Mark Jansen[1,2]

AVG en beveiliging: passende maatregelen voortaan proactiever nemen en monitoren

Computerrecht 2017/152

In de aankomende algemene verordening gegevensbescherming (AVG) krijgt het onderwerp beveiliging ruimschoots aandacht. Diverse overwegingen zijn aan het onderwerp gewijd en diverse artikelen bevatten verplichtingen omtrent beveiliging. Er lijkt meer van de verwerkingsverantwoordelijke te worden verwacht, maar er lijkt ook wel veel oude wijn in nieuwe zakken te worden gedaan. In dit artikel zet ik op een rij wat de huidige verplichtingen zijn, wat de AVG brengt en in hoeverre dat nieuw is.

1. Huidige juridisch kader op Europees niveau

1.1 *Richtlijn*

De huidige verplichting persoonsgegevens te beveiligen vloeit voort uit artikel 17 lid 1 van de Richtlijn 95/46/EG ("Privacyrichtlijn 1995"). Het artikel verplicht lidstaten om verantwoordelijken te verplichten een "*passend beveiligingsniveau*" te garanderen "*gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen*". Dat passende niveau moet persoonsgegevens beveiligen "*tegen vernietiging, (…) verlies, vervalsing, niet-toegelaten verspreiding of toegang (...) dan wel tegen enige andere vorm van onwettige verwerking*". In de Privacyrichtlijn 1995 staan geen aanwijzingen wat dat passende niveau in concreto precies inhoudt.

Onder de systematiek van de Privacyrichtlijn 1995 geldt voor bewerkers altijd de beveiligingsnorm uit de wetgeving van de eigen lidstaat,[3] ook al worden persoonsgegevens verwerkt voor een in een ander land gevestigde verantwoordelijke.[4] In de opinie van de Artikel 29 Werkgroep[5] (hierna: WP29) wordt hierover opgemerkt "*dat in Europees perspectief de beveiligingseisen aanzienlijk uiteenlopen tussen de lidstaten: sommige kennen zeer gedetailleerde regels, terwijl andere de algemene formuleringen uit de richtlijn hebben overgenomen*".

1.2 *Rechtspraak Hof van Justitie*

Voor zover mij bekend zijn er nog geen zaken gewezen waarin het Hof van Justitie zich inhoudelijk over de norm van artikel 17 Privacyrichtlijn 1995 heeft uitgelaten. Blijkens de meta-data van EUR-lex[6] zijn er twee prejudiciële vragen gesteld over de interpretatie van artikel 17 lid 1 Privacyrichtlijn 1995:

1. Onder zaaknummer C-683/13 zijn er vragen gesteld over de beveiligingsverplichting voor de Portugese staat van een arbeidstijdenregister van een werkgever (niet zijnde de Staat). Bij arrest van 19 juni 2014[7] oordeelde het Hof, onder verwijzing naar het Worten-arrest,[8] dat de vraag over artikel 17 lid 1 Privacyrichtlijn 1995 niet relevant was, aangezien de beveiligingsplicht op de verantwoordelijke en niet op de Staat rust.
2. Onder zaaknummer C-73/16 is aan het Hof gevraagd of bewijs dat verkregen is middels doorbreking van beveiligingsmaatregelen overeenkomstig artikel 47 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest) moet worden geweigerd. Deze prejudiciële vraag is nog niet beantwoord.

In het aangehaalde Worten-arrest overweegt het Hof letterlijk dat "*de uitlegging van artikel 17, lid 1, van richtlijn 95/46 voor de beslechting van het hoofdgeding irrelevant*" is (r.o. 29). Er is dus geen inhoudelijk oordeel gegeven over de norm van artikel 17 Privacyrichtlijn 1995.

In het Digital Rights Ireland-arrest[9] heeft het Hof zich uitgelaten over beveiliging van persoonsgegevens in het kader van artikel 8 Handvest. Dit arrest ging over de geldigheid van Richtlijn 2006/24/EG, die zag op de grootschalige verzameling van verkeersgegevens. Richtlijn 2006/24/EG kende de verplichting om "*passende technische en organisatorische maatregelen*" te treffen om de verkeersgegevens te beveiligen tegen o.m. onrechtmatige verwerking. Het Hof kwalificeerde de grootschalige opslag van verkeersgegevens als "*een zeer ruime en bijzonder zware inmenging*" (r.o. 37) in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten. In die context overwoog het Hof dat de verplichting passende maatregelen te treffen "*onvoldoende garanties biedt (…) tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik ervan*" (r.o. 66), onder meer omdat er geen "*specifieke regels*" zijn opgenomen die zijn afgestemd op de omvang en gevoeligheid van de gegevens (r.o. 66), de regels er niet toe "*strekken de bescherming en de beveiliging van de betrokken gegevens duidelijk en strikt te regelen om de volle integriteit en vertrouwelijkheid ervan te waarborgen*" (r.o. 66), aanbieders

1 Mr. drs. M. Jansen is advocaat bij Dirkzwager advocaten & notarissen te Arnhem.
2 De auteur is veel dank verschuldigd aan Arno Stoffelsma voor zijn hulp bij het redigeren van het artikel.
3 Artikel 17 lid 3 Privacyrichtlijn 1995.
4 Zij het dat er mijns inziens geen bezwaar is om contractueel verderstrekkende afspraken te maken.
5 "*Advies 8/2010 over toepasselijk recht*", goedgekeurd op 16 december 2010, WP179, Artikel 29 Werkgroep.
6 http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:31995L0046, geraadpleegd op 14 april 2017.
7 Alleen beschikbaar in het Frans en Portugees, ik baseer mijn conclusies dan ook op machinevertalingen daarvan.
8 Arrest van het Hof van Justitie d.d. 30 mei 2013, zaak C-342/12.
9 Arrest van het Hof van Justitie d.d. 8 april 2014, gevoegde zaken C-293/12 en C-594/12.

