

Editie 2023/24

en Uitvoeringswet AVG

Artikelsgewijs commentaar

Arnoud Engelfriet
Caroline van Ekeren
Peter Kager



De Algemene Verordening Gegevensbescherming

Editie 2023/24

**en Uitvoeringswet AVG
Artikelsgewijs commentaar**

Arnoud Engelfriet
Caroline van Ekeren
Peter Kager



ISBN 978-90-830957-4-5

Copyright © 2023 ICTRecht B.V.

Uitgever: Ius Mentis te Amsterdam

Omslag, ontwerp, zetwerk: Marian van Helden, Deventer

Alles uit deze uitgave mag worden verveelvoudigd en/of openbaar worden gemaakt door middel van druk, fotokopie, geluidsband, elektronisch of op welke wijze dan ook, onder de vereisten van de Creative Commons licentie Naamsvermelding-Gelijkdelen versie 2.5 Nederlands, zie <https://creativecommons.org/licenses/by-sa/2.5/nl/>

Voorwoord

**prof. mr. Gerrit-Jan Zwenne, Universiteit Leiden en Open Universiteit,
alsmede advocaat te Den Haag**

Er is nog steeds veel onduidelijk in de Algemene verordening gegevensbescherming. Deze privacywet, of gegevensbeschermingswet zoals sommigen wel zeggen, kent vele open begrippen, vage normen en niet zonder meer begrijpelijke regels. Het is de bedoeling dat die in de praktijk moeten worden ingevuld en geconcretiseerd, en opgehelderd. En dat gebeurt ook wel, vooral in de rechtspraak, maar wel mondjesmaat.

Zo heeft de hoogste bestuursrechter, de Afdeling bestuursrecht van de Raad van State, inmiddels bevestigd dat een IP-adres geen persoonsgegeven is als de verwerkingsverantwoordelijke niet kan beschikken over de benodigde gegevens om een koppeling te kunnen maken tussen dat IP-adres en internetgebruiker die daarvan gebruik maakte (aldus ABRvS 13 juli 2022 ECLI:NL:RVS:2022:1993, rov. 5.3).

In de rechtspraak over het vergeetrecht is duidelijk geworden dat er pas sprake is van strafrechtelijk gegeven als het gaat om 'zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring kunnen dragen'. Er moet sprake zijn van 'een zwaardere verdenking dan een redelijk vermoeden van schuld'. Een fraudesignaal is dus nog niet een strafrechtelijk gegeven, maar zou dat in voorkomend geval wel kunnen zijn. (zie o.a. rechtbank Den Haag 12 januari 2017, ECLI:NL:RBDHA:2017:264, rov 4.12-14).

Maar veel is nog onduidelijk. Of hangt af, zoals juristen het graag zeggen, van de omstandigheden van het geval. Is uw geboortedatum een gezondheidsgegeven? En uw lichaamslengte al dan niet in combinatie met gewicht? Wie is verwerkingsverantwoordelijke of verwerker als u bij ChatGTP navraag doet naar de sollicitanten? En hoezo zou een zuiver commercieel belang niet kunnen worden opgevat als een gerechtvaardigd belang? Het zijn vragen waarop het antwoord nog niet gegeven is.

In het naslagwerk dat u nu in handen hebt zult u, het kan niet anders, niet alle antwoorden vinden op al uw vragen over de Avg. Maar als wetgever of rechter het antwoord, of een begin van een antwoord, hebben gegeven, dan vindt u dat in dit naslagwerk.

Genève / Den Haag

april 2023

Inhoudsopgave

Voorwoord	5
ALGEMENE VERORDENING GEGEVENSBESCHERMING	
Hoofdstuk I	
Algemene bepalingen	17
Artikel 1. Onderwerp en doel van de AVG	17
Artikel 2. Materiële toepasselijkheid van de AVG	19
Artikel 3. Territoriale toepasselijkheid	22
Artikel 4. Definities	26
Hoofdstuk II	
Beginnelsen voor verwerking	45
Artikel 5. Beginselen inzake de verwerking van persoonsgegevens	45
Artikel 6. Rechtmatigheid van de verwerking	50
Artikel 7. Voorwaarden voor toestemming	58
Artikel 8. Voorwaarden voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij	62
Artikel 9. Verwerking van bijzondere persoonsgegevens	64
Artikel 10. Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten	75
Artikel 11. Geen identificatieplicht	77
Hoofdstuk III	
Rechten van de betrokkene	79
<i>Afdeling 1</i>	
<i>Transparantie en regelingen</i>	79
Artikel 12. Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene	80
<i>Afdeling 2</i>	
<i>Informatie en toegang tot persoonsgegevens</i>	85
Artikel 13. Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld	85
Artikel 14. Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen	89
Artikel 15. Recht van inzage van de betrokkene	96

Afdeling 3

Rectificatie en wissing van gegevens 100

Artikel 16. Recht op rectificatie 100

Artikel 17. Recht op gegevenswissing ("recht op vergetelheid") 101

Artikel 18. Recht op beperking van de verwerking 106

Artikel 19. Kennisgevingsplicht inzake rectificatie, wissing of beperking 109

Artikel 20. Recht op overdraagbaarheid van gegevens 110

Afdeling 4

Recht van bezwaar en geautomatiseerde individuele besluitvorming 113

Artikel 21. Recht van bezwaar 114

Artikel 22. Geautomatiseerde individuele besluitvorming, waaronder profilering 116

Afdeling 5

Beperkingen 120

Artikel 23. Beperkingen 120

Hoofdstuk IV

Verwerkingsverantwoordelijke en verwerker 127

Afdeling 1

Algemene verplichtingen 127

Artikel 24. Verantwoordelijkheid van de verwerkingsverantwoordelijke 127

Artikel 25. Gegevensbescherming door ontwerp en door standaardinstellingen 131

Artikel 26. Gezamenlijke verwerkingsverantwoordelijken 133

Artikel 27. Vertegenwoordigers van niet in de Unie gevestigde verwerkingsverantwoordelijken of verwerkers 135

Artikel 28. Verwerker 138

Artikel 29. Verwerking onder gezag van de verwerkingsverantwoordelijke of de verwerker 147

Artikel 30. Register van de verwerkingsactiviteiten 147

Artikel 31. Medewerking met de toezichhoudende autoriteit 151

Afdeling 2

Persoonsgegevensbeveiliging 152

Artikel 32. Beveiliging van de verwerking 152

Artikel 33. Melding van een inbreuk in verband met persoonsgegevens aan de toezichhoudende autoriteit 155

Artikel 34. Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene 159

Afdeling 3

Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging 163

Artikel 35. Gegevensbeschermingseffectbeoordeling 163

Artikel 36. Voorafgaande raadpleging 170

<i>Afdeling 4</i>	
<i>Functionaris voor gegevensbescherming</i>	173
Artikel 37. Aanwijzing van de functionaris voor gegevensbescherming	173
Artikel 38. Positie van de functionaris voor gegevensbescherming	178
Artikel 39. Taken van de functionaris voor gegevensbescherming	180
<i>Afdeling 5</i>	
<i>Gedragscodes en certificering</i>	182
Artikel 40. Gedragscodes	183
Artikel 41. Toezicht op goedgekeurde gedragscodes	189
Artikel 42. Certificering	191
Artikel 43. Certificeringsorganen	195
Hoofdstuk V	
Doorgifte aan derde landen en internationale organisaties	201
Artikel 44. Algemeen beginsel inzake doorgiften	201
Artikel 45. Doorgiften op basis van adequaatheidsbesluiten	203
Artikel 46. Doorgiften op basis van passende waarborgen	208
Artikel 47. Bindende bedrijfsvoorschriften	212
Artikel 48. Niet bij Unierecht toegestane doorgiften of verstrekkingen	218
Artikel 49. Afwijkingen voor specifieke situaties	219
Artikel 50. Internationale samenwerking voor de bescherming van persoonsgegevens	224
Hoofdstuk VI	
Onafhankelijke toezichthoudende autoriteiten	227
<i>Afdeling 1</i>	
<i>Onafhankelijkheid</i>	227
Artikel 51. Toezichthoudende autoriteit	227
Artikel 52. Onafhankelijkheid van de toezichthouder	229
Artikel 53. Algemene voorwaarden voor de leden van de toezichthoudende autoriteit	231
Artikel 54. Regels inzake de oprichting van de toezichthoudende autoriteit	232
<i>Afdeling 2</i>	
<i>Competentie, taken en bevoegdheden</i>	233
Artikel 55. Competentie van toezichthouders	233
Artikel 56. Competentie van de leidende toezichthoudende autoriteit	235
Artikel 57. Taken	238
Artikel 58. Bevoegdheden van toezichthouders	244
Artikel 59. Activiteitenverslagen	251

Hoofdstuk VII

Samenwerking en coherentie 253

Afdeling 1

Samenwerking 253

Artikel 60. Samenwerking tussen de leidende toezichthoudende autoriteit
en andere betrokken toezichthoudende autoriteiten 254

Artikel 61. Wederzijdse bijstand 258

Artikel 62. Gezamenlijke werkzaamheden van toezichthoudende
autoriteiten 261

Afdeling 2

Coherentie 264

Artikel 63. Coherentiemechanisme 264

Artikel 64. Advies van het Comité 265

Artikel 65. Geschillenbeslechting door het Comité 269

Artikel 66. Spoedprocedure 272

Artikel 67. Uitwisseling van informatie 274

Afdeling 3

Europees Comité voor gegevensbescherming 274

Artikel 68. Europees Comité voor gegevensbescherming 275

Artikel 69. Onafhankelijkheid 276

Artikel 70. Taken van het Comité 277

Artikel 71. Rapportage 284

Artikel 72. Procedure 285

Artikel 73. Voorzitter 285

Artikel 74. Taken van de voorzitter 286

Artikel 75. Secretariaat 286

Artikel 76. Vertrouwelijkheid 288

Hoofdstuk VIII

Beroep, aansprakelijkheid en sancties 289

Artikel 77. Recht om klacht in te dienen bij een toezichthoudende
autoriteit 289

Artikel 78. Recht om een doeltreffende voorziening in rechte in te
stellen tegen een toezichthoudende autoriteit 290

Artikel 79. Voorziening in rechte tegen verwerkingsverantwoordelijke of
verwerker 293

Artikel 80. Vertegenwoordiging van betrokkenen 295

Artikel 81. Schorsing van de procedure 296

Artikel 82. Recht op schadevergoeding en aansprakelijkheid 297

Artikel 83. Voorwaarden aan het opleggen van administratieve geldboeten 300

Artikel 84. Andere sancties 306

Hoofdstuk IX

Specifieke verwerkingen 309

Artikel 85. Verwerking en vrijheid van meningsuiting en van informatie	309
Artikel 86. Verwerking en recht van toegang van het publiek tot officiële documenten	312
Artikel 87. Verwerking van het nationaal identificatienummer	313
Artikel 88. Verwerking in het kader van de arbeidsverhouding	314
Artikel 89. Waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden	315
Artikel 90. Geheimhoudingsplicht	321
Artikel 91. Bestaande gegevensbeschermingsregels van kerken en religieuze verenigingen	322

Hoofdstuk X

Gedelegeerde handelingen 323

Artikel 92. Uitoefening van de bevoegdheidsdelegatie	323
Artikel 93. Comitéprocedure	324

Hoofdstuk XI

Slotbepalingen en overgangsrecht 327

Artikel 94. Intrekking van Richtlijn 95/46/EG	327
Artikel 95. Verhouding tot Richtlijn 2002/58/EG	328
Artikel 96. Verhouding tot eerder gesloten overeenkomsten	329
Artikel 97. Evaluatie Commissieverslagen	329
Artikel 98. Toetsing van andere Unierechtshandelingen inzake gegevensbescherming	331
Artikel 99. Inwerkingtreding en toepassing	331

UITVOERINGSWET ALGEMENE VERORDENING GEGEVENSBESCHERMING

Hoofdstuk 1

Algemene bepalingen 335

Artikel 1. Definities	335
Artikel 2. Materiële reikwijdte	336
Artikel 2a. Inachtneming behoeften kleine, middelgrote en micro-ondernemingen	337
Artikel 3. Schakelbepaling verwerkingen buiten werkingssfeer verordening	337
Artikel 4. Territoriale reikwijdte	339
Artikel 5. Toestemming van wettelijk vertegenwoordiger	340

Hoofdstuk 2

De Autoriteit persoonsgegevens 343

Paragraaf 2.1

Oprichting en inrichting van de autoriteit persoonsgegevens 343

Artikel 6. Oprichting en aanwijzing als toezichthoudende autoriteit 343

Artikel 7. Samenstelling 344

Artikel 8. Disciplinaire maatregelen voorzitter en andere leden 345

Artikel 9. Rechtspositie voorzitter, andere leden en buitengewone leden 346

Artikel 10. Secretariaat 346

Artikel 11. Begroting, verantwoording en vertegenwoordigingsbevoegdheid 347

Artikel 12. Beperking inlichtingenplicht jegens minister 348

Artikel 13. Uitzonderingen bevoegdheden inzake beleidsregels, vernietiging en
taakverwaarlozing 348

Paragraaf 2.2

De uitoefening van de taken en bevoegdheden van de Autoriteit persoonsgegevens 348

Artikel 14. Taken en bevoegdheden 348

Artikel 15. Toezicht op de naleving 350

Artikel 16. Last onder bestuursdwang 351

Artikel 17. Boete bij onrechtmatige verwerking persoonsgegevens
strafrechtelijke aard 351

Artikel 18. Bestuurlijke boete aan overheden 352

Artikel 19. Samenwerking met andere toezichthouders 353

Artikel 20. In rechte optreden tegen inbreuken op verordening inzake doorgifte
naar derde land 353

Artikel 21. Aanwijzing accrediterende instantie 355

Artikel 21a. Toezicht op naleving PSD II 356

Hoofdstuk 3

Bepalingen ter uitvoering van de verordening 359

Paragraaf 3.1

Bijzondere categorieën van persoonsgegevens 359

Artikel 22. Verwerkingsverbod bijzondere categorieën persoonsgegevens en
algemene uitzonderingen uit verordening 359

Artikel 23. Nationaalrechtelijke algemene uitzonderingen 360

Artikel 24. Uitzonderingen voor wetenschappelijk of historisch onderzoek of
statistische doeleinden 361

Artikel 25. Uitzonderingen inzake verwerking persoonsgegevens waaruit ras of
etnische afkomst blijkt 362

Artikel 26. Uitzonderingen inzake verwerking persoonsgegevens waaruit
politieke opvattingen blijken voor vervulling openbare functies 363

Artikel 27. Uitzonderingen inzake verwerking persoonsgegevens waaruit
religieuze of levensbeschouwelijke overtuigingen blijken voor
geestelijke verzorging 364

Artikel 28. Uitzonderingen inzake genetische gegevens	364
Artikel 29. Uitzonderingen inzake biometrische gegevens	365
Artikel 30. Uitzonderingen inzake gegevens over gezondheid	366
<i>Paragraaf 3.2</i>	
<i>Persoonsgegevens van strafrechtelijke aard</i>	369
Artikel 31. Uitzonderingen op de verplichting tot verwerking onder overheidstoezicht	369
Artikel 32. Algemene uitzonderingsgronden inzake gegevens van strafrechtelijke aard	369
Artikel 33. Overige uitzonderingsgronden inzake gegevens van strafrechtelijke aard	371
<i>Paragraaf 3.3</i>	
<i>Rechtsbescherming</i>	373
Artikel 34. Toepasselijkheid Algemene wet bestuursrecht bij beslissing van bestuursorganen	373
Artikel 35. Toepasselijkheid burgerlijk recht bij beslissing van niet-bestuursorganen	374
Artikel 36. Geschilbeslechting door Autoriteit persoonsgegevens of via gedragscode	375
Artikel 37. Vertegenwoordiging van betrokkenen	376
Artikel 38. Opschortende werking bezwaar en beroep	376
<i>Paragraaf 3.4</i>	
<i>De functionaris voor gegevensbescherming</i>	377
Artikel 39. Geheimhoudingsplicht	377
Hoofdstuk 4	
Uitzonderingen en beperkingen	379
Artikel 40. Uitzonderingen op verbod geautomatiseerde individuele besluitvorming	379
Artikel 41. Uitzonderingen op rechten betrokkene en plichten verwerkingsverantwoordelijke	380
Artikel 42. Uitzondering op meldplicht datalekken aan de betrokkene	382
Artikel 43. Uitzonderingen inzake journalistieke doeleinden of academische, artistieke of literaire uitdrukkingvormen	382
Artikel 44. Uitzonderingen inzake wetenschappelijk onderzoek en statistiek	385
Artikel 45. Uitzonderingen inzake archivering in het algemeen belang	386
Artikel 46. Verwerking nationaal identificatienummer	387
Artikel 47. Uitzonderingen op rechten betrokkene bij openbare registers	387

Hoofdstuk 5	
Overgangs- en slotbepalingen	389
Artikel 48. Overgangsrecht	389
Artikel 48a. Overgangsrecht II	392
Artikel 49. Samenloop	393
Artikel 50. Evaluatie	393
Artikel 51. Intrekking Wet bescherming persoonsgegevens	394
Artikel 52. Citeertitel verordening	394
Artikel 53. Inwerkingtreding	394
Artikel 54. Citeertitel wet	394
 Index	 395
 Bijlage 1: Referentietabel artikelen AVG	 401
 Bijlage 2: Omnummeringstabel Richtlijn → AVG	 407
 Bijlage 3: Lijst van afkortingen	 413

ALGEMENE VERORDENING GEGEVENSBE SCHERMING

Hoofdstuk I

Algemene bepalingen

Het recht op bescherming van persoonsgegevens is een grondrecht, vastgelegd in artikel 8 lid 1 van het Handvest van de grondrechten van de Europese Unie (Handvest grondrechten EU). Dit grondrecht geldt zowel in horizontale als in verticale verhoudingen. De Algemene verordening gegevensbescherming (AVG) is als verordening opgesteld om een coherent kader voor gegevensbescherming in de Europese Unie (EU) te verzorgen, zodat een eenvormige bescherming van persoonsgegevens wordt geboden. De uitdrukkelijke wens daarbij was dit kader te voorzien van strenge handhaving (overweging 7), om zo “de digitale economie voldoende vertrouwen en rechtszekerheid te geven zich in de hele interne markt te laten ontwikkelen”.

Deze bescherming was voorheen uitgewerkt in Richtlijn 95/46/EG, waar de Nederlandse Wet bescherming persoonsgegevens (Wbp) op gebaseerd was. Daarnaast kende Richtlijn 95/46/EG een zelfstandige implementatie in de Wet basisregistratie personen (Wet BRP) en de Kieswet. Technologische ontwikkelingen en bijbehorende “nieuwe uitdagingen voor de bescherming van persoonsgegevens” sinds 1995, hebben geleid tot een verordening, een eenvormige wet die in de gehele EU van kracht is, en die (in samenspraak met de Uitvoeringswet Algemene verordening gegevensbescherming, hierna de Uitvoeringswet) de Wet bescherming persoonsgegevens vervangt.

De AVG is opgezet als 11 hoofdstukken. Hoofdstuk 1 van de AVG bepaalt het onderwerp en de doelstellingen van de AVG (art. 1), wanneer zij toepasselijk is (art. 2 en 3) en definieert de in de AVG gebruikte terminologie (art. 4).

Artikel 1. Onderwerp en doel van de AVG

I.1	Bij deze verordening worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens.
-----	---

De AVG heeft als doel het reguleren van de omgang met persoonsgegevens, oftewel de verwerking van persoonsgegevens. Door deze regulering ontstaat een markt voor diensten die gebruik maken van of afgestemd zijn op persoonsgegevens. Hiermee realiseert de EU het vrij verkeer van persoonsgegevens, analoog aan het vrij verkeer van goederen en diensten in de EU.

- 1.2 Deze verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens.

De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht (art. 8 lid 1 Handvest grondrechten EU, art. 16 lid 1 Verdrag Werking EU). Ook kan het worden gezien als een invulling van het grondrecht op bescherming van het privéleven (art. 8 Europees Verdrag voor de Rechten van de Mens (EVRM)).

Territoriale scope. De AVG is van toepassing bij verwerking van persoonsgegevens van betrokkenen die zich in de Europese Economische Ruimte bevinden, ongeacht waar de verwerkingsverantwoordelijke of verwerker gevestigd is (artikel 3). De bescherming uit de AVG geldt ongeacht nationaliteit of verblijfplaats van de betrokkene, zolang deze binnen de Europese Economische Ruimte (de EU plus Liechtenstein, Noorwegen en IJsland) verblijven.

Gegevens over ondernemingen. De AVG heeft geen betrekking op de verwerking van gegevens over rechtspersonen en met name als rechtspersonen gevestigde ondernemingen, zoals de naam en de rechtsvorm van de rechtspersoon en de contactgegevens van de rechtspersoon (overweging 14). Gegevens over zakelijk handelende natuurlijke personen, zoals zelfstandig ondernemers en eenmanszaken, zijn wél persoonsgegevens (Rb. Amsterdam 12 september 2014, ECLI:NL:RBAMS:2014:5938).

- 1.3 Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.

De interne markt voor met name online dienstverlening leunt steeds meer op het gebruik van persoonsgegevens. Voor de goede werking van de interne markt is het nodig dat het vrije verkeer van persoonsgegevens in de Unie niet nodeloos wordt beperkt of verboden door al te strenge regels omtrent persoonsgegevens. Technologie heeft zowel de economie als het maatschappelijk leven ingrijpend veranderd en moet het vrije verkeer van persoonsgegevens binnen de Unie en de doorgifte aan derde landen en internationale organisaties verder vergemakkelijken en daarbij een hoge mate van bescherming van persoonsgegevens garanderen.

Artikel 2. Materiële toepasselijkheid van de AVG

2.1 Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

De bescherming van persoonsgegevens wordt technologie-neutraal geformuleerd in de AVG om niet afhankelijk te zijn van de gebruikte technologieën van vandaag. Het criterium is hetzelfde als onder de Wbp: iedere geautomatiseerde verwerking valt onder de werkingssfeer, en de niet-geautomatiseerde verwerking alleen wanneer sprake is van een bestand. Verwerking is iedere handeling met betrekking tot persoonsgegevens (zie artikel 4 definitie 2).

Geautomatiseerde verwerking. Zodra de verwerking van persoonsgegevens op enigerlei wijze een computer of dergelijk middel vereist, is sprake van een geheel of gedeeltelijk geautomatiseerde verwerking. Slechts wanneer alle stappen binnen een verwerking handmatig gebeuren, zal geen sprake zijn van een zelfs maar gedeeltelijk geautomatiseerde verwerking. Anno 2023 is dit nog maar moeilijk voor te stellen, afgezien wellicht van een enkele kapper die alle afspraken met pen noteert. Iedere handeling via ICT-middelen of internet is al te zien als een geheel of gedeeltelijk geautomatiseerde verwerking (zie ook HvJ EU 6 november 2003, ECLI:EU:C:2002:513 (Linqvist)).

Verwerking in bestand. Een in het geheel niet geautomatiseerde verwerking valt slechts onder de AVG wanneer sprake is van een bestand met persoonsgegevens (artikel 4, definitie 6). Het spreekwoordelijke gele briefje met “Peter terugbellen 06-12345678” valt dus buiten de AVG, maar de Rolodex (wie kent deze nog?) is wel degelijk onderworpen aan de verordening.

Papieren kopie. Een papieren kopie van een geautomatiseerde verwerking valt onder het regime van die geautomatiseerde verwerking.

2.2 Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

2.2(a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;

Omdat de AVG gebaseerd is op Unierecht, kan zij alleen van toepassing zijn op activiteiten die binnen het Unierecht vallen. Met name uitgesloten zijn activiteiten betreffende de nationale veiligheid van lidstaten.

Unierecht. De term Unierecht moet extensief worden uitgelegd. Alle maatregelen die op een of andere manier verband houden met het EU-recht vallen hieronder (HvJ EU 26 februari 2013, ECLI:EU:C:2013:105 (Akerberg Fransson)). In

de praktijk betreft deze uitzondering dan ook eigenlijk alleen verwerkingen in het kader van de nationale veiligheid.

Wet basisregistratie personen. De Uitvoeringswet (artikel 2) is niet van toepassing op gegevensverwerkingen in het kader van de Wet BRP. De AVG is niet direct van toepassing op verwerkingen onder de Wet BRP, maar de Wet BRP verwijst op diverse plaatsen (bijvoorbeeld hoe het inzagerecht werkt op iemands registratie) expliciet naar regelingen uit de AVG. Hetzelfde geldt voor de Kieswet.

Inachtneming behoeften kleine, middelgrote en micro-ondernemingen. In overweging 13 van de AVG beveelt de Europese Unie uitdrukkelijk om bij toepassing van de verordening rekening te houden met de omvang van bedrijven en organisaties. In de Uitvoeringswet (artikel 2a) wordt hierbij aangesloten, zodat de behoeften van bedrijven en organisaties die minder dan 250 werknemers bevatten, een jaaromzet van minder dan 50 miljoen euro draaien of onder een balanstotaal van 43 miljoen euro zitten door de Autoriteit Persoonsgegevens (AP) nadrukkelijk in aanmerking dienen te worden genomen bij toepassing van de AVG.

Krijgsmacht. De AVG is van toepassing op de verwerking van persoonsgegevens door de Nederlandse krijgsmacht (artikel 3 Uitvoeringswet), tenzij deze handelt ter verdediging en bescherming van de belangen van het Koninkrijk (artikel 97 Grondwet).

2.2(b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;

Titel V, hoofdstuk 2 van het Verdrag betreffende de Europese Unie (VEU) bevat specifieke bepalingen betreffende het gemeenschappelijk buitenlands en veiligheidsbeleid van de lidstaten. Artikel 39 VEU bepaalt dat de Raad van Ministers (en dus niet het Europees Parlement) besluiten neemt over de voorschriften betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van dit hoofdstuk vallen. Toezicht gebeurt door nationale toezichthouders (zie artikel 57).

2.2(c) door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;

De AVG kent een ondergrens bij louter persoonlijke of huishoudelijke activiteiten die als zodanig geen enkel verband houden met een beroeps- of handelsactiviteit, kort gezegd het verwerken van persoonsgegevens door consumenten. Voorbeelden hiervan zijn de privéadresboeken van particulieren, het voeren van correspondentie, maar ook het sociaal netwerken en andere online-activiteiten door particulieren (overweging 18).

Persoonlijk gebruik. Ook wanneer een persoon zakelijk handelt, kan sprake zijn van persoonlijk gebruik in de zin van deze uitzondering. Het moet dan gaan om

een verwerking die uitsluitend voor die persoon zelf bedoeld is, zoals gespreks-aantekeningen of een eigen adresboek. Wanneer echter zo'n verwerking meer dan incidenteel wordt gedeeld met anderen (al is het maar de zakenpartner of secretaresse) dan is geen sprake meer van persoonlijk gebruik.

Cameratoezicht. Ook cameratoezicht door particulieren valt in principe onder een zuiver huishoudelijke activiteit, zij het dat de grens dan ligt bij de openbare ruimte (HvJ EU 11 december 2014, ECLI:EU:C:2014:2428 (Rynes)).

Online publicaties. De AVG lijkt bij online-activiteiten een lichte verruiming te kiezen: onder de Richtlijn viel het op internet publiceren van persoonsgegevens niet onder deze uitzondering (HvJ EU 6 november 2003, ECLI:EU:C:2002:513 (Linqvist)). Zie in dit verband ook artikel 85 over de balans met de informatievrijheid. Dat heeft te maken met dat zo aan het publiek beschikbaar stellen van informatie, niet gezien kan worden als het delen van informatie met een beperkte kring. Zo zien we ook dat in zaken waarbij op een openbaar profiel op Facebook (een foto) wordt gepost, de huishoudelijke exceptie niet opgaat (Rb. Gelderland 13 mei 2020, ECLI:NL:RBGEL:2020:2521). Dit kan weer anders zijn als de kring van ontvangers (dus als het niet gaat om een openbaar profiel) kleiner is en wel kwalificeert als een kleine beperkte kring mensen.

Middelen voor huishoudelijke activiteiten. Lid 2 punt c geldt niet voor verwerkingsverantwoordelijken of verwerkers die slechts middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten. Denk bijvoorbeeld aan een internetdienst waarbij men als particulier een online adresboek kan bijhouden. Deze dienstverlener zal als verwerker van de particulier aan de AVG moeten conformeren.

2.2(d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

De verwerking van persoonsgegevens in verband met straf(proces-)recht wordt in andere Europese wetgeving geregeld, met name in de simultaan aangenomen Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad. Wanneer bevoegde autoriteiten in de lidstaten andere taken verrichten (met name het bewaken van de openbare orde), vallen deze wél onder de AVG. Lidstaten mogen bij wet nadere regels stellen over dit onderwerp (artikel 23 lid 1 punt d). Zie nader artikel 10 over strafrechtelijke persoonsgegevens in het algemeen.

Gerechten. Verwerkingen door gerechtelijke instanties en bestuursrechtelijke toezichthouders vallen wel onder de AVG, zij het met enige beperkingen. Zo zijn de toezichthouders (vanwege de onafhankelijkheid van de rechterlijke macht) niet bevoegd om tegen hen op te treden (artikel 55 lid 3). Deze organisaties moeten zelf naleving en toezicht regelen.

- 2.3 Op de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie is Verordening (EG) nr. 45/2001 van toepassing. Verordening (EG) nr. 45/2001 en andere rechtshandelingen van de EU die van toepassing zijn op een dergelijke verwerking van persoonsgegevens worden overeenkomstig artikel 98 aan de beginselen en regels van de onderhavige verordening aangepast.

De AVG is niet van toepassing op verwerkingen door instanties van de Europese Unie. Deze verwerkingen zijn apart geregeld in Verordening (EG) nr. 2018/1725 van het Europees Parlement en de Raad. Deze verving in november 2018 de oude Verordening 45/2001 over hetzelfde onderwerp.

- 2.4 Deze verordening laat de toepassing van Richtlijn 2000/31/EG (e-commerce-richtlijn), en met name van de regels in de artikelen 12 tot en met 15 van die richtlijn betreffende de aansprakelijkheid van als tussenpersoon optredende dienstverleners onverlet.

De e-commercerichtlijn bepaalt onder meer dat dienstverleners zoals internet-toegangsproviders, hosting providers en online platforms (bijvoorbeeld Marktplaats of Twitter) beperkt aansprakelijk zijn voor informatie die hun klanten opslaan of verspreiden via hun dienst (art. 6:196c Burgerlijk Wetboek (BW)). Artikel 2 lid 4 verduidelijkt dat dit ook geldt wanneer de informatie persoonsgegevens betreft. Daarmee kan de beperkte aansprakelijkheid van een tussenpersoon dus niet opengebroken worden enkel omdat het hier persoonsgegevens betreft.

Een tussenpersoon kan in diverse gevallen als verwerker (zie artikel 4 definitie 8) optreden wanneer hij bewust voor de klant persoonsgegevens opslaat of anderszins verwerkt. Een beroep op de e-commercerichtlijn om verantwoordelijkheid uit de weg te gaan omdat het een tussenpersoon is, gaat hier dus niet op.

De Verordening betreffende een eengemaakte markt voor digitale diensten vervangt de e-commercerichtlijn. Deze Verordening is bekend als de “Digital Services Act” en is vanaf 17 februari 2024 van toepassing.

Artikel 3. Territoriale toepasselijkheid

- 3.1 Deze verordening is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie plaatsvindt.

Een belangrijk punt van discussie bij de totstandkoming van de AVG was op welke entiteiten wereldwijd deze van toepassing verklaard kon worden. Veel

verwerkingen worden door Amerikaanse bedrijven verricht, denk aan Twitter of Google. Sommige van deze bedrijven hebben daarbij een Europese dochteronderneming opgezet, zoals Facebook of Microsoft, maar lang niet altijd. De AVG is van toepassing als men een vestiging in de EU heeft, ongeacht of deze dan ook verwerkingen uitvoert.

Vestiging. Een vestiging is iedere duurzame, reële en daadwerkelijke activiteit in een lidstaat, zelfs indien deze activiteit slechts gering is (HvJ EU 1 oktober 2015, ECLI:EU:C:2015:639 (Weltimmo)). Een “vestiging” veronderstelt het effectief en daadwerkelijk uitoefenen van activiteiten via bestendige verhoudingen. De rechtsvorm van dergelijke verhoudingen, of het nu gaat om een handelsagent, een bijkantoor of een dochteronderneming met rechtspersoonlijkheid, is daarbij niet doorslaggevend. Zelfs alleen een werknemer, kan een vestiging zijn. De lat om te kwalificeren als vestiging kan bij online dienstverlening best laag liggen. De verwerkingen moeten wel in het kader van de activiteiten van die vestiging worden uitgevoerd, dan is de AVG van toepassing (Europees Comité voor gegevensbescherming (het Comité), Richtsnoeren 3/2018 inzake het territoriale toepassingsgebied van de AVG (artikel 3), 12 november 2019). De AVG zal van kracht zijn bij het hebben van een werknemer.

Gevestigd in EU. Wie in de EU een vestiging heeft en verwerkingsverantwoordelijke of verwerker is, valt onder de werkingssfeer van de AVG. Dit geldt, zoals altijd wanneer er in de AVG gerefereerd wordt aan de EU, ook voor de Europese Economische Ruimte (EU met Noorwegen, IJsland en Liechtenstein).

Verwerking buiten de EU. Uit artikel 3 lid 1 volgt dat de plaats van de verwerking irrelevant is. Ook al vindt de verwerking zelf niet in de EU plaats, kan de AVG alsnog van toepassing zijn. Dat is het geval als persoonsgegevens verwerkt worden in het kader van een vestiging in de EU. Denk bijvoorbeeld aan een Human Resources bedrijf gevestigd in Zweden, dat alle gegevensverwerkingen in India laat uitvoeren. De AVG is hierop van toepassing omdat in India een gegevensverwerking plaatsvindt in het kader van het bedrijf in Zweden.

In het kader van de activiteiten van een vestiging. Het is niet noodzakelijk dat de verwerking wordt uitgevoerd door de vestiging, maar het moet “in het kader van de activiteiten van de vestiging” gebeuren. Er is geen zwart-wit invulling voor dit vereiste. Dit moet gelezen worden in het licht van relevante jurisprudentie. De Europese toezichthouder adviseert te kijken welke persoonsgegevens er worden verwerkt, welke link er is tussen de activiteit waarvoor de persoonsgegevens worden verwerkt, en de activiteiten van de vestiging in de EU. Hierbij is de relatie tussen de partij buiten de EU en de vestiging in de EU relevant om de afweging te maken Richtsnoeren 3/2018 inzake het territoriale toepassingsgebied van de AVG (artikel 3) van het Comité, 12 november 2019).

Zie nader de Richtsnoeren 3/2018 over het territoriale toepassingsgebied van de AVG (artikel 3) van het Comité en de *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain (WP179 update)* van de Artikel 29-Werkgroep.

- 3.2 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 verband houdt met:

Gevestigd buiten EU. Wanneer de hoofdvestiging van een verwerkingsverantwoordelijke buiten de EU gevestigd is, was onder de Richtlijn een Europees bureau dat reclame-inkomsten incasseert (maar geen persoonsgegevens verwerkt) soms aan te spreken op handelen van het hoofdkantoor (HvJ EU 13 mei 2014, ECLI:EU:C:2014:317 (Costéja)). Onder de AVG werpt lid 2 van artikel 3 een veel breder net uit: het bedrijf valt gewoon onder de AVG. Het blijft wel mogelijk om een Europees bureau aan te spreken, wat in verband met executiemogelijkheden voordelig kan zijn. Zie ook artikel 27 over de verplichting aan te stellen vertegenwoordiger.

Wanneer de verwerkingsverantwoordelijke of verwerker niet in de EU gevestigd is, verklaart de AVG zichzelf toch van toepassing als het gaat om persoonsgegevens van personen die zich in Europa bevinden wanneer aan één van twee eisen is voldaan. De betreffende verwerkingsverantwoordelijke of verwerker moet dan een vertegenwoordiger in de EU aanstellen (artikel 27).

- 3.2(a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of

Het eerste criterium voor niet een in de EU gevestigde verwerkingsverantwoordelijke of verwerker is of hij goederen of diensten aanbiedt in de EU. Hierbij geldt een open norm. Algemene zaken zoals de toegankelijkheid in de EU van de website van het bedrijf, het aanbieden van contactgegevens met internationale kengetallen en dergelijke of het hanteren van een algemeen gebruikte taal (zoals Engels), zijn op zich ontoereikend om tot deze conclusie te komen. Een optelsom van factoren zoals taal, Europese munteenheid of referenties van andere personen die zich in de EU bevinden kan wel tot deze conclusie leiden.

De AVG sluit hiermee aan bij jurisprudentie over gerechtelijke bevoegdheid voor door consumenten gesloten overeenkomsten (HvJ EU 7 december 2010, gevoegde zaken C-585/08 en C-144/09) dat een vergelijkbare lijst factoren formuleerde (zoals taal of munteenheid uit het land van de consument of een land-specifieke domeinnaam) die gezamenlijk bijdragen aan de bepaling op welk land een ondernemer zich richt.

De vraag rijst of dit vereiste ook geldt bij het verwerken van gegevens in het geval van B2B marketing of sales, of in het verlengde daarvan het benaderen of actief richten van marketing op bedrijven in de EU. Op dit moment is de interpretatie geschreven door de toezichthouder beperkt tot B2C activiteiten. In de praktijk zien we dat veel organisaties de AVG van toepassing achten bij B2B contact, doordat er contact wordt gelegd met een individu. De vraag blijft of dit wenselijk en realistisch is in elke situatie, en nog wel in lijn is met de doelstelling van de AVG om vrij verkeer van persoonsgegevens te faciliteren.

3.2(b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.

Het monitoren van gedrag is dermate populair en invasief dat deze handeling, ongeacht vestigingsplaats of gerichtheid op de EU, maakt dat men als organisatie onder de AVG valt. Vaak zal het gaan om monitoring via internet, telefoon of apps, maar naar de letter vallen ook andere vormen van monitoring er onder, hoewel het moeilijk is daar een concreet voorbeeld van te verzinnen.

Het criterium is of natuurlijke personen worden gevolgd, en onder meer of in dat verband eventueel technieken worden gebruikt waarbij een profiel wordt opgesteld van een natuurlijke persoon, in het bijzonder om besluiten ten aanzien van hem te nemen of om zijn persoonlijke voorkeuren, gedragingen en attitudes te analyseren of te voorspellen.

Het gaat hier waarschijnlijk wel om meer dan enkel het analyseren van het gebruik van de eigen website (zoals met Google Analytics). Zogeheten cross-site targeting, waarbij personen over meerdere websites of diensten worden gevolgd, voldoet aan deze omschrijving. Er zijn geen uitspraken over de toepasselijkheid van dit artikel specifiek bij de dienst Google Analytics. Weliswaar hebben drie toezichthouders (Frankrijk, Oostenrijk en Italië) bepaald dat Google Analytics niet toegestaan is te gebruiken onder de AVG, maar de motivatie is geschoeid op het niet legaal kunnen overbrengen van persoonsgegevens naar Google in de VS (zie hoofdstuk V).

3.3 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 het lidstatelijke recht van toepassing is.

In enkele bijzondere gevallen, zoals bij een diplomatieke vertegenwoordiging of een consulaire post van een EU-lidstaat, is uit hoofde van het internationale publiekrecht het lidstatelijke recht van toepassing. De AVG is ook dan van toepassing.

Artikel 4. Definities

Voor de toepassing van deze verordening wordt verstaan onder:

Gezien de omvang van de AVG is het cruciaal de terminologie correct te hebben. Artikel 4 definieert 26 termen die algemeen gebruikt worden in de AVG. Ten opzichte van de Richtlijn is een fors aantal veranderingen doorgevoerd, zoals bij persoonsgegevens (definitie 1), verwerkingsverantwoordelijke (definitie 7, voorheen de verantwoordelijke) en verwerker (definitie 8, voorheen de bewerker) en zijn er veel definities toegevoegd.

4.1 “persoonsgegevens”: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

De essentieelste definitie in de AVG is die van ‘persoonsgegevens’. Dit betreft net als in de Richtlijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (en dus niet een overledene of een rechtspersoon), maar de reikwijdte van ‘identificeerbaar’ is behoorlijk vergroot.

Identificeerbaar. 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. Ook wanneer identificatie de hulp van een derde vereist, kunnen gegevens nog persoonsgegevens zijn (HvJ EU 26 april 2023, ECLI:EU:T:2023:219).

Herleidbaarheid. Een betrokkene is geïdentificeerd als hij of zij kan worden herleid oftewel geïndividualiseerd binnen een groep, onderscheiden van de rest. Een naam of paspoortnummer is hiervoor niet vereist: “die lange meneer achterin” of “bezoeker met cookie THX1138” zijn ook identificaties. Het is daarbij niet vereist dat alle informatie waarmee de betrokkene kan worden geïdentificeerd, bij een en dezelfde persoon berust (HvJ EU 19 oktober 2016, C-582/14, Breyer). De vraag is of de verwerkingsverantwoordelijke redelijke en legale middelen tot zijn beschikking heeft om bijvoorbeeld pseudonimisering ongedaan te maken (HvJ EU 26 april 2023, ECLI:EU:T:2023:219).

Redelijke middelen. Identificeerbaarheid hangt af van de vraag of de verwerkingsverantwoordelijke of een ander redelijkerwijs in staat is de betrokkene

te identificeren. Daarbij 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 (overweging 26).

Anonieme gegevens. De AVG is niet van toepassing op anonieme gegevens. Hiervan is sprake in twee situaties: 1) de gegevens hebben überhaupt geen betrekking op identificeerbare natuurlijke personen, zoals bedrijfsgegevens of gegevens van overledenen, en 2) de gegevens zijn zodanig anoniem gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Anonimiseren vereist meer dan enkel namen en contactgegevens weglaten, de gegevens van klant 481 of student s383104 zijn nog steeds persoonsgegevens. Middels aggregatie (het samenvoegen van gegevens tot informatie als “de gemiddelde bezoeker is tussen de 40 en 55”) of het randomiseren van gegevens (bijvoorbeeld geboortedata en woonplaatsen willekeurig wisselen in een grote lijst) kan men tot anonieme gegevens komen. Meestal zal men dus niet anonimiseren maar slechts *pseudonimiseren* (definitie 5). De AVG blijft dan van toepassing, maar het is makkelijker om met pseudonieme gegevens aan de eisen te voldoen.. Meer algemeen over anonimiseren is *Advies 5/2014 inzake anonimiseringstechnieken* (WP 216, 10 april 2014) van de Artikel 29-Werkgroep.

Genetisch, biometrisch en gezondheid. Voor genetische-, biometrische- en gezondheidsgegevens zie nadere definities 13, 14 en 15.

Online identifier. Een identifier is een element waarmee een persoon kan worden geïdentificeerd. Op internet wordt daarbij vaak gewerkt met unieke nummers zoals een IP-adres (vergelijk HvJ EU zaaknr. C-582/14, Breyer), cookie, RFID-tag of MAC-adres dan wel IMEI-nummer van een smartphone. Deze nummers dienen om diverse bezoeken te kunnen koppelen, met name om daarmee interesseprofielen op te stellen van natuurlijke personen voor reclame. Gebruik van dergelijke identificatoren telt dus als een verwerking van persoonsgegevens, ook als men niet in staat is om een naam te koppelen aan de identifier. De identifier is in feite al de benaming van de betrokkene.

- 4.2 “verwerking”: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

Het tweede kernbegrip (na persoonsgegeven) is dat van ‘verwerking’. Een verwerking is iedere handeling met persoonsgegevens. De definitie noemt een

waslijst aan voorbeelden, welke niet limitatief moet worden opgevat. Merk op dat ook het wissen en vernietigen van persoonsgegevens als verwerking worden gezien.

Geautomatiseerd. Het is niet relevant of de handeling geautomatiseerd of handmatig wordt verricht. In beide gevallen is sprake van een verwerking. Dit aspect is wel van belang bij de vraag of de verwerking onder de AVG valt: bij een geautomatiseerde verwerking is dit altijd het geval (behalve bij de uitzonderingen van artikel 2 lid 2), maar bij een niet-geautomatiseerde verwerking is daarvan alleen sprake als de persoonsgegevens in een bestand (zie definitie 6) zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (artikel 2 lid 1).

Internet. Plaatsen en gebruiken van informatie op internet is een geautomatiseerde handeling en valt dus onder het begrip ‘verwerking’. In het Costéja-arrest (HvJ EU 13 mei 2014, zaaknr. C-131/12) werden indexatie en beschikbaarstelling van informatie door zoekmachines al als ‘verwerking’ aangemerkt onder de Richtlijn. Eerder bepaalde het Lindqvist-arrest (HvJ EU 6 november 2003, zaaknr. C-101/01) dat het publiceren van informatie op internet al als verwerking te zien is, ook indien dat in ongestructureerde vorm gebeurde (zoals door op een webpagina te schrijven dat een collega haar voet had bezeerd).

-
- 4.3 “beperken van de verwerking”: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;
-

Een nieuw recht in de AVG is het kunnen laten beperken van de verwerking. Dit houdt in dat persoonsgegevens tijdelijk als het ware worden bevroren, bijvoorbeeld omdat een bezwaar tegen de verwerking moet worden uitgezocht. Zie over het begrip ‘beperking’ nader artikel 18.

-
- 4.4 “profilering”: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;
-

Een steeds belangrijker techniek bij veel bedrijven, maar ook bij overheden, is profileren. Dit is kort gezegd het geautomatiseerd opbouwen van een beeld over de persoonlijke aspecten van een individu. Profileren wordt gebruikt om voorspellingen te doen over mensen. Het woord “geëvalueerd” impliceert dat profileren een soort assessment of besluit over iemand inhoudt. Profielen kunnen bijvoorbeeld worden opgebouwd door van een websitebezoeker bij te houden welke pagina’s hij of zij lange tijd bekijkt; de onderwerpen daarvan zullen dan wel relevant zijn voor deze bezoeker. Profielen kunnen ook zijn gebaseerd op algemenere gegevens, zoals koop- of betaalgedrag in een postcodegebied.

Vergelijk Artikel 29-Werkgroep, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, 6 februari 2018 en Artikel 29-Werkgroep, *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation*, 13 mei 2013.

Informeren over profilering. Wordt gewerkt met profilering in combinatie met geautomatiseerde besluitvorming, dan moet de betrokkene actief daarover worden geïnformeerd (artikel 13 lid 2 punt f en artikel 14 lid 2 punt g), met in ieder geval nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene. Deze informatie moet ook worden verstrekt op verzoek (artikel 15 lid 1 punt h). Uitleg over de onderliggende logica kan raken aan handelsgeheimen (of auteursrechten) van de verwerkingsverantwoordelijke of de verwerker. In die situaties moet een balans worden gevonden in welke informatie wordt verstrekt; geheel weigeren iets te onthullen met een beroep op deze gronden is niet toegestaan (overweging 63).

Bezwaar tegen profilering. De betrokkene kan bezwaar maken (artikel 21 lid 1) tegen profilering in het kader van een overheidstaak (artikel 6 lid 1 punt e) of profilering op grond van een gerechtvaardigd belang (artikel 6 lid 1 punt f). Dient het profileren het doel van direct marketing, dan dient dit te allen tijde te worden gestaakt bij bezwaar (artikel 21 lid 2). Als het profileren gebaseerd is op de grondslag toestemming, dan is bezwaar niet mogelijk. Wel kan de betrokkene de toestemming dan te allen tijde intrekken (artikel 7 lid 3).

Besluitvorming door profilering. Een besluit mag niet uitsluitend zijn gebaseerd op informatie verkregen uit profilering (artikel 22). Een klant mag dus bijvoorbeeld niet achterafbetaling worden geweigerd omdat in zijn postcodegebied veel wanbetalers wonen, en een sollicitant mag niet worden afgewezen enkel op basis van een automatische analyse van zijn online activiteiten.

- 4.5 “pseudonimisering”: 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;

Van pseudonimisering is sprake wanneer direct identificeerbare gegevens, zoals naam, telefoonnummer of huisadres worden losgekoppeld van overige gegevens en vervangen door een aanvullend gegeven zoals een klantnummer of een code. De gegevens blijven dan persoonsgegevens, maar identificatie is lastiger tenzij men de lijst heeft die de aanvullende gegevens koppelt aan de directe gegevens.

Gevolgen van pseudonimisering. Het toepassen van pseudonimisering maakt het gemakkelijker aan een aantal eisen uit de AVG te voldoen. Zo levert pseudonimisering een mogelijke passende waarborg op (artikel 6 lid 4) bij verwerkingen op andere gronden dan toestemming, en is het een mogelijkheid om aan de vereisten van privacy by design (artikel 25 lid 1) en beveiliging (artikel 32) te voldoen. Ook bij wetenschappelijk onderzoek geldt pseudonimisering als een mogelijke waarborg (artikel 89 lid 1). Gedragscodes kunnen vermelden hoe pseudonimisering kan worden toegepast (artikel 40 lid 2 punt d). De onbevoegde ongedaanmaking van pseudonimisering is een datalek dat meldingsplichting is (artikel 33 en 34).

Wijze van pseudonimisering. De AVG schrijft niet voor hoe pseudonimisering moet worden uitgevoerd. In het algemeen komt het erop neer dat een bestand met persoonsgegevens in tweeën wordt geknipt, met als koppeling tussen die twee een nummer of andere code, zoals een klantnummer of willekeurig gekozen letter- of cijfercode. Het eerste deel bevat dan de direct identificerende gegevens, met name de naam en contactgegevens van de betrokkenen. Het tweede deel bevat de indirect identificerende gegevens, bijvoorbeeld aankoopgedrag, voorkeuren of antwoorden op een enquête. Werken met dit tweede deel levert dan minder risico's op voor wie niet ook beschikt over het eerste deel omdat het klantnummer minder onthult dan de direct identificerende gegevens. Het is daarbij toegestaan dat dezelfde organisatie het eerste en het tweede deel beheert, zolang zij dit maar apart bewaart (overweging 29). Tevens moeten passende technische en organisatorische maatregelen worden genomen (artikel 24) om te zorgen dat de pseudonimisering intact blijft.

Verschil met anonimisering. Het pseudonimiseren van persoonsgegevens ontdoet deze niet van hun status als persoonsgegevens. Pas wanneer gegevens zodanig anoniem zijn gemaakt dat de betrokkene in het geheel niet of niet meer identificeerbaar is, vallen ze buiten het regime van de AVG. Het omkeerbaar wissen van de koppeling (bijvoorbeeld het verwijderen van klantnummers) zou een manier zijn om van pseudonieme naar anonieme gegevens te gaan.

4.6 “bestand”: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

Bij de volledig handmatige verwerking van persoonsgegevens is het van belang of sprake is van een bestand, aangezien alleen dan de AVG van toepassing is (artikel 2 lid 1).

Gestructureerd geheel. De persoonsgegevens moeten allereerst gestructureerd zijn. Dit houdt in dat het geheel op grond van meer dan één kenmerk een onderlinge samenhang moet vertonen (zie nader ECLI:NL:HR:2005:AT1093 overweging 3.4.2). Enkel brieven op bijvoorbeeld chronologische volgorde bewaren

is dus niet genoeg. Een verzameling hangmappen die per cliënt stukken op chronologische volgorde bevat voldoet wel aan dit criterium. De samenhang kan worden gevonden in een structuur in het dossier, maar ook in een raadpleegmethode om in ongestructureerde documenten te zoeken (denk aan aangebrachte labeltjes). Back-ups en kopieën (schaduwdoSSIers) worden gerekend onder het ‘geheel’ en zijn dus geen apart bestand.

Bepaalde criteria. De persoonsgegevens moeten via zekere criteria, zoals namen of andere kenmerken van personen, te vinden of selecteren zijn. Dossiers of een verzameling dossiers en de omslagen ervan, die niet volgens specifieke criteria zijn gestructureerd, vallen niet onder het toepassingsgebied van de AVG.

Verspreid. Vandaag de dag is het staande praktijk een bestand of databank niet op één locatie op te slaan. De definitie verduidelijkt dat ook dan sprake kan zijn van een ‘bestand’.

4.7 “verwerkingsverantwoordelijke”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

De verwerkingsverantwoordelijke is de entiteit die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze entiteit is dan ook verplicht de waarborgen te nemen die bij die verwerking nodig zijn (artikel 24). Een entiteit die een verwerking uitvoert binnen het doel en de middelen gesteld door een verwerkingsverantwoordelijke heet een verwerker (zie definitie 8 en nader artikel 28). Onduidelijk is de situatie waarin de ene partij het doel bepaalt en de andere partij de middelen. Waarschijnlijk moet de balans dan doorslaan naar de partij die het doel bepaalt, gezien dit uiteindelijk de meest fundamentele keuze is. De partij die dan ‘slechts’ de middelen vaststelt, is dan de verwerker.

Doel. Het voornaamste criterium is het doel of de doelen van een verwerking. Het doel is het sine qua non van verwerking, zonder doel is een verwerking haast niet denkbaar. De doelen moeten welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn (artikel 6 lid 1 punt b, het beginsel van doelbinding). Alleen bij wetenschappelijk onderzoek binnen ethische kaders kan soms worden volstaan met een generiek doel (overweging 33, zie nader artikel 89).

Middelen. De middelen zijn alle gereedschappen en andere middelen waarmee een verwerking wordt uitgevoerd. Dit kan uiteenlopen van een softwarepakket tot de stickers waarmee papieren in een dossier visueel gecategoriseerd worden.

Verwerkingsverantwoordelijke buiten EU. Indien de verwerkingsverantwoordelijke buiten de EU gevestigd is, moet deze - als artikel 3 lid 2 AVG van toepassing is - in beginsel altijd een vertegenwoordiger aanstellen die in de EU is gevestigd (zie definitie 17 en nader artikel 27).

Meerdere verwerkingsverantwoordelijken. Het is mogelijk dat meerdere partijen samenwerken in de uitvoering van een verwerking. Afhankelijk van wie van hen dan het doel en de middelen bepaalt, is dan sprake van een verwerkersrelatie of van gezamenlijke verwerkingsverantwoordelijken. Hierover nader artikel 26.

Aanwijzing als verwerkingsverantwoordelijke. Als een verwerking wettelijk wordt geregeld, is het toegestaan dat de betreffende regeling vermeldt wie daarbij als verwerkingsverantwoordelijke wordt aangemerkt. Deze aanwijzing gaat dan boven de hoofdregel uit deze definitie. Een voorbeeld is artikel 3 lid 2 Handelsregisterwet 2007, dat de Kamer van Koophandel aanwijst als verwerkingsverantwoordelijke voor de wettelijke taak van beheer van het handelsregister.

4.8 “verwerker”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

De verwerker is een entiteit die een verwerking uitvoert binnen het doel en de middelen gesteld door een verwerkingsverantwoordelijke (zie definitie 7). De verwerker heeft een uitvoerende taak en dus geen zeggenschap over de wijze van verwerken. Zijn taken en verplichtingen staan in artikel 28.

Doel en middelen. Het criterium of iemand verwerkingsverantwoordelijke dan wel verwerker is, is of deze zelfstandig het doel en de middelen vaststelt van de verwerking. De verwerkingsverantwoordelijke bepaalt het doel en de middelen. In de praktijk kiezen verwerkers vaak zelf de middelen waarmee zij werken, zoals de te gebruiken software of de wijze van archiveren van documenten. De verwerker kan in haar rol bepalen over niet wezenlijke middelen van de verwerking, die zien op de meer praktische uitvoering. Denk hierbij aan welke software gebruikt kan worden bij het outsourcen naar een derde partij van de betaling van salarissen. In twijfelgevallen geeft wie het doel bepaalt van de verwerking de doorslag. Een administratiekantoor met eigen softwaremiddelen is dus een verwerker. De klant bepaalt namelijk voor welk doel de administratie van die klant wordt verwerkt en door haar keuze voor dat administratiekantoor impliciet ook de middelen kiest. Zie nader de Richtsnoeren 07/2020 over de begrippen ‘verwerkingsverantwoordelijke’ en ‘verwerker’ in de AVG van het Comité, 7 juli 2021 en Artikel 29-Werkgroep, Advies 1/2010 over de begrippen ‘verantwoordelijke’ en ‘verwerker’ (WP 169), 16 februari 2010.

Afzonderlijke entiteit. Een verwerker moet een afzonderlijke (rechts)persoon zijn ten opzichte van de verwerkingsverantwoordelijke. Een werknemer of een uit-

zendkracht is dus geen verwerker, maar slechts een hulppersoon die onder gezag van de verantwoordelijke werkt (zie nader artikel 29). Een aparte bv binnen hetzelfde concern kan wél een verwerker zijn, denk aan de bekende constructie van het shared service center dat als aparte rechtspersoon facilitaire processen zoals HR of salarisadministratie uitvoert voor alle entiteiten in een concern.

Verwerker buiten EU. Indien de verwerker buiten de EU gevestigd is, en de AVG via artikel 3 lid 2 van toepassing is, moet deze in beginsel altijd een vertegenwoordiger aanstellen die in de EU is gevestigd (zie definitie 17 en nader artikel 27).

4.9 “ontvanger”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;

Een ontvanger is de partij aan wie gegevens worden verstrekt. Dit is dus breder dan alleen de verwerkingsverantwoordelijken of verwerkers met wie de partij werkt. Overheidsinstanties die ingevolge hun wettelijke verplichting persoonsgegevens worden medegedeeld, moeten niet gezien worden als ontvanger (overweging 31). Deze kwalificatie is relevant om controle op de verwerkte persoonsgegevens te houden. Bijvoorbeeld voor de informatieplicht aan betrokkenen, hierbij moeten onder meer de categorieën van ontvangers aan de betrokkene worden medegedeeld (artikel 12 en verder). Daarnaast moeten rectificaties op basis van het recht op rectificatie ook aan de ontvangers van de desbetreffende persoonsgegevens worden medegedeeld (artikel 19), en verwerkingsverantwoordelijken zijn ook verplicht de ontvangers op te nemen in het register van de verwerkingsactiviteiten (artikel 30).

Overheidsinstanties. Overheidsinstanties die op grond van een wettelijke verplichting persoonsgegevens vorderen, worden niet gezien als ontvangers indien de afgifte noodzakelijk is voor de uitvoering van een onderzoek van algemeen belang binnen een wettelijke regeling. Voorbeelden zijn belasting- of douaneautoriteiten, financiëleonderzoeksdiensten, onafhankelijke bestuurlijke autoriteiten of financiëlemarktautoriteiten die belast zijn met de regulering van en het toezicht op de effectenmarkten. Door overheidsinstanties ingediende verzoeken om verstrekking moeten in ieder geval schriftelijk, gemotiveerd en incidenteel zijn, en mogen geen volledig bestand betreffen of resulteren in het onderling combineren van bestanden. De verwerking van persoonsgegevens door bedoelde overheidsinstanties moet stroken met de voor de doeleinden van de verwerking toepasselijke gegevensbeschermingsregels.

4.IO “derde”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;

Een derde is iedere entiteit anders dan de betrokkene zelf, de verwerkingsverantwoordelijke, de verwerker(s) of de personen onder hun rechtstreeks gezag. Deze definitie speelt eigenlijk alleen een rol bij een verwerking krachtens gerechtvaardigd belang (artikel 6 lid 1 punt f); ook het belang van zo’n derde kan een grondslag bieden voor die verwerking.

Rechtstreeks gezag. Een persoon handelt onder rechtstreeks gezag als hij werknemer is of als inhuurkracht direct opereert binnen de verwerkingsverantwoordelijke of verwerker (zie artikel 29). Deze persoon is geen derde.

