google on Google Privacy Policy, 23 September 2014 (incl. a list of possible compliance measures).

[13] Vgl. Art. 29 Werkgroep, Advies 01/2012 over de voorstellen voor de hervorming van het gegevensbeschermingskader, WP191, 23 maart 2012; Advies 08/2012 met aanvullende input voor de bespreking over de hervorming van de gegevensbeschermingswetgeving, WP199, 5 oktober 2012; Letters from the Art. 29 WP to LV Ambassador Ilze Juhansone, Commissioner Věra Jourová and MEP Jan Peter Albrecht in view of the trilogue, 17 June 2015; Letter from the Art. 29 WP to MEP Jan Philipp Albrecht on the European Data Protection Board Internal Structure 25 September 2015; Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), WP 236, 2 February 2016.

In de verordening komt een soortgelijk orgaan terug, te weten: het Europees Comité voor Gegevensbescherming, afgekort 'het Comité'. De taken van dit orgaan, dat onder de verordening rechtspersoonlijkheid verkrijgt, zijn een uitbreiding van die van de werkgroep. Evenals de werkgroep gaat het Comité zich bezighouden met advisering over aangelegenheden in verband met de bescherming van persoonsgegevens in de Unie, over bindende bedrijfsvoorschriften en over het recht op vergetelheid. Het Comité kan richtsnoeren vaststellenen aanbevelingen doen, beste praktijken (bedoeld zijn *best practices*) opstellen, en dat allemaal gevraagd en ongevraagd. Wat nieuw is, althans onder de richtlijn niet uit de verf is gekomen, is dat het Comité gaat bevorderen dat er gedragscodes tot stand komen. Ook is nieuw dat het zich gaat bezighouden met accreditatie van certificeringsorganen en van de periodieke evaluatie ervan, etc. (art. 70(1)(a) t/m (y) AVG).

Op basis van de uitvoerige takenlijst van het Comité zou daarom kunnen worden afgeleid dat we veel meer gaan merken van het Comité dan van de werkgroep. Echter, als we kijken naar wat de werkgroep thans al doet, lijkt er betrekkelijk weinig te gaan veranderen. Er wordt wel gesuggereerd dat het Comité, gelet op zijn verdergaand in de verordening verankerde institutionele positie, zou moeten overwegen om soms nogal controversiële standpunten en opvattingen van de werkgroep te heroverwegen. Of dat gaat gebeuren is de vraag.

10. En ten slotte substantiële boetes

Er is betrekkelijk veel aandacht voor de boetes die nationale toezichthouder onder de verordening kunnen gaan opleggen aan verwerkingsverantwoordelijken en verwerkers voor overtredingen van de bepalingen uit de verordening. Dat is wellicht terecht. Als sluitstuk op de handhaving zijn deze boetes waarschijnlijk bepalend voor de naleving van de verordening.

Er zijn twee boetecategorieën. Er zijn boetes van ten hoogste €10 miljoen of 2 procent van de wereldwijde omzet van de verwerkingsverantwoordelijke of verwerker (art. 83(4) AVG). En er zijn boetes van ten hoogste €20 miljoen of 4 procent van de wereldwijde omzet (art. 83(5) AVG).

Onder de eerste boetecategorie (€10 miljoen of 2 procent van omzet) vallen onder andere overtredingen van de informatieverplichtingen en verplichtingen om te voldoen aan inzage- en verbeteringsrechten, en het recht op vergetelheid, alsmede verplichting om zorg te dragen voor 'gegevensbescherming door ontwerp en door standaardinstellingen' (bedoeld is: *privacy by design*, *privacy by default*).

Onder de tweede boetecategorie (€20 miljoen of 4 procent van omzet) vallen verder overtredingen van de verplichting om persoonsgegevens alleen te verwerken overeenkomstig de zgn. gegevensverwerkingsbeginselen, zoals met betrekking tot zorgvuldigheid en behoorlijkheid, transparantie, doelbinding en gegevensminimalisatie (art. 5 AVG), op basis van een toereikende verwerkingsgrondslag (art. 6 AVG), alsook de verplichtingen om inzage- en andere rechten van betrokkenen te respecteren (art. 12 t/m 20 AVG), verplichtingen met betrekking tot internationale gegevensdoorgiften (art. 44 t/m 49 AVG) etc.

Interessant wordt de situatie waarin verschillende toezichthouders zich bevoegd achten een boete op te leggen voor een overtreding. Wie van hen mag de boete incasseren? Het antwoord op deze vraag is nog niet zo heel eenvoudig.[14]

Afsluiting

Er zijn nog talloze andere veranderingen die de verordening met zich brengt. Welke daarvan belangrijk zijn hangt af van wat de verwerkingsverantwoordelijke of verwerker met persoonsgegevens doet. Vast staat wel dat de verordening op een of andere manier betekenis gaat hebben voor vrijwel iedereen die zich bezighoudt met compliance.

[14] Lezersvraag: uw beantwoording van deze vraag kunt u binnen een maand na de verschijning van deze bijdrage naar de redactie van dit tijdschrift sturen. Onder de goede inzendingen wordt een exemplaar verloot van het standaardwerk P.C. Knol & G-J. Zwenne (red.), *Tekst & Commentaar Privacy- en telecommunicatierecht*, Kluwer Deventer 2015 (winkelwaarde ca. €297).