# 91. De Algemene Verordening Gegevensbescherming[1]

MW. MR. N.M. BROUWER

**Op 25 mei 2018 treedt de Europese Algemene Verordening Gegevensbescherming ('AVG') in werking. Deze Verordening vervangt de huidige Europese Richtlijn 95/46/EG ('de Richtlijn') en de daarop gebaseerde Nederlandse Wet bescherming persoonsgegevens ('Wbp'). Hoewel de AVG grotendeels voortbouwt op reeds bestaande beginselen, introduceert zij een aantal nieuwe elementen die grote invloed kunnen hebben op organisaties. Door een groter toepassingsbereik, een sterkere positie voor betrokkenen, extra verplichtingen voor organisaties en meer nadruk op compliance zullen privacy en gegevensbescherming hoger op de agenda moeten komen te staan.**

## 1. Inleiding

Door razendsnelle technologische ontwikkelingen, digitalisering en globalisering worden tegenwoordig enorme hoeveelheden data verzameld. Vrijwel iedere organisatie verwerkt persoonsgegevens. Het gaat dan niet alleen om grote organisaties zoals ziekenhuizen, verzekeringsmaatschappijen of scholen, maar ook om de lokale kapper met een klantensysteem of de sportvereniging met een ledenbestand. Alle organisaties die persoonsgegevens verwerken, hebben te maken met privacyregelgeving.

Tot 24 mei waren de regels neergelegd in de Wbp.[2] De Wbp vloeide voort uit de Europese Richtlijn uit 1995.[3] Op 25 mei 2018 is echter de AVG, een Europese verordening, inwerking getreden. Doordat Europese verordeningen rechtstreekse werking hebben, komen de Richtlijn en de Wbp vanaf dat moment te vervallen.

In dit artikel wordt een aantal elementen uit de AVG uitgelicht en wordt bekeken wat daarvan de betekenis kan zijn voor de praktijk.

## 2. Gegevensbescherming: van beginselen tot Verordening

Privacy is als fundamenteel mensenrecht neergelegd in verschillende mensenrechtenverdragen en in Nederland in de Grondwet.[4] Met de opkomst van de informatiemaatschappij is de nadruk steeds meer komen te liggen op het informationele aspect van privacy: de bescherming van persoonlijke gegevens. Het recht op gegevensbescherming is zelfstandig gecodificeerd in artikel 16 VWEU[5] en artikel 8 EU-Grondrechtenhandvest.[6]

Ondanks dat de Richtlijn was gebaseerd op breed gedragen beginselen[7] en harmonisatie werd nagestreefd,[8] is als gevolg van verschillende wijzen van implementatie door de afzonderlijke lidstaten een gefragmenteerd beschermingsniveau ontstaan. Hierdoor ontstaat rechtsonzekerheid en wordt de interne markt belemmerd.[9] Deze ontwikkelingen kunnen bovendien een bedreiging vormen voor de bescherming van de grondrechten en vrijheden van natuurlijke personen.

Het doel van de AVG is derhalve tweeledig: ten eerste streeft de AVG naar een hoger beschermingsniveau van de grondrechten. Ten tweede beoogt de AVG door meer harmonisatie de belemmeringen voor het vrije verkeer van persoonsgegevens weg te nemen. Er moet gezorgd worden voor een 'coherente en homogene toepassing' van het gegevensbeschermingsrecht.[10] Daarvoor is een verordening nodig,

1 Verordening (EU) 2016/679.

2 Naast de Wbp zijn er ook in andere wetten bepalingen rondom gegevensbescherming te vinden, zoals de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens en de Telecommunicatiewet. Deze wetten worden in dit artikel niet behandeld.

3 Richtlijn 95/46/EG.

4 Artikel 12 Universele Verklaring voor de Rechten van de Mens; artikel 17 IVBPR; artikel 8 EVRM; artikel 10 Gw.

5 Verdrag betreffende de Werking van de Europese Unie, *PbEU* 2010, C 83/47.

6 Handvest van de Grondrechten van de Europese Unie, 7 december 2000, PbEG 2000 C 364/1.

7 Deze beginselen (de '*Privacy Principles*') zijn in 1980 opgesteld door de Europese Organisatie voor Economische Samenwerking en Ontwikkeling (OESO). De *Principles* zijn te raadplegen op http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

8 Zie bijvoorbeeld HvJ EU 24 november 2011, ECLI:EU:C:2011:777 (*Asnef*).

9 Zie overwegingen 6 t/m 10 AVG.

10 Overweging 10 AVG. Het verdient de opmerking dat de AVG de Lidstaten op meerdere punten ruimte geeft om met nationale wetgeving keuzes te maken, hetgeen een belemmering kan vormen voor daadwerkelijke harmonisatie. In Nederland is deze keuzeruimte ingevuld met (het voorstel voor) de Uitvoeringswet AVG, *Kamerstukken II* 2017/18, 34851, 1-23.

