## Algemene verordening gegevensbescherming

# Waar gaat het heen met de Avg?

De Europese regels ter bescherming van persoonsgegevens worden hervormd in één Europese wet: de Algemene verordening gegevensbescherming (Avg). Deze hervorming beoogt verdergaande bescherming van persoonsgegevens. Hoe is deze hervorming tot stand gekomen, waar gaat het naartoe, en waarmee moet de informatieprofessional rekening houden?

***Joost Gerritsen***

Op 25 januari 2012 deed Eurocommissaris Vivian Reding namens de Europese Commissie een belangrijke mededeling. Zij maakte bekend dat de Europese regels ter bescherming van persoonsgegevens worden hervormd in één Europese wet: de Algemene verordening gegevensbescherming (Avg).
Sinds die dag is er veel gezegd en geschreven over de Avg, of specifieker uitgedrukt: het voorstel van de Europese Commissie voor een Avg. Het Europese wetgevingstraject bepaalt dat het Europees Parlement en de Raad van Ministers beide een eigen voorstel van de verordening formuleren, naast dat van de Commissie. In totaal zijn er dus drie voorstellen voor een Europese verordening die beoogt persoonsgegevens te beschermen, afkomstig van drie EU-organen: de Commissie, het Parlement en de Raad van Ministers.
Vanaf medio juni vergaderen de EU-organen periodiek met elkaar in een zogeheten triloog. De uitkomst van de triloog leidt tot één definitieve tekst en dat is dan dé verordening. De definitieve tekst voor de verordening is vermoedelijk medio 2016 gereed.
De Europese hervorming beoogt verdergaande bescherming zodra gegevens – data – te kwalificeren zijn als persoonsgegevens. Voor informatieprofessionals is dit belangrijk omdat gegevens al snel bestempeld kunnen worden als persoonsgegevens. Hoe is deze hervorming tot stand gekomen, waar gaat het naartoe, en waarmee moet de informatieprofessional rekening houden?

### Geschiedenis

Vandaag de dag geldt de Privacyrichtlijn[1] als de belangrijkste Europese rechtsbron voor de bescherming van persoonsgegevens. Die richtlijn dateert van 1995. Een jaar waarin het world wide web nog in de kinderschoenen stond. De online-diensten van Google, Facebook en Twitter bestonden nog niet. Slechts 1 procent van alle Europeanen had in de jaren 90 toegang tot het internet en daarmee tot online-diensten. Juist vanaf 1995 nam het aantal internetgebruikers enorm toe. Inmiddels maken 8 van de 10 Europeanen gebruik van het web en in Nederland is dat zelfs 9 van de 10 inwoners.
De regelgeving uit de jaren 90 is inmiddels verouderd en moet hervormd worden, aldus de Europese Commissie. Bovendien zorgde de Privacyrichtlijn ervoor dat alle 28 EU-lidstaten ieder een eigen nationale wet hebben die persoonsgegevens beschermt. Zo is in Nederland de richtlijn omgezet in de Wet bescherming persoonsgegevens (Wbp). De Wbp is niet geheel hetzelfde als de andere nationale wetten van de lidstaten. Hierdoor ontstaat een lappendeken aan wetgeving die soms tegenstrijdig is en een uniforme digitale markt in de weg staat, zo vindt de Commissie. Tijd voor hervorming.
Begin 2012 deed de Europese Commissie een

**[1] Richtlijn 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281).**

voorstel om de regels voor gegevensbescherming te hervormen met als hoofddoel één uniforme digitale markt. Hiervoor is consumentenvertrouwen essentieel. Persoonsgegevens zijn tegenwoordig immers het betaalmiddel van de digitale markt, zo verklaarde Eurocommissaris Reding in haar speech. Net als een betaalmiddel moet ook de markt van persoonsgegevens stabiel en betrouwbaar zijn. Het idee is dat als consumenten ervan overtuigd zijn dat hun persoonsgegevens zorgvuldig worden behandeld, zij online-diensten gaan gebruiken – en dat is goed voor de Europese markt.