"*economische overwegingen*" mogen laten meetellen bij het vaststellen van de beveiligingsmaatregelen (r.o. 67) en niet is geborgd dat de gegevens "*na de bewaarperiode onherroepelijk worden vernietigd*". Het Hof legt de lat dus hoog. Het is de vraag of het Hof gelijk zo zou oordelen over beveiliging in een andere, minder verstrekkende, kwestie. Het Hof overweegt immers zelf uitdrukkelijk in r.o. 45 dat het oordeel over de evenredigheid van de inmenging wordt gegeven in het kader van de reeds vastgestelde omstandigheden.

De Europese wetgever en Europese rechtspraak geven dus vooralsnog, behoudens laatstgenoemde zaak, weinig concrete handvaten over wat passende beveiliging precies inhoudt.

1.3 *De Artikel 29 Werkgroep*

De WP29 haalt in diverse opinies de norm als zodanig aan, maar wijdt daar niet over uit. In enkele opinies wordt de norm nader gepreciseerd:

1. In de opinie over *behavorioural advertising* uit 2010[10] stelt de WP29 dat van aanbieders en advertentienetwerken mag worden verwacht dat zij "*geavanceerde technische en organisatorische maatregelen* [treffen] *om te zorgen voor de veiligheid en vertrouwelijkheid van informatie*".
2. In de opinie over het concept van de verantwoordelijke en de bewerker uit 2010[11] lijkt de WP29 te stellen dat van een verantwoordelijke mag worden verwacht dat proactief en met voldoende middelen aan beveiliging wordt gedaan.
3. In een opinie over "*the internet of things*"[12] wordt uit artikel 17 Privacyrichtlijn 1995 afgeleid dat verantwoordelijken (in ieder geval bij the internet of things) verplicht zijn om een veiligheidsbeoordeling te verrichten, dat het principe van *composable security*[13] moet worden toegepast, dat apparaten moeten worden gecertificeerd, dat aansluiting moet worden gezocht bij internationaal erkende standaarden en dat systemen voortdurend onderhouden moeten worden.

Gelet op de door de WP29 gesignaleerde verschillen in implementatie van de beveiligingsverplichting in nationale wetgeving, is het niet verrassend dat de WP29, behalve de hiervoor genoemde opmerkingen, niet meer uitgesproken visies heeft gegeven over artikel 17 Privacyrichtlijn 1995.

10 "*Advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising')*" goedgekeurd op 22 juni 2010, WP171, Artikel 29 Werkgroep, p. 25.

11 "*Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker""* goedgekeurd op 16 februari 2010, WP169, Artikel 29 Werkgroep, p. 6.

12 "*Advies 8/2014 over de recente ontwikkelingen op het gebied van het internet van de dingen*" goedgekeurd op 16 september 2014, WP223, Artikel 29 Werkgroep, p. 20.

13 Van 'composable security'. Hiervan bestaan diverse definities. De WP29 lijkt er, gelet op de context van de opinie, op te doelen dat van een systeem zowel de delen van het systeem op zichzelf als de som der delen veilig moeten zijn.

2. Huidige juridische kader op nationaal niveau

2.1 *Nederlandse wetgeving*

Nederland heeft er voor gekozen om de verplichting uit artikel 17 Privacyrichtlijn 1995 bijna letterlijk over te nemen in artikel 13 van de Wet bescherming persoonsgegevens (Wbp). Artikel 13 Wbp verplicht de verantwoordelijke om, samengevat, persoonsgegevens op zodanige wijze te beveiligen dat een "passend" beveiligingsniveau wordt gegarandeerd. De maatregelen moeten de persoonsgegevens volgens artikel 13 Wbp beveiligen "*tegen verlies of tegen enige vorm van onrechtmatige verwerking*" en moeten er "*mede op gericht* [zijn] *onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen*".

Wat passend is hangt volgens de Nederlandse wetgever af van alle omstandigheden van het geval. De Nederlandse wetgever heeft er bewust voor gekozen geen concretere norm te noemen. Uit de wetsgeschiedenis blijkt dat het "*niet aan de wetgever* [is] *om nadere details te geven over de aard van de beveiliging. Dergelijke details zouden sterk tijdgebonden zijn en daarmee afbreuk doen aan het nagestreefde niveau van beveiliging*".[14] In sommige wetten wordt een iets concretere keuze gemaakt, door te verwijzen naar normen als ISO27001 of NEN7510.

2.2 *Nederlandse rechtspraak*

Uit de weinige voorbeelden uit de Nederlandse rechtspraak over artikel 13 Wbp noem ik hier twee kwesties:[15] (1) de toetsing van de infrastructuur van het landelijk schakelpunt; en (2) de aan KPN opgelegde boete na een hack.

ad. 1. *Toetsing infrastructuur landelijke schakelpunt*

Het Gerechtshof Arnhem-Leeuwarden heeft bij arrest van 8 maart 2016[16], samengevat, geoordeeld dat de door VZVZ geëxploiteerde landelijke infrastructuur voor uitwisseling van zorggegevens niet onrechtmatig is. Uit r.o. 4.17 volgt dat passend iets anders is dan perfect:

> "Anders dan VPH c.s. betogen volgt uit die maatstaf noch uit de Parlementaire Geschiedenis ten aanzien van dat artikel dat VZVZ in casu dient te streven naar de hoogst mogelijke beveiliging."

Voor het overige geldt dat partijen het er over eens waren dat de beveiligingseisen in de zorgsector nader worden ingekleurd door de normen uit de NEN751x serie. Het gerechtshof heeft zich – gelet op de civielrechtelijke procesvoering – over de normen inhoudelijk dus niet hoeven uitlaten.

14 *Kamerstukken II* 1997/98, 25892, 3, p. 98-99.

15 Zonder de pretentie te hebben op dit punt volledig te zijn.

16 ECLI:NL:GHARL:2016:1697.

ad. 2. *Aan KPN opgelegde boete na hack*

Het College van Beroep voor het Bedrijfsleven heeft in de uitspraak van 16 november 2016[17] het beroep van KPN tegen een door de Autoriteit Consument en Markt (ACM) opgelegde boete na een hack op het netwerk van KPN verworpen. Het College oordeelt dat de beveiligingsnorm uit de Telecommunicatiewet (Tw) een aanvulling vormt op de Wbp (r.o. 4.2) en dat wat geldt voor de uitleg van de Tw dus niet onverkort geldt voor de uitleg van de Wbp (r.o. 6.2). Niettemin is interessant om te zien dat het College de benadering van de ACM, waarbij "*ACM heeft gekeken naar wat in de wereld van informatievoorziening als minimaal noodzakelijke maatregelen worden gezien (..) gebaseerd op NEN-normen en op vakliteratuur op het gebied van informatiebeveiliging*" volledig onderschrijft (r.o. 9.2). Juist omdat de ACM heeft gekeken naar de volgens de literatuur minimaal vereiste maatregelen, en gebleken was dat deze minimale maatregelen niet of onvoldoende waren getroffen, ziet het College ook geen aanleiding prejudiciële vragen te stellen (r.o. 15).

Hoewel laatstgenoemde kwestie formeel gezien over de Tw en niet over de Wbp gaat, en het College ook benadrukt dat wat voor de Tw geldt niet onverkort voor de Wbp geldt, zou mijn inschatting zijn dat een vergelijkbare kwestie onder de Wbp tot hetzelfde resultaat zou leiden. Met andere woorden: een verantwoordelijke die niet de op grond van algemeen aanvaarde literatuur minimaal te nemen beveiligingsmaatregelen heeft genomen, zal in de regel (dus) de Wbp overtreden en daarvoor ook onder de Wbp een boete kunnen krijgen.[18]

2.3 ***Autoriteit Persoonsgegevens***

De Autoriteit Persoonsgegevens (AP) heeft in 2013 de Richtsnoeren 'Beveiliging van persoonsgegevens' gepubliceerd.[19] Samengevat is de AP van oordeel dat algemeen geaccepteerde beveiligingsstandaarden moeten worden gehanteerd en dat middels een plan-do-check-act (PDCA) cyclus voortdurend moet worden getoetst of de toegepaste beveiliging nog voldoet.

Zoals blijkt uit de hiervoor aangehaalde wetsgeschiedenis past het aansluiting zoeken bij internationaal erkende normen bij de bedoeling van de wetgever. Op dat onderdeel van de beleidsregels (en daarop gebaseerde handhaving) lijkt dan ook weinig af te dingen. Het hanteren van de PDCA-cyclus is niet direct te relateren aan een verplichting uit de Wbp, doch wel enigszins aan de AVG (daarover hierna meer).

17 ECLI:NL:CBB:2016:346.

18 Met de kanttekening dat onder de Wbp voor een boete de drempel van opzet of ernstig verwijtbare nalatigheid genomen moet worden op grond van artikel 66 Wbp.

19 Directe link: www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf. Zie voor de opvattingen van de Belgische toezichthouder www.privacycommission.be/nl/informatiebeveiliging.

3. Toekomstig juridisch kader – normenkader

Vanaf 25 mei 2018 is de algemene verordening gegevensbescherming (AVG)[20] van toepassing. De grootste verandering die de AVG mijns inziens brengt is het introduceren van allerlei verplichtingen in de sfeer van "compliance". De grootste veranderingen zijn niet gelegen in de materiële normen ten aanzien van de verwerking van persoonsgegevens.

Ook de AVG stelt de norm van "passende maatregelen" ter beveiliging van persoonsgegevens. Deze norm komt op meerdere plaatsen terug:[21]

- de verantwoordelijke moet ervoor zorgen dat persoonsgegevens "*door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("integriteit en vertrouwelijkheid")*"[22]; en
- het is aan de verwerkingsverantwoordelijke en de verwerker om, "*rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, (…) passende technische en organisatorische maatregelen* [te treffen, MJ] *om een op het risico afgestemd beveiligingsniveau te waarborgen*".[23]

Bij de beoordeling van het beveiligingsniveau moet rekening worden gehouden met de verwerkingsrisico's.[24] Er is één (beveiligings)maatregel die altijd genomen moet worden:[25] waarborgen dat natuurlijke personen persoonsgegevens – behoudens wettelijke plichten – slechts in opdracht van de verwerkingsverantwoordelijke verwerken[26]. Enkele maatregelen die volgens het artikel getroffen zouden kunnen worden zijn:

a. de pseudonimisering en versleuteling van persoonsgegevens;

20 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).

21 Artikel 24 lid 1 AVG bepaalt bovendien dat "*passende technische en organisatorische maatregelen*" moeten worden getroffen "*om te waarborgen (…) dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd*". Dat zijn dus passende maatregelen om onder meer passende beveiligingsmaatregelen te treffen.

22 Artikel 5 lid 1 sub f AVG.

23 Artikel 32 lid 1 AVG.

24 Artikel 32 lid 2 AVG.

25 Artikel 32 lid 4 AVG.

26 Overigens verbiedt artikel 29 AVG de natuurlijk persoon al om zonder opdracht persoonsgegevens te verwerken. Artikel 32 lid 4 AVG ziet dus alleen nog op de organisatorische maatregelen om te borgen dat de betreffende natuurlijk persoon zich aan de wet houdt (soort van zorgplicht dus).

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

In de AVG gaat de opsomming van deze maatregelen voorafdoor de woorden "*waar passend*". Het lijkt er dan ook op dat het treffen van deze maatregelen niet per definitie verplicht is. Geheel vrijblijvend lijkt het treffen van deze maatregelen echter ook niet. Hopelijk wordt vòòr 25 mei 2018 duidelijker wat van verwerkingsverantwoordelijken verwacht wordt.

De opsomming roept overigens nog wel de nodige vragen op. Zo klinkt het "*permanent*" kunnen "*garanderen*" van de integriteit van gegevens (voorbeeld onder b) best zwaar voor een "*passende maatregel*". Voor onderdeel d uit de opsomming geldt juist weer dat vreemd is dat de beveiliging kennelijk alleen "*waar passend*" periodiek geëvalueerd moet worden. Een periodieke evaluatie lijkt mij echter – behoudens bij incidentele verwerkingen – de enige manier om te kunnen toetsen of de getroffen maatregelen nog steeds passend zijn.

4. "Privacy by design" en "privacy by default"

Artikel 25 AVG introduceert verplichtingen die geschaard kunnen worden onder beveiligingsverplichtingen, te weten (vrij vertaald) de verplichting tot "privacy by design" en "privacy by default".

De verwerkingsverantwoordelijke is verplicht om, rekening houdend met alle omstandigheden van het geval, "*passende technische en organisatorische maatregelen*" te treffen "*met als doel de gegevensbeschermingsbeginselen (…) op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen*".[27]

Daarnaast is de verwerkingsverantwoordelijke verplicht om "*passende technische en organisatorische maatregelen*" te treffen "*om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan*".[28]

27 Artikel 25 lid 1 AVG.
28 Artikel 25 lid 2 AVG.

Hoewel er in diverse media heel hoog wordt opgegeven over deze twee verplichtingen,[29] vraag ik mij af of:[30]

1. "privacy by design" en "privacy by default" werkelijk veel nieuws brengen ten opzichte van huidig recht; en
2. het artikel over "privacy by design" en "privacy by default" iets toevoegt op andere artikelen uit de AVG.

4.1 *Toevoeging ten opzichte huidig recht*

Zoals hiervoor uiteengezet verplicht artikel 13 Wbp al om passende maatregelen te treffen om onrechtmatige verwerkingen van persoonsgegevens te voorkomen. Onder huidig recht is het al onrechtmatig gegevens zonder grondslag te verwerken (artikel 8 Wbp), gegevens te verwerken in strijd met het verzameldoel (artikel 9 Wbp), gegevens te lang te bewaren (artikel 10 Wbp) en gegevens te verwerken die niet toereikend, niet ter zake dienend of bovenmatig zijn (artikel 11 Wbp).

Onder huidig recht moeten de beveiligingsmaatregelen (dus) al zien op het voorkomen van dergelijke onrechtmatige verwerkingen. De verplichtingen uit artikel 25 AVG brengen mijns inziens dus niet zo heel veel nieuws. Illustratief voor mijn stelling is dat de AP in de richtsnoeren beveiliging van persoonsgegevens uit 2013 het gebruik van 'Privacy Enhancing Technologies' inleest in artikel 13 Wbp.[31] Hooguit biedt het artikel voor de (buitenlandse) toezichthouders een extra kapstok om te kunnen betogen dat je de beveiligingsverplichting uit de AVG inderdaad zo ruim moet lezen dat je daar ook "privacy by design" en "privacy by default" in moet lezen.

4.2 *Toevoeging op de overige bepalingen uit de AVG?*

Het is verder de vraag wat beide bepalingen in de AVG toevoegen op andere bepalingen in de AVG. De verwerkingsverantwoordelijke is immers al verplicht om aan te kunnen tonen dat hij persoonsgegevens overeenkomstig de belangrijkste beginselen uit de verordening verwerkt.[32] Dat veronderstelt mijns inziens – om dezelfde reden als hiervoor voor de Wbp aangevoerd – dat er daartoe maatregelen getroffen zijn.

Datzelfde geldt in feite voor het bepaalde in artikel 25 lid 2 AVG: de verantwoordelijke is toch al verplicht om niet meer gegevens te verzamelen dan noodzakelijk,[33] om maat-

29 Illustratief is dat wanneer ik bij Google zoek op "*privacy by design*"+*avg* er bij mij meer dan 6.500 treffers verschijnen.
30 Zie ook dr. J. Holvast in "Algemene verordening gegevensbescherming: veel gespin en weinig wol" in *P&I* 2016/103 nr. 3: "Privacy by design is niets anders dan de verplichting om alles in overeenstemming te brengen met de verordening en dat daarvoor passende, waaronder technische, middelen moeten worden gebruikt. Privacy by default is weinig anders dan de uit de richtlijn bekende beginselen van minimale gegevensopslag en doelbinding.".
31 Zie onder meer pagina 10 van voornoemde richtsnoeren. Overigens was de Registratiekamer, de rechtsvoorgang van de Autoriteit Persoonsgegevens, al in 1995 van oordeel dat PET gestimuleerd diende te worden. Zie de publicatie "*Privacy-enhancing technologies: the path to anonimity*" dat zij in 1995 samen met haar Canadese zusterorganisatie heeft uitgebracht (serie Achtergrondstudies en Verkenningen 5A en 5B).
32 Artikel 5 lid 2 AVG.
33 Artikel 5 lid 1 sub c AVG.

regelen te treffen tegen onrechtmatige – waaronder dus te grootschalige of ongerichte – verwerkingen[34] aan te kunnen tonen dat hij daadwerkelijk niet meer gegevens verzamelt dan noodzakelijk en daadwerkelijk daartoe maatregelen heeft getroffen.[35] Het is onduidelijk wat artikel 25 lid 2 AVG daaraan toevoegt.

5. Pseudonimisering

Een vreemde eend in de bijt voor wat betreft beveiliging is pseudonimisering. De AVG schenkt ruimschoots aandacht aan het onderwerp. Niettemin roept het enkele interessante vragen op.

5.1 *Pseudonimisering in de AVG*

Het begrip pseudonimisering komt in de AVG op diverse plaatsen voor.[36] Het is in artikel 4 onder 5 AVG gedefinieerd als "*het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld*". De kern van pseudonimisering is aldus het (tijdelijk) wegnemen van de identificeerbaarheid.

5.2 *Persoonsgegevens, gepseudonimiseerde gegevens en anonieme gegevens*

Uit overweging 26 – verderop in het artikel geciteerd – volgt dat onder de AVG onderscheid moet worden gemaakt tussen drie soorten gegevens:

1. reguliere persoonsgegevens (de AVG is van toepassing);
2. gepseudonimiseerde persoonsgegevens (de AVG is van toepassing);
3. anonieme gegevens (de AVG is niet van toepassing).

De vraag is of de AVG op dit punt veel wijzigingen met zich meebrengt.

5.3 *Onderscheid anonieme gegevens en persoonsgegevens*

Onder huidig recht geldt dat gegevens als persoonsgegevens moeten worden aangemerkt indien het verkrijgen van de daarvoor eventueel vereiste identificerende gegevens "*een middel vormt waarvan mag worden aangenomen dat het redelijkerwijs kan worden ingezet om de betrokken persoon te identificeren*".[37] Dat is volgens het Hof niet het geval indien die verkrijging "*een excessieve inspanning vergt*".[38] Aan de hand van deze criteria moet worden bepaald of gegevens als persoonsgegevens te beschouwen zijn. Het Hof baseert dat oordeel met name op overweging 26 van de Privacyrichtlijn 1995.

Wanneer het kernelement uit die overweging 26 Privacyrichtlijn 1995 wordt vergeleken met overweging 26 van de AVG, dan valt op dat de overwegingen een grote overlap kennen:

Privacyrichtlijn	**AVG**
(…) om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren; (…)	(…) Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen

Het is dan ook de vraag of de AVG op dit punt wezenlijk verschilt van de Privacyrichtlijn 1995. Ik vermoed dat dit niet het geval is. Het onderscheid tussen persoonsgegevens en anonieme gegevens lijkt onder de AVG dus niet te wijzigen ten opzichte van de Privacyrichtlijn 1995.

In de praktijk is het daadwerkelijk anonimiseren van gegevens overigens erg lastig. De WP29 heeft in de opinie uit 2014 over anonimiseringstechnieken[39] er op gewezen dat vermeend anonieme gegevens in de praktijk veelal wel herleidbaar zijn tot natuurlijke personen. Dit wordt bijvoorbeeld veroorzaakt omdat gegevens dusdanig uniek zijn dat ze op grond van de kenmerken eenvoudig te herleiden zijn tot een bepaald persoon (hetzij op zichzelf, hetzij door te koppelen met andere gepseudonimiseerde gegevens).

34 Artikel 4 lid 1 sub f AVG.
35 Artikel 5 lid 2 AVG.
36 In artikel 6 lid 4 onder e, in artikel 25 lid 1, in artikel 32 lid 1, in artikel 20 en in artikel 89.
37 Arrest van het Hof (Tweede kamer) 19 oktober 2016, zaak C-582/14, r.o. 45.
38 Voornoemd arrest, r.o. 46.
39 "*Advies 4/2007 over het begrip persoonsgegeven*" goedgekeurd op 20 juni 2007, WP136, Artikel 29 Werkgroep.

5.4 *Toepassing regels op verwerking gepseudonimiseerde gegevens*

Ook wanneer gekeken wordt naar de regels omtrent het gebruik van gepseudonimiseerde gegevens, is de vraag of de AVG veel nieuws brengt. Het lijkt er veelal op dat de AVG met de introductie van het begrip "pseudonimiseren" expliciteert wat reeds in opinies van de WP29 was opgenomen.

De WP29 heeft immers in de opinie over het begrip persoonsgegeven uit 2007 gepseudonimiseerde aangemerkt als "*indirect identificeerbare informatie*" en gesteld dat de regels uit de Privacyrichtlijn 1995 weliswaar van toepassing zijn bij de verwerking van dergelijke informatie, maar "*soepeler [worden] toegepast dan bij de verwerking van informatie over direct identificeerbare personen*".[40] En in de opinie over anonimisering heeft dezelfde werkgroep opgemerkt dat pseudonimisering "*een nuttige beveiligingsmaatregel*" is.[41]

Het soepeler toepassen van regels omtrent gegevensbescherming zodra gegevens gepseudonimiseerd zijn ligt sterk in lijn met het bepaalde in artikel 6 lid 4 onder e AVG (gebruik in strijd met verzameldoel) en artikel 89 AVG (wetenschappelijk onderzoek).

Het beschouwen van pseudonimisering als een beveiligingsmaatregel past bij het bepaalde in artikel 25 AVG (privacy by design), artikel 32 AVG (beveiliging) en artikel 40 (gedragscodes).

Een gemiste kans is dat de AVG niet in algemene zin bepaalt dat de AVG soepeler moet worden toegepast op de verwerking van gepseudonimiseerde gegevens dan op de verwerking van persoonsgegevens. Mogelijk dat verwerkingsverantwoordelijken in voorkomend geval steun kunnen vinden in artikel 94 lid 2 AVG, dat bepaalt dat verwijzingen naar de WP29 moeten worden beschouwd als verwijzingen naar het Europees Comité voor gegevensbescherming. Aangezien dat Comité op grond van artikel 70 lid 1 onder e AVG o.m. tot taak heeft aanbevelingen uit te brengen over de toepassing van de AVG, mag de opinie uit 2007 mogelijk als dergelijke aanbeveling voor (de toepassing van) de AVG worden gelezen.

5.5 *Re-identificatie en artikel 11 AVG*

Artikel 11 AVG verdient in dit verband nog wel bijzondere vermelding. Artikel 11 lid 1 AVG maakt expliciet dat de verwerkingsverantwoordelijke in beginsel vrij is om van gepseudonimiseerde gegevens geanonimiseerde gegevens te maken, als identificeerbaarheid geen vereiste meer is.

Het tweede lid van artikel 11 AVG is interessanter. De eerste zin van dit lid introduceert een aanvullende informatieverplichting door te bepalen dat de verwerkingsverantwoordelijke de betrokkene "*indien mogelijk*" moet informeren over de anonimisering.[42] De tweede zin bepaalt – m.i. zinledig[43] – dat de rechten die de AVG aan de betrokkene toekent niet van toepassing zijn indien de verwerkingsverantwoordelijke aantoont dat hij de betrokkene niet kan identificeren. Het slot van het artikellid is het meest interessant: het bepaalt dat de betrokkene zijn rechten kan inroepen indien hij "*aanvullende gegevens verstrekt die het mogelijk maken hem te identificeren*". De betrokkene kan er dus voor zorgen dat anonieme gegevens, in ieder geval in relatie tot de door de AVG aan de betrokkene toegekende rechten, (tijdelijk) herleven als persoonsgegevens.

De vraag is zelfs of de AVG daarmee op die gegevens **algeheel** opnieuw van toepassing wordt. De verwerkingsverantwoordelijke zal immers op grond van de verantwoordingsplicht uit de AVG en de wettelijke administratieplicht vermoedelijk die door de betrokkene verstrekte identificerende gegevens wensen te bewaren. Zodra de verwerkingsverantwoordelijke daartoe besluit, is echter evident dat persoonsgegevens (en geen anonieme gegevens) worden verwerkt en is op die (verdere) verwerking dus de AVG van toepassing. En mogelijk dat vervolgens moet worden geconcludeerd dat er voor die verdere verwerking helemaal geen grondslag is of dat de gegevens te lang worden bewaard (de gegevens waren immers niet voor niets geanonimiseerd). In die redenering zou de betrokkene daarmee effectief de verwerking van geanonimiseerde gegevens tot op zekere hoogte kunnen frustreren. Een belangrijk aandachtspunt voor alle partijen die zich bezighouden met (*big data*) analyses van anonieme gegevensets.

6. Verantwoordingsplicht over beveiligingsmaatregelen

De AVG introduceert op twee plaatsen een algemene verantwoordingsplicht:

a. in artikel 5 lid 2: deze heeft betrekking op de beginselen genoemd in artikel 5 lid 1 AVG en lijkt in omvang verder niet begrensd;
b. in artikel 24 lid 1: deze heeft betrekking op de gehele verordening, maar deze plicht is qua omvang weer beperkt tot wat onder de gegeven omstandigheden redelijkerwijs gevergd mag worden.

Aangezien de beveiligingsverplichtingen, zoals hiervoor al gesignaleerd, in verschillende artikelen worden genoemd,[44] betekent dit dus dat de verwerkingsverantwoordelijke zowel op een in omvang/strekking onbegrensde[45] als begrensde[46] wijze verantwoording moet kunnen afleggen over het gevoerde beveiligingsbeleid. Die innerlijke tegenstrijdig-

40 "*Advies 4/2007 over het begrip persoonsgegeven*" goedgekeurd op 20 juni 2007, WP136, Artikel 29 Werkgroep, pagina 19.
41 "*Advies 5/2014 over anonimiseringstechnieken*" goedgekeurd op 10 april 2014, WP216, Artikel 29 Werkgroep, pagina 23.
42 Het valt voor de praktijk te hopen dat het volstaat om bij eerste verkrijging van de gegevens de betrokkene te informeren dat op termijn mogelijk anonimisering plaatsvindt. Informeren vlak voor de daadwerkelijke anonimisering lijkt onpraktisch en de vraag is ook welk belang daarmee is gediend.
43 De AVG is immers niet van toepassing op de verwerking van anonieme gegevens.
44 Artikel 5 lid 1, artikel 32 en artikel 24 AVG.
45 Artikel 5 lid 2 AVG.
46 Artikel 24 lid 1 AVG.

heid in de (omvang van de) verantwoordingsplichten lijkt me voer voor juristen.

Daar komt nog eens bij dat één van de maatregelen die moet worden getroffen in het kader van naleving van de verordening "*een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd*" is, maar alleen "*wanneer zulks in verhouding staat tot de verwerkingsactiviteiten*".[47] Onder, (vooralsnog) onbekende, omstandigheden moet de verantwoordelijke zich dus kunnen verantwoorden en onder, eveneens (vooralsnog) onbekende, omstandigheden omvat de maatregel waarover verantwoording moet worden afgelegd dus het gevoerde "*gegevensbeschermingsbeleid*".

Kennelijk hoeft er niet altijd een "*gegevensbeschermingsbeleid*" te zijn (anders is de drempel uit lid 2 niet te verklaren). Ik leid hier verder uit af dat het onder artikel 5 lid 2 AVG niet van de verwerkingsverantwoordelijke gevergd kan worden een beleid aan de toezichthouder te overleggen. Anders zou de in artikel 24 lid 2 geïntroduceerde drempel voor het hebben van dergelijk beleid immers zinledig zijn. Organisaties die op kleine schaal persoonsgegevens verwerken zijn aldus vermoedelijk niet verplicht een uitgewerkt beveiligingsbeleid te hebben. De verwerkingsverantwoordelijken die op grotere schaal persoonsgegevens verwerken, zullen onder de AVG echter verplicht zijn op eerste verzoek van de toezichthouder een "*gegevensbeschermingsbeleid*" te overleggen dat passend is en dat daadwerkelijk wordt uitgevoerd.

Het voorgaande in ogenschouw nemend is de vraag of de AVG ten aanzien van verantwoording daadwerkelijk veel nieuws brengt. Grote organisaties zullen ook nu al enigszins uitgewerkt beleid moeten hebben om thans aan de Wbp te kunnen voldoen. Kleinere organisaties hebben wellicht geen uitgewerkt beleid nodig om beveiligingsmaatregelen te treffen, maar zullen feitelijk wel maatregelen moeten treffen. Informatie over het getroffen beleid althans de getroffen maatregelen kan de AP thans ook opvragen. Het verschil is wellicht dat grotere organisaties onder de AVG lastig meer kunnen stellen dat zij **zonder** beleid aan privacywetgeving kunnen voldoen, terwijl dat thans – bij gebreke van een verplichting tot het hebben van beleid – onder de Wbp strikt genomen wel een valide verweer is.

Let wel: het voorgaande verweer geldt **niet** voor aanbieders van openbare elektronische communicatienetwerken van openbare elektronische communicatiediensten in de zin van de Telecommunicatiewet (Tw). Zij zijn op grond van artikel 11.3 lid 2 onder c Tw verplicht een "*veiligheidsbeleid met betrekking tot de verwerking van persoonsgegevens*" ingevoerd te hebben.

47 Artikel 23 lid 2 AVG.

7. Documentatieplicht

In lijn met het vorige punt valt ook de documentatieplicht op.[48] Er moet een register aangelegd worden van verwerkingsactiviteiten en dat register moet "*indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1*" bevatten.

Deze verplichting geldt zowel voor de verwerkingsverantwoordelijke als voor de verwerker. De documentatieplicht is echter niet van toepassing op organisaties die minder dan 250 personen in dienst hebben,[49] tenzij de verwerking niet incidenteel is[50] en:

- het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen; of
- sprake is van de verwerking bijzondere categorieën van gegevens, als bedoeld in artikel 9, lid 1 AVG, of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 AVG.

Het is onduidelijk wanneer het wel en wanneer het niet mogelijk is de beveiligingsmatregelen te documenteren. De bijzin "*indien mogelijk*" roept dus meer vragen op dan deze beantwoordt. Hooguit maakt de bijzin duidelijk dat de documentatieplicht niet altijd ziet op het documenteren van de genomen beveiligingsmaatregelen. Deze verplichting kent aldus dezelfde onduidelijkheid als de verantwoordingsplicht die hiervoor is beschreven.

8. Gedragscodes

De AVG introduceert verder gedragscodes en certificeringsmechanismen. Voor beveiliging zijn deze relevant omdat is bepaald dat aansluiting bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme **kan** worden gebruikt als **element** om aan te tonen dat aan de vereisten van artikel 32 lid 1 AVG wordt voldaan.[51] De gedragscodes en certificeringsmechanismen werken in de kern als volgt.

Verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen kunnen gedragscodes opstellen.[52] Die gedragscodes

48 Artikel 30 AVG.

49 Artikel 30 lid 5 AVG.

50 Let wel, dit criterium van de "niet incidentele verwerking" heb ik uit de tekst gelicht en als algemene eis opgenomen. Kijkend naar de Nederlandse, Engelse en Duitse variant van de verordening is de plaats in de zin van dit criterium in de bepaling mij onduidelijk. Gelet op wat er in de considerans in overweging 13 is opgenomen over de ratio van de afwijking (vermindering administratieve lasten), en gelet op het gegeven dat ook kleinere ondernemingen en instellingen altijd wel bijzondere persoonsgegevens zullen verwerken, moet het criterium van "niet incidenteel" wel een algemeen criterium voor de uitzondering zijn. Anders zou iedere werkgever die bijvoorbeeld registreert dat zijn personeel ziek is toch weer aan de documentatieplicht gebonden zijn. Met andere woorden: hier lijkt sprake te zijn van een kennelijke verschrijving in de AVG.

51 Artikel 32 lid 3 AVG, welk artikel eigenlijk overbodig is omdat artikel 23 lid 3 AVG in meer algemene zin hetzelfde bepaalt.

52 Artikel 40 AVG.

kunnen onder meer voorschriften bevatten omtrent de te nemen beveiligingsmaatregelen en kunnen aan de nationale toezichthouder worden voorgelegd. Wanneer de gedragscode betrekking heeft op verwerkingen in één lidstaat, dan kan de betreffende nationale toezichthouder de gedragscode goedkeuren. Wanneer de gedragscode betrekking heeft op verwerkingen in meerdere lidstaten, dan dient de gedragscode via een specifieke goedkeuringsprocedure aan de andere toezichthouders en de Europese Commissie te worden voorgelegd. Vervolgens kan de Commissie beslissen dat de betreffende gedragscode algemeen geldig is.

De toezichthouder en/of geaccrediteerde certificeringsorganen kunnen certificaten afgeven waarmee de verwerkingsverantwoordelijke of de verwerker kan aantonen in overeenstemming met de AVG te handelen.[53] De certificaten worden afgegeven op grond van criteria die door de nationale toezichthouder of door het Comité (lees: WP29) zijn vastgesteld. Voor zover mij bekend zijn er op dit moment geen certificeringscriteria gepubliceerd, dus vooralsnog zal het nog niet van certificering kunnen komen. Naar mijn verwachting hebben de toezichthouders (voorlopig) wel andere zaken aan hun hoofd dan het vaststellen van dergelijke criteria. Het is daarmee maar zeer de vraag of het certificeringsproces snel op gang zal komen.

Het zou verder voor de praktijk zeer wenselijk zijn indien aansluiting gezocht wordt bij bestaande certificeringsmethoden. Dat lijkt echter niet mogelijk. Zowel de gedragscodes als de certificeringsmechanismen zijn immers bedoeld om aan te tonen dat de **gehele** AVG wordt nageleefd (en niet bijvoorbeeld louter de beveiligingsmaatregelen). Bestaande certificering tegen normen zoals ISO27001 en ISAE3402 is dus logischerwijs voor de AVG-certificering niet relevant. Dat is wat mij betreft een gemiste kans, mede ook omdat er al allerlei soorten ISO27001-/ISAE3402-certifcaten circuleren waarvan de kwaliteit en "waarde" niet altijd even duidelijk is.

9. Meldplicht datalekken

De AVG introduceert een EU-brede meldplicht datalekken. Het artikel lijkt wel wat op de huidige Nederlandse meldplicht datalekken.[54]

9.1 *Definitie datalek*

De AVG spreekt niet over datalekken maar over "*een inbreuk in verband met persoonsgegevens*", gedefinieerd als "*een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens*".[55]

Het is wat mij betreft winst dat de AVG, anders dan de Wbp, beschrijft wat bedoeld is met een dergelijke inbreuk en dat er aansluiting wordt gezocht bij de **gevolgen** van een bepaalde handeling.[56]

9.2 *Melding aan toezichthouder*

Een dergelijke inbreuk moet binnen 72 uur na kennisname worden gemeld aan de toezichthouder. Eventueel kan binnen 72 uur een melding worden gedaan waarin gemotiveerd wordt aangegeven waarom vertraging bij de melding zal ontstaan. Ook mag de aan te leveren informatie, indien nodig, in stappen worden verstrekt.[57] De melding aan de toezichthouder kan achterwege blijven indien "*niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen*".[58] De vraag is of deze drempel van "*een risico*" lager ligt dan het huidige Nederlandse criterium van "*aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens*".

De vraag voor de praktijk zal met name zijn hoe de AP en de andere Europese toezichthouders het criterium interpreteren. Strikt genomen is denkbaar dat de AP voor datalekken met alleen gevolgen in Nederland een eigen interpretatie geeft, en aldus voor Nederlandse datalekken een ander beleid voert dan voor datalekken met grensoverschrijdende gevolgen. Dat lijkt me echter geen wenselijke situatie. Het ligt dan ook eerder voor de hand dat via het in artikel 63 e.v. AVG opgenomen coherentiemechanisme EU-breed beleid wordt geformuleerd.

9.3. *Melding aan betrokkene*

De inbreuk moet eveneens aan de betrokkene worden medegedeeld indien de inbreuk "*waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen*". In drie gevallen mag deze melding aan de betrokkene achterwege blijven:[59]

a. er zijn "*passende technische en organisatorische beschermingsmaatregelen genomen*" op de betreffende persoonsgegevens "*met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling*";
b. er zijn "*achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen*";[60]

53 Artikel 42 AVG.
54 Artikel 33 AVG.
55 Artikel 4 sub 12 AVG.
56 De wetgever (en in navolging daarvan de AP) legt het criterium "*inbreuk op de beveiligingsmaatregelen*" uit als een inbreuk op al dan niet genomen maatregelen (meldplicht geldt ook bij ontbreken beveiliging) en zelfs op maatregelen die niet genomen hadden hoeven worden (meldplicht geldt ook als er ondanks passende beveiliging iets misgaat, dus bijvoorbeeld bij een hacker die de passende maatregelen te slim af is).
57 Artikel 33 lid 4 AVG.
58 Artikel 33 lid 1 AVG.
59 Artikel 34 lid 3 AVG.
60 Dit doet denken aan het resetten van wachtwoorden van een online dienstverlener of aan *remote wipe* van apparatuur. De vraag is echter of er voorafgaand aan het treffen van die maatregelen niet reeds een dusdanig hoog risico was dat alsnog een melding moet plaatsvinden.

c. "*de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd*".

9.4 *Documentatieplicht*

De verwerkingsverantwoordelijke is verder verplicht om alle inbreuken te documenteren.[61] Onder de huidige Nederlandse wetgeving hoeven alleen de meldingsplichtige inbreuken te worden gedocumenteerd. Naar de letter van de AVG moet iedere onrechtmatige toegang tot persoonsgegevens worden gedocumenteerd, ongeacht of dit opzettelijk of per ongeluk plaatsvindt. Dat gaat wel heel ver. Hopelijk leggen de toezichthouders de AVG op dit punt uit naar de geest/ratio van een dergelijke bepaling, en wordt in beleid vastgelegd dat alleen de meldingsplichtige inbreuken gedocumenteerd hoeven worden.

10. Internationale aspecten

Zoals hiervoor uiteengezet geldt onder de huidige Privacyrichtlijn 1995 dat een bewerker gehouden is de onder zijn nationale wetgeving verplichte beveiligingsmaatregelen te treffen. Onder het huidige regime is het dus principieel zo dat er nationale normen inzake de beveiliging van persoonsgegevens gelden. De beveiligingsnormen kunnen dus op dit moment verschillen in de 28 lidstaten van de EU.

De vraag is of dat onder de AVG straks anders wordt. Het gegeven dat er onder de AVG gedragscodes kunnen zijn die alleen op lidstatelijk niveau zijn goedgekeurd,[62] evenals certificaten die op lidstatelijk niveau worden afgegeven,[63] en dat aansluiting bij een gedragscode dan wel voeren van een dergelijk certificaat er toe kan bijdragen om aan te tonen dat de vereiste beveiligingsmaatregelen zijn genomen,[64] doet denken dat er nog steeds nationale verschillen in normen denkbaar zijn.

Voor grensoverschrijdende situaties geldt, zowel voor de gedragscode als de certificering, wel dat er via procedures een overkoepelende Europese norm wordt gehanteerd. Het ligt dus in de lijn der verwachting dat op termijn de nationale verschillen ten aanzien van beveiliging wel zullen vervagen.

11. Conclusie

Het onderwerp beveiliging krijgt ruimschoots aandacht onder de AVG.

Het wettelijk criterium was en blijft dat er "passende maatregelen" moeten worden genomen. De Nederlandse wetgever, de Nederlandse rechtspraak en de AP zoeken thans al aansluiting bij internationale normen als ISO27001 en het daarop gebaseerde NEN7510. Het lijkt voor de hand te liggen dat dit onder de AVG niet anders wordt.

Ogenschijnlijk nieuwe verplichtingen als "privacy by design" en "privacy by default" staan bij nadere beschouwing in feite al in de huidige Wbp. De AP stelt zich in ieder geval vanaf 2013 ook al ook op dat standpunt.

De AVG schenkt verder ruimschoots aandacht aan verantwoording en "compliance". In dat kader valt op dat van met name de grotere organisaties waarschijnlijk onder de AVG verwacht mag worden dat ze gedocumenteerd beveiligingsbeleid hebben. Ook onder huidig recht doen grotere organisaties daar echter al verstandig aan.

Verder valt op dat die (nieuwe) compliance-achtige verplichtingen met veel "mitsen en maren" zijn omgeven. De precieze strekking zal dus in de praktijk nog moeten blijken. Niettemin kan de introductie van al die verplichtingen wel als signaal worden beschouwd. Het lijkt er op dat de Europese wetgever van oordeel is dat van de verwerkingsverantwoordelijke meer mag worden verwacht op het gebied van beveiliging.

Met andere woorden: de norm verandert weliswaar niet (passend blijft passend), maar de Europese wetgever lijkt wel van oordeel te zijn dat de verwerkingsverantwoordelijke proactiever met (onder meer) het onderwerp beveiliging moet omgaan.

61 Artikel 33 lid 5 AVG.
62 Artikel 40 lid 6 AVG.
63 Artikel 42 lid 5 AVG.
64 Artikel 32 lid 3 AVG.