Derden binnen concern. Binnen een concernrelatie (definitie 19) gelden de moeder-, dochter- en zustermaatschappijen naar elkaar als derde in de zin van deze definitie.

4.II “toestemming” van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt;

Onder de grondslag toestemming is in beginsel elke verwerking te rechtvaardigen (behalve sommige verwerkingen van bijzondere en strafrechtelijke persoonsgegevens, zie artikelen 9 en 10). Toestemming moet vrij (vrijelijk, vrijwillig) worden gegeven, gericht zijn op een specifieke (categorie van) verwerking, op informatie berusten en ondubbelzinnig zijn. Dit vereist een duidelijke actieve handeling. Het kanaal doet er minder toe: een schriftelijke verklaring, maar ook elektronische communicatie of een mondelinge verklaring is adequaat. Zie meer algemeen de *Richtsnoeren over toestemming onder Verordening 2016/679* (WP 259) van de Artikel 29-Werkgroep, 28 november 2017 en *Advies 15/2011 over de definitie van het begrip ‘toestemming’* (WP 187) van de Artikel 29-Werkgroep, 13 juli 2011.

Vrijelijk. Toestemming moet vrij oftewel vrijwillig worden gegeven. Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen. Het bundelen van toestemmingsvragen voor verschillende verwerkingen (zodat men niet per verwerking ja en nee kan zeggen) maakt het antwoord in beginsel niet vrijwillig (overweging 43). Ook wanneer toestemming wordt geëist bij het verlenen van een dienst terwijl deze niet feitelijk noodzakelijk is, is er geen sprake van vrijwilligheid.

Specifiek. De toestemmingsvraag moet specifiek aangeven voor welke doel (of gelijke doeleinden) toestemming wordt gevraagd. “Ik wil een seintje krijgen als dit product weer op voorraad is” is bijvoorbeeld specifiek genoeg, maar “Ik geef toestemming voor de in de privacyverklaring genoemde verwerkingen” is dat niet. Bij meerdere doeleinden moet per doel apart toestemming worden gevraagd (overweging 32). Toestemmingsvragen kunnen niet in algemene voorwaarden of privacyverklaringen worden opgenomen (Rechtbank Rotterdam 24 september 2014, ECLI:NL:RBROT:2014:7808). Zie hierover nader artikel 7 lid 2.

Geïnformeerd. Toestemming kan pas worden gegeven als men in duidelijke en eenvoudige taal is geïnformeerd over het wat en hoe (zie nader artikel 7 lid 2). Hierbij mag niet worden volstaan met een verwijzing naar een privacyverklaring (artikelen 13 en 14). Wel volstaat een korte toelichting in combinatie met zo’n verwijzing.

Ondubbelzinnig. Een toestemmingsverklaring moet ondubbelzinnig zijn. Dit houdt in dat de handeling waarmee toestemming wordt gegeven, niet voor meerdere interpretaties vatbaar mag zijn. Een bestelknop in een webwinkel kan dus niet tevens worden gebruikt om toestemming mee te vragen, zoals met een tekst “Door uw bestelling te plaatsen, gaat u tevens akkoord met ontvangst van onze nieuwsbrief” onder die knop. Het is immers niet ondenkbaar dat mensen wel de prominent vormgegeven knop zien maar niet de tekst daaronder.

Elektronisch kanaal. Toestemming kan prima langs elektronische weg worden gegeven, zoals door een tekst per e-mail, het drukken op een knop of het veranderen van instellingen bij een internetdienst. Indien de betrokkene zijn toestemming moet geven na een verzoek via elektronische middelen, dient dat verzoek duidelijk en beknopt te zijn en niet onnodig storend voor het gebruik van de dienst in kwestie (overweging 32).

Stilzwijgen als toestemming. De toestemmingshandeling moet actief zijn. Uit stilzwijgen of het niet weghalen van voorafgeplaatste kruisjes of vinkjes mag geen toestemming worden afgeleid (HvJ EU 1 oktober 2019, ECLI:EU:C:2019:801 (Planet49 GmbH)). Ook uit stilzitten (bijvoorbeeld het niet verlaten van een ruimte nadat wordt aangekondigd dat er zal worden gefilmd door de lokale televisieomroep) mag geen toestemming worden geconcludeerd.

Toestemming bij bijzondere persoonsgegevens. Bij bijzondere persoonsgegevens geldt bij de grondslag toestemming (artikel 9 lid 1 punt a) tevens het vereiste van uitdrukkelijkheid. Dit impliceert vooral dat uit een handeling dan in beginsel geen toestemming kan worden afgeleid; er moet sprake zijn van een expliciete wilsuiting gericht op het geven van toestemming.

Toestemming bij kinderen. Bij het gebruik van diensten van de informatiemaatschappij door kinderen gelden er aanvullende eisen (artikel 8). De toestemming

is alleen geldig als het kind ten minste 16 jaar is, jonger dan 16 jaar is toestemming van de ouder nodig (hierover meer bij artikel 8).

Toestemming bij wetenschappelijk onderzoek. Bij onderzoek is het vaak vooraf niet mogelijk het doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven. Indien wetenschappelijk onderzoek echter erkende ethische normen in acht neemt, is een generiekere vorm van toestemming mogelijk (overweging 33). Wanneer de toestemming ziet op deelname aan wetenschappelijke onderzoeksactiviteiten in klinische proeven, geldt (overweging 161) het toestemmingsvereiste uit artikel 2 lid 21 van Verordening 536/2014. Zie over onderzoek nader artikel 89.

Wanverhouding. Wanneer sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name tussen burger en overheid, en deze het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk wordt verleend, is geen sprake van een rechtsgeldige toestemming (overweging 43). Een voorbeeld is de UWV-medewerker die toestemming vraagt een woning te betreden en te inspecteren en bij weigering de werkloosheidsuitkering kort of zelfs opschort. Ook bij de arbeidsverhouding kan snel een dergelijke wanverhouding ontstaan. Zo probeerden werkgevers in de coronacrisis regelmatig, op basis van toestemming, werknemers te verzoeken informatie te delen over hun vaccinatiestatus. In dit geval maakt de hiërarchische verhouding dat toestemming lastig te verantwoorden is, daargelaten dat het gaat om bijzondere persoonsgegevens. Zie verder hierover de *Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers* van de Autoriteit Persoonsgegevens uit 2016

4.12 “inbreuk in verband met persoonsgegevens”: 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;

Er is sprake van een inbreuk in verband met persoonsgegevens (Engels: *personal data breach*), oftewel een datalek, in het geval van een inbreuk op de beveiliging van persoonsgegevens (zie artikel 32) die leidt tot enige ongeoorloofde verwerking daarvan. Datalekken moeten worden gemeld bij de toezichthouder (artikel 33) en vaak ook bij de betrokkenen (artikel 34).

Ongeoorloofde verwerking. De definitie noemt specifiek vernietiging, verlies, wijziging, verstrekking en toegang tot persoonsgegevens wanneer dit per ongeluk (zoals bij achterlating in de trein of bij brand) of op onrechtmatige wijze (bijvoorbeeld door een inbraak of misbruik van andermans computer) gebeurt. Uiteindelijk komt de definitie erop neer dat persoonsgegevens moeten zijn (1) vernietigd of verloren, (2) gewijzigd, (3) verstrekt of (4) toegankelijk gemaakt, alles op een manier die onrechtmatig is oftewel buiten de regels van de AVG (zie

met name artikel 5, de beginselen). Alle vier zijn te zien als een ‘lek’: persoonsgegevens komen waar zij niet behoren te zijn.

Inbreuk op beveiliging. Van een datalek is alleen sprake als daadwerkelijk de beveiliging van persoonsgegevens is geschonden. Een zwakke plek in de beveiliging is dus nog geen datalek.

Schade. Een datalek kan, zo meldt overweging 85, resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens of de beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie. Of deze schade zich daadwerkelijk voordoet, is echter niet relevant voor de vraag of sprake is van een datalek.

Inbreuk op de AVG. Op diverse plaatsen gebruikt de AVG de frase “inbreuk op deze Verordening” (*violation*). Dit is niet per se een inbreuk (*breach*) in de zin van deze definitie. De inbreuken bedoeld in definitie 12 worden behandeld in artikelen 33 (meldplicht toezichthouder), 34 (mededeling aan betrokkene), 40 lid 2 punt i (wijze van melden in gedragscode) en 70 lid 1 punt g (richtsnoeren over datalekken door Comité).

4.13 “genetische gegevens”: persoonsgegevens die verband houden met de overgeërfdde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;

Genetische gegevens zijn persoonsgegevens ten aanzien van overgeërfdde of verworven genetische kenmerken van een natuurlijke persoon. Deze verschaffen immers unieke informatie over diens fysiologie of gezondheid. Genetische gegevens worden gewoonlijk verkregen uit een analyse van een biologisch monster van de persoon in kwestie, met name een chromosoomanalyse of een analyse van desoxyribonucleïnezuur (DNA) of van ribonucleïnezuur (RNA). Genetische gegevens zijn bijzondere persoonsgegevens in de zin van artikel 9.

4.14 “biometrische gegevens”: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

Biometrische gegevens zijn persoonsgegevens verkregen uit iemands fysieke, fysiologische of gedragsgerelateerde kenmerken die eenduidige identificatie

mogelijk maken, zoals portretten, irisscans of vingerafdrukken. Wanneer deze gegevens worden verwerkt met het oog op de unieke identificatie van een persoon, worden het bijzondere persoonsgegevens (zie artikel 9 lid 1). Een straatfoto met daarop herkenbaar iemands gezicht is dus niet per definitie een bijzonder persoonsgegeven. Een pasfoto op een identiteitskaart is dat wel.

4.15 “gegevens over gezondheid”: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

Gegevens over gezondheid betreffen alle persoonsgegevens over fysieke of mentale gezondheid van een persoon, zoals ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de fysiologische of biomedische staat van de betrokkene, ongeacht de bron. Dit betreft niet alleen actuele gezondheidsgegevens maar ook gegevens uit verleden en toekomst. Ook gegevens over verleende medische behandelingen en dergelijke vallen hieronder, net als gegevens over gezondheidsdiensten (medische zorg, zoals bedoeld in Richtlijn 2011/24/EU). Overweging 35 voegt daar nog de patiëntnummers aan toe: een aan een natuurlijke persoon toegekend cijfer, symbool of kenmerk dat als unieke identificatie van die natuurlijke persoon geldt voor gezondheidsdoeleinden. Daarnaast zijn uitslagen van onderzoeken aan het lichaam of aan lichaamseigen stoffen (zoals bloed) ook gegevens over gezondheid. Gegevens over gezondheid zijn bijzondere persoonsgegevens in de zin van artikel 9.

4.16 “hoofdvestiging”:

4.16(a) met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd;

4.16(b) met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;

De locatie van de hoofdvestiging van een verwerkingsverantwoordelijke bepaalt welke toezichthouder bevoegd is bij een grensoverschrijdende verwerking (zie artikel 56 lid 1).

Vestiging. Een vestiging is iedere duurzame, reële en daadwerkelijke activiteit in een lidstaat, zelfs indien slechts gering (Hv) EU 1 oktober 2016, zaaknr. C-230/14, Weltimmo). Ook een handelsagent kan als ‘vestiging’ kwalificeren wanneer hij belast is met het innen van gelden in verband met een internetdienst en de verwerkingsverantwoordelijke vertegenwoordigt bij geschillen (idem).

Hoofdvestiging bij verwerkingsverantwoordelijke. In beginsel geldt als hoofdvestiging de vestiging waar de centrale administratie van de verwerkingsverantwoordelijke wordt gevoerd. Uitzondering geldt echter wanneer de beslissingen over de verwerking (doel en middelen) elders in de EU worden genomen. In dat geval is die locatie de hoofdvestiging. Als deze beslissingen buiten de EU worden genomen, maar de centrale administratie ligt wel in de EU, dan is de administratie-vestiging de hoofdvestiging. Waar feitelijk de verwerking plaatsvindt, is niet relevant voor of een vestiging de hoofdvestiging is (overweging 36).

Hoofdvestiging bij concerns. Indien de verwerking door een concern (zie definitie 19) wordt uitgevoerd, is het moederbedrijf de verwerkingsverantwoordelijke tenzij het doel en de middelen uitsluitend binnen een specifieke dochter worden bepaald (overweging 37).

Hoofdvestiging bij verwerker. Bij de verwerker geldt net als bij de verwerkingsverantwoordelijke als hoofdregel de vestiging waar de centrale administratie wordt gevoerd. Uitzondering geldt hier echter voor het geval de voornaamste verwerkingsactiviteiten elders plaatsvinden; dan is dát de hoofdvestiging.

4.17 “vertegenwoordiger”: een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;

Wanneer een verwerkingsverantwoordelijke of verwerker buiten de EU is gevestigd, dient zij in beginsel (zie artikel 27 lid 2 voor de criteria) een vertegen-

woordiger binnen de EU aan te wijzen die haar vertegenwoordigt. De vertegenwoordiger moet zijn gevestigd in een lidstaat van de Europese Unie, meer specifiek een lidstaat waar de betrokkenen zijn om wie de verwerking door de niet-Europese verwerkingsverantwoordelijke of verwerker gaat (artikel 27 lid 3). De vertegenwoordiger dient ten behoeve van de verwerkingsverantwoordelijke of de verwerker op te kunnen treden en kan door iedere toezichthoudende autoriteit worden benaderd (artikel 27 lid 4). De vertegenwoordiger kan aan handhavingprocedures worden onderworpen in geval van niet-naleving door de verwerkingsverantwoordelijke of de verwerker (artikel 27 lid 5).

4.18 “onderneming”: een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;

Een onderneming is iedere natuurlijke of rechtspersoon die een economische activiteit ontplooit. De rechtsvorm is niet van belang: naast bijvoorbeeld de besloten vennootschap zijn ook de eenmanszaak en de vennootschap onder firma dus ondernemingen in de zin van de AVG. Ook verenigingen en stichtingen kunnen ondernemingen zijn in deze zin, wanneer zij actief zijn in het economisch verkeer.

Economische activiteit. Het begrip ‘onderneming’ wordt onder de AVG breed uitgelegd; het omvat iedere entiteit die een economische activiteit uitoefent. Voor de uitleg van dit criterium wordt aangesloten bij de karteljurisprudentie rond artikelen 101 en 102 van het Verdrag betreffende de Werking van de Europese Unie (VWEU). Zie bijvoorbeeld HvJ EU 23 april 1991, zaaknr. C-41/90, Höfner.

Regels voor ondernemingen. Een onderneming met minder dan 250 man personeel hoeft geen register van verwerkingsactiviteiten bij te houden, tenzij er sprake is van een gegevensverwerking die onder een van de uitzonderingen valt (artikel 30). Voor ondernemingen kunnen boetes ook berekend worden als maximaal 2% of 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is dan de gewone boetes (artikel 83 lid 4 en lid 5). Daarnaast is deze definitie van belang bij de definitie van ‘concern’ (zie definitie 19).

Gegevens van ondernemingen. De AVG heeft geen betrekking op de verwerking van gegevens over rechtspersonen en met name als rechtspersonen gevestigde ondernemingen, zoals de naam en de rechtsvorm van de rechtspersoon en de contactgegevens van de rechtspersoon (overweging 14). Gegevens van specifieke personen binnen de onderneming zijn wél persoonsgegevens, ook wanneer de gegevens slechts zakelijke doeleinden dienen (denk aan het zakelijk doorkiesnummer van een medewerker of een e-mailadres dat een persoonsnaam bevat).

- 4.19 “concern”: een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend;

Wanneer bedrijven economisch met elkaar zijn verweven, is sprake van een concern. Een bekende concern-constructie is die van het moederbedrijf met zeggenschap over een of meer dochterbedrijven. Zeggenschap volgt onder meer uit het hebben van 51% van de stemgerechtigde aandelen of het voeren van directie (zie ook art. 2:24a BW). Naar Nederlands recht wordt ook wel gesproken van een groep (art. 2:24b BW). Binnen een concern kan zowel het moederbedrijf als een dochter de verwerkingsverantwoordelijke (definitie 7) zijn. De vraag blijft wie doel en middelen vaststelt. Een shared service center dat voor alle afdelingen de HR uitvoert, is bijvoorbeeld eerder verwerker dan verwerkingsverantwoordelijke. Een dochterbedrijf dat de IT-infrastructuur beheert en naar eigen inzicht monitoring uitvoert, zal ondanks de status als dochter wél als verwerkingsverantwoordelijke kwalificeren. Een bedrijfsonderdeel dat toezicht houdt op de verwerking van persoonsgegevens elders in het concern wordt meegerekend met het concern (overweging 37).

- 4.20 “bindende bedrijfsvoorschriften”: beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;

Bindende bedrijfsvoorschriften, ook wel *binding corporate rules* of BCR, zijn beleidsregels binnen een concern over hoe persoonsgegevens intern worden gedeeld met dochter- of zustermaatschappijen buiten de Europese Unie. Zie nader artikel 47.

- 4.21 “toezichthoudende autoriteit”: een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;

Ter handhaving van de bepalingen uit de AVG dient iedere lidstaat een onafhankelijke toezichthouder in te stellen (artikel 51). Voor taken en bevoegdheden zie artikelen 57 en 58. Toezichthouders moeten samenwerken (artikel 61) en kunnen gezamenlijk optrekken (artikel 62). Als een verwerking grensoverschrijdend is (definitie 23), wordt één van hen leidend (zie nader artikel 60). De Nederlandse toezichthoudende autoriteit is de AP.

- 4.22 “betrokken toezichthoudende autoriteit”: een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat:

In gevallen waarin meerdere toezichthouders competent zijn ten aanzien van een verwerking (artikel 56), wordt één van hen de leidende toezichthouder. Dit

is de toezichthouder die bevoegd is voor het land van de hoofdvestiging van de verwerkingsverantwoordelijke. De overige toezichthouders (bijvoorbeeld zij die competent zijn ten aanzien van een verwerker of een andere vestiging van de verwerkingsverantwoordelijke) worden als ‘betrokken’ aangemerkt en hebben het recht deel te nemen aan het onderzoek van de leidende toezichthouder (zie nader artikel 60).

4.22(a) de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd;

Het eerste en belangrijkste criterium is dat de verwerkingsverantwoordelijke of de verwerker een vestiging (zie definitie 16) heeft in de lidstaat waarvoor de toezichthouder competent is.

4.22(b) de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of

Wanneer de verwerkingsverantwoordelijke of de verwerker geen vestiging heeft in de lidstaat van een toezichthouder, is deze desondanks bevoegd wanneer betrokkenen wezenlijke gevolgen (waarschijnlijk) zullen ondervinden. Zie nader artikel 56 lid 1 over dit begrip.

4.22(c) bij die toezichthoudende autoriteit een klacht is ingediend;

Wanneer situaties a noch b van toepassing zijn, maar de toezichthouder wel een klacht (artikel 77) ontvangt, kan hij een wél competente toezichthouder aansporen tot onderzoek over te gaan (artikel 56). De betreffende toezichthouder wordt dan betrokken (artikel 4 definitie 22) bij dit onderzoek.

4.23 “grensoverschrijdende verwerking”:

Een verwerking is grensoverschrijdend als zij plaatsvindt hetzij in vestigingen in meerdere landen, hetzij als betrokkenen uit meerdere landen wezenlijke gevolgen kunnen ondervinden van de verwerking. In deze situatie zullen meerdere toezichthouders betrokken zijn (zie artikel 56 over de dan geldende competentieregels en Guidelines WP 244 for identifying a controller or processor’s lead supervisory authority (alleen beschikbaar in het Engels), 13 december 2016). Wanneer een land buiten de EU is betrokken, is sprake van doorgifte (artikel 44).

4.23(a) verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of

Het eerste criterium voor een grensoverschrijdende verwerking is wanneer vestigingen (zie definitie 16) in meerdere lidstaten de verwerking van persoonsge-

gevens uitvoeren. Een verwerking is ook grensoverschrijdend als een verwerker in een ander land is gevestigd dan de verwerkingsverantwoordelijke. Enkel het feit dat persoonsgegevens kunnen worden opgevraagd via internet in een andere lidstaat maakt een verwerking nog niet grensoverschrijdend (zie het Lindqvist-arrest, HvJ EU 6 november 2003, zaaknr. C-101/01).

4.23(b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden;

Wanneer slechts één vestiging de verwerking uitvoert, zal gewoonlijk geen sprake zijn van een grensoverschrijdende verwerking. Echter, wanneer betrokkenen in meerdere lidstaten wezenlijke gevolgen ondervinden, wordt de verwerking alsnog grensoverschrijdend genoemd.

Wezenlijke gevolgen. De AVG bevat geen definitie van het begrip ‘wezenlijk’. *Guidelines WP 244 for identifying a controller or processor’s lead supervisory authority* (alleen beschikbaar in het Engels), 13 december 2016, werken het begrip nader uit, zoals besproken bij artikel 56 lid 1.

4.24 “relevant en gemotiveerd bezwaar”: een bezwaar over het al dan niet bestaan van een inbreuk op deze verordening of over de vraag of de voorgenomen maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangegeven van de risico’s die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;

Een toezichthouder kan bezwaar maken tegen een ontwerpbesluit van een andere toezichthouder in het kader van een grensoverschrijdende verwerking (artikel 60 lid 4). Dit bezwaar moet per definitie relevant en gemotiveerd zijn. Het Comité heeft richtsnoeren opgesteld over de invulling van deze criteria overeenkomstig artikel 70 lid 1 sub t. Zie hiervoor de Richtsnoeren 9/2020 inzake relevant en gemotiveerd bezwaar overeenkomstig Verordening 2016/679 van het Comité, 9 maart 2021.

4.25 “dienst van de informatiemaatschappij”: een dienst als gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad;

Volgens Richtlijn 2015/1535 is een dienst van de informatiemaatschappij een dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht. Zie in Nederland artikel 3:15d lid 3 BW. Het gaat dus niet slechts om het gebruik van

elektronica, maar vooral om het op afstand en op verzoek van de afnemer ver-
richten van een dienst.

Diensten van de informatiemaatschappij. Om als dienst van de informatie-
maatschappij te worden aangemerkt, gelden drie eisen. Allereerst moet deze
worden geleverd zonder dat de partijen gelijktijdig aanwezig zijn, zoals bij een
videostreamingapp. Ten tweede moet deze worden geleverd via elektronische
apparatuur, al dan niet draadloos. Een spraaktelefoon of fax voldoet niet aan
dit criterium, online bellen zoals via Skype wel. Als derde moet de dienst pas
worden gestart als de afnemer daarom vraagt. Radio en televisie vallen hier niet
onder. Muziek via Spotify bijvoorbeeld wel.

Regels voor diensten van de informatiemaatschappij. Bij dergelijke diensten
geldt een apart regime voor toestemming bij kinderen (artikel 8). Ook is het
recht van gegevenswissing dan van toepassing (artikel 17 lid 1 punt f), en het
recht van bezwaar (artikel 21 lid 5) moet in dit geval geautomatiseerd uitgeoef-
end kunnen worden.

4.26 “internationale organisatie”: een organisatie en de daaronder vallende interna-
tionaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of
op grond van een overeenkomst tussen twee of meer landen.

Een internationale organisatie is iedere organisatie (of orgaan daarvan) die is
opgericht krachtens internationaal publiekrecht of bij internationale overeen-
komst tussen staten. Voorbeelden zijn de Wereldhandelsorganisatie, de Ver-
enigde Naties, het Internationaal Strafhof te Den Haag (een orgaan van de VN)
en het Europees Octrooibureau (opgericht krachtens het Europees Octrooiver-
drag, een los van de EU staand verdrag). EU-organisaties vallen hier niet onder.

Regels voor internationale organisaties. De internationale organisatie wordt op
één lijn gesteld met het derde land, waardoor de regels over doorgifte (hoofdstuk
V) van toepassing zijn bij verstrekking aan internationale organisaties.

Hoofdstuk II

Beginnelsen voor verwerking

Hoofdstuk II bevat de algemene regels voor een rechtmatige verwerking van persoonsgegevens. Allereerst formuleert artikel 5 zes algemene beginselen ten aanzien van alle verwerkingen. Artikel 6 introduceert dan zes grondslagen voor verwerking, waarbij artikel 7 de grondslag toestemming in het algemeen uitwerkt en artikel 8 toestemming door kinderen bij internetdiensten. Bijzondere persoonsgegevens worden geregeld in artikel 9, met een apart artikel 10 voor strafrechtelijke persoonsgegevens. Als laatste bepaalt artikel 11 dat een verwerkingsverantwoordelijke niet gehouden is extra informatie te verzamelen om maar betrokkenen (direct) te kunnen identificeren.

Artikel 5. Beginselen inzake de verwerking van persoonsgegevens

5.1. Persoonsgegevens moeten:

De AVG gaat uit van zes basisbeginselen waaraan elke verwerking moet voldoen. Verwerking van persoonsgegevens valt onder het grondrecht ter eerbiediging van de persoonlijke levenssfeer, en iedere verwerking moet dus uiteindelijk dat grondrecht respecteren. Deze beginselen zijn bedoeld als algemene borging en werken door in de interpretatie van de rechten en plichten elders uit de AVG. Zij zijn gebaseerd op de *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) uit 1980.

De basisbeginselen zijn niet slechts mooie woorden ter inleiding maar hebben zelfstandige betekenis als norm (zie ook HvJ EU 20 mei 2003, zaken C-465/00, C-138/01 en C-139/01). Een betrokkene kan zich er rechtstreeks op beroepen bij de rechter of toezichthouder om bijvoorbeeld een belangenafweging anders te laten uitvallen of een bepaalde verwerking te doen staken.

Er staan boetes op het niet naleven van deze beginselen (artikel 83 lid 5 punt a). Zo gaf de AP een boete omdat een organisatie een kopie van een paspoort vroeg om een identiteit te verifiëren in het geval een betrokkene haar rechten uitoefende (hoofdstuk III). Dit was niet in lijn met het beginsel van dataminimalisatie: dat doel (verificatie van identiteit) kon gediend worden met minder, en minder gevoelige, gegevens (AP, Boetebesluit DPG Media, 24 februari 2022).

- 5.1(a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (“rechtmatigheid, behoorlijkheid en transparantie”);

Het beginsel van rechtmatigheid, behoorlijkheid en transparantie houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet dus eenvoudig toegankelijk en begrijpelijk zijn, en er moet duidelijke en eenvoudige taal worden gebruikt. Dit geldt dus voor de privacyverklaring (zie artikel 12, 13 en 14) maar ook voor andere communicatie, zoals wanneer de betrokkene om inzage verzoekt (artikel 15) of bij het afhandelen van bezwaren (artikel 21). Juridische taal is dus zeer ongewenst.

Naast uitleg over het gebruik van persoonsgegevens moet ook op transparante wijze duidelijk worden gemaakt welke risico’s, regels, waarborgen en rechten betrokkenen hebben, alsook over de wijze waarop zij hun rechten onder de AVG kunnen uitoefenen.

Rechtmatig. De term ‘rechtmatig’ lijkt naar Nederlands recht een tautologie: een verwerking die onrechtmatig is, is per definitie niet toegestaan. Deze term komt echter uit het Angelsaksische recht, waar “fairly and lawfully” een zelfstandige betekenis heeft. De beste Nederlandse benadering zou zijn dat niet in strijd wordt gehandeld met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt (art. 6:162 BW), een open norm dus voor netjes handelen.

- 5.1(b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (“doelbinding”);

Aansluitend op het beginsel van rechtmatigheid, behoorlijkheid en transparantie geldt het doelbindingsprincipe.

Welbepaald. Verwerking mag alleen gebeuren voor specifieke en gerechtvaardigde doeleinden, die zijn vastgesteld en omschreven voordat men begint met de verwerking, of voor andere doelen die daarmee verenigbaar zijn. Een omschrijving van het soort “wij verzamelen uw gegevens voor onze bedrijfsdoeleinden” is te generiek. Ook vage verwijzingen naar toekomstige mogelijke verwerkingen zijn onvoldoende. Zie over dit beginsel in het kader van de Richtlijn *Advies 03/2013 over doelbinding bij verwerking van persoonsgegevens* (WP 203, 2 april 2013) van de Artikel 29-Werkgroep.

Gerechtaardigd. De verwerking mag alleen gebeuren voor gerechtvaardigde doeleinden. Dit gaat verder dan enkel dat het doel rechtmatig (niet in strijd met de wet) moet zijn. Er moet een reden zijn die de inperking van het grondrecht privacy kan rechtvaardigen. Zo kan een verwerkingsverantwoordelijke zich daarbij beroepen op de ondernemingsvrijheid (HvJ EU 24 november 2011, ECLI:EU:C:2011:771, Sabam/Scarlet) of de vrijheid van meningsuiting, waarna een belangenafweging plaats dient te vinden.

Verenigbaar. Verwerking mag alleen plaatsvinden voor de vooraf gemelde doelen, of voor doelen die verenigbaar zijn met deze doelen. Dit geldt niet alleen voor verwerkingen door derden; ook de verwerkingsverantwoordelijke zelf mag alleen verdere verwerkingen uitvoeren die verenigbaar zijn met de oorspronkelijke verwerkingsdoelen. Zie bovengenoemd Advies dat tevens ingaat op het concept verenigbaarheid.

Verenigbaarheid en grondslag. Wanneer een nieuwe verwerking als verenigbaar met een eerdere verwerking te zien is, is geen aparte grondslag (zoals hernieuwde toestemming, artikel 6 lid 1) nodig voor de nieuwe verwerking. Zij is dan te zien als een uitweiding binnen de originele grondslag (overweging 50).

Archivering en onderzoek. Verdere verwerkingen ten behoeve van archivering of wetenschappelijk onderzoek worden per definitie als verenigbaar beschouwd met het doel van de oorspronkelijke verwerking. Zij zijn dus in beginsel altijd toegestaan, ook als deze doelen niet expliciet zijn gemeld. Natuurlijk moeten deze verdere verwerkingen wel voldoen aan andere eisen, zoals de beginselen van rechtmatigheid, transparantie en juistheid. Zie hiervoor nader artikel 89.

5.1(c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (“minimale gegevensverwerking”);

Het beginsel van dataminimalisatie brengt met zich mee dat niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is voor het doel. Hieruit volgt ook dat persoonsgegevens zo snel mogelijk moeten worden gewist of onherkenbaar gemaakt. Er mogen echter ook weer niet te weinig persoonsgegevens worden verzameld, dat kan immers leiden tot een onjuist beeld van de betrokkene.

Uit dit beginsel vloeit tevens voort dat persoonsgegevens alleen mogen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt, bijvoorbeeld met geaggregeerde gegevens.

- 5.1(d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (“juistheid”);

Wanneer wordt gewerkt met onjuiste of achterhaalde gegevens, kan dat vervelende gevolgen hebben voor de betrokkene. Vandaar dat het vierde beginsel, dat van juistheid, eist dat gegevens juist en actueel moeten zijn. De verwerkingsverantwoordelijke heeft daarbij een vérgaande inspanningsplicht om deze juistheid te borgen.

Blijken gegevens onjuist of achterhaald, dan moeten zij worden gewist. Dit beginsel is nader uitgewerkt in de rechten van rectificatie (artikel 16) en gegevenswissing (artikel 17), maar uit het beginsel vloeit een zelfstandige plicht voort voor de verwerkingsverantwoordelijke om actief zorg te dragen voor de juistheid van de persoonsgegevens die hij onder zich heeft. Het is dus onjuist (en boetewaardig, artikel 83 lid 5 punt a) om passief te wachten tot betrokkenen klagen over onjuiste of achterhaalde persoonsgegevens.

- 5.1(e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen (“opslagbeperking”);

Het beginsel van opslagbeperking dient ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerking.

Termijnen. De AVG noemt geen harde getalsmatige termijnen maar verlangt van de verwerkingsverantwoordelijke dat deze gezien zijn beoogde verwerkingen concrete termijnen vaststelt voor het wissen van gegevens of voor een periodieke toetsing ervan. Termijnen mogen functioneel omschreven zijn (“zo lang als nodig is om onze diensten aan u te leveren”), maar moeten wel een duidelijk vast te stellen einde hebben.

Voorbeelden. Enkele concrete bewaartermijnen uit de wet zijn:

- Personeelsdossier (documenten waaruit verplichtingen volgen): Tot twee jaar na einde dienstverband (art. 52 Algemene Wet Rijksbelastingen)
- Loonbelastingverklaringen en kopie identiteitsbewijs: Tot vijf jaar na einde dienstverband (art. 7.5 Uitvoeringsregeling Loonbelasting)

- Facturen in verband met omzetbelasting: Zeven jaar vanaf dag van opstellen (art. 31 Uitvoeringsbeschikking omzetbelasting)
- Debiteuren- en crediteurenadministratie: Zeven jaar vanaf 1 januari van het jaar na opstellen (art. 52 Wet Rijksbelastingen, art. 8 Douanewet)

Vrijstellingsbesluit. Onder de Wbp was een zogeheten Vrijstellingsbesluit beschikbaar dat bepaalde welke verwerkingen vrijgesteld waren van de destijds verplichte melding bij de AP. Deel van de omschrijving was een maximale verwerkingstermijn. Dit werd door velen opgevat als een wettelijk toegestane bewaartermijn. Ondanks dat dit Besluit met de Wbp is ingetrokken, zien wij nog vele verwijzingen naar dit Besluit als rechtvaardiging voor een bewaartermijn (zoals dat camerabeelden 28 dagen bewaard mogen worden). Dit is echt onjuist: de termijn moet door de verwerkingsverantwoordelijke zelf worden bepaald en gemotiveerd. Dat de AP onder de Wbp die termijn als maximum voor de vrijstelling tot melden had genoemd, is daarbij in het geheel geen argument.

Bewaarplicht. Diverse wetgeving (zoals fiscale wetten) verplichten de verwerkingsverantwoordelijke om bepaalde gegevens te bewaren gedurende een bepaalde periode. Dit is dan gerechtvaardigd onder de AVG vanwege de verwerkingsgrond wettelijke plicht (artikel 6 lid 1 punt c), en daaruit volgt dat de gegevens mogen (moeten) worden bewaard gedurende de wettelijke termijn.

Archivering en onderzoek. Langere opslag ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is toegestaan, mits passende waarborgen worden genomen (zie nader artikel 89).

- 5.1(f) 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”).

Ter borging van het beginsel van integriteit en vertrouwelijkheid moet de verwerkingsverantwoordelijke technische en organisatorische beveiligingsmaatregelen nemen om ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens te voorkomen. Dit beginsel wordt nader uitgewerkt in artikel 32, met daaraan gekoppeld de datalekmeldplicht uit artikel 33 en 34.

- 5.2 De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen (“verantwoordingsplicht”).

De AVG legt de bal voor het voldoen aan deze beginselen expliciet bij de verwerkingsverantwoordelijke. Deze dient erop toe te zien dat de beginselen worden nageleefd, en belangrijker: moet in staat zijn dit aan te kunnen tonen. Deze

verantwoordingsplicht introduceert echter ook een omgekeerde bewijslastverdeling. Kan de verwerkingsverantwoordelijke niet aantonen dat hij heeft voldaan aan een beginsel, dan is sprake van een boetewaardige overtreding van de AVG. Zie ook de *Richtlijn inzake transparantie overeenkomstig Verordening 2026/679* van de Artikel 29-Werkgroep, 11 april 2018 (WP260).

Artikel 6. Rechtmatigheid van de verwerking

- 6.1 De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

Het beginsel van rechtmatigheid uit artikel 5 wordt nader uitgewerkt in artikel 6, dat de grondslagen voor verwerking biedt. Uitsluitend de hier genoemde grondslagen bieden een rechtvaardiging om persoonsgegevens te mogen verwerken. Het is toegestaan deze grondslagen bij (nationale of Europese) wet anders te regelen of andere grondslagen te introduceren als dat noodzakelijk is voor de vrijheid van meningsuiting (artikel 85) of een goede regeling van arbeidsverhoudingen (artikel 88).

- 6.1(a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

Toestemming is iedere vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene aanvaardt dat zijn persoonsgegevens worden verwerkt (artikel 4 definitie 11). Deze wilsuiting moet actief worden gedaan, stilzwijgen is nimmer voldoende. De toestemmingsvraag moet duidelijk en eenvoudig zijn geformuleerd (zie hierover nader artikel 7).

Toestemming door kinderen. Kinderen zijn in beginsel handelingsonbekwaam om toestemming te geven (art. 1:234 BW), tenzij de verwerking gebruikelijk is voor personen van hun leeftijd. Er is geen bijzondere leeftijdsgrens onder de AVG, behalve bij internet- en telefoniediensten (zie artikel 8). De Uitvoeringswet (artikel 5 lid 1) bepaalt echter dat bij personen onder de zestien toestemming van de ouder/verzorger nodig is.

Toestemming bij een onder curatele of in mentorschap gestelde betrokkene. Toestemming voor de gegevensverwerking van een onder curatele gestelde, dan wel van een in mentorschap gestelde betrokkene, dient te worden gegeven door diens wettelijk vertegenwoordiger (artikel 5 Uitvoeringswet).

- 6.1(b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;

Naast toestemming is ook de noodzaak voor de uitvoering van een overeenkomst een grondslag voor verwerking. Dit omvat mede precontractuele maatregelen.

Noodzakelijk. De noodzaak moet objectief vastgesteld worden en betekent meer dan een contractuele verplichting (Richtsnoeren 2/2019 van de EDPB). De vraag is waarom wezenlijke aspecten van de overeenkomst met de betrokkene feitelijk niet kunnen worden uitgevoerd als de specifieke verwerking van de betreffende persoonsgegevens niet plaatsvindt (Rb. Amsterdam 15 maart 2023, ECLI:NL:RBAMS:2023:1407).

Rechtmatig. Een verwerking die noodzakelijk is in het kader van een overeenkomst of een voorgenomen overeenkomst, dient rechtmatig te zijn (overweging 44). Dit volgt mede uit het rechtmatigheidsbeginsel (artikel 5 lid 1 punt a).

Precontractuele maatregelen. Ook verwerkingen die noodzakelijk zijn in de aanloop tot de sluiting van een overeenkomst kunnen onder punt b worden gerechtvaardigd. Wel moeten deze verwerkingen op verzoek (en dus initiatief) van de betrokkene zijn genomen. Direct marketing, waarbij betrokkenen ongevraagd worden aangespoord een overeenkomst te sluiten is dus niet te rechtvaardigen onder dit punt. Het verwerken van persoonsgegevens voor het laten doorlopen van een sollicitatieproces gebeurt in de regel op basis van de grondslag uitvoering van de overeenkomst, waarbij het gaat om de voorbereiding van een eventuele arbeidsovereenkomst, oftewel de precontractuele fase.

- 6.1(c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

Een derde grondslag is wanneer de verwerkingsverantwoordelijke wettelijk verplicht is om de verwerking uit te voeren. Een voorbeeld is de verstrekking van gegevens over werknemers aan de Belastingdienst. De wettelijke verplichting moet worden gevonden in Unierecht of in nationaal recht (zie nader lid 3).

- 6.1(d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

Als vierde grondslag geldt een noodzaak om de vitale belangen van de betrokkene (of een ander persoon, zoals diens kind) te beschermen. Een vitaal belang raakt aan het leven van die persoon. Te denken valt aan verwerkingen van medische gegevens bij een ongeval, of in humanitaire noodsituaties zoals natuurrampen of door de mens veroorzaakte rampen.

Geen andere grond. Verwerking van persoonsgegevens op grond van het vitale belang voor een andere natuurlijke persoon is in beginsel alleen toegestaan indien de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd (overweging 46).

6.1(e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

Een verwerking is ook gerechtvaardigd als deze noodzakelijk is voor een taak van algemeen belang of een taak voor het openbaar gezag.

Algemeen belang. De AVG definieert niet wanneer sprake is van een algemeen belang. Dit belang is in ieder geval niet beperkt tot overheidsinstanties. Overweging 45 noemt gezondheidsdoeleinden zoals volksgezondheid, sociale bescherming en het beheer van gezondheidszorgdiensten. Denk bijvoorbeeld aan het verwerken van informatie over coronabesmettingen door de overheid gedurende de coronapandemie, om de bewegingen van de ziekte te monitoren en op basis daarvan beleid te vormen om de volksgezondheid te bevorderen. De taak van algemeen belang dient wel op een of andere manier tot een wettelijke regeling te herleiden zijn (zie ook lid 3).

Openbaar gezag. Van openbaar gezag is sprake wanneer overheidsinstanties of -organen hun bij wet geregelde taak uitvoeren (een zogenoemde publieke taak). In het Unierecht of het lidstatelijke recht zou dan nader moeten worden vastgesteld en gespecificeerd voor welke taken en doeleinden de verdere verwerking als rechtmatig en verenigbaar met de aanvankelijke doeleinden moet worden beschouwd (overweging 50). Het is hiervoor niet noodzakelijk dat de publieke taak of de gegevensverwerking uitputtend is geregeld in een wet in formele zin. Voldoende is dat de hoofdlijnen kenbaar zijn in de wet. Dit is in overeenstemming met jurisprudentie van het EVRM waarin is bepaald dat ‘voorzienbaar bij wet’ ziet op een materieel wetsbegrip (Memorie van Toelichting (MvT) Uitvoeringswet, p. 43). Dit is dus breder dan een wettelijke plicht: die ziet namelijk echt op het gegevensgebruik. Bij het algemeen belang of een taak van openbaar gezag gaat het eerder om een algemeen belang of taak die wettelijk te herleiden is, waarvoor het gebruiken van persoonsgegevens noodzakelijk is.

Geen gegevenswissing. Bij een verwerking op deze grondslag heeft de betrokkene geen recht van gegevenswissing (artikel 17 lid 3 punt b). Wel zal vanuit de beginselen van juistheid (artikel 5 lid 1 punt d) en opslagbeperking (artikel 5 lid 1 punt e) de betreffende wettelijke regeling moeten bepalen wanneer persoonsgegevens zullen worden verwijderd.

Bezwaar. De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen een verwerking onder deze grondslag (artikel 21 lid 1). De verwerkingsverantwoordelijke

moet dan de verwerking staken, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die het bezwaar passeren.

- 6.1(f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De zesde en laatste grondslag is het eigen gerechtvaardigde belang van de verwerkingsverantwoordelijke (of een derde). Deze grondslag vereist wel een belangenafweging met de grondrechten van de betrokkene.

Belangenafweging. De belangenafweging stelt het belang van de verwerkingsverantwoordelijke tegenover de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene. Dit is een open norm en de afweging wordt dan ook uitgevoerd op basis van alle omstandigheden van het geval. Een belangrijke factor hierbij is in hoeverre de betrokkene redelijkerwijs mag verwachten dat verwerking met dat doel kan plaatsvinden. Bij deze verwachtingen speelt de verhouding tot de verwerkingsverantwoordelijke een belangrijke rol. In omstandigheden waarin de betrokkenen redelijkerwijs geen verdere verwerking verwachten, mag geen beroep op deze grondslag worden gedaan (overweging 47).

Bezwaar. De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen een verwerking onder deze grondslag (artikel 21 lid 1). De verwerkingsverantwoordelijke moet dan de verwerking staken, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die het bezwaar passeren. Betreft het eigen belang de uitvoering van direct marketing of bijbehorende profilering, dan is het bezwaar te allen tijde doeltreffend (artikel 21 lid 3).

Verwerking binnen concern. Verwerkingsverantwoordelijken die deel uitmaken van een concern of een groep van instellingen kunnen een gerechtvaardigd belang hebben bij de doorzending van persoonsgegevens binnen het concern voor interne administratieve doeleinden (overweging 48). Een concern of groep kan bindende bedrijfsvoorschriften (artikel 47) treffen om doorgifte te regelen wanneer delen van het concern of de groep buiten de EU zijn gevestigd.

Fraudepreventie. Fraudepreventie is een gerechtvaardigd belang (overweging 47). Uiteraard moet bij de verwerking voor dit belang nog steeds een passende belangenafweging worden gemaakt. De analyse mag dus niet onnodig diep ingaan op de privacy van de vermoedelijke fraudeur. Meestal wordt dit uitgewerkt in een fraudeprotocol, waarbij men na algemene signalen van mogelijke fraude nader onderzoek opstart dat dieper kijkt naar persoonlijke informatie.

Direct marketing. Onder direct marketing wordt verstaan het totstandbrengen of instandhouden van een directe relatie tussen aanbieder en betrokkene met het oog op werving voor commerciële doelen. Deze term is afkomstig uit Richtlijn 2002/58/EG (vergelijk ECLI:NL:CBB:2014:206) en is een gerechtvaardigd belang (overweging 47). Er moet dus enige vorm van gerichtheid in de communicatie zijn; een generieke 'banner' op internet of een poster in een abri zijn geen direct marketing. Uiteraard moet bij de verwerking voor dit belang nog steeds een passende belangenafweging worden gemaakt. Een voorbeeld van een toegelaten direct marketing activiteit is het verstrekken van namen en postadressen van leden van een vereniging aan een adverteerder die daar reclame heen stuurt, waarbij leden vooraf bezwaar ("optout") kunnen maken en deze verstrekking goedgekeurd is door de Algemene Ledenvergadering. Het recht van bezwaar geldt ongeclausuleerd bij direct marketing (zie artikel 21 lid 3).

Aangifte. Een verwerkingsverantwoordelijke mag bij wijze van eigen gerechtvaardigd belang persoonsgegevens gebruiken in een aangifte of vergelijkbaar bestuursrechtelijk traject wanneer het gaat om mogelijke strafbare feiten of gevaren voor de openbare veiligheid. Uiteraard mag dat niet als op hem een wettelijke, beroepsmatige of anderszins bindende geheimhoudingsplicht rust (overweging 50).

Netwerkbeveiliging. De verwerking van persoonsgegevens voor zover die strikt noodzakelijk en evenredig is met het oog op netwerk- en informatiebeveiliging wordt in beginsel als gerechtvaardigd belang aangemerkt (overweging 49). Dit betreft maatregelen om te zorgen dat een netwerk of informatiesysteem op een bepaald vertrouwelijkheidsniveau bestand is tegen incidentele gebeurtenissen of onrechtmatige of kwaadaardige acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of doorgegeven persoonsgegevens in het gedrang brengen, en meer algemeen de beveiliging van de daarmee verband houdende. Dit belang geldt voor overheidsinstanties, computercrisisteam (computer emergency response teams), computercalamiteitenteams (computer security incident response teams), aanbieders van elektronische communicatienetwerken en -diensten en aanbieders van beveiligingstechnologie en -diensten.

Archieven. Het beheer van archieven van kranten, tijdschriften en dergelijke geldt als een gerechtvaardigd belang (Europees Hof voor de Rechten van de Mens (EHRM) 10 maart 2009, ECLI:EU:C:2011:255 (Times v. UK); Raad van State 8 september 2010, ECLI:NL:RVS:BN6172). Dit belang wordt dan gevonden in het grondrecht van de uitingsvrijheid.

De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

Overheidsinstanties kunnen zich niet beroepen op een verwerking krachtens een eigen belang. Dit omdat dergelijke verwerkingen tot een wet te herleiden

moeten zijn (overweging 47) en derhalve eigenlijk altijd dus onder lid 1 punt e (goede uitvoering overheidstaak) te rechtvaardigen zullen zijn. Let wel, dat is dus ten aanzien van verwerkingen die in het kader liggen van de uitoefening van hun taken.

Commercieel belang. Zoals eerder gesteld, is direct marketing in overweging 47 erkend als gerechtvaardigd belang. Desalniettemin is er discussie over in hoeverre een commercieel belang als gerechtvaardigd belang kan dienen. De AP interpreteert de gerechtvaardigde belangen als *“uitsluitend tot de wet behorende, wet zijnde, in een wet vastgestelde, belangen”* (Rb. Amsterdam 22 september 2022, ECLI:NL:RBAMS:2022:5565). Zuiver commerciële belangen zouden de toets niet doorstaan. Naar aanleiding van deze nauwe interpretatie van de grondslag gerechtvaardigd belang, is de AP op de vingers getikt door de Europese Commissie. Weliswaar moet een beroep op deze grondslag beperkt worden uitgelegd (HvJ EU 4 mei 2017, C-13/16, ECLI:EU:C:2017:336 (Rigas), punt 30), maar op voorhand uitsluiten is niet de bedoeling. In een procedure tussen KNLTB en AP zijn vragen voorgelegd aan het Hof van Justitie (Rb. Amsterdam 22 september 2022, ECLI:NL:RBAMS:2022:5565).

6.2 De lidstaten kunnen specifiekere bepalingen handhaven of invoeren ter aanpassing van de manier waarop de regels van deze verordening met betrekking tot de verwerking met het oog op de naleving van lid 1, punten c) en e), worden toegepast; hiertoe kunnen zij een nadere omschrijving geven van specifieke voorschriften voor de verwerking en andere maatregelen om een rechtmatige en behoorlijke verwerking te waarborgen, ook voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX.

Lidstaten mogen bij de gronden wettelijke verplichting (lid 1 punt c) en algemeen belang (lid 1 punt e) specifiekere regels invoeren, bijvoorbeeld dat aan nadere voorwaarden moet zijn voldaan om hier een beroep op te mogen doen of dat aanvullende procedurele regels gelden bij een verwerking op een van deze grondslagen. Zie meer algemeen hoofdstuk IX voor de mogelijkheid om specifieke wetgeving in te voeren bij bepaalde categorieën verwerkingen.

6.3 De rechtsgrond voor de in lid 1, punten c) en e), bedoelde verwerking moet worden vastgesteld bij:

6.3(a) Unierecht; of

6.3(b) lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.

Een verwerking die zijn grondslag vindt in een wettelijke plicht (lid 1 punt c) of een algemeen belang (lid 1 punt e) moet te herleiden zijn tot een specifieke wettelijke regeling in het Unierecht of nationaal recht.

Geen wet in formele zin. Een wet in formele zin hoeft deze regeling niet te zijn, wel moet de regeling voldoen aan de algemene eisen van duidelijkheid en nauwkeurigheid (overweging 41) zoals door het Hof van Justitie en het Europese Hof voor de Rechten van de Mens geformuleerd (bijvoorbeeld EHRM 26 april 1979, NJ 1980/146, Sunday Times). In HvJ EU 8 april 2014, gevoegde zaken C-293/12 en C-594/12 (Dataretentie) werd bepaald dat de bewaarplicht van telecommunicatiegegevens uit Richtlijn 2002/58 niet voldoet aan deze eis.

Geen verwerkingsspecifieke wetgeving. De AVG schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is (overweging 47). Er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen.

Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de in lid 1, punt e), bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend.

De wettelijke regeling moet in ieder geval bepalen wat het doel is van de verwerking. Uit overweging 45 volgt dat de verwerking ook noodzakelijk moet zijn voor het doel.

Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX.

Een dergelijke wettelijke regeling mag afwijken van de AVG, onder meer door de algemene beginselen (artikel 5) anders uit te werken en de regels rond de persoonsgegevens, betrokkenen, ontvangers, doel(en), bewaarperiode en procedures op eigen manier in te vullen. Wel moet deze regeling te allen tijde voldoen aan de algemene beginselen van een rechtmatige en behoorlijke verwerking (artikel 5 lid 1 punt a), net zoals de wettelijke regelingen die onder hoofdstuk IX mogen worden ingevoerd.

Het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.

De wettelijke regeling moet als laatste passen binnen een doel van algemeen belang, en mag niet verder gaan dan nodig (proportionaliteitseis) om dat doel te realiseren.

- 6.4 Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld niet berust op toestemming van de betrokkene of op een Unierechtelijke bepaling of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen houdt de verwerkingsverantwoordelijke bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld onder meer rekening met:

Een verdere verwerking, oftewel een verwerking voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, moet apart gerechtvaardigd worden (artikel 5 lid 1 punt b, het beginsel van doelbinding). Wanneer een dergelijke verwerking niet gerechtvaardigd wordt door de grondslag toestemming (lid 1 punt a) of een wettelijke plicht (lid 1 punt c) op grond van een van de uitzonderingen uit artikel 23, moet de verwerkingsverantwoordelijke een extra afweging maken of dit andere doel wel verenigbaar is. Hierbij gelden de volgende factoren:

- 6.4(a) ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenenomene verdere verwerking;

De eerste factor is het verband tussen het oorspronkelijke en de andere doelen. Hoe nauwer deze doelen aan elkaar verwant zijn, hoe eerder zij als verenigbaar worden aangemerkt.

- 6.4(b) het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;

Het kader van verzamelen van de persoonsgegevens is ook een belangrijke factor. Bij persoonsgegevens die direct bij de betrokkene zijn verzameld, zal in het algemeen eerder verenigbaarheid worden aangenomen dan bij persoonsgegevens die langs andere weg zijn verkregen. Ook de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan speelt hier een rol.

- 6.4(c) de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig artikel 9, en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig artikel 10;

De aard van de persoonsgegevens speelt ook een rol, met name als sprake is van bijzondere persoonsgegevens (artikel 9) of strafrechtelijke persoonsgegevens (artikel 10). Bij dergelijke persoonsgegevens komt de lat van verenigbaarheid zéér hoog te liggen.

6.4(d) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;

Een vierde factor is welke gevolgen de verdere verwerking kan hebben voor betrokkenen. Hoe kleiner deze gevolgen, hoe eerder de verwerking als verenigbaar kan worden gezien.

6.4(e) het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

Voor verenigbaarheid is verder vereist dat passende waarborgen worden genomen. Deze kunnen omvatten het versleutelen van de persoonsgegevens of het pseudonimiseren (artikel 4 definitie 5) daarvan om zo de risico's van oneigenlijk gebruik te beperken.

Artikel 7. Voorwaarden voor toestemming

7.1 Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

In veel gevallen zal worden gewerkt met toestemming als grondslag (artikel 6 lid 1 punt a). In dat geval berust de bewijslast voor de vraag of toestemming is verkregen bij de verwerkingsverantwoordelijke (zie meer algemeen artikel 5 lid 2). De betrokkene moet vóór het geven van de toestemming erop worden gewezen dat hij deze op ieder moment mag intrekken (lid 3). Zie over het begrip toestemming de *Richt snoeren inzake toestemming overeenkomstig Verordening 2016/679* van het Comité, 28 november 2017 en het *Advies 15/2011 over de definitie van het begrip 'toestemming'* (WP 187) van de Artikel 29-Werkgroep, 13 juli 2011.

Bewijs. Het bewijs dat toestemming is verkregen, is vormvrij. Bekende manieren om toestemming te bewijzen zijn een ondertekende schriftelijke verklaring, een online vinkje dat moet worden aangevinkt om door te gaan of een opgenomen mondelinge verklaring. In de praktijk wordt vaak gewerkt met generiek bewijs, zoals bij het online vinkje: men bewijst dan dat het systeem op de betreffende dag zo werkte dat toestemming geven vereist was om door te gaan, waaruit dan volgt dat deze betrokkene ook wel toestemming zal hebben gegeven.

Bewijs bij e-mail. Specifiek bij e-mailnieuwsbrieven en -reclame wordt vaak gewerkt met 'double opt-in' en 'confirmed opt-in'. Bij een confirmed opt-in ontvangt de betrokkene een bevestiging van de inschrijving in zijn mailbox zodat hij deze ongedaan kan maken; bij een double opt-in ontvangt hij een bericht met het verzoek de inschrijving nogmaals te bevestigen. De double-opt in levert in de praktijk adequaat bewijs op van de wens tot ontvangen van de betreffende e-mails.

- 7.2 Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.

Om te voorkomen dat een toestemmingsvraag wordt ‘verstopt’ in een grotere tekst, dient die vraag apart te worden gesteld. De vraag moet in een begrijpelijke en gemakkelijk toegankelijke vorm worden gesteld en moet duidelijk en eenvoudige taal gebruiken.

Begrijpelijk en gemakkelijk toegankelijke vorm. De vraag moet zo worden gesteld dat deze opgevat zal worden als toestemmingsvraag, en de vraag moet in eenvoudig toegankelijke vorm zijn. Bij voorkeur wordt toestemming dus altijd in de vragende vorm geformuleerd (“Wilt u onze nieuwsbrief ontvangen?”), of als expliciete toestemmingsfrase die geaccordeerd moet worden (“Ik geef het assessmentbureau toestemming mijn toetsresultaten aan mijn werkgever te verstrekken [ja/nee]”).

Duidelijk en eenvoudig. De toestemmingsvraag moet in duidelijke en eenvoudige taal worden geformuleerd. Wat duidelijk en eenvoudig is, zal afhangen van de categorie(ën) van betrokkenen, maar hoger dan taalniveau B2 van het Europees Referentiekader Talen lijkt in het algemeen ongepast. “Ik wil de wekelijkse nieuwsbrief van ICTRecht BV ontvangen” is een adequate toestemmingsvraag; “Ik verstrek hierbij ICTRecht BV toestemming voor verwerking van mijn persoonsgegevens teneinde wekelijks commerciële communicatie te ontvangen” is dat niet.

Granulaire toestemming. De AVG is niet expliciet over het al dan niet mogen combineren van onderwerpen waarvoor toestemming wordt gevraagd. Uit het *Advies 15/2011 over de definitie van het begrip ‘toestemming’* valt te halen dat dit in strijd zou zijn met de AVG. Naar onze mening gaat dat te ver; zolang de individuele onderwerpen duidelijk en specifiek zijn omschreven en de toestemming voor het geheel niet wordt afgedwongen, lijkt ons de gecombineerde toestemmingsvraag verdedigbaar.

Onerlijke bedingen. Overweging 42 verwijst naar Richtlijn 93/13/EEG betreffende oneerlijke bedingen. Artikel 5 van deze Richtlijn vereist dat bedingen in consumentenovereenkomsten “duidelijk en begrijpelijk” zijn opgesteld, en voegt daaraan toe dat in geval van twijfel over de betekenis van een beding, de voor de consument gunstigste interpretatie prevaleert. Een toestemmingsverklaring mag geen oneerlijke bedingen bevatten.

Duidelijk onderscheid. De toestemmingsvraag moet zodanig worden gepresenteerd dat een duidelijk onderscheid wordt gemaakt met andere zaken. Een voorbeeld is een apart aanvinkvakje in een formulier, waarbij vakje en tekst visueel gescheiden zijn van de overige informatie op het formulier. Bij een internetdienst kan een *pop-up* (floepvenster) met enkel en uitsluitend de toestemmingsvraag (en uiteraard een ja/nee knop en verwijzing naar de privacyverklaring) voldoende zijn.

Niet bindend. Een toestemmingsvraag die niet voldoet aan de eisen van dit lid 2, levert geen rechtsgeldige grondslag toestemming op. Als meerdere toestemmingsvragen worden gesteld, geldt dit gebrek alleen voor die vragen die niet voldoen.

Identiteit en doeleinden. Bij het vragen van toestemming moeten de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking expliciet worden genoemd. Enkel verwijzen naar een privacyverklaring (artikel 12, 13 en 14) is dus niet genoeg.

- 7.3 De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven ervan.

Eenmaal gegeven toestemming kan te allen tijde worden ingetrokken. Dit heeft geen terugwerkende kracht; eerder onder de toestemming verrichte verwerkingen blijven rechtmatig. De verwerking zal nu wel moeten worden gestaakt, tenzij de verwerking tevens onder een andere grondslag kan worden gerechtvaardigd.

Voortgezette verwerking. Als toestemming is ingetrokken, moet de verwerking worden gestaakt tenzij er nog een andere grondslag is die voortgezette verwerking rechtvaardigt. De lat ligt hierbij hoog. De Artikel 29-Werkgroep noemt het zelfs misleidend om de grondslag toestemming te hanteren als na intrekking daarvan een andere grondslag even goed kan worden gebruikt (*Advies 15/2011 over de definitie van het begrip 'toestemming'*, 13 juli 2011, WP 187, p. 15). Een specifieke wettelijke plicht (artikel 6 lid 1 punt c) zou ons inziens de enige reële optie zijn. Het eigen belang (artikel 6 lid 1 punt f) zou slechts in zéér uitzonderlijke situaties een grondslag kunnen bieden voor verwerking na ingetrokken toestemming. De betrokkene moet uiteraard altijd worden geïnformeerd over de voortgezette verwerking en de daarbij behorende alternatieve grondslag.

Reeds verrichte verwerkingen. Intrekking kan de rechtmatigheid van reeds verrichte verwerkingen (natuurlijk) niet aantasten.

Informatieplicht. De betrokkene moet vóór het geven van de toestemming erop worden gewezen dat hij deze op ieder moment mag intrekken. De AVG bepaalt niet hoe dit moet gebeuren. Een vermelding in de privacyverklaring (artikel 13 en 14) lijkt ons adequaat. Verstandig kan zijn de dienst anders te presenteren: in plaats van een verplichting zich op de nieuwsbrief te abonneren om een gratis rapport te ontvangen krijgt men een rapport gratis bij een abonnement op de nieuwsbrief.

Even eenvoudig. Het intrekken van toestemming moet net zo eenvoudig kunnen als het geven daarvan. Het is dus bijvoorbeeld niet toegestaan om toestemming voor vermelding op een socialemediadienst alleen per aangetekende brief te kunnen intrekken als men de vermelding online kon aangaan. Vergelijk art. 6:236 punt o BW dat eenzelfde eis stelt bij het opzeggen van duurovereenkomsten. De Franse privacywaakhond (CNIL) heeft in 2022 boetes uitgedeeld aan Facebook (60 miljoen), Google (150 miljoen) en Youtube omdat de cookies van deze partijen niet zo gemakkelijk te weigeren zijn als dat ze te accepteren zijn.

Dwingend recht. Het is niet mogelijk het recht van intrekking op te geven of daar afstand van te doen. Een verklaring dat men een gegeven toestemming nimmer zal intrekken, is dus niet rechtsgeldig. Bij een verwerking voor journalistieke, academische, artistieke of literaire uitingen is dit artikel in Nederland buiten toepassing verklaard (artikel 43 lid 2 punt a Uitvoeringswet). Toestemming voor een interview of foto (de zogeheten *quitclaim* of *model release*) is dus niet intrekbaar. Bij wetenschappelijk of statistisch onderzoek blijft het recht van intrekking onverkort van kracht.

Misbruik van recht. In zeer uitzonderlijke gevallen zou een intrekking als misbruik van recht (art. 3:13 BW) kunnen worden geconstrueerd, maar gezien verwerking van persoonsgegevens aan een grondrecht raakt, en betrokkenen zonder reden moeten kunnen beschikken over hun grondrechten, ligt dit niet voor de hand.

- 7.4 Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

Toestemming moet vrij oftewel vrijwillig worden gegeven. Hiervan is geen sprake indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen. Een voorbeeld is 'toestemming' vragen aan een werknemer: gezien de gezagsverhouding zal deze zelden echt vrijelijk kunnen weigeren. Dergelijke toestemmingsverklaringen zijn dus niet rechtsgeldig (zie nader *Advies 8/2001 over de verwerking van persoonsgegevens in het kader van de arbeidsverhouding* (WP 48, 13 september 2001) van de Artikel 29-Werkgroep.).

Toestemming vereist bij overeenkomst. Bij veel overeenkomsten, met name informatiediensten, wordt toestemming gevraagd voor gebruik van allerlei persoonsgegevens. Wie deze toestemming niet verleent, krijgt dan geen toegang tot de dienst. De rechtvaardiging is dat de persoonsgegevens dan gebruikt kunnen worden voor gerichte advertenties, welke zorgen voor inkomsten om de (vaak gratis) informatiediensten te kunnen bekostigen. Een dergelijke afgedwongen toestemming is niet per se ongeldig maar moet onder dit lid 4 zeer kritisch worden bekeken.

Artikel 8. Voorwaarden voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij

8.1 Wanneer artikel 6, lid 1, punt a), van toepassing is in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, is de verwerking van persoonsgegevens van een kind rechtmatig wanneer het kind ten minste 16 jaar is. Wanneer het kind jonger is dan 16 jaar is zulke verwerking slechts rechtmatig indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt.

Wanneer een internetdienst zoals een online spel of een sociaal netwerk een dienst levert aan een kind onder de 16 jaar en daarbij persoonsgegevens verzamelt onder de grondslag toestemming (artikel 6 lid 1 onder a), is toestemming van de wettelijke vertegenwoordiger van die personen nodig. Vanaf 16 jaar kunnen deze personen zelf de benodigde toestemming geven.

De informatieplichten (artikel 12 lid 1) richting kinderen vereisen in alle gevallen extra aandacht. Deze moeten dan worden opgesteld in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in voor kinderen duidelijke en eenvoudige taal. Ook de toestemmingsvraag (artikel 7 lid 2) moet aan deze eis voldoen.

Toestemming. De regeling van dit artikel geldt alleen bij een verwerking met als grondslag toestemming (artikel 6 lid 1 punt a). Een dienst die wordt geleverd onder een andere grondslag, zoals het nakomen van een overeenkomst (artikel 6 lid 1 punt b) of een eigen gerechtvaardigd belang (punt f), vereist dus geen ouderlijke toestemming.

Dienst van de informatiemaatschappij. Een dienst van de informatiemaatschappij is kort gezegd iedere internetdienst of mobiele telefoniedienst (zie artikel 4 definitie 25). Ouderlijke toestemming is dus onder de AVG niet nodig voor verwerking van kinderpersoonsgegevens bij andere vormen van verwerking met als grondslag toestemming. Denk aan een speelhal die middels Bluetooth-sensoren monitort welke spellen kinderen het interessantst vinden, of een aan kinderen gerichte enquête voor marketingdoeleinden in een tijdschrift. Naar de

letter van de AVG kan het kind daar zelf toestemming voor geven, binnen de grenzen van artikel 1:234 BW. De Uitvoeringswet bepaalt echter (art. 5 lid 1) dat te allen tijde bij personen onder de zestien deze toestemming van de ouders of verzorgers afkomstig moet zijn.

Preventieve diensten en adviesdiensten. Wanneer de dienst kan worden gezien als een preventieve- of adviesdienst is de ouderlijke toestemming niet vereist (overweging 38). Hierbij kan bijvoorbeeld worden gedacht aan een chatdienst om slachtoffers van pesten te helpen. Dergelijke diensten zouden geen commercieel oogmerk of marketingdoel moeten hebben. Een ‘adviesdienst’ over hoe een betaald spel moet worden gespeeld, valt natuurlijk onder de hoofdregel en vereist ouderlijke toestemming. De Uitvoeringswet (artikel 5 lid 5) spreekt overigens van “hulp- en adviesdiensten”.

Rechtstreeks aanbod. De diensten moeten rechtstreeks aan de kinderen aangeboden worden. Wanneer het gaat om diensten voor het algemene publiek waar toevallig kinderen afnemers zijn, zoals een nieuwswebsite, geldt dit artikel dus niet.

Marketingdoeleinden. De reden voor deze specifieke bepaling is (overweging 38) met name een zorg dat kindergegevens worden gebruikt voor marketingdoeleinden of voor het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. De strekking is echter breder dan enkel marketing- of profileringsdoeleinden.

De lidstaten kunnen dienaangaande bij wet voorzien in een lagere leeftijd, op voorwaarde dat die leeftijd niet onder 13 jaar ligt.

Bij totstandkoming van de AVG kon geen overeenstemming worden bereikt over welke leeftijd hier als ondergrens zou moeten gelden. Sommige lidstaten wilden 13, anderen 16 en weer anderen daar tussen. De AVG laat het dan ook aan de lidstaten om hier zelf een besluit over te nemen. Nederland heeft in de Uitvoeringswet geen nadere leeftijd gekozen, zodat in Nederland 16 jaar de grens is en blijft (MvT Uitvoeringswet, p. 59).

- 8.2 Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.

Een praktisch probleem bij een internetdienst is dat het lastig is na te gaan of de volgens lid 1 vereiste ouderlijke toestemming wel verleend is. De AVG introduceert hier nu een inspanningsverplichting voor de verwerkingsverantwoordelijke om dit na te gaan.

Redelijke inspanningen. De AVG vermeldt geen manieren waarmee de verwerkingsverantwoordelijke de bedoelde controle moet uitvoeren. De al langer bestaande Amerikaanse COPPA-wetgeving (15 U.S.C. §§ 6501-6506) over dit zelfde onderwerp vereist *verifiable parental consent* voordat men persoonlijke informatie van personen onder de dertien jaar verwerkt. De uitvoeringsregels (16 C.F.R. § 312.5(c)) noemen diverse opties: een getekend formulier, een geldige creditcard, een telefonisch contact met iemand die getraind is kinderstemmen te herkennen en, bij verwerkingen zonder derdenverstrekking, of een reactie per mail van de ouder dat een en ander akkoord is.

- 8.3 Lid 1 laat het algemene overeenkomstenrecht van de lidstaten, zoals de regels inzake de geldigheid, de totstandkoming of de gevolgen van overeenkomsten ten opzichte van kinderen, onverlet.

In Nederland is een persoon onder de 18 handelingsonbekwaam om rechtshandelingen te verrichten zoals het sluiten van overeenkomsten (art. 1:234 BW), behalve met toestemming van zijn wettelijke vertegenwoordiger of bij overeenkomsten die in het maatschappelijk verkeer gebruikelijk zijn voor kinderen van die leeftijd. De AVG verandert hier niets aan. Het is dus mogelijk dat een persoon van 16 rechtsgeldig toestemming geeft voor verwerking van zijn persoonsgegevens onder de AVG maar geen rechtsgeldige aanvaarding van de bijbehorende dienstverleningsovereenkomst kan verrichten. Evenzo is het mogelijk dat een persoon van 12 een overeenkomst tot dienstverlening sluit bij een dienst die in het maatschappelijk verkeer gebruikelijk is voor twaalfjarigen (bijvoorbeeld deelname aan een gratis discussieforum over stripfiguren), maar daarbij geen toestemming heeft van zijn ouders tot de bijbehorende verwerking van persoonsgegevens.

Artikel 9. Verwerking van bijzondere persoonsgegevens

- 9.1 Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Persoonsgegevens die door hun aard bijzonder gevoelig zijn, verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de betrokkene. Voor deze bijzondere persoonsgegevens geldt een strenger regime: verwerking is verboden tenzij de AVG een uitzondering maakt, en dan alleen binnen de grenzen van die uitzondering.

Waaruit blijken. Een persoonsgegeven is niet alleen bijzonder wanneer het direct het betreffende bijzondere onderwerp onthult, zoals "Hafsa is lid van vakbond FNV Bondgenoten". Ook gegevens die indirect dergelijke informatie

bevatten, worden aangemerkt als bijzondere persoonsgegevens. Het woonadres van deze Hafsa zoals opgenomen in de administratie van deze vakbond onthult immers ook zijn lidmaatschap.

Ras of etnische afkomst. Dit begrip moet ruim worden opgevat en omvat ook huidskleur, afkomst en nationale of etnische afstamming. Ten overvloede merkt overweging 51 op dat de term ‘ras’ niet mag worden opgevat als zou de Europese Unie onderscheid maken in menselijke rassen. Foto’s werden onder de Richtlijn gezien als een bijzonder persoonsgegeven inzake ras (HR 23 maart 2010, ECLI:NL:HR:2010:BK6331), maar de AVG kwalificeert ze nu als biometrische gegevens (zie artikel 4, definitie 14) en ze zijn alleen bijzondere persoonsgegevens als verwerking gebeurt met het oog op identificatie (zie hieronder).

Politieke opvattingen. Onder politieke opvattingen worden verstaan alle opvattingen over hoe de maatschappij of samenleving moet worden ingericht of bestuurd. Naast de klassieke politieke stromingen zoals liberalisme en socialisme vallen ook meer randverschijnselen als het anarchisme hieronder.

Religieuze of levensbeschouwelijke overtuigingen. Het is lastig een definitie te geven van religie, maar als algemene lijn geldt dat sprake moet zijn van zingeving waarbij een of meer hogere machten betrokken zijn. Wanneer geen hogere macht wordt erkend, wordt eerder gesproken van levensbeschouwing (zoals bij het humanisme). Erkenning van een organisatie die deze zingeving predikt, is geen vereiste. Zie meer algemeen artikel 10 Handvest grondrechten EU en artikel 9 EVRM.

Lidmaatschap vakbond. Een vakbond of vakvereniging is een vereniging (soms een stichting) die de individuele en collectieve belangen behartigt van aangesloten werknemers. Een personeelsvereniging kan hieronder vallen wanneer zij (mede) bij de werkgever opkomt voor werknemersbelangen. Een personeelsvereniging die zich alleen inzet om de saamhorigheid binnen het bedrijf te bevorderen, bijvoorbeeld door uitjes en activiteiten te organiseren, is geen vakbond.

Genetische gegevens. Genetische gegevens betreffen overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid (zie artikel 4, definitie 13). Genetische gegevens worden met name verkregen uit DNA- en RNA-onderzoek.

Biometrische gegevens. Biometrische gegevens komen voort uit een specifieke verwerking van fysieke, fysiologische of gedragsgerelateerde kenmerken die eenduidige identificatie mogelijk maken, zoals portretten of vingerafdrukken (zie artikel 4, definitie 14). Deze gegevens zijn uitsluitend bijzondere persoonsgegevens als ze worden verwerkt met het oog op identificatie. Een straatfoto met daarop herkenbaar iemands gezicht is dus geen bijzonder persoonsgegeven. Een pasfoto op een identiteitskaart is dat wel. Bij een opname van een beveiligingscamera hangt het van het doel van de opname af.

Gegevens over gezondheid. Gezondheidsgegevens (zie artikel 4, definitie 15) betreffen alle persoonsgegevens over de fysieke of mentale gezondheid van een persoon (zowel in het heden, verleden als toekomst), waaronder gegevens over verleende gezondheidsdiensten. In een rechtszaak in 2022 in Rotterdam werden bewijzen omtrent doktersafspraken, tandartsafspraken, ziekenhuisbezoeken en thuisbezorgd gekwalificeerd als bijzondere persoonsgegevens. De Gemeente Rotterdam vorderde deze documenten bij een onderzoek of de betreffende persoon nog daadwerkelijk op het adres woonde zoals aangegeven bij de gemeente. De rechtbank oordeelde dat dit bijzondere persoonsgegevens zijn omdat ze een indicatie kunnen geven over iemands gezondheid (Rb. Rotterdam 25 juli 2022, ECLI:NL:RBROT:2022:7256).

Gegevens over seksueel gedrag of seksuele gerichtheid. Dit betreft gegevens aangaande amoureuze betrekkingen of erotische verlangens van een persoon. De term ‘gerichtheid’ is daarbij ruimer dan voorkeur of geaardheid (zie ook artikel 21 Handvest grondrechten EU), zodat ook kwesties als transgenderisme en genderdysforie hieronder kunnen worden geschaard. In 2022 oordeelt het Hof van Justitie van de Europese Unie dat in sommige gevallen, de naam van een partner gezien kan worden als een bijzonder persoonsgegeven. In dit geval ging het om de overheid waarbij het voor een bepaalde registratie verplicht was de naam van je partner te registreren. Omdat - in dit geval - van de voornaam de gender van de persoon af te leiden was, was de naam van de partner in dit geval een gegeven dat een indicatie gaf over de seksuele gerichtheid van de betrokkene (HvJ EU 1 augustus 2022, ECLI:EU:C:2022:601).

Strafrechtelijke persoonsgegevens. In tegenstelling tot de Richtlijn schaaft de AVG gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten niet onder het kopje bijzondere persoonsgegevens. Hierop is een apart, strenger, regime van toepassing dat is neergelegd in artikel 10.

Burgerservicenummer. Het burgerservicenummer (BSN) is onder de AVG in beginsel geen bijzonder persoonsgegeven, maar kent zijn eigen regime onder artikel 87 AVG en in de nationale wetten van lidstaten. Zie nader artikel 87 en meer specifiek artikel 46 Uitvoeringswet.

-
- 9.2 Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan:

Het verwerken van bijzondere persoonsgegevens is alleen mogelijk in een van de situaties genoemd in dit lid 2 of lid 3. Daarnaast biedt artikel 23 de mogelijkheid voor lidstaten om afwijkende regels te stellen die ook gelden voor bijzondere persoonsgegevens als dat noodzakelijk is voor bijvoorbeeld de nationale veiligheid, bestrijding van strafbare feiten of volksgezondheid. Deze uitzonderingen zijn in Nederland ook van toepassing op strafrechtelijke persoonsgegevens (artikel 32 Uitvoeringswet).

Directe werking. De uitzonderingen uit leden a, c, d, e en f hebben directe werking. De uitzonderingen uit b, g, h, i en j hebben dit niet, maar bieden een basis voor nadere uitwerking in nationale wetgeving.

Geen grondslag. Formeel biedt dit lid 2 geen grondslagen voor verwerking. Wanneer een situatie uit dit lid 2 opgaat, geldt het verbod uit lid 1 niet. Er moet nog steeds een grondslag worden gevonden onder artikel 6, zij het dat in de praktijk de uitzonderingen vrijwel altijd samen zullen vallen met een grond onder artikel 6.

9.2(a) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven;

De eerste uitzondering op het verbod om bijzondere persoonsgegevens te verwerken is de uitdrukkelijke toestemming van de betrokkene.

Uitdrukkelijke toestemming. Bij het geven van toestemming (artikel 4 definitie 11) is het mogelijk toestemming af te leiden uit een handeling, zolang maar duidelijk blijkt dat de betrokkene instemt met de voorgestelde verwerking. Uitdrukkelijke toestemming vereist meer: er moet sprake zijn van een expliciete wilsuiting gericht op het geven van toestemming. Zie over grenzen aan toestemming artikel 7.

Niet op te heffen. Het Europees recht of een nationale regeling kan bepalen dat een betrokkene geen toestemming kan geven voor verwerking van een bijzonder persoonsgegeven. Een land zou bijvoorbeeld ter handhaving van het stemgeheim kunnen bepalen dat het publiceren van *stemfies* (zelfportretten met ingevuld stembiljet) in het stembokje niet toegestaan is, omdat dit het bijzonder persoonsgegeven van politieke voorkeur onthult.

Grondslag. Uitdrukkelijke toestemming levert tevens de grondslag toestemming op (artikel 6 lid 1 punt a).

9.2(b) de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijk recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt;

Bijzondere persoonsgegevens mogen worden verwerkt als dat nodig is om wettelijke plichten of rechten te dienen binnen het arbeidsrecht of socialezekerheids- en socialebeschermingsrecht. Dit dient in een wettelijke regeling of een

cao te zijn vastgelegd en daarbij dienen waarborgen te zijn getroffen ter bescherming van de betrokkene. In Nederland is dit gebeurd in artikel 30 Uitvoeringswet voor gegevens over gezondheid. Deze mogen worden verwerkt door bestuursorganen, pensioenfondsen en werkgevers indien noodzakelijk voor een wettelijke taak of re-integratie van de werknemer.

Nadere regels. Artikel 88 biedt lidstaten de mogelijkheid nadere regels te stellen over persoonsgegevens van werknemers in het kader van de arbeidsverhouding, zoals over werving en selectie maar ook gelijkheid en diversiteit op het werk. Deze regels mogen ook bijzondere persoonsgegevens betreffen, mits dit noodzakelijk is voor de betreffende regels en er passende waarborgen zijn genomen ter bescherming van de privacy en andere fundamentele rechten en belangen van de werknemers.

Grondslag. Deze uitzondering levert tevens de grondslag op van de wettelijke plicht (artikel 6 lid 1 punt c).

9.2(c) de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;

Een verwerking van bijzondere persoonsgegevens is ook toegestaan als deze noodzakelijk is voor een vitaal belang (levensbelang). De betrokkene moet dan niet in staat zijn om toestemming te geven.

Vitaal belang. Van een vitaal belang is sprake als het belang voor het leven van de betrokkene of dat van een andere natuurlijke persoon essentieel is. Verwerking van persoonsgegevens op grond van het vitale belang voor een andere natuurlijke persoon is in beginsel alleen toegestaan indien de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd (overweging 46). Een voorbeeld is toegang tot een medisch dossier geven in een spoedgeval bij een bewusteloos persoon.

Niet in staat tot toestemming. Een beroep op een vitaal belang als grondslag is alleen mogelijk als de betrokkene niet in staat is toestemming te geven. Dit kan zowel fysiek (de persoon is bijvoorbeeld bewusteloos) als juridisch (de persoon is bijvoorbeeld handelingsonbekwaam). Zie meer algemeen over toestemming bij medische behandelingen artikel 7:450 BW.

Grondslag. Deze noodzaak levert tevens de grondslag vitaal belang op (artikel 6 lid 1 punt d).

9.2(d) de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;

Het verbod geldt om evidente redenen niet voor politieke, religieuze en levensbeschouwelijke organisaties en voor vakbonden wanneer een en ander noodzakelijk is voor beheer van personalia van leden, begunstigers en dergelijke. In Nederland is dit uitgewerkt in artikel 22 lid 2 punt c Uitvoeringswet voor wat betreft de gerechtvaardigde activiteiten van deze organisaties.

Instantie zonder winstoogmerk. Het verbod vervalt alleen als de verwerkende instantie opereert zonder winstoogmerk. Een politieke partij, kerk, humanistische instelling of vakbond voldoet hier in de regel aan.

Gerechtvaardigde activiteiten. De verwerkingen moeten gerechtvaardigd zijn binnen de instantie. De ledenadministratie zal in het algemeen gerechtvaardigd zijn, maar bijvoorbeeld het publiceren van foto's van leden op de website is lastiger te rechtvaardigen. In Nederland is bepaald (artikel 27 Uitvoeringswet) dat het een instelling is toegestaan om religieuze en levensbeschouwelijke gegevens te verwerken, wanneer dit noodzakelijk is voor de geestelijke verzorging van de betrokkene. Deze uitzonderingsgrond vervalt wanneer de betrokkene schriftelijk bezwaar tegen deze gegevensverwerking heeft gemaakt. Tevens geldt het verbod om politieke persoonsgegevens te verwerken niet (artikel 26 Uitvoeringswet) indien de verwerking noodzakelijk is in verband met eisen die in redelijkheid aan de vervulling van functies in bestuursorganen en adviescolleges kunnen worden gesteld.

Werkzaam op gebied. De instantie moet actief zijn op het gebied waarvoor zij de bijzondere persoonsgegevens wil verwerken. Daarvan is sprake als zij op een of andere manier de uitoefening van de fundamentele vrijheden mogelijk maakt (overweging 51). Een politieke partij mag dus persoonsgegevens over politieke voorkeur verwerken, hoewel niet ook bijvoorbeeld seksuele gerichtheid van haar leden. Een meer algemene non-profit organisatie (zoals de Consumentenbond of stichting Natuurmonumenten) kan zich niet op deze uitzonderingsgrond beroepen.

Betrekking op leden. De verwerking moet beperkt zijn tot zaken aangaande (huidige of voormalige) leden of begunstigers en andere personen die regelmatig contact hebben met de instantie (zoals regelmatige bezoekers van levensbeschouwelijke bijeenkomsten).

Derdenverstrekking. De betreffende bijzondere persoonsgegevens mogen alleen met aparte toestemming aan derden worden verstrekt. De instantie kan zich dus niet beroepen op andere grondslagen, zoals uitvoering van een overeenkomst of een eigen gerechtvaardigd belang (artikel 6 lid 1 punten b en f).

Passende waarborgen. Kerkgenootschappen en religieuze verenigingen die bij inwerkingtreden van de AVG reeds uitgebreide regelingen hadden omtrent de omgang met persoonsgegevens, mogen deze in stand houden (artikel 91).

Grondslag. Deze noodzaak levert in beginsel de grondslag uitvoering (lidmaatschaps- of begunstigers-)overeenkomst op (artikel 6 lid 1 punt b). In concrete gevallen kan aanvullende toestemming (artikel 6 lid 1 punt a) of een eigen noodzaak (artikel 6 lid 1 punt f) nodig zijn.

9.2(e) de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;

Een andere uitzondering is wanneer de betrokkene de persoonsgegevens kennelijk (evident) zelf openbaar heeft gemaakt. Het moet dan gaan om een spontane handeling van de betrokkene waardoor het persoonsgegeven kenbaar wordt voor anderen.

Kennelijk. Het woord ‘kennelijk’ geeft aan dat de bewijslast hoog ligt. Er mag geen twijfel zijn dat de persoon zelf gehandeld heeft om het persoonsgegeven openbaar te maken. Een persoon die bijvoorbeeld zichzelf als homoseksueel aanduidt op een sociale netwerkdienst, maakt dit gegeven kennelijk openbaar. Bij een datingsite kan men daar vraagtekens bij stellen, omdat de openbaarheid van dergelijke sites beperkter is. In een zaak tussen Ziggo en Brein oordeelde de rechter dat 50 gebruikers die samen een peer2peer (onrechtmatige) bestandsdeling uitvoerden, waarbij elke peer elkaars IP-adres in die bubbel kan zien, niet gezien kan worden als kennelijk openbaar gemaakte informatie (Gerechtshof Arnhem-Leeuwarden 11 oktober 2022, ECLI:NL:GHARL:2022:8676).

Gevolg beoogd. Deze handeling moet ook dit gevolg beoogd hebben. Een persoon die bijvoorbeeld als bestuurslid van een vakbond zich laat interviewen op televisie, heeft beoogd dat anderen te weten komen dat hij lid is van die vakbond. Het enkele feit dat een persoonsgegeven te constateren is aan een persoon (zoals een zichtbare medische aandoening of een etnisch kenmerk), maakt nog niet dat sprake is van openbaar gemaakte persoonsgegevens.

Grondslag. Het feit dat persoonsgegevens kennelijk openbaar gemaakt zijn, levert geen grondslag voor de verwerking op. In het kader van journalistiek zal de eigen noodzaak (artikel 6 lid 1 punt f) de grondslag vormen.

9.2(f) de verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer de gerechten handelen in het kader van hun rechtsprekende taken;

De verwerking van bijzondere persoonsgegevens is daarnaast toegestaan indien dat noodzakelijk is in het kader van gerechtelijke procedures, bijvoorbeeld omdat een bewijsstuk moet worden overlegd waarin relevante doch bijzondere persoonsgegevens zijn opgenomen.

Grondslag. De noodzaak uit deze uitzondering levert geen grondslag voor verwerking op. Een beroep op de grondslag eigen noodzaak (artikel 6 lid 1 punt f) ligt echter voor de hand.

9.2(g) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene;

Een verwerking van bijzondere persoonsgegevens is verder niet verboden als dat noodzakelijk is voor een zwaarwegend algemeen belang dat bij wet is vastgelegd.

Algemeen belang. De AVG kent geen eenduidige definitie van een algemeen belang. Overweging 55 noemt als voorbeeld de verwerking van persoonsgegevens door overheidsinstanties ter verwezenlijking van in het constitutionele recht of in het volkenrecht vastgelegde doelstellingen van officieel erkende religieuze verenigingen. Overweging 56 noemt nog de verzameling door politieke partijen van persoonsgegevens over de politieke opvattingen van personen. In ieder geval moeten passende waarborgen worden vastgesteld voor de verwerking.

Nederland. In Nederland wordt een volkenrechtelijke verplichting aangemerkt als een algemeen belang (artikel 23 punt a Uitvoeringswet). Verwerking van persoonsgegevens omtrent ras of etnische afkomst is toegestaan indien dat onvermijdelijk is ter identificatie dan wel indien de verwerking dient om nadelen die verband houden met het ras of de etnische afkomst op te heffen (artikel 25 punt a Uitvoeringswet). Verder is het de AP of ombudsman toegestaan (artikel 23 punt b Uitvoeringswet) om bij zwaarwegende belangen bijzondere persoonsgegevens te verwerken.

Grondslag. Deze noodzaak levert tevens de grondslag algemeen belang op (artikel 6 lid 1 punt e).

- 9.2(h) de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;

Het verbod op verwerking van bijzondere persoonsgegevens vervalt wanneer dit noodzakelijk is voor medische redenen, met name in verband met de arbeid. Voorbeelden zijn het beoordelen van de arbeidsgeschiktheid van de werknemer en het stellen van medische diagnoses. Wel moeten de medische handelingen uitgewerkt zijn in een wettelijke regeling of voortvloeien uit een medische behandelovereenkomst. Tevens dient het medisch beroepsgeheim van toepassing te zijn op de verwerking (lid 3). In Nederland kent artikel 30 lid 3 Uitvoeringswet een dergelijke regeling voor zorgaanbieders en gezondheidsverzekeraars.

Grondslag. Deze noodzaak zal in beginsel vallen onder de grondslag van de wettelijke plicht (artikel 6 lid 1 punt c) of uitvoering van een (behandel-)overeenkomst (artikel 6 lid 1 punt b). In andere gevallen zal uitdrukkelijke toestemming (artikel 9 lid 1 punt a) nodig zijn.

- 9.2(i) de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim; of

Een andere grond om bijzondere persoonsgegevens te mogen verwerken ondanks het verbod is indien dit nodig is in het algemeen belang op het gebied van de volksgezondheid. De verwerking moet beperkt blijven tot het medisch domein. Overweging 54 bepaalt specifiek dat een verwerking onder deze grond er niet toe mag leiden dat derden zoals werkgevers of verzekeringsmaatschappijen en banken de persoonsgegevens voor ander grondslagen verwerken. Nederland kent vooralsnog geen dergelijke wettelijke regeling.

Volksgezondheid. De volksgezondheid betreft alle elementen in verband met de gezondheid, namelijk gezondheidstoestand, inclusief morbiditeit en beperkingen, de determinanten die een effect hebben op die gezondheidstoestand, de behoeften aan gezondheidszorg, middelen ten behoeve van de gezondheidszorg, de verstrekking van en de universele toegang tot gezondheidszorg, alsmede de

uitgaven voor en de financiering van de gezondheidszorg, en de doodsoorzaken (artikel 3 punt c van Verordening 1338/2008).

Beroepsgeheim. De betreffende wettelijke regeling moet rekening houden met de rechten en vrijheden van de betrokkene, met name van het medisch beroepsgeheim. Zie hierover nader lid 3. In de Uitvoeringswet (artikel 30 lid 4) is bepaald dat er, ten behoeve van de volksgezondheid, enkel bijzondere persoonsgegevens mogen worden verwerkt door personen die uit hoofde van ambt, beroep, wettelijk voorschrift of overeenkomst tot geheimhouding zijn gebonden. Daarnaast zijn alle verwerkingsverantwoordelijken die nog niet aan geheimhouding waren gebonden, dit alsnog op basis van lid 2 van dit artikel van de Uitvoeringswet.

Grondslag. Deze noodzaak levert tevens de grondslag algemeen belang op (artikel 6 lid 1 punt e).

9.2(j) de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.

Als laatste grond kan verwerking van bijzondere persoonsgegevens toegestaan zijn als dat noodzakelijk is voor archivering in het openbaar belang of voor onderzoek of statistiek. Dit wordt nader uitgewerkt in artikel 89. Wel moeten passende waarborgen worden genomen om de basis van het grondrecht privacy en de belangen van de betrokkene te beschermen.

Nederland. In de Uitvoeringswet (artikel 24) is bepaald dat de verwerking van bijzondere persoonsgegevens in het kader van archivering in het openbaar belang of voor onderzoek of statistiek is toegestaan, indien de verwerking een algemeen belang dient en het vragen van uitdrukkelijke toestemming onmogelijk blijkt, of onevenredige inspanning zou vergen. Wel moeten dan voldoende waarborgen zijn ingesteld zodat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Grondslag. Deze noodzaak levert tevens de grondslag algemeen belang op (artikel 6 lid 1 punt e).

- 9.3 De in lid 1 bedoelde persoonsgegevens mogen worden verwerkt voor de in lid 2, punt h), genoemde doeleinden wanneer die gegevens worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden, of door een andere persoon die eveneens krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels tot geheimhouding is gehouden.

Beoefenaars van specifieke vrije beroepen, zoals advocaten, artsen of psychiaters, die een wettelijk vastgelegd beroepsgeheim hebben, mogen bijzondere persoonsgegevens verwerken als dat noodzakelijk is voor medische doeleinden zoals bedoeld in lid 2 punt h. Andere personen of instellingen mogen dit dus niet, behalve als een van de situaties uit lid 2 zich voordoet.

- 9.4 De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren.

Verschillende lidstaten van de EU hebben andere opvattingen over hoe om te gaan met de specifieke categorieën genetische, biometrische en gezondheidsgegevens. De AVG laat daarom ruimte over voor nadere nationale regelingen omtrent de verwerkingen daarvan.

Nederland, genetische gegevens. Het verwerken van genetische gegevens is op basis van de Uitvoeringswet (artikel 28) in beginsel enkel toegestaan wanneer de gegevens bij de betrokkene zijn verkregen. Uitzondering geldt wanneer een zwaarwegend geneeskundig belang prevaleert, of de verwerking noodzakelijk is voor wetenschappelijk onderzoek of statistiek waarbij de betrokkene hiervoor uitdrukkelijke toestemming heeft gegeven.

Nederland, biometrische gegevens. Het is toegestaan om biometrische gegevens te verwerken voor authenticatie- of beveiligingsdoeleinden (artikel 29 Uitvoeringswet). Wel moet de noodzaak van deze wijze van authenticeren of beveiligen zijn aangetoond; zijn werkelijk geen alternatieven zoals pincodes of pasjes mogelijk? Een onbekende organisatie gebruikte voor een lange tijd vingerafdrukken om werknemers te laten inklokken. De AP deelde hiervoor een boete uit. Het was namelijk niet noodzakelijk om deze biometrische gegevens te gebruiken voor het inklokken van de werknemers of voor de beveiliging van het pand. De biometrische gegevens waren te gevoelig om daarvoor te gebruiken (AP, Boetebesluit Boete voor bedrijf voor verwerken vingerafdrukken werknemers, 30 april 2020).

Het is onder omstandigheden eveneens toegestaan om biometrische gegevens te verwerken indien de betrokkene hiervoor in vrijheid toestemming heeft ge-

geven. Of er sprake is van vrije toestemming hangt af van de omstandigheden van het geval. In de relatie tussen aanbieder en klant kan in sommige gevallen worden uitgegaan van vrije toestemming. In de relatie tussen werkgever en werknemer, daarentegen meestal niet. Zeker niet wanneer de verwerking van de gegevens is verbonden aan de toegang tot, bijvoorbeeld, de werkplek of informatiesystemen (artikelsgewijze toelichting MvT Uitvoeringswet).

Nederland, gezondheidsgegevens. De verwerking van gegevens betreffende iemands gezondheid is toegestaan door personen die tot geheimhouding zijn verplicht (artikel 30 Uitvoeringswet). Het moet dan gaan om zorgverleners, maatschappelijke dienstverleners, verzekeraars, scholen (in geval van bijzondere begeleiding), reclassering en kinderbescherming. Bestuursorganen, pensioenfondsen, werkgevers en hiervoor werkzaam zijnde instellingen mogen deze gegevens ook verwerken, indien noodzakelijk ter uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten welke afhankelijk zijn van de gezondheid van de betrokkene, of bij re-integratie of begeleiding van werknemers of uitkeringsgerechtigden bij ziekte of arbeidsongeschiktheid.

Artikel 10. Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid.

Waar onder de Richtlijn strafrechtelijke persoonsgegevens nog gewoon als bijzondere persoonsgegevens aangemerkt werden, kiest de AVG voor een apart, strenger regime ter bescherming hiervan.

Wettelijke waarborgen. De verwerking van strafrechtelijke persoonsgegevens is alleen toegestaan door of vanwege de overheid (zoals in Nederland bijvoorbeeld in de Wet politiegegevens uitgewerkt is), of binnen andere Europese of nationale wetgeving. Registers, zoals zwarte lijsten, met dergelijke gegevens mogen alleen onder overheidstoezicht worden gevoerd.

Verwerkingen door overheid. De overheid mag strafrechtelijke persoonsgegevens verwerken conform Richtlijn 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opspo-

ring en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Deze verwerkingen vallen daarmee buiten de AVG.

Uitdrukkelijke toestemming. Verwerking is toegestaan wanneer de betrokkene uitdrukkelijk toestemming (artikel 9 lid 2 punt a) verleent (artikel 32 punt a Uitvoeringswet). Iedere vorm van dwang of druk maakt deze toestemming ongeldig. Een werkgever kan dus bij een sollicitatie bijvoorbeeld niet om deze gegevens vragen onder het mom van toestemming.

Verwerking door private partijen. Een private partij mag voor zichzelf strafrechtelijke persoonsgegevens verwerken ter beoordeling van een verzoek van betrokkene om een beslissing of een prestatie zoals een bestelling (artikel 33 lid 2 punt a Uitvoeringswet). Hetzelfde geldt ter bescherming van de eigen belangen wanneer de strafrechtelijke feiten jegens deze partij zelf zijn gepleegd (artikel 33 lid 2 punt b Uitvoeringswet). Dit recht geldt ook voor anderen in dezelfde groep van bedrijven (artikel 33 lid 4 punt b Uitvoeringswet). Daarnaast mogen deze persoonsgegevens worden verwerkt door een verwerkingsverantwoordelijke die optreedt krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus, of die vergunning is verleend door de AP (artikel 33 lid 4 punten a en c Uitvoeringswet). Dit is een terugkerend punt in de rechtszaken tussen Ziggo en Brein. Ziggo, de internetprovider, wordt door Brein (de organisatie die de auteursrechten van makers van film en muziek beschermt), regelmatig verzocht om de gegevens van mensen die online onrechtmatig auteursrechtelijk beschermde werken uploaden, te verstrekken. Omdat auteursrechtinbreuk een strafrechtelijk misdrijf is, zijn dit persoonsgegevens betreffende strafbare feiten. In 2022 oordeelde de rechtbank dat de uitzonderingen van de Uitvoeringswet niet van toepassing zijn. Daardoor mag Ziggo de persoonsgegevens niet verstrekken aan Brein (Rb Midden-Nederland 9 juni 2022, ECLI:NL:RBMNE:2022:2198 en bekrachtigd in ECLI:NL:GHARL:2022:8676).

Werkgevers. De verwerking van strafrechtelijke persoonsgegevens door werkgevers dient plaats te vinden overeenkomstig de Wet op de ondernemingsraden (artikel 33 lid 3 Uitvoeringswet). De werkgever kan zich dus niet beroepen op de bovengenoemde belangen.

Publiekrechtelijke samenwerkingsverbanden. Verwerking is tevens toegestaan indien dit noodzakelijk is ter uitvoering van publiekrechtelijke samenwerkingsverbanden (artikel 33 lid 1 punt b Uitvoeringswet).

Verwerking voor onderzoek. In Nederland is de verwerking van strafrechtelijke persoonsgegevens en gegevens betreffende een rechterlijk verbod inzake onrechtmatig of hinderlijk gedrag toegestaan voor wetenschappelijk of statistisch onderzoek indien dit een algemeen belang dient, toestemming verkrijgen onmogelijk is of onevenredige inspanning kost en goede waarborgen zijn getroffen (artikel 32 punt f en 24 Uitvoeringswet).

Strafrechtjournalistiek. Een journalistiek artikel over een strafzaak zal strafrechtelijke persoonsgegevens van de verdachte of dader bevatten. Hierop is artikel 10 van toepassing, maar artikel 43 lid 3 Uitvoeringswet stelt dit artikel buiten toepassing voor zover noodzakelijk is voor het journalistieke doel. Hierbij vindt dus de klassieke afweging met vrijheid van meningsuiting (artikel 11 Handvest grondrechten EU) plaats. Zie ook artikel 85, dat bepaalt dat de bescherming van persoonsgegevens in balans moet blijven met het recht op vrijheid van meningsuiting.

Bestuurlijke boete. De AVG stelt geen bestuurlijke boete op overtreding van dit artikel 10. In Nederland kan de AP voor overtredingen van artikel 10 een bestuurlijke boete opleggen van maximaal 20.000.000 euro, of 4% van de totale wereldwijde jaaromzet (artikel 17 Uitvoeringswet, vergelijk artikel 83 lid 5).

Artikel 11. Geen identificatieplicht

II.1 Indien de doeleinden waarvoor een verwerkingsverantwoordelijke persoonsgegevens verwerkt, niet of niet meer vereisen dat hij een betrokkene identificeert, is hij niet verplicht om, uitsluitend om aan deze verordening te voldoen, aanvullende gegevens ter identificatie van de betrokkene bij te houden, te verkrijgen of te verwerken.

Bij diverse rechten die een betrokkene onder de AVG heeft, is redelijkerwijs verdedigbaar dat de verwerkingsverantwoordelijke identificatie verlangt. Zo is het niet de bedoeling dat een inzageverzoek (artikel 15) door een ander dan de persoon zelf kan worden gedaan, dus kan men redelijkerwijs een identificatie-eis bij de betrokkene leggen. De AVG wil echter voorkomen dat verwerkingsverantwoordelijken altijd zodanig veel gegevens verwerken zodat de betrokkene geïdentificeerd kan worden, omdat dit ingaat tegen het beginsel van dataminimalisatie (artikel 5 lid 1 punt c). Een verwerkingsverantwoordelijke mag dus ook persoonsgegevens verwerken en bewaren binnen de AVG zonder de mogelijkheid te hebben de betrokkene(n) te identificeren.

Digitale identificatie. Overweging 57 noemt specifiek de mogelijkheid om de identiteit van de betrokkene digitaal vast te stellen aan de hand van de inloggegevens die hij of zij gebruikt bij die dienst. Wie na inloggen dus bijvoorbeeld een inzageverzoek doet, mag niet worden afgewimpeld met het verzoek een kopie identiteitsbewijs op te sturen.

II.2 Wanneer de verwerkingsverantwoordelijke in de in lid 1 van dit artikel bedoelde gevallen kan aantonen dat hij de betrokkene niet kan identificeren, stelt hij de betrokkene daarvan indien mogelijk in kennis. In dergelijke gevallen zijn de artikelen 15 tot en met 20 niet van toepassing, behalve wanneer de betrokkene, met het oog op de uitoefening van zijn rechten uit hoofde van die artikelen, aanvullende gegevens verstrekt die het mogelijk maken hem te identificeren.

Wanneer de verwerkingsverantwoordelijke de betrokkene niet kan identificeren, ontstaat een probleem wanneer deze zijn rechten uit artikelen 15-20 (inzage, rectificatie, wissen, afschermen en export) wenst uit te oefenen. De kans is dan aanwezig dat een ander het verzoek doet, met het risico op identiteitsfraude (wat een datalek oplevert, artikel 33). De verwerkingsverantwoordelijke is dan niet verplicht mee te werken aan het verzoek van de betrokkene.

Echter, wanneer de betrokkene zichzelf op een andere manier kan identificeren, moet de verwerkingsverantwoordelijke alsnog meewerken. Een persoon kan bijvoorbeeld een toegangskaartje hebben gekregen met een nummer, aan de hand waarvan de transactiegegevens of bezoekgegevens (of camerabeelden) wellicht te achterhalen zijn.

Hoofdstuk III

Rechten van de betrokkene

Bescherming van privacy is een grondrecht. De betrokkene wiens persoonsgegevens worden verwerkt, heeft dan ook een aantal sterke rechten ten aanzien van verwerkingsverantwoordelijken (maar ook verwerkers). De belangrijkste artikelen in dit hoofdstuk zijn de informatieplichten (artikelen 12, 13 en 14), en de rechten van inzage (artikel 15), rectificatie (artikel 16) en gegevenswissing (artikel 17) en het recht van bezwaar (artikel 21).

Vanwege de omvang is dit hoofdstuk onderverdeeld in vijf afdelingen. De eerste afdeling betreft de wijze van informatieverstrekking in bijvoorbeeld de privacyverklaring. De tweede afdeling werkt informatie en toegang tot persoonsgegevens nader uit. Afdeling drie gaat in op het recht van rectificatie en wissing (het ‘vergeetrecht’). Afdeling vier regelt het nieuwe recht van bezwaar tegen verwerkingen. Tenslotte legt afdeling vijf een aantal beperkingen neer die lidstaten mogen invoeren ter bescherming van andere belangen.

AFDELING 1. TRANSPARANTIE EN REGELINGEN

Zie meer algemeen over transparantie de *Richtsnoeren inzake transparantie overeenkomstig Verordening 2016/679* van het Comité.

Afdeling 1 bevat algemene bepalingen over de wijze waarop verwerkingsverantwoordelijken informatie moeten verstrekken aan betrokkenen over welke persoonsgegevens worden verwerkt (zie nader afdeling 2) en hoe betrokkenen hun rechten (zie nader afdelingen 3 en 4) kunnen uitoefenen.

Artikel 12. Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene

12.1 De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is. De informatie wordt schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen, verstrekt. Indien de betrokkene daarom verzoekt, kan de informatie mondeling worden meegedeeld, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is.

Het transparantiebeginsel (artikel 5 lid 1 punt a) vereist dat betrokkenen kunnen achterhalen dat hun persoonsgegevens worden verwerkt en waarom. Dit wordt uitgewerkt in twee informatieplichten: informatie bij verkrijging bij de betrokkene (artikel 13) en informatie bij verkrijging elders (artikel 14). Ook moeten betrokkenen weten welke rechten zij hebben (artikelen 15-22) en hoe wordt omgegaan met datalekken (artikel 34). Dit artikel 12 stelt een algemeen kader over het verstrekken van deze informatie.

Procedure. Een verzoek om informatie of uitoefening van een recht dient in beginsel binnen een maand te worden gehonoreerd (lid 3). Als dat niet gebeurt, moet binnen die periode in ieder geval worden gemeld waarom niet (lid 4). Informatieverstrekking is in beginsel kosteloos (lid 5).

Beknopt, eenvoudig toegankelijk en begrijpelijk. Te verstrekken informatie moet voor de doelgroep wel toegankelijk zijn. Dit vertaalt zich in eisen van beknoptheid (geen lange, wollige verhalen maar een paar concrete en toegespitste zinnen), toegankelijkheid (gemakkelijk te vinden en te raadplegen, bij voorkeur elektronisch) en begrijpelijk (geen juridische taal of technisch jargon). Het gebruik van visuele hulpmiddelen wordt aangemoedigd (overweging 58). Bij de informatieverstrekking kan worden gewerkt met door de Commissie gestandaardiseerde iconen (lid 7) zodat men in één oogopslag ziet waar men aan toe is.

Privacyverklaring. Een bekend middel om aan informatieplichten te voldoen is de privacyverklaring, ook wel *privacy statement* of *privacy notice* geheten. Deze wordt op de website van de verwerkingsverantwoordelijke gepubliceerd en bespreekt dan alle privacy-aspecten van een dienst, of zelfs de privacyaspecten van alle dienstverlening van deze organisatie. Een privacyverklaring is niet verplicht; informatie mag ook in brokjes worden verstrekt als deze daarmee eenvoudiger te behappen wordt. Bij een inschrijfformulier zou bijvoorbeeld de verplichte informatie op het formulier kunnen worden opgenomen.

Duidelijke en eenvoudige taal. Wat duidelijk en eenvoudig is, zal afhangen van de categorie(ën) van betrokkenen, maar hoger dan taalniveau B2 van het Europees Referentiekader Talen lijkt in het algemeen ongepast (zie nader artikel 7 lid 2 over dit begrip). Bij informatie voor kinderen (bijvoorbeeld toestemming bij internetdiensten, artikel 8) zal op kinderen afgestemde taal moeten worden gebruikt (overweging 58). In 2022 is TikTok, een platform voor jongeren waarop filmpjes worden geplaatst over allerlei onderwerpen, beboet door de AP. TikTok had, hoewel zij veel Nederlandse kinderen als gebruiker had, geen privacyverklaring beschikbaar gesteld in de Nederlandse taal. Volgens de toezichthouder was dit niet “eenvoudig” genoeg (AP, Boetebesluit TikTok, 22 juli 2021).

Identiteit betrokkene. Bij het faciliteren van iemands rechten dient de verwerkingsverantwoordelijke vast te stellen met de juiste persoon te maken te hebben. Het is echter niet toegestaan een aanspraak op een recht af te wijzen enkel vanwege twijfel aan identiteit (lid 2). Aanvullende informatie mag wel worden verlangd (lid 6). Let wel: het opvragen van de informatie ter verificatie van de identiteit van de betrokkene moet wel proportioneel zijn. DPG Media werd door de AP beboet omdat zij een identiteitsbewijs opvroeg om de identiteit van een betrokkene te verifiëren voor een inzageverzoek. Gezien de gevoeligheid van deze gegevens, was dit een te vergaand middel voor verificatie van identiteit, aldus de AP (Autoriteit Persoonsgegevens, Boetebesluit PDG Media, 24 februari 2022). Zie nader artikel 11 over deze problematiek.

12.2 De verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene uit hoofde van de artikelen 15 tot en met 22. In de in artikel 11, lid 2, bedoelde gevallen mag de verwerkingsverantwoordelijke niet weigeren gevolg te geven aan het verzoek van de betrokkene om diens rechten uit hoofde van de artikelen 15 tot en met 22 uit te oefenen, tenzij de verwerkingsverantwoordelijke aantoont dat hij niet in staat is de betrokkene te identificeren.

De verwerkingsverantwoordelijke dient erop toe te zien dat de betrokkene zijn rechten kan uitoefenen. Hiervoor zal in de praktijk vaak vereist zijn dat de betrokkene zich identificeert, zodat de verwerkingsverantwoordelijke in staat is de betrokkene te identificeren. Dit levert een probleem op bij het uitvoeren van verzoeken: is dit wel de juiste persoon om de gevraagde informatie aan te geven? Artikel 11 bepaalt dat de verwerkingsverantwoordelijke dan de beweerdelijke betrokkene hierover moet informeren, waarna deze aanvullende informatie kan leveren om de identificatie alsnog mogelijk te maken.

Niet weigeren. Dit lid 2 maakt duidelijk dat het niet weten wie de betrokkene is, geen argument is om een verzoek te weigeren, tenzij het onmogelijk is om vast te stellen dat deze persoon gerechtigd is tot de gevraagde informatie. De verwerkingsverantwoordelijke mag daarbij niet weigeren aanvullende informatie ter identificatie aan te nemen, maar moet dus daarna een nieuwe poging doen de betrokkene te identificeren.

Inloggegevens. Identificatie hoeft niet per se middels een overheidsidentificatiebewijs zoals een paspoort. Bij online diensten zouden de inloggegevens van het account prima kunnen dienen als bewijs (overweging 57). Iemand die in kan loggen op een zeker account, wordt vermoed de accounthouder te zijn en daarmee recht te hebben op de persoonsgegevens van die houder.

- 12.3 De verwerkingsverantwoordelijke verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens de artikelen 15 tot en met 22 informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

Zeker bij elektronische verwerkingen ligt het voor de hand dat een inzage- of ander verzoek snel af te handelen is. De AVG biedt echter meer ruimte: onverwijld, maar uiterlijk binnen een maand reageren.

Verlenging. Een verlenging met maximaal twee maanden is mogelijk, mits de verwerkingsverantwoordelijke dit onderbouwt op grond van complexiteit en aantal verzoeken van de betreffende betrokkene. Dit moet dan binnen de eerste maand na het verzoek worden gemeld.

Elektronische communicatie. Wanneer een verzoek elektronisch wordt gedaan, moet daar eveneens elektronisch gehoor aan worden gegeven. De enige uitzondering is nog wanneer de betrokkene verzoekt om een ander middel, zoals papier. Een verzoek om grote stapels papier zou wellicht als buitensporig kunnen worden aangemerkt (zie lid 5 hieronder).

- 12.4 Wanneer de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, deelt hij deze laatste onverwijld en uiterlijk binnen een maand na ontvangst van het verzoek mee waarom het verzoek zonder gevolg is gebleven, en informeert hij hem over de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen.

De verwerkingsverantwoordelijke moet in beginsel gehoor geven aan ieder verzoek. Het weigeren van verzoeken zal een uitzondering zijn, waarvoor de gronden uit het betreffende artikel volgen (of uit lid 5 als het gaat om kennelijk ongegronde of buitensporige verzoeken). Heeft hij zo'n grond, dan zal de verwerkingsverantwoordelijke toch in ieder geval de betrokkene moeten informeren over de redenen. Tevens is hij dan verplicht de betrokkene te wijzen op zijn

klachtrecht bij de toezichthouder en de mogelijkheid naar de rechter te stappen om het verzoek af te dwingen.

- 12.5 Het verstrekken van de in de artikelen 13 en 14 bedoelde informatie, en het verstrekken van de communicatie en het treffen van de maatregelen bedoeld in de artikelen 15 tot en met 22 en artikel 34 geschieden kosteloos.

De AVG vereist dat de verwerkingsverantwoordelijke kosteloos de vereiste informatie (artikelen 13 en 14) verstrekt en eveneens kosteloos betrokkenen hun rechten van inzage, wissing et cetera (artikelen 15-22) of informatie over datalekken (artikel 34) verstrekt. Dat het voor de verwerkingsverantwoordelijke complex of duur is om gehoor te geven aan het verzoek, is dus geen argument.

Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de verwerkingsverantwoordelijke ofwel:

Er zijn slechts twee gronden om een verzoek te weigeren: het verzoek is kennelijk ongegrond, of het verzoek is buitensporig.

Kennelijk ongegrond. Een verzoek is kennelijk ongegrond als evident niet is voldaan aan de randvoorwaarden bij een verzoek, of als wordt gevraagd om iets waar men evident geen recht in de AVG op heeft. Een voorbeeld zou zijn een inzageverzoek in persoonsgegevens van een ander of een wissingsverzoek op een openstaande factuur.

Buitensporig. Een verzoek is buitensporig als het een zeer disproportionele last legt op de verwerkingsverantwoordelijke, bijvoorbeeld wanneer elke week grote dossiers opgevraagd worden of iemand dagelijks verlangt dat zijn achternaam wordt weggehaald en vervolgens weer toegevoegd.

- 12.5(a) een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan; ofwel

- 12.5(b) weigeren gevolg te geven aan het verzoek.

De verwerkingsverantwoordelijke heeft de keuze om óf het verzoek te weigeren, óf een redelijke vergoeding aan te rekenen. Bij een weigering mogen dus geen kosten worden gerekend. De AVG laat in het midden of de kosten sowieso in rekening gebracht mogen worden of alleen na een apart akkoord daarop. Gezien de focus van de AVG op het beschermen van betrokkenen ligt het laatste het meest in de rede.

Het is aan de verwerkingsverantwoordelijke om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

De bewijslast dat sprake is van een kennelijk ongegrond of buitensporig verzoek ligt bij de verwerkingsverantwoordelijke. Gezien de focus van de AVG zal de lat hierbij hoog liggen en kan de verwerkingsverantwoordelijke niet enkel volstaan met de mededeling dat het verzoek wordt afgewezen wegens de kennelijk ongegronde of buitensporige aard daarvan.

- 12.6 Onverminderd artikel 11 kan de verwerkingsverantwoordelijke, wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het verzoek indient als bedoeld in de artikelen 15 tot en met 21, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

Niet in alle gevallen zal de afzender van een verzoek direct identificeerbaar zijn aan de hand van bijvoorbeeld een paspoort of identiteitskaart. Vanuit het beginsel van rechtmatigheid en behoorlijkheid (zie artikel 5 lid 1 punt a) en de beveiligingsplicht (artikel 32) moet een verwerkingsverantwoordelijke er zorg voor dragen dat persoonsgegevens niet bij de verkeerde persoon terecht komen. Een verzoek mag niet zonder meer worden afgewezen enkel omdat er niet genoeg informatie is om de betrokkene te identificeren (zie lid 2 en artikel 11). Verzoeken om aanvullende informatie is dan de gepaste tussenstap.

De aanvullende informatie hoeft niet per se een overheidsidentificatiedocument te zijn (zie ook lid 2). Een verzoek ingediend na online inloggen zou ook genoeg moeten zijn (overweging 57). Bij een verzoek door een werknemer zou identificatie met de toegangspas voor kantoor wellicht adequaat kunnen zijn.

- 12.7 De krachtens de artikelen 13 en 14 aan betrokkenen te verstrekken informatie mag worden verstrekt met gebruikmaking van gestandaardiseerde iconen, om de betrokkene een nuttig overzicht, in een goed zichtbare, begrijpelijke en duidelijk leesbare vorm, van de voorgenomen verwerking te bieden. Wanneer de iconen elektronisch worden weergegeven, zijn ze machinaal leesbaar.

De te verstrekken informatie over de verwerking (artikel 13: indien verkregen bij betrokkene, artikel 14: indien elders verkregen) moet in beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal gebeuren (zie lid 1). Om de verwerkingsverantwoordelijke hierbij te helpen, bevat de AVG de mogelijkheid gestandaardiseerde iconen te gebruiken. Deze bieden dan directe herkenning van de belangrijkste privacyaspecten waarover moet worden geïnformeerd.

Iconen. Tot op heden (februari 2023) is nog niet bekend welke iconen zullen worden gekozen en op welke manier zij worden vormgegeven.

Machine-leesbaar. Bij internetdiensten is het mogelijk informatie te voorzien van metadata die door computers kan worden geïnterpreteerd. Deze metadata kan dan automatisch worden gebruikt, bijvoorbeeld door zoekmachines om een website te selecteren (of uit te sluiten) op basis van de privacy-keuzes die gebruikers hebben gemaakt.

- 12.8 De Commissie is bevoegd overeenkomstig artikel 92 gedelegeerde handelingen vast te stellen om te bepalen welke informatie de iconen dienen weer te geven en via welke procedures de gestandaardiseerde iconen tot stand dienen te komen.

Bij de totstandkoming van de AVG kon men het niet eens worden over welke iconen moesten worden voorgeschreven en hoe deze worden gekozen. Dit lid 8 laat de beslissing nu aan de Commissie, zij het dat deze een bindend advies moet krijgen van de artikel 92-commissie (artikel 92).

AFDELING 2. INFORMATIE EN TOEGANG TOT PERSOONSGEGEVENS

Afdeling 2 werkt de informatieplichten voor verwerkingsverantwoordelijken nader uit. Deze moet informatie verschaffen (bijvoorbeeld in een privacyverklaring) over welke persoonsgegevens worden verwerkt, met welke doelen en op welke wijze. Als de persoonsgegevens bij de betrokkene zelf worden verkregen, moet deze informatie bij verkrijging worden verschaft (artikel 13). Verkrijgt men de gegevens van anderen, dan moet de informatie alsnog zo snel mogelijk worden verschaft (artikel 14). In beide gevallen geldt dat de betrokkene mag opvragen welke gegevens worden verwerkt en waartoe, en daar ook een kopie van opvragen (artikel 15).

Artikel 13. Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld

- 13.1 Wanneer persoonsgegevens betreffende een betrokkene bij die persoon worden verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene al bij de verkrijging van de persoonsgegevens de volgende informatie:

Een verwerkingsverantwoordelijke heeft een actieve informatieplicht naar betrokkenen toe, waarbij we een onderscheid kunnen maken in twee situaties. Dit artikel 13 behandelt de situatie dat de persoonsgegevens direct bij de persoon zelf worden verzameld; artikel 14 ziet op de situatie dat de persoonsgegevens langs andere route worden verkregen. Lid 1 noemt algemene informatie, lid 2 meer specifieke en lid 3 gaat in op het doelbindingsvereiste. Zie artikel 12 voor aanvullende algemene eisen aan de informatie. De informatie overlapt gedeeltelijk met wat de verwerkingsverantwoordelijke in het register (artikel 30) moet bijhouden.

Privacyverklaring. Zeker bij digitale diensten is het instrument van de privacyverklaring of *privacy statement* gebruikelijk om deze informatie te verstrekken. Alle vereiste informatie wordt dan op één plek aangeboden. Het is theoretisch ook voldoende om de informatie op andere manieren te verstrekken, bijvoorbeeld als toelichtende zinnen bij velden op een invulformulier. Dit kan echter snel leiden tot versnipperde en dus inadequate informatieverstrekking.

Akkoord op privacyverklaringen. Op privacyverklaringen hoeft overigens geen akkoord te worden gevraagd; het betreft immers een informatieplicht. Akkoord vraagt men in het kader van de grondslag toestemming (artikel 6 lid 1 punt a en artikel 7).

Beknopt en transparant. De gevraagde informatie dient in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekt te worden (artikel 12 lid 1). Dit betekent in de praktijk dus dat geen juridisch jargon mag worden gebruikt. Zie nader artikel 12 lid 1. Zie ook de aanbevelingen van het Comité in de *Richtsnoeren inzake transparantie overeenkomstig Verordening 2016/679*.

Kosteloos. Het verstrekken van informatie onder dit artikel dient kosteloos te gebeuren (artikel 12 lid 5).

Iconen. Bij deze informatieverstrekking mag worden gewerkt met gestandaardiseerde iconen, zodra deze zijn vastgesteld door de Commissie (zie artikel 12 lid 7).

13.1(a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;

Allereerst dient de verwerkingsverantwoordelijke zijn identiteit (volledige of statutaire naam) en zijn contactgegevens (adres, telefoonnummer, e-mail, social media indien gebruikt voor communicatie) op te nemen. Indien de verwerkingsverantwoordelijke buiten de EU is gevestigd, maar wel onder de AVG valt (volgens artikel 3 lid 2), dient hij een vertegenwoordiger (artikel 27) aan te stellen. Diens identiteit dient dan eveneens te worden verstrekt.

13.1(b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;

Indien de verwerkingsverantwoordelijke een functionaris voor gegevensbescherming heeft aangesteld (artikel 37), dienen ook zijn of haar contactgegevens te worden vermeld.

- 13.1(c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, als-
ook de rechtsgrond voor de verwerking;

Tevens dient te worden gemeld voor welke doeleinden de persoonsgegevens worden gebruikt, en op welke grond (artikel 6 lid 1) men deze persoonsgegevens wenst te verwerken. De grondslag voor verwerking moet ook worden gemeld (zie ook lid 2 punten c en e en dit lid 1 punt d).

- 13.1(d) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd;

Wanneer een verwerking wordt verricht op grond van het gerechtvaardigd belang (artikel 6 lid 1 punt f) dient de betrokkene te weten om welk belang het gaat. Dit belang moet concreet worden gemotiveerd.

- 13.1(e) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;

Wanneer persoonsgegevens aan verwerkers of derden (artikel 4 definitie 10) worden verstrekt, moeten deze ontvangers (artikel 4 definitie 9) worden genoemd. Dit mag gebeuren bij naam, maar als een vermelding van categorie voldoende is, mag daarmee worden volstaan. Een webwinkel kan bijvoorbeeld verwijzen naar de categorieën 'Betaaldienstverleners' en 'Bezorgdiensten' zonder concreet namen te hoeven noemen.

- 13.1(f) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

In het geval van internationale data doorgifte naar ontvangers moet de betrokkene geïnformeerd worden over welke maatregelen uit hoofdstuk V er worden genomen om die doorgifte veilig te stellen. Er wordt dan opgenomen of er een adequaatheidsbesluit (artikel 45) geldt, of er passende waarborgen (artikel 46) zijn genomen, of dat bindende bedrijfsvoorschriften gelden (artikel 47).

- 13.2 Naast de in lid 1 bedoelde informatie verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens de volgende aanvullende informatie om een behoorlijke en transparante verwerking te waarborgen:

In aanvulling op de algemene informatieplichten uit lid 1 bepaalt lid 2 een zestal aanvullende informatieplichten. Deze zijn gericht op de wijze van verwerking en dienen ter voorlichting van de betrokkene over zijn rechten.

- 13.2(a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;

Persoonsgegevens mogen niet langer worden bewaard dan nodig is (artikel 5 lid 1 punt e). De verwerkingsverantwoordelijke moet derhalve melden hoelang persoonsgegevens worden bewaard. Dit kan als een hard getal, maar ook als functioneel criterium zoals “tot zes maanden na uw laatste aankoop” of “zodra uw bestelling in ontvangst is genomen”.

- 13.2(b) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;

De betrokkene moet expliciet worden gewezen op zijn rechten: inzage (artikel 15), rectificatie (artikel 16), gegevenswissing (artikel 17), beperking (artikel 18), bezwaar (artikel 21) en het recht zijn gegevens in digitaal formaat te krijgen (artikel 20). Het recht van bezwaar moet duidelijk en apart worden gemeld van overige informatie (artikel 21 lid 4).

- 13.2(c) wanneer de verwerking op artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;

Toestemming voor verwerking (artikel 6 lid 1 punt a bij gewone en artikel 9 lid 2 punt a bij bijzondere persoonsgegevens) kan te allen tijde worden ingetrokken (artikel 7 lid 3). De verwerkingsverantwoordelijke moet de betrokkene hier actief over informeren. Intrekken van toestemming heeft geen terugwerkende kracht.

- 13.2(d) dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;

Als de betrokkene meent dat zijn rechten worden geschonden, heeft hij het recht daar een klacht over in te dienen bij een toezichthouder (artikel 77). Dit moet expliciet worden gemeld aan de betrokkene.

- 13.2(e) of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;

Persoonsgegevens kunnen nodig zijn voor nakoming van een overeenkomst (artikel 6 lid 1 punt b) of om te voldoen aan een wettelijke verplichting (artikel

6 lid 1 punt c). Als deze gronden worden gebruikt, moet dit worden gemeld aan de betrokkene in aansluiting op lid 1 punt c.

- 13.2(f) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer de persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming (artikel 22) moet dit apart worden gemeld. Daarbij moet tevens worden gemeld om wat voor besluitvorming het gaat en welke gevolgen dit kan hebben voor de betrokkene. Ook moet de onderliggende logica op hoofdlijnen worden uitgelegd, bijvoorbeeld: “Op basis van uw postcode en uw eerdere aankopen of uw aankoopgedrag wordt geautomatiseerd bepaald of u in aanmerking komt voor achterafbetaling in onze webwinkel.”

- 13.3 Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.

Als derde component dient de verwerkingsverantwoordelijke het te melden als hij van plan is de persoonsgegevens ook voor andere doelen te gebruiken. De informatie over deze doelen dient in ieder geval te bevatten wat in lid 2 genoemd is. Uiteraard dienen deze andere doelen verenigbaar te zijn met het doel van verkrijging (zie artikel 5 lid 1 punt b, doelbinding en artikel 6 lid 4).

- 13.4 De leden 1, 2 en 3 zijn niet van toepassing indien en voor zover de betrokkene reeds over de informatie beschikt.

Uiteraard hoeft informatie niet meerdere malen verstrekt te worden. De bewijslast dat de betrokkene de informatie reeds heeft, ligt bij de verwerkingsverantwoordelijke (artikel 5 lid 2). Het gaat hierbij om een concrete vaststelling dat deze betrokkene weet heeft van de informatie of geacht moet worden deze te kennen, op basis van concrete gedragingen of uitspraken van de betrokkene.

Artikel 14. Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen

- 14.1 Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie:

Een verwerkingsverantwoordelijke heeft in twee situaties een actieve informatieplicht naar betrokkenen toe. Dit artikel 14 behandelt de situatie waarin per-

soonsgegevens langs andere weg dan bij de betrokkene zelf zijn verkregen. Voor verkrijging bij de betrokkene zie artikel 13. Lid 1 noemt algemene informatie, lid 2 meer specifieke en lid 3 werkt uit hoe deze informatie moet worden verstrekt aan betrokkenen. Zie artikel 12 voor aanvullende algemene eisen aan de informatie.

Verskil met verkrijging bij betrokkene. Ten opzichte van artikel 13 lid 1 (verkrijging bij betrokkene) zijn de enige inhoudelijke toevoegingen dat de categorieën van persoonsgegevens (punt d) en de bron (lid 2 punt f) moeten worden genoemd, alsook dat niet hoeft te worden gewezen op gevolgen voor eventuele overeenkomsten (punt e). Let op dat het melden van het gerechtvaardigde belang bij dit artikel 14 in lid 2 (punt b) opgenomen is, terwijl artikel 13 dit in lid 1 (punt d) vermeldt. Praktisch heeft dit geen gevolg.

Twee informatieplichten. Wanneer persoonsgegevens van een andere verwerkingsverantwoordelijke worden verkregen, moet deze de betrokkene bij verkrijging van de persoonsgegevens daarover informeren (artikel 13 lid 1 punt e). Deze plicht staat los van de plicht voor de ontvangende verwerkingsverantwoordelijke om onder dit artikel 14 de betrokkene te informeren. Echter, wanneer een van beide verwerkingsverantwoordelijken al weet dat de betrokkene reeds over de informatie beschikt, hoeft deze niet nogmaals te worden verschaft (lid 5 punt a). In de praktijk zou de eerste verwerkingsverantwoordelijke bij verkrijging alle informatie uit artikel 13 verschaffen, en de tweede verwerkingsverantwoordelijke hoeft dan alleen nog zijn identiteit, de categorieën en de bron te noemen.

Geen contactgegevens. Het is mogelijk dat de verwerkingsverantwoordelijke beschikt over persoonsgegevens van betrokkenen zonder daarbij contactgegevens te hebben. Denk aan een interesseprofiel gekoppeld aan een cookie dat wordt aangekocht van een internetdienst. Men zou dan een zeer grote inspanning moeten verrichten om alsnog die contactgegevens te achterhalen. Op grond van lid 5 punt b is dit niet vereist (vergelijk artikel 11). Vaak zal uiteindelijk wel worden gecommuniceerd met betrokkenen, in het voorbeeld om ze gepaste reclame aan te bieden. In dat geval moet bij het eerste contact de informatie worden verstrekt (lid 3 punt b).

14.1(a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;

Allereerst dient de verwerkingsverantwoordelijke zijn identiteit (volledige of statutaire naam) en zijn contactgegevens (adres, telefoonnummer, e-mail, social media indien gebruikt voor communicatie) te verstrekken. Indien de verwerkingsverantwoordelijke buiten de EU is gevestigd, maar wel onder de AVG valt (volgens artikel 3 lid 2), dient hij een vertegenwoordiger (artikel 27) aan te stellen. Diens identiteit dient dan eveneens te worden verstrekt.

14.1(b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;

Indien de verwerkingsverantwoordelijke een functionaris voor gegevensbescherming heeft aangesteld (artikel 37), dienen ook zijn of haar contactgegevens te worden gemeld aan de betrokkene.

14.1(c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking;

Tevens dient de betrokkene te worden gemeld voor welke doeleinden de persoonsgegevens worden gebruikt, en op welke grond (artikel 6 lid 1) men deze persoonsgegevens wenst te verwerken. De grondslag voor verwerking moet ook worden gemeld (zie ook lid 2 punten b en d).

14.1(d) de betrokken categorieën van persoonsgegevens;

De betrokkene moet ook worden gemeld om welke (categorieën van) persoonsgegevens het gaat, zoals “naam en adres” of “uw aankoopgeschiedenis inclusief totaalbedragen en of deze tijdig zijn betaald”.

14.1(e) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;

Wanneer persoonsgegevens aan verwerkers of derden (artikel 4 definitie 10) worden verstrekt, moeten deze ontvangers (artikel 4 definitie 9) worden gemeld. Dit mag gebeuren bij naam, maar als een vermelding van categorie voldoende is, mag daarmee worden volstaan. Een webwinkel kan bijvoorbeeld verwijzen naar de categorieën ‘Betaaldienstverleners’ en ‘Bezorgdiensten’ zonder concreet namen te hoeven noemen.

14.1(f) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een ontvanger in een derde land of aan een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van de in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

In het geval van internationale data doorgifte naar ontvangers moet de betrokkene geïnformeerd worden over welke maatregelen uit hoofdstuk V er worden genomen om die doorgifte veilig te stellen. Er wordt dan opgenomen of er een adequaatheidsbesluit (artikel 45) geldt, of er passende waarborgen (artikel 46) zijn genomen, of dat bindende bedrijfsvoorschriften gelden (artikel 47).

14.2 Naast de in lid 1 bedoelde informatie verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie om ten overstaan van de betrokkene een behoorlijke en transparante verwerking te waarborgen:

Ten opzichte van artikel 13 lid 2 (verkrijging bij betrokkene) is de enige wezenlijke toevoeging dat de bron van de persoonsgegevens (punt f) wordt genoemd.

14.2(a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

Persoonsgegevens mogen niet langer worden bewaard dan nodig is (artikel 5 lid 1 punt e). De verwerkingsverantwoordelijke moet derhalve melden hoelang persoonsgegevens worden bewaard. Dit kan als een hard getal, maar ook als functioneel criterium zoals “tot zes maanden na uw laatste aankoop” of “zodra uw bestelling in ontvangst is genomen”.

14.2(b) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd;

Wanneer een verwerking wordt verricht op grond van het gerechtvaardigd belang (artikel 6 lid 1 punt f) dient de betrokkene te weten om welk belang het gaat. Dit belang moet concreet worden gemotiveerd.

14.2(c) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens of om beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking van bezwaar te maken en het recht op gegevensoverdraagbaarheid;

De betrokkene moet expliciet worden gewezen op zijn rechten: inzage (artikel 15), rectificatie (artikel 16), gegevenswissing (artikel 17), beperking (artikel 18), bezwaar (artikel 21) en het recht zijn gegevens in digitaal formaat te krijgen (artikel 20). Het recht van bezwaar moet duidelijk en apart worden gemeld van overige informatie (artikel 21 lid 4).

14.2(d) wanneer verwerking op artikel 6, lid 1, punt a) of artikel 9, lid 2, punt a), is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;

Toestemming voor verwerking (artikel 6 lid 1 punt a bij gewone en artikel 9 lid 2 punt a bij bijzondere persoonsgegevens) kan te allen tijde worden ingetrokken (artikel 7 lid 3). De verwerkingsverantwoordelijke moet de betrokkene hier actief over informeren. Intrekken van toestemming heeft geen terugwerkende kracht.

14.2(e) dat de betrokkene het recht heeft een klacht in te dienen bij de toezichthoudende autoriteit;

Als de betrokkene meent dat zijn rechten worden geschonden, heeft hij het recht daar een klacht over in te dienen bij een toezichthouder (artikel 77). Dit moet expliciet worden gemeld aan de betrokkene.

14.2(f) de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen;

Wanneer persoonsgegevens niet bij de betrokkene zelf zijn verkregen, moet de betrokkene natuurlijk worden geïnformeerd over wat dan wel de bron is. Wanneer de oorsprong van de persoonsgegevens niet aan de betrokkene kan worden meegedeeld omdat verschillende bronnen zijn gebruikt, moet algemene informatie worden verstrekt (overweging 61).

14.2(g) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer de persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming (artikel 22) moet dit apart worden gemeld. Daarbij moet tevens worden gemeld om wat voor besluitvorming het gaat en welke gevolgen dit kan hebben voor de betrokkene. Ook moet de onderliggende logica op hoofdlijnen worden uitgelegd, bijvoorbeeld: “Op basis van uw postcode en uw eerdere aankopen of uw aankoopgedrag wordt geautomatiseerd bepaald of u in aanmerking komt voor achterafbetaling in onze webwinkel.”

14.3 De verwerkingsverantwoordelijke verstrekt de in de leden 1 en 2 bedoelde informatie:

Wanneer persoonsgegevens niet van de betrokkene zelf (zoals in artikel 13) worden verkregen, wordt het lastiger de betrokkene te informeren over wat er met zijn persoonsgegevens gebeurt. Dit lid 3 vult nader in hoe hier gehoor aan te geven. Uitzonderingen op de informatieverstrekking zijn opgenomen in lid 5.

14.3(a) binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;

Hoofdgeregeld is dat de betrokkene uiterlijk binnen een maand na de verkrijging moet worden geïnformeerd dat zijn persoonsgegevens worden gebruikt. Alleen als uitzonderlijke omstandigheden een langere termijn vergen, kan dit toegestaan zijn.

14.3(b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of

Specifiek wanneer de persoonsgegevens worden gebruikt om met de betrokkene te communiceren, is het genoeg om op het moment van het eerste contact de informatie te verstrekken. Bij bijvoorbeeld een mailing kan men in de laatste alinea of voettekst uitleggen waarom men deze mail stuurt en hoe men aan het e-mailadres komt.

14.3(c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

In ieder geval moet de betrokkene zijn geïnformeerd voordat de verkrijgende verwerkingsverantwoordelijke de persoonsgegevens aan een andere ontvanger gaat verstrekken. Hiermee kan de betrokkene dan nog tijdig bijvoorbeeld bezwaar (artikel 21) maken of zijn gegevens laten wissen (artikel 17).

14.4 Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.

De verwerkingsverantwoordelijke dient het te melden als hij van plan is de persoonsgegevens ook voor andere doelen te gebruiken. De informatie over deze doelen dient in ieder geval te bevatten wat in lid 2 genoemd is. Uiteraard dienen deze andere doelen verenigbaar te zijn met het doel van verkrijging (zie artikel 5 lid 1 punt b, doelbinding en artikel 6 lid 4).

14.5 De leden 1 tot en met 4 zijn niet van toepassing indien en voor zover:

14.5(a) de betrokkene reeds over de informatie beschikt;

Wanneer de betrokkene de betreffende informatie al heeft, hoeft deze uiteraard niet nogmaals verschaft te worden. Vergelijk artikel 13 lid 4. De bewijslast dat de informatie al bij de betrokkene is, ligt bij de verwerkingsverantwoordelijke (artikel 5 lid 2).

14.5(b) het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen, of voor zover de in lid 1 van dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt de verwerkingsverantwoordelijke passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;

Wanneer de informatieverstrekking aan de betrokkene onmogelijk blijkt of onevenredig veel inspanningen zou kosten, kan de verwerkingsverantwoordelijke afzien van het informeren van betrokkenen. Deze situatie zal zich met name voordoen bij archivering in het algemeen belang of bij wetenschappelijk of historisch onderzoek (zie daarover nader artikel 89), omdat daarbij grote hoeveelheden persoonsgegevens van veel betrokkenen worden verwerkt.

Onmogelijk of onevenredig veel inspanning. Dat het verstrekken van de informatie onmogelijk is, zal niet snel worden aangenomen. Zolang de gegevens persoonsgegevens zijn, is immers per definitie de persoon te traceren. De praktijk zal zich dus richten op de vraag of de verstrekking onevenredig veel inspanning zou vergen. Overweging 62 noemt daarbij drie relevante factoren: om hoeveel betrokkenen het gaat, hoe oud de persoonsgegevens zijn en welke passende waarborgen moeten worden ingebouwd om langs andere weg de betrokkenen te beschermen.

Passende waarborgen. Wel dient de verwerkingsverantwoordelijke passende maatregelen te nemen om langs andere weg de privacy van betrokkenen te beschermen. In ieder geval moet hij dan de informatie uit leden 1 t/m 4 openbaar maken (bijvoorbeeld middels een privacyverklaring), zodat betrokkenen deze langs die weg kunnen verkrijgen.

14.5(c) het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unierecht of lidstatelijk recht die op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of

Wanneer het verkrijgen of verstrekken van persoonsgegevens bij wet is verplicht, en deze wet een eigen regeling heeft om de belangen van betrokkenen te beschermen, dan is het verstrekken van de informatie uit dit artikel 14 niet nodig. Zie artikel 23 over dergelijke wetgeving.

14.5(d) de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lidstatelijke recht, waaronder een wettelijke geheimhoudingsplicht.

Wanneer de verwerkingsverantwoordelijke gehouden is aan een beroepsgeheim, zoals het medisch beroepsgeheim of het verschoningsrecht van de advocaat, gaat dit boven de informatieplicht uit dit artikel 14. Een voorbeeld zou zijn een advocaat die van zijn cliënt een dossier krijgt met daarin persoonsgegevens van derden. De advocaat is dan niet gehouden deze derden te informeren over deze verkrijging, aangezien dat in strijd zou zijn met zijn beroepsgeheim ten aanzien van zijn cliënt. Zie over beroepsgeheim versus persoonsgegevens meer algemeen artikel 90.

Artikel 15. Recht van inzage van de betrokkene

15.1 De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitend te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van de volgende informatie:

De betrokkene heeft het recht om te informeren of zijn persoonsgegevens worden verwerkt. Als dat het geval blijkt, heeft hij recht op uitleg over het wat en hoe, alsook op inzage en een kopie van zijn persoonsgegevens (zie nader artikel 20). De verwerkingsverantwoordelijke kan verlangen dat de betrokkene zich op adequate wijze identificeert (zie meer algemeen artikel 11). Het recht van inzage is mede bedoeld om uitoefening van de rechten van rectificatie (artikel 16), gegevenswissing (artikel 17) en beperking (artikel 18) mogelijk te maken.

Kosten. Uitoefening van het recht van inzage kan kosten met zich meebrengen. Voor één enkel exemplaar mogen deze niet in rekening worden gebracht. Voor aanvullende kopieën mag een redelijke vergoeding worden verlangd. Zie nader lid 3.

Gestructureerde vorm. Bij verwerkingen krachtens toestemming of overeenkomst heeft de betrokkene het recht een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen (zie artikel 20). Hiermee kan deze de persoonsgegevens zelf gebruiken. De verwerkingsverantwoordelijke mag hem daarin niet hinderen.

Interne notities. Veel dossiers bevatten werkdocumenten, interne notities en dergelijke documenten die de persoonlijke gedachten van de opsteller (zoals een personeelsmedewerker) bevatten en die uitsluitend bedoeld zijn voor intern overleg en beraad. Het inzagerecht strekt zich niet uit tot deze stukken,

vanwege lid 4 dat bepaalt dat het inzagerecht geen afbreuk doet aan de rechten en vrijheden van anderen. Het meesturen van deze informatie kan een inbreuk zijn op de privacy van de betrokken medewerkers, waardoor lid 4 opgaat en dat deel geanonimiseerd moet worden (bijvoorbeeld). Vergelijk onder de Richtlijn Gerechtshof Amsterdam 5 juli 2011, ECLI:NL:GHAMS:2011:BR3020).

Overheidsbesluiten. Specifiek bij overheidsbesluiten heeft het Hof van Justitie een uitzondering gecreëerd voor juridische analyses die ten grondslag liggen aan (ontwerp-)besluiten. Dergelijke documenten zijn geen persoonsgegevens (HvJ EU 17 juli 2014, zaken C-141/12 en C-372/12). Aan dergelijke voorbereidende documenten kleven namelijk geen privacy-aspecten; inzage moet via de Wet open overheid worden verzocht.

15.1(a) de verwerkingsdoeleinden;

Allereerst dient te worden gemeld voor welke doeleinden de persoonsgegevens worden gebruikt, en op welke grond (artikel 6 lid 1) men deze persoonsgegevens wenst te verwerken. Vergelijk artikel 13 lid 1 punt c.

15.1(b) de betrokken categorieën van persoonsgegevens;

De betrokkene moet ook worden gemeld om welke (categorieën van) persoonsgegevens het gaat, zoals “naam en adres” of “uw aankoopgeschiedenis inclusief totaalbedragen en of deze tijdig zijn betaald”. Vergelijk artikel 14 lid 1 punt d.

15.1(c) de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;

Wanneer persoonsgegevens aan verwerkers of derden (artikel 4 definitie 10) worden verstrekt, moeten deze ontvangers (artikel 4 definitie 9) worden genoemd. Dit geldt ook voor ontvangers in derde landen, waarover nader lid 2. Vergelijk artikel 13 lid 1 punt e.

15.1(d) indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

Persoonsgegevens mogen niet langer worden bewaard dan nodig is (artikel 5 lid 1 punt e). De verwerkingsverantwoordelijke moet derhalve melden hoelang persoonsgegevens worden bewaard. Vergelijk artikel 13 lid 2 punt a.

15.1(e) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;

De betrokkene moet expliciet worden gewezen op zijn rechten: inzage (artikel 15), rectificatie (artikel 16), gegevenswissing (artikel 17), beperking (artikel 18), bezwaar (artikel 21) en het recht zijn gegevens in digitaal formaat te krijgen (artikel 20). Zie nader artikel 13 lid 2 punt b.

15.1(f) dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;

Als de betrokkene meent dat zijn rechten worden geschonden, heeft hij het recht daar een klacht over in te dienen bij een toezichthouder (artikel 77). Dit moet expliciet worden gemeld aan de betrokkene. Vergelijk artikel 13 lid 2 punt d.

15.1(g) wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;

Wanneer persoonsgegevens niet bij de betrokkene zelf zijn verkregen, moet de betrokkene ook worden geïnformeerd over wat dan wel de bron is. Vergelijk artikel 14 lid 2 punt f.

15.1(h) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer de persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming (artikel 22) moet dit apart worden gemeld. Daarbij moet tevens worden gemeld om wat voor besluitvorming het gaat en welke gevolgen dit kan hebben voor de betrokkene. Ook moet de onderliggende logica op hoofdlijnen worden uitgelegd, bijvoorbeeld: "Op basis van uw postcode en uw eerdere aankopen of uw aankoopgedrag, wordt geautomatiseerd bepaald of u in aanmerking komt voor achterafbetaling in onze webwinkel." Vergelijk artikel 13 lid 2 punt f.

15.2 Wanneer persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie, heeft de betrokkene het recht in kennis te worden gesteld van de passende waarborgen overeenkomstig artikel 46 inzake de doorgifte.

Specifiek wanneer de persoonsgegevens worden doorgegeven aan een land buiten de EU dient de betrokkene ook te worden gemeld met welke passende

waarborgen (artikel 46) dit is omgeven wanneer het land geen adequaat beschermingsniveau (artikel 45) kent.

- 15.3 De verwerkingsverantwoordelijke verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt. Indien de betrokkene om bijkomende kopieën verzoekt, kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding aanrekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.

Op verzoek dient de betrokkene een kopie te ontvangen van alle persoonsgegevens die worden verwerkt. Deze kopie dient in een gangbare elektronische vorm te worden verstrekt, tenzij het verzoek op papier is gedaan of de betrokkene expliciet om een papieren kopie verzoekt.

Kopie. Een kopie is een getrouwe reproductie van de data zoals bekend bij de verwerkingsverantwoordelijke, niet slechts een samenvatting of overzicht (waarover lid 1 handelt). Kopieën van documenten mogen worden beperkt tot uitsluitend de persoonsgegevens, maar moet de betrokkene in staat stellen zijn overige rechten uit de AVG (zoals correctie of verwijdering) na te komen. Context is daarmee essentieel. Zie HvJ EU 4 mei 2023, ECLI:EU:C:2023:369.

Gangbare elektronische vorm. De betrokkene heeft het recht deze kopie in een gangbare elektronische vorm te verkrijgen. Niet vereist echter is dat het formaat gestructureerd en machinaal leesbaar is (zodat geautomatiseerde verwerking mogelijk wordt), behalve bij een verwerking krachtens toestemming of overeenkomst (zie nader artikel 20). Een pdf-bestand waarin tekst niet te selecteren en kopiëren is, is dus een “gangbare elektronische vorm”. De verwerkingsverantwoordelijke mag het hergebruik van deze kopie niet hinderen, bijvoorbeeld door geheimhouding te verlangen of een auteurs- of databankrechtclaim te leggen op de informatie.

Administratieve kosten. Het verstrekken van de kopie dient kosteloos te gebeuren. Wil de betrokkene meerdere kopieën van dezelfde persoonsgegevens in hetzelfde verzoek, dan mogen daarvoor redelijke administratiekosten worden gerekend. Deze kosten mogen niet worden gebruikt ter afschrikking van de uitoefening van het recht.

Excessieve verzoeken. Het inzagerecht moet eenvoudig en met redelijke tussenpozen uit te oefenen zijn (overweging 63). Wie al te vaak om kopieën verzoekt, kan daarmee een verwerkingsverantwoordelijke aanzienlijk belasten. In beginsel is dat rechtmatig; de regeling over administratieve kosten moet deze belasting dekken (artikel 12 lid 5 punt a). In theorie zou het excessief opvragen van persoonsgegevens als misbruik van recht kunnen worden geconstrueerd, met name als blijkt dat dit alleen zou gebeuren om de verwerking te frustreren. Dit wordt in de praktijk niet snel aangenomen (Hoge Raad 29 juli 2007, ECLI:NL:HR:2007:AZ4663).

- 15.4 Het in lid 3 bedoelde recht om een kopie te verkrijgen, doet geen afbreuk aan de rechten en vrijheden van anderen.

Een kopie van iemands persoonsgegevens kan aan rechten of vrijheden van anderen raken. Het meest voor de hand liggende voorbeeld is wanneer de kopie ook persoonsgegevens van anderen betreft, zoals bij opvraging van beveiligingscamera-beelden. Deze andere persoonsgegevens zullen dan moeten worden verwijderd of onleesbaar worden gemaakt. Simpelweg om die reden weigeren te verstrekken is niet toegestaan (overweging 63). Een ander voorbeeld is dat de kopie inzicht kan geven in bedrijfsgevoelige gegevens of zou vereisen dat auteursrechtelijk beschermde software wordt meegeleverd. Ook deze grond mag geen reden tot weigering zijn. Een compromis hier kan zijn dat de kopie in een algemeen bekend formaat zoals pdf, XML of Microsoft Excel wordt geleverd, zodat geen software hoeft te worden meegeleverd.

AFDELING 3. RECTIFICATIE EN WISSING VAN GEGEVENS

Afdeling 3 werkt nader uit hoe de betrokkene om kan gaan met onjuiste of achterhaalde gegevens in zijn of haar dossier. Hij kan deze laten rectificeren (artikel 16) of zelfs geheel laten wissen (artikel 17) – ook wel het “recht te worden vergeeten” genoemd. Daarnaast kan de betrokkene een beperking op de verwerking laten leggen (artikel 18). Dit is met name van belang als het enige tijd vergt uit te zoeken of een rectificatie of wissing gepast is.

De verwerkingsverantwoordelijke moet iedere ontvanger van dezelfde persoonsgegevens in kennis stellen van een rectificatie, wissing of beperking (artikel 19). Hiermee ontstaat voor deze anderen dezelfde plicht. Als laatste bepaalt artikel 20 dat wanneer de betrokkene een kopie van zijn persoonsgegevens wenst te ontvangen (zie ook artikel 15) dit in een gestructureerde, gangbare en machinaal leesbare vorm dient te gebeuren.

Artikel 16. Recht op rectificatie

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken.

Wanneer verwerkte persoonsgegevens onjuist of onvolledig zijn, heeft de betrokkene het recht deze te laten corrigeren of aanvullen. Dit artikel is een uitwerking van artikel 5 lid 1 punt d, het beginsel van juistheid van persoonsgegevens. De verwerkingsverantwoordelijke en de verwerker moeten alle redelijke maat-

regelen nemen om ervoor te zorgen dat onjuiste persoonsgegevens worden gecorrigeerd (overweging 39). Het is daarbij irrelevant of de onjuistheid berust op een fout van de verwerkingsverantwoordelijke of verwerker. Ook bijvoorbeeld het aanpassen van iemands naam omdat deze wijzigt na een huwelijk valt onder het recht uit dit artikel.

Evidente fouten. Het recht van rectificatie is bedoeld om evidente fouten of omissies te herstellen bij op eenvoudige en objectieve wijze vast te stellen onjuistheden (Gerechtshof 's-Hertogenbosch 25 mei 2009, ECLI:NL:GHSHE:2009:BI6357). Denk aan het aanpassen van iemands geboortedatum, achternaam of geslacht. Dit recht dient niet om een (extra) inhoudelijke toetsing van het vastgelegde persoonsgegeven af te dwingen. Een student kan bijvoorbeeld een onvoldoende niet laten rectificeren. Meer algemeen is dit recht niet bedoeld om indrukken, meningen, onderzoeksresultaten en conclusies te laten corrigeren (Raad van State 3 februari 2010, ECLI:NL:RVS:2010:BL1852).

Tijdelijke beperking. Als de correctie of aanvulling niet evident is, kan er enige tijd overheen gaan totdat een en ander uitgezocht is. Om problemen te voorkomen, kan de betrokkene dan verlangen dat de verwerking gedurende die tijd wordt beperkt (artikel 18).

Correctie in archieven. Ook persoonsgegevens in archieven dienen te worden gecorrigeerd. Lidstaten kunnen echter nationale wetgeving aannemen om bij archieven in het algemeen belang dit recht te beperken (artikel 89). In Nederland is deze mogelijkheid categorisch uitgesloten in artikel 45 lid 1 Uitvoeringswet. Wanneer correctie technisch niet mogelijk is (zoals bij archieven met papieren bestanden of digitale informatie op niet wijzigbare media) kan worden volstaan met een aanvulling op het archief dat de correctie bevat.

Doorgeven rectificatie. De verwerkingsverantwoordelijke dient iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis te stellen van rectificaties daarop (artikel 19).

Artikel 17. Recht op gegevenswissing (“recht op vergetelheid”)

- 17.1 De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:

Op grond van de beginselen van juistheid (artikel 5 lid 1 punt d) en opslagbeperking (artikel 5 lid 1 punt e) mogen persoonsgegevens niet langer worden bewaard dan nodig is voor het doel van hun verwerking. Het recht van gegevenswissing werkt dit nader uit tot een recht voor de betrokkene om overbodige

persoonsgegevens gewist te krijgen, met corresponderende plicht voor de verwerkingsverantwoordelijke (en uiteraard zijn verwerkers).

Recht te worden vergeten. Bij invoering van de AVG werd gesproken van een ‘recht te worden vergeten’: het recht van gegevenswissing geldt ook bij openbare archieven en internetzoekresultaten. Dit recht kwam met name in de belangstelling na de Costéja-zaak (HvJ EU 13 mei 2014, ECLI:EU:C:2014:317), die zoekmachine Google verplichtte bepaalde persoonsgebonden zoekresultaten op klacht te verwijderen en aldus een ‘recht te worden vergeten’ onder de Richtlijn invoerde. Dit recht staat op gespannen voet met de vrijheid van meningsuiting, en het daarvan afgeleide beginsel dat de integriteit van archieven gewaarborgd moet blijven. Dit artikel 17 kent dan ook diverse waarborgen, met meer algemeen in artikel 23 en 85 nadere mogelijkheden uitwassen te bestrijden.

Kosten. Het uitoefenen van het recht van gegevenswissing dient kosteloos te gebeuren (artikel 12 lid 5).

Wissen. Hoofdregel is dat persoonsgegevens moeten worden gewist, dat wil zeggen dat zij feitelijk niet meer aanwezig zijn. Het is denkbaar dat persoonsgegevens technisch niet of slechts met veel moeite kunnen worden gewist. Denk aan opslag in een papieren archief waarbij individuele regels op een stuk papier gewist zouden moeten worden, of aan grote backup-opslagmedia waarbij één bestand zou moeten worden verwijderd. Waar de Richtlijn in dergelijke gevallen nog het afschermen als optie aandroeg, kent de AVG een dergelijk compromis niet. De verwerkingsverantwoordelijke zal hier dus een oplossing voor moeten vinden.

Zonder onredelijke vertraging. De verwerkingsverantwoordelijke moet een correct verzoek tot wissing zo snel mogelijk, althans zonder onredelijke vertraging afhandelen. Dit zal in beginsel een maand zijn (artikel 12 lid 3).

17.1(a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;

Wanneer persoonsgegevens niet langer nodig zijn voor het doel waarvoor ze zijn verkregen, moeten ze worden gewist. Dit volgt rechtstreeks uit het beginsel van opslagbeperking (artikel 5 lid 1 punt e).

17.1(b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), berust, in, en er is geen andere rechtsgrond voor de verwerking;

Toestemming kan op ieder moment worden ingetrokken (artikel 7 lid 3). Daarmee komt deze verwerkingsgrond te vervallen. De betreffende persoonsgegevens moeten dan worden gewist, tenzij er nog een andere grondslag is onder artikel 6 om de persoonsgegevens te mogen blijven verwerken.

Toestemming als kind. Enigszins overbodig merkt overweging 65 nog op dat dit met name relevant is wanneer de betrokkene toestemming heeft gegeven als kind, toen hij zich nog niet volledig bewust was van de verwerkingsrisico's. Deze toestemming mag dan ook nog worden ingetrokken als men volwassen is. Toestemming intrekken kan echter een ieder te allen tijde doen (artikel 7 lid 3).

Andere rechtsgrond. Geen wissing is nodig als naast toestemming ook een andere grondslag (artikel 6 lid 1) bestaat voor de verwerking. Dit zal met name het eigen gerechtvaardigd belang (artikel 6 lid 1 punt f) zijn, maar ook een wettelijke plicht (artikel 6 lid 1 punt c) kan in voorkomende gevallen een duidelijke rechtsgrond bieden.

17.1(c) de betrokkene maakt overeenkomstig artikel 21, lid 1 bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking overeenkomstig artikel 21, lid 2;

Op grond van artikel 21 kan de betrokkene bezwaar maken tegen een verwerking op grond van een overheidstaak (artikel 6 lid 1 punt e) of het eigen gerechtvaardigd belang (artikel 6 lid 1 punt f). De verwerkingsverantwoordelijke moet dan dwingende gerechtvaardigde gronden voor de verwerking aan kunnen voeren die zwaarder wegen dan het belang van de betrokkene, of anders de verwerking staken en de persoonsgegevens wissen.

Direct marketing. Bij een verwerking voor direct marketing kan te allen tijde bezwaar worden gemaakt, waarna de verwerking moet worden gestaakt (artikel 21 lid 2) en de gegevens worden gewist. Aan een belangenafweging wordt niet toegekomen (artikel 21 lid 3).

17.1(d) de persoonsgegevens zijn onrechtmatig verwerkt;

Persoonsgegevens mogen alleen worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (artikel 5 lid 1 punt a). Blijkt dat persoonsgegevens in strijd met dit beginsel, of meer algemeen de AVG als geheel, worden verwerkt dan dient dat per direct te worden gestaakt. De betrokkene kan echter zich verzetten tegen wissing en in plaats daarvan verzoeken om een beperking (artikel 18 lid 1 punt b), wat met name van belang zal zijn als de persoonsgegevens nodig zijn als bewijs in een gerechtelijke procedure.

17.1(e) de persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

Wanneer een wettelijke bepaling verplicht tot wissing van persoonsgegevens, dient daaraan op verzoek van de betrokkene gehoor te worden gegeven.

17.1(f) de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als bedoeld in artikel 8, lid 1.

Wanneer sprake is van een internetdienst of mobiele telefoniedienst die rechtstreeks aan kinderen wordt aangeboden onder de grondslag toestemming (artikel 8 lid 1), moet een wissingsverzoek altijd worden toegewezen. Voorbeelden zijn het verwijderd krijgen van een sociale media-account of een interesseprofiel bij een op advertenties gebaseerde dienst. Dit verzoek kan ook worden ingediend als de betrokkene inmiddels geen kind meer is (overweging 65).

17.2 Wanneer de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

Wanneer persoonsgegevens moeten worden gewist op grond van lid 1, heeft de verwerkingsverantwoordelijke tevens de taak om andere verwerkingsverantwoordelijken op de hoogte te stellen dat hiervan sprake is.

Redelijke maatregelen. De verwerkingsverantwoordelijke moet redelijke maatregelen nemen, rekening houdend met de beschikbare technologie en de uitvoeringskosten.

Op de hoogte stellen. De plicht van de verwerkingsverantwoordelijke strekt tot op de hoogte stellen. Dit gaat niet zo ver dat hij moet afdwingen dat de persoonsgegevens dienen te worden gewist bij deze andere verwerkingsverantwoordelijken. Een verwerkingsverantwoordelijke die een dergelijk bericht ontvangt, zal echter in veel gevallen zelf tot wissing over moeten gaan omdat een grondslag voor wissing bij één verwerkingsverantwoordelijke in beginsel ook op zal gaan voor iedere andere verwerkingsverantwoordelijke. In de gevallen uit lid 3 is het echter mogelijk dat de andere verwerkingsverantwoordelijke(n) hun verwerking voort mogen zetten, zoals bij een archief in het algemeen belang.

17.3 De leden 1 en 2 zijn niet van toepassing voor zover verwerking nodig is:

Niet in alle gevallen is het wenselijk dat betrokkenen hun persoonsgegevens kunnen doen wissen. Dit lid 3 noemt vijf gevallen. Artikel 23 noemt meer algemeen een aantal situaties waarin de rechten van betrokkenen, en dus ook het recht van wissing, beperkt mogen worden. Verder kunnen lidstaten nadere

wetgeving opvoeren ter bescherming van vrijheid van meningsuiting (artikel 85), toegang tot officiële documenten (artikel 86) en onderzoek en archieven (artikel 89).

17.3(a) voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;

Het wissen van persoonsgegevens kan op gespannen voet staan met de uitingsvrijheid, net als privacy een grondrecht (artikel 10 EVRM). Mede vanwege de discussie over het ‘recht te worden vergeten’ (zie lid 1) is expliciet de mogelijkheid opgenomen dat in voorkomende gevallen een afweging wordt gemaakt tussen het privacybelang van de betrokkene en het uitings- of informatiebelang van de verwerkingsverantwoordelijke en anderen. In Nederland geldt het vergeetrecht, net als de overige rechten van betrokkenen, niet bij uitingen voor journalistieke, academische, artistieke of literaire verwerkingen (artikel 43 lid 2 punt b Uitvoeringswet). Zo oordeelde het Nederlandse gerechtshof dat een website met publicaties over oplichtingspraktijken de informatie over een fraudeur niet hoefde te verwijderen naar aanleiding van een verzoek tot gegevenswissing, omdat die publicaties een journalistiek doel hebben (Gerechtshof Amsterdam 25 oktober 2022, ECLI:NL:GHAMS:2022:3023). Zie ook artikel 85.

17.3(b) voor het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;

Wanneer een wettelijke plicht de verwerking vereist, is het niet mogelijk tot wissing van de betreffende gegevens te verzoeken. Denk bijvoorbeeld aan de wettelijke plicht gegevens die relevant zijn voor de belasting zeven jaar lang te bewaren. Ook bij verwerkingen in het algemeen belang of verwerkingen door of vanwege het openbaar gezag kan geen gegevenswissing worden verlangd. Zie ook artikel 86.

17.3(c) om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9, lid 2, punten h) en i), en artikel 9, lid 3;

Wanneer sprake is van een algemeen belang op het gebied van de volksgezondheid (zie artikel 9 lid 2 punten h en i) kan ook geen gegevenswissing worden verlangd. Dit algemeen belang zal er met name in zitten dat instanties op dit gebied volledige informatie moeten hebben over gezondheid, ontwikkeling en verspreiding van ziektes en dergelijke.

17.3(d) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, voor zover het in lid 1 bedoelde recht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;

Bij openbare archieven (zoals rijksarchieven) is het niet wenselijk dat betrokkenen hun gegevens laten wissen. Dit zou de integriteit van deze archieven aantasten, en gezien het belang van deze archieven is dat onacceptabel. Zeker in het kader van openbaarheid van bestuur in een steeds meer digitaliserende wereld waarin gegevens gemakkelijk aan te passen zijn, is die integriteit zeer relevant. Vergelijk Raad van State 8 september 2010, ECLI:NL:RVS:2010:BN6172 en meer algemeen EHRM 10 maart 2009, ECLI:EU:C:2011:255 (Times) en EHRM 16 juli 2013, zaaknr. 33846/07, Wegrzynowski).

Ook bij wetenschappelijk, historisch of statistisch onderzoek is het niet wenselijk dat betrokkenen hun persoonsgegevens wissen, aangezien dit de betrouwbaarheid of herhaalbaarheid van het onderzoek aantast. Dit raakt aan de fundamenteën van goed onderzoek. Zie nader artikel 89 over deze problematiek. Het recht van bezwaar (artikel 21) biedt afhankelijk van de omstandigheden mogelijk wel een grond om een verwerking gestaakt te krijgen.

17.3(e) voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Wanneer een partij een rechtsvordering wil instellen (al dan niet tegen de betrokkene), dan kunnen daar persoonsgegevens bij nodig zijn. Denk aan het opvoeren van bewijs dat een persoon iets gezegd of gedaan heeft. Wanneer dit gebeurt, is het onwenselijk en dus niet toegestaan dat de betrokkene deze persoonsgegevens zou kunnen wissen. Dit geldt ook indien de persoonsgegevens onrechtmatig verwerkt zijn, gezien het belang dat de waarheid boven tafel komt bij een rechtszaak. De rechter mag dergelijk bewijs natuurlijk waarderen zoals het hem voorkomt (artikel 152 lid 2 Wetboek van Burgerlijke Rechtsvordering (Rv)). Zie bijvoorbeeld Gerechtshof Arnhem 24 mei 2011, ECLI:NL:GHAMS:2011:BR1260.

Artikel 18. Recht op beperking van de verwerking

18.1 De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen indien een van de volgende elementen van toepassing is:

Een nieuw recht onder de AVG is het recht op beperking. Beperking is enigszins circulair gedefinieerd (artikel 4 definitie 3) als het markeren van opgeslagen

persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken. Kort gezegd komt het erop neer dat men een tijdelijk slot op de persoonsgegevens wil totdat een bezwaar of probleem is opgelost. Er zijn vier situaties waarin men een beperking kan verlangen.

Ook bij verwerker. De rechten c en d hieronder zijn geschreven tegen de verwerkingsverantwoordelijke, maar gelden onverkort wanneer de verwerking feitelijk door een verwerker plaatsvindt. Artikel 28 verplicht de verwerkingsverantwoordelijke immers te regelen dat de verwerker de AVG nakomt en de rechten van de betrokkene waarborgt.

- 18.1(a) de juistheid van de persoonsgegevens door de betrokkene wordt betwist, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren;

De eerste situatie waarin een beperking op zijn plaats is, is wanneer de betrokkene betwist dat de persoonsgegevens juist zijn. Het is dan wenselijk deze tijdelijk niet te gebruiken, om schade te voorkomen door het gebruik van onjuiste persoonsgegevens. In beginsel zal dit recht worden ingeroepen bij een verzoek tot rectificatie (artikel 16).

- 18.1(b) de verwerking onrechtmatig is en de betrokkene zich tegen het wissen van de persoonsgegevens verzet en in de plaats daarvan om beperking van het gebruik ervan verzoekt;

De tweede situatie waarin een beperking kan worden geëist, is wanneer een verwerking onrechtmatig is gebleken maar de betrokkene niet wil dat deze volledig worden gewist (artikel 17). De betrokkene kan er bijvoorbeeld belang bij hebben dat zijn gegevens op een zwarte lijst blijven staan om hernieuwde verwerking te voorkomen.

- 18.1(c) de verwerkingsverantwoordelijke de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene deze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;

Een derde situatie waarin de betrokkene beperking kan verlangen, is waarin de betrokkene een rechtsvordering wil instellen, uitoefenen of onderbouwen en daarbij de betreffende persoonsgegevens nodig heeft. Het is dan niet wenselijk dat de verwerkingsverantwoordelijke de persoonsgegevens wist (wissen is een vorm van verwerking) voordat over de rechtsvordering is beslist. In Nederland zou zo'n rechtsvordering bijvoorbeeld op grond van de exhibitieplicht uit artikel 843a Rv kunnen worden ingesteld. Ook bij een aangifte tegen de verwerkingsverantwoordelijke zou dit recht van beperking nuttig kunnen zijn ter behoud van bewijs.

18.1(d) de betrokkene overeenkomstig artikel 21, lid 1, bezwaar heeft gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

De vierde en laatste situatie waarin de betrokkene een beperking kan verlangen is wanneer er bezwaar is gemaakt (zie artikel 21) en de verwerkingsverantwoordelijke niet onmiddellijk beslist op het bezwaar. Om te voorkomen dat de verwerking wordt voortgezet en achteraf blijkt dat dit gezien het bezwaar niet had gemogen, kan de betrokkene beperking daarvan verlangen.

18.2 Wanneer de verwerking op grond van lid 1 is beperkt, worden persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.

Als een verzoek om beperking is ontvangen dat voldoet aan lid 1, dan moet de verwerkingsverantwoordelijke iedere verwerking staken (en zorgen dat de eventuele verwerker dit ook doet). Er zijn slechts vier soorten verwerking die nog mogen worden voortgezet.

- Toestemming
- Rechtsvordering
- Rechten van anderen
- Gewichtige redenen van algemeen belang

Opslag. Het is ondanks een beperking toegestaan persoonsgegevens op te slaan. Dit is niet meer dan logisch, omdat het altijd mogelijk is dat een beperking opgeheven wordt zonder dat de persoonsgegevens moeten worden gewist of vernietigd.

Toestemming. Een beperking kan slechts worden gepasseerd met toestemming (artikel 4 definitie 11) van de betrokkene. Deze toestemming moet specifiek gericht zijn op het passeren van de beperking en moet dus apart en wel na het instellen van de beperking worden verkregen.

Rechtsvordering, rechten of gewichtige redenen. Wanneer de verwerkingsverantwoordelijke de persoonsgegevens nodig heeft voor een rechtsvordering (bijvoorbeeld tegen de betrokkene) of ter bescherming van de rechten van een ander of meer algemeen “gewichtige redenen”, mag de verwerkingsverantwoordelijke de persoonsgegevens voor dit doel verwerken. De bewijslast dat hiervan sprake is, ligt bij de verwerkingsverantwoordelijke (artikel 5 lid 2). Deze moet dus gemotiveerd stellen waarom hiervan sprake is.

- 18.3 Een betrokkene die overeenkomstig lid 1 een beperking van de verwerking heeft verkregen, wordt door de verwerkingsverantwoordelijke op de hoogte gebracht voordat de beperking van de verwerking wordt opgeheven.

De verwerkingsverantwoordelijke heeft de plicht de betrokkene op de hoogte te brengen van het voornemen de beperking op te heffen, bijvoorbeeld omdat het bezwaar (artikel 21) is afgewezen of omdat na onderzoek de gegevens toch juist zijn gebleken. Op die manier kan de betrokkene, als die het oneens is met dit voornemen, nog tijdig een klacht bij de toezichthouder (artikel 77) of een voorziening in rechte in te stellen tegen de verwerkingsverantwoordelijke (artikel 79).

Artikel 19. Kennisgevingsplicht inzake rectificatie, wissing of beperking

De verwerkingsverantwoordelijke stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie of wissing van persoonsgegevens of beperking van de verwerking overeenkomstig artikel 16, artikel 17, lid 1, en artikel 18, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

Wanneer de verwerkingsverantwoordelijke een rectificatie (artikel 16), gegevenswissing (artikel 17 lid 1) of beperking (artikel 18) op persoonsgegevens van een betrokkene uitvoert, is hij verplicht alle ontvangers van die persoonsgegevens hierover in te lichten. Doel van deze kennisgeving is dat deze ontvangers vervolgens de betreffende rectificatie, wissing of beperking ook doorvoeren.

Ontvanger. Een ontvanger is (artikel 4 definitie 9) iedere natuurlijke persoon of rechtspersoon (maar ook overheidsinstanties) die persoonsgegevens ontvangt van de verwerkingsverantwoordelijke. Dit betreft naast derden (artikel 4 definitie 10) ook verwerkers en partijen die onder rechtstreeks gezag van verwerkingsverantwoordelijke of verwerker opereren.

Informatieverstrekking. De verwerkingsverantwoordelijke moet de betrokkene op diens verzoek melden om welke ontvangers het gaat. Dit zal naast de naam ook contactinformatie betreffen, zodat de betrokkene bij deze ontvangers terecht kan om na te gaan of dit correct is uitgevoerd of om aanvullende verzoeken te doen (zoals wissing bij een door hem ongewenste ontvanger). Specifiek bij wissing geldt een aanvullende informatieplicht voor de verwerkingsverantwoordelijke (zie artikel 17 lid 2).

Onmogelijk of onevenredig. De kennisgeving hoeft niet te worden gedaan als dit onmogelijk is (bijvoorbeeld omdat de betreffende informatie niet meer aanwezig is) of als dit onevenredig veel inspanning vergt. De evenredigheid zal worden afgewogen via de grootte van het belang dat de betrokkene zal hebben bij de

kennisgeving aan de ontvanger. Dit kan onder meer volgen uit de aard van de gegevens: een rectificatie op strafrechtelijke gegevens vereist meer inspanning dan een typfout in een verouderd huisadres.

Voortgang. De kennisgeving zelf dient zo snel als redelijkerwijs mogelijk uitgevoerd te worden vanuit het beginsel van juistheid (artikel 5 lid 1 punt d). De verwerkingsverantwoordelijke moet de betrokkene onverwijld informeren over het gevolg dat is gegeven aan zijn verzoek over informatie (artikel 12 lid 3).

Artikel 20. Recht op overdraagbaarheid van gegevens

20.1 De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt, [...] indien:

Naast het al langer bekende recht van inzage in persoonsgegevens (artikel 15 lid 3) introduceert de AVG een nieuw recht, namelijk dat van dataportabiliteit oftewel overdraagbaarheid van gegevens. Hiermee kan de betrokkene een kopie van zijn persoonsgegevens eisen die bruikbaar is bij een andere dienstverlener. Een voorbeeld is een Facebook-profiel, dat men dan kan overzetten naar de concurrent Diaspora.

Gestructureerde, gangbare en machinaal leesbare vorm. Dataportabiliteit is alleen mogelijk als de persoonsgegevens op een manier worden verstrekt waarmee anderen kunnen werken. Gestructureerd wil hier zeggen dat de persoonsgegevens los van elkaar te verwerken zijn. Gangbaar wil zeggen dat het technisch formaat bekend is bij de markt, en machinaal leesbaar wil zeggen dat het overnemen van de persoonsgegevens zonder menselijke tussenkomst mogelijk is. Een simpel voorbeeld zou zijn om de persoonsgegevens in een Excel-bestand aan te leveren. Dergelijke bestanden zijn door iedereen te maken en te lezen op een gestructureerde en geautomatiseerde manier. De betrokkene moet de gegevens zelf kunnen downloaden en niet afhankelijk zijn van de medewerking van de helpdesk, aldus de *Richtsnoeren inzake het recht op gegevensoverdraagbaarheid* (WP 242, editie 5 april 2017) van de Artikel 29-Werkgroep. Een verzoek moeten indienen bij de verwerkingsverantwoordelijke is dus niet genoeg.

Alleen brongegevens. De Richtsnoeren inzake het recht op gegevensoverdraagbaarheid (WP 242, editie 5 april 2017) van de Artikel 29-Werkgroep maken duidelijk dat het recht beperkt is tot brongegevens, oftewel persoonsgegevens die door de betrokkene zijn verstrekt, zowel actief als passief. Voorbeelden van actieve verstrekking zijn ingevulde formulieren of online ingestuurde aanvragen of pasfoto's. Onder passieve verstrekking wordt onder meer verstaan het loggen

(meten) van bezoek van een webwinkel, het uitlezen van een meter of het middels een app verkrijgen van informatie van een telefoon. Persoonsgegevens die zijn “gededuceerd en afgeleid” vallen buiten het recht. De interesseprofielen afgeleid uit bezoekgedrag vallen dus niet onder dit recht. Wel zal hier het algemene inzagerecht (artikel 15) op gelden.

Interoperabiliteit. Overweging 68 noemt nog de eis van interoperabiliteit, wat zo veel wil zeggen als dat verschillende verwerkingsverantwoordelijken elkaars persoonsgegevens technisch kunnen verwerken. Op dit moment zijn er eigenlijk geen standaarden voor formaten waarmee dit mogelijk is. De overweging moedigt dan ook verwerkingsverantwoordelijken aan dergelijke interoperabele formaten te ontwikkelen die gegevensoverdraagbaarheid mogelijk maken, maar zegt tegelijkertijd dat er geen verplichting is om technisch compatibele systemen voor gegevensverwerking op te zetten of te houden.

Zonder hinder. De verwerkingsverantwoordelijke mag de betrokkene niet hinderen bij het uitoefenen van dit recht. Hij kan dus niet bijvoorbeeld eisen dat een geheimhoudingsverklaring wordt getekend, verbieden dat naar concurrent X wordt overgestapt of rechten van intellectuele eigendom (zoals auteursrecht of databankrecht) claimen op de verstrekte persoonsgegevens. Ook niet toegestaan zijn meer indirecte vormen van hinder, zoals een bestandsformaat dat alleen onder licentie van de verwerkingsverantwoordelijke gebruikt kan worden. De verstrekking moet kosteloos gebeuren (artikel 12 lid 5).

Hem betreffende persoonsgegevens. Enkel persoonsgegevens gerelateerd aan de betrokkene vallen binnen de toepassing van het recht op dataportabiliteit. Het begrip ‘betreffende’ dient, aldus de Richtsnoeren, breed te worden opgevat. Zo omvat het begrip zowel persoonsgegevens van de betrokkene zelf, als gepseudonimiseerde gegevens en gegevens van derden die aan de betrokkene kunnen worden gelinkt. Voorwaarde hiervoor is wel, dat er een link bestaat tussen de betrokkene en de gepseudonimiseerde gegevens (zoals door het verschaffen van aanvullende gegevens in de zin van art. 11 lid 2) en de gegevens van derden.

20.1(a) de verwerking berust op toestemming uit hoofde van artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), of op een overeenkomst uit hoofde van artikel 6, lid 1, punt b); en

Het recht van dataportabiliteit kan alleen worden uitgeoefend wanneer de persoonsgegevens krachtens toestemming (art. 6 lid 1 punt a voor gewone en art. 9 lid 2 punt a voor bijzondere persoonsgegevens) of krachtens uitvoering overeenkomst (art. 6 lid 1 punt b) worden verwerkt. Wanneer een verwerkingsverantwoordelijke bijvoorbeeld persoonsgegevens verwerkt krachtens een eigen gerechtvaardigd belang (art. 6 lid 1 punt f), bestaat dus geen recht van dataportabiliteit. Wel kan de betrokkene dan een kopie verlangen onder artikel 15 lid 3 in het kader van het algemene inzagerecht, maar deze kopie hoeft niet in een gestructureerde, gangbare en machinaal leesbare vorm te zijn.

20.1(b) de verwerking via geautomatiseerde procedés wordt verricht.

Het recht van dataportabiliteit bestaat alleen bij verwerkingen door geautomatiseerde procedés, oftewel de geheel geautomatiseerde verwerking bedoeld in artikel 4, definitie 2.

20.2 Bij de uitoefening van zijn recht op gegevensoverdraagbaarheid uit hoofde van lid 1 heeft de betrokkene het recht dat de persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere worden doorgezonden.

De hoofdregel uit lid 1 bepaalt dat de betrokkene het recht heeft de persoonsgegevens te ontvangen. Omdat het vaak zal gaan om zeer grote gegevensverzamelingen en dit recht vrijwel altijd zal worden uitgeoefend teneinde de persoonsgegevens elders te gebruiken, bepaalt lid 2 dat het recht mede inhoudt te verlangen dat de gegevens rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere worden doorgezonden. Dit vergemakkelijkt de uitoefening van dit recht door de betrokkene.

Technische haalbaarheid. Aangezien dit proces geautomatiseerd moet worden uitgevoerd, en het niet te verwachten is dat verwerkingsverantwoordelijken vergelijkbare systemen gebruiken, is het geen gegeven dat deze rechtstreekse doorzending technisch haalbaar is. Er is geen verplichting om technisch compatibele systemen voor gegevensverwerking op te zetten of te houden (overweging 68).

20.3 De uitoefening van het in lid 1 van dit artikel bedoelde recht laat artikel 17 onverlet. Dat recht geldt niet voor de verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend.

Gegevenswissing na data-export. Wie een kopie van zijn gegevens opvraagt bij een verwerkingsverantwoordelijke, kan daarna nog steeds zijn recht van gegevenswissing (artikel 17) uitoefenen. Daar staat tegenover dat een verwerkingsverantwoordelijke niet mag besluiten (overweging 68) de gegevens te wissen nadat de betrokkene het recht van dataportabiliteit uitoefent, althans wanneer het gaat om een verwerking ter uitvoering van een overeenkomst (artikel 6 lid 1 punt b). Een verwerkingsverantwoordelijke zou bij verwerking op grond van toestemming (artikel 6 lid 1 punt a) dus wél kunnen zeggen dat uitoefening van dit recht met zich meebrengt dat de gegevens bij hem worden gewist.

Algemeen belang of openbaar gezag. Het recht van dataportabiliteit geldt niet voor persoonsgegevens die worden verwerkt bij een taak van algemeen belang of openbaar gezag (artikel 6 lid 1 punt e). De aard van het recht is immers dat men van de ene naar de andere verwerkingsverantwoordelijke kan overstappen,

iets dat bij dergelijke verwerkingen niet aan de orde is. Dit is enigszins overbodig bepaald nu lid 1 het recht al beperkt tot gebruik onder de grondslagen toestemming of uitvoering overeenkomst.

20.4 Het in lid 1 bedoelde recht doet geen afbreuk aan de rechten en vrijheden van anderen.

Rechten en vrijheden. De in lid 1 op te vragen persoonsgegevens kunnen ook raken aan fundamentele rechten en vrijheden van anderen. Voorbeelden zijn een foto waar meerdere personen op staan, of een interne notitie met persoonlijke opvattingen van een manager in een digitaal personeelsdossier. Ook rechten van intellectuele eigendom, bedrijfsgeheimen en rechten van personen op basis van de AVG vallen hieronder. Persoonsgegevens kunnen zijn vervat in auteursrechtelijk beschermde werken, zoals bij een disco of club die online foto's van bezoekers publiceert welke door een ingehuurd fotograaf zijn gemaakt. Via dataportabiliteit opvragen van die foto en deze 'zonder hinder' willen gebruiken, botst dan met het auteursrecht van de fotograaf.

Proportionaliteit en subsidiariteit. Een weigering persoonsgegevens te verstrekken op grond van lid 4 gaat erg ver en kan worden geconstrueerd als een inbreuk op het recht van bescherming van persoonsgegevens (artikel 1 lid 2). Het ligt dan ook voor de hand dat weigering slechts mag als er geen enkele manier is om de gegevens te verstrekken zonder de rechten van anderen te raken. Wanneer het bijvoorbeeld mogelijk is gegevens van anderen weg te laten (zoals middels het uitblurren van gezichten of weglaten van beschermde informatie), dan is weigering geen optie. Bij het algemene inzagerecht (artikel 15) is in dezelfde situatie bepaald dat het bestaan van deze rechten niet ertoe mag leiden dat de betrokkene alle informatie wordt onthouden.

Administratieve lasten. Administratieve lasten en daarmee gepaard gaande kosten voor de verwerkingsverantwoordelijke zijn in theorie te zien als een inbreuk op "rechten en vrijheden van anderen", omdat de verwerkingsverantwoordelijke een 'andere' is in de zin van dit lid. Gezien de aard van het recht op dataportabiliteit en het feit dat dit recht kosteloos moet kunnen worden uitgeoefend (artikel 12 lid 5) ligt het niet in de rede dat een verwerkingsverantwoordelijke zich snel kan beroepen op administratieve lasten om een verzoek te weigeren.

AFDELING 4. RECHT VAN BEZWAAR EN GEAUTOMATISEERDE INDIVIDUELE BESLUITVORMING

In afdeling 4 worden twee rechten uitgewerkt: het recht bezwaar te maken tegen een verwerking op grond van algemeen belang of een gerechtvaardigd eigen belang (artikel 21) en het recht niet onderworpen te worden aan geautomatiseerde besluitvorming (artikel 22). Het recht van bezwaar is bedoeld om een heroverweging vanuit persoonlijke gronden te kunnen afdwingen. Geautomatiseerde

besluitvorming kan eveneens problematisch zijn, zodat daartegen maatregelen moeten worden genomen.

Artikel 21. Recht van bezwaar

21.1 De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens op basis van artikel 6, lid 1, onder e) of f), met inbegrip van profilering op basis van die bepalingen. De verwerkingsverantwoordelijke staakt de verwerking van de persoonsgegevens tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

Wanneer een verwerkingsverantwoordelijke zich beroept op de grondslag “taak van algemeen belang” (artikel 6 lid 1 punt e) of “gerechtvaardigd eigen belang” (punt f), dient deze een belangenafweging uit te voeren ten aanzien van de privacy van betrokkenen. Deze belangenafweging zal naar zijn aard een abstracte zijn. Een betrokkene kan echter in een specifieke situatie anders tegen deze afweging aankijken. Het recht van bezwaar geeft hem de mogelijkheid van de verwerkingsverantwoordelijke te verlangen dat deze de afweging nogmaals maakt met de specifieke situatie in het achterhoofd.

Specifieke situatie. Het bezwaar moet gebaseerd zijn op de specifieke situatie van de betrokkene. Hij mag dus niet volstaan met algemene of principiële bezwaren tegen verwerking van zijn gegevens, maar moet specifieke omstandigheden aandragen. Een voorbeeld zou zijn dat een medewerker in een rolstoel bezwaar maakt tegen een vertoning van camerabeelden waar gezichten zijn uitgeblurd; in zijn specifieke situatie is hij dan immers nog steeds herkenbaar.

Staken verwerking na bezwaar. Wanneer een verwerkingsverantwoordelijke een bezwaar ontvangt, dient hij in beginsel de verwerking te staken. Een bezwaar mag slechts worden gepasseerd als de verwerkingsverantwoordelijke kan aantonen dat zijn dwingende gerechtvaardigde belangen zwaarder wegen dan de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene. Dit is een hoge lat.

Geen bezwaar bij toestemming. Wanneer een verwerking is gebaseerd op de grondslag toestemming (artikel 6 lid 1 punt a) is bezwaar maken niet mogelijk. Het is ook niet nodig: de betrokkene heeft het recht zijn toestemming te allen tijde in te trekken (artikel 7 lid 3). Hij hoeft daarbij geen redenen op te geven.

- 21.2 Wanneer persoonsgegevens ten behoeve van direct marketing worden verwerkt, heeft de betrokkene te allen tijde het recht bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens voor dergelijke marketing, met inbegrip van profilering die betrekking heeft op direct marketing.

Bij verwerkingen voor het doel direct marketing (het via gerichte communicatie persoonlijk benaderen van personen) geldt in afwijking van lid 1 dat het bezwaar te allen tijde gevolgd moet worden. Specifieke omstandigheden zoals in lid 1 hoeven niet te worden gesteld.

- 21.3 Wanneer de betrokkene bezwaar maakt tegen verwerking ten behoeve van direct marketing, worden de persoonsgegevens niet meer voor deze doeleinden verwerkt.

Lid 3 bevestigt lid 2: de verwerking voor direct marketing dient te worden gestaakt. Uiteraard kunnen de persoonsgegevens eventueel nog wel voor andere doeleinden (zoals het leveren van een bestelling of het sturen van een nieuwsbrief met aparte toestemming) worden gebruikt.

- 21.4 Het in de leden 1 en 2 bedoelde recht wordt uiterlijk op het moment van het eerste contact met de betrokkene uitdrukkelijk onder de aandacht van de betrokkene gebracht en duidelijk en gescheiden van enige andere informatie weergegeven.

Om de betrokkene te informeren over dit recht van bezwaar, dient de verwerkingsverantwoordelijke dit expliciet aan hen te melden. Deze informatie moet uitdrukkelijk en apart gebeuren.

Uitdrukkelijk. Dit dient uitdrukkelijk te gebeuren, dus niet iets dat men tussen de regels door moet concluderen. Zie ook wat hierover wordt gezegd bij toestemming (artikel 4, definitie 11).

Gescheiden. De melding moet gescheiden van andere informatie gebeuren, dus niet bijvoorbeeld slechts in de privacyverklaring.

- 21.5 In het kader van het gebruik van diensten van de informatiemaatschappij, en niettegenstaande Richtlijn 2002/58/EG, mag de betrokkene zijn recht van bezwaar uitoefenen via geautomatiseerde procedés waarbij wordt gebruikgemaakt van technische specificaties.

Bij internetdiensten (zie artikel 4, definitie 25) is het vereist dat betrokkenen geautomatiseerd bezwaar kunnen maken. Zij mogen dus niet enkel via brieven of contact met een helpdesk dit recht kunnen uitoefenen.

Geautomatiseerde procedés. Een geautomatiseerd procedé is iedere manier om zonder menselijke tussenkomst een bezwaar te effectueren. Een manier om dit te realiseren is een beheerscherm voor persoonlijke instellingen, waar men vinkjes kan plaatsen of weghalen. Men kan de betrokkene een menu met enkele veel voorkomende specifieke situaties bieden waar men zich op kan beroepen.

Richtlijn 2002/58/EG. De E-privacyrichtlijn (2002/58/EG) kent geen recht van bezwaar, vandaar dat de AVG hier bepaalt dat het recht van bezwaar niet-tengestaande deze Richtlijn bestaat. Ook de aangekondigde vervanger van de E-privacyrichtlijn kent een dergelijk bezwaar niet.

21.6 Wanneer persoonsgegevens overeenkomstig artikel 89, lid 1, met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, heeft de betrokkene het recht om met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

Ook wanneer persoonsgegevens worden verwerkt voor onderzoek kan de betrokkene bezwaar maken op grond van zijn specifieke situatie. Dit bezwaar moet ook te allen tijde worden toegewezen, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang. Daarvan kan alleen sprake zijn (overweging 45) als die taak is uitgewerkt in een wettelijke regeling. Zie over onderzoek nader artikel 89.

Artikel 22. Geautomatiseerde individuele besluitvorming, waaronder profilering

22.1. De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

Steeds meer besluitvorming (zowel civiel- als bestuursrechtelijk) wordt geautomatiseerd, waarbij de uitkomst van een computeranalyse ook steeds zwaarder is in die besluitvorming. Persoonsgegevens van de betrokkene (zoals de consument die iets wil kopen) kunnen in dat besluitvormingsproces worden betrokken. Dit individualiseert de besluitvorming, met mogelijk negatieve effecten voor de betrokkene. Vanuit het beginsel van rechtmatigheid, behoorlijkheid en transparantie (artikel 5 lid 1 punt a) dienen hier waarborgen tegen te zijn opgenomen. Zie nader de *Richtsnoeren voor geautomatiseerde beslissingen en profilering* van de Artikel 29-Werkgroep, 3 oktober 2017 (WP251). Let op dat het hier gaat om een “uitsluitend” op geautomatiseerde verwerking gebaseerd besluit. Dat betekent dus niet dat geautomatiseerde verwerkingen, waaronder profilering, geen onderdeel van een proces kunnen zijn.

Profileren. Van profileren is sprake (artikel 4 definitie 4) wanneer langs geautomatiseerde weg bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd om zo voorspellingen te kunnen doen over bijvoorbeeld iemands economische situatie, persoonlijke voorkeuren of gedrag. Profileren an sich is toegestaan, zij het dat een bezwaar (artikel 21) hiertegen al snel toegewezen zal worden. Op basis van een dergelijke evaluatie een besluit over iemand nemen loopt echter in beginsel altijd tegen dit artikel 22 aan. Het Comité kan richtsnoeren opstellen over profileren (artikel 70 lid 1 punt f).

Rechtsgevolgen of aanzienlijk treffen. Het verbod op geautomatiseerde besluitvorming raakt allereerst de besluiten met rechtsgevolgen, zoals besluiten onder de Algemene wet bestuursrecht of een verplichting als consument een online aankoop vooruit te betalen. Een besluit kan echter ook zonder directe rechtsgevolgen iemand treffen. Voorbeeld is de weigering een koopovereenkomst te sluiten of iemand een sollicitatiegesprek ontzeggen.

Individuele besluitvorming. Het moet gaan om een besluit dat individueel is voor de betrokkene. De vaststelling van de WOZ-waarde van een woonhuis gebeurt bijvoorbeeld niet op basis van persoonsgegevens van de eigenaar. Dit besluit valt dus buiten de reikwijdte van dit artikel.

Informatieplicht. Wordt gewerkt met geautomatiseerde besluitvorming, dan moet de betrokkene actief daarover worden geïnformeerd (artikel 13 lid 2 punt f en artikel 14 lid 2 punt g), met in ieder geval nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene. Deze informatie moet ook worden verstrekt op verzoek (artikel 15 lid 1 punt h).

Gegevensbeschermingseffectbeoordeling. Wanneer de geautomatiseerde beoordeling systematisch en uitgebreid is, dient een gegevensbeschermingseffectbeoordeling te zijn uitgevoerd (artikel 35). Een gegevensbeschermingseffectbeoordeling is meer bekend onder zijn Engelse naam, namelijk *data protection impact assessment (DPIA)*.

22.2 Lid 1 geldt niet indien het besluit:

Vanwege de impact die geautomatiseerde besluitvorming kunnen hebben, is de hoofdregel (lid 1) dat dit niet toegestaan is. Dit lid 2 noemt drie uitzonderingssituaties, waarbij lid 3 passende waarborgen vereist wanneer deze situaties opgaan.

Kinderen. Overweging 71 merkt op dat kinderen nimmer mogen worden onderworpen aan geautomatiseerde besluitvorming, dus ook niet in de gevallen in dit lid 2 genoemd.

22.2(a) noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;

De eerste en belangrijkste uitzondering is wanneer het besluit noodzakelijk is bij de sluiting of uitvoering van een overeenkomst (vergelijk artikel 6 lid 1 punt b dat ditzelfde criterium hanteert als grondslag voor verwerking). Hieronder vallen tevens maatregelen die dienen ter handhaving van de veiligheid en betrouwbaarheid van een dienst die door de verwerkingsverantwoordelijke wordt verleend. Een automatisch proces bij een internetprovider dat internetverkeer analyseert om na te gaan of klanten gehackt zijn en ze voor de zekerheid afsluit van internet zou dus onder dit punt a toegestaan zijn.

22.2(b) is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of

Een Europese of nationale wet mag een uitzondering creëren, mits deze wet daarbij voorziet in passende maatregelen om de betrokkene te beschermen. Deze maatregelen zullen gewoonlijk aansluiten bij wat in lid 3 wordt vereist. In Nederland stelt de Uitvoeringswet als aanvullende eisen dat zo'n wettelijke verplichting noodzakelijk is voor de uitvoering van een taak van algemeen belang, en dat de verwerkingsverantwoordelijke passende maatregelen neemt ter bescherming van de gerechtvaardigde belangen van de betrokkene. Daarnaast dient aan de betrokkene de logica te worden meegedeeld, welke ten grondslag ligt aan de geautomatiseerde gegevensverwerking (artikel 40 Uitvoeringswet).

22.2(c) berust op de uitdrukkelijke toestemming van de betrokkene.

Als derde uitzonderingsgrond geldt dat een besluit wel uitsluitend geautomatiseerd mag worden genomen wanneer de betrokkene daar toestemming voor heeft gegeven. Deze toestemming moet uitdrukkelijk worden gegeven (vergelijk artikel 9 lid 2 punt a) en kan te allen tijde worden ingetrokken (artikel 7 lid 3). Een bedrijf zou bijvoorbeeld een snelle geautomatiseerde afhandeling van verzoeken kunnen aanbieden tegenover een langzamere handmatige afhandeling. Wie dan toestemming geeft voor de snelle route, kan dan geen bezwaar meer maken tegen het geautomatiseerd karakter van de afhandeling.

- 22.3 In de in lid 2, punten a) en c), bedoelde gevallen treft de verwerkingsverantwoordelijke passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.

Wanneer besluitvorming geautomatiseerd wordt, dient te worden voorkomen dat de betrokkene met lege handen staat wanneer een besluit onjuist of onrechtvaardig blijkt. Hiertoe dient de verwerkingsverantwoordelijke passende maatregelen te nemen, zoals in dit lid 3 nader uitgewerkt. In het geval b (wettelijke regeling) van lid 2 zijn de passende maatregelen reeds daar vereist. Vergelijk daarbij artikel 4:7 Algemene wet bestuursrecht.

Menselijke tussenkomst. Het belang dat centraal staat in lid 1 is dat de computer niet de mens vervangt. Het besluit genomen onder lid 2 punt a (uitvoering overeenkomst) of punt c (uitdrukkelijke toestemming) vereist dus een mogelijkheid een mens te betrekken bij de uitkomst. Dit betekent niet dat het besluit niet automatisch genomen mag worden, of dat een conceptbesluit altijd eerst gezien moet worden door een mens, maar wel dat de betrokkene een mens aan de mouw moet kunnen trekken om te kunnen reageren op het besluit.

Standpunt kenbaar maken. In ieder geval moet de betrokkene in staat worden gesteld zijn standpunt ten aanzien van het besluit kenbaar te maken. De verwerkingsverantwoordelijke moet hierop reageren.

Besluit aanvechten. De betrokkene moet tevens in staat zijn het geautomatiseerde besluit aan te vechten. Dit vereist niet per se een formele bezwaar- en beroepscommissie, maar wel enige reële procedure met reële kans op een herziening van het besluit. Vergelijk de bezwaarregeling uit artikel 21.

Passende maatregelen. Vanuit de algemene zorgplicht van de verwerkingsverantwoordelijke (artikel 24 lid 1) dient deze bij geautomatiseerde besluitvorming in het bijzonder passende maatregelen te nemen om foute besluiten te voorkomen. Overweging 71 noemt als voorbeelden het hanteren van wiskundige en statistische procedures waarmee factoren die aanleiding geven tot onjuistheden van persoonsgegevens worden gecorrigeerd en het risico op fouten wordt geminimaliseerd, en het zodanig bewaren van persoonsgegevens dat rekening wordt gehouden met de potentiële risico's voor de belangen en rechten van de betrokkene.

- 22.4 De in lid 2 bedoelde besluiten worden niet gebaseerd op de in artikel 9, lid 1, bedoelde bijzondere categorieën van persoonsgegevens, tenzij artikel 9, lid 2, punt a) of g), van toepassing is en er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene zijn getroffen.

Het is niet toegestaan om bijzondere persoonsgegevens (artikel 9 lid 1) te gebruiken in geautomatiseerde besluitvorming. Uitzondering geldt alleen bij uitdrukkelijke toestemming (artikel 9 lid 2 punt a, vergelijk hierboven lid 2 punt c) of bij een besluit in het algemeen belang (artikel 9 lid 2 punt g, vergelijk hierboven lid 2 punt b). In die twee gevallen is het wel toegestaan de bijzondere persoonsgegevens te betrekken, mits passende maatregelen zijn genomen om de belangen van de betrokkene te beschermen. Deze maatregelen zullen overeenkomen met het in lid 3 bepaalde, maar wel toegespitst moeten zijn op de bijzondere persoonsgegevens.

AFDELING 5. BEPERKINGEN

Afdeling 5 biedt een aantal mogelijkheden om de rechten en plichten uit dit hoofdstuk te beperken door middel van nationale of Europese wetgeving. Daarnaast biedt hoofdstuk IX de mogelijkheid meer algemene afwijkingen van de AVG te introduceren.

De term ‘wetgeving’ impliceert niet per se een wet in formele zin. Ook lagere wetgeving kan genoeg zijn. Vereist is wel dat de wetgeving in kwestie vastgelegd is (dus geen vage open norm) en duidelijk en nauwkeurig is, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is, zoals vereist door de rechtspraak van het Hof van Justitie en het Europees Hof voor de Rechten van de Mens.

Artikel 23. Beperkingen

- 23.1 De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 20, worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:

De Europese wetgever, maar ook de nationale wetgever in iedere lidstaat, mag nadere wetgeving invoeren die de rechten van betrokkenen inperkt of de over-

eenkomstige verplichtingen anders invult. Deze wetgeving dient aan drie eisen te voldoen: (1) de grondslag is genoemd in dit artikel 23, (2) de regeling is noodzakelijk en evenredig ter waarborging van die grondslag, en (3) de regeling laat de kern van het betreffende recht onaangetast. Verder moet de wettelijke regeling specifiek zijn over welke persoonsgegevens mogen worden gebruikt en voor welke doeleinden (zie lid 2).

Noodzakelijk en evenredig. Aangezien de omgang met persoonsgegevens aan het grondrecht privacy (artikel 8 EVRM) raakt, dient een wettelijke regeling op dit punt aan strenge eisen te voldoen. De inperking van het grondrecht dient noodzakelijk te zijn voor het beoogde doel en mag niet verder gaan dan nodig (proportionaliteit) voor dat doel.

Overige nadere bepalingen. Lidstaten mogen hiernaast nadere wettelijke bepalingen treffen ter waarborging van de uitingsvrijheid (artikel 85), toegang tot overheidsinformatie (artikel 86) en archivering en onderzoek (artikel 89). Ook mogen zij gebruik van een nationaal identiteitsnummer apart regelen (artikel 87) en afwijkende regels stellen over gebruik van persoonsgegevens in arbeidsverhoudingen (artikel 88) en gebruik door verwerkingsverantwoordelijken met een verschoningsrecht of wettelijke geheimhoudingsplicht (artikel 90).

23.1(a) de nationale veiligheid;

23.1(b) landsverdediging;

23.1(c) de openbare veiligheid;

De meest algemene gronden zijn de nationale veiligheid en defensie. Daarnaast is ook de openbare veiligheid een generieke grond. Hieronder wordt tevens verstaan de bescherming van het menselijk leven, met name bij natuurrampen of door de mens veroorzaakte rampen (overweging 73). Ook toezicht en inspectie vanuit de overheid hierop mag anders worden geregeld (punt h).

23.1(d) de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;

Ook de bestrijding van strafbare feiten en het ten uitvoer leggen van straffen is een grond om de rechten van betrokkenen onder de AVG in te mogen perken. Hetzelfde geldt voor het voorkomen van gevaren voor de openbare veiligheid (zie punt c hierboven). De AVG is overigens niet van toepassing bij deze activiteiten wanneer zij worden uitgevoerd door bevoegde autoriteiten (artikel 2 lid 2 punt d). Ook toezicht en inspectie vanuit de overheid hierop mag anders worden geregeld (punt h).

23.1(e) andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

Wanneer een algemeen belang dit dringend vergt, mag worden afgeweken van rechten en plichten van betrokkenen. Hierbij wordt met name gedacht aan economische en financiële belangen, zoals fiscale aangelegenheden. Te denken valt aan een belastingwet die het recht van inzage of correctie inperkt om zo de inning van belastingen te vergemakkelijken. Wel zal zo'n wet dan eigen waarborgen moeten bevatten om de rechten van betrokkenen niet volledig van tafel te krijgen. Ook toezicht en inspectie vanuit de overheid hierop mag anders worden geregeld (punt h).

23.1(f) de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;

De AVG is van toepassing op verwerkingen door gerechten, hoewel de toezichthouder niet competent is om daartegen op te treden (artikel 55 lid 3). De ratio hiervan is dat de AP, door de wet te handhaven, mogelijk indirect invloed zou kunnen hebben op de besluitvorming van rechters (zie voorbeeld bij HvJ EU 24 maart 2022, ECLI:EU:C:2022:216). Het is echter toegestaan om in specifieke regelingen over de onafhankelijkheid van de rechter en van gerechtelijke procedures de rechten en plichten ten aanzien van betrokkenen anders vorm te geven.

23.1(g) de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscode voor gereguleerde beroepen;

Vanwege het belang van gereguleerde beroepen kan specifieke regelgeving daarover afwijkende regels stellen ten aanzien van rechten en plichten van betrokkenen tegenover deze beroepsgroepen. Ook afgeleide werkzaamheden kunnen hieronder vallen, zoals het werk van een privédetective die voor een beroepsorganisatie onderzoek verricht naar schendingen van de beroepscode van een gereguleerd beroep (HvJ EU 7 november 2013, ECLI:EU:C:2013:715). Ook toezicht en inspectie vanuit de overheid hierop mag anders worden geregeld (punt h). Zie over het beroepsgeheim nader artikel 90.

23.1(h) een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a), b, c), d), e) en g) bedoelde gevallen;

Bij toezicht of inspectie vanuit de overheid op de hierboven genoemde gevallen (met uitzondering van de onafhankelijkheid van de rechter, waar dit niet speelt)

mogen eveneens andersluidende regelingen worden getroffen over de rechten en plichten van betrokkenen.

23.1(i) de bescherming van de betrokkene of van de rechten en vrijheden van anderen;

In uitzonderlijke gevallen mag ter bescherming van de betrokkene een regeling worden ingevoerd die zijn rechten of plichten onder de AVG anders vormgeeft. Het is moeilijk hier een praktijkvoorbeeld voor aan te dragen. Bij rechten en vrijheden moet al snel aan grondrechten worden gedacht; zie hierover nader artikelen 85 t/m 91.

23.1(j) de inning van civielrechtelijke vorderingen.

In het kader van incasso en executie van civielrechtelijke vorderingen kunnen regels worden gesteld over de verwerking van persoonsgegevens daarvan. Een Nederlands voorbeeld is de Regeling gegevensverstrekking Kentekenregister, krachtens welke deurwaarders kentekenhoudergegevens kunnen verkrijgen bij de Rijksdienst voor het Wegverkeer bij vermeend tanken zonder betalen, zodat zij daarmee de wegrijder kunnen dagvaarden.

Merk op dat verwerkingen binnen het strafrechtelijk kader buiten de AVG vallen (artikel 2 lid 2 punt d). Verwerkingen door civiele rechtbanken vallen wel onder de AVG, zij het dat de toezichthouder niet competent is om daartegen op te treden (artikel 55 lid 3).

23.2 De in lid 1 bedoelde wettelijke maatregelen bevatten met name specifieke bepalingen met betrekking tot, in voorkomend geval, ten minste:

Wanneer een wettelijke regeling wordt ingevoerd onder lid 1, die de rechten van betrokkenen inperkt of de overeenkomstige verplichtingen anders invult, moet deze wetgeving expliciet en specifiek daarover zijn. Met deze waarborg wil men voorkomen dat een wet gemakkelijk over het aspect persoonsgegevens heen kan stappen.

23.2(a) de doeleinden van de verwerking of van de categorieën van verwerking,

Allereerst moet de wettelijke regeling specifiek benoemen voor welke doelen de verwerking plaats mag vinden. Een voorbeeld zou kunnen zijn een nadere regeling voor het Uitvoeringsorgaan Werk en Zekerheid (UWV) om onderzoek naar zwartwerken door uitkeringsgerechtigden te mogen uitvoeren en daarbij persoonsgegevens te betrekken, bijvoorbeeld door online zoekopdrachten op basis van dergelijke persoonsgegevens. Het zou daarbij wenselijk kunnen zijn om het recht van inzage (artikel 15) buiten werking te plaatsen.

23.2(b) de categorieën van persoonsgegevens;

De wettelijke regeling moet ook benoemen welke categorieën persoonsgegevens mogen worden gebruikt, bijvoorbeeld alleen namen en adressen of ook andere zaken zoals telefoonnummers of socialemedia-accounts.

23.2(c) het toepassingsgebied van de ingevoerde beperkingen,

De wettelijke regeling moet specifiek benoemen op welk gebied de beperkingen gelden, bijvoorbeeld het uitvoeren van online onderzoek naar personen door het al genoemde UWV.

23.2(d) de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte,

Wanneer een wettelijke regeling de rechten van een betrokkene beperkt of buiten toepassing laat, moet de regeling andere waarborgen nemen om misbruik of onrechtmatige toegang of doorgifte van die persoonsgegevens te voorkomen.

23.2(e) de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken,

De wettelijke regeling moet specifiek benoemen welke verwerkingsverantwoordelijke(n) onder de regeling vallen.

23.2(f) de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking,

De wettelijke regeling moet specifiek benoemen hoe lang persoonsgegevens mogen worden opgeslagen en welke waarborgen ten aanzien van veilige opslag (en vernietiging daarna) zullen worden genomen.

23.2(g) de risico's voor de rechten en vrijheden van de betrokkenen, en

De wettelijke regeling moet specifiek rekening houden met de risico's die betrokkenen lopen onder de regeling, met name waar het gaat om de risico's die werden ondervangen met het recht dat nu wordt ingeperkt. Als bijvoorbeeld de rechten van inzage (artikel 15) en rectificatie (artikel 16) worden beperkt, dan kan de betrokkene geen fouten meer signaleren en corrigeren. De wettelijke regeling moet dan een eigen correctiemechanisme hebben (zie overweging 73).

23.2(h) het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

Als laatste moet de wettelijke regeling bepalen hoe betrokkenen op de hoogte kunnen komen van de afwijking van de AVG. Dit zou bijvoorbeeld in een privacyverklaring van de verwerkingsverantwoordelijke kunnen gebeuren. Geen uitleg hoeft te worden gegeven als dit het doel van de beperking zou schaden. Bij inlichtingen- en veiligheidsdiensten zou dit het geval kunnen zijn.

Hoofdstuk IV

Verwerkingsverantwoordelijke en verwerker

Centraal in hoofdstuk IV staan verplichtingen voor de verwerkingsverantwoordelijke en de verwerker. De belangrijkste entiteit is de verwerkingsverantwoordelijke, de partij die het doel en de middelen van een verwerking bepaalt. Deze kan verwerkers inschakelen om een verwerking te laten uitvoeren. Beide partijen hebben specifieke plichten om de beveiliging van persoonsgegevens goed te regelen en om *privacy by design* te reguleren. Zij moeten daarnaast, onder omstandigheden, een functionaris voor gegevensbescherming (FG) aanstellen.

Hoofdstuk IV bestaat uit vijf afdelingen. De eerste afdeling beschrijft algemene verplichtingen voor de verwerkingsverantwoordelijke (artikel 24) en de verwerker (artikel 28), zoals *privacy by design* (artikel 25). Afdeling twee gaat nader in op de beveiligingseisen (artikel 32) en omgang met datalekken (artikel 33 en 34). In afdeling drie wordt de gegevensbeschermingseffectbeoordeling (artikel 35) en voorafgaande raadpleging bij verhoogde risico's (artikel 36) uitgewerkt. Afdeling vier regelt wanneer een FG moet worden aangesteld (artikel 37) en afdeling vijf tenslotte werkt uit hoe middels gedragscodes (artikel 40) en certificering (artikel 42) een betere nakoming gerealiseerd kan worden.

AFDELING 1. ALGEMENE VERPLICHTINGEN

De eerste afdeling van hoofdstuk IV bevat algemene regels over de verwerkingsverantwoordelijke (voorheen verantwoordelijke) en de verwerker (voorheen bewerker), zoals over *privacy by design* (artikel 25) en het verwerkingsregister (artikel 30). Over de verwerker nader nog artikel 28.

Artikel 24. Verantwoordelijkheid van de verwerkingsverantwoordelijke

24.1 Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

De verwerkingsverantwoordelijke is verplicht passende en effectieve maatregelen te nemen om naleving van de AVG te borgen, en moet kunnen aantonen

dat elke verwerkingsactiviteit past binnen de AVG. Dit volgt uit de beginselen (artikel 5), met name het beginsel van integriteit en vertrouwelijkheid.

Verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is de entiteit die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 definitie 7). Deze entiteit is dan ook verplicht de waarborgen te nemen die bij die verwerking nodig zijn. Wanneer de verwerkingsverantwoordelijke een verwerker inschakelt (zie artikel 28), moet deze afdoende garanties bieden dat ook zijn verwerkingen met passende waarborgen omkleed zijn. Zie nader de Richtsnoeren 07/2020 over de begrippen “verwerkingsverantwoordelijke” en “verwerker” in de AVG van het Comité, 7 juli 2021.

Passende maatregelen. De AVG formuleert het benodigde niveau met een open norm: de genomen maatregelen moeten passen bij de aard, omvang, context en het doel van de verwerking en proportioneel zijn daarvoor. Het is dus niet nodig steeds de zwaarste maatregelen te nemen, maar algemeen geldt wel: hoe gevoeliger de persoonsgegevens, hoe zwaarder de waarborgen moeten zijn. De AVG bepaalt, in tegenstelling tot de Richtlijn, niet expliciet dat de verwerkingsverantwoordelijke de stand der techniek en kosten mag betrekken in de overweging van passendheid. Deze factoren zullen in de praktijk natuurlijk meewegen, en komen wel expliciet terug bij de vereisten tot gegevensbescherming door ontwerp en door standaardinstellingen (artikel 25) en beveiliging (artikel 32).

Uiteenlopende risico's. De risico's voor betrokkenen kunnen sterk uiteen lopen. Ongewenste reclame door een per abuis onthuld e-mailadres is formeel net zo goed een overtreding als het aan een werkgever verstrekken van de medische dossiers van alle werknemers, maar de impact is natuurlijk wezenlijk anders. Het risico bij een specifieke verwerking moet worden bepaald op basis van een objectieve beoordeling en vastgesteld moet worden of de verwerking gepaard gaat met een gewoon risico of een hoog risico (overweging 76). Bij een hoog risico is een voorafgaande gegevensbeschermingseffectbeoordeling nodig (artikel 35).

Overweging 75 legt de nadruk op risico's die kunnen resulteren in “ernstige lichamelijke, materiële of immateriële schade”, zoals discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, ongeoorloofde ongedaanmaking van pseudonimisering, of enig ander aanzienlijk economisch of maatschappelijk nadeel (dezelfde criteria als bij een datalek, artikel 33). Ook het niet kunnen uitoefenen van rechten of controle ten aanzien van persoonsgegevens of het verwerken van bijzondere persoonsgegevens, het maken van persoonlijke profielen op persoonlijke aspecten, het verwerken van persoonsgegevens van kinderen of andere kwetsbare personen of het verwerken van grote hoeveelheden persoonsgegevens leveren versterkte risico's op.

Technisch en organisatorisch. Onder technische maatregelen worden alle maatregelen verstaan die zonder menselijk ingrijpen een aspect van naleving van de AVG afdwingen. Bekende voorbeelden zijn encryptie (versleuteling) van digitale bestanden met persoonsgegevens en het analoge equivalent van de kluis, maar ook toegangscontrole via een gebruikersnaam en wachtwoord. Organisatorische maatregelen betreffen regelingen met menselijk toezicht, zoals een portier die bezoekers identificeert of een klantsysteem dat een bericht naar een manager stuurt bij ongebruikelijke handelingen door personeel.

Aantonen. De AVG verlangt dat men kan aantonen dat alle passende maatregelen zijn genomen. Dit volgt ook uit de verantwoordingsplicht van artikel 5 lid 2. Hiertoe is in beginsel het in lid 2 van dit artikel 24 bedoelde gegevensbeschermingsbeleid of *data protection policy* het aangewezen instrument.

24.2 Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.

Van de verwerkingsverantwoordelijke wordt verwacht dat hij de genomen maatregelen uitwerkt tot beleid en dat vervolgens in de praktijk ook daadwerkelijk uitvoert.

In verhouding. Het maken van beleid is alleen vereist wanneer dat in verhouding staat tot de betreffende activiteiten. Bij een eenvoudige verwerking zou het opstellen van uitgebreide beleidsdocumenten en toezien op de naleving daarvan bijvoorbeeld niet verplicht zijn. Daar staat tegenover dat beleid voor een eenvoudige verwerking ook eenvoudig zou moeten zijn. Uiteindelijk ligt de bal bij de verwerkingsverantwoordelijke om te bewijzen dat hij voldoet aan de AVG (artikel 5 lid 2) en het hebben van geïmplementeerd beleid lijkt de eerst aangewezen weg voor dit bewijs.

Gegevensbeschermingsbeleid. Een *data protection policy* documenteert hoe een organisatie omgaat met gegevensbescherming, zowel organisatorisch als technisch. Aan te bevelen is om algemeen beleid te maken dat naleving van de AVG op hoofdlijnen beschrijft (van de doelen waarvoor wordt verwerkt en de stappen ter beveiliging daarvan tot de wijze waarop betrokkenen hun rechten kunnen uitoefenen), gevolgd door specifieke aanvullingen op verschillende gebieden.

Privacyverklaring. Het gegevensbeschermingsbeleid is niet hetzelfde als de informatie die onder artikel 12, 13 en 14 wordt verstrekt (in bijvoorbeeld de privacyverklaring) maar de inhoud zal wel samenhangen. De doelgroep voor een privacyverklaring is de betrokkene, terwijl het beleid geschreven wordt voor uitvoering door werknemers van de verwerkingsverantwoordelijke. Beleid zal dus gedetailleerder zijn en kan vertrouwelijke interne processtappen beschrijven.

Het beleid kan worden gecombineerd met het onder artikel 25 verplichte beleid ten aanzien van *privacy by design* (gegevensbescherming door ontwerp) en *privacy by default* (gegevensbescherming door standaardinstellingen).

Rol FG. De FG moet worden betrokken bij het opstellen en uitvoeren van dit beleid (artikel 38 lid 1). In de praktijk ligt het in de verwachting dat de ICT-afdeling het beleid opstelt en evalueert, waarna de FG het toetst, in overleg met een aanwezige security officer.

Evaluatie. Het beleid moet periodiek worden geëvalueerd en zo nodig aangepast (lid 1, laatste zin). Het beleid moet vermelden hoe vaak en op welke wijze dit zal gebeuren.

24.3 Het aansluiten bij goedgekeurde gedragscodes als bedoeld artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen.

Teneinde verwerkingsverantwoordelijken meer zekerheid te geven dat hun genomen maatregelen passend zijn, biedt de AVG de mogelijkheid om aan te sluiten bij gedragscodes of certificeringen. Dit is echter geen automatische goedkeuring: de verwerkingsverantwoordelijke moet uiteindelijk zelf de eindafweging maken of de verwerkingen rechtmatig zijn onder de AVG.

Gedragscodes. Onder artikel 40 kan een sector of brancheorganisatie gedragscodes opstellen over een passende verwerking van persoonsgegevens. Gedragscodes mogen ook beveiligingsbeleid betreffen (artikel 40 lid 2 punt h). Als deze gedragscode is goedgekeurd door de toezichthouder (artikel 41), mag een verwerkingsverantwoordelijke in beginsel vermoeden dat handelen binnen de gedragscode voldoet aan de AVG.

Certificering. Onder artikel 42 kunnen certificeringsmechanismen worden ingevoerd waarmee organisaties kunnen aantonen dat zij in overeenstemming met de AVG handelen. Langs deze weg kunnen bijvoorbeeld beveiligingstechnologieën worden gecertificeerd. Een beveiliging die dan is opgebouwd uit gecertificeerde technologieën, zal in beginsel voldoen aan de vereisten uit de AVG. Het inzetten van gecertificeerde middelen ontslaat de verwerkingsverantwoordelijke echter niet van zijn eindverantwoordelijkheid (artikel 42 lid 5).

Artikel 25. Gegevensbescherming door ontwerp en door standaardinstellingen

25.1 Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, 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.

Naast de algemene verplichting tot beveiliging van persoonsgegevens (artikel 24) kent de AVG een plicht om verwerkingen zo in te richten dat rekening wordt gehouden met *privacy by design* en *privacy by default*.

Privacy by design. Gegevensbescherming door ontwerp, in het Engels *privacy by design*, houdt in dat de voor verwerking gebruikte mechanismen zo zijn ontworpen dat zij zo veel mogelijk rekening houden met de privacy van betrokkenen en de vereisten uit de AVG. Een systeem dat hieraan voldoet, zou dus bijvoorbeeld knoppen ingebouwd hebben waarmee betrokkenen inzage (artikel 15) in hun persoonsgegevens kunnen krijgen. Ook andere maatregelen, gericht op bijvoorbeeld het minimaliseren van de hoeveelheid persoonsgegevens en het zo spoedig mogelijk pseudonimiseren van persoonsgegevens (zie hieronder), vallen onder dit beginsel.

Privacy by default. In een gegevensverwerking is sprake van *privacy by default* wanneer de standaardinstellingen zo zijn gekozen dat de privacy maximaal wordt geborgd. Bij een sociaal netwerk zouden conform dit beginsel bijvoorbeeld berichten standaard slechts aan directe vrienden worden getoond, en pas na een actieve handeling van de gebruiker aan alle gebruikers of de gehele wereld.

Producenten. Producenten van toepassingen, diensten en producten die persoonsgegevens verwerken, of die persoonsgegevens verwerken bij de uitvoering van hun opdracht, dienen te worden gestimuleerd om bij de ontwikkeling en de uitwerking daarvan rekening te houden met privacy (overweging 78). Een opdrachtgever zou bijvoorbeeld in zijn offerteverzoek of programma van eisen kunnen verlangen dat de leverancier laat zien hoe deze hieraan zal voldoen, of zelfs garanderen dat het opgeleverde resultaat de opdrachtgever in staat zal stellen te voldoen aan zijn verplichtingen inzake gegevensbescherming. Expliciet bepaalt overweging 78 nog dat deze beginselen ook bij openbare aanbestedingen in aanmerking moeten worden genomen.

Passende maatregelen. Regelmatig worden voor passende maatregelen de ISO normeringen toegepast. Met deze normeringen kunnen organisaties aantonen dat ze aan bepaalde eisen voor bijvoorbeeld beveiliging voldoen. In januari van 2023 is de ISO31700 normering gepubliceerd die ziet op een lat ten aanzien van privacy by design en default. Zie nader artikel 24 lid 1.

Uiteenlopende risico's. Zie hierover nader bij artikel 24 lid 1.

Stand der techniek en uitvoeringskosten. In hoeverre maatregelen haalbaar zijn, volgt uit de stand van de techniek (wat is er mogelijk) en de uitvoeringskosten (wat kost dat) afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Dit impliceert tevens dat de gekozen maatregelen periodiek moeten worden herzien (zie ook artikel 24 lid 2) omdat de stand der techniek immers voortschrijdt.

Pseudonimisering. Pseudonimisering is (artikel 4 definitie 5) het zodanig aanpassen van persoonsgegevens dat zij niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder aanvullende gegevens (die dan vervolgens apart bewaard worden). Toepassing hiervan kan de risico's voor de betrokkenen verminderen (overweging 28) en is dus een logische maatregel bij *privacy by design*-implementaties.

25.2 De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen 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 periode waarin zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Vanuit het beginsel van minimale gegevensverwerking (artikel 5 lid 1 punt c) is verwerking alleen toegestaan wanneer de gebruikte persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit lid 2 werkt dit uit: het beginsel geldt expliciet voor elk specifiek doel (zie ook de doelbinding, artikel 5 lid 1 punt b).

Onbeperkt aantal natuurlijke personen. Specifiek legt de AVG de plicht op te zorgen dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt. Dit ziet met name op publicaties op internet van persoonsgegevens. Een geautomatiseerd systeem moet dus zo zijn ontworpen dat de eindbeslissing tot publicatie een menselijke stap is.

- 25.3 Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.

Onder artikel 42 kunnen certificeringsmechanismen worden ingevoerd waarmee organisaties kunnen aantonen dat zij in overeenstemming met de AVG handelen. Langs deze weg kunnen bijvoorbeeld informatietechnologieën worden gecertificeerd als werkend conform de principes van *privacy by design* of *by default*. Wanneer een verwerkingsverantwoordelijke dan alleen dergelijke technologieën inzet, kan hij onderbouwen dat hij voldoet aan de eisen uit lid 1. Het inzetten van gecertificeerde middelen ontslaat de verwerkingsverantwoordelijke echter niet van zijn eindverantwoordelijkheid (artikel 42 lid 5).

Artikel 26. Gezamenlijke verwerkingsverantwoordelijken

- 26.1 Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de in de artikelen 13 en 14 bedoelde informatie te verstrekken, door middel van een onderlinge regeling, tenzij en voor zover de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijken zijn vastgesteld bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijken van toepassing is. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.

De verwerkingsverantwoordelijke is de entiteit die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 definitie 7). Wanneer twee partijen dit gezamenlijk vaststellen, maakt dit hen gezamenlijke verwerkingsverantwoordelijken. Zij dienen dan hun onderlinge relatie en de verplichtingen onder de AVG vast te leggen.

Verwerker of gezamenlijk verantwoordelijk. De relatie tussen gezamenlijke verwerkingsverantwoordelijken is wezenlijk anders dan die van de verwerkingsverantwoordelijke en de verwerker (zie artikel 28); de verwerker is niet betrokken bij het vaststellen van de doelen en middelen. In de praktijk zullen veel verwerkers zelf de middelen kiezen en/of aandragen, maar zolang de eindbeslissing daarover bij de andere partij ligt, wordt de verwerker geen (gezamenlijke) verwerkingsverantwoordelijke. Zie nader artikel 28 lid 1.

Verantwoordelijkheden vaststellen. De gezamenlijke verwerkingsverantwoordelijken moeten in onderling overleg vaststellen wie welke verantwoordelijkheden

op zich neemt ten aanzien van verplichtingen uit de AVG. Het gaat dan met name om het faciliteren van de rechten van betrokkenen (zoals inzage, correctie of gegevenswissing) en het voldoen aan informatieplichten aan de betrokkene.

Vastlegging. De AVG stelt geen formele eisen aan hoe de verantwoordelijkheden worden vastgelegd. Het is dus niet nodig een aparte overeenkomst hiervoor op te stellen; opname in een algemenere samenwerkingsovereenkomst zou al genoeg zijn. Vanuit de verantwoordingsplicht (artikel 5 lid 2) is het aan te raden de verantwoordelijkheidsverdeling (al dan niet elektronisch) op schrift te stellen.

Vastgesteld bij regeling. Wanneer een Europese of nationale wet of andere regeling uitwerkt hoe twee partijen samen moeten werken ten aanzien van persoonsgegevens, is het niet nodig dit te herhalen in een onderlinge regeling. Zo'n wettelijke regeling kan tevens bepalen wie het aanspreekpunt is voor betrokkenen.

- 26.2 Uit de in lid 1 bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.

De regeling moet duidelijk benoemen wie van de verwerkingsverantwoordelijken welke rol op zich neemt (bijvoorbeeld: wie handelt inzageverzoeken af, wie regelt de beveiliging en wie verstrekt de privacyverklaring) en hoe men zich opstelt naar de betrokkenen. Dit is mede van belang voor het toezicht door en de maatregelen van de toezichthoudende autoriteiten (overweging 79).

Beschikbaar stellen. De regeling moet aan de betrokkene beschikbaar worden gesteld, bijvoorbeeld als onderdeel van de privacyverklaring (artikel 13 en 14). Dit volgt uit het beginsel van transparantie (artikel 5 lid 1 punt a).

Wezenlijke inhoud. Het gaat hierbij alleen om het delen van de wezenlijke inhoud van deze regeling. Irrelevante of vertrouwelijke details (zoals vergoedingen die de ene aan de andere verwerkingsverantwoordelijke betaalt of een verdeling van intellectueel eigendom) hoeven daarbij niet te worden gedeeld.

- 26.3 Ongeacht de voorwaarden van de in lid 1 bedoelde regeling, kan de betrokkene zijn rechten uit hoofde van deze verordening met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

De in lid 1 genoemde verdeling van verantwoordelijkheden kan leiden tot onderling verwijzen wanneer een betrokkene zich bij één der verwerkingsverantwoordelijken meldt. Daarom bepaalt dit lid 3 dat de betrokkene iedere verwerkingsverantwoordelijke mag aanspreken tot nakoming van zijn rechten, zoals een recht van

inzage (artikel 15) of gegevenswissing (artikel 17). Verder zijn alle verwerkingsverantwoordelijken jegens de betrokkene hoofdelijk aansprakelijk voor alle schade die voortvloeit uit de verwerking, ongeacht welke van hen deze feitelijk uitvoerde (artikel 82 lid 4). Natuurlijk kunnen partijen onderling een verhaalsregeling afspreken (zie ook 82 lid 5). Zie nader de Richtsnoeren 07/2020 over de begrippen “verwerkingsverantwoordelijke” en “verwerker” in de AVG van het Comité.

Artikel 27. Vertegenwoordigers van niet in de Unie gevestigde verwerkingsverantwoordelijken of verwerkers

27.1 Wanneer artikel 3, lid 2, van toepassing is, wijst de verwerkingsverantwoordelijke of de verwerker schriftelijk een vertegenwoordiger in de Unie aan.

De AVG is krachtens artikel 3 lid 2 in twee situaties van toepassing op verwerkingsverantwoordelijken en verwerkers buiten de EU. Om betrokkenen uit de EU makkelijker hun rechten te laten uitoefenen, moet in die situaties een vertegenwoordiger binnen de EU worden aangewezen.

Toepassingsgebied. De eerste situatie doet zich voor bij het aanbieden van goederen of diensten aan betrokkenen in de EU (al dan niet gratis) en de tweede bij het monitoren van gedrag van betrokkenen in de EU. Om praktische redenen is daarom vereist dat deze verwerkingsverantwoordelijken en verwerkers een entiteit aanwijzen in de EU die hen kan vertegenwoordigen.

Vertegenwoordiger. Een vertegenwoordiger (artikel 4 definitie 17) is een in de EU gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om hem te vertegenwoordigen in kwesties aangaande de AVG.

Aansprakelijkheid. De vertegenwoordiger wordt aan handavingsprocedures onderworpen als de verwerkingsverantwoordelijke zelf niet thuis geeft (overweging 80). Dit kan dus zowel de bevoegdheden uit artikel 58 betreffen (herstel of staking van de verwerking) als de boetes uit artikel 83. Een vertegenwoordiger doet er dus goed aan een stevige vrijwaring op te nemen in zijn opdrachtovereenkomst (Rb. Den Haag 22 november 2016, ECLI:NL:RBDHA:2016:14088). Betrokkenen kunnen onder artikel 79 de vertegenwoordiger echter niet in rechte aanspreken.

Afdwingbaar. In december 2020 legde de Autoriteit Persoonsgegevens een boete van 525.000 euro op aan de Canadese genealogiewebsite Locatefamily.com vanwege het niet hebben gesteld van een vertegenwoordiger. Tevens werd een dwangsom van 20.000 euro per twee weken opgelegd voor het na de boete alsnog niet voldoen, tot een plafond van 120.000 euro. Bij het ter perse gaan van dit boek (editie 2023) was niet bekend of Locatefamily.com inmiddels een vertegenwoordiger had gesteld.

27.2 Deze verplichting geldt niet voor:

27.2(a) incidentele verwerking die geen grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, betreft noch verwerking van persoonsgegevens die verband houden met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10, en waarbij de kans gering is dat zij een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, rekening houdend met de aard, de context, de omvang en de verwerkingsdoeleinden; of

Vanwege de administratieve lasten voor buitenlandse ondernemingen zijn uitzonderingen gemaakt voor incidentele verwerkingen, zoals wanneer een Canadees bedrijf bezoekersstatistieken van zijn website maakt en daarbij af en toe een bezoeker die zich in de EU bevindt aantreft. Formeel is dit het “monitoren van gedrag” bedoeld in artikel 3 lid 2, maar de kosten wegen hier niet tegen de baten op en het risico is gering.

Incidentele verwerking. Het gaat bij dit criterium om de vraag of de verwerking van persoonsgegevens van betrokkenen die zich in de EU bevinden zich slechts incidenteel zal voordoen, zoals bij voornoemde Canadese website. Een dienst in Canada kan zich natuurlijk richten op Europese burgers en dan zal geen sprake meer zijn van ‘incidentele’ verwerking.

Gering risico. Een randvoorwaarde bij de incidentele verwerking is dat deze slechts een gering risico met zich meebrengt voor de privacy van betrokkenen. De AVG kent geen definitie van ‘gering’ maar gezien de context wordt hier bedoeld op een minimale inbreuk op de persoonlijke levenssfeer, zoals bij algemene website-statistieken of een eenvoudige internetdienst waarbij slechts zeer weinig persoonsgegevens worden gevraagd (zoals een e-mailadres en IP-adres, maar niet meer).

Grootschalige verwerking van bijzondere persoonsgegevens. Wanneer sprake is van grootschalige verwerking van bijzondere of strafrechtelijke persoonsgegevens (zie artikel 9 en 10), moet de buitenlandse verwerkingsverantwoordelijke of verwerker wél een vertegenwoordiger stellen (vergelijk artikel 35 lid 3 punt b over dit criterium), ook als de verwerking slechts incidenteel gebeurt.

27.2(b) een overheidsinstantie of overheidsorgaan.

Buitenlandse overheden hoeven geen vertegenwoordigers aan te stellen wanneer zij persoonsgegevens verwerken binnen de criteria van artikel 3 lid 2. Dit zou ook niet veel toevoegen; dergelijke vertegenwoordigers zouden al snel onder het Verdrag van Wenen diplomatieke onschendbaarheid genieten.

- 27.3 De vertegenwoordiger is gevestigd in een van de lidstaten waar zich de betrokkenen bevinden wier persoonsgegevens in verband met het hun aanbieden van goederen of diensten worden verwerkt, of wier gedrag wordt geobserveerd.

Per definitie is de vertegenwoordiger gevestigd in een lidstaat van de Europese Unie (artikel 4 definitie 17). Dit lid 3 eist een nauwere band: het moet gaan om een lidstaat waar de betrokkenen zijn om wie de verwerking door de niet-Europese verwerkingsverantwoordelijke of verwerker gaat. Op die manier hebben deze betrokkenen een laagdrempeliger toegang tot de rechter of toezichthouder (artikel 79). De vertegenwoordiger kan zelf in rechte worden betrokken door betrokkenen (overweging 80).

- 27.4 Teneinde de naleving van deze verordening te waarborgen, wordt de vertegenwoordiger door de verwerkingsverantwoordelijke of de verwerker gemachtigd om naast hem of in zijn plaats te worden benaderd, meer bepaald door de toezichthoudende autoriteiten en betrokkenen, over alle met de verwerking verband houdende aangelegenheden.

De vertegenwoordiger dient ten behoeve van de verwerkingsverantwoordelijke of de verwerker op te kunnen treden en kan door iedere toezichthoudende autoriteit worden benaderd. De vertegenwoordiger moet zijn taken verrichten volgens het van de verwerkingsverantwoordelijke of de verwerker ontvangen mandaat, en moet onder meer samenwerken met de bevoegde toezichthoudende autoriteiten met betrekking tot alle maatregelen die ter naleving van de AVG worden genomen (artikel 31 en 58). In het bijzonder moet de vertegenwoordiger het register uit artikel 30 bijhouden.

- 27.5 Het feit dat de verwerkingsverantwoordelijke of de verwerker een vertegenwoordiger aanwijzen, doet niet af aan de mogelijkheid om tegen de verwerkingsverantwoordelijke of de verwerker zelf vorderingen in te stellen.

Uiteraard blijven verwerkingsverantwoordelijke en verwerker aansprakelijk voor het correct nakomen van de AVG, ook wanneer zij een vertegenwoordiger benoemen. Wel bepaalt overweging 80 dat de vertegenwoordiger aan handhavingprocedures kan worden onderworpen in geval van niet-naleving van de AVG door de verwerkingsverantwoordelijke of de verwerker.

Artikel 28. Verwerker

28.1 Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

Een verwerker is een partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4 definitie 8). Deze laatste is de partij die het doel van en de middelen voor de verwerkingen kiest (zie artikel 4 definitie 7). De verwerker kiest dus per definitie niet het doel en de middelen. Doet hij dat toch, dan is hij een verwerkingsverantwoordelijke, al dan niet gezamenlijk (artikel 26) met zijn wederpartij. Zie nader Richtsnoeren 07/2020 over de begrippen ‘verwerkingsverantwoordelijke’ en ‘verwerker’ van het Europees Comité voor gegevensbescherming. In haar boetebesluit van 27 november 2018 (Uber) laat de Autoriteit Persoonsgegevens uitgebreid zien hoe zij deze afweging maakt.

Doel en middelen. In de praktijk komt het vaak voor dat een verwerker zelf de middelen kiest waarmee de verwerkingen worden uitgevoerd. Een administratiekantoor heeft bijvoorbeeld gewoonlijk zelf de software en dergelijke gekozen om voor haar klanten administraties te beheren. Een Software-as-a-Service dienstverlener werkt natuurlijk met de door haarzelf ontwikkelde softwaredienst. Dit betekent echter nog niet dat deze partijen (gezamenlijke) verwerkingsverantwoordelijken zijn geworden. Het is dan immers nog steeds de klant die besluit om met deze bedrijven in zee te gaan en hoe breed hij de opdracht wil insteken. Zouden de opdrachtnemers het recht bedingen zelf verwerkingen uit te voeren, zoals het sturen van mailings naar de personen in de administratie of het maken van persoonlijke profielen van gebruikers van de softwaredienst, dan zouden zij daarmee wel hun status als verwerker verliezen (zie ook lid 10). Het verschil ligt er hier in of het gaat om het bepalen van wezenlijke middelen, of niet wezenlijke middelen. Wezenlijke middelen houden nauw verband met het doel en de reikwijdte van de verwerking, denk aan de duur van de verwerking of de soort persoonsgegevens. Niet wezenlijke middelen zien op meer praktische aspecten zoals beveiliging of het type hardware of software. Zie nader de Richtsnoeren 07/2020 over de begrippen “verwerkingsverantwoordelijke” en “verwerker” in de AVG van het Comité.

Afdoende garanties. De verwerkingsverantwoordelijke moet passende technische en organisatorische maatregelen nemen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd (artikel 24 lid 1). Bij de inzet van een verwerker vertaalt zich dit naar een borging dat de verwerker eveneens in staat is om de AVG na te komen. De gevraagde ga-

ranties moeten met name betrekking hebben op het gebied van deskundigheid, betrouwbaarheid en middelen (overweging 81). De verwerker kan opereren onder een goedgekeurde gedragscode of een goedgekeurde certificeringsregeling (zie lid 5) om zo te onderbouwen dat aan de gevraagde garanties wordt voldaan. Verder moet de verwerker in bepaalde gevallen een register bijhouden (artikel 30 lid 2) van alle categorieën van verwerkingsactiviteiten die hij ten behoeve van een verwerkingsverantwoordelijke heeft verricht.

Aansprakelijkheid. Bij verwerking door een verwerker kan de betrokkene zowel hem als de verwerkingsverantwoordelijke hoofdelijk aansprakelijk stellen (artikel 82 lid 1). Een verwerker is echter slechts aansprakelijk voor de schade die door een verwerking is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van de AVG of buiten, dan wel in strijd met, de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld (artikel 82 lid 2).

- 28.2 De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

Teneinde te borgen dat de verwerkingsverantwoordelijke het overzicht houdt op de verwerkingen buiten zijn directe invloedssfeer, is de verwerker gehouden voorafgaande toestemming te verkrijgen voor inzet van een subverwerker.

Specifieke of algemene toestemming. Toestemming voor het inschakelen van een subverwerker kan specifiek (gericht op een specifieke subverwerker) worden gegeven, maar ook algemeen (bijvoorbeeld door een functionele omschrijving van wat uitbesteed mag worden). In het laatste geval dient de verwerker te informeren over de ingezette subverwerker(s), en heeft de verwerkingsverantwoordelijke het recht bezwaar te maken tegen een verandering. De AVG bepaalt niet letterlijk wat er na zo'n bezwaar moet gebeuren. Voor de hand ligt dat de verwerker de verandering dan niet mag doorvoeren. Partijen kunnen echter andere afspraken maken, zoals dat de verwerkingsverantwoordelijke dan de gehele dienstenovereenkomst moet opzeggen of opdraait voor de kosten die het gevolg zijn van het niet inzetten van de nieuwe verwerker.

- 28.3 De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:

Verwerkingsverantwoordelijke en verwerker zijn verplicht om de voorgenomen verwerking te regelen in een andere overeenkomst of andere rechtshandeling. Het hiervoor gebruikelijke instrument is de verwerkersovereenkomst (voorheen bewerkersovereenkomst).

Vormvereisten. De AVG eist dat de verwerkersovereenkomst schriftelijk of elektronisch wordt aangegaan (lid 9). De AVG kent echter geen eis dat de verwerkersovereenkomst als apart document wordt aangegaan. De betreffende bepalingen mogen dus geïntegreerd worden in bijvoorbeeld een overeenkomst van opdracht of algemene (inkoop- dan wel verkoop-)voorwaarden. De bepalingen moeten echter wel specifiek de omgang met persoonsgegevens betreffen. Een algemene alinea dat de opdrachtnemer geheimhouding betracht rondom de opdracht voldoet bijvoorbeeld niet aan lid 3 punt b en is dus onvoldoende.

Subverwerker. Wanneer de verwerker een subverwerker inschakelt, dienen deze verwerkingsbepalingen te worden doorgegeven aan de subverwerker (zie lid 4). Het zal in de praktijk acceptabel zijn om equivalente of strengere bepalingen te hanteren.

Standaard verwerkersbepalingen. De Europese Commissie kan standaardbepalingen opstellen voor een verwerkersovereenkomst (zie lid 6). Het staat verwerkingsverantwoordelijke en verwerker vrij om daar al dan niet gebruik van te maken.

Kosten. Partijen zijn verplicht afspraken te maken zoals in dit lid 2 opgenomen. De AVG laat partijen vrij om kosten te verbinden aan de nakoming, bijvoorbeeld wanneer personeel van de verwerker uren moet besteden om instructies uit te voeren of wanneer de gebruikte softwaresystemen moeten worden aangepast op instructie van de verwerkingsverantwoordelijke. Dit wordt bij voorkeur op voorhand afgesproken, en gezien de strekking van de AVG mogen deze kosten niet zodanig hoog zijn dat de verwerkingsverantwoordelijke in de praktijk de afspraken niet zou invoeren.

28.3(a) de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;

De verwerker verwerkt uitsluitend in opdracht van de verwerkingsverantwoordelijke (artikel 29). Verwerking dient dan ook gebaseerd te zijn op schriftelijke instructies van de verwerkingsverantwoordelijke. Op die manier wordt geborgd dat de verwerker niet op eigen houtje verwerkingen kan uitvoeren.

Schriftelijke instructies. De instructies kunnen tijdens de uitvoering worden verstrekt, maar partijen kunnen ook overeenkomen dat de instructies vooraf moeten worden gegeven. De instructies kunnen betrekking hebben op alle aspecten van de AVG, maar gezien het belang van een veilige doorgifte aan derde landen (zie hoofdstuk 5) wordt dit apart benoemd.

Wettelijk voorschrift. Een verwerker kan wettelijk verplicht zijn bepaalde verwerkingen uit te voeren, bijvoorbeeld in het kader van een bewaarplicht. Instructies van de verwerkingsverantwoordelijke kunnen deze plicht natuurlijk niet opzij zetten. Wel dient de verwerker de verwerkingsverantwoordelijke vooraf hierover te informeren. Een uitzondering geldt als de wet dat informeren verbiedt, zoals artikel 126bb lid 5 Wetboek van Strafvordering dat doet in het kader van informatievorderingen bij bedrijven.

28.3(b) waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;

De verwerkersovereenkomst of andere afspraken dienen te borgen dat personen die gemachtigd zijn om de persoonsgegevens te verwerken aan geheimhouding zijn gebonden. Voor de hand ligt om dit te doen door deze personen een geheimhoudingsovereenkomst te laten tekenen welke qua strekking overeenkomt met de verwerkersovereenkomst.

Werknemers. Werknemers zijn van rechtswege al gebonden aan geheimhouding (art. 272 Strafrecht), en in de arbeidsovereenkomst kan een nadere geheimhouding worden opgelegd. Het tijdens het dienstverband eenzijdig opleggen van geheimhoudingsbedingen kan slechts voor zover dit als werkinstructie (art. 7:660 BW) kan worden gegeven of onder de strenge regels voor eenzijdige wijziging van de arbeidsovereenkomst (art. 7:613 BW) kan worden gerechtvaardigd.

digd. Een werknemer verplichten zijn handtekening onder een geheimhoudingsovereenkomst te zetten, levert geen gebondenheid op.

28.3(c) alle overeenkomstig artikel 32 vereiste maatregelen neemt;

Artikel 32 verplicht de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen. In de verwerkersovereenkomst kunnen partijen nader uitwerken wat een passend niveau is, bijvoorbeeld door navolging van een specifieke beveiligingsstandaard te verlangen of het systeem te laten keuren door een onafhankelijke derde. Zie nader artikel 32.

28.3(d) aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;

De verwerker mag geen subverwerkers inschakelen zonder toestemming van de verwerkingsverantwoordelijke (lid 2). Deze dient daarbij dezelfde verplichtingen opgelegd te krijgen als de verwerker opgelegd heeft gekregen van de verwerkingsverantwoordelijke (lid 4).

28.3(e) rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;

Wanneer een betrokkene een verzoek indient om zijn rechten uit te oefenen ten aanzien van inzage (artikel 15), rectificatie (artikel 16), gegevenswissing (artikel 17), beperking (artikel 18) of data-export (artikel 19), zal de verwerkingsverantwoordelijke in de praktijk vaak de hulp van de verwerker nodig hebben om hieraan te voldoen. Denk bijvoorbeeld aan het geval dat de persoonsgegevens alleen opgeslagen zijn in computersystemen van de verwerker. De verwerkersovereenkomst dient te verplichten tot bijstand bij het uitvoeren van deze rechten.

28.3(f) rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;

De verwerker is verplicht de verwerkingsverantwoordelijke bij te staan bij het nakomen van de beveiligingsplicht (artikel 32), het melden van een datalek (artikel 33 en 34), het uitvoeren van een gegevensbeschermingseffectbeoordeling (artikel 35) en een voorafgaande raadpleging bij een verwerking met hoog risico (artikel 36). Deze bijstand kan bijvoorbeeld bestaan uit het verschaffen van informatie over het datalek of de voorgenomen verwerking met hoog risico.

28.3(g) na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;

Als de verwerking is afgerond dient de verwerker de persoonsgegevens terug te geven of te wissen. De keuze hiervoor ligt bij de verwerkingsverantwoordelijke. In de context van elektronische verwerkingen is ‘terugbezorgen’ een onduidelijk begrip. Gezien de strekking van de AVG wordt bedoeld dat de verwerker dan een kopie verschaft. Een uitzondering geldt ook hier als de verwerker onder de wet verplicht is bepaalde persoonsgegevens te bewaren.

28.3(h) de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt.

De verwerker moet alle informatie verschaffen waarmee de verwerkingsverantwoordelijke kan nagaan dat de verwerker voldoet aan de verwerkersovereenkomst en meer algemeen de AVG.

Audits. De verwerker is verplicht mee te werken aan audits ter verificatie dat hij de verwerkersovereenkomst nakomt. Deze audits kunnen worden uitgevoerd door de verwerkingsverantwoordelijke of een door hem gemachtigde controleur, zoals een externe ICT-deskundige of registeraccountant. De verwerker zal in de praktijk zelden de verwerkingsverantwoordelijke toe willen laten, omdat deze zo ook commercieel relevante informatie onder ogen krijgt. Aan te bevelen is dus op voorhand vast te leggen wie de audit uit mag voeren, maar ook wanneer deze uitgevoerd mag worden. Zo is vast te leggen dat de verwerkingsverantwoordelijke een notificatie moet geven binnen een bepaalde tijdsperiode, en dat eerst reeds gemaakte vergelijkbare rapportages opgevraagd moeten worden alvorens dat een audit mag plaatsvinden. Het is eveneens aan te bevelen een afspraak over kosten van audits te maken, bijvoorbeeld dat de verwerker de kosten draagt bij (niet-triviale) schendingen van de verplichtingen uit de verwerkersovereenkomst.

Waar het gaat om de eerste alinea, punt [a], stelt de verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

Hoewel de verwerkingsverantwoordelijke de doelen en middelen van de verwerking bepaalt en daarbij instructies geeft (punt a), ontslaat dit de verwerker niet van de plicht de verwerkingsverantwoordelijke te melden wanneer naar zijn me-

ning de instructie in strijd is met de AVG of andere wetgeving (vergelijk artikel 7:402 BW over de algemene verplichting dienaangaande voor de overeenkomst van opdracht).

Punt h. De tekst van de AVG verwijst naar “de eerste alinea, punt h”. Gezien de verwijzing naar instructies moet hier “punt a” worden gelezen.

- 28.4 Wanneer een verwerker een andere verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in de in lid 3 bedoelde overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in deze verordening voldoet. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker.

Een verwerker kan voor bepaalde verwerkingen een derde nodig hebben. Het inschakelen van een dergelijke subverwerker mag alleen met toestemming gebeuren (zie lid 2), en deze dient daarbij dezelfde verplichtingen te worden opgelegd als de verwerker opgelegd heeft gekregen van de verwerkingsverantwoordelijke.

Overeenkomst of andere rechtshandeling. De subverwerkersafspraken kunnen in een verwerkersovereenkomst worden opgenomen (zie lid 3) maar ook deel uitmaken van andere afspraken. Dit laatste zal met name van belang zijn als verwerker en subverwerker reeds eerder afspraken hadden gemaakt. Het openbreken daarvan om een klantspecifieke verwerkersovereenkomst toe te voegen is dan niet aantrekkelijk. Een mogelijkheid is om in zulke algemene afspraken te bepalen dat klantspecifieke afwijkingen boven de algemene afspraken gaan.

Aansprakelijkheid. Om te voorkomen dat partijen naar elkaar wijzen bij overtredingen van de AVG, bepaalt dit lid 4 dat de eerste verwerker naar de verwerkingsverantwoordelijke aansprakelijk is. De verwerkingsverantwoordelijke blijft aansprakelijk naar de betrokkene (artikel 82), hoewel ook de verwerker direct aangesproken kan worden door betrokkenen voor de gehele schade (artikel 82 lid 4). Uiteraard kunnen partijen onderling verhaalsregelingen of vrijwaringen afspreeken.

- 28.5 Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat voldoende garanties als bedoeld in de leden 1 en 4 van dit artikel worden geboden.

Gedragscodes. Onder artikel 40 kan een sector of brancheorganisatie gedragscodes opstellen over een passende verwerking van persoonsgegevens. Als deze is goedgekeurd door de toezichthouder (artikel 41), kan de verwerker hieraan conformeren en zo aan de verwerkingsverantwoordelijke laten zien dat hij handelt binnen de AVG.

Certificering. Onder artikel 42 kunnen certificeringsmechanismen worden ingevoerd waarmee organisaties kunnen aantonen dat zij in overeenstemming met de AVG handelen. De verwerkingsverantwoordelijke kan deze inzetten om aan de verwerkingsverantwoordelijke te laten zien dat hij handelt binnen de AVG. Het inzetten van gecertificeerde middelen ontslaat de verwerkingsverantwoordelijke echter niet van zijn eindverantwoordelijkheid (artikel 42 lid 5).

- 28.6 Onverminderd een individuele overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker kan de in de leden 3 en 4 van dit artikel bedoelde overeenkomst of andere rechtshandeling geheel of ten dele gebaseerd zijn op de in de leden 7 en 8 van dit artikel bedoelde standaardcontractbepalingen, ook indien zij deel uitmaken van de certificering die door een verwerkingsverantwoordelijke of verwerker uit hoofde van de artikelen 42 en 43 is verleend.

Onder de AVG bestaat de mogelijkheid (lid 7) dat de Commissie standaardbepalingen opstelt voor een verwerkersovereenkomst. Het staat partijen vrij om hiervoor te kiezen, al dan niet ter aanvulling van maatwerkafspraken. Leden 7 en 8 werken nader uit hoe deze standaardbepalingen tot stand komen.

- 28.7 De Commissie kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure standaardcontractbepalingen vaststellen.

Bij het vaststellen van standaardbepalingen voor een verwerkersovereenkomst volgt de Commissie de onderzoeksprocedure (artikel 93 lid 2): de concepttekst wordt voorgelegd aan het artikel 93-comité, dat vervolgens met meerderheid van stemmen beslist over een positief of negatief advies. Indien het advies positief is, neemt de Commissie de standaardbepalingen aan. Deze standaardbepalingen zijn door de Commissie aangenomen (zie Uitvoeringsbesluit (EU) 2021/915 van de Commissie van 4 juni 2021, L199/18).

- 28.8 Een toezichthoudende autoriteit kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens het in artikel 63 bedoelde coherentiemechanisme standaardcontractbepalingen opstellen.

Ook nationale toezichthouders mogen standaardbepalingen vaststellen. Zij dienen daarbij het coherentiemechanisme (artikel 63) in acht te nemen: de AVG moet consequent worden toegepast in de gehele Unie. Samenwerking en overleg is dus vereist. Deze vaststelling vereist advies van het Comité (artikel 64 lid 1 punt d).

- 28.9 De in de leden 3 en 4 bedoelde overeenkomst of andere rechtshandeling wordt in schriftelijke vorm, waaronder elektronische vorm, opgesteld.

Vanuit de verantwoordingsplicht van de verwerkingsverantwoordelijke (artikel 5 lid 2) moet de verwerkersovereenkomst schriftelijk worden aangegaan. Een elektronisch geschrift wordt hiermee gelijk gesteld. Formeel vraagt de AVG niet om ondertekening van het geschrift, maar gezien de dwingende bewijskracht die dit oplevert, ligt dat wel voor de hand bij papieren geschriften. Bij elektronische geschriften (bijvoorbeeld een online gesloten overeenkomst met verwerkersbepalingen) zou de identiteit langs een andere weg kunnen worden vastgesteld.

- 28.10 Indien een verwerker in strijd met deze verordening de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.

De rol van de verwerker is om ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens te verwerken en daarbij binnen de grenzen te blijven die de verwerkingsverantwoordelijke stelt. Dit lid 10 bepaalt dat wanneer de verwerker zijn grenzen te buiten gaat, hij wordt aangemerkt als verwerkingsverantwoordelijke voor de 'eigen' verwerkingen. Hij dient daarvoor dan ook zelf alle verplichtingen uit de AVG (zoals rechten van inzage, rectificatie en wissing honoreren en een adequate grondslag, artikel 6, te hebben) na te komen. Zie hiervoor ook het boetebesluit van de AP over Uber van 6 november 2018.

Boetes. De boetebevoegdheden en schadevergoedingsmogelijkheden uit artikelen 82, 83 en 84 gelden allen expliciet voor zowel de verwerkingsverantwoordelijke als de verwerker. Een verwerker kan dus gewoon langs die weg worden beboet voor zijn tekortschieten als verwerker, of worden aangesproken om schadevergoeding te betalen, ook wanneer hij krachtens dit lid 10 als verwerkingsverantwoordelijke wordt aangemerkt.

Artikel 29. Verwerking onder gezag van de verwerkingsverantwoordelijke of de verwerker

De verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van de verwerkingsverantwoordelijke, tenzij hij Unierechtelijk of lidstaatrechtelijk tot de verwerking gehouden is.

Eenieder die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, mag dat uitsluitend doen in diens opdracht. Andere verwerkingen zijn niet toegestaan. Wanneer een verwerker dit toch zou doen, wordt hij aangemerkt als verwerkingsverantwoordelijke (artikel 28 lid 10). De norm uit dit artikel wordt nader uitgewerkt in artikel 32 lid 4.

Dienstverband. Deze verplichting geldt zowel voor personeel (met een arbeidsovereenkomst) als ingeschakelde derden (zoals een ingehuurde zzp'er, een ingeleende uitzendkracht of een stagiair). Zzp'ers zijn in veel gevallen te kwalificeren als verwerker, een partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4 definitie 8). Maar bij een uitzendkracht kan men zich afvragen of dit opgaat, en bij een stagiair al helemaal. Dit artikel sluit iedere twijfel uit dat ook dan de persoon zich moet houden aan de opdracht van de verwerkingsverantwoordelijke.

Wettelijke verplichtingen. De wet kan een verwerker of andere entiteit verplichten tot bepaalde verwerkingen, zoals een fiscale bewaarplicht of afgifte van gegevens op bevel van de Officier van Justitie in het kader van een strafrechtelijk onderzoek. Uiteraard is deze entiteit dan gehouden daar gevolg aan te geven.

Artikel 30. Register van de verwerkingsactiviteiten

30.1 De verwerkingsverantwoordelijken en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden.

Om de naleving van deze verordening aan te kunnen tonen, dient de verwerkingsverantwoordelijke een register bij te houden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden. Als de verwerkingsverantwoordelijke buiten de EU is gevestigd, komt deze plicht bij de vertegenwoordiger (artikel 27) te rusten. Ook de verwerker moet een register bijhouden, zie nader lid 2.

Geen melding van verwerking. De meldplicht bij de toezichthouder van verwerkingen uit de Richtlijn is onder de AVG komen te vervallen. Alleen voorgenomen verwerkingen met verhoogd risico moeten nog worden gemeld bij de toezichthouder (artikel 36).

Incidentele verwerking. Het middel en kleine bedrijven (mkb) is vrijgesteld van het registreren van incidentele verwerkingen, zoals een uitnodiging voor een jubileum (lid 5). Structurele verwerkingen zoals de personeelsadministratie moeten dus wel gewoon worden geregistreerd. Ook risicovolle incidentele verwerkingen en verwerkingen van bijzondere persoonsgegevens moeten door het mkb worden geregistreerd.

Dat register bevat alle volgende gegevens:

30.1(a) de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;

Het register dient naam en contactgegevens te vermelden van de verwerkingsverantwoordelijke(n) of hun vertegenwoordiger, alsook van de FG (artikel 37). Dit komt overeen met de eerste informatieplichten aan betrokkenen (artikel 13 lid 1 punten a en b en artikel 14 lid 1 punten a en b).

30.1(b) de verwerkingsdoeleinden;

Het register dient tevens te vermelden voor welke doelen iedere verwerking plaatsvindt. In tegenstelling tot de informatieplichten aan betrokkenen (artikel 13 lid 1 punt c en artikel 14 lid 1 punt c) hoeft niet ook de grondslag (artikel 6) te worden vermeld. Wij raden dit wel dringend aan.

30.1(c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;

Het register vermeldt daarnaast om welke categorieën betrokkenen het gaat en welke soort persoonsgegevens daarvan worden verwerkt. Vergelijk de informatieplichten aan betrokkenen, die niet vereisen dat ook categorieën van betrokkenen worden bijgehouden (artikel 14 lid 1 punt d).

30.1(d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;

Tevens dient het register te vermelden aan wie de persoonsgegevens worden verstrekt. Dit geldt zowel voor de ontvangers in derde landen als ontvangers binnen de EU. Dit gaat dus om een bredere groep partijen dan alleen verwerkers. Vergelijk de informatieplichten aan betrokkenen (artikel 13 lid 1 punt d en e en artikel 14 lid 1 punten e en f).

30.1(e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;

Wanneer gegevens worden doorgegeven aan derde landen (of internationale organisaties), moet het register vermelden om welke landen het gaat (vergelijk artikel 13 lid 1 punt e en artikel 14 lid 1 punt f). Als de grondslag voor doorgifte is dat de doorgifte slechts incidenteel is (artikel 49 lid 1 tweede alinea), dan moeten de beoordeling daarvan en de passende waarborgen in het register worden opgenomen.

30.1(f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;

Het register moet verder vermelden hoelang de verschillende persoonsgegevens worden bewaard. Vergelijk de informatieplichten aan betrokkenen (artikel 13 lid 2 punt a en artikel 14 lid 2 punt a).

30.1(g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

Als laatste dient het register een korte beschrijving te bevatten van de beveiligingsmaatregelen die zijn genomen (artikel 32 lid 1).

30.2 De verwerker, en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.

Ook de verwerker (of zijn vertegenwoordiger, als de verwerker buiten de EU is gevestigd) moet een register bijhouden, tenzij de verwerking binnen de uitzondering van lid 5 valt. Het register van de verwerker is per verwerkingsverantwoordelijke georganiseerd.

Dit register bevat de volgende gegevens:

30.2(a) de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de functionaris voor gegevensbescherming;

Het register dient naam en contactgegevens te vermelden van de verwerker en zijn verwerkingsverantwoordelijke, of hun vertegenwoordiger, alsook van de FG

(artikel 37). Vergelijk lid 1 punt a voor de overeenkomstige plicht bij de verwerkingsverantwoordelijke.

30.2(b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;

Het register van de verwerker vermeldt per verwerkingsverantwoordelijke welke categorieën verwerkingen voor deze zijn uitgevoerd. Dit zal corresponderen met de doeleinden van verwerking die de verwerkingsverantwoordelijke in zijn register opneemt (lid 1 punt b).

30.2(c) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;

Wanneer gegevens worden doorgegeven aan derde landen (of internationale organisaties), moet het register van de verwerker vermelden om welke landen het gaat (vergelijk artikel 13 lid 1 punt e en artikel 14 lid 1 punt f). Als de grondslag voor doorgifte is dat er een specifieke regeling met de ontvanger is getroffen (artikel 49 lid 1 tweede alinea), dan moet de documentatie inzake die regeling in het register worden opgenomen.

30.2(d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

Als laatste dient het register een korte beschrijving te bevatten van de beveiligingsmaatregelen die de verwerker heeft genomen (artikel 32 lid 1). Dit zal aansluiten bij hetgeen opgenomen is in de verwerkersovereenkomst (zie artikel 28 lid 3 punt c).

30.3 Het in de leden 1 en 2 bedoelde register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.

Vanwege het gebruik als bewijs dient het register schriftelijk te worden vastgelegd, waarbij elektronische geschriften gelijk worden gesteld met papieren geschriften. Een elektronische database of dergelijke registratie is dus adequaat.

30.4 Desgevraagd stellen de verwerkingsverantwoordelijke of de verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker het register ter beschikking van de toezichthoudende autoriteit.

De toezichthouder kan inzage verlangen in het register. De verwerkingsverantwoordelijke of verwerker dient hieraan mee te werken.

30.5 De in de leden 1 en 2 bedoelde verplichtingen zijn niet van toepassing op ondernemingen of organisaties die minder 250 personen in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking bijzondere categorieën van gegevens, als bedoeld in artikel 9, lid 1, of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 betreft.

Een organisatie is vrijgesteld van het bijhouden van een register wanneer zij minder dan 250 personen in dienst heeft (dit aantal verwijst naar het aantal werknemers, ongeacht het aantal uren dat deze werkzaam zijn).

Toch registerplichtig. Uitzonderingen op deze vrijstelling – en dus wél registerplichtig – zijn (a) wanneer de verwerking risico's inhoudt voor betrokkenen (iets dat de verwerkingsverantwoordelijke onder artikel 24 moet inschatten), (b) wanneer de verwerking structureel en dus niet incidenteel is, en (c) wanneer bijzondere en strafrechtelijke gegevens (artikelen 9 en 10) worden verwerkt (ook indien incidenteel). Punt b maakt dat in de praktijk de meeste verwerkingen binnen een mkb-organisatie alsnog gewoon moeten worden geregistreerd. Personeelsadministraties, ledenbestanden en dergelijke zijn immers structurele verwerkingen.

Artikel 31. Medewerking met de toezichthoudende autoriteit

De verwerkingsverantwoordelijke en de verwerker en, in voorkomend geval, hun vertegenwoordigers, werken desgevraagd samen met de toezichthoudende autoriteit bij het vervullen van haar taken.

Wanneer een toezichthouder verzoekt om medewerking, zijn de verwerkingsverantwoordelijke en de verwerker verplicht daaraan mee te werken. Dit artikel voegt weinig toe: artikel 58 bepaalt al dat de toezichthoudende autoriteiten onderzoeksbevoegdheden hebben, onder meer om de verwerkingsverantwoordelijke, de verwerker en hun vertegenwoordigers te gelasten alle voor de uitvoering van haar taken vereiste informatie te verstrekken. Daarnaast bepaalt artikel 5:20 Awb dat eenieder verplicht is aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen, die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.

AFDELING 2. PERSOONS-GEGEVENS-BEVEILIGING

Afdeling 2 werkt de verplichtingen van de verwerkingsverantwoordelijke en de verwerker nader uit ten aanzien van beveiliging (artikel 32) en de meldplicht datalekken (artikelen 33 en 34).

Artikel 32. Beveiliging van de verwerking

32.1 Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

Vanuit het algemene behoorlijkheidsbeginsel (artikel 5 lid 1) en met name het integriteit- en vertrouwelijkheidsbeginsel (artikel 5 lid 2 punt f) is het essentieel dat een verwerkingsverantwoordelijke, maar ook een verwerker, passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Aanvullend is de plicht om de toezichthouder te informeren over inbreuken op de beveiliging (artikel 33), en onder omstandigheden ook betrokkenen (artikel 34).

Waarborgen. De term 'waarborg' suggereert een garantie dat nooit en te nimmer een inbreuk zal plaatsvinden. Onder de Richtlijn werd een vërgaande inspanningsplicht verlangd (Rechtbank Rotterdam 8 januari 2015, ECLI:NL:RBROT:2015:22). Gezien de formulering over het passend zijn van de maatregelen en hetgeen waar rekening mee gehouden moet worden, ligt het voor de hand dat de AVG de lat niet véél hoger legt (zie ook artikel 22). Gezien de aard van beveiliging zou een keiharde resultaatsverplichting ook het onmogelijke vragen. Beveiliging is een proces, geen resultaat.

Passende maatregelen. De beveiligingsmaatregelen dienen een "passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens". Deze brede formulering laat (te) veel ruimte voor onzekerheid. De AVG probeert deze weg te nemen door een viertal belangrijke aspecten te benoemen (hieronder) en door te benadrukken dat het gaat om de risico's voor betrokkenen (lid 2), alsook door het introduceren van goedgekeurde gedragscodes (artikel 40) en goedgekeurde certificeringsmechanismen (artikel 42). In de zorg is vastgesteld dat bepaalde zorgaanbieders en aanbieders van elektronisch uitwisselingsystemen moeten voldoen aan hetgeen bepaald is in NEN 7510 (zie Besluit elektronisch gegevensverwerking door zorgaanbieders van 1-10-2020). Dit betekent niet dat

deze partijen gecertificeerd moeten zijn, maar alleen dat ze moeten voldoen aan de vereisten uit deze norm. De invulling van artikel 32 AVG voor deze zorg-aanbieders met NEN 7510 is ook bevestigd in de rechtspraak. De rechter gaf in deze zaak aan dat de desbetreffende partij niet voldoende beveiligingsmaatregelen had genomen omdat er niet werd voldaan aan de vereisten van NEN 7510 (Rechtbank Zeeland-West-Brabant, ECLI:NL:RBZWB:2022:5457, 21-09-2022).

32.1(a) de pseudonimisering en versleuteling van persoonsgegevens;

Twee belangrijke waarborgen worden gezien in het pseudonimiseren en het versleutelen van persoonsgegevens. Na het nemen van deze waarborgen zijn de persoonsgegevens veel minder bruikbaar in geval van onrechtmatige toegang.

Pseudonimisering. Pseudonimisering is (artikel 4 lid 5) het zodanig verwerken van persoonsgegevens dat deze zonder aanvullende gegevens niet herleidbaar zijn, bijvoorbeeld door klantnamen te vervangen door nummers en de koppeling elders op te slaan. Zie ook artikel 25 lid 1.

Versleutelen. Versleutelen is het langs wiskundige (cryptografische) weg omzetten van gegevens tot een onbruikbare brij zodanig dat zonder de sleutel de gegevens niet hersteld kunnen worden. De keuze van een goed cryptografisch algoritme en vooral een sterke, lastig te raden sleutel zijn hierbij cruciaal.

32.1(b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

Een andere belangrijke waarborg is een kwalitatief goede inrichting van de diensten en systemen waarmee de verwerking plaatsvindt. Deze moet gericht zijn op een goede beschikbaarheid en veerkracht (om kunnen gaan met storingen), en ontwikkeld zijn om persoonsgegevens vertrouwelijk en met integriteit (weerstand tegen ongewenste aanpassingen of wissingen) te kunnen behandelen. Zie meer algemeen artikel 25 over *privacy by design*.

32.1(c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

Een belangrijke waarborg is verder de mogelijkheid om bij een incident te zorgen dat persoonsgegevens niet permanent verloren gaan. Een storing waardoor persoonsgegevens niet te benaderen zijn, kan ernstig nadelig zijn voor betrokkenen. Denk aan het niet in kunnen zien van financiële gegevens zoals een bankrekening of het niet kunnen regelen van administratie.

- 32.1(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.

De beveiliging dient periodiek te worden getest en geëvalueerd. De in 2013 geformuleerde beleidsregels *Beveiliging van persoonsgegevens* van de Autoriteit Persoonsgegevens adviseren te handelen binnen een Plan-Do-Check-Act cyclus: beoordeel de risico's, gebruik erkende beveiligingsstandaarden en controleer en evalueer de resultaten. De wijze van testen, beoordelen en evalueren dient als beleid vastgelegd te zijn (artikel 5 lid 2). Bij het opstellen van dit beleid dient de FG te zijn betrokken (artikel 39 lid 1).

- 32.2 Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

De beoordeling van het passende beveiligingsniveau is een open norm. De nadruk bij die beoordeling moet echter liggen bij de verwerkingsrisico's: wat kan er misgaan, en hoe kan daartegen worden gewapend? Vernietiging en verlies zijn daarbij belangrijke zorgen, maar ook aanpassen van en toegang tot gegevens vallen onder deze risico's. Daarbij kan het zowel gaan om onvoorziene ("per ongeluk") verwerkingen alsook om meer opzettelijke verwerkingen die in strijd zijn met de AVG.

- 32.3 Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

Om verwerkingsverantwoordelijken meer zekerheid te geven dat hun genomen beveiligingsmaatregelen passend zijn, biedt de AVG de mogelijkheid om aan te sluiten bij gedragscodes of certificeringen. Dit is echter geen automatische goedkeuring: de verwerkingsverantwoordelijke moet uiteindelijk zélf de eindafweging maken of de verwerkingen rechtmatig zijn onder de AVG.

Gedragscodes. Onder artikel 40 kan een sector of brancheorganisatie gedragscodes opstellen over een passende verwerking van persoonsgegevens. Gedragscodes mogen ook beveiligingsbeleid betreffen (artikel 40 lid 2 punt h). Als deze gedragscode is goedgekeurd door de toezichthouder (artikel 41), mag een verwerkingsverantwoordelijke in beginsel vermoeden dat handelen binnen de gedragscode voldoet aan de AVG.

Certificering. Onder artikel 42 kunnen certificeringsmechanismen worden ingevoerd waarmee organisaties kunnen aantonen dat zij in overeenstemming met de AVG handelen. Langs deze weg kunnen bijvoorbeeld beveiligingstechnologieën worden gecertificeerd. Een beveiliging die dan is opgebouwd uit gecertificeerde technologieën, zal dan in beginsel voldoen aan de vereisten uit de AVG. Het inzetten van gecertificeerde middelen ontslaat de verwerkingsverantwoordelijke echter niet van zijn eindverantwoordelijkheid (artikel 42 lid 5).

- 32.4 De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.

Dit lid 4 is een invulling van de algemene norm uit artikel 29 die bepaalt dat eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, deze uitsluitend in diens opdracht mag verwerken (tenzij een wettelijke plicht anders bepaalt). Dit lid 4 preciseert deze norm in die zin dat concrete maatregelen moeten worden getroffen om een en ander af te dwingen (technische beveiliging, zoals wachtwoorden of functiebeperkingen) en te kunnen controleren (organisatorische beveiliging, zoals logbestanden of een audit).

Artikel 33. Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

- 33.1 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.

Wanneer sprake blijkt van een inbreuk in verband met persoonsgegevens (*personal data breach*) oftewel een datalek, moet dit datalek zonder vertraging worden gemeld aan de toezichthouder. Een melding moet vaak ook aan de betrokkenen worden gedaan (zie artikel 34). Zie nader de *Richtsnoren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679* van het Comité van 6 februari 2018.

Inbreuk in verband met persoonsgegevens. Van een inbreuk oftewel een datalek is sprake (zie artikel 4 definitie 12) wanneer persoonsgegevens daadwerkelijk zijn (1) vernietigd of verloren, (2) gewijzigd, (3) verstrekt of (4) toegankelijk ge-

maakt, alles op een manier die onrechtmatig is oftewel buiten de regels van de AVG plaatsvindt (zie met name artikel 5, de beginselen). Alle vier zijn te zien als een 'lek': persoonsgegevens komen waar zij niet behoren te zijn.

Risico onwaarschijnlijk. Geen melding hoeft te worden gedaan als het niet waarschijnlijk is dat de inbreuk redelijkerwijs een risico voor betrokkenen met zich meebrengt. Deze datalekken moeten wel worden gedocumenteerd (lid 5) zodat daaruit lering voor de toekomst kan worden getrokken.

Dreigend datalek. Melding is alleen verplicht bij een daadwerkelijk datalek, en dus niet bij een ontdekte zwakheid waar nog geen misbruik van is gemaakt. Natuurlijk moet men wel kunnen uitsluiten dát er misbruik is gemaakt, bijvoorbeeld met logbestanden of forensisch onderzoek. Wanneer geen garantie hieromtrent kan worden gegeven, moet de zwakheid als datalek worden behandeld.

Melding. De melding is vormvrij en meldt in ieder geval de aard van de inbreuk, de contactgegevens van de FG of andere verantwoordelijke persoon, waarschijnlijke gevolgen van de inbreuk en de maatregelen die men neemt of zal nemen (lid 3). Als een organisatie een FG heeft, wordt deze bij de melding betrokken en coördineert hij of zij de afwikkeling (artikel 39 lid 1 punt e). Het is niet verplicht dat de FG zelf de melding doet, maar het ligt wel voor de hand. De toezichthouder of het Comité kan richtsnoeren uitgeven over het doen van meldingen (artikel 70 lid 1 punt d). Zie nader *Guidelines 9/2022 on personal data breach notification under GDPR* (alleen beschikbaar in het Engels) van het Comité, 12 oktober 2022. Om te helpen bij de kwalificatie of iets al dan niet gemeld moet worden, stelde de AP de "Voorbeeldlijst wel/niet melden datalek" op. Zie verder ook de Richtsnoeren 01/2021 over voorbeelden betreffende de melding van inbreuken in verband met persoonsgegevens van het Comité, 14 december 2021 en *Guidelines 9/2022 on personal data breach notification under GDPR* (alleen beschikbaar in het Engels) van het Comité, 12 oktober 2022. Let wel: dit blijft een analyse die je per geval moet bekijken.

Binnen 72 uur. Als streeftijd voor het doen van een melding geldt 72 uur na daadwerkelijk ter kennis komen bij de verwerkingsverantwoordelijke. Indien niet alle informatie binnen 72 uur beschikbaar is, mag worden volstaan met een incomplete melding dát er een datalek is opgetreden, waarna resterende vereiste informatie zo snel mogelijk (eventueel in stappen) wordt verstrekt (lid 4). Let op dat als iemand binnen de organisatie weet van het incident, maar het niet meldt aan de relevante personen (bijvoorbeeld de juridische afdeling of de privacy officer), dat de 72-uur teller alsnog kan gaan lopen. Grof gezegd: als die persoon had moeten weten dat dit om een mogelijk datalek ging, kan de teller al gaan lopen. Zie hiervoor verder ook het Boetebesluit van de AP over Booking.com van 31 maart 2022.

Verifiëren melding. Wanneer een melding van een datalek niet direct duidelijk is, mag de verwerkingsverantwoordelijke een onderzoek instellen om na te gaan

of werkelijk sprake is van een lek of niet. De tijd benodigd voor dit onderzoek, mits voortvarend ingesteld en uitgevoerd, telt niet mee bij de 72-uurstermijn (*Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679* van het Comité van 6 februari 2018).

Onderzoek. De toezichthouder kan een onderzoek opstarten als uit de melding een vermoeden van een overtreding door de verwerkingsverantwoordelijke of zijn verwerker(s) blijkt, en corrigerend optreden als het vermoeden gestaafd wordt. Of er sprake is van zo'n overtreding staat los van de vraag of een datalek gemeld moet worden. Ook datalekken zonder enige schuld moeten worden gemeld.

Openbaar. Een melding wordt niet actief openbaar gemaakt door de toezichthouder. Toezichthouders mogen in hun jaarverslagen (artikel 59) lijsten opnemen van gemelde inbreuken en bijbehorende maatregelen, maar hierbij ligt vermelding van de verwerkingsverantwoordelijken niet in de rede. De AP zal krachtens de Wet open overheid (Woo) ook inzage moeten geven in meldingen, maar zal zich daarbij kunnen beroepen op de uitzondering voor vertrouwelijke informatie uit artikel 5.1 lid 1 punt c Woo.

- 33.2 De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

De verwerker is verplicht om zonder onredelijke vertraging de verwerkingsverantwoordelijke te informeren over een datalek, zodat deze vervolgens binnen 72 uur (zie lid 1) de toezichthouder kan informeren. Betrokkenen moeten evenzo onverwijld worden geïnformeerd als sprake is van een datalek met hoog risico (zie hierover artikel 34).

Samenloop van termijnen. De 72-uurstermijn voor de verwerkingsverantwoordelijke start wanneer deze daadwerkelijk kennis heeft van het datalek (zie lid 1). De tijd die de verwerker nodig had om een melding te doen aan de verwerkingsverantwoordelijke is dus niet relevant voor deze termijn.

- 33.3 In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:

De melding is vormvrij en kan op iedere manier worden gedaan. De toezichthouder (Autoriteit Persoonsgegevens) heeft op haar website een formulier gepubliceerd voor het melden van datalekken. Indien niet alle informatie binnen de meldingstermijn van 72 uur beschikbaar is, mag gefaseerd worden gemeld (lid 4). Van ieder datalek (ook indien deze niet gemeld hoeven te worden onder lid 1) moet de verwerkingsverantwoordelijke intern een dossier bijhouden (lid 5).

- 33.3(a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

De aard van de inbreuk is uiteraard de belangrijkste. Voorbeelden zijn verlies van gegevens door het per abuis wissen van de enige kopie, doorgifte aan een derde in plaats van aan de klant vanwege een typefout in een e-mailadres, of een hack van een via internet toegankelijke database.

Categorieën en persoonsgegevensregisters. De verwerkingsverantwoordelijke moet in de melding opgaaf doen van de categorieën van betrokkenen en gegevensrecords, inclusief het geschat aantal daarvan.

- 33.3(b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

Als een organisatie een FG heeft, doet deze de melding (artikel 39 lid 1 punt e). Tevens treedt deze dan op als contactpunt voor de opvolging van de melding.

- 33.3(c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;

De toezichthouder moet tevens worden geïnformeerd over de gevolgen die zich waarschijnlijk kunnen voordoen, zoals verlies van controle over hun persoonsgegevens, het niet kunnen uitoefenen van hun rechten (zoals wissing of rectificatie), discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongedaanmaking van pseudonimisering en reputatieschade. Hiermee kan de toezichthouder een eerste inschatting maken van de ernst van het datalek.

- 33.3(d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

De verwerkingsverantwoordelijke moet bij de melding voorstellen wat hij zal ondernemen om de te verwachten gevolgen (zie punt c) te beperken of voorkomen, en meer algemeen wat hij gaat doen om het datalek als zodanig aan te pakken. Hieronder valt dus bijvoorbeeld het dichten van een beveiligingslek, maar ook het aanscherpen van een procedure of mogelijk het indienen van een schadeclaim bij een verwerker.

- 33.4 Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

Om te voorkomen dat een melding van een datalek wordt opgehouden door het feit dat bepaalde informatie ontbreekt, is het toegestaan een incomplete melding te doen, oftewel melden dát er een datalek is opgetreden met al hetgeen op dat moment bekend is. Resterende informatie wordt zo snel mogelijk verstrekt. Dit mag in stappen of fases gebeuren.

- 33.5 De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

Ieder datalek, ongeacht of het moet worden gemeld, moet worden gedocumenteerd inclusief de gevolgen en de genomen maatregelen om dit in de toekomst te voorkomen. De toezichthouder kan toegang verlangen tot deze documentatie (artikel 58 lid 1 punt a), en de documentatie moet adequaat zijn om de toezichthouder te laten controleren of datalekken daadwerkelijk worden gemonitord en opgevolgd.

Artikel 34. Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

- 34.1 Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

Wanneer een datalek zich voordoet, is het wel zo logisch dat ook de getroffen betrokkenen daarvan op de hoogte worden gesteld. De AVG hanteert daarbij het criterium van een “waarschijnlijk hoog risico” voor de betrokkene. De toezichthouder kan de verwerkingsverantwoordelijke opdragen een mededeling te doen (artikel 58 lid 2 punt e). Zie nader lid 2 over de inhoud van de mededeling.

Inbreuk in verband met persoonsgegevens. Van een inbreuk oftewel een datalek is sprake (zie artikel 4 definitie 12) wanneer persoonsgegevens daadwerkelijk zijn (1) vernietigd of verloren, (2) gewijzigd, (3) verstrekt of (4) toegankelijk gemaakt, alles op een manier die onrechtmatig is oftewel buiten de regels van de AVG plaatsvindt (zie met name artikel 5, de beginselen). Alle vier de vormen van inbreuk zijn te zien als een ‘lek’: persoonsgegevens komen waar zij niet behoren te zijn.

Hoog risico. Van een hoog risico is sprake wanneer de te verwachten gevolgen van het datalek zich met grote waarschijnlijkheid voordoen. Zie artikel 35 lid 1 over dit criterium. Negatieve gevolgen voor de rechten en vrijheden van betrokkenen kunnen bijvoorbeeld zijn: verlies van controle over hun persoonsgegevens, het niet kunnen uitoefenen van hun rechten (zoals wissing of rectificatie), discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongedaanmaking van pseudonimisering en reputatieschade. Let wel: het gaat om “waarschijnlijk een hoog risico”. Het hoeft dus niet zeker te zijn dat het een hoog risico oplevert of dat dat intreedt. Zie lid 3 voor uitzonderingssituaties waarin wel sprake is van een hoog risico maar toch geen mededeling hoeft te worden gedaan.

Termijn. De mededeling moet onverwijld oftewel zonder onredelijke vertraging oftewel zo snel als redelijkerwijs mogelijk (overweging 86) worden gedaan. De termijn hangt vooral af van de aard van het risico; hoe acuter het risico is hoe sneller de mededeling moet worden gedaan. Een mededeling mag worden uitgesteld als de verwerkingsverantwoordelijke nog bezig is met passende maatregelen te nemen. Denk bijvoorbeeld aan de situatie waarbij creditcardgegevens zijn ingezien door onbevoegden. Het is dan zaak om zo snel mogelijk de betrokkene(n) in te lichten, want die persoon kan schade voorkomen door zijn of haar creditcard te blokkeren. Zonder die informatie kan de schade groter worden. Zie voor een praktijkvoorbeeld hiervan het Boetebesluit van de AP over Booking.com van 31 maart 2022.

Financiële ondernemingen. De mededelingsplicht is niet van toepassing voor financiële ondernemingen, als bedoeld in de Wet op het financieel toezicht (artikel 42 Uitvoeringswet). Deze ondernemingen hebben in beginsel wel een mededelingsplicht aan betrokkenen op grond van hun zorgplicht als professioneel dienstverlener.

34.2 De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, punten b), c) en d), voorgeschreven gegevens en aanbevelingen.

De betrokkene moet dezelfde informatie krijgen als de toezichthouder (artikel 33 lid 3 punten b, c, en d) over het datalek. De aard van de inbreuk (artikel 33 lid 3 punt a) moet echter in duidelijke en eenvoudige taal worden omschreven, en de mededeling moet tevens aanbevelingen bevatten waarmee de betrokkene zelf aan de slag kan.

Vorm. De mededeling is vormvrij en mag dus schriftelijk maar ook elektronisch worden gedaan. Een verwerkingsverantwoordelijke wiens discussieforum gehackt is, zou bijvoorbeeld alle forumbezoekers een privébericht via het forum kunnen sturen. Een algemene mededeling op de website van de verwerkings-

verantwoordelijke is geen ‘mededeling’ aangezien daarvan niet kan worden vastgesteld of deze concreet de betrokkenen heeft bereikt.

Aanbevelingen. Naast de verplichte informatie uit artikel 33 lid 3 moet de kennisgeving ook aanbevelingen bevatten over hoe de natuurlijke persoon in kwestie mogelijke negatieve gevolgen kan beperken (overweging 86).

Duidelijke en eenvoudige taal. Waar naar de toezichthouder nog vakjargon en technische details mogen worden gebruikt, moet naar de betrokkene toe de aard van de inbreuk in duidelijke en eenvoudige taal worden omschreven. Wat duidelijk en eenvoudig is, zal afhangen van de categorie(ën) van betrokkenen, maar hoger dan taalniveau B2 van het Europees Referentiekader Talen lijkt in het algemeen ongepast. Vergelijk artikel 7 lid 2 over toestemmingsvragen in duidelijke en eenvoudige taal en artikel 12 lid 1 over informatieverstrekking in duidelijke en eenvoudige taal.

34-3 De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

Een mededeling aan de betrokkenen van een datalek is alleen vereist als sprake is van een datalek dat waarschijnlijk een hoog risico inhoudt (lid 1). Dit lid 3 formuleert drie uitzonderingen op deze regel. Daarnaast vermeldt overweging 88 dat een mededeling kan wachten wanneer dit een onderzoek door toezichthouder(s) en/of rechtshandhavingsautoriteiten (zoals Justitie)odeloos zou hinderen.

34-3(a) de verwerkingsverantwoordelijke passende technische en organisatorische beschermingsmaatregelen heeft genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

Wanneer de geleeke persoonsgegevens op passende wijze (artikel 32) zijn beveiligd tegen misbruik, is het niet nodig een datalek mede te delen aan de betrokkenen. Door die beveiliging is misbruik dan immers uit te sluiten, zodat mensen slechts nodeloos bang gemaakt zouden worden.

Onbegrijpelijk. Encryptie of versleuteling is een beste praktijk om dergelijk misbruik te voorkomen. Hiermee worden gegevens getransformeerd tot een brij schijnbaar willekeurige tekens, die slechts kan worden gelezen door partijen die de bijbehorende sleutel hebben. Ook andere maatregelen zijn denkbaar, zoals het in een plokoffer opnemen van dossiers. Onbevoegd openen daarvan vernietigt dan de dossiers, bijvoorbeeld door er verf overheen te lekken.

34.3(b) de verwerkingsverantwoordelijke achteraf maatregelen heeft 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;

Wanneer de verwerkingsverantwoordelijke direct na het datalek maatregelen neemt om de gevolgen van het datalek te voorkomen, is het niet meer nodig betrokkenen alsnog te informeren. Uiteraard moeten de maatregelen zijn genomen voordat de risico's zich waarschijnlijk hebben gemanifesteerd.

Kredietbescherming. In de Amerikaanse markt is de kredietbeschermingsverzekering in opkomst. Hierbij is de betrokkene verzekerd tegen onverwachte schulden als gevolg van bijvoorbeeld identiteitsfraude. Een dergelijke maatregel kan verstandig zijn om de gevolgen van een datalek te mitigeren, maar zorgt er niet voor dat de risico's zich niet meer voor kunnen doen. Daarmee ontheft zo'n verzekering de verwerkingsverantwoordelijke niet van de plicht tot informeren.

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

Het informeren van alle betrokkenen kan zware inspanningen van de verwerkingsverantwoordelijke eisen, bijvoorbeeld omdat het om een zeer groot aantal betrokkenen gaat (zoals bij een gehackte gratis internetdienst) of omdat deze lastig te contacteren zijn (bijvoorbeeld omdat enkel een IP-adres beschikbaar is). In dergelijke gevallen is een mededeling per betrokkene niet nodig en worden betrokkenen op een andere manier geïnformeerd.

Openbare mededeling. Een openbare mededeling kan bijvoorbeeld in landelijke nieuwswebsites of kranten worden gedaan, of als persbericht verspreid door de toezichthouder.

Soortgelijke maatregel. Een alternatief voor de openbare mededeling kan een meer gerichte communicatie zijn die met grote waarschijnlijkheid alle betrokkenen bereikt. Een voorbeeld is een *banner* of ander bericht op de website.

34.4 Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.

Wanneer de verwerkingsverantwoordelijke niet zelf een mededeling doet, kan de toezichthouder hem opdragen die mededeling te doen (artikel 58 lid 2 punt e). De toezichthouder maakt dan een eigen beoordeling of sprake is van het in

lid 1 vereiste hoog risico dan wel een van de uitzonderingen uit lid 3 op grond waarvan geen mededeling hoeft te worden gedaan. Deze beoordeling is een besluit waartegen bezwaar en beroep open staan.

AFDELING 3. GEGEVENSBESCHERMINGSEFFECTBEOORDELING EN VOORAFGAANDE RAADPLEGING

In afdeling 3 wordt de gegevensbeschermingseffectbeoordeling (artikel 35) en de bijbehorende voorafgaande raadpleging van de toezichthouder (artikel 36) uiteengezet. De gegevensbeschermingseffectbeoordeling is eerder bekend onder de Engelse naam, *Data Protection Impact Assessment* (“DPIA”).

Artikel 35. Gegevensbeschermingseffectbeoordeling

35.1 Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Een beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens is de verwerkingsverantwoordelijke gehouden een zogeheten DPIA uit te voeren voor verwerkingen die waarschijnlijk een verhoogd risico opleveren. Dit is een open norm (zie lid 3). De inhoud van een dergelijke beoordeling wordt in lid 7 behandeld. Het advies van de functionaris voor gegevensbescherming (“FG”) moet worden ingewonnen (lid 2).

Verhoogd risico. De norm van een waarschijnlijk hoog risico is een open norm. De zinsnede over nieuwe technologieën maakt duidelijk dat verhoogde risico's waarschijnlijk gevonden worden in situaties waarin de impact van een verwerking lastig in te schatten zal zijn. Lid 3 noemt enkele voorbeelden van situaties waarin hiervan sprake is: grootschalige geautomatiseerde besluitvorming, grootschalige verwerking van bijzondere persoonsgegevens en grootschalig monitoren van het publiek. Meer algemeen voegt overweging 91 nog toe dat het moeilijker kunnen uitoefenen van *rechten van betrokkenen* een belangrijke factor is bij de bepaling of een risico verhoogd is. De *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen* (WP 248, editie 4 oktober 2017) noemen negen factoren: (1) evaluatie of scoretoekenning (2) geautomatiseerde besluitvorming (3) stelselmatige monitoring (4) gevoelige gegevens (5) op grote schaal verwerkte gegevens (6) samenvoeging van databases (7) kwetsbare betrokkenen (8) inno-

vatieve toepassingen (9) geen beroep op rechten kunnen doen. Wanneer aan twee van deze factoren is voldaan moet een DPIA worden uitgevoerd.

Drietrapsraket. De DPIA is in feite een drietrapsraket. Bij iedere verwerking moet de verwerkingsverantwoordelijke een eerste beoordeling maken van de risico's die daarbij kunnen bestaan. Volgt daaruit dat er waarschijnlijk een hoog risico kleeft aan een verwerking, dan moet daarop een uitgebreide DPIA worden uitgevoerd. Als vervolgens daaruit blijkt dat het hoge risico niet kan worden beperkt met redelijke middelen, dan moet de toezichthouder eerst worden geraadpleegd (artikel 36).

Witte en zwarte lijst. Toezichthouders kunnen verwerkingen op zwarte lijsten (DPIA altijd verplicht) en witte lijsten (nooit nodig) plaatsen. Zie nader lid 4 en 5.

Reeks verwerkingen. Wanneer meerdere verwerkingen gelijksoortig zijn, en de risico's vergelijkbaar, is het toegestaan deze in één DPIA te behandelen.

Grotere scope. Een DPIA kan breder in scope worden opgezet dan een enkel project, wanneer de aard van de verwerkingen dat rechtvaardigt. Overweging 92 noemt als voorbeelden wanneer overheidsinstanties of -organen een gemeenschappelijk applicatie- of verwerkingsplatform willen opzetten of wanneer meerdere verwerkingsverantwoordelijken van plan zijn een gemeenschappelijke applicatie- of verwerkingsomgeving in te voeren voor een hele bedrijfstak, of een segment daarvan, of voor een gangbare horizontale activiteit.

35.2 Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.

Een organisatie kan een FG (artikel 37) hebben ingesteld. Deel van diens taak is te adviseren bij het uitvoeren van DPIA's. Diens advies behoort dan ook verwerkt te zijn in de beoordeling. De AVG eist echter niet dat de FG persoonlijk de DPIA uitvoert. Zie ook de Richtlijnen voor functionarissen voor gegevensbescherming (WP 243 rev.01) van de Artikel 29-Werkgroep, zoals aangepast op 5 april 2017.

Het advies zal in eerste instantie gaan over de vraag of er een DPIA moet worden uitgevoerd, maar kan ook ingaan op de vraag welke methode moet worden gevolgd, welke waarborgen moeten worden genomen en of de conclusies en adviezen correct zijn. Wanneer de verwerkingsverantwoordelijke of verwerker het advies niet overneemt, dient dit beargumenteerd in de DPIA opgenomen te worden.

- 35.3 Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:

De DPIA is vereist in alle gevallen waarin de verwerking waarschijnlijk een hoog risico voor betrokkenen oplevert. Dit is een open norm, maar er zijn drie gevallen waarin dit geacht wordt aan de orde te zijn: de geautomatiseerde beoordeling van personen, de grootschalige verwerking van bijzondere persoonsgegevens en het grootschalig monitoren van openbare ruimtes.

- 35.3(a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;

Het eerste geval waarbij een DPIA verplicht is, is bij situaties waarin grootschalig besluiten worden genomen gebaseerd op geautomatiseerde verwerkingen van persoonsgegevens, zoals bij profilering (artikel 4 definitie 4, zie ook artikel 22). Denk aan een verzekeraar die claims geautomatiseerd laat beoordelen, of een door een analyse van een Facebookprofiel.

Grootschalig. Onder grootschalig wordt verstaan een aanzienlijke hoeveelheid persoonsgegevens op regionaal, nationaal of supranationaal niveau (overweging 91). Er zijn geen getalsmatige grenzen gepubliceerd door AP of andere autoriteiten.

Rechtsgevolgen of aanzienlijk treffen. Zie over dit begrip de opmerkingen uit artikel 22.

- 35.3(b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of

Als tweede grond geldt de grootschalige verwerking van bijzondere persoonsgegevens (artikel 9) en strafrechtelijke persoonsgegevens (artikel 10). Overweging 91 noemt daarbij nadrukkelijk de biometrische persoonsgegevens, maar de grond geldt natuurlijk voor alle soorten bijzondere persoonsgegevens.

Nederland, grootschalig. Bij nieuwsbericht van 31 mei 2018 heeft de AP aangegeven dat zij vindt dat sprake is van grootschalige gegevensverwerking in de zorg bij meer dan 10.000 ingeschreven of daadwerkelijk onder behandeling staande patiënten van huisartsenpraktijken en instellingen voor medisch specialistische zorg, niet zijnde ziekenhuizen. De verwerking van persoonsgegevens van ziekenhuizen, apotheken (geen solistisch werkende zorgverlener), huisartsenposten en zorggroepen is altijd grootschalig.

35.3(c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Een DPIA is tevens nodig voor de stelselmatig en grootschalige monitoring van openbaar toegankelijke ruimten. Voorbeelden zijn beveiligingscamera's ter bewaking en het volgen van smartphones om zo interesses van hun eigenaren te achterhalen voor marketingdoeleinden.

Stelselmatig en grootschalig. Zie voor deze termen punt a.

Openbaar toegankelijke ruimten. Een openbaar toegankelijke ruimte kan ook particulier terrein betreffen, zoals bij winkelcentra of parkeergarages. Het criterium is grofweg of het publiek zonder bijzondere hindernissen of grenzen toegang tot de ruimte zou kunnen krijgen. Ook een café zou hier dus onder kunnen vallen.

35.4 De toezichthoudende autoriteit stelt een lijst op van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling overeenkomstig lid 1 verplicht is, en maakt deze openbaar. De toezichthoudende autoriteit deelt die lijsten mee aan het in artikel 68 bedoelde Comité.

Toezichthouders kunnen een nadere invulling geven aan de criteria voor verwerkingen waarvoor een DPIA verplicht is (zwarte lijst). Via het Comité worden deze criteria openbaar zodat verwerkingsverantwoordelijken zich hieraan kunnen houden.

Criterium. De toezichthouder moet daarbij als criterium hanteren of de verwerking een groot risico inhoudt voor de rechten en vrijheden van betrokkenen, met name omdat betrokkenen als gevolg van deze verwerkingen een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst, of omdat deze verwerkingen systematisch op grote schaal worden uitgevoerd (overweging 91).

Verwerking van cliëntgegevens. De verwerking van persoonsgegevens mag niet als een grootschalige verwerking worden beschouwd als het gaat om de verwerking van persoonsgegevens van patiënten of cliënten door een individuele arts, een andere zorgprofessional of door een advocaat (overweging 91). In die situaties mag dus geen DPIA vooraf worden verplicht.

Coherentie. Toezichthouders moeten bij het opstellen en aanpassen van deze lijst het coherentiemechanisme (artikel 63) naleven om te zorgen dat de criteria in heel Europa hetzelfde blijven (zie lid 6). De invoering van een dergelijke lijst vereist advies van het Comité (artikel 64 lid 1 punt a).

Nederland, zwarte lijst. De AP heeft op haar website de volgende vormen van verwerking gepubliceerd waarvoor een DPIA verplicht is: (1) Heimelijk onderzoek, zoals verborgen camera's (2) Zwarte lijsten gedeeld tussen organisaties (3) Grootschalige fraudebestrijding (4) Grootschalige creditscoring (5) Grootschalige analyse van financiële situaties (6) Grootschalige verwerking van genetische persoonsgegevens (7) Grootschalige analyse van gezondheidsgegevens (8) Publiek/private samenwerkingsverbanden (9) Grootschalig cameratoezicht in de openbare ruimte (10) Structurele inzet van flexibel cameratoezicht, zoals met drones of bodycams (11) Stelselmatige controle van werknemers (12) Stelselmatige monitoring van locatiegegevens (13) Stelselmatige monitoring van telecommunicatiegegevens inclusief metadata, indien niet noodzakelijk voor telecomdienstverlening (14) Inzet van 'slimme' apparaten (Internet of things) (15) Systematische en uitgebreide geautomatiseerde beoordeling van persoonlijke aspecten (16) Monitoring en beïnvloeding van gedrag (17) Stelselmatige monitoring van biometrische gegevens met als doel identificatie van betrokkenen.

- 35.5 De toezichthoudende autoriteit kan ook een lijst opstellen en openbaar maken van het soort verwerking waarvoor geen gegevensbeschermingseffectbeoordeling is vereist. De toezichthoudende autoriteit deelt deze lijst mee aan het Comité.

Naast de zwarte lijst (lid 4) kunnen toezichthouders ook een witte lijst opstellen: criteria voor verwerkingen waarvoor een DPIA niet nodig is. Via het Comité worden ook deze criteria openbaar zodat verwerkingsverantwoordelijken zich hieraan kunnen houden. Ook hier moet het coherentiemechanisme (artikel 63) worden gehanteerd om te zorgen dat de criteria in heel de EU hetzelfde blijven (zie lid 6).

- 35.6 Wanneer de in de leden 4 en 5 bedoelde lijsten betrekking hebben op verwerkingen met betrekking tot het aanbieden van goederen of diensten aan betrokkenen of op het observeren van hun gedrag in verschillende lidstaten, of op verwerkingen die het vrije verkeer van persoonsgegevens in de Unie wezenlijk kunnen beïnvloeden, past de bevoegde toezichthoudende autoriteit voorafgaand aan de vaststelling van die lijsten het in artikel 63 bedoelde het coherentiemechanisme toe.

Het invoeren van lijsten waarvoor wel (lid 4) of geen (lid 5) DPIA nodig is, vereist afstemming (artikel 63) met andere toezichthouders wanneer de verwerkingen effect hebben in meerdere lidstaten.

35.7 De beoordeling bevat ten minste:

- 35.7(a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;

Allereerst moet uit de DPIA naar voren komen wat de beoogde verwerkingen en verwerkingsdoeleinden zijn. Als dit gebeurt onder de grondslag van een gerechtvaardigd belang (artikel 6 lid 1 punt f) dan moet ook dit belang worden gesteld en gemotiveerd. Eventuele gedragscodes die worden gevolgd, mogen ook worden meegewogen (lid 8).

- 35.7(b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;

De verwerking moet vervolgens worden beoordeeld op noodzakelijkheid en evenredigheid (proportionaliteit) met betrekking tot het doel van de verwerking.

- 35.7(c) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en

Bij de beoordeling moet voorts worden uitgewerkt welke risico's er kunnen ontstaan en met name wanneer deze een verhoogde kans hebben om op te treden.

- 35.7(d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

Als laatste dient de DPIA te vermelden welke maatregelen zullen worden genomen om de gesignaleerde risico's (lid 1) terug te dringen. Deze maatregelen moeten gericht zijn op een adequate bescherming van de privacy en persoonsgegevens van betrokkenen, en moeten hun rechten en belangen respecteren.

- 35.8 Bij het beoordelen van het effect van de door een verwerkingsverantwoordelijke of verwerker verrichte verwerkingen, en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van de in artikel 40 bedoelde goedgekeurde gedragscodes naar behoren in aanmerking genomen.

Wanneer de verwerkingsverantwoordelijke opereert onder een gedragscode (artikel 40), is in hoeverre de verwerking binnen de gedragscode valt een relevante factor. Wanneer een gedragscode immers goedgekeurd is, ligt het minder voor de hand dat een verwerking binnen die gedragscode onaanvaardbaar hoge risico's zal opleveren.

- 35.9 De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.

Bij uitvoering van een DPIA kan het wenselijk zijn om betrokkenen of hun vertegenwoordigers (zoals een consumentenorganisatie) te vragen om hun mening over de voorgenomen verwerking. Een verwerking die consumenten grosso modo prima vinden, zou eerder acceptabel zijn. Natuurlijk hoeft een verwerkingsverantwoordelijke daarbij geen vertrouwelijke commerciële informatie te onthullen of details over de beveiliging te verschaffen.

- 35.10 Wanneer verwerking uit hoofde van artikel 6, lid 1, punt c) of e), haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is, en de specifieke verwerking of verwerkingen in kwestie daarbij wordt geregeld, en er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een gegevensbeschermingseffectbeoordeling is uitgevoerd, zijn de leden 1 tot en met 7 niet van toepassing, tenzij de lidstaten het noodzakelijk achten om voorafgaand aan de verwerkingen een dergelijke beoordeling uit te voeren.

Een DPIA is niet nodig bij verwerkingen onder de grondslagen wettelijke plicht (artikel 6 lid 1 punt c) of algemeen belang dan wel openbaar gezag (artikel 6 lid 1 punt e), wanneer de wet die dit regelt specifiek is over de verwerking en reeds een algemene privacy-afweging heeft gemaakt. Dit zou moeten blijken uit de wetsgeschiedenis of uit een regeling in de wet die de privacy-afweging laat zien.

- 35.11 Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

De verwerkingsverantwoordelijke is gehouden zijn verwerkingen te toetsen op nakoming van de uitkomsten van de DPIA. Dit dient in ieder geval te gebeuren als er risico's veranderen, maar bij voorkeur gebeurt dit periodiek.

Artikel 36. Voorafgaande raadpleging

- 36.1 Wanneer uit een gegevensbeschermingseffectbeoordeling krachtens artikel 35 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit.

Wanneer een DPIA (artikel 35) laat zien dat een verwerking een hoog risico zou opleveren, ondanks redelijke maatregelen, is de verwerkingsverantwoordelijke verplicht voorafgaande toestemming te vragen aan de toezichthouder. Deze onderzoekt dan de verwerking (lid 2). Tot het onderzoek is afgerond, mag de verwerkingsverantwoordelijke de verwerking niet uitvoeren.

- 36.2 Wanneer de toezichthoudende autoriteit van oordeel is dat de in lid 1 bedoelde voorgenomen verwerking inbreuk zou maken op deze verordening, met name wanneer de verwerkingsverantwoordelijke het risico onvoldoende heeft onderkend of beperkt, geeft de toezichthoudende autoriteit binnen een maximumtermijn van acht weken na de ontvangst van het verzoek om raadpleging schriftelijk advies aan de verwerkingsverantwoordelijke en in voorkomend geval aan de verwerker, en mag zij al haar in artikel 58 bedoelde bevoegdheden uitoefenen. Die termijn kan, naargelang de complexiteit van de voorgenomen verwerking, met zes weken worden verlengd. Bij een dergelijke verlenging stelt de toezichthoudende autoriteit de verwerkingsverantwoordelijke en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van onder meer de redenen voor de vertraging. Die termijnen kunnen worden opgeschort totdat de toezichthoudende autoriteit informatie heeft verkregen waarom zij met het oog op de raadpleging heeft verzocht.

De toezichthouder moet binnen acht weken advies geven over de voorgenomen verwerking, waarbij het advies met name moet toelichten waarom de verwerking de AVG zou schenden en welke risico's daarbij centraal staan.

Bevoegdheden. Bij het geven van het advies mag de toezichthouder al haar bevoegdheden (artikel 58) inzetten, bijvoorbeeld door een waarschuwing te geven (artikel 58 lid 1 punt a) dat de AVG zou worden overtreden, door aan te geven hoe de verwerking moet worden aangepast (artikel 58 lid 1 punt d), of door een verbod uit te spreken (artikel 58 lid 1 punt f).

Termijn. De termijn voor het advies is acht weken. Bij complexe zaken mag deze worden verlengd. De toezichthouder moet binnen een maand na ontvangst van het verzoek de verlenging aanzeggen, en daarbij motiveren waarom er vertraging optreedt. Als echter de verwerkingsverantwoordelijke niet de benodigde informatie aanlevert (lid 3), mag de toezichthouder de termijn opschorten totdat dit wel is gebeurd.

Uitblijven van een reactie. De AVG vermeldt niet of uitblijven van een reactie moet worden opgevat als een goedkeuring of een verbod. Naar Nederlands bestuursrecht zou stilzwijgen opgevat worden als een fictief besluit (artikel 6:2 Algemene wet bestuursrecht). Overweging 94 merkt op dat het uitblijven van een reactie eventueel later optreden (bijvoorbeeld verbieden) niet onverlet mag laten. Dit kan worden opgevat als interpretatie dat uitblijven van een reactie te zien is als voorlopige toestemming.

36.3 Wanneer de verwerkingsverantwoordelijke de toezichthoudende autoriteit uit hoofde van lid 1 raadpleegt, verstrekt hij haar informatie over:

Een verzoek om een advies bij een verwerking met een hoog risico moet alle informatie bevatten waarmee de toezichthouder een beoordeling kan maken. Gebeurt dit niet, dan mag de toezichthouder zijn advies opschorten (lid 2) totdat de informatie ontvangen is. Er zijn zes elementen die in ieder geval moeten worden verstrekt:

36.3(a) indien van toepassing, de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijke, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder voor verwerking binnen een concern;

Allereerst moet worden gemeld wie de verwerkingsverantwoordelijke(n) zijn, en eventueel welke verwerkers betrokken zijn. In geval van een concern moet ook de concernstructuur en de plaats van de verwerkingsverantwoordelijke daarbinnen worden gemeld.

36.3(b) de doeleinden en de middelen van de voorgenomen verwerking;

Tevens moet worden gemeld welke doelen de verwerking heeft en welke middelen daarvoor worden ingezet.

36.3(c) de maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van deze verordening;

Daarnaast moet worden gemeld welke maatregelen en waarborgen men neemt om de rechten en de privacy van betrokkenen te beschermen.

36.3(d) indien van toepassing, de contactgegevens van de functionaris voor gegevensbescherming;

Als de verwerkingsverantwoordelijke een FG heeft, moeten diens contactgegevens zijn opgenomen.

36.3(e) de gegevensbeschermingseffectbeoordeling waarin bij artikel 35 is voorzien; en

Bij het verzoek moet de uitkomst van de DPIA als bijlage worden meegestuurd. Dit moet alle informatie bevatten over de verwerking en de risico's, plus de maatregelen die de verwerkingsverantwoordelijke zelf al overwogen had (zie nader artikel 35 lid 7).

36.3(f) alle andere informatie waar de toezichthoudende autoriteit om verzoekt.

De toezichthouder kan aangeven dat zij aanvullende informatie nodig heeft. Deze moet dan worden nageleverd. Totdat deze informatie is verstrekt, kan de termijn voor het advies worden opgeschort (lid 2). Het verzoek kan na ontvangst van de informatie onder punten a tot en met e worden ingediend, maar een toezichthouder mag ook op voorhand een algemene opgaaf doen van aanvullende informatie die met een verzoek moet worden meegestuurd.

36.4 De lidstaten raadplegen de toezichthoudende autoriteit bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel, of een daarop gebaseerde regelgevingsmaatregel in verband met verwerking.

Wanneer lidstaten een nationale wet willen invoeren op grond waarvan persoonsgegevens zullen worden verwerkt, is raadgeving van de toezichthouder daarbij verplicht. Doel daarvan is ervoor te zorgen dat de voorgenomen verwerking strookt met de AVG, en met name om de risico's daarvan voor betrokkenen te beperken.

Raadpleging in Nederland. In Nederland is een dergelijke betrokkenheid van een toezichthouder geregeld in de Kaderwet adviescolleges, zij het dat de term 'raadpleging' en de opname van dit lid 4 suggereert dat de toezichthouder de voorgenomen verwerking (en dus het wetsvoorstel) zou mogen verbieden. De Kaderwet biedt daar geen ruimte voor.

36.5 Niettegenstaande lid 1 kunnen de verwerkingsverantwoordelijken lidstaatrechtelijk ertoe worden verplicht overleg met de toezichthoudende autoriteit te plegen en om haar voorafgaande toestemming te verzoeken wanneer zij met het oog op de vervulling van een taak van algemeen belang verwerken, onder meer wanneer verwerking verband houdt met sociale bescherming en volksgezondheid.

Een lidstaat kan ervoor kiezen een voorafgaande toestemming van de toezichthouder verplicht te stellen bij verwerkingen op grond van het algemeen belang (zie artikel 6 lid 1 punt e), zoals bij sociale zekerheid en volksgezondheid.

AFDELING 4. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

De functionaris voor gegevensbescherming (“FG”) oftewel de *data protection officer* (DPO) is een onafhankelijk en deskundig persoon binnen de organisatie van de verwerkingsverantwoordelijke of verwerker (artikel 38) met als taak informeren en adviseren over de omgang met persoonsgegevens. De FG moet onder omstandigheden verplicht worden aangesteld (artikel 37) en verricht toezichthoudende en adviserende taken (artikel 39).

Artikel 37. Aanwijzing van de functionaris voor gegevensbescherming

37.1 De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin:

Aanstellen van een FG is verplicht in drie situaties: overheidsinstantie (punt a hieronder), stelselmatige observatie (punt b) en grootschalige verwerking van bijzondere persoonsgegevens (punt c). Nadere Europese of nationale wetgeving kan voorschrijven dat in andere gevallen een FG verplicht is (lid 4). Het staat organisaties vrij daarnaast vrijwillig een FG te benoemen (lid 4). Zie nader *Richtlijnen inzake de Functionaris Gegevensbescherming* (5 april 2017) van de 29-Werkgroep.

Rol. De FG is geen toezichthouder en heeft geen corrigerende bevoegdheden. De aanbevelingen van de FG wegen wel zwaar bij bepaling of een verwerking rechtmatig is (overweging 77). De FG opereert onafhankelijk (artikel 38). De taken van de FG zijn opgenomen in artikel 39.

Natuurlijk persoon. De FG moet een natuurlijk persoon zijn. Wanneer een bedrijf een commissie of ander orgaan (zoals een afdeling Corporate Compliance) inricht dat toeziet op verwerkingen, dan moet een van de leden daarvan worden aangewezen als de FG, met bijbehorende onafhankelijke positie.

37.1(a) de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken;

Benoeming van een FG is verplicht bij overheidsinstanties of –organen, zijnde alle organen van rechtspersonen die krachtens publiekrecht zijn ingesteld en andere personen of colleges die met enig openbaar gezag bekleed zijn (artikel 1:1 lid 1 Awb). Private organisatie die publieke taken uitvoeren vallen hier niet onder. De *Richtlijnen inzake de Functionaris Gegevensbescherming* (WP 243, editie 5 april 2017) van de Artikel 29-Werkgroep adviseren dergelijke organisaties echter wel een FG aan te stellen.

Gezamenlijke FG. Verschillende overheidsorganen kunnen één gezamenlijke FG benoemen (lid 3) die dan voor al deze organen als de FG optreedt. Uiteraard stelt dit hogere eisen aan de professionele kwaliteiten (lid 5) van de FG.

Gerechten. Hoewel de AVG ook geldt voor rechtbanken, is het vanwege de onafhankelijkheid van de rechterlijke macht voor rechtbanken niet verplicht een FG te benoemen. Overweging 20 van de AVG roept de rechterlijke macht wel op specifieke instanties in het leven te roepen die toezien op de naleving van de bepalingen uit de AVG.

37.1(b) een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of

Benoeming van een FG is verder verplicht bij organisaties die het uitvoeren van regelmatige en stelselmatige observatie op grote schaal van betrokkenen als hoofdactiviteit hebben. Te denken valt aan recherchebureaus, maar ook aan internetbedrijven die diensten aanbieden om websitebezoek zeer gedetailleerd te monitoren (*analytics*). Dit criterium lijkt enigszins op dat van de systematische en uitgebreide beoordeling van persoonlijke aspecten (artikel 35 lid 3 punt a) op grond waarvan een DPIA vereist is.

Hoofdactiviteit. De hoofdactiviteit van een verwerkingsverantwoordelijke ziet op de kerntaken die noodzakelijk zijn om de doeleinden van een verwerkingsverantwoordelijke, of verwerker te bereiken. Denk hierbij aan een ziekenhuis dat als doel heeft om mensen gezond te maken, en hiertoe hoofdzakelijk gezondheidsdossiers verwerkt.

Regelmatige en stelselmatige observatie. Onder regelmatige en stelselmatige observatie valt onder andere het online monitoren, volgen en profileren van betrokkenen (inclusief het samenstellen van persoonlijke advertenties). Daarnaast vallen volgens de *Richtlijnen inzake de Functionaris Gegevensbescherming* ook alle andere online- en offline activiteiten onder deze noemer, indien er “doorlopend, op vaststaande termijnen of tijden, herhaaldelijk, constant of periodiek” persoonsgegevens worden verwerkt op systematische, planmatige, georganiseerde, strategische of methodische wijze.

Op grote schaal. De *Richtlijnen inzake de Functionaris Gegevensbescherming* van 16 december 2016 van de Artikel 29-Werkgroep geven aan dat relevante factoren van het verwerken van persoonsgegevens op grote schaal zijn: de hoeveelheid persoonsgegevens die wordt verwerkt, het aantal betrokkenen, de duur van de verwerking en de geografische omvang. Voorbeelden van organisaties die voldoen aan dit criterium zijn volgens de Richtlijnen: ziekenhuizen, openbare vervoerders, verzekeringsmaatschappijen, banken, zoekmachines en telecom- en internetproviders.

37.1(c) de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.

Benoeming van een FG is daarnaast verplicht bij organisaties die op grote schaal bijzondere (artikel 9) of strafrechtelijke (artikel 10) persoonsgegevens verwerken. Bij dergelijke verwerkingen is tevens een DPIA verplicht (zie nader artikel 35 lid 3 punt b). Zie voor duiding van de begrippen ‘hoofdzakelijk’ (hoofdactiviteit) en ‘grootschalige’ (grote schaal) hetgeen hierover onder punt b is bepaald.

Nederland, grootschalig. De AP heeft aangegeven dat zij vindt dat sprake is van grootschalige gegevensverwerking in de zorg bij meer dan 10.000 ingeschreven of daadwerkelijk onder behandeling staande patiënten van huisartsenpraktijken en instellingen voor medisch specialistische zorg, niet zijnde ziekenhuizen. De verwerking van persoonsgegevens van ziekenhuizen, apotheken (geen solistisch werkende zorgverlener), huisartsenposten en zorggroepen is altijd grootschalig.

37.2 Een concern kan één functionaris voor gegevensbescherming benoemen, mits de functionaris voor gegevensbescherming vanuit elke vestiging makkelijk te contacteren is.

Formeel is iedere rechtspersoon binnen een concern (zie artikel 4 definitie 19) verplicht een eigen FG te benoemen wanneer deze voldoet aan een van de criteria uit lid 1. Vanwege de nauwe verbondenheid tussen deze rechtspersonen is het echter toegestaan om één centrale FG te benoemen in dit geval. De FG moet dan voor alle entiteiten binnen het concern makkelijk te benaderen zijn, efficiënt met betrokkenen kunnen communiceren en (indien noodzakelijk) samen kunnen werken met een toezichthouder.

37.3 Wanneer de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie of overheidsorgaan is, kan één functionaris voor gegevensbescherming worden aangewezen voor verschillende dergelijke instanties of organen, met inachtneming van hun organisatiestructuur en omvang.

Een FG is verplicht bij overheidsinstanties (lid 1 punt a). Het is dergelijke instanties echter toegestaan om gezamenlijk één FG te benoemen die voor de gehele organisatie als FG optreedt. Denk aan samenwerkende gemeenten of verschillende rijksdiensten. Uiteraard moet hij of zij dan bij al deze organen de juiste positie en bevoegdheden ontvangen.

- 37.4 In andere dan de in lid 1 bedoelde gevallen kunnen of, indien dat Unierechtelijk of lidstaatrechtelijk is verplicht, moeten de verwerkingsverantwoordelijke of de verwerker of verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, een functionaris voor gegevensbescherming aanwijzen. De functionaris voor gegevensbescherming kan optreden voor dergelijke verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen.

Een verwerkingsverantwoordelijke of verwerker mag vrijwillig een FG aanwijzen. Ook brancheorganisaties en dergelijke verenigingen mogen een FG aanstellen, die dan optreedt namens alle instanties uit die branche of vereniging.

Brancheorganisaties. Het is mogelijk dat binnen een branche een vereniging optreedt namens marktpartijen. Deze vereniging kan dan één FG aanstellen die namens de aangesloten partijen opereert. Uiteraard moet deze FG dan bij alle aangesloten partijen de bevoegdheden en vrijheden genieten die hij op grond van de AVG krijgt.

Wettelijk verplicht. Europese of nationale wetgeving mag bepalen dat in een bepaalde branche een FG moet worden aangesteld ook als dat volgens lid 1 niet vereist is. In Nederland is aanvullend een FG verplicht bij een verwerkingsverantwoordelijke voor een elektronisch uitwisselingsstelsel onder de Wet aanvullende bepalingen verwerkingen persoonsgegevens zorg, en voor zorginstellingen onder artikel 1 Wet kwaliteit, klachten en geschillen zorg (artikel 2 Besluit elektronische gegevensverwerking door zorgaanbieders).

- 37.5 De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen.

De FG heeft een zorgplicht om op een professionele en deskundige manier zijn taken te kunnen vervullen. In het bijzonder moet hij op gepaste wijze kunnen informeren en adviseren, toezien op naleving en contact onderhouden met de toezichthouder (artikel 39). De werkgever of opdrachtgever heeft de plicht de FG te ondersteunen, met name door hem de benodigde kennis en vaardigheden te laten opdoen (artikel 38 lid 2).

Professionele kwaliteiten en deskundigheid. De AVG formuleert de zorgplicht als het hebben van professionele kwaliteiten en deskundigheid, in het bijzonder diepgaande kennis van de nationale en Europese privacywetgeving. Een FG bij een overheidsinstelling dient daarnaast kennis te hebben van het bestuursrecht en procedures binnen het orgaan. Elders wordt bepaald dat de FG bij de uitvoering van zijn taken naar behoren rekening houdt met het aan verwerkingen

verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoel-einden (artikel 39 lid 2). Het vereiste niveau van deskundigheid dient daarbij, aldus overweging 97, met name te worden bepaald op grond van de uitgevoerde gegevensverwerkingsactiviteiten en de bescherming die voor de door de verwerkingsverantwoordelijke of de verwerker verwerkte gegevens vereist is. Deze formulering is nieuw en het is daarmee nog niet duidelijk waar de lat behoort te liggen. Waarschijnlijk is de norm wel strenger dan de gewone zorgplicht van de opdrachtnemer (artikel 7:401 BW).

Ontslag. De FG geniet ontslagbescherming (artikel 7:670 lid 10 sub d BW) vanwege zijn onafhankelijkheid. Hij kan niet worden ontslagen of gestraft voor de uitvoering van zijn taken. Het niet (meer) bezitten van de benodigde professionele kwaliteiten kan wél een grondslag zijn voor ontheffing uit zijn aanstelling als FG.

- 37.6 De functionaris voor gegevensbescherming kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten.

Werknemer. Een FG kan worden aangesteld als werknemer binnen de organisatie. Vanwege het vereiste van onafhankelijkheid (artikel 38 lid 3) geniet deze werknemer dan ontslagbescherming (artikel 7:670 lid 10 sub d BW), gelijk aan de bescherming die leden van een ondernemingsraad genieten.

Dienstverleningsovereenkomst. Het is ook mogelijk een FG extern in te huren onder een overeenkomst van opdracht (artikel 7:400 BW). De AVG stelt geen expliciete eisen aan deze overeenkomst. Gezien de aard van de dienstverlening ligt het niet voor de hand dat deze eenvoudig door de opdrachtgever opzegbaar zou zijn (vergelijk artikel 7:408 lid 1 BW). Ook de bevoegdheid tot het geven van aanwijzingen (artikel 7:402 BW) zal zeer beperkt moeten zijn.

- 37.7 De verwerkingsverantwoordelijke of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de toezichthoudende autoriteit.

De FG fungeert als eerste aanspreekpunt voor de toezichthouder (artikel 39 lid 1 punt e) en voor betrokkenen (artikel 38 lid 4). Derhalve moeten zijn of haar zakelijke contactgegevens, zoals naam, telefoonnummer en e-mailadres, beschikbaar zijn voor deze partijen.

Mededelen aan toezichthouder. De contactgegevens van de FG worden ter informatie aan de bevoegde toezichthouder gemeld. De AVG vermeldt niet dat deze de contactgegevens vervolgens actief openbaar maakt, maar het ligt in de rede dat de toezichthouder een register zou kunnen opzetten.

Overige verstrekkingen. De contactgegevens van de FG moeten ook in privacyverklaringen worden opgenomen (artikelen 13 lid 1 punt b en 14 lid 1 punt b) en in het register van gegevensverwerkingen (artikel 30) binnen de organisatie. Bij meldingen van datalekken (artikel 33 lid 3 punt b) en voorafgaande raadplegingen (artikel artikel 36 lid 3 punt d) worden deze verstrekt aan de toezichthouder.

Artikel 38. Positie van de functionaris voor gegevensbescherming

38.1 De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

De taak van de FG is de verwerkingsverantwoordelijke of de verwerker bij te staan bij het toezicht op de interne naleving van de AVG. Dit vereist dat de FG tijdig wordt betrokken bij alle organisationele aangelegenheden waar persoonsgegevens bij komen kijken. De taken van de FG staan nader in artikel 39.

38.2 De verwerkingsverantwoordelijke en de verwerker ondersteunen de functionaris voor gegevensbescherming bij de vervulling van de in artikel 39 bedoelde taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.

De verwerkingsverantwoordelijke of de verwerker waarbij de FG actief is, dient te zorgen dat de FG de middelen heeft om zijn taak uit te voeren. Dit omvat ook het toegang krijgen tot persoonsgegevens. Tevens heeft de FG de plicht zijn deskundigheid op peil te houden; de verwerkingsverantwoordelijke of verwerker moet hem daarbij steunen, bijvoorbeeld door hem of haar aan cursussen over relevante onderwerpen te laten deelnemen. In het algemeen geldt de regel dat hoe complexer of gevoeliger de gegevensverwerking, hoe meer ondersteuning de FG dient te worden geboden. De *Richtlijnen inzake de Functionaris Gegevensbescherming* (5 april 2017) van de 29-Werkgroep noemen een aantal ondersteuningspunten, welke in ieder geval door de verwerkingsverantwoordelijke of verwerker in acht dienen te worden genomen.

- 38.3 De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken. Hij wordt door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft voor de uitvoering van zijn taken. De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan het hoogste leidinggevende niveau van de verwerkingsverantwoordelijke of de verwerker.

De FG moet onafhankelijk kunnen opereren, en mag dus geen instructies krijgen over hoe zijn taken als FG uit te voeren. Hij moet daarbij naar behoren en tijdig worden betrokken bij alle aangelegenheden omtrent persoonsgegevens (lid 1) en alle benodigde toegang en middelen krijgen om zijn werk te doen (lid 2).

Ontslagen of gestraft. De FG mag geen (dreiging van) negatieve gevolgen onderkennen van de onafhankelijke uitvoering van zijn taak. Hij geniet om die reden dan ook ontslagbescherming (artikel 7:670 lid 10 sub d BW).

Verslag aan directie. De FG rapporteert direct aan de hoogste leidinggevende bij zijn organisatie. Dit waarborgt de onafhankelijkheid van de FG en voorkomt dat adviezen blijven ‘steken’ bij lagere echelons.

- 38.4 Betrokkenen kunnen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening.

Wanneer een organisatie een FG heeft, is deze het eerste aanspreekpunt naar betrokkenen toe. Zijn of haar contactgegevens staan mede om die reden in privacyverklaringen die de organisatie verstrekt (artikelen 13 lid 1 punt b en 14 lid 1 punt b).

- 38.5 De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken overeenkomstig het Unierecht of het lidstatelijk recht tot geheimhouding of vertrouwelijkheid gehouden.

Uiteraard is gezien zijn of haar positie de FG gehouden tot geheimhouding van alles hetgeen hem of haar ter kennis komt (vergelijk artikel 273 lid 1 Wetboek van Strafrecht). In de Uitvoeringswet (artikel 39) wordt deze geheimhoudingsplicht nader gepreciseerd.

Verschoningsrecht. Onduidelijk is of met dit lid 5 een wettelijk verschoningsrecht voor de FG in het leven wordt geroepen in de zin van artikel 218 Wetboek van Strafvordering. De bevoegdheden van toezichthouders (artikel 58) maken geen voorbehoud voor informatieverstrekking door een FG.

- 38.6 De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

De persoon in kwestie mag naast zijn werk als FG ook ander werk bekleden, zolang dit ander werk maar niet conflicteert met het werk als FG. Een parttime invulling van de functie is dus in beginsel toegestaan. Een belangenconflict zou bijvoorbeeld kunnen ontstaan als de persoon een persoonlijk belang heeft bij beslissingen die ingaan tegen de rechten van betrokkenen. Ook wanneer de persoon in kwestie de bevoegdheid heeft tot het beslissen over de doeleinden en wijze van gegevensverwerking, of bij senior management functies en directiefuncties (zoals bij het hoofd personeelszaken, financiële zaken en marketing), kan al snel sprake zijn van belangenconflicten. Verder adviseert de artikel 29 Werkgroep de verwerkingsverantwoordelijke of verwerker om interne documentatie in te richten over de met de taken van een FG conflicterende posities, interne regels hieromtrent en de hiertoe ingerichte waarborgen.

Artikel 39. Taken van de functionaris voor gegevensbescherming

- 39.1 De functionaris voor gegevensbescherming vervult ten minste de volgende taken:

De takenlijst van de FG genoemd in dit artikel dient te worden beschouwd als een minimum. De verwerkingsverantwoordelijke en verwerker hebben dan ook de mogelijkheid om het takenpakket van de FG naar behoeven uit te breiden. Zo adviseert de artikel 29 Werkgroep om de FG ook de taak tot het bijhouden van een register op te dragen (artikel 30 AVG).

- 39.1(a) de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van deze verordening en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen;

De eerste en belangrijkste taak van de FG is het informeren en adviseren van alle betrokken partijen over hoe de AVG (en andere privacywetgeving) na te komen. Een belangrijk voorbeeld is het advies bij de DPIA (artikel 35 lid 2).

39.1(b) toezien op naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;

Een tweede taak van de FG is het toezien op de naleving van de AVG en andere wetgeving op het gebied van privacy en persoonsgegevens, alsook op het interne beleid van de organisatie waar de FG optreedt.

Toezicht. De FG is geen (verlengstuk van de) toezichthouder en heeft geen corrigerende bevoegdheden. Het gaat dus meer om controleren, meekijken en rapporteren van de verwerkingen en al hetgeen daarmee samenhangt, en om het aanklaarten bij de betrokken eindverantwoordelijken van zaken die mis dreigen te gaan. De toezichthouder blijft bevoegd om op te treden, zij het dat deze zich terughoudend zal opstellen wanneer een organisatie een goed functionerende FG heeft aangesteld. Daarnaast blijft de verwerkingsverantwoordelijke of verwerker eindverantwoordelijk indien er door een organisatie niet in overeenstemming met privacywetgeving wordt gehandeld. De FG draagt geen persoonlijke verantwoordelijkheid of aansprakelijkheid.

Bewustmaking en opleiding. Tevens heeft de FG tot taak het betrokken personeel bewust te maken van de risico's en randvoorwaarden bij de omgang met persoonsgegevens. Dit kan bijvoorbeeld gebeuren door interne opleidingen of trainingen te verzorgen en adviesmateriaal te verstrekken.

39.1(c) desgevraagd advies verstrekken met betrekking tot de gegevensbeschermings-effectbeoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 35;

Bij een voorgenomen verwerking met hoog risico voor betrokkenen is het uitvoeren van een DPIA verplicht (artikel 35). Wanneer een FG is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een DPIA diens advies in (artikel 35 lid 2). Dit advies zal in eerste instantie gaan over de vraag of er een DPIA moet worden uitgevoerd, maar kan ook ingaan op de vraag welke methode moet worden gevolgd, welke waarborgen moeten worden genomen en of de conclusies en adviezen correct zijn. Wanneer de verwerkingsverantwoordelijke of verwerker het advies niet overneemt, dient dit beargumenteerd in de DPIA opgenomen te worden.

39.1(d) met de toezichthoudende autoriteit samenwerken;

De FG is het eerste aanspreekpunt voor de toezichthouder (zie ook punt e hieronder). Het ligt dan ook voor de hand dat de FG de leiding neemt in de samenwerking met de toezichthouder. De FG mag de toezichthouder ook actief benaderen, bijvoorbeeld om informatie over rechtmatige verwerkingen te krijgen (artikel 57 lid 1 punt d).

39.1(e) optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 36 bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.

De FG treedt naar de toezichthouder op als eerste aanspreekpunt in alle aangelegenheden betreffende persoonsgegevens. De contactgegevens van de FG worden voor dit doel verstrekt aan de toezichthouder (zie artikel 37 lid 7).

Voorafgaande raadpleging. Bij voorgenomen verwerkingen waarbij een hoog risico kan ontstaan (artikel 36) moet voorafgaand de toezichthouder worden geraadpleegd. De FG is hierbij het eerste aanspreekpunt.

39.2 De functionaris voor gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

Het optreden als FG is geen kwestie van simpel een standaardchecklist aflopen. Hij of zij zal iedere verwerking moeten wegen naar de beginselen van de AVG (artikelen 5 en 6) en ten volle moeten toetsen aan hetgeen de AVG vereist. Dit sluit aan op de zorgplicht (artikel 37 lid 5) die hij of zij heeft. De opdrachtgever of werkgever van de FG is verplicht de FG te ondersteunen, met name door hem de benodigde kennis en vaardigheden te laten opdoen (artikel 38 lid 2).

AFDELING 5. GEDRAGSCODES EN CERTIFICERING

Afdeling 5 stelt nadere regels aan de invoering van gedragscodes voor verwerkingen in specifieke branches (artikel 40 en 41). Ook kunnen verwerkingen of daarbij gebruikte middelen worden gecertificeerd (artikel 42 en 43), hetgeen bijdraagt aan een correcte navolging van de AVG.

Artikel 40. Gedragscodes

40.1 De lidstaten, de toezichthoudende autoriteiten, het Comité en de Commissie bevorderen de opstelling van gedragscodes die, met inachtneming van de specifieke kenmerken van de diverse gegevensverwerkingssectoren en de specifieke behoeften van kleine, middelgrote en micro-ondernemingen, moeten bijdragen tot de juiste toepassing van deze verordening.

De AVG bevat naar zijn aard zeer algemene regels. Vanuit de markt is vaak behoefte aan specifieke regels, toegesneden op een specifieke branche of toepassing. De AVG biedt hier ruimte voor middels het systeem van gedragscodes. Brancheorganisaties kunnen hiermee bij wijze van zelfregulering specifieke uitwerkingen van de AVG voor hun branche opstellen (lid 2) en deze laten goedkeuren door de toezichthouder (lid 5). Gedragscodes zijn in beginsel niet bindend, maar kunnen Uniebreed algemeen bindend worden verklaard (lid 9). Op naleving van gedragscode dient toezicht te worden gehouden (artikel 41). De toezichthouder doet dit gratis (artikel 57 lid 3). Zie ook *Richtsnoeren voor gedragscodes en toezichthoudende organen in de zin van Verordening 2016/679* van het Comité, 2 juni 2019.

Effect. Het naleven van een gedragscode kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen (artikel 24 lid 3). Hetzelfde geldt voor de verwerker (artikel 28 lid 5). Als een gedragscode (mede) betrekking heeft op beveiliging, kan ook daar het volgen van de gedragscode worden gebruikt ter ondersteuning van de stelling dat een adequate beveiliging is toegepast (artikel 32 lid 3). Volgen van de gedragscode werkt ook door in een DPIA (artikel 35 lid 8).

Voorbeelden. In Nederland zijn onder de Wbp bijvoorbeeld goedgekeurd als gedragscode: de *Gedragscode slimme meters van energieleveranciers* (2013), de *Gedragscode Verwerking Persoonsgegevens Financiële Instellingen* (2010), de *Gedragscode voor (handels)informatiebureaus* (2011) en de *Gedragscode voor particuliere recherchebureaus* (2016). De Autoriteit Persoonsgegevens heeft de *Data Pro Code* van branchevereniging NLdigital goedgekeurd (2020) en de *Gedragscode Slim Netbeheer* van Netbeheer Nederland (2022). Meer voorbeelden zijn te vinden op de website van het Comité, waar een lijst aan goedgekeurde gedragscodes wordt bijgehouden.

40.2 Verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, kunnen gedragscodes opstellen, of die codes wijzigen of uitbreiden, teneinde de toepassing van deze verordening nader toe te lichten, zoals met betrekking tot:

De inhoud van een gedragscode is bedoeld om de AVG nader uit te werken voor een specifieke branche. Het ligt dan ook voor de hand dat een gedragscode

vanuit de branche wordt ontwikkeld, bijvoorbeeld door een branchevereniging of samenwerkingsverband van marktpartijen.

Vertegenwoordigers. Gedragscodes kunnen worden opgesteld door alle organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen. Voorbeelden zijn brancheverenigingen en belangenorganisaties. Niet vereist is dat vertegenwoordigers van betrokkenen een stem hebben, hoewel overweging 99 wel oproept tot overleg en inspraak van betrokkenen.

Toezicht. Naast de in dit lid 2 genoemde punten moet een gedragscode mechanismen bevatten waarmee het toezichthoudend orgaan in staat is toezicht uit te oefenen op de naleving van de bepalingen van de gedragscode (lid 4).

40.2(a) behoorlijke en transparante verwerking;

Een gedragscode is bedoeld om een nadere uitwerking te geven van de AVG. Het belangrijkste beginsel daarbij is dan ook dat van een behoorlijke en transparante verwerking (artikel 5 lid 1 punt a). De gedragscode moet dus motiveren waarom de daarin beschreven verwerkingen voldoen aan dit beginsel.

40.2(b) de gerechtvaardigde belangen die door verwerkingsverantwoordelijken in een specifieke context worden behartigd;

De gedragscode moet verder uitwerken welke belangen in de branche een rol spelen binnen de gedragscode.

40.2(c) de verzameling van gegevens;

De gedragscode moet daarnaast beschrijven hoe persoonsgegevens worden verzameld (en bij voorkeur ook hoe ze verder worden verwerkt).

40.2(d) de pseudonimisering van persoonsgegevens;

De gedragscode moet ook beschrijven hoe (indien van toepassing) persoonsgegevens worden gepseudonimiseerd. Middels pseudonimisering (artikel 4 definitie 5) kunnen de risico's op misbruik van persoonsgegevens worden verkleind. Pseudonimisering levert een mogelijke passende waarborg op (artikel 6 lid 4) bij verwerkingen op andere gronden dan toestemming, en biedt een mogelijkheid om aan de vereisten van *privacy by design* (artikel 25 lid 1) en beveiliging (artikel 32) te voldoen.

40.2(e) de aan het publiek en betrokkenen verstrekte informatie;

De gedragscode kan daarnaast uitwerken hoe betrokkenen en meer algemeen het publiek toegang krijgen tot informatie over verwerkingen onder de gedrags-

code en meer algemeen zaken die raken aan de gedragscode. Dit staat los van de informatieplichten onder artikel 13 en 14.

40.2(f) de uitoefening van de rechten van betrokkenen;

Een gedragscode werkt verder uit hoe betrokkenen hun rechten kunnen uitoefenen, zoals ten aanzien van inzage (artikel 15), rectificatie (artikel 16), gegevenswissing (artikel 17), beperking (artikel 18) of dataportabiliteit (artikel 19).

40.2(g) de informatie verstrekt aan en de bescherming van kinderen en de wijze waarop de toestemming wordt verkregen van de personen die de ouderlijke verantwoordelijkheid voor kinderen dragen;

Indien de branche (mede) gericht is op kinderen, of de belangen van kinderen bijzondere aandacht verdienen in die branche, kan een gedragscode uitwerken hoe met deze belangen wordt omgegaan. De gedragscode kan dan bijvoorbeeld nader uitwerken hoe op kinderen gerichte informatie (vergelijk artikel 12 lid 1) wordt verstrekt en hoe ouderlijke toestemming wordt verkregen.

Ouderlijke toestemming. Onder artikel 8 is ouderlijke toestemming voor verwerkingen van kinderen alleen nodig voor diensten van de informatiemaatschappij. Het lijkt niet de bedoeling te zijn geweest dat gedragscodes hierin verder moeten gaan. Het kan natuurlijk wel netjes zijn om ook waar de wet dat niet vereist, ouders te betrekken in een verwerking ten aanzien van kinderen.

40.2(h) de maatregelen en procedures als bedoeld in de artikelen 24 en 25 en de maatregelen ter beveiliging van de verwerking als bedoeld in artikel 32;

Een gedragscode kan verder uitwerken hoe de verwerkingsverantwoordelijke borgt dat persoonsgegevens alleen rechtmatig worden verwerkt (artikel 24) en hoe *privacy by design and default* (artikel 25) worden gerealiseerd. Tevens kan worden uitgewerkt welke beveiligingsmaatregelen (in ieder geval) moeten worden getroffen (artikel 32).

40.2(i) de kennisgeving van inbreuken in verband met persoonsgegevens aan toezichthoudende autoriteiten en de mededeling van die inbreuken in verband met persoonsgegevens aan betrokkenen;

Een gedragscode zou ook een uitgewerkte regeling kunnen bevatten over melden van datalekken (artikel 33) en over het mededelen daarvan aan betrokkenen (artikel 34).

40.2(j) de doorgifte van persoonsgegevens aan derde landen of internationale organisaties; of

Wanneer onder een gedragscode persoonsgegevens aan derde landen zouden worden doorgegeven, moet ook dit worden uitgewerkt in de gedragscode. Zie nader artikel 44.

40.2(k) buitengerechtelijke procedures en andere procedures voor de beslechting van geschillen tussen verwerkingsverantwoordelijken en betrokkenen met betrekking tot verwerking, onverminderd de rechten van betrokkenen op grond van de artikelen 77 en 79.

Als laatste mag een gedragscode een geschilbeslechtingsprocedure bevatten, bijvoorbeeld via een geschillencommissie die bindend advies (artikel 7:900 lid 2 BW) kan geven of een arbitragecommissie (artikel 1020 Rv). Het gebruik van deze procedure mag nooit in de plaats komen van de gang naar de toezichthouder (artikel 77) of de rechter (artikel 79). Vergelijk artikel 6:236 sub n BW dat een dergelijk verbod kent in algemene voorwaarden.

40.3 Behalve door verwerkingsverantwoordelijken of verwerkers die onder deze verordening vallen, kan bij overeenkomstig lid 5 van dit artikel goedgekeurde gedragscodes die overeenkomstig lid 9 van dit artikel algemeen geldig zijn verklaard, eveneens worden aangesloten door verwerkingsverantwoordelijken of verwerkers die overeenkomstig artikel 3 niet onder deze verordening vallen, om te voorzien in passende waarborgen voor doorgifte van persoonsgegevens naar derde landen of internationale organisaties onder de voorwaarden als bedoeld in artikel 46, lid 2, punt e). Die verwerkingsverantwoordelijken of verwerkers doen, via contractuele of andere juridisch bindende instrumenten, bindende en afdwingbare toezeggingen om die passende waarborgen toe te passen, ook wat betreft de rechten van de betrokkenen.

Het volgen van algemeen verbindend verklaarde gedragscodes kan ook van belang zijn voor verwerkingsverantwoordelijken of verwerkers buiten de EU, wanneer deze niet volgens de criteria uit artikel 3 onder de AVG vallen. Het aansluiten bij zo'n gedragscode kan worden aangemerkt als een passende waarborg (artikel 46 lid 2 punt e), hetgeen vereist is voor doorgifte van persoonsgegevens aan zo'n partij wanneer het land in kwestie niet als adequaat is aangemerkt onder artikel 45. Vergelijk artikel 42 lid 2 voor dezelfde constructie middels certificering.

Bindende toezeggingen. Naast certificering is voor de passende waarborg ook vereist dat deze verwerkingsverantwoordelijken en verwerkers bindende en afdwingbare middelen bieden om nakoming van de waarborgen af te dwingen en met name om betrokkenen hun rechten uit te laten oefenen.

- 40.4 Een in lid 2 van dit artikel bedoelde gedragscode bevat mechanismen die het in artikel 41, lid 1, bedoelde orgaan in staat stellen het verplichte toezicht uit te oefenen op de naleving van de bepalingen van de code door de verwerkingsverantwoordelijken of verwerkers die zich tot toepassing ervan verbinden, onverminderd de taken en bevoegdheden van de overeenkomstig artikel 55 of 56 bevoegde toezichthoudende autoriteiten.

Een gedragscode dient mechanismen te bevatten waarmee het toezichthoudend orgaan (artikel 41) daadwerkelijk kan nagaan of aangesloten partijen de gedragscode nakomen. Dit kan bijvoorbeeld een rapportageplicht of een auditrecht zijn.

- 40.5 De in lid 2 van dit artikel bedoelde verenigingen en andere organen die voornemens zijn een gedragscode op te stellen of een bestaande gedragscode te wijzigen of uit te breiden, leggen de ontwerpgedragscode, de wijziging of uitbreiding voor aan de overeenkomstig artikel 51 bevoegde toezichthoudende autoriteit. De toezichthoudende autoriteit brengt advies uit over de vraag of de ontwerpgedragscode, de wijziging of uitbreiding strookt met deze verordening, en keurt deze ontwerpgedragscode, die wijziging of uitbreiding goed indien zij van oordeel is dat de code voldoende passende waarborgen biedt.

Een ontwerpgedragscode moet worden goedgekeurd door de bevoegde toezichthouder (zoals bepaald in artikel 51). De toezichthouder brengt advies uit en keurt de code goed of af. Daarna wordt deze bekendgemaakt (lid 6). Als de gedragscode grensoverschrijdende verwerkingen beschrijft, is advies van het Comité nodig (lid 7). Zie nader de concept *Richtlijn voor gedragscodes en toezichthoudende organen in de zin van de Verordening 2016/679 van het Comité, 4 juni 2019* van het Comité (12 februari 2019).

- 40.6 Wanneer de ontwerpgedragscode, de wijziging of uitbreiding wordt goedgekeurd overeenkomstig lid 5, en indien de gedragscode in kwestie geen betrekking heeft op verwerkingsactiviteiten in verschillende lidstaten, registreert de toezichthoudende autoriteit de gedragscode en maakt zij deze bekend.

Als een goedgekeurde gedragscode uitsluitend bedoeld is voor één lidstaat, dan kan de toezichthouder voor dat land deze registreren en bekendmaken. Als de gedragscode grensoverschrijdende verwerkingen voorziet, wordt deze via lid 7 voorgelegd aan het Comité en de Commissie.

- 40.7 Wanneer een ontwerpgedragscode betrekking heeft op verwerkingsactiviteiten in verschillende lidstaten, legt de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit deze, vóór goedkeuring van de gedragscode, de wijziging of uitbreiding, via de in artikel 63 bedoelde procedure voor aan het Comité, dat advies geeft over de vraag of de ontwerpgedragscode, de wijziging of uitbreiding strookt met deze verordening, of, in de in lid 3 bedoelde situatie, voorziet in passende waarborgen.

Een gedragscode kan grensoverschrijdende verwerkingen beschrijven. In dat geval moet de toezichthouder advies van het Comité inwinnen (artikel 64 lid 1 punt b) alvorens hij deze goed mag keuren. Het advies wordt tevens voorgelegd aan de Commissie (lid 8) die de gedragscode eventueel algemeen geldig mag verklaren (lid 9).

- 40.8 Wanneer in het in lid 7 bedoelde advies wordt bevestigd dat de gedragscode, de wijziging of uitbreiding strookt met deze verordening of, in de in lid 3 bedoelde situatie, passende waarborgen biedt, legt het Comité zijn advies voor aan de Commissie.

Nadat onder lid 7 een positief advies van het Comité is opgesteld, wordt dit voorgelegd aan de Commissie. Deze kan vervolgens onder lid 9 de gedragscode in kwestie algemeen verbindend verklaren.

- 40.9 De Commissie kan bij uitvoeringshandelingen vaststellen dat de goedgekeurde gedragscode, wijziging of uitbreiding die haar op grond van lid 8 zijn voorgelegd, binnen de Unie algemeen geldig zijn. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure.

De Commissie is bevoegd gedragscodes algemeen verbindend te verklaren met positief advies van het Comité (leden 7 en 8). Hiermee worden zij dwingend recht voor alle partijen in de betreffende branche of deel daarvan.

Sancties. De toezichthouder is bevoegd partijen die onder een algemeen verbindende gedragscode vallen, te gelasten deze na te komen (artikel 58 lid 2 punt d). Wordt een dergelijk bevel niet opgevolgd, dan mag de toezichthouder een boete uit de hoogste categorie opleggen (artikel 83 lid 6). Dit zou echter een uiterst middel moeten zijn; nakoming van gedragscodes zal in beginsel via de eigen geschillenregeling worden afgedwongen.

40.10 De Commissie zorgt ervoor dat aan de goedgekeurde codes die zij overeenkomstig lid 9 algemeen geldig heeft verklaard, passende bekendheid wordt verleend.

Wanneer gedragscodes algemeen verbindend worden verklaard, dient de Commissie ervoor te zorgen dat dit feit bekend wordt gemaakt. Voor de hand ligt dit te publiceren in het Publicatieblad van de Europese Unie, en via het register van gedragscodes dat het Comité onderhoudt (lid 11).

40.11 Het Comité verzamelt alle goedgekeurde gedragscodes, wijzigingen en uitbreidingen in een register en maakt deze via geëigende kanalen openbaar.

Om het publiek te kunnen informeren, publiceert het Comité alle goedgekeurde gedragscodes. Dit sluit aan bij haar taak om het opstellen van gedragscodes te bevorderen (artikel 70 lid 1 punt n).

Artikel 41. Toezicht op goedgekeurde gedragscodes

41.1 Onverminderd de taken en bevoegdheden van de bevoegde toezichthoudende autoriteit uit hoofde van de artikelen 57 en 58, kan het op grond van artikel 40 uitgevoerde toezicht op de naleving van een gedragscode worden uitgeoefend door een orgaan dat over de passende deskundigheid met betrekking tot het onderwerp van de gedragscode beschikt en daartoe door de bevoegde toezichthoudende autoriteit is geaccrediteerd.

Een gedragscode kan een eigen toezichthoudend orgaan aanwijzen dat maatregelen kan nemen bij overtreding van de gedragscode of onderliggende verwerkingen (lid 4). Een dergelijk orgaan moet worden geaccrediteerd (zie lid 2), en accreditatie kan natuurlijk worden ingetrokken (lid 5). De criteria voor accreditatie moeten door de toezichthouder worden opgesteld, en worden afgestemd met het Comité (lid 3). Overheden mogen niet werken op basis van gedragscodes (lid 6).

41.2 Een orgaan als bedoeld in lid 1 kan daartoe worden geaccrediteerd om toezicht te houden op de naleving van een gedragscode indien het:

Om te worden geaccrediteerd, dient een toezichthoudend orgaan te voldoen aan vier eisen ten aanzien van onafhankelijkheid. Deze worden hieronder genoemd.

41.2(a) ten genoegen van de bevoegde toezichthoudende autoriteit zijn onafhankelijkheid en deskundigheid met betrekking tot het onderwerp van de gedragscode heeft aangetoond;

De eerste eis is dat het toezichthoudend orgaan onafhankelijk en deskundig opereert. Zij dient hiervan bewijs te overleggen aan de toezichthouder. Dit kan

bijvoorbeeld gebeuren door daartoe strekkende statuten die de onafhankelijkheid borgen en de cv's van leden waaruit hun deskundigheid blijkt.

4I.2(b) procedures heeft vastgesteld op grond waarvan het kan beoordelen of de betrokken verwerkingsverantwoordelijken en verwerkers in aanmerking komen om de gedragscode toe te passen, toezicht kan houden op de naleving van de bepalingen van de gedragscode door deze laatsten en het de werking van de gedragscode op gezette tijden kan toetsen;

Als tweede eis dient het toezichthoudend orgaan procedures op te stellen over hoe de gedragscode wordt nageleefd en hoe dat wordt gecontroleerd. De procedures moeten aangeven wanneer verwerkingsverantwoordelijken en verwerkers zich onder de gedragscode mogen scharen, hoe naleving wordt gecontroleerd en hoe de gedragscode zelf periodiek wordt getoetst en zo nodig herzien.

4I.2(c) procedures en structuren heeft vastgesteld om klachten te behandelen over inbreuken op de gedragscode of over de wijze waarop daaraan uitvoering is of wordt gegeven door een verwerkingsverantwoordelijke of verwerker, en om die procedures en structuren voor betrokkenen en het publiek transparant te maken; en

De derde eis is dat de gedragscode een procedure heeft voor klachten over de gedragscode in de praktijk (zie ook artikel 40 lid 2 punt k). Deze procedures dienen transparant te zijn voor het publiek en voor betrokkenen.

4I.2(d) ten genoegen van de bevoegde toezichthoudende autoriteit aantoonst dat zijn taken en bevoegdheden niet tot een belangenconflict leiden.

Als laatste eis geldt dat het handelen van het toezichthoudend orgaan niet mag leiden tot belangenconflicten. Voorbeelden zijn dat leden van de toezichthouder banden hebben met aangesloten bedrijven (en deze leden niet gehouden zijn zich dan te verschonen) of giften ontvangen van dergelijke organisaties. Een procedure over hoe om te gaan met potentiële belangenconflicten is dan ook belangrijk.

4I.3 De bevoegde toezichthoudende autoriteit legt de ontwerpeisen inzake accreditatie van een in lid 1 van dit artikel bedoeld orgaan overeenkomstig het in artikel 63 bedoelde coherentiemechanisme voor aan het Comité.

De criteria op grond waarvan een toezichthoudend orgaan van een gedragscode wordt geaccrediteerd, worden door de toezichthouder opgesteld (lid 2). Invoering van deze criteria vereist advies van het Comité (artikel 64 lid 1 punt c).

- 41.4 Onverminderd de taken en bevoegdheden van de bevoegde toezichthoudende autoriteit en de bepalingen van hoofdstuk VIII neemt een in lid 1 bedoeld orgaan, mits er passende waarborgen zijn, de nodige maatregelen ingeval een verwerkingsverantwoordelijke of verwerker een inbreuk pleegt op de gedragscode, waaronder schorsing of uitsluiting van de betrokken verwerkingsverantwoordelijke of verwerker van de gedragscode. Het orgaan stelt de bevoegde toezichthoudende autoriteit in kennis van die maatregelen en van de redenen daarvoor.

Het toezichthoudend orgaan is verplicht om maatregelen te nemen wanneer een verwerkingsverantwoordelijke of verwerker een inbreuk pleegt op de gedragscode. Deze maatregelen moeten redelijk en effectief zijn, en schorsing of uitsluiting moet dus een reële optie zijn bij overtredingen van de gedragscode. Het toezichthoudend orgaan zal de AP of andere toezichthouders hiervan op de hoogte stellen.

- 41.5 De bevoegde toezichthoudende autoriteit trekt de accreditatie van een in lid 1 bedoeld orgaan in indien niet of niet meer wordt voldaan aan de eisen inzake accreditatie of indien de door het orgaan genomen maatregelen inbreuk maken op deze verordening.

De accreditatie van een toezichthoudend orgaan van een gedragscode kan worden ingetrokken wanneer het orgaan niet meer voldoet aan de eisen (lid 2) of wanneer het orgaan maatregelen neemt die in strijd zijn met de AVG. Een voorbeeld van dit laatste zou zijn het goedkeuren van een verwerking die evident niet mag onder de AVG, of het laten passeren van schendingen.

- 41.6 Dit artikel geldt niet voor de verwerking door overheidsinstanties en -organen.

Hoewel ook overheidsinstanties zich mogen conformeren aan een gedragscode, al dan niet specifiek voor die instanties geformuleerd, mogen zij daarbij geen gebruik maken van een geaccrediteerd toezichtsorgaan.

Artikel 42. Certificering

- 42.1 De lidstaten, de toezichthoudende autoriteiten, het Comité en de Commissie bevorderen, met name op Unieniveau, de invoering van certificeringsmechanismen voor gegevensbescherming en gegevensbeschermingszegels en -merktekens waarmee kan worden aangetoond dat verwerkingsverantwoordelijken en verwerkers bij verwerkingen in overeenstemming met deze verordening handelen. Er wordt ook rekening gehouden met de specifieke behoeften van kleine, middelgrote en micro-ondernemingen.

Om betrokkenen in staat te stellen snel het beschermingsniveau van hun privacy bij producten en diensten te laten beoordelen, kent de AVG het mechanisme

van certificering. Hierbij kan een verwerkingsverantwoordelijke of een verwerker via een speciale procedure (het certificeringsmechanisme) een proces van verwerking, een middel voor verwerking of een daarbij ondersteunend middel zoals een beveiliging laten toetsen. Blijkt dit te voldoen aan de certificeringscriteria, dan mag men een bijbehorend zegel of merkteken voeren.

Invoering van mechanismen. Zowel op nationaal- als op Unieniveau zullen mechanismen oftewel procedures voor certificering van technologieën, middelen of verwerkingen worden ingevoerd met bijbehorende zegels en merktekens.

Nut van certificering. Gebruik van gecertificeerde technologieën en middelen dient met name ter versterking van het bewijs dat men als verwerkingsverantwoordelijke zijn verplichtingen nakomt (artikel 24 lid 3). Hetzelfde geldt voor de verwerker (artikel 28 lid 5). Tevens kan een certificering worden gebruikt om te onderbouwen dat de gebruikte middelen voor verwerking voldoen aan *privacy by design* en *by default* (artikel 25 lid 3), dat de beveiliging op orde is (artikel 32 lid 3). Als laatste is de inzet van gecertificeerde mechanismen een boeteverlagende factor bij een schending van de AVG (artikel 83 lid 2 punt j en lid 4 punt b). Een beroep op certificering is echter niet genoeg om een boete of corrigerende maatregel te kunnen voorkomen (zie lid 4).

Behoeften van mkb. Een veelgehoorde klacht onder de Richtlijn was dat het naleven van de vereisten lastig was voor het mkb, omdat er geen manier was om zekerheid te krijgen of iets nu legaal was of niet, of een beveiliging adequaat was et cetera. Het systeem van certificering moet hieraan tegemoet komen.

- 42.2 Ter aanvulling op de naleving door verwerkingsverantwoordelijken of verwerkers die onder deze verordening vallen, kunnen tevens uit hoofde van lid 5 van dit artikel goedgekeurde certificeringsmechanismen voor gegevensbescherming, gegevensbeschermingszegels of -merktekens worden ingevoerd om aan te tonen dat de verwerkingsverantwoordelijken of verwerkers die overeenkomstig artikel 3 niet onder deze verordening vallen, in het kader van de doorgiften van persoonsgegevens aan derde landen of internationale organisaties onder de voorwaarden als bedoeld in artikel 46, lid 2, punt f), passende waarborgen bieden. Die verwerkingsverantwoordelijken of verwerkers doen, via contractuele of andere juridisch bindende instrumenten, bindende en afdwingbare toezeggingen om die passende waarborgen toe te passen, ook wat betreft de rechten van de betrokkenen.

Het gebruik van certificering kan ook van belang zijn voor verwerkingsverantwoordelijken of verwerkers buiten de EU, wanneer deze niet volgens de criteria uit artikel 3 onder de AVG vallen. Gebruik van gecertificeerde middelen of het verrichten van gecertificeerde verwerkingen kan worden aangemerkt als een passende waarborg (artikel 46 lid 2 punt f), hetgeen vereist is voor doorgifte van persoonsgegevens aan zo'n partij wanneer het land in kwestie niet als adequaat

is aangemerkt onder artikel 45. Vergelijk artikel 40 lid 3 voor dezelfde constructie middels gedragscodes.

Bindende toezeggingen. Naast certificering is voor de passende waarborg ook vereist dat deze verwerkingsverantwoordelijken en verwerkers bindende en afdwingbare middelen bieden om nakoming van de waarborgen af te dwingen en met name om betrokkenen hun rechten uit te laten oefenen.

42.3 De certificering is vrijwillig en toegankelijk via een transparant proces.

Gekozen is voor een systeem van vrijwillige certificering. Een verwerkingsverantwoordelijke of verwerker kan dan ook niet worden tegengeworpen dat hij geen gecertificeerde middelen of verwerkingen hanteert. Wel is het gebruiken van gecertificeerde middelen of het binnen een certificering verwerken een boeterverlagende factor (artikel 83 lid 2 punt j).

42.4 Een certificering op grond van dit artikel doet niets af aan de verantwoordelijkheid van de verwerkingsverantwoordelijke of de verwerker om deze verordening na te leven en laat de taken en bevoegdheden van de overeenkomstig artikel 55 of 56 bevoegde toezichthoudende autoriteiten onverlet.

Gebruik van gecertificeerde middelen of zelfs een certificering van een verwerking is niet genoeg om een boete of andere corrigerende maatregel van de toezichthouder (artikel 57 lid 2) te kunnen voorkomen wanneer achteraf blijkt dat deze niet aan de AVG voldoet. Blijkt dat een certificering ten onrechte is afgegeven, dan is het certificeringsorgaan daar mogelijk voor aansprakelijk (artikel 43 lid 4).

42.5 Een certificaat uit hoofde van dit artikel wordt afgegeven door de in artikel 43 bedoelde certificerende organen of door de bevoegde toezichthoudende autoriteit, op grond van de criteria die zijn goedgekeurd door die bevoegde toezichthoudende autoriteit op grond van artikel 58, lid 3, of door het Comité overeenkomstig artikel 63. Indien de criteria door het Comité zijn goedgekeurd, kan dit leiden tot een gemeenschappelijke certificaat, het Europees gegevensbeschermingszegel.

Certificering kan gebeuren door een bevoegde toezichthouder of door een van de daarvoor goedgekeurde certificerende organen (artikel 43). De criteria hiervoor dienen vooraf te zijn opgesteld door de bevoegde toezichthouder (artikel 58 lid 3). Ook het Comité mag criteria opstellen (artikel 63).

Europees gegevensbeschermingszegel. Het Comité kan criteria goedkeuren voor adequate gegevensbescherming (artikel 70 lid 1 punt n). Gecertificeerd worden onder deze criteria betekent dat men het nader in te voeren Europees gegevensbeschermingszegel mag gebruiken naar betrokkenen toe.

- 42.6 De verwerkingsverantwoordelijke of de verwerker die zijn verwerking aan het certificeringsmechanisme onderwerpt, verstrekt aan het in artikel 43 bedoelde certificeringsorgaan, of, waar van toepassing, aan de bevoegde toezichthoudende autoriteit de voor de uitvoering van de certificeringsprocedure noodzakelijke informatie en verleent het orgaan of de autoriteit toegang tot zijn verwerkingsactiviteiten.

Wanneer men een verwerking wil laten certificeren, moet de certificerende instantie (een toezichthouder of een onder artikel 43 lid 1 geautoriseerd orgaan) toegang krijgen tot alle noodzakelijke informatie. Ook moet toegang worden gegeven tot alle betreffende activiteiten, zodat kan worden getoetst of de verwerking werkelijk voldoet aan de eisen van de certificering.

- 42.7 Het certificaat wordt afgegeven aan een verwerkingsverantwoordelijke of een verwerker voor een maximumperiode van drie jaar en kan worden verlengd onder dezelfde voorwaarden, mits bij voortdurend aan de relevante criteria kan worden voldaan. Indien van toepassing wordt het certificaat ingetrokken door de in artikel 43 bedoelde certificerende organen of door de bevoegde toezichthoudende autoriteit, wanneer aan de criteria voor de certificering niet of niet meer wordt voldaan.

Een certificering is maximaal drie jaar geldig en kan worden verlengd. Onduidelijk is voornamelijk of verlenging stilzwijgend gebeurt of dat men na drie jaar opnieuw het certificeringsmechanisme moet doorlopen. Wel kan de certificering op ieder moment worden ingetrokken als blijkt dat niet of niet meer wordt voldaan aan de betreffende eisen.

- 42.8 Het Comité verzamelt alle certificeringsmechanismen en gegevensbeschermingszegels en -merktekens in een register en maakt deze via de daartoe geëigende kanalen openbaar.

Om transparantie naar het publiek te bevorderen, publiceert het Comité informatie over alle mechanismen tot certificering en de zegels en tekens die gecertificeerde mechanismen of processen kunnen ontvangen.

Artikel 43. Certificeringsorganen

43.1 Onverminderd de taken en bevoegdheden van de bevoegde toezichthoudende autoriteit uit hoofde van de artikelen 57 en 58, gaan certificeringsorganen die over de passende deskundigheid met betrekking tot gegevensbescherming beschikken, in voorkomend geval na kennisgeving aan de toezichthoudende autoriteit met het oog op de uitoefening van haar bevoegdheden overeenkomstig artikel 58, lid 2, punt h), over tot afgifte en verlenging van het certificaat.

Om het werk van de toezichthouder te verlichten, kunnen andere instanties worden aangewezen die het proces van certificering (artikel 42) kunnen uitvoeren. Deze instanties controleren een aanvraag voor een certificaat conform de procedure van die certificering, en verstrekken het certificaat alsook het recht om het bijbehorende zegel of merkteken te mogen voeren.

Passende deskundigheid. Alleen een instantie die beschikt over passende deskundigheid met betrekking tot gegevensbescherming mag opereren als certificeringsorgaan. Hiertoe wordt een proces van accreditatie in het leven geroepen (zie hieronder). De instanties moeten verder aan een aantal specifieke eisen voldoen (lid 2). Accreditatie gebeurt voor periodes van vijf jaar en kan daarna worden verlengd (lid 4).

Kennisgeving. Een certificeringsorgaan stelt de betrokken toezichthouder in kennis van een certificering (lid 5). Deze kan de certificering vervolgens intrekken of het certificeringsorgaan opdragen dit te doen (artikel 58 lid 2 punt h).

Toezichthouder. Certificering door een certificeringsorgaan beperkt de taken en bevoegdheden van de bevoegde toezichthouder niet. Een toezichthouder mag dus nog steeds bijvoorbeeld een verwerking verbieden of zelfs een administratieve boete opleggen nadat een certificeringsorgaan heeft bepaald dat de verwerking voldoet aan de AVG.

De lidstaten zorgen ervoor dat die certificeringsorganen worden geaccrediteerd door één van de volgende instanties:

a. de toezichthoudende autoriteit die bevoegd is overeenkomstig artikel 55 of 56;

Een certificeringsorgaan mag worden geaccrediteerd door een bevoegde toezichthouder. Een toezichthouder is bevoegd wanneer het certificeringsorgaan op het grondgebied van de lidstaat van die toezichthouder is gevestigd (artikel 55 lid 1). Indien een certificeringsorgaan is gevestigd in meerdere lidstaten, is de toezichthouder bevoegd van de lidstaat waar de hoofdvestiging van het certificeringsorgaan is gevestigd (artikel 56 lid 1). Zie nader de *Richtlijn 4/2018 inzake de accreditatie van certificeringsorganen op grond van artikel 843 van de algemene verordening gegevensbescherming (2016/679)* van het Comité, 4 juni 2019.

- b. de nationale accreditatie-instantie die is aangewezen in overeenstemming met Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad, in overeenstemming met EN-ISO/IEC 17065/2012 en met de aanvullende eisen die door de overeenkomstig artikel 55 of 56 bevoegde toezichthoudende autoriteit zijn vastgesteld.

Een certificeringsorgaan mag ook worden geaccrediteerd door de nationale accreditatie-instantie. Deze is ingesteld onder Verordening (EG) nr. 765/2008 (die met name de CE-markering voor consumentenelektronica regelt). In Nederland is deze instantie de Raad voor Accreditatie. De voor het certificeringsorgaan bevoegde toezichthouder (zie punt a) mag aanvullende eisen stellen aan de wijze van accreditatie.

- 43.2 De in lid 1 bedoelde certificeringsorganen kunnen overeenkomstig lid 1 uitsluitend worden geaccrediteerd indien zij:

- 43.2(a) ten genoegen van de bevoegde toezichthoudende autoriteit, hun onafhankelijkheid en deskundigheid met betrekking tot het certificeringsonderwerp hebben aangetoond;

De eerste eis voor accreditatie als certificeringsorgaan is dat de instantie onafhankelijk opereert en deskundig is met betrekking tot het onderwerp waarvoor zij certificeringen wenst te verrichten.

- 43.2(b) er zich toe verbonden hebben aan de in artikel 42, lid 5, bedoelde criteria te voldoen, welke zijn goedgekeurd door de op grond van artikel 55 of 56 bevoegde toezichthoudende autoriteit of, overeenkomstig artikel 63, door het Comité;

Als tweede eis voor accreditatie geldt dat de instantie bereid is te werken onder de criteria voor certificering zoals vastgesteld door de toezichthouder of het Comité (artikel 42 lid 5).

- 43.2(c) procedures hebben vastgesteld voor de uitgifte, periodieke toetsing en intrekking van certificeringsmechanismen voor gegevensbescherming, gegevensbeschermingszegels en -merktekens;

De derde eis voor accreditatie is dat de instantie interne procedures en werkregels heeft om certificering uit te voeren en om het gebruik van de bijbehorende zegels en merken te regelen.

43.2(d) procedures en structuren hebben vastgesteld om klachten te behandelen over inbreuken op de certificering of de wijze waarop daaraan uitvoering is of wordt gegeven door de verwerkingsverantwoordelijke of de verwerker, en om die procedures en structuren voor betrokkenen en het publiek transparant te maken; en

Als vierde eis voor accreditatie dient een instantie een transparante klachtprocedure te hebben voor betrokkenen en anderen die signaleren dat een verwerkingsverantwoordelijke of verwerker in strijd handelt met het uitgereikte certificaat.

43.2(e) ten genoegen van de bevoegde toezichthoudende autoriteit, aantoonst dat hun taken en plichten niet tot een belangenconflict leiden.

Als vijfde en laatste eis voor accreditatie dient de instantie aan te tonen dat haar werk als certificeringsorgaan geen belangenconflict zal geven met haar overige werkzaamheden. Een bedrijf dat bijvoorbeeld technische beveiligingen wil certificeren, zal deze tak duidelijk apart moeten opzetten van haar commerciële adviespraktijk over technische beveiliging.

43.3 De accreditatie van de in de leden 1 en 2 bedoelde certificeringsorganen vindt plaats op basis van eisen die zijn goedgekeurd door de op grond van artikel 55 of 56 bevoegde toezichthoudende autoriteit of, overeenkomstig artikel 63, door het Comité. In het geval van een accreditatie in de zin van lid 1, punt b), van dit artikel zijn die eisen een aanvulling op de eisen van Verordening (EG) nr. 765/2008 en de technische regels die een beschrijving van de methoden en procedures van de certificeringsorganen geven.

Voor accreditatie van certificeringsorganen kan de toezichthouder nadere criteria opstellen in aanvulling op lid 2. In het kader van het coherentiemechanisme (artikel 63) mag ook het Comité nadere criteria uitvaardigen voor deze accreditatie (artikel 70 lid 1 punt p). Wanneer accreditatie gebeurt door de nationale accreditatie-instantie (zoals beschreven in lid 1 punt b) worden deze nadere criteria opgezet als aanvulling op hetgeen in de CE-Verordening (765/2008) is bepaald.

43.4 De in lid 1 bedoelde certificeringsorganen zijn verantwoordelijk voor de juiste beoordeling, die tot certificering of de intrekking van die certificering leidt, onverminderd de verantwoordelijkheid van de verwerkingsverantwoordelijke of de verwerker voor de naleving van deze verordening. De accreditatie wordt afgegeven voor een maximumperiode van vijf jaar en kan onder dezelfde voorwaarden worden verlengd, mits het certificeringsorgaan aan de in dit artikel gestelde eisen blijft voldoen.

De certificeringsorganen beoordelen een aanvraag tot certificering en maken daarbij een eigen inschatting in hoeverre de verwerking of het middel in kwestie

voldoet aan de AVG. Dit leidt tot afgifte van een certificaat of afwijzing van de aanvraag. Verstrekking van een certificaat betekent niet dat de verwerkingsverantwoordelijke of verwerker automatisch voldoet aan de AVG.

Accreditatie-periode. Accreditatie gebeurt voor periodes van vijf jaar en kan daarna worden verlengd, aangenomen uiteraard dat het certificeringsorgaan dan nog steeds voldoet aan de eisen voor accreditatie.

43.5 De in lid 1 bedoelde certificeringsorganen stellen de bevoegde toezichthoudende autoriteiten op de hoogte van de redenen voor het afgeven of het intrekken van het aangevraagde certificaat.

Wanneer een certificeringsorgaan een certificering afgeeft of juist intrekt, doet zij daarvan opgaaf aan de toezichthouder. Deze kan de certificering vervolgens intrekken of het certificeringsorgaan opdragen dit te doen (artikel 58 lid 2 punt h).

43.6 De in lid 3 van dit artikel bedoelde voorschriften en de in artikel 42, lid 5, bedoelde criteria worden door de toezichthoudende autoriteit in een eenvoudig toegankelijke vorm openbaar gemaakt. De toezichthoudende autoriteiten delen die eisen en criteria ook mee aan het Comité.

De voorschriften voor accreditatie (lid 3) en de criteria voor certificeringen (artikel 42 lid 5) worden door de toezichthouder openbaar gemaakt en aan het Comité gemeld.

Eenvoudig toegankelijke vorm. De voorschriften en criteria moeten eenvoudig toegankelijk zijn zodat het publiek er makkelijk kennis van kan nemen.

43.7 Indien de voorwaarden voor de accreditatie niet of niet meer worden vervuld of indien de door een certificeringsorgaan genomen maatregelen inbreuk maken op deze verordening trekt de bevoegde toezichthoudende autoriteit of de nationale accreditatie-instantie, onverminderd hoofdstuk VIII, de overeenkomstig lid 1 van dit artikel aan een certificeringsorgaan afgegeven accreditatie in.

Een toezichthouder of accreditatie-instantie is te allen tijde bevoegd de accreditatie van een certificeringsorgaan in te trekken wanneer deze niet meer voldoet aan de voorwaarden voor accreditatie (lid 2) of wanneer deze certificeringen afgeeft die in strijd zijn met de AVG. Een toezichthouder kan tevens administratieve boetes opleggen aan dit certificeringsorgaan (artikel 83 lid 4).

- 43.8 De Commissie is bevoegd overeenkomstig artikel 92 gedelegeerde handelingen vast te stellen met het oog op de nadere invulling van de in aanmerking te nemen eisen voor de in artikel 42, lid 1, bedoelde certificeringsmechanismen voor gegevensbescherming.

De Europese Commissie mag nadere eisen formuleren ten aanzien van procedures voor certificering. Hierbij is inwinnen van advies door het Comité verplicht (artikel 70 lid 1 punt g). Een gedane delegatie moet worden gemeld aan het Europees Parlement en de Raad van Ministers. Zij kunnen vervolgens binnen drie maanden bezwaar daartegen maken.

- 43.9 De Commissie kan uitvoeringshandelingen vaststellen die voorzien in technische normen voor certificeringsmechanismen en gegevensbeschermingszegels en -merktekens en mechanismen ter bevordering en erkenning van die certificeringsmechanismen en gegevensbeschermingszegels en -merktekens. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure.

De Europese Commissie mag normen opstellen voor procedures voor certificering en voor de zegels en merktekens die bij certificering mogen worden gevoerd. Ook mag zij nadere maatregelen nemen om certificering te promoten. Hierbij dient de Commissie het artikel 93-comité te raadplegen, dat vervolgens met meerderheid van stemmen beslist over een positief of negatief advies. Indien het advies positief is, neemt de Commissie de normen of maatregelen aan.

Hoofdstuk V

Doorgifte aan derde landen en internationale organisaties

De Europese Unie is tot op zekere hoogte uniek in haar focus op de bescherming van persoonsgegevens. Zeker over de AVG kan zonder twijfel worden gezegd dat het de strengste wetgeving wereldwijd is waar het de bescherming van dergelijke informatie betreft. Om te voorkomen dat deze bescherming aan kracht verliest, is het doorgeven of laten verwerken van persoonsgegevens door entiteiten buiten de rechtsmacht van de EU aan banden gelegd. Dit hoofdstuk 5 werkt uit op welke wijze dit gebeurt.

Binnen het algemene beginsel van artikel 44 mogen persoonsgegevens worden doorgegeven aan landen met een adequaat (met de EU vergelijkbaar) beschermingsniveau (artikel 45) of wanneer passende waarborgen genomen zijn (artikel 46) dan wel bindende bedrijfsregels vastgelegd zijn (artikel 47). Als geen van deze situaties van toepassing is, dan kunnen persoonsgegevens mogelijk worden doorgegeven op basis van uitdrukkelijke toestemming of een andere specifieke grondslag uit artikel 49. Doorgifte op grond van een gerechtelijk bevel uit een derde land is in principe verboden (artikel 48). Harmonisatie in internationaal verband wordt nagestreefd onder artikel 50.

Artikel 44. Algemeen beginsel inzake doorgiften

Persoonsgegevens die worden verwerkt of die zijn bestemd om na doorgifte aan een derde land of een internationale organisatie te worden verwerkt, mogen slechts worden doorgegeven indien, onverminderd de overige bepalingen van deze verordening, de verwerkingsverantwoordelijke en de verwerker aan de in dit hoofdstuk neergelegde voorwaarden hebben voldaan; dit geldt ook voor verdere doorgiften van persoonsgegevens vanuit het derde land of een internationale organisatie aan een ander derde land of een andere internationale organisatie. Alle bepalingen van dit hoofdstuk worden toegepast opdat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.

Als algemeen beginsel geldt dat doorgifte of verwerking door entiteiten buiten de EU slechts toegestaan is wanneer dit hoofdstuk daartoe een regeling biedt. Wanneer deze entiteiten op zichzelf weer de persoonsgegevens aan anderen willen verstrekken, moet daarvoor apart opnieuw een grondslag binnen dit hoofdstuk aan te wijzen zijn.

Doorgifte. Doorgifte is een vorm van verwerking waarbij persoonsgegevens verstrekt worden aan een andere entiteit. Dit kan zowel een verwerkingsverantwoordelijke als een verwerker zijn. In hoofdstuk V van de AVG gaat het om doorgifte van binnen de EU naar een organisatie in een land buiten de EU. De term ‘doorgifte’ is als zodanig niet gedefinieerd in de AVG. Volgens het Lindqvist-arrest (HvJ EU 6 november 2003, zaaknr. C-101/01) is er nog geen sprake van doorgifte aan derde landen enkel wanneer een internetpagina benaderd kan worden vanuit die derde landen. Het hosten of in de cloud opslaan kan wél een dergelijke doorgifte zijn, wanneer de betrokken dienstverleners in derde landen gevestigd zijn. Ook bij EU-overstijgende verstrekking binnen een concern (bijvoorbeeld van een Europese dochter naar het Amerikaanse moederbedrijf) is sprake van ‘doorgifte’. Door de snelle ontwikkeling van technologie is het lastig, en zijn juristen verdeeld, over de interpretatie van deze term. We zien toezichthouders en gerechtelijke organen “doorgifte” steeds breder interpreteren. Het hosten van software of data in een derde land wordt vaak gezien als doorgifte, maar de Duitse voorzieningenrechter trok dit nog verder door te zeggen dat toegang vanuit een derde land, tot servers in de EU, ook doorgifte is (Bestuursrechter Wiesbaden, 1 december 2021, zaaknummer: Az. 6 L 738/21.WI). Inmiddels biedt het Comité nadere uitleg in de *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (ten tijde van schrijven alleen beschikbaar in het Engels, 24 februari 2023). Daarin wordt ook uitgelegd dat “remote access” kan kwalificeren als doorgifte.

Derde land. De AVG kent geen definitie van een ‘derde land’, maar logischerwijs gaat het hier net als bij de Richtlijn om alle landen buiten de Europese Economische Ruimte (de EU plus Liechtenstein, Noorwegen en IJsland). Zwitserland is weliswaar lid van de Europese Vrijhandelsassociatie (EVA) maar geen lid van de EER, en dus een derde land in de zin van de AVG.

Geen ondermijning. Wanneer een bepaling in dit hoofdstuk voor meerdere interpretaties vatbaar is, dient de interpretatie te worden gekozen die de meeste bescherming geeft aan betrokkenen. Hiermee wordt voorkomen dat de bescherming van de AVG wordt ondergraven.

Overeenkomsten. De EU kan overeenkomsten met derde landen sluiten om de doorgifte van persoonsgegevens naar dat derde land te regelen mits daarin passende waarborgen voor de betrokkenen zijn opgenomen. Een voorbeeld is de Passenger Name Record (PNR) Agreements over vliegtuigpassagier gegevens met de Verenigde Staten, Canada en Australië. De AVG doet geen afbreuk aan dergelijke overeenkomsten (overweging 102). Ook lidstaten kunnen dergelijke overeenkomsten sluiten, echter alleen als deze binnen de regels van de AVG blijven en een adequaat beschermingsniveau bieden voor de grondrechten van de betrokkenen.

Artikel 45. Doorgiften op basis van adequaatheidsbesluiten

45.1 Een doorgifte van persoonsgegevens aan een derde land of een internationale organisatie kan plaatsvinden wanneer de Commissie heeft besloten dat het derde land, een gebied of één of meerdere nader bepaalde sectoren in dat derde land, of de internationale organisatie in kwestie een passend beschermingsniveau waarborgt. Voor een dergelijke doorgifte is geen specifieke toestemming nodig.

De Commissie kan besluiten dat een derde land, een gebied of een welbepaalde sector in een derde land, of een internationale organisatie een passend niveau van gegevensbescherming biedt. Dit besluit heeft dan rechtskracht voor de gehele Unie, en doorgifte naar dat land vereist dan geen nadere waarborgen. De Commissie kan eveneens besluiten om een dergelijk besluit in te trekken. Zie nader het *Werkdocument over adequate doorgifte* (WP 254, december 2017) van de Artikel 29-Werkgroep.

Besluitprocedure. Alvorens een besluit te nemen, dient de Commissie een beoordeling te maken op grond van de criteria van lid 2. Vervolgens legt de Commissie conform lid 3 een conceptbesluit voor aan het comité (artikel 92), dat vervolgens met meerderheid van stemmen beslist over een positief of negatief advies. Na een positief advies neemt de Commissie het besluit en monitort zij vervolgens de praktijk in het betreffende land of organisatie (lid 4), om eventueel tot wijziging, intrekking of schorsing over te gaan (lid 5).

Passend beschermingsniveau. Het beschermingsniveau in derde landen moet passend (adequaat) zijn. Dit houdt niet in dat het niveau minstens dat van de EU zelf moet zijn, oftewel dat men wettelijke bepalingen heeft die stuk voor stuk overeenkomen met de AVG. De bescherming van de grondrechten moet in essentie hetzelfde zijn als in de EU (HvJ EU 6 oktober 2015, ECLI:EU:C:2015:650, Schrems I en HvJ EU 16 juli 2020, ECLI:EU:C:2020:559, Schrems II).

Adequate landen. Bij het schrijven van dit boek bestonden besluiten ten aanzien van Andorra, Argentinië, Canada (alleen voor de commerciële sector en alleen in gebieden waar de *Canadian Personal Information Protection and Electronic Documents Act* van toepassing is), de Faeröer Eilanden, Guernsey, Israël, het Isle of Man, Japan, Jersey, Nieuw-Zeeland, Uruguay, de Republiek Korea, het Verenigd Koninkrijk en Zwitserland. Voor de VS, zie het volgende kopje. Afgezien van Japan, Korea en het Verenigd Koninkrijk zijn deze besluiten genomen onder de Richtlijn. Lid 9 van dit artikel bepaalt echter dat deze besluiten in stand blijven totdat zij worden gewijzigd of ingetrokken door de Commissie. Er zijn geen besluiten ten aanzien van internationale organisaties.

Verenigde Staten. Onder de Richtlijn werd de VS als adequaat land gezien mits men uitsluitend persoonsgegevens doorgaf of liet bewerken door bedrijven die waren aangesloten bij de Safe Harbor-regeling. Deze regeling, en het

daarop gebaseerde adequaatheidsbesluit, werd in 2015 ongeldig verklaard in de Schremszaak (HvJ EU 6 oktober 2015, zaaknr. ECLI:EU:C:2015:650). Na veel politiek gesoebat werd een nieuwe overeenkomst tussen EU en VS gesloten: het Privacy Shield. Op basis van deze overeenkomst werd de VS wederom adequaat verklaard in beslissing 2016/1250 van 12 juli 2016. Ook deze overeenkomst is inmiddels ongeldig verklaard. Dit gebeurde in de zomer van 2020 in de zogenaamde Schrems II zaak (16 juli 2020, ECLI:EU:C:2020:559). Op het moment van het schrijven van dit boek ligt er wederom een nieuwe regeling voor het waarborgen van doorgifte tussen de VS en de EU, het EU-U.S. Data Privacy Framework. De Commissie heeft 13 december 2022 een concept adequaatheidsbesluit hierover gepubliceerd. Dit is nog niet definitief.

Grondslag blijft nodig. Wanneer een derde land (of gebied dan wel specifieke sector in dat land) door de Commissie wordt aangewezen als een land met een passend beschermingsniveau, dan is geen specifieke toestemming nodig voor een doorgifte naar een entiteit in dat land. Dit ontslaat echter verwerkingsverantwoordelijken er natuurlijk niet van een grondslag onder artikel 6 te hebben voor de verwerking in het derde land en zo nodig een verwerkersovereenkomst met de ontvanger aldaar. Bedoeld wordt slechts dat geen toestemming onder artikel 49 lid 1 punt a nodig is voor de doorgifte an sich.

45.2 Bij de beoordeling van de vraag of het beschermingsniveau adequaat is, houdt de Commissie met name rekening met de volgende aspecten:

45.2(a) de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden, de toepasselijke algemene en sectorale wetgeving, onder meer inzake openbare veiligheid, defensie, nationale veiligheid en strafrecht en de toegang van overheidsinstanties tot persoonsgegevens, evenals de tenuitvoerlegging van die wetgeving, gegevensbeschermingsregels, beroepsregels en veiligheidsmaatregelen, met inbegrip van regels voor de verdere doorgifte van persoonsgegevens aan een ander derde land of een andere internationale organisatie die in dat land of die internationale organisatie worden nageleefd, precedenter in de rechtspraak, alsmede het bestaan van effectieve en afdwingbare rechten van betrokkenen en effectieve mogelijkheden om administratief beroep of beroep in rechte in te stellen voor betrokkenen wier persoonsgegevens worden doorgegeven;

45.2(b) het bestaan en het effectief functioneren van een of meer onafhankelijke toezichthoudende autoriteiten in het derde land of waaraan een internationale organisatie is onderworpen, welke tot taak heeft of hebben de naleving van de gegevensbeschermingsregels te verzekeren en deze onder meer met passende handhavingsbevoegdheden te handhaven, betrokkenen bij de uitoefening van hun rechten bij te staan en te adviseren en met de toezichthoudende autoriteiten van de lidstaten samen te werken; en

45.2(c) de internationale toezeggingen die het derde land of de internationale organisatie in kwestie heeft gedaan, of andere verplichtingen die voortvloeien uit juridisch bindende overeenkomsten of instrumenten, alsmede uit de deelname van dat derde land of die internationale organisatie aan multilaterale of regionale regelingen, in het bijzonder met betrekking tot de bescherming van persoonsgegevens.

De Europese Commissie neemt besluiten ten aanzien van adequate bescherming van persoonsgegevens op basis van alle omstandigheden van het geval, maar de nadruk zal liggen op de wijze waarop in het derde land (of de internationale organisatie) in het algemeen tegen persoonsgegevens aan wordt gekeken en hoe de daarbij behorende rechtspraak is georganiseerd. Ook de onafhankelijke toezichthouder op bescherming van persoonsgegevens is een belangrijke factor, net als het doen van toezeggingen of het onderschrijven van internationale regelingen zoals het Internationaal Verdrag betreffende Burgerrechten en Politieke Rechten (IVBPR of BUPO).

45.3 De Commissie kan, na de beoordeling van de vraag of het beschermingsniveau adequaat is, door middel van een uitvoeringshandeling besluiten dat een derde land, een gebied of één of meerdere nader bepaalde sectoren in een derde land, of een internationale organisatie een passend beschermingsniveau in de zin van lid 2 van dit artikel waarborgt. De uitvoeringshandeling voorziet in een mechanisme voor periodieke toetsing, minstens om de vier jaar, waarbij alle relevante ontwikkelingen in het derde land of de internationale organisatie in aanmerking worden genomen. In de uitvoeringshandeling worden het territoriale en het sectorale toepassingsgebied vermeld, alsmede, in voorkomend geval, de in lid 2, punt b), van dit artikel genoemde toezichthoudende autoriteit(en). De uitvoeringshandeling wordt vastgesteld volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure.

Zoals hierboven is aangegeven, neemt de Commissie het besluit pas nadat zij dit aan het comité van artikel 93 heeft voorgelegd en een positief advies heeft ontvangen. Ook het Comité geeft advies (artikel 70 lid 1 punt s).

Periodieke toetsing. Het besluit dient een mechanisme te bevatten dat de Commissie dwingt tot periodieke toetsing (ten minste elke vier jaar) of het besluit nog gehandhaafd kan worden. Het besluit dient tevens te verwijzen in welke gebied(en) in het land het geldt en welke toezichthouder (indien aanwezig) in het betreffende land betrokken is. Zie ook het doorlopend toezicht uit het volgende lid.

Overleg. De periodieke toetsing dient in overleg met het derde land of de internationale organisatie in kwestie te worden uitgevoerd en moet rekening houden met alle relevante ontwikkelingen in het derde land of de internationale organisatie. Verder dient de Commissie rekening te houden met de opvattingen en

bevindingen van het Europees Parlement en van de Raad, evenals met andere relevante organisaties en bronnen. De Commissie moet binnen een redelijke termijn de werking van laatstgenoemde besluiten evalueren en alle relevante vaststellingen rapporteren aan het comité bedoeld in artikel 93.

- 45-4 De Commissie houdt doorlopend toezicht op ontwikkelingen in derde landen en internationale organisaties die mogelijk gevolgen hebben voor het functioneren van krachtens lid 3 van dit artikel vastgestelde besluiten en van op grond van artikel 25, lid 6, van Richtlijn 95/46/EG vastgestelde besluiten.

Nadat het besluit is genomen, dient de Commissie de betreffende derde landen en organisaties te monitoren op het gebied van persoonsgegevens. Wanneer zij vermoedt dat een land of organisatie niet langer als adequaat te zien is, gaat zij over tot intrekking, wijziging of schorsing conform lid 5. Deze monitorplicht geldt ook voor de besluiten genomen ten tijde van de Richtlijn (zie ook lid 9).

- 45-5 De Commissie gaat, wanneer uit beschikbare informatie blijkt, in het bijzonder naar aanleiding van de in lid 3 van dit artikel bedoelde toetsing, dat een derde land, een gebied of één of meerdere nader bepaalde sectoren in een derde land, of een internationale organisatie niet langer een passend beschermingsniveau in de zin van lid 2 van dit artikel waarborgt, voor zover nodig, bij uitvoeringshandelingen zonder terugwerkende kracht over tot intrekking, wijziging of schorsing van het in lid 3 van dit artikel bedoelde besluit. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure.

Wanneer de Commissie vermoedt dat een land of organisatie niet langer als adequaat te zien is, gaat zij over tot intrekking, wijziging of schorsing van het betreffende besluit. De wijziging kan ook het uitsluiten van een gebied of sector betreffen. Hierbij is advies van het Comité nodig (artikel 70 lid 1 punt s).

Geen terugwerkende kracht. Vanuit het oogpunt van rechtszekerheid mogen intrekking, wijziging of schorsing geen terugwerkende kracht hebben.

Onderzoeksprocedure. Tot intrekking, wijziging of schorsing wordt besloten op dezelfde manier als het oorspronkelijke besluit tot stand kwam (zie lid 3).

Om naar behoren gemotiveerde dwingende redenen van urgentie, stelt de Commissie onmiddellijk van toepassing zijnde uitvoeringshandelingen vast volgens de in artikel 93, lid 3, bedoelde procedure.

In urgente gevallen mag de Commissie gemotiveerd afwijken van de gewone overlegprocedure (artikel 93 lid 3). De Commissie mag dan zonder voorafgaande voorlegging aan het artikel 93-comité een besluit nemen dat gedurende ten hoogste zes maanden van kracht is. Dit zal in de regel een opschorting zijn van het adequaatheidsbesluit, maar zou ook een tijdelijke wijziging kunnen zijn.

Binnen 14 dagen moet het comité de handeling voorgelegd krijgen voor advies. Indien het advies negatief is, trekt de Commissie de betreffende uitvoeringshandeling onmiddellijk in.

- 45.6 De Commissie pleegt overleg met het derde land of de internationale organisatie om de situatie naar aanleiding waarvan het besluit overeenkomstig lid 5 is vastgesteld, te verhelpen.

Doel van het overleg is met het derde land of de internationale organisatie te komen tot een compromis waarmee het besluit in stand kan blijven. Eventueel kan het besluit worden gewijzigd.

- 45.7 Een overeenkomstig lid 5 van dit artikel vastgesteld besluit laat de doorgiften van persoonsgegevens aan het derde land, of een gebied of één of meerdere nader bepaalde sectoren in dat derde land, of de internationale organisatie in kwestie overeenkomstig de artikelen 46 tot en met 49 onverlet.

Wanneer een besluit wordt ingetrokken, geschorst of gewijzigd, blijft het mogelijk om doorgiften te verrichten onder de andere artikelen uit dit hoofdstuk.

- 45.8 De Commissie maakt in het Publicatieblad van de Europese Unie en op haar website een lijst bekend van de derde landen, gebieden en nader bepaalde sectoren in derde landen en internationale organisaties waarvoor zij bij besluit heeft vastgesteld dat deze wel of niet langer een passend beschermingsniveau waarborgen.

Genomen besluiten worden in het Publicatieblad van de Europese Unie gepubliceerd, alsook op de website van de Commissie. De huidige versie van de lijst is te vinden op https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

- 45.9 De besluiten die de Commissie op grond van artikel 25, lid 6, van Richtlijn 95/46/EG heeft vastgesteld, blijven van kracht, totdat zij worden gewijzigd, vervangen of ingetrokken bij een overeenkomstig lid 3 of lid 5 van dit artikel vastgesteld besluit van de Commissie.

Het mechanisme uit dit artikel bestond ook al onder de Richtlijn. Om nu te voorkomen dat al deze besluiten opnieuw moeten worden genomen, bepaalt lid 9 dat deze van kracht blijven totdat de Commissie ze wijzigt, vervangt of intrekt. Zie ook artikel 96 dat de bijbehorende overeenkomsten met de derde landen in stand laat.

Artikel 46. Doorgiften op basis van passende waarborgen

- 46.1 Bij ontstentenis van een besluit uit hoofde van artikel 45, lid 3, mag een doorgifte van persoonsgegevens aan een derde land of een internationale organisatie door een verwerkingsverantwoordelijke of een verwerker alleen plaatsvinden mits zij passende waarborgen bieden en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken.

Wanneer een land of organisatie niet als adequaat is aangemerkt onder artikel 45, is doorgifte alleen toegestaan wanneer sprake is van passende waarborgen (zoals uitgewerkt in lid 2) en afdwingbare rechten en rechtsmiddelen voor betrokkenen. Zowel de verwerkingsverantwoordelijke als de verwerker heeft daarbij de plicht na te gaan of die waarborgen er zijn, en passende maatregelen te nemen als dat niet het geval blijkt.

Passende waarborgen. De AVG introduceert een open norm: als de verwerkingsverantwoordelijke (of verwerker) kan aantonen dat waarborgen zijn genomen die passen bij de betreffende doorgifte, dan is aan artikel 46 voldaan. Lid 2 noemt een aantal standaardwaarborgen, en lid 3 biedt de mogelijkheid contractuele waarborgen in te voeren met toestemming van de toezichthouder. In theorie zou een verwerkingsverantwoordelijke ook op andere manieren aan de norm kunnen voldoen, al is moeilijk voorstelbaar hoe.

Vereisten. De genomen waarborgen moeten de rechten van betrokkenen en plichten voor verwerkingsverantwoordelijken (en verwerkers) effectueren. Betrokkenen moeten met name hun rechten kunnen afdwingen, in beroep kunnen bij rechter of toezichthouder tegen handelen van een verwerkingsverantwoordelijke buiten de EU en daarbij naleving of een schadevergoeding kunnen eisen. Ook moeten zij de beginselen uit de AVG borgen; naast de algemene beginselen (artikel 6) met name de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (artikel 25).

- 46.2 De in lid 1 bedoelde passende waarborgen kunnen worden geboden door de volgende instrumenten, zonder dat daarvoor specifieke toestemming van een toezichthoudende autoriteit is vereist:

- 46.2(a) een juridisch bindend en afdwingbaar instrument tussen overheidsinstanties of -organen;

Doorgiften kunnen worden verricht door overheidsinstanties of -organen met overheidsinstanties of -organen in derde landen of met internationale organisaties met overeenkomstige taken en functies. In die situaties moeten wettelijke of administratieve, maar in ieder geval juridisch bindende, regelingen worden getroffen om de passende waarborgen uit lid 1 te kunnen garanderen. Overweging 108 noemt een memorandum van overeenstemming met afdwingbare en bruikbare rechten voor betrokkenen. Wanneer een niet juridisch bindende ad-

ministratieve regeling wordt gebruikt, moet de betreffende overheidsinstantie toestemming hebben van de toezichthouder (lid 3 punt b).

46.2(b) bindende bedrijfsvoorschriften overeenkomstig artikel 47;

Binnen een concern of groep van ondernemingen is het mogelijk passende waarborgen te realiseren middels bindende bedrijfsvoorschriften (*binding corporate rules* of BCR). Dit zijn (zie artikel 4 definitie 20) beleidsregels over doorgifte(n) van persoonsgegevens aan concernonderdelen in derde landen. Deze beleidsregels moeten voldoen aan de algemene eisen uit lid 1 en zijn goedgekeurd door de toezichthouder (zie artikel 47).

46.2(c) standaardbepalingen inzake gegevensbescherming die door de Commissie volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure zijn vastgesteld;

De Commissie heeft de mogelijkheid standaardbepalingen inzake gegevensbescherming (*model clauses*) op te stellen. Door deze in een overeenkomst met een ontvanger in een derde land op te nemen, kunnen de benodigde passende waarborgen contractueel worden gerealiseerd. Op moment van schrijven is de laatste versie van deze standaardbepalingen uit juni 2021. In tegenstelling tot de vorige versies, zijn er nu vier modules die zien op de verhoudingen verwerkingsverantwoordelijke naar verwerker, verwerker naar subverwerker, verwerker naar verwerkingsverantwoordelijke en verwerkingsverantwoordelijke naar verwerkingsverantwoordelijke. Bovendien voldoen deze standaardbepalingen ook aan alle vereisten van artikel 28 voor een verwerkersovereenkomst. Het is niet nodig om deze bepalingen in een apart document af te sluiten.

DTIA. Onder clause 12 van de standaardbepalingen worden partijen verplicht om te concluderen dat de lokale wetten en praktijken geen belemmering vormen voor de partij in het derde land om aan de verplichtingen onder de standaardbepalingen te kunnen voldoen. Dit was onder de vorige standaardbepalingen ook al het geval, maar in de nieuwe bepalingen moet deze analyse op verzoek van de toezichthouder beschikbaar aan haar worden gesteld. Deze analyse noemt men vaak de Data Transfer Impact Assessment, of DTIA.

Onderzoeksprocedure. De Commissie dient ontwerpbeoordelingen voor te leggen aan het artikel 93-comité. Na een positief advies worden deze goedgekeurd.

46.2(d) standaardbepalingen inzake gegevensbescherming die door een toezichthoudende autoriteit zijn vastgesteld en die door de Commissie volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure zijn goedgekeurd;

Naast de Commissie mogen individuele toezichthouders ook standaardbepalingen opstellen. Inhoudelijk geldt hiervoor hetzelfde als de standaardbepalingen die de Commissie onder punt c kan opstellen. De goedkeuring door de toezichthouder vereist advies van het Comité (artikel 64 lid 1 punt d).

Afstemming. Op grond van artikel 63 dienen toezichthoudende autoriteiten met elkaar en waar passend met de Commissie samen te werken om te zorgen voor een consequente toepassing van de AVG. Bovendien dient de Commissie (na advies van het artikel 93-comité) de standaardbepalingen goed te keuren. De kans is daarmee klein dat een toezichthouder standaardbepalingen zou voorstellen die afwijken van de koers die de Commissie wil varen.

46.2(e) een overeenkomstig artikel 40 goedgekeurde gedragscode, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen, onder meer voor de rechten van de betrokkenen, toe te passen; of

Onder artikel 40 kan een sector of brancheorganisatie gedragscodes opstellen over een passende verwerking van persoonsgegevens. Een gedragscode mag ook regelen hoe doorgifte naar derde landen wordt geborgd. Als deze gedragscode is goedgekeurd door de toezichthouder (artikel 41), kan op grond van de gedragscode worden doorgegeven.

46.2(f) een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen, onder meer voor de rechten van de betrokkenen, toe te passen.

Onder artikel 42 kunnen certificeringsmechanismen worden ingevoerd waarmee organisaties kunnen aantonen dat zij in overeenstemming met de AVG handelen. Een certificering kan gericht zijn op doorgifte aan derde landen. Wanneer daarbij juridisch bindende toezeggingen van de ontvanger in het derde land worden getroffen, biedt een certificering een passende waarborg.

46.3 Onder voorbehoud van de toestemming van de bevoegde toezichthoudende autoriteit kunnen de in lid 1 bedoelde passende waarborgen ook worden geboden door, met name:

De in lid 2 genoemde waarborgen mogen worden ingezet zonder nadere toestemming. Lid 3 biedt nog twee aanvullende waarborgen, die echter wel vooraf moeten zijn goedgekeurd door de bevoegde toezichthouder.

46.3(a) contractbepalingen tussen de verwerkingsverantwoordelijke of de verwerker en de verwerkingsverantwoordelijke, de verwerker of de ontvanger van de persoonsgegevens in het derde land of de internationale organisatie; of

Verwerkingsverantwoordelijken of verwerkers kunnen ook eigen contractuele bepalingen opstellen voor doorgifte naar ontvangers in derde landen. Dit biedt ten opzichte van de standaardbepalingen uit lid 2 punten c en d het voordeel dat de bepalingen op maat gesneden kunnen worden voor de voorgenomen verwerking. Dergelijke bepalingen moeten vooraf zijn goedgekeurd door de

toezichthouder (artikel 57 lid 1 punt r), waarbij de toezichthouder een en ander af moet stemmen met de andere toezichthouders en de Commissie (zie lid 4). Deze goedkeuring is in Nederland een besluit in de zin van de Algemene wet bestuursrecht. De goedkeuring vereist advies van het Comité (artikel 64 lid 1 punt e).

46.3(b) bepalingen die moeten worden opgenomen in administratieve regelingen tussen overheidsinstanties of -organen, waaronder afdwingbare en effectieve rechten van betrokkenen.

Onder lid 2 punt a kunnen overheidsinstanties passende waarborgen opnemen in een juridisch bindend en afdwingbaar instrument met hun tegenhangers in derde landen. Wanneer zij echter kiezen voor een niet-bindend instrument is de voorafgaande toestemming van de toezichthouder nodig. Het instrument zal dan de rechten van betrokkenen afdwingbaar moeten maken. De toezichthouder moet een en ander afstemmen met andere toezichthouders en de Commissie (zie lid 4).

46.4 De toezichthoudende autoriteit past het in artikel 63 bedoelde coherentiemechanisme toe in de in lid 3 van dit artikel vermelde gevallen.

Artikel 63 vereist een consequente toepassing van de AVG in alle lidstaten. Op grond van dit lid 4 geldt dit beginsel natuurlijk ook bij het goedkeuren van de contractuele bedingen en administratieve regelingen uit lid 3.

46.5 Toestemmingen die een lidstaat of een toezichthoudende autoriteit op grond van artikel 26, lid 2, van Richtlijn 95/46/EG heeft verleend, blijven geldig totdat zij door die toezichthoudende autoriteit, indien nodig, worden gewijzigd, vervangen of ingetrokken. De besluiten die de Commissie op grond van artikel 26, lid 4, van Richtlijn 95/46/EG heeft vastgesteld, blijven van kracht totdat zij bij een overeenkomstig lid 2 van dit artikel vastgesteld besluit van de Commissie, indien nodig, worden gewijzigd, vervangen of ingetrokken.

Toestemming door lidstaat. Op grond van artikel 26 lid 2 van de Richtlijn (in Nederland artikel 77 lid 2 Wbp) kon een lidstaat toestemming geven voor een doorgifte of een categorie van doorgiften van persoonsgegevens naar een derde land dat geen adequaat niveau van gegevensbescherming bood, mits de betrokken verwerkingsverantwoordelijke langs contractuele of andere weg wél adequate bescherming kon bieden. Deze besluiten tot toestemming blijven van kracht tot hun eerstvolgende wijziging, vervanging of intrekking. Nederland heeft nooit van deze mogelijkheid gebruik gemaakt.

Besluiten modelcontracten. Op grond van artikel 26 lid 4 van de Richtlijn kon de Commissie besluiten dat bepaalde modelcontractbepalingen voldoende waarborgen boden in de zin van lid 2 van diezelfde Richtlijn. Dit betreft twee sets besluiten voor overdracht tussen twee verwerkingsverantwoordelijken

(2001/497/EC en 2004/915/EC) en één besluit voor overdracht van een verwerkingsverantwoordelijke binnen de EU naar een verwerker daarbuiten (2010/87/EU). Deze besluiten zijn inmiddels niet meer geldig, aangezien de nieuwe standaardbepalingen deze verhoudingen dekken.

Artikel 47. Bindende bedrijfsvoorschriften

47.1 De bevoegde toezichthoudende autoriteit keurt in overeenstemming met het in artikel 63 bedoelde coherentiemechanisme bindende bedrijfsvoorschriften goed, op voorwaarde dat deze:

Wanneer een land of organisatie niet als adequaat is aangemerkt onder artikel 45, is doorgifte alleen toegestaan wanneer sprake is van passende waarborgen. Specifiek binnen een concern of groep van ondernemingen is het mogelijk dergelijke waarborgen te realiseren middels zogeheten bindende bedrijfsvoorschriften (*binding corporate rules* of BCR). Dit zijn (zie artikel 4 definitie 20) beleidsregels over doorgifte(n) van persoonsgegevens aan concernonderdelen in derde landen. Bindende bedrijfsvoorschriften mogen pas worden gebruikt nadat zij zijn goedgekeurd (artikel 57 lid 1 punt s) door de bevoegde toezichthouder.

Concern of groepering. Bindende bedrijfsvoorschriften mogen worden gebruikt door bedrijven in een concern of groepering (zie punt a). Naast de groep (artikel 2:24b BW) valt hier in beginsel ook een lossere samenwerking tussen bedrijven onder zoals in een joint venture (overweging 85). Het is niet relevant of een bedrijf in de groep verwerker of verwerkingsverantwoordelijke is. BCR borgen de doorgifte naar een bedrijfsonderdeel buiten Europa, en dat staat los van de rol waarin men verwerkt.

Bevoegde toezichthouder. De bevoegde toezichthouder is de toezichthouder van de lidstaat waar de hoofdvestiging van het concern gevestigd is (artikel 56 lid 1). Als deze buiten de EU ligt, is de toezichthouder bevoegd voor de lidstaat waar de vertegenwoordiger (artikel 27) gevestigd is.

Coherentiemechanisme. De toezichthouder moet ook bij goedkeuring van bindende bedrijfsvoorschriften het coherentiemechanisme (artikel 63) in acht nemen. Zo lopen deze besluiten niet uiteen. De goedkeuring vereist verder nog advies van het Comité (artikel 64 lid 1 punt f).

47.1(a) juridisch bindend zijn voor, van toepassing zijn op en worden gehandhaafd door alle betrokken leden van het concern, of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen, met inbegrip van hun werknemers;

Zoals de naam al aangeeft, moeten de bedrijfsvoorschriften bindend zijn voor de betrokken organisaties binnen het concern of de groep van ondernemingen.

De meest voor de hand liggende manier is een contractuele afspraak tussen de betreffende organisaties. Ook eenzijdig bindende verklaringen kunnen juridisch bindend zijn. Het is formeel niet verplicht dat bindende bedrijfsvoorschriften in één document zijn opgenomen, maar dit is wel sterk aan te bevelen.

47.1(b) betrokkenen uitdrukkelijk afdwingbare rechten toekennen met betrekking tot de verwerking van hun persoonsgegevens; en

Een belangrijke eis bij bindende bedrijfsvoorschriften is dat zij betrokkenen afdwingbare rechten geven, meer precies de rechten uit hoofdstuk III. Dit kan naar Nederlands recht worden vormgegeven door hen als derde-begunstigde bij de overeenkomst tussen de organisaties op te nemen. Ook zou men ervoor kunnen kiezen te bepalen dat de organisatie die direct met de betrokkenen zaken doet, namens hen deze rechten kan invoeren.

47.1(c) voldoen aan de in lid 2 vastgestelde vereisten.

Lid 2 werkt nader uit welke elementen in ieder geval in bindende bedrijfsvoorschriften moeten worden opgenomen. Meer algemeen moeten bindende bedrijfsvoorschriften voldoen aan de eisen uit artikel 46 lid 1.

47.2 In de in lid 1 bedoelde bindende bedrijfsvoorschriften worden minstens de volgende elementen vastgelegd:

Bindende bedrijfsvoorschriften zijn bij voorkeur opgezet als contracten met daarin de in dit lid 2 genoemde elementen. De werkdocumenten over Binding Corporate Rules (WP 256 voor verwerkingsverantwoordelijken en WP 257 voor verwerkers) van de Artikel 29-Werkgroep zetten de gewenste inhoud van dergelijke concern-overeenkomsten op een rijtje.

47.2(a) de structuur en de contactgegevens van het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen en van elk van haar leden;

Allereerst dienen de bindende bedrijfsvoorschriften de bedrijfsstructuur te schetsen van het concern of de groep van ondernemingen. Dit kan gebeuren middels een organogram dat per organisatie de positie laat zien, gecombineerd met een lijst van de statutaire namen, KVK-inschrijvingen en aanduidingen van het soort rechtspersoon.

47.2(b) de gegevensdoorgiften of reeks van doorgiften, met inbegrip van de categorieën van persoonsgegevens, het soort verwerking en de doeleinden daarvan, het soort betrokkenen in kwestie en de identificatie van het derde land of de derde landen in kwestie;

De bindende bedrijfsvoorschriften moeten ook toelichten welke categorieën persoonsgegevens worden doorgegeven en aan welke derde landen. Tevens moet daarbij worden vermeld in het kader van welke verwerkingen en voor welke doelen dat gebeurt. Vergelijk artikel 13 lid 1 waarin vergelijkbare informatie moet worden verstrekt wanneer persoonsgegevens worden verkregen.

47.2(c) het intern en extern juridisch bindende karakter;

De bindende bedrijfsvoorschriften moeten expliciet benadrukken dat zij bindend zijn, zowel tussen de organisaties van het concern als ten behoeve van betrokkenen. De regels moeten niet bijvoorbeeld uitsluitend als intern beleid worden opgesteld.

47.2(d) de toepassing van de algemene beginselen inzake gegevensbescherming, met name doelbinding, minimale gegevensverwerking, beperkte opslagtermijnen, kwaliteit van gegevens, gegevensbescherming door standaardinstellingen en door ontwerp, rechtsgrond voor verwerking, verwerking van bijzondere categorieën van persoonsgegevens, maatregelen om gegevensbeveiliging te waarborgen, en de vereisten inzake verdere doorgiften aan organen die niet door bindende bedrijfsvoorschriften zijn gebonden;

De bindende bedrijfsvoorschriften moeten verder expliciet benoemen dat de algemene beginselen van gegevensbescherming (artikel 5) en specifiek die van *privacy by design and default* (artikel 25) gewaarborgd zullen worden binnen het concern. Ook de rechtsgronden voor verwerking (artikel 6) en de beveiligingsmaatregelen (artikel 32) en verdere doorgifte (artikel 44) moeten worden genoemd.

47.2(e) de rechten van betrokkenen in verband met verwerking en de middelen om die rechten uit te oefenen, waaronder het recht om niet te worden onderworpen aan louter op geautomatiseerde verwerking gebaseerde besluiten, met inbegrip van profilering overeenkomstig artikel 22, het recht om een klacht in te dienen bij de bevoegde toezichthoudende autoriteit, om een vordering in te stellen bij de bevoegde gerechten van de lidstaten overeenkomstig artikel 79, en om schadeloosstelling en, in voorkomend geval, een vergoeding te verkrijgen voor een inbreuk op de bindende bedrijfsvoorschriften;

Ten behoeve van bescherming van betrokkenen moeten bindende bedrijfsvoorschriften expliciet benoemen dat deze betrokkenen de rechten hebben uit hoofdstuk III. Met name van belang zijn de geautomatiseerde besluitvorming

(artikel 22), het klachtrecht (artikel 79) en het recht op schadevergoeding. Dit recht op schadevergoeding zal moeten worden vormgegeven als een contractueel recht analoog aan artikel 82.

47.2(f) de aanvaarding door de op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker van aansprakelijkheid voor alle inbreuken op de bindende bedrijfsvoorschriften door een niet in de Unie gevestigd betrokken lid; de verwerkingsverantwoordelijke of de verwerker wordt alleen geheel of gedeeltelijk van deze aansprakelijkheid ontheven, indien hij bewijst dat dat lid niet verantwoordelijk is voor het schadebrengende feit;

Omdat handhaving van bindende bedrijfsvoorschriften op concernonderdelen buiten de EU lastig kan zijn, is gekozen voor een systeem waarbij een verwerkingsverantwoordelijke of verwerker binnen de EU aansprakelijk dient te zijn voor naleving van deze voorschriften.

Niet verantwoordelijk. Het Europese concernonderdeel ontsnapt slechts aan aansprakelijkheid wanneer zij kan bewijzen in het geheel niet verantwoordelijk te zijn voor de schade. Vergelijk artikel 82 lid 3. Hiervan zal niet snel sprake zijn; doorgifte aan een concern-lid dat de AVG niet naleeft, is al snel een verwijtbare fout van de doorgevende entiteit.

47.2(g) de wijze waarop, in aanvulling op de in de artikelen 13 en 14 bedoelde informatie, aan betrokkenen informatie wordt verschaft over de bindende bedrijfsvoorschriften, met name over de bepalingen in de punten d), e) en f);

De bindende bedrijfsvoorschriften dienen aan te geven hoe zij ter kennis worden gebracht van betrokkenen. Dit kan gebeuren in combinatie met de gewone informatieverstrekking onder artikelen 13 en 14.

47.2(h) de taken van elke overeenkomstig artikel 37 aangewezen FG, of elke andere persoon of entiteit die is belast met het toezicht op de naleving van de bindende bedrijfsvoorschriften binnen het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen, op opleiding en op de behandeling van klachten;

Wanneer een concern een of meer functionarissen voor gegevensbescherming (artikel 37) heeft benoemd, moeten hun taken en onderlinge samenwerking in de bindende bedrijfsvoorschriften zijn benoemd. Buiten de EU kunnen deze personen andere rollen of verantwoordelijkheden krijgen, bijvoorbeeld als taak van een algemene *compliance officer* of bedrijfsjurist.

47.2(i) de klachtenprocedures;

De bindende bedrijfsvoorschriften moeten uitwerken hoe klachten kunnen worden ingediend en hoe deze vervolgens zullen worden afgehandeld.

47.2(j) de binnen het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen bestaande procedures om te controleren of de bindende bedrijfsvoorschriften zijn nageleefd. Dergelijke procedures omvatten gegevensbeschermingsaudits en -methoden om te zorgen voor corrigerende maatregelen ter bescherming van de rechten van de betrokkene. De resultaten van dergelijke controles dienen te worden meegedeeld aan de in punt h) bedoelde persoon of entiteit en aan de raad van bestuur van de onderneming die zeggenschap uitoefent over een concern, of van de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen, en dienen op verzoek ter beschikking van de bevoegde toezichthoudende autoriteit te worden gesteld;

Bindende bedrijfsvoorschriften moeten verder aangeven hoe hun interne naleving wordt geborgd. Deze borging dient in ieder geval audits en procedures te omvatten om naleving te controleren en gemaakte fouten te verbeteren zodat zij niet nogmaals optreden.

Rapportage. Resultaten van de borging moeten worden gerapporteerd aan de functionaris(sen) voor gegevensbescherming (of andere daartoe aangestelde persoon, zie punt h) en aan de raad van bestuur of een ander hoogste orgaan binnen het concern. Ook de toezichthouder kan een kopie van deze resultaten verlangen.

47.2(k) de procedures om die veranderingen in de regels te melden, te registreren en aan de toezichthoudende autoriteit te melden;

Bindende bedrijfsvoorschriften kunnen worden herzien. Zij dienen dan ook op dit punt een wijzigingsprocedure te bevatten. Omdat bindende bedrijfsvoorschriften slechts mogen worden ingevoerd na goedkeuring (zie lid 1), geldt dit natuurlijk ook voor de wijzigingen.

“Die veranderingen in de regels”. De originele tekst van dit punt k spreekt van “procedures om *die* veranderingen in de *regels* te melden”. Dit laatste lijkt een vertaalfout van het Engelse *rules: binding corporate rules* heten in het Nederlands bindende bedrijfsvoorschriften. Het woord ‘die’ is onverklaarbaar.

47.2(l) de procedure voor samenwerking met de toezichthoudende autoriteit om ervoor te zorgen dat alle leden van het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen de bindende bedrijfsvoorschriften naleven, in het bijzonder door de resultaten van de in punt j) bedoelde controles ter beschikking van de toezichthoudende autoriteit te stellen;

Bindende bedrijfsvoorschriften moeten verder aangeven hoe alle onderdelen van het concern samen zullen werken met de bevoegde toezichthouder. Dit betreft afgifte van de rapportages uit punt j, maar kan ook andere verstrekking van informatie of aanpassing van procedures betreffen.

47.2(m) de procedures om eventuele wettelijke voorschriften waaraan een lid van het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen in een derde land is onderworpen en die waarschijnlijk een aanzienlijk negatief effect zullen hebben op de door de bindende bedrijfsvoorschriften geboden waarborgen, aan de bevoegde toezichthoudende autoriteit te melden; en

Landen buiten de EU kunnen andere wetgeving hebben die bedrijven verplicht om (persoons)gegevens te verstrekken die zij onder zich hebben. Dit kan strijd met de AVG opleveren. Bindende bedrijfsvoorschriften dienen dan ook een procedure te bevatten om dit tijdig te signaleren en de toezichthouder te informeren over het waarschijnlijke negatieve effect van deze wetgeving. De toezichthouder kan dan besluiten tot een corrigerende maatregel (artikel 57 lid 2) of een intrekking van de goedkeuring van de bedrijfsvoorschriften.

47.2(n) de passende opleiding inzake gegevensbescherming voor personeel dat permanent of op regelmatige basis toegang tot persoonsgegevens heeft.

Als laatste dienen bindende bedrijfsvoorschriften te vermelden hoe het betrokken personeel wordt opgeleid en bijgeschoold om passende kennis op het gebied van persoonsgegevens te hebben. Dit kennisniveau zal niet hetzelfde hoeven te zijn als dat van een functionaris (artikel 38 lid 2) maar moet genoeg zijn om zijn of haar werk te doen en daarbij te weten of de AVG zou worden overtreden.

47.3 De Commissie kan het model en de procedures voor de uitwisseling van informatie over bindende bedrijfsvoorschriften in de zin van dit artikel tussen verwerkingsverantwoordelijken, verwerkers en toