De Algemene Verordening Gegevensbescherming

mr. C.C.M Kroeks-de Raaij, mr. R.J.J. Westerdijk en prof. mr. G.J. Zwenne[1]

Het is (bijna) zover: de aloude Privacyrichtlijn 95/46 wordt na ruim 20 jaar vervangen. Na een lang en moeizaam traject is in de eerste helft van dit jaar een akkoord bereikt over een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Deze verordening brengt op tal van terreinen vernieuwingen in de regels inzake de bescherming van persoonsgegevens, en de impact daarvan zal groot zijn. In dit artikel belichten wij enige belangrijke wijzigingen.

1. Inleiding

Privacy is een hot topic, en is in vele opzichten relevant voor diensten die via internet worden aangeboden. Veel diensten, zoals bijvoorbeeld op het gebied van sociale media, worden gratis aan eindgebruikers aangeboden, maar echt gratis zijn die diensten natuurlijk niet. De aanbieders van dergelijke diensten verdienen hun geld door advertenties te verkopen in combinatie met hun gratis diensten, en advertenties worden beter verkocht wanneer deze beter gericht kunnen worden op de afnemers van de Internet diensten. Daarvoor wordt het gebruik van internetdiensten geanalyseerd, hetgeen op grote schaal het verwerken van persoonsgegevens inhoudt. Een ander voorbeeld is het gebruik van software online, en/of het daaraan gekoppelde opslaan van gegevens op afstand, in de cloud. Ook hierbij vindt op grote schaal verwerking van persoonsgegevens plaats, veelal door cloud-aanbieders in hun rol als verwerker. Het belang van regelgeving op het gebied van de verwerking van persoonsgegevens neemt daarmee uiteraard ook exponentieel toe.

De huidige privacyregelgeving is grotendeels gebaseerd op de aloude Privacyrichtlijn 95/46[2] die ruim 20 jaar geleden werd vastgesteld. Nu wordt die richtlijn vervangen door een verordening (hierna: 'de AVGB')[3], in een veel meer gedetailleerde regeling die er toe strekt om de bescherming van persoonsgegevens te vergroten. Daartoe worden ook de bevoegdheden van de toezichthoudende autoriteiten vergroot door de Europese introductie van het opleggen van boetes in geval van overtreding van de privacyregels: de maximale geldboete die kan worden opgelegd onder de AVGB bedraagt € 20 miljoen of 4% van de totale wereldwijde jaaromzet (zie art. 83). Het is daarmee duidelijk dat de AVGB een grote impact zal hebben op de vele diensten die via het Internet worden aangeboden.

In dit artikel zullen wij een aantal belangrijke elementen van de nieuwe regeling belichten. Volledigheid betrachten wij daarmee niet.[4] Wij gaan achtereenvolgens in op het proces van totstandkoming en inwerkingtreding van de AVGB, de vraag wanneer sprake is van een persoonsgegeven onder de AVGB, de territoriale reikwijdte van de AVGB, de uitbreiding van verplichtingen (met name voor verwerkers), de uitbreiding van de rechten van betrokkenen en de meldplicht voor datalekken.

Voordat wij overgaan tot deze inhoudelijke bespreking nog een kort woord over terminologie. Anders dan in het Engels introduceert de Nederlandse versie van de AVGB , in vergelijking met de huidige Wet bescherming persoonsgegevens ('Wbp'), enige nieuwe termen voor begrippen die in de huidige (rechts)praktijk al breed geworteld zijn. De 'verantwoordelijke' wordt in de AVGB aangeduid als 'verwerkingsverantwoordelijke' en de 'bewerker' heet nu 'verwerker'. Het doel van deze wijziging is ons onbekend en wij achten dit, gegeven de inburgering van deze termen en het groot aantal overeenkomsten waarin deze terminologie wordt gebruikt, bepaald ongelukkig. Desalniettemin hanteren wij in

1. Kea Kroeks-de Raaij is senior-jurist bij ABN AMRO te Amsterdam. Reinoud Westerdijk is advocaat bij Kennedy Van der Laan te Amsterdam. Gerrit-Jan Zwenne is advocaat bij Brinkhof te Amsterdam en hoogleraar Recht en de Informatiemaatschappij bij eLaw aan de Universiteit Leiden. De auteurs zijn alle drie lid van de redactie van dit tijdschrift.
2. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
3. 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).
4. Zie voor een algemeen overzicht van de AVGB tevens H.H. de Vries & M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming', *NJB* 2016, p. 1553-1560.

dit artikel toch alvast de nieuwe terminologie, ook voor gevallen waarin wordt verwezen naar de huidige regels onder de Wbp. In verband met deze en andere taalissues zijn sommige citaten uit de AVGB in dit artikel wel in het Engels opgenomen.