waarin de rechten van betrokkenen worden versterkt, de verplichtingen voor verantwoordelijken en verwerkers worden uitgebreid, naleving van de verordening consistent wordt gehandhaafd en overtredingen gesanctioneerd.[11]
Van een echte aardverschuiving in het gegevensbeschermingsrecht is echter geen sprake. De AVG bouwt inhoudelijk grotendeels voort op de beginselen van gegevensbescherming uit de Richtlijn: rechtmatigheid, behoorlijkheid, transparantie, doelbinding, dataminimalisatie, juistheid, opslagbeperking, integriteit en vertrouwelijkheid. Toch is er zeker een aantal (ver)nieuw(d)e elementen aan te wijzen die grote invloed kunnen hebben op de praktijk. In deze bijdrage bespreek ik een aantal van deze elementen. Ik houd daarbij qua volgordelijkheid in grote lijnen de structuur van de AVG aan.

## 3. Terminologie

De AVG introduceert een aantal nieuwe begrippen, die inhoudelijk niet altijd verschillen met de begrippen die reeds in de Wbp werden gehanteerd: de 'verantwoordelijke' wordt de 'verwerkingsverantwoordelijke',[12] de 'bewerker' wordt de 'verwerker'.[13] Een aantal begrippen dat al wel bekend was maar nog niet in regelgeving was neergelegd, wordt in de AVG gecodificeerd en voorziet onze taal van prachtige nieuwe scrabble-woorden. Voorbeelden zijn de 'gegevensbeschermingseffectbeoordeling' (artikel 35 AVG), pseudonimisering (artikel 4 sub 5 AVG), bindende bedrijfsvoorschriften (artikel 4 sub 20 AVG) en de verantwoordingsplicht (artikel 5 lid 2 AVG).

## 4. Ruimer toepassingsbereik

De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Bij handmatige verwerking is de AVG van toepassing als de gegevens zijn opgenomen in een bestand[14] (artikel 2 lid 1 AVG). 'Persoonsgegevens' is een ruim begrip en omvat alle informatie over een geïdentificeerde of (direct of indirect) identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG). Het begrip 'verwerking' dient ook ruim te worden opgevat en omvat in feite ieder werkwoord, zoals het verzamelen, vastleggen, structureren, bewerken, wijzigen, of gebruiken van persoonsgegevens (artikel 4 sub 2 AVG).[15]

Het materiële toepassingsgebied van de AVG is hiermee gelijk aan dat van de Richtlijn. Het territoriale toepassingsgebied van de AVG is echter ruimer. De AVG is van toepassing op organisaties die in de Europese Unie ('EU') gevestigd zijn, ook als de verwerking zelf niet in de EU plaatsvindt. Anders dan onder de Richtlijn het geval was, geldt dit niet alleen voor vestigingen van de verwerkingsverantwoordelijke, maar ook voor de verwerker (artikel 3 lid 1 AVG).[16]
Daarnaast is de AVG van toepassing op organisaties die niet in de EU zijn gevestigd, maar die wel persoonsgegevens van EU-burgers verwerken, mits de verwerking verband houdt met (1) het aanbieden van goederen of diensten aan deze betrokkenen, waarbij betaling niet is vereist, of (2) het monitoren van het gedrag van deze betrokkenen, voor zover dat in de Unie plaatsvindt (artikel 3 lid 2 AVG). Deze nieuwe toepasselijkheidsregels verruimen de reikwijdte van de AVG aanzienlijk en maken heel wat niet-EU-bedrijven zenuwachtig. Zo kan bijvoorbeeld een Amerikaans bedrijf zonder vestigingen in de EU, maar dat wel persoonsgegevens van EU-burgers verwerkt, onder de AVG vallen. Dit ruime toepassingsbereik onderstreept de waarde die de AVG hecht aan de bescherming van persoonsgegevens van EU-burgers en haakt aan bij hedendaagse grensoverschrijdende (gratis) diensten, zoals clouddiensten of e-mailservices.

## 5. Verplichtingen voor verwerkingsverantwoordelijken én verwerkers

De AVG legt een sterke nadruk op het accountability-beginsel, wat is neergelegd in artikel 5 lid 2 AVG: "*De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 [de beginselen van gegevensverwerking] en kan deze aantonen ('verantwoordingsplicht')*". Dit is een belangrijk uitgangspunt voor verwerkingsverantwoordelijken, omdat dit nogal wat nieuwe verplichtingen met zich brengt.

> Niet alleen dient de verwerkingsverantwoordelijke te voldoen aan de beginselen van gegevensverwerking, hij moet dit ook kunnen laten zien

Niet alleen dient de verwerkingsverantwoordelijke te voldoen aan de beginselen van gegevensverwerking, hij moet dit ook kunnen laten zien. De verwerkingsverantwoordelijke dient passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd (artikel 24 AVG). Die maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd.

11 Overwegingen 11 t/m 13 AVG.
12 De partij die het doel en de middelen van de verwerking van persoonsgegevens vaststelt (artikel 4 sub 7 AVG en 1 sub d Wbp).
13 De partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder daarbij zeggenschap te hebben over het doel of de middelen van de verwerking (artikel 4 sub 8 AVG en artikel 1 sub e Wbp).
14 Bestand: een gestructureerd geheel van persoonsgegevens, artikel 4 sub 6 AVG.
15 Verwerkingen met het oog op openbare veiligheid, het opsporen van strafbare feiten of verwerkingen door een natuurlijk persoon voor zuiver persoonlijke of huishoudelijke activiteiten zijn uitgezonderd (artikel 2 lid 2 AVG).
16 Zie ook HvJ EU 13 mei 2014, C-131/12 (*Google Spain/Costeja*).

Waar nodig moet bovendien een gegevensbeschermingsbeleid worden ingericht.
Het verantwoordingsbeginsel impliceert dus een continu proces van afwegingen. Deze afwegingen dienen op transparante wijze te worden vastgelegd, zodat de verwerkingsverantwoordelijke kan aantonen dat hij voldoet aan de verplichtingen ('compliant' is).[17]
De AVG schrijft een aantal verplichtingen voor die de verwerkingsverantwoordelijke kan (moet) gebruiken om zijn verwerkingen te kunnen verantwoorden, zoals het bijhouden van een verwerkingsregister (artikel 30 AVG), het uitvoeren van een gegevensbeschermingseffectbeoordeling (artikel 35 AVG) en het aanstellen van een Functionaris Gegevensbescherming (artikel 37 AVG).[18]
Een belangrijk verschil tussen het oude recht en de AVG is dat een deel van deze verplichtingen niet langer alleen voor de verwerkingsverantwoordelijke, maar ook voor de verwerker geldt. De verwerker kan rechtstreeks worden aangesproken op de naleving daarvan. Onder de AVG is het dus van groot belang dat verwerkers en verwerkingsverantwoordelijken de onderlinge verdeling van verantwoordelijkheden contractueel goed vastleggen in de (verplichte) verwerkingsovereenkomst.[19]

### 5.1 Registerplicht

De verantwoordelijke én de verwerker dienen zelf een register van verwerkingsactiviteiten bij te houden (artikel 30 AVG). Dit is een belangrijk verschil met de Wbp, waarin verwerkingen niet door de verantwoordelijke zelf hoefden te worden bijgehouden, maar juist vooraf aan de Autoriteit Persoonsgegevens ('AP') of de Functionaris Gegevensbescherming ('FG') dienden te worden gemeld (artikelen 27-30 Wbp).[20]
Dit register van verwerkingsactiviteiten vormt enerzijds een goede prikkel voor bedrijven om hun verwerkingen in kaart te brengen en op die manier een heldere basis voor (verdere) compliance te creëren. Anderzijds kan het een enorme klus zijn om het register aan te leggen,[21] met name voor het MKB waarbij niet altijd de benodigde middelen aanwezig zullen zijn. In artikel 30 lid 5 AVG worden bedrijven met minder dan 250 medewerkers daarom van de registerplicht uitgezonderd. Let wel, dit is weer niet het geval indien de verwerking een risico inhoudt voor de rechten en vrijheden van betrokkenen, als de verwerking niet incidenteel is of als het bijzondere persoonsgegevens (artikel 9 AVG) betreft. Om te bepalen of zij wel of niet aan de registerplicht moeten voldoen, zullen ook MKB-ondernemingen dus alsnog een risico-inventarisatie moeten verrichten. Men kan zich zelfs afvragen of deze toevoeging aan artikel 30 lid 5 de MKB-uitzondering niet grotendeels illusoir maakt. Welk bedrijf verwerkt immers slechts 'incidenteel' gegevens? Zoals Schermer ook terecht heeft opgemerkt, is alleen al het gebruik maken van e-mail of een klantenbestand een structurele verwerking.[22]
Het maken en bijhouden van het verwerkingsregister roept daarnaast ook andere praktische vragen op. Wie beheert het register? Hoe wordt het actueel gehouden? Hoe gedetailleerd moet het zijn? De AVG geeft hier niet direct antwoord op; de praktijk zal dit moeten uitwijzen.

### 5.2 Privacy by design and by default

Een ander voorbeeld van een instrument voor accountability is de verplichting om systemen technisch en organisatorisch zodanig in te richten (bijvoorbeeld door pseudonimisering) dat zoveel mogelijk rekening wordt gehouden met de beginselen van gegevensbescherming, bijvoorbeeld dataminimalisatie (privacy by design and by default, artikel 25 AVG). Een bedrijf kan zich dus niet langer verschuilen achter 'het systeem' en moet kunnen uitleggen waarom de gevraagde gegevens daadwerkelijk benodigd zijn.[23]

### 5.3 Gegevensbeschermingseffectbeoordeling / privacy impact assessment ('PIA')

In bepaalde gevallen dient de verwerkingsverantwoordelijke voorafgaand aan de verwerking een PIA uit te voeren. Een PIA moet worden uitgevoerd indien de verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 35 lid 1 AVG). Het gaat dan met name om geautomatiseerde verwerkingen (profilering), grootschalige verwerking van bijzondere persoonsgegevens en stelselmatige monitoring van openbaar toegankelijke ruimten (artikel 35 lid 3 AVG).
Bij een ziekenhuisinformatiesysteem, automatische nummerplaatherkenning, of een fraudedatabank dient een PIA te worden uitgevoerd. Een individuele arts of advocaat die gegevens van patiënten en cliënten verwerkt, kan een PIA achterwege laten,[24] net als het online tijdschrift dat zijn mailinglist gebruikt om de abonnees dagelijks een bericht toe te sturen.[25] Het door de wetgever gekozen voorbeeld

17 De introductie van verplichtingen in de sfeer van 'compliance' wordt ook wel gezien als een van de grootste veranderingen van de AVG, zie M. Jansen, 'AVG en beveiliging: passende maatregelen voortaan proactiever nemen en monitoren', *Computerrecht* 2017/152, p. 208-216.

18 Zie in dit kader ook D.E. Comijs, 'Accountability in de AVG: betere processen en een sterkere positie voor betrokkenen', *P&I* 2016/6, p. 253 en B.W. Schermer, 'Van meldplicht naar registerplicht: de registratie van verwerkingen onder de AVG', *Computerrecht* 2017/151, p. 203-207.

19 Zie over de verhouding tussen de verwerkingsverantwoordelijke en de verwerker uitgebreid T. van de Bunt en A. Strijbos, 'De bewerkersovereenkomst onder de AVG', *NJB* 2018/357, p. 479-485.

20 Zie hiervoor uitgebreid B.W. Schermer, 'Van meldplicht naar registerplicht: de registratie van verwerkingen onder de AVG', *Computerrecht* 2017/151, p. 203-207.

21 Hierbij zij opgemerkt dat de inhoud van het verwerkingsregister deels kan overeenkomen met hetgeen het transparantiebeginsel vereist. Organisaties kunnen dus twee vliegen in één klap slaan. Zie uitgebreid over transparantie WP29, 'Guidelines on transparency under Regulation 2016/679', 17/EN, WP260.

22 Idem noot 19.

23 Zie uitgebreider M. Jansen, 'AVG en beveiliging: passende maatregelen voortaan proactiever nemen en monitoren', *Computerrecht* 2017/152, p. 208-216.

24 Overweging 91 AVG.

25 Zie voor gedetailleerde toelichting en meer voorbeelden de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen van de WP29, 17/NL, WP248 rev.01, te raadplegen op https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf.

van de individuele arts en advocaat acht ik wat ongelukkig. Het feit dat het om een individuele arts of advocaat gaat, zegt immers niets over de mate waarin de (vaak zeer gevoelige) gegevens worden verwerkt. Het voorbeeld maakt daarom niet duidelijk wanneer nu wel of niet een PIA moet worden uitgevoerd. Integendeel, het roept juist vragen op hoe de criteria grootschaligheid en aard van de gegevens moeten worden geïnterpreteerd en gewaardeerd.

**5.4 Beveiligingsverplichtingen**

Net als in de Richtlijn zijn in de AVG verschillende beveiligingsverplichtingen opgenomen (artikel 32 AVG). Verwerkersverantwoordelijken én verwerkers dienen passende technische en organisatorische maatregelen te treffen. Wat voor maatregelen dat zijn, vermeldt de AVG niet. Wel noemt de AVG een aantal voorbeelden, zoals pseudonimisering en versleuteling. Bovendien blijkt uit artikel 32 lid 1 sub b-d AVG dat het treffen van beveiligingsmaatregelen niet een eenmalige actie, maar een continu proces dient te zijn. De lat voor te treffen beveiligingsmaatregelen wordt blijkens de rechtspraak hoog gelegd.[26]

Het niveau van beveiliging is afhankelijk van het risico van de verwerking, waarbij ook rekening mag worden gehouden met uitvoeringskosten. Dit betekent dat van het grote ziekenhuis, dat met een grote hoeveelheid zeer gevoelige gegevens werkt, meer mag worden verwacht dan van de kapper op de hoek.

Gezien de nadruk van de AVG op de bescherming van de rechten van betrokkenen in combinatie met de verantwoordingsplicht is het voor iedere organisatie (groot en klein) aan te raden om op papier te zetten welke beveiligingsmaatregelen zijn getroffen en waarom. Afhankelijk van de verwerkingsactiviteiten kan een beveiligingsbeleid bovendien verplicht zijn op grond van artikel 24 lid 2 AVG.

**5.5 Meldplicht datalekken**

De introductie van de Wet meldplicht datalekken (artikel 34a Wbp) op 1 januari 2016 heeft in Nederland al de nodige stof doen opwaaien. De meldplicht datalekken die in de AVG is opgenomen (artikel 33 en 34 AVG), is voor Nederland dus minder nieuw dan voor de meeste andere Europese lidstaten.

De term 'datalek' komt in de AVG overigens niet voor; de AVG spreekt van een 'inbreuk in verband met persoonsgegevens'. Dit houdt in een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot bijvoorbeeld verlies, vernietiging of ongeoorloofde verstrekking van gegevens (artikel 4 sub 12 AVG).

De verwerkingsverantwoordelijke dient de inbreuk te melden aan Autoriteit Persoonsgegevens ('AP'). Dit dient te geschieden zonder onredelijke vertraging, maar uiterlijk binnen 72 uur nadat een redelijke mate van zekerheid is verkregen dat sprake is van een inbreuk die tot een risico voor persoonsgegevens leidt.[27]

De WP29[28] had eerder het standpunt ingenomen dat de termijn van 72 uur al zou beginnen te lopen na kennisname door de verwerker.[29] In de laatst aangepaste versie van de Guidelines lijkt zij daarop te zijn teruggekomen en benadrukt zij dat het niet de verwerker is die de eerste risicoanalyse hoeft uit te voeren na een inbreuk. Dat is de verantwoordelijke. De verwerker dient vast te stellen of sprake is van een inbreuk en moet dan onmiddellijk ('promptly')[30] de verwerkingsverantwoordelijke inlichten. De termijn van 72 uur gaat dus lopen op het moment dat de verwerkingsverantwoordelijke door de verwerker van de inbreuk op de hoogte is gesteld.[31]

De meldingssystematiek verandert kort gezegd van 'melden, mits ernstig risico' (Wbp) naar 'melden, tenzij geen risico'(AVG). Melding kan achterwege blijven indien de verwerkingsverantwoordelijke conform het accountability-beginsel kan aantonen dat het onwaarschijnlijk is dat de inbreuk een risico vormt voor de rechten en vrijheden van natuurlijke personen. Deze formulering verschilt van de huidige Wbp, waarin wordt gesproken van '(een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens'. Of de AVG hiermee een andere meldingsdrempel heeft geïntroduceerd, blijkt hier niet duidelijk uit. Wat daar ook van zij, in beide gevallen dient in een zeer korte tijd een risicoanalyse te worden gemaakt.

Indien sprake is van een waarschijnlijk hoog risico voor de rechten en vrijheden van natuurlijke personen, dan moet niet alleen de AP, maar ook de betrokkenen worden ingelicht. Bij adequate versleuteling van de gegevens hoeft dit niet. Indien mededeling aan iedere betrokkene onevenredige inspanningen zou vergen, dan kan worden volstaan met bijvoorbeeld een openbare mededeling (artikel 34 lid 3 sub a-c AVG).

In de praktijk zullen veel verwerkingsverantwoordelijken de verwerking hebben uitbesteed aan een derde partij, de verwerker. De kans dat een inbreuk niet bij de verwerkingsverantwoordelijke, maar bij de verwerker plaatsvindt, is dan ook reëel. Een goede uitvoering van de meldplicht vergt daarom een goede samenwerking tussen de verwerker en de verwerkingsverantwoordelijke. De verwerker dient contractueel te worden verplicht om de verwerkingsverantwoordelijke te helpen bij de meldplicht (artikel 28 lid 3 sub f AVG). De verwerker wordt bovendien in artikel 33 lid 2 AVG expliciet verplicht om een inbreuk zonder onre-

26 Zie bijvoorbeeld Hof van Justitie EU, 8 april 2014, C-293/12 en C-594/12 (*Digital Rights Ireland*).

27 Zie ook de concept Guidelines van de WP29 over datalekken (Guidelines on personal breach notification under Regulation 2016/679, 17/EN, WP 250rev.01, p. 11. Te raadplegen op <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827>

28 Article 29 Working Party, een Europees adviesorgaan bestaande uit vertegenwoordigers van de toezichthoudende autoriteit uit iedere lidstaat.

29 WP 29, Guidelines on personal data breach notification under Regulation 2016/679 (17/EN, WP 250), p. 11, te raadplegen op <https://tinyurl.com/y7ekv726>.

30 *Ibid* nt. 25, p. 14.

31 *Ibid*, p. 13.

delijke vertraging aan de verwerkingsverantwoordelijke te melden. Gezien de korte termijn voor de melding en de uitgebreide handhavingsbevoegdheden van de AP (zie ook hierna), doen verwerkers en verwerkingsverantwoordelijkheden er goed aan om de verwerkingsovereenkomsten op dit punt te controleren en waar nodig aan te passen.
Vanwege de korte meldingstermijn zullen bedrijven ervoor moeten zorgen dat ze een goed meldingsprotocol en risk assessment model hebben klaarstaan. De informatie die de organisatie reeds over de eigen verwerkingen heeft, bijvoorbeeld door het verwerkingsregister of door een PIA, kan daarbij behulpzaam zijn. Daarbij moet in het oog worden gehouden dat een PIA niet hetzelfde is als een risicoanalyse na een inbreuk. Een PIA ziet immers op hypothetische gevallen, terwijl na een inbreuk de focus op de daadwerkelijke gevolgen dient te worden gelegd.[32] Een bedrijf dat zijn eigen verwerkingen en datastromen goed in beeld heeft, zal evenwel sneller en beter aan de meldplicht kunnen voldoen.

**5.6 Functionaris Gegevensbescherming ('FG')[33]**
Onder de oude wetgeving is het aanstellen van een FG niet verplicht (artikel 62 Wbp). Dit is anders onder de AVG: een FG is verplicht voor overheidsinstellingen en -organen, voor organisaties die zich hoofdzakelijk bezighouden met regelmatige en stelselmatige observatie op grote schaal en organisaties die zich hoofdzakelijk bezighouden met het verwerken van bijzondere persoonsgegevens (artikel 37 lid 1 sub a-c AVG). Dit geldt zowel voor verwerkingsverantwoordelijken als voor verwerkers.
Ook voor dit onderwerp heeft de WP29 ter verduidelijking richtlijnen uitgebracht.[34] Deze richtlijnen geven echter niet overal antwoord op. Wat dient er bijvoorbeeld te worden verstaan onder 'overheidsorgaan' in de zin van artikel 37 lid 1 sub a AVG? Zijn dit ook de zogeheten 'b-organen' in de zin van de Awb? De Richtlijn merkt hierover slechts op dat dit begrip in de nationale wetgeving bepaald dient te worden en dat dit onder nationale wetgeving vaak een reeks 'andere' publiekrechtelijke instellingen omvat.[35] Naast dat dit niet in ieder land hetzelfde is en dit punt daarmee strijdig lijkt aan het doel van harmonisatie, zou dit in Nederland betekenen dat ook iedere autogarage die bevoegd is om APK-keuringen uit te voeren, verplicht een FG dient aan te stellen.
De WP29 noemt bij artikel 37 lid 1 sub b en c bijvoorbeeld ziekenhuizen. De kerntaak van een ziekenhuis is het bieden van zorg, maar volgens de WP29 kan die kerntaak niet worden uitgevoerd zonder daarbij gegevens te verwerken en dus moet de verwerking van gegevens ook als een van de kerntaken worden beschouwd.[36]
De taak van een FG is een belangrijke: hij dient de organisatie te informeren en adviseren over de verplichtingen uit de AVG en toezicht te houden op de naleving daarvan. Gezien het karakter van gegevensbescherming en de implementatie daarvan in organisaties kan dit informatievoorziening en advisering op bestuursniveau zijn. Hij is het aanspreekpunt voor de AP (artikel 39 AVG) en de betrokkenen (artikel 38 lid 4 AVG) en dient zijn taken onafhankelijk te kunnen vervullen, ongeacht of hij bij de organisatie in dienst is. Bovendien geniet hij ontslagbescherming (artikel 38 lid 3 AVG).[37]
Het is derhalve niet voor niets dat de FG wordt aangewezen op grond van zijn deskundigheid op het gebied van de wetgeving en de praktijk (artikel 37 lid 5 AVG). In de praktijk is de vraag waar alle organisaties die al dan niet vrijwillig een FG aanstellen, deze deskundige persoon vandaan moeten halen. Er zal lang niet binnen iedere organisatie een medewerker aanwezigheid zijn die over de vereiste deskundigheid beschikt.
De FG mag echter ook een externe functionaris zijn. De taken worden dan verricht op grond van een dienstverleningsovereenkomst (artikel 37 lid 6 AVG). Een interessante vraag is of de FG naast de verwerkingsverantwoordelijke en/of de verwerker met succes aansprakelijk kan worden gesteld voor non-compliance van de organisatie, bijvoorbeeld doordat de FG onjuist heeft geadviseerd. Een vraag die in het verlengde daarvan ligt, is of de aansprakelijk gehouden organisatie regres zou kunnen nemen op een externe FG. Moet/kan een FG zich daartegen bovendien verzekeren?
De WP29 heeft in haar richtlijn betreffende de FG opgenomen: "Functionarissen voor gegevensbescherming zijn niet persoonlijk verantwoordelijk bij niet-naleving van de algemene verordening gegevensbescherming."[38] De WP29 verwijst expliciet naar de verantwoordelijkheid van de verwerkingsverantwoordelijke en de verwerker. In de situatie dat de FG correct heeft geadviseerd maar de organisatie het advies niet heeft overgenomen, kan ik deze aanwijzing van de WP29 volgen. Heeft de FG echter niet correct geadviseerd en de organisatie handelt overeenkomstig dat advies, dan lijkt mij dat in ieder geval ten aanzien van de externe FG toch anders te liggen. Mede gezien het arrest van de Hoge Raad van 18 september 2015 (Breeweg/Wijnkamp)[39] is bepaald niet uit te sluiten dat een externe FG op grond van onrechtmatige daad aansprakelijk kan zijn jegens derden en/of de organisatie zelf. Als de FG als 'beroepsbeoefenaar' moet worden beschouwd – en dat lijkt bij een externe FG wel voor de hand te liggen – dan verdient de stellige aanwijzing van de WP29 wel wat nuancering.

32 *Ibid*, p. 23.
33 Vaak aangeduid met de Engelse term *Data Protection Officer*.
34 Zie WP29, Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), 16/NL, WP 243rev.01, te raadplegen op <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243rev01_nl.pdf>.
35 *Ibid*, p. 7-8.
36 *Ibid*, p. 8.
37 Zie ook Overweging 97 AVG.
38 *Ibid* nt. 29, p. 6.
39 ECLI:NL:HR:2015:2745. Zie uitgebreid over dit arrest D.K. Baas en L. Verlinden, 'Beroepsaansprakelijkheid van de advocaat die geen opdrachtnemer is', *AV&S* 2016/44, p. 219-224.

## 6. (Scherpere) tanden voor de AP: boetes en handhavingsbevoegdheden

De AVG is inmiddels min of meer berucht doordat zij forse handhavingsboetes introduceert. Overtreding van de AVG – en dus niet enkel van het niet (tijdig) melden van een datalek! – kan leiden tot boetes van maximaal € 20 miljoen of 4% van de totale wereldwijde omzet, als dat cijfer hoger is (artikel 83 AVG). Voorheen was dat maximaal € 830.000,- of 10% van de jaaromzet (artikel 66 Wbp).
Ondanks dat de WP29 stelt dat de boete geen ultimum remedium is,[40] zal deze niet zomaar worden opgelegd; deze moet proportioneel zijn in het licht van de overtreding.[41] Bij het bepalen van de omvang van de boete wordt rekening gehouden met (kort gezegd) alle omstandigheden van het geval, waaronder de door de verwerkingsverantwoordelijke of verwerker genomen beveiligingsmaatregelen. Een boetebesluit is bovendien een besluit in de zin van de Awb, waartegen bezwaar en beroep openstaat en heeft een punitief karakter. De bewijslast rust bij de AP.[42]
Naast de boetebevoegdheid geeft de AVG de AP nog een aantal andere handhavingsbevoegdheden (artikel 58 AVG). Deze zijn laagdrempeliger en zullen daarom wellicht sneller worden ingezet. De AP kan bijvoorbeeld een tijdelijk of definitief verwerkingsverbod opleggen (artikel 58 lid 2 sub f AVG). Dergelijke maatregelen kunnen grote gevolgen hebben voor een organisatie.

## 7. Aansprakelijkheid en schade

Zowel de verwerkingsverantwoordelijke als de verwerker kunnen aansprakelijk worden gehouden voor materiële en immateriële schade als gevolg van een inbreuk op de AVG (artikel 82 AVG). Indien sprake is van meerdere verwerkingsverantwoordelijken of verwerkers, dan zijn zij hoofdelijk verbonden en kunnen zij ieder voor het geheel door de benadeelde worden aangesproken.
In artikel 80 AVG wordt de mogelijkheid van een class action geopend. De betrokkene heeft het recht om zich te laten vertegenwoordigen door een non-profit organisatie die namens hem/haar het recht op schadevergoeding uitoefent. Dit laatst kan enkel indien het lidstatelijke recht daarin voorziet. In Nederland is daarvoor weliswaar een wetsvoorstel aanhangig,[43] maar het verkrijgen van een schadevergoeding via een class action is onder het huidige recht niet mogelijk.

De vraag is wel wat voor materiële schade een benadeelde precies kan oplopen door een schending van de AVG en hoe dergelijke schade (naar Nederlands recht) kan worden gekwantificeerd. De drempels van het aansprakelijkheidsrecht kunnen bovendien hoog zijn voor benadeelden; denk aan het aantonen van causaal verband, een mogelijkheid tot een eigen schuld verweer (artikel 6:101 BW) of het ontbreken van voldoende concrete schade.
Ten aanzien van immateriële schade gelden eveneens drempels: er dient sprake te zijn van geestelijk letsel, dan wel van een ernstige schending van een fundamenteel recht.[44] In hoeverre benadeelden succesvol hun schade vergoed kunnen krijgen, zal dus verder moeten worden uitgekristalliseerd. Het verkrijgen van schadevergoeding is overigens ook weer niet ondenkbaar: onlangs nog werd de Britse supermarktketen Morrison jegens de betrokkenen aansprakelijk gehouden voor een inbreuk (nota bene bewust veroorzaakt door een eigen personeelslid).[45] Indien door nationaal recht gecreëerde barrières conflicteren met de doelstellingen van de AVG, is het bovendien niet uit te sluiten dat het nationale recht terzijde moet worden geschoven.[46]
Op basis van de verplichtingen in de AVG en de nadruk op compliance zijn meer procedures te verwachten tegen verwerkingsverantwoordelijken en verwerkers. Dit kan voor organisaties een grote kostenpost zijn, zeker als daarvoor verzekeringsdekking ontbreekt.[47] Bovendien kan dit een negatieve invloed hebben op de reputatie van een bedrijf. Het is derhalve verstandig dat organisaties privacybeleid en gegevensbescherming als vast onderdeel opnemen in het algemene risicomanagement.
Hier ligt ook een taak voor het bestuur. De mate waarin de gemiddelde bedrijfsvoering tegenwoordig digitaal verloopt en waarin persoonsgegevens worden verwerkt, is zodanig dat een bestuurder daarvan notie moet hebben. Dit geldt niet alleen ten aanzien van techniek, maar omvat de gehele organisatie: mensen, processen en technologie. Bestuurders van organisaties die min of meer bewust met verouderde IT-systemen en gebrekkige beveiliging blijven werken of proberen om inbreuken te verzwijgen, lopen mijns inziens een reëel risico om persoonlijk aansprakelijk te worden gesteld.[48]

40 WP29, 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679', 17EN, WP 253, p. 7, te raadplegen op https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889.

41 Zie ook *Kamerstukken II* 2017/18, 34851, 3, p. 25 (MvT).

42 Zie bijvoorbeeld CBb 27 juli 2017, ECLI:NL:CBB:2017:224, "*4.1 Het College stelt voorop dat het – mede in het licht van de in artikel 6, tweede lid, van het Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) vervatte onschuldpresumptie – aan ACM is om te bewijzen dat de voorliggende overtredingen zijn begaan.*"

43 Wetsvoorstel Afwikkeling van massaschade in een collectieve schadevergoedingsactie, *Kamerstukken II* 2016/17, 34 608, nr. 2.

44 Vgl. HR 18 maart 2005, ECLI:NL:HR:2005:AR5213, (*Baby Kelly*); HR 9 juli 2004, ECLI:NL:HR:2004:AO7721 (*Groninger Oudejaarsrellen*); HR 29 juni 2012, ECLI:NL:HR:2012:BW1519, (*Blauw oog*), r.o. 3.5.; Rb. Noord-Nederland 1 maart 2017, ECLI:NL:RBNNE:2017:715 (*NAM*), r.o. 4.4.6. Zie ook T.F. Walree, 'De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens', *WPNR* 2017/7172, p. 921-930.

45 High Court (Verenigd Koninkrijk) 1 december 2017, *Various Claimants v Wm Morrisons Supermarket Plc* [2017] EWHC 3133 (QB).

46 Zie in dit kader ook overweging 146 AVG en uitgebreid T.F. Walree, 'De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens', *WPNR* 2017/7172, p. 921-930. Zie ook T.F.E. Tjong Tjin Tai, 'Een Europees schadebegrip?', *NTBR* 2018/5, p. 31-36.

47 Of onder traditionele verzekeringen zoals de AVB-verzekering dekking bestaat voor dit soort schade, is de vraag. Zie in dit kader ook bijvoorbeeld E.P.M. Thole e.a., De Algemene meldplicht datalekken en de cyberverzekering', *TAV* 2015/2.

48 Zie ook W.C.T. Weterings, 'Persoonlijke aansprakelijkheid bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, p. 209-210.

## 8. Aanbevelingen voor de praktijk

Gegevensbescherming is een fundamenteel recht. In de AVG staat de bescherming van dit recht centraal. Eén van de kernwaarden van de AVG is dat betrokkenen controle houden over hun persoonsgegevens. De AVG dwingt organisaties om daarvan doordrongen te zijn en daar ook naar te handelen. Organisaties dienen hun gegevensbeschermingsbeleid niet vanuit hun eigen positie, maar vanuit de positie van de betrokkenen te bekijken en in te richten.

De nadruk op de verantwoordingsplicht zou bedrijven in beweging moeten brengen om een helder beeld te krijgen van hun verwerkingen: zij dienen een risico-inventarisatie uit te voeren, dit te vertalen in helder beleid en dat over de gehele organisatie uit te spreiden.

De gevolgen van een schending van de verplichtingen van de AVG kunnen groot zijn; niet alleen door de forse handhavingsbevoegdheid van de AP, maar ook door de aansprakelijkheidsrisico's die zowel de verwerkingsverantwoordelijke als de verwerker loopt, met alle bijkomende kosten van dien.

Verwerkingsverantwoordelijken en verwerkers dienen de verdeling van verantwoordelijkheden duidelijk in een verwerkersovereenkomst op te nemen. Partijen zouden er bovendien goed aan doen om te controleren in hoeverre zij verzekeringsdekking hebben voor schade en kosten door inbreuken op de privacy. Organisaties zullen privacy dus permanent hoog op de (bestuurs)agenda moeten hebben staan.

> Adequate gegevensbescherming is een continu proces en niet slechts een status waaraan enkel op 25 mei 2018 hoeft te worden voldaan

Adequate gegevensbescherming is immers een continu proces en niet slechts een status waaraan enkel op 25 mei 2018 hoeft te worden voldaan.

**Over de auteur**

**Mr. N.M. Brouwer**

Nynke Brouwer is advocaat bij Dirkzwager advocaten & notarissen te Arnhem.