Anders dan de Privacyrichtlijn is het de bedoeling dat de toekomstige verordening in Europa op dezelfde wijze wordt toegepast. Daarnaast biedt het consumenten en bedrijven meer duidelijkheid. Eurocommissaris Reding noemde daarnaast expliciet dat het voorstel van de Commissie tegemoetkomt aan innovatieve start-ups en het mkb. Deze bedrijfsgroepen kampen met hoge administratieve lasten om aan de huidige regels van de Privacyrichtlijn te voldoen. De nalevingskosten worden geraamd op jaarlijks 2,3 miljard euro. Zo zouden kleine bedrijven als hoofdregel geen Privacy Impact Assessment (PIA) hoeven uit te voeren, omdat dit een te grote belasting is.

De PIA en aanverwante begrippen worden uitgebreid beschreven in het artikel van Jeroen van Puijenbroek *(pagina 35)*.

Het voorstel van de Commissie werd met gemengde gevoelens ontvangen. Burgerrechtenorganisaties reageerden aanvankelijk enthousiast, omdat zij de voorgestelde verordening zien als een stap die burgers meer bescherming biedt. Het bedrijfsleven daarentegen toonde zich kritisch, omdat de verordening tegen de bedoeling in, zou leiden tot een toename van de administratieve lasten. Het zou ook de gebruiksmogelijkheden met persoonsgegevens te sterk beperken.

Het dossier over de hervorming werd met de Commissie-tekst van de verordening ondergebracht bij het Europees Parlement onder verantwoordelijkheid van rapporteur Jan Philipp Albrecht, Europarlementariër voor de Groenen. Er werd een recordaantal van 3.999 amendementen ingediend op het Commissie-voorstel.[2] Op 12 maart 2014 nam het Europees Parlement de voorgestelde tekst van de Commissie aan, met een reeks amendementen. De tekstvoorstellen van de Commissie en het Parlement zijn dan ook verschillend.

Op 15 juni 2015 is de Raad van Ministers het eens geworden over hun visie op het voorstel van de Commissie. Ook de Raad heeft een eigen 'versie' van de verordening opgesteld. Nu de drie voorstellen gereed zijn, zijn in juni 2015 de onderhandelingen gestart voor een definitieve tekst. Deze onderhandelingen moeten volgens de planning eind 2015 afgerond zijn.[3] Welke thema's komen dan zo al aan de orde, en welke voorstellen hebben de drie EU-organen hierover geformuleerd?

## Het recht om vergeten te worden

Eén van de meest besproken thema's is het 'recht om vergeten te worden'. Deze frase werd in 2014 bij het grote publiek bekend toen het Europees Hof van Justitie oordeelde over het verzoek van de heer Costeja. Hij verzocht Google om bepaalde zoekresultaten over hem te verwijderen. Volgens het Hof kan Google – op basis van de huidige Privacyrichtlijn – inderdaad verplicht zijn om in de zoekresultaten links te verwijderen naar websites zodra er via de zoekmachine werd gezocht naar, in dit geval, de heer Costeja.[4]

**Net als een betaalmiddel moet ook de markt van persoonsgegevens stabiel en betrouwbaar zijn**

Costeja's inmiddels irrelevante verleden kan op deze manier worden 'vergeten'.

De Commissie hecht veel waarde aan dit 'recht om vergeten te worden'. Dit recht omvat volgens het Commissie-voorstel ook de mogelijkheid voor mensen om hun persoonsgegevens te laten verwijderen als er geen gerechtvaardigde gronden zijn om de gegevens te bewaren.

Ook het Europees Parlement pleit in haar voorstel van de verordening voor een vergelijkbaar recht maar noemt dit een 'verwijderingsrecht'. Persoonsgegevens moeten op verzoek worden verwijderd als de gegevensverwerking niet in lijn is met de regels, de gegevens niet langer nodig zijn voor de doeleinden waarvoor ze destijds zijn verzameld, of als het individu zijn toestemming voor de gegevensverwerking intrekt. Dit betekent ook dat een partij die een verwijderverzoek ontvangt dit verzoek doorstuurt naar alle andere partijen in de keten die dezelfde gegevens hebben verwerkt.

**[2] Europees Parlement, 'Q&A on EU data protection reform' (http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform)**

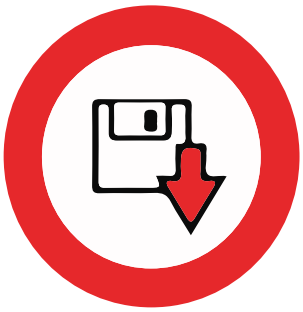
**[3] Persbericht Europese Commissie, 15 juni 2015, 'Ministers van Justitie steunen voorstel van de Commissie over nieuwe regels gegevensbescherming om digitale eengemaakte markt EU te stimuleren' (http://europa.eu/rapid/press-release_IP-15-5176_nl.htm)**

**[4] Persbericht Hof van Justitie van de Europese Unie, 13 mei 2014, 'Arrest in zaak C-131/12 Google Spain SL, Google Inc / Agencia Española de Protección de Datos, Mario Costeja González' (http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070nl.pdf)**

Uitzonderingen op dit recht blijven volgens het Parlement denkbaar, bijvoorbeeld wanneer de gegevensverwerking nodig is voor historische, statistische of wetenschappelijke doeleinden, omwille van de volksgezondheid of als het recht van vrijheid van meningsuiting zwaarder weegt. Het 'vergeetrecht' is ook niet van toepassing als de gegevensverwerking noodzakelijk is bij de uitvoering van een overeenkomst of als dit wettelijke verplicht is.
De Raad van Ministers benadrukt dat het 'recht om vergeten te worden' geen absoluut recht is. Er kunnen, volgens de Raad, goede redenen zijn om gegevens te blijven bewaren. Denk aan krantenarchieven. Het voorstel van de Raad van Ministers bepaalt dan ook expliciet dat het recht om vergeten te worden geen inbreuk mag maken op andermans recht op vrijheid van meningsuiting en van informatie.

## Profiling

Profiling is de verzameling en koppeling van gegevens om zo een 'profiel' op te kunnen stellen van een individu. Met behulp van geautomatiseerde processen worden op basis van dit profiel maatregelen en voorspellingen toegepast die effect hebben op het individu. Bijvoorbeeld de uitkomst van een berekening over diens kredietwaardigheid.
De Commissie noemt het recht van het individu om niet op basis van profiling aan een maatregel te worden onderworpen, maar geeft tegelijkertijd enkele uitzonderingen op basis waarvan profiling is toegestaan. Bijvoorbeeld als het opstellen van een profiel nodig is voor de uitoefening van een overeenkomst, als het is toegestaan op grond van de wet, of als het individu voor profiling toestemming geeft.
Het Europees Parlement denkt daar hetzelfde over, maar voegt daaraan toe dat profiling nooit mag leiden tot discriminatie en ook niet gebaseerd mag zijn op gevoelige gegevens, zoals gegevens over iemands etniciteit, politieke mening, religie, seksuele voorkeur, genetische of biometrische gegevens of strafbare gedragingen.
De Raad van Ministers hanteert een vergelijke bepaling over profiling als dat van de Commissie en het Parlement.
Het LIBE-comité, waarvan rapporteur Albrecht vice-voorzitter is, acht het daarbij van belang dat een mens betrokken blijft bij de geautomatiseerde processen. Een taak voor de informatieprofessional?



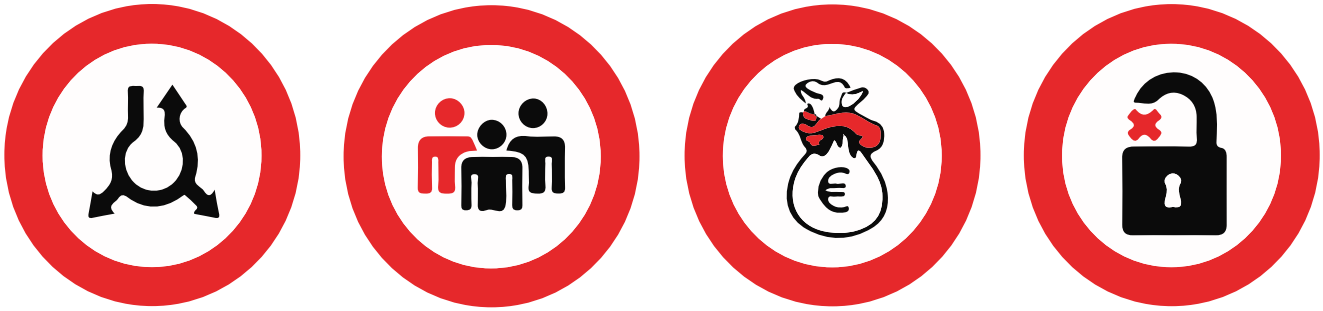
## Informatievoorziening en toestemming

***Informatievoorziening***

De Commissie vindt dat het individu moet worden voorzien in duidelijke informatie over hoe er met zijn persoonsgegevens wordt omgegaan. Een privacybeleid moet daarom worden opgesteld in heldere, begrijpelijke taal. Bedrijven moeten daarbij transparant zijn over het gegevensgebruik in privacy statements.
Het Europees Parlement vindt dit ook. Het parlement noemt daarnaast dat de taal van de informatie afgestemd moet zijn op de doelgroep, bijvoorbeeld kinderen. Als gegevens worden verzameld, dan moet aan de persoon waarop de gegevens betrekking hebben worden uitgelegd hoe deze data wordt verstrekt aan bijvoorbeeld commerciele partijen of deze data verkocht wordt en of er encryptie wordt toegepast. Ook moet er duidelijkheid worden verschaft over hoe lang de gegevens worden bewaard, wie de gegevens mogen ontvangen, of profielen worden toegepast, en hoe de individuen hun rechten – zoals het verwijderrecht – kunnen toepassen.
De Raad van Ministers is ook voorstander van duidelijke en eenvoudige taal in de informatievoorziening richting individuen, al ontbreken de 'privacy-iconen' (zie afbeelding) van het Europees Parlement in het voorstel van de Raad.

***Toestemming***

De Commissie vindt dat voor de verwerking van persoonsgegevens als hoofdregel geldt dat de betreffende persoon hiervoor zijn toestemming heeft gegeven. De toestemming kan niet worden 'verondersteld', maar moet uitdrukkelijk zijn gegeven.
Het Europees Parlement hanteert eenzelfde visie en voegt daaraan toe dat de toestemming ook op ieder moment eenvoudig kan worden ingetrokken. De toestemming kan worden gegeven als statement of bij een duidelijke, goedkeurende actie. Het LIBE-comité merkt daarbij op dat toestemming voor gegevensverwerking niet als voorwaarde mag worden gebruikt voor bijvoorbeeld het sluiten van een overeenkomst of bij gebruik-



making van een dienst. Zogeheten 'take it or leave it'-overeenkomsten zijn uit den boze. Daarbij vervalt de toestemming automatisch zodra de gegevens niet meer in lijn met de oorspronkelijke verwerkingsdoeleinden worden verwerkt.
Het voorstel van de Raad van Ministers bevat veel verwijzingen naar het toestemmingsbegrip en stelt onder andere dat toestemming niet wordt geacht vrijelijk te zijn verleend indien het individu geen echte vrije keuze heeft als hij zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.

## 'Data protection officer'

In Nederland kennen we sinds geruime tijd de functionaris voor de gegevensbescherming, ook wel de 'data protection officer' (DPO). Deze persoon vervult binnen een bedrijf of organisatie een functie waarin hij toezicht houdt op de zorgvuldige verwerking van persoonsgegevens. Een informatieprofessional zal zich thuis kunnen voelen in deze rol.
De Commissie vindt dit een belangrijke functie en meent dat alle overheidsorganisaties verplicht een DPO moeten aanstellen; commerciële bedrijven tot 250 werknemers hoeven dit niet te doen. Volgens VNO-NCW zullen er in Nederland ongeveer 25.000 DPO's aangesteld moeten worden. De taken van de DPO bestaan vooral uit informeren en adviseren over de gegevensverwerkingen, alsook het uitoefenen van toezicht. Ook is voor hem een rol weggelegd in het kader van 'privacy by design', 'privacy by default' en PIA's. DPO's moeten worden aangesteld voor een periode van twee jaar.
Ook het Europees Parlement vindt dat alle overheidsorganisaties een DPO moeten hebben. Met betrekking tot het bedrijfsleven wordt echter geen koppeling gemaakt met het aantal werknemers, maar is een DPO verplicht bij verschillende soorten risicovolle gegevensverwerkingen. Bijvoorbeeld indien de verwerking betrekking heeft op meer dan vijfduizend individuen (jaarlijks), bij gevoelige data zoals gegevens over locaties of kinderen, of als er mensen – bijvoorbeeld werknemers – gemonitord worden. DPO's moeten worden aangesteld voor een periode van vier jaar indien het een werknemer betreft, en twee jaar als het om een externe DPO gaat. Het LIBE-comité meent dat DPO's onafhankelijk moeten kunnen opereren en gedurende hun aanstelling niet ontslagen kunnen worden.
De Raad van Ministers beperkt de verplichting om een DPO aan te stellen tot 'gevallen waarin daaraan duidelijk behoefte is.' Een DPO is daarmee optioneel, waarbij EU-lidstaten zelf ervoor kunnen kiezen om een DPO verplicht te stellen.

## Internationaal gegevensverkeer

De huidige wet- en regelgeving bevatten ingewikkelde regelingen over hoe men dient om te gaan met persoonsgegevens die de Europese grenzen overschrijden of binnen internationale organisaties. Ook de verordening gaat hierop uitgebreid in. De Commissie stelt voorop dat persoonsgegevens alleen naar landen mogen worden gestuurd indien dat land een 'passend beschermingsniveau' heeft. De Commissie bepaalt welke landen dat zijn. Worden gegevens doorgegeven aan een land zonder goedkeuring van de Commissie, dan moet de dataverstrekker zorgen voor (contractuele) garanties met de ontvanger van de gegevens. Ook moeten bij internationale gegevensverwerkingen, bijvoorbeeld multinationals gebruik kunnen maken van gestroomlijnde goedkeuringsprocessen, zodat een eenmaal goedgekeurde BCR ('Binding Corporate Rules') overal in Europa geldt. BCR staat voor intern bindende gedragscodes voor gegevensbescherming in grote bedrijven.
Het Europees Parlement gaat mee met de ideeën van de Commissie over BCR's en contractuele garanties en benadrukt dat gegevens die in Europa verwerkt worden niet zomaar aan derde partijen mogen worden verstrekt. Als een land buiten Europa aan bijvoorbeeld een zoekmachine of cloudprovider vraagt om persoonsgegevens uit de EU te verstrekken, dan moet de aangezochte partij hiervoor eerst toestemming vragen bij zijn nationale toezichthouder. Ook moet de persoon waarop de gegevens betrekking hebben op de hoogte worden gebracht over de voorgenomen dataverstrekking.

**Ten behoeve van de informatievoorziening heeft het Europees Parlement een reeks 'privacy-iconen' ontworpen.**

Ook moet er volgens het parlement een 'Europese Gegevensbeschermingszegel' worden ingevoerd, waarmee de houder van het zegel laat zien dat zijn gegevensverwerkingen in lijn zijn met de Europese regelgeving. Niet-Europese bedrijven zouden een dergelijke zegel ook kunnen ontvangen.
De Raad van Europa noemt dat ook door de toezichthouder goedgekeurde gedragscodes en certificeringsmechanismen ervoor kunnen zorgen dat internationaal gegevensverkeer mogelijk is naar een land zonder passend beschermingsniveau.

## 'One-stop-shop'

Bij de discussies over de verordening is veel te doen geweest over de zogeheten 'one-stop-shop'. Het idee achter de one-stop-shop is dat Europeanen slechts rekening hoeven te houden met één toezichthoudend loket. Volgens de Commissie hoeft een bedrijf slechts rekening te houden met één toezichthouder die als one-stop-shop fungeert. Dit is de toezichthouder in het land van de hoofdvestiging van het betreffende bedrijf. Voor individuen betekent het principe van one-stop-shop dat zij met klachten altijd terecht kunnen bij de toezichthouder uit hun eigen land, zelfs als de gegevens zijn verwerkt door een organisatie van buiten de EU.
Het Europees Parlement introduceert een toezichthouder die de leiding heeft over de gegevensverwerking van een bedrijf, de zogeheten 'lead Data Protection Authority'. De 'lead DPA' komt uit het land waarin het bedrijf in Europa zijn hoofdvestiging heeft en neemt de leiding zodra er maatregelen tegen dat bedrijf moeten worden genomen. De lead DPA kan als enige toezichthouder boetes en dergelijke opleggen. Zo nodig pleegt de lead DPA overleg met andere toezichthouders, bijvoorbeeld een toezichthouder uit het land van de klager. Als de toezichthouders er met elkaar niet uitkomen over de aanpak van een zaak, dan kan een procedure van de 'European Data Protection Board' soelaas bieden. Dit nieuwe instituut coördineert de grensoverschrijdende handhavingsacties van toezichthouders.
Het voorstel van het Parlement bepaalt daarnaast dat als individuen beklag willen doen over bijvoorbeeld een internetbedrijf gevestigd in een andere EU-lidstaat, zij deze klacht kunnen neerleggen bij een toezichthouder naar keuze: gevestigd in het eigen land of in het land van het internetbedrijf. Zo kunnen klachten worden ingediend in de eigen taal.

Het tekstvoorstel van de Raad houdt in dat alleen in grote transnationale zaken een beroep op het principe van one-stop-shop kan worden gedaan. Vervolgens werken de betrokken toezichthouders dan samen en nemen zij samen een besluit. Om het individu en de beslissingsinstantie dichter bij elkaar te brengen, wordt het gezamenlijk besluit vastgesteld door de toezichthouder die het best in staat is om vanuit het oogpunt van het individu de meest doeltreffende bescherming te bieden. Dit is een lange en complexe procedure.

## Meldplicht bij datalekken

Een datalek komt erop neer dat de beveiliging van persoonsgegevens is doorbroken of dat persoonsgegevens zijn vernietigd, verloren of verstrekt als gevolg van ongeoorloofde verstrekking of toegang tot de gegevens. Kortom: de gegevens liggen op straat of kúnnen op straat liggen, terwijl dat niet de bedoeling is. In aanloop naar de verordening wordt in Nederland al op 1 januari 2016 een meldplicht voor datalekken verplicht gesteld. *(Zie hierover het artikel van Rutger Alsbach en Saskia Sjardin op pagina 14)*.
De Commissie noemt in haar voorstel dat datalekken binnen 24 uur na de ontdekking van het lek worden gemeld bij de toezichthouder. Als het datalek waarschijnlijk negatieve gevolgen heeft voor de privacy van individuen, dan moeten ook de betreffende individuen hierover geïnformeerd worden. Het Europees Parlement denkt er ongeveer hetzelfde over als de Commissie.
In het voorstel van de Raad van Ministers maakt de meldplicht datalekken onderdeel uit van een breder concept, de zogeheten risico-georiënteerde benadering. De meldplicht datalekken komt daarom pas aan de orde als er sprake is van een hoog risico voor de individuen. Het voorstel van de Raad kent dan ook verschillende uitzonderingen op de regel dat er gemeld moet worden bij de toezichthouder of het individu.

## Handhaving en boetes

Dankzij nationale wetgeving kan de Nederlandse toezichthouder waarschijnlijk vanaf 1 januari 2016 boetes opleggen tot 810.000 euro of 10 procent van de jaaromzet van de overtreder.[5] De verordening zal ook een boetebevoegdheid bevatten, maar de drie EU-organen hanteren verschillende ideeën over de bandbreedte van die boetes.
De Commissie hanteert drie categorieën boetes. De laagste boetecategorie is 250.000 euro of 0,5

**[5] Auteurs Rutger Alsbach en Saskia Sjardin gaan in hun artikel meer uitgebreid in op deze uitbreiding van bevoegdheden.**

## Waarmee dient de informatieprofessional rekening te houden?

De verschillende thema's uit de verordening, in dit artikel op hoofdlijnen uiteengezet, laten zien dat wie persoonsgegevens verwerkt met heel wat nieuwe regels rekening dient te houden. In sommige gevallen zijn de regels uit de verordening compleet nieuw, zoals het one-stop-shop-principe of de regels over internationaal gegevensverkeer. Ook zijn er thema's die in Nederland al actueel worden vóórdat de verordening in werking treedt: denk aan de meldplicht datalekken en de uitbreiding van de boetebevoegdheid van de toezichthouder. In andere gevallen gaat het om bestaande regels die meer worden aangekleed, bijvoorbeeld het recht om vergeten te worden en de informatievoorziening en toestemming van individuen. Daarnaast bestaat er nu al een functionaris voor de gegevensbescherming, maar als dergelijke DPO's in de toekomst verplicht worden dan is dit mogelijk een mooie kans voor de informatieprofessional.

Hoewel de regels nog niet in marmer zijn gebeiteld, doet de informatieprofessional er in ieder geval verstandig aan om rekening te houden met de volgende thema's die die nu al gelden:

- De rechten van de individuen: Hoe ga je als organisatie om met verzoeken om 'vergeten te worden'? Zijn de systemen in staat om gegevens permanent te verwijderen, als dat nodig is?
- Profiling: Maakt de organisatie keuzes op basis van geautomatiseerde processen die rechtsgevolgen hebben voor individuen? Zo ja, is er een persoon die dit proces overziet?
- Informatievoorziening en toestemming: Hoe is de informatievoorziening geregeld naar het individu toe? Is alles duidelijk genoeg? Moet voor de verwerking toestemming worden gevraagd? Zo neen, wat is dan de grondslag voor de gegevensverwerking?

procent van de jaarlijkse – wereldwijde – omzet van de overtreder. Boetes voor overtredingen uit de middelste categorie bestaan uit 500.000 euro of 1 procent van de jaarlijkse omzet. De hoogste boetecategorie kent een boete van 1 miljoen euro of 2 procent van de jaaromzet van de overtreder. De toezichthouder is vrij te kiezen voor het boetebedrag genoemd in euro's of het percentage van de omzet, het grootste bedrag geldt uiteindelijk. Voor first offenders zullen toezichthouders waarschijnlijk eerst een waarschuwingsbrief sturen, maar bij serieuze overtredingen kunnen direct boetes worden opgelegd. Bijvoorbeeld in gevallen waarin er gevoelige gegevens worden verwerkt zonder toestemming. Een voorbeeld van de laagste boetecategorie is het geval waarin een bedrijf ongeoorloofd hoge bedragen vraagt voor de afhandeling van een verzoek persoonsgegevens te verwijderen of in te zien. Bij overtredingen uit de middelste categorie kan gedacht worden aan een bedrijf dat geen informatievoorziening over de verwerking verstrekt of dat weigert persoonsgegevens te corrigeren.

Het Europees Parlement vindt dat er bij minder ernstige overtredingen eerst een schriftelijke waarschuwing moet zijn van de toezichthouder. Ook kunnen periodieke audits worden opgelegd. De boetes die door het Parlement worden opgelegd zijn hoger dan de eerdere genoemde boetes: maximaal 100 miljoen euro of 5 procent van de wereldwijde jaarlijkse omzet, welk bedrag maar hoger is.

Het Parlement vindt dat diverse omstandigheden een rol spelen bij de vaststelling van de handhavende maatregel, bijvoorbeeld de duur van de privacy-inbreuk, de mate van nalatigheid, de bereidheid om mee te werken en de omvang van de aangerichte schade als gevolg van de niet-naleving van de verordening. De Raad van Ministers hanteert dezelfde boetecategorieën als de Europese Commissie maar vindt dat de boetecategorieën als glijdende schaal in elkaar overlopen.

**Volgens VNO-NCW zullen er ongeveer 25.000 'data protection officers' aangesteld moeten worden**

Als alles goed gaat, dan wordt medio 2016 onder Nederlands voorzitterschap duidelijk hoe de definitieve tekst van de Avg eruit ziet. De verordening treedt dan twintig dagen na publicatie in werking. Naar verwachting wordt er een overgangstermijn van twee jaar in acht genomen. Dit betekent dat bedrijven en organisaties tot medio 2018 de tijd hebben om volledig te voldoen aan de Algemene verordening gegevensbescherming.

*Mr. Joost Gerritsen (joostgerritsen@degierstam.nl) is advocaat informatietechnologie & privacyrecht bij De Gier | Stam & Advocaten te Utrecht.*