2. Proces van totstandkoming van de AVGB; inwerkingtreding

Na een lang en moeizaam traject is het er dan toch eindelijk van gekomen: de AVGB is vastgesteld. Zo'n 4 jaar eerder had de Commissie een voorstel hiertoe gepubliceerd.[5] Nadat het Europees Parlement en de Raad in respectievelijk 2014[6] en 2015[7] hun standpunten hadden gepubliceerd over de concept-AVGB, is vanaf juni 2015 een trialoog-proces gestart waarin de Raad, Commissie en Europees Parlement met elkaar hebben onderhandeld over de definitieve tekst van de AVGB. In niet minder dan 10 trialogen is overeenstemming over een compromistekst bereikt op 15 december 2015, welke tekst vervolgens is geaccordeerd door het Comité van Permanente Vertegenwoordigers en de Commissie LIBE van het Europees Parlement.

In de eerste maanden van 2016 is het vervolgens snel gegaan. Eind januari werd een politiek akkoord over de concept-verordening gepubliceerd.[8] Definitieve vaststelling van de verordening leek vervolgens nog geen gelopen race toen de Oostenrijkse regering aangaf niet akkoord te zijn met de compromistekst.[9] Niets bleek echter minder waar: nadat de Raad op 17 maart 2016 een concept 'Council Position at first reading' publiceerde[10], heeft de Raad vervolgens op 6 april 2016 zijn standpunt in eerste lezing aangenomen.[11] Na de Raad was het Europees Parlement aan de beurt om het politiek akkoord aan te nemen, en het Parlement heeft dat zeer voortvarend gedaan slechts twee dagen na de Raad, op 13 april 2016.[12]

De AVGB is gepubliceerd in het Publicatieblad van de Europese Unie op 4 mei 2016[13] en is daarmee in werking getreden op 25 mei 2016 (art. 99 lid 1 AVGB). De AVGB wordt vervolgens van toepassing op 25 mei 2018 (art. 99 lid 2 AVGB). Op dat moment wordt Richtlijn 95/46 ingetrokken (art. 94 lid 1 AVGB). Als verordening geldt de AVGB rechtstreeks binnen de gehele EU en dus ook in Nederland, en daardoor zal de Wbp per 25 mei 2018 ook grotendeels moeten worden ingetrokken. De AVGB laat de wetgever echter ook allerlei gebieden de mogelijkheid om bepaalde onderwerpen nader of anders te regelen[14], en het is nog niet duidelijk hoe onze wetgever daar invulling aan gaat geven.

3. Het persoonsgegeven: identificeerbaarheid of ook single-out?

Evenals Richtlijn 95/46 is de AVGB van toepassing op de verwerking van persoonsgegevens. De werkingssfeer van de AVGB, en daarmee de bevoegdheden van de toezichthouders, worden daardoor allereerst bepaald door wat wordt verstaan onder een persoonsgegeven. In haar voorstel van 25 januari 2012 ging de Commissie uit van eenzelfde definitie als thans wordt gebruikt in Richtlijn 95/46. Volgens deze begripsomschrijving is er sprake van een persoonsgegeven als het gaat om een gegeven betreffende een betrokkene of datasubject, zijnde

> *'een geïdentificeerde natuurlijke persoon of een natuurlijke persoon die direct of indirect, met behulp van middelen waarvan redelijkerwijs te verwachten is dat zij door de voor de verwerking verantwoordelijke dan wel door een andere natuurlijke persoon of rechtspersoon in te zetten zijn, kan worden geïdentificeerd'*

Een persoonsgegeven is, en blijft, dan een gegeven dat betrekking heeft op iemand van wie de identiteit bekend is of zonder onevenredige inspanning kan worden achterhaald.

5. Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), Brussel 25.1.2012, COM(2012) 11 final.
6. Standpunt Europees Parlement in eerste lezing van 12 maart 2014 (7427/14).
7. Algemene oriëntatie van de Raad d.d. 15 juni 2015 (9565/15).
8. Interinstitutioneel dossier 2012/0011 (COD), nr. 5455/16, Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming) [eerste lezing] - Politiek akkoord, Brussel 28 januari 2016. Zie http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/nl/pdf.
9. Zie de verklaring van Oostenrijk zoals gepubliceerd op 10 februari 2016, 5455/16 ADD 1 REV 1.
10. Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Draft Statement of the Council's reasons, dossier 2012/0011 (COD), nr. 5419/16, Brussel 17 maart 2016 (http://data.consilium.europa.eu/doc/document/ST-5419-2016-ADD-1/en/pdf).
11. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN.
12. Zie het persbericht van 14 april: http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era.
13. *PbEU* L 119/1.
14. Vergelijk bijvoorbeeld art. 8 (grens minderjarigheid) en 88 (verwerking in het kader van de arbeidsverhouding).

Vooruitlopend op de stemming in het Europees Parlement bleek dat vooral enkele privacybelangenorganisaties en toezichthouders een veel ruimere definitie wensten. In hun visie zou er niet alleen sprake zijn van een persoonsgegeven als het zou gaan om iemand waarvan de identiteit bekend is of zonder onevenredige inspanning bekend kan worden, maar ook als iemand kan worden onderscheiden van anderen ('singled-out') zonder dat zijn of haar identiteit bekend is. Volgens de Artikel 29 Werkgroep zou daarom de definitie van het persoonsgegeven ook de gegevens moeten omvatten betreffende een persoon die kan worden onderscheiden van anderen en daarom verschillend kan worden behandeld. De consequentie daarvan zou volgens de toezichthouders zijn dat bijvoorbeeld een IP-adres of MAC-adres, waarmee bijvoorbeeld een laptop of tablet op internet wordt geïdentificeerd, altijd als persoonsgegeven kwalificeert.[15]
Om deze verruiming van het persoonsgegevensbegrip tot uitdrukking te brengen, drong de werkgroep er op aan om dit op de volgende wijze in de preambule van de verordening op te nemen:

> *(23) The principles of protection should apply to any information concerning an identified or identifiable person and any information allowing a natural person to be singled out and treated differently. [onderstreping toegevoegd]*

In de begripsomschrijving van art. 4(2) zou vervolgens, in het voorstel van de werkgroep, moeten worden vastgelegd dat er niet alleen sprake zou zijn van een persoonsgegevens als het gaat om iemand die kan worden geïdentificeerd, maar ook als die persoon kan worden onderscheiden van anderen, zonder dat zijn of haar identiteit bekend is.

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

De werkgroep heeft heel hard gelobbyd voor deze verruiming van het persoonsgegevensbegrip[16] maar kon niet daarvoor de handen op elkaar krijgen. In Nederland liet de regering aan de Tweede Kamer in opmerkelijk duidelijke taal weten dat er bij haar en andere lidstaten '*geen enkele steun [was] voor het verder verfijnen van het begrip "persoonsgegevens" met categorieën als "singling out"*'.[17] In de versie waarover het Europees Parlement in oktober 2013 stemde, wordt dan ook slechts eenmaal het begrip single-out gebruikt, namelijk waar het gaat om de middelen waarvan gebruik kan worden gebruikt om te komen tot identificatie. Dezelfde bewoordingen worden gebruikt in de tekst van de verordening die uiteindelijk in het Publicatieblad staat. In overweging 26 staat nu

> *(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. [...] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. [onderstreping toegevoegd]*

Daaruit kan worden opgemaakt dat de identificeerbaarheid nog steeds bepalend is voor de kwalificatie van een gegeven als persoonsgegeven. Aan 'singling-out' komt alleen betekenis toe als het erom gaat van welke middelen gebruik kan worden gemaakt om iemand te identificeren. De mogelijkheid om iemand te onderscheiden van anderen draagt eraan bij dat deze persoon op enig moment kan worden geïdentificeerd, maar is géén zelfstandig criterium. In zoverre brengt de verordening dus toch geen wijzigingen ten opzichte van Richtlijn 95/46.[18]

4. De territoriale reikwijdte van de AVGB

De AVGB bevestigt de trend van een (langzaam) uitdijende toepasselijkheid van het Europese privacyrecht. Art. 4 Richtlijn 95/46 was al van toepassing op een verwerkingsverantwoordelijke die was gevestigd buiten de EU, mits voor het verwerken van persoonsgegevens gebruik werd gemaakt van al dan niet geautomatiseerde middelen die zich bevinden op het grondgebied van een EU-lidstaat.

15. In Nederland ging het College bescherming persoonsgegevens c.q. de Autoriteit persoonsgegevens al sinds 2007 in zo een tiental handhavingsonderzoeken uit van deze verruimde begripsomschrijving. Zie daarover o.a. G-J Zwenne, 'Nog enkele opmerkingen over IP-adressen en persoonsgegevens, identificeerbaarheid en 'single out'', *P&I* 2015/6, p. 206 t/m 221; G-J. Zwenne, De verwaterde privacywet, oratie Leiden, 12 april 2013; G-J. Zwenne, 'De regulering van IP-adressen', *IR* 2011/2, p. 40-43 en G-J. Zwenne, 'Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren', *IR* 2011/1, p. 4-9.
16. Zie bijv. Art. 29 Working Party, Opinion 08/2012 providing further input on the data protection reform discussions, 5 October 2012, p. 5-6; Der Hessische Datenschutzbeauftragte, Key data protection points for the trilogue on the General Data Protection Regulation 14 August 2015, p. 4-5.
17. *Kamerstukken II* 2012/13, 32761, nr. 51, p. 2.
18. Een bevestiging dat in de richtlijn niet al werd uitgegaan van een dergelijk verruimd persoonsgegevensbegrip kan worden gevonden in de Conclusie van A-G Campos Sánchez-Bordona van 12 mei 2016 in Zaak C-582/14 (*Patrick Breyer* vs *Bondsrepubliek Duitsland*), waarin afstand wordt genomen van de opvatting dat IP-adressen, zoals betoogd door de Art. 29 Werkgroep in Advies 4/2007 van 20 juni 2007, per definitie kwalificeren als persoonsgegevens.

Het Hof van Justitie heeft dat vervolgens behoorlijk verruimd in de bekende *Google Spain* uitspraak[19], door het hoofdcriterium van de 'verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke in Nederland' zodanig te interpreteren dat een lokale vestiging in een lidstaat van de EU voldoende kan zijn voor de toepassing van lokaal Europees recht zelfs daar waar de verwerkingsverantwoordelijke in de VS is gevestigd, indien de diensten van de lokale vestiging onlosmakelijk zijn verbonden met de activiteiten van de verwerkingsverantwoordelijke. De activiteiten van de lokale vestiging hoeven daarbij niet eens betrokken te zijn bij de verwerking van persoonsgegevens door de verwerkingsverantwoordelijke. Daarbij geldt bovendien dat het Hof nadien ook nog een ruime uitleg heeft gegeven aan het begrip 'vestiging', in de *Weltimmo*-uitspraak: het is voldoende indien de verwerkingsverantwoordelijke 'via een duurzame vestiging op het grondgebied van die lidstaat een, zelfs geringe, reële en daadwerkelijke activiteit uitoefent, in het kader waarvan die verwerking plaatsvindt'.[20] Deze verruimingen zijn recent vast gelegd in een update van de opinie van de Artikel 29 Werkgroep over het toepasselijk recht.[21]
De AVGB bepaalt ten aanzien van territoriale toepasselijkheid het volgende:

> *Artikel 3 - Territoriaal toepassingsgebied*
>
> *1. Deze verordening is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie plaatsvindt of niet.*
>
> *2. Deze verordening is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking betrekking heeft op:*
>
> *a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of*
>
> *b) het monitoren van hun gedrag, voor zover dit gedrag in de Europese Unie plaatsvindt.*
>
> *3. Deze verordening is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet in de Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht de nationale wetgeving van een lidstaat van toepassing is.*

Art. 3 lid 1 sluit aan bij het huidige art. 4 lid 1 Wbp (zoals gebaseerd op Richtlijn 95/46), met dien verstande dat het nu ook mag gaan om de vestiging van een verwerker en met de aanvullende verduidelijking 'ongeacht of de verwerking in de Unie plaatsvindt of niet'. Dit is in lijn met *Google Spain*, en ook met de update van de opinie van de Artikel 29 Werkgroep over het toepasselijk recht (WP 179).[22] De bestaande uitleg van het Hof van Justitie en de Artikel 29 Werkgroep blijft aldus relevant en van toepassing onder de AVGB. Een verschil met de huidige situatie is uiteraard dat het nu niet meer gaat om de toepasselijkheid van nationaal recht, maar dat bovengenoemd art. 3 AVGB bepaalt wanneer de *verordening* van toepassing is.
Art. 3 lid 2 bevat vervolgens een verdere verruiming vergeleken met de huidige situatie. Het huidige criterium van 'verwerking van persoonsgegevens door of ten behoeve van een verwerkingsverantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden' is niet langer van toepassing. Daarvoor in de plaats wordt nu een meer extraterritoriale toepasselijkheid bepaald, waarbij voor een verwerkingsverantwoordelijke *of verwerker* (!) buiten de EU in essentie van belang is dat sprake is van verwerking van persoonsgegevens van betrokkenen die zich in de Europese Unie bevinden. Daarbij gelden wel enige aanvullende criteria, namelijk dat het moet gaan om het aanbieden van goederen of diensten in de EU (zelfs als daarvoor niet wordt betaald), of het monitoren van het gedrag van de betrokkenen voor zover dit in de EU plaatsvindt. Wij kunnen ons bij lezing van deze aanvullende criteria niet aan de indruk onttrekken dat deze geschreven zijn om eventuele discussie over de toepasselijkheid van de verordening op gratis diensten van met name grote Amerikaanse social media en online aanbieders, zoals Google, Facebook en Amazon, te voorkomen.

5. Uitbreiding van verplichtingen, met name voor verwerkers

De AVGB kent op vele punten een uitbreiding van verplichtingen. Vergeleken met de huidige situatie vervalt echter ook een belangrijke verplichting, namelijk die van de verplichte melding van de verwerking van persoonsgegeven bij de toezichthoudende autoriteit. Overweging 89 van de AVGB zegt daarover het volgende:

> *'Richtlijn 95/46/EG voorzag in een algemene verplichting om de verwerking van persoons-*

19. Hof van Justitie 13 mei 2014, zaak C-131/12.
20. Hof van Justitie 1 oktober 2015, zaak C-230/14, r.o. 41.
21. Article 29 Data Protection Working Party, Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, WP 179 update (176/16/EN) van 16 december 2015.
22. Vergelijk WP 179, par. 4 op p. 7.

gegevens aan de toezichthoudende autoriteiten te melden. Die verplichting leidt tot administratieve en financiële lasten, maar heeft niet in alle gevallen bijgedragen tot betere bescherming van de persoonsgegevens. Die ongedifferentieerde algemene kennisgevingsverplichtingen moeten derhalve worden afgeschaft en worden vervangen door doeltreffende procedures en mechanismen die gericht zijn op de soorten verwerkingen die naar hun aard, reikwijdte, context en doeleinden waarschijnlijk grote risico's voor de rechten en vrijheden van natuurlijke personen met zich brengen. Dergelijke verwerkingen kunnen die zijn waarbij met name wordt gebruikgemaakt van nieuwe technologieën, of die welke van een nieuw type zijn en waarbij er vooraf geen gegevensbeschermingseffectbeoordeling is verricht door de verwerkingsverantwoordelijke, of wanneer zij noodzakelijk worden gelet op de tijd die sinds de aanvankelijke verwerking is verstreken.'

Naar onze mening lijkt dit echter mooier dan het is: onder de nieuwe noemer van 'accountability' worden veel van de verplichtingen die voorheen samenhingen met meldingen alsnog gehandhaafd. Dit zullen we in deze paragraaf toelichten.

Een ander belangrijk verschil onder de AVGB is de positie van de verwerker. Onder de Wbp lijken er in beginsel maar weinig verplichtingen direct te rusten op de verwerker. De verwerkingsverantwoordelijke is de partij die zich dient te houden aan de vereisten op grond van de Wbp en deze zal de afspraken ook zorgvuldig overeenkomen met eventuele verwerkers (en die op zijn beurt met mogelijke sub-verwerkers). Daarbij is met name van belang dat de technische waarborgen goed worden geregeld, het was immers de gedachte – bij het schrijven van de wet – dat wanneer dat goed geregeld is de persoonsgegevens veilig zijn. Het is de verwerkingsverantwoordelijke die deze afspraken vastlegt in een overeenkomst met de betreffende verwerker. Met de komst van de meldplicht datalekken, is dat nu ook vermeld als onderdeel van de te maken afspraken tussen verwerkingsverantwoordelijke en verwerker. Wat er nog meer in de verwerkersovereenkomst moet staan, wordt niet voorgeschreven door de Wbp, maar volgt uit CBP Richtsnoeren en Beleidsregels van de AP, en laatstelijk ook in een persbericht van AP.

Dit is anders onder de AVGB. Evenals onder de Wbp is duidelijk dat het treffen van de juiste organisatorische en technische beschermingsmaatregelen van belang is. Art. 28 AVGB begint met de verplichting aan de verwerkingsverantwoordelijke om alleen gebruik te maken van verwerkers als deze afdoende garanties bieden met betrekking tot het toepassen van organisatorische en technische maatregelen ten aanzien van de bescherming van de rechten van de betrokkene. Het artikel vervolgt direct in lid 2 met een verplichting aan de verwerker: het is niet toegestaan om een sub-verwerker in te schakelen zonder voorafgaande toestemming van de verwerkingsverantwoordelijke. Dit is duidelijk, maar niet nieuw. Wel nieuw is dat nu ook is beschreven hoe deze toestemming verkregen moet worden. Dit kan een specifieke of algemene toestemming zijn, welke schriftelijk moet worden verstrekt. Als een algemene toestemming is verkregen, dient de verwerker nog wel bij het daadwerkelijk inschakelen van een nieuwe verwerker de verwerkingsverantwoordelijke in te lichten en deze de mogelijkheid te bieden tot bezwaar.

5.1. Verwerkersovereenkomst

Zoals kort aangegeven staat in de Wbp vrijwel niets over de verwerkersovereenkomst. De Autoriteit Persoonsgegevens heeft in juli 2013, in haar rapport Smart TV[23], aangegeven dat een verwerkersovereenkomst noodzakelijk is en welke onderdelen daar in horen terug te komen. Erg helder was dit overigens niet want dit was niet de vraag die ten grondslag lag aan het rapport. Het gebrek aan een duidelijk juridisch kader voor de verhouding tussen de verwerkingsverantwoordelijke en verwerker is een risico voor de bescherming van de rechten en vrijheden van betrokkene. Daar komt nu een einde aan onder het nieuwe regime van de AGVB.

Art. 28 lid 3 AGVB benoemt alle elementen die ten minste onderdeel moeten uitmaken van de verwerkersovereenkomst, te weten:

a. de duur van de verwerking;
b. de aard en het doel van de verwerking;
c. het soort gegevens en de categorieën van betrokkenen;
d. de rechten en verplichtingen van de verwerkingsverantwoordelijke en dat de persoonsgegevens uitsluitend verwerkt mogen worden op basis van schriftelijke instructies van de verwerkingsverantwoordelijke;
e. vertrouwelijkheid;
f. het passend beveiligen van de persoonsgegevens (oftewel de technische en organisatorische maatregelen die getroffen moeten worden);
g. het uitvoeren van audits;
h. het na afloop vernietigen of terug leveren van de persoonsgegevens aan de verwerkingsverantwoordelijke.

De verwerker zal, wanneer hij overeenkomstig dit artikel gebruik maakt van een sub-verwerker, verplicht zijn om al zijn verplichtingen ook overeen te komen met de desbetreffende sub-verwerker.

5.2. Accountability

Een nieuw begrip onder de AVGB is 'accountability'. Het betreft hier een algemeen beginsel dat een zorgvuldige en correcte verwerking moet verzekeren. Onder de AVGB zal een verwerkingsverant-

23. 'Onderzoek naar de verwerking van persoonsgegevens met of door een Philips Smart tv door TP Vision Netherlands B.V. z2012-00605': https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/pb/pb_20130822-persoonsgegevens-smart-tv.pdf.

woordelijke, maar ook een verwerker, de passende en effectieve maatregelen treffen en moeten kunnen aantonen dat elke verwerking in lijn met de AVGB plaats vindt.[24] Dit uit zich in verschillende nieuwe verplichtingen, en deze verplichtingen gelden niet alleen voor de verwerkingsverantwoordelijke maar in veel gevallen ook voor de verwerker.
Een aantal voorbeelden:
- register van de verwerkingen (art. 30);
- gegevens bescherming door ontwerp en standaardinstelling ('Privacy by design and default) (art. 25);
- in bepaalde situaties een verplichte 'gegevensbeschermingseffectbeoordeling' (een 'Privacy Impact Analyse') door de verwerkingsverantwoordelijke (en waar nodig medewerking van de verwerker) (art. 35 en 36);
- in detail beschreven beveiligingsmaatregelen (art. 32);
- meldplicht van datalekken (art. 33).

Register
Iedere verwerkingsverantwoordelijke is verplicht een register bij te houden van alle verwerkingsactiviteiten. Dit kan schriftelijk of elektronisch. In het register moeten alle activiteiten worden omschreven waarbij het gaat om een verwerking van persoonsgegevens. Ook bedrijven met minder dan 250 werknemers die stelselmatig (bijzondere) persoonsgegevens verwerken, of als de verwerking een risico voor de betrokkene inhoudt, moeten een register bijhouden.
In het register moeten tenminste de volgende gegevens worden opgenomen:
- contactgegevens;
- de doeleinden van de gegevensverwerking;
- beschrijving van de categorieën van betrokkenen;
- eventuele ontvangers van de persoonsgegevens;
- beschrijving van de beveiligingsmaatregelen;
- en de beoogde bewaartermijnen.

De toezichthouder kan verzoeken tot inzage in het register voor controle. Het bijhouden van een register kan worden gezien als de vervanging van de meldplicht die is geschrapt. Daarmee is dus de lastenverlichting die de schrapping voor ogen had teniet gedaan.

Privacy by design and default
Bij de ontwikkeling van nieuwe producten en diensten moet men al rekening houden met de bescherming van de rechten van de betrokkenen. Hierdoor is het mogelijk om bijvoorbeeld gebruik te maken van bepaalde technieken, zoals pseudonimisering[25] van de gegevens. Maar denk ook aan de standaardinstellingen van bijvoorbeeld applicaties. Deze instellingen mogen niet standaard minder gunstig voor de betrokkene zijn ingesteld dan mogelijk. Waar vaak zoveel mogelijk gegevens worden verzameld, geldt dat alleen de noodzakelijke persoonsgegevens mogen worden verwerkt. Dit is op zich niet anders onder de huidige beginselen in de Wbp. Dit geldt ook voor de toegankelijkheid tot de gegevens, alleen die personen die er noodzakelijkerwijs bij moeten mogen toegang krijgen. Dit is niet nieuw. Wel nieuw aan dit fenomeen is dat men er dus reeds bij aanvang al over na zal moeten denken en zich er niet van af kan maken met een privacy statement na ontwikkeling.

Privacy Impact Analyse
De AVGB geeft aan dat een onderzoek moet worden verricht als de verwerking van persoonsgegevens een hoog risico voor de betrokkene kan opleveren. Het onderzoek is verplicht in het geval van 'profiling', grootschalige verwerking van bijzondere persoonsgegevens of bij monitoring van openbare ruimten. Bij het onderzoek staat centraal welke risico's aanwezig zijn bij de verwerking en zal dit duidelijk moeten worden vastgelegd, evenals de beoordeling van deze risico's. Het onderzoek moet ook de basisgegevens van de verwerking vermelden zoals de termijn, waarom en hoe de persoonsgegevens verwerkt worden. Het kan in sommige gevallen nodig zijn om als verwerkingsverantwoordelijke met de betrokkene de uitslag van het rapport te bespreken.

Beveiligingsmaatregelen
In tegenstelling tot de Wbp bevat de AGVB gedetailleerde bepalingen over de te treffen beschermingsmaatregelen. Zo bevat art. 32 lid 1 een viertal maatregelen die ten minste moeten worden geïmplementeerd om te kunnen spreken van passende maatregelen. De minimale maatregelen zijn:
- pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- 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.

Hoewel dit enerzijds verplichtingen met zicht mee brengt, is het ook duidelijk. Althans dat hopen we.

24. Zie overweging 74 bij de AVGB.
25. Dit begrip is in de AVGB ook gedefinieerd, in art. 4 sub 5: '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 tekst zelf biedt nog steeds erg veel ruimte voor interpretatie, maar de tijd zal leren of dit voldoende is.
Hoewel de AVGB strekt tot het verder verstevigen van de bescherming van de rechten en vrijheden van de betrokkene, was tevens een doelstelling om tot een financiële en organisatorische lastenverlichting te komen. Dat laatste lijkt niet te worden bereikt met de invoering van de AVGB. Of het eerste wel bereikt wordt, zullen we moeten afwachten.

6. Uitbreiding van rechten van betrokkenen

Een van de belangrijkere doelstellingen van de verordening, zo blijkt uit de preambule ervan, is het versterken van de rechtspositie van de betrokkenen. In de preambule lezen we niet alleen de misschien niet helemaal goed doordachte veronderstelling dat iedereen controle zou moeten hebben over zijn en haar gegevens, maar ook dat de rechten van betrokkenen moeten worden versterkt en nader moeten worden uitgewerkt.[26]
De versterking en nadere uitwerking van de rechten van betrokkenen blijkt allereerst uit de veel gedetailleerdere regels met betrekking tot de informatieverplichtingen van verwerkingsverantwoordelijken en de inzage- en verbeteringsrechten van betrokkenen. Wat dat betreft zien we dat de AVGB in veel meer detail uiteenzet welke informatie in elk geval door verwerkingsverantwoordelijken moet worden verstrekt aan betrokkenen. Zo moet, waar het gaat om de aan de betrokkene te verstrekken informatie, niet alleen mededeling worden gedaan van de identiteit van de verwerkingsverantwoordelijke en de verwerkingsdoeleinden, maar ook van achtereenvolgens:

- de contactgegevens van een functionaris als die er is;
- de verwerkingsgrondslagen en in voorkomend geval het gerechtvaardigd belang van de verwerkingsverantwoordelijke als van die grondslag gebruik wordt gemaakt;
- de (categorieën van) ontvangers van de gegevens;
- doorgiften naar derde landen als daarvan sprake is;
- bewaartermijnen;
- de mogelijkheden om gebruik te maken van inzage- en verbeteringsrechten of verzetsrechten;
- de mogelijkheden om te klagen bij de toezichthouder;
- eventuele verwerkingen in het kader van geautomatiseerde besluitvorming en profilering, en,
- als de gegevens bij een ander zijn verkregen, ook de bron waaruit deze zijn verkregen.

Een inzageverzoek kan *grosso modo* op al deze gegevens betrekking hebben.

In aanvulling op deze reeds in Richtlijn 95/46 opgenomen, maar in de AVGB verder uitgewerkte rechten wordt er voorzien in een aantal heel nieuwe rechten. Het gaat dan om het vergeetrecht ('right to be forgotten' of in de wat oubollige Nederlandse vertaling 'recht op vergetelheid') van art. 17 AVGB en het recht op gegevensoverdraagbaarheid van art. 20 AVGB.
Het *'vergeetrecht'* is natuurlijk pas goed onder de aandacht gekomen door de *Google Spain*-uitspraak.[27] In de AVGB ziet dit op de situatie waarin persoonsgegevens op verzoek van de betrokkene zonder onredelijke vertraging moeten worden gewist, bijvoorbeeld omdat deze werden verwerkt op basis van door de betrokkene verleende toestemming en deze inmiddels is ingetrokken door de betrokkene. In een dergelijk geval kan de betrokkene, onder voorwaarden, ook verlangen dat de verwerkingsverantwoordelijke redelijke maatregelen neemt om anderen ervan op de hoogte te stellen dat die betrokkene heeft verzocht de gegevens te verwijderen. Het recht wordt, zo blijkt uit de overwegingen, door de uniewetgever vooral relevant geacht als de betrokkene zijn of haar toestemming heeft gegeven als kind, toen hij of zijn zich nog niet volledig bewust was van de verwerkingsrisico's, en hij dergelijke persoonsgegevens later wil verwijderen, met name van het Internet.[28]
Het recht op *gegevensoverdraagbaarheid* stelt de betrokkene in de gelegenheid de door hem of haar zelf aan een verwerkingsverantwoordelijke verstrekte gegevens onder voorwaarden op te vragen in een gestructureerde, gangbare ('interoperabel') en machineleesbare vorm. Vervolgens kan de betrokkene deze gegevens overdragen aan een andere verwerkingsverantwoordelijke. Voor zover dit technisch haalbaar is, heeft de betrokkene het recht dat de gegevens direct van de ene naar de andere verwerkingsverantwoordelijke worden doorgezonden.[29]
Het wordt daarmee mogelijk om gemakkelijk van bijvoorbeeld het éne sociale netwerk over te stappen naar het andere.

7. Meldplicht datalekken

Sinds januari 2016 geldt in Nederland op basis van een wijziging van de Wbp al een meldplicht voor datalekken. Deze lijkt ruimer te zijn dan de meldplicht zoals opgenomen in de AVGB als men bijvoorbeeld kijkt naar de tijdslijnen die daar gehanteerd worden.
Het nieuwe art. 34a Wbp heeft de meldplicht als volgt verwoord in lid 1:

> *1. De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen*

26. Resp. overweging 7 en 11.

27. Hof van Justitie 13 mei 2014, zaak C-131/12.
28. Overweging 65.
29. Overweging 68.

> *dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.*

Naast de meldplicht aan de Autoriteit Persoonsgegevens, moet de verwerkingsverantwoordelijke ook melden aan de betrokkene als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (art. 34a lid 2 Wbp). Als de verwerkingsverantwoordelijke gebruikmaakt van een verwerker zal hierover een afspraak gemaakt moeten worden in de verwerkersovereenkomst om te verzekeren dat de verwerkingsverantwoordelijke op tijd wordt geïnformeerd om aan zijn verplichtingen te kunnen voldoen.
De AGVB kent een drietal meldplichten voor datalekken: 1) de meldplicht aan de toezichthoudende autoriteit, 2) de meldplicht aan de betrokkene, en 3) de meldplicht van de verwerker aan de verwerkingsverantwoordelijke. Art. 33 bevat de melding aan de toezichthoudende autoriteit. In lid 1 van dit artikel staat het volgende:

> *1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.*

Uit deze tekst volgt dat wanneer sprake is van een inbreuk waarbij persoonsgegevens zijn betrokken, ongeacht of dit opzettelijk is gebeurd of per ongeluk, hiervan binnen 72 uur melding moeten worden gemaakt bij de toezichthouder. Uit lid 2 van hetzelfde artikel blijkt dat de verwerker de verwerkingsverantwoordelijke zonder onredelijke vertraging moet informeren over een dergelijke inbreuk. Van belang is dat de melding moet geschieden vanaf het moment dat 'hij' kennis heeft genomen van de inbreuk, waarbij het 'hij' in lid 1 betrekking heeft op de verantwoordelijk en in lid 2 op de verwerker. Dit biedt ruimte voor de tijdslijnen. Onder de Wbp gaat de klok tikken op het moment dat het lek is ontdekt, ongeacht of dit bij de verwerkingsverantwoordelijke is of een verwerker. [30]
Onder de AVGB hoeft de melding aan de toezichthouder alleen plaats te vinden in die situaties waarin het waarschijnlijk is dat het datalek een risico voor de rechten en vrijheden van de betrokkene met zich mee brengt. Er is alleen dan sprake van een datalek in geval van een inbreuk op de beveiliging met betrekking tot persoonsgegevens.
Dit lijkt af te wijken van de huidige meldplicht datalekken. Daarbij kan volgens de toezichthouder al sprake zijn van een datalek (inbreuk op de beveiliging) wanneer bij het incident de onrechtmatige verwerking van persoonsgegevens niet kan worden uitgesloten. En die situatie moet, als dit leidt tot een aanzienlijke kans op nadelige gevolgen voor de betrokkene, gemeld worden bij de Autoriteit Persoonsgegevens. Onder de Wbp zal mogelijk in meer situaties dan het aantal dat gemeld moet worden onder de AVGB, een melding bij de Autoriteit Persoonsgegevens moeten plaatsvinden. Wellicht dat hier een lastenverlichting is beoogd te bewerkstelligen?
Daarnaast hoeft onder de AVGB de betrokkene alleen te worden geïnformeerd wanneer het lek waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkene meebrengt, zo blijkt uit art. 34 AVGB.
De meldplicht onder de AVGB lijkt daarmee minder strikt dan de huidige meldplicht die in Nederland geldt op basis van de Wbp. Dit zal een gunstige uitwerking kunnen hebben voor de verwerkingsverantwoordelijken. Zo zijn de tijdslijnen waarschijnlijk beter te implementeren. Ook wordt het waarschijnlijk makkelijker om afspraken te maken met eventuele verwerkers omdat zij nu ook een wettelijke meldplicht gaan hebben.

8. Varia; afronding

Het is in het kader van dit artikel helaas niet mogelijk om in te gaan op alle aspecten van de nieuwe AVGB. Interessant en zeer relevant voor de praktijk is bijvoorbeeld ook de regeling voor doorgifte van persoonsgegevens aan landen buiten de EU. Dit is in de AVGB geregeld in art. 45 en 46 en in essentie verandert hier niet zoveel. Het onderwerp is echter zeer actueel en 'explosief' vanwege het *Schrems*-arrest van het Hof van Justitie en het sneuvelen van het Safe Harbor regime in de Verenigde Staten. Verder wil het met de opvolger ervan, het EU-US Privacy Shield, nog niet zo vlotten.[31] Op dit punt zal vermoedelijk wel meer duidelijkheid zijn op het moment dat de AVGB daadwerkelijk van toepassing is.
Een ander interessant onderwerp betreft de vraag welke toezichthouder (primair) bevoegd is om de privacyregels te handhaven jegens partijen die ergens anders zijn gevestigd dan in de betreffende lidstaat van de toezichthouder. De AVGB beoogt

30. College bescherming persoonsgegevens, 'Onderzoek naar de verwerking van persoonsgegevens met of door een Philips Smart tv door TP Vision Netherlands B.V.', z2012-00605; p.32 (via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf).

31. Zie recent ook Opinion 4/2016 van de European Data Protection Supervisor van 30 mei 2016 'Opinion on the EU-U.S. Privacy Shield draft adequacy decision', https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf.

op dit punt meer stroomlijning te bewerkstelligen door de introductie van een zogenaamde 'one stop shop', waarbij sprake is van 1 leidende toezichthouder. De regeling hiervoor in art. 56 bevat echter nog de nodige ruimte voor betrokkenheid van andere toezichthouders, dus het is de vraag in hoeverre op dit punt werkelijk een verbetering zal worden gerealiseerd.

Al met al is echter duidelijk dat ook de komende jaren het privacyrecht duidelijk op de kaart staat. Bedrijven zullen aanzienlijke investeringen moeten doen om zich voor te bereiden op de situatie na 25 mei 2018. Ook de rechters zullen meer en meer met het onderwerp geconfronteerd worden, al was het maar omdat de AVGB veel meer bepalingen kent dan voorheen, bepalingen die uiteraard geïnterpreteerd en uitgelegd moeten worden. Of betrokkenen hiermee uiteindelijk gediend zijn, is een vraag, die hopelijk de komende jaren beantwoord gaat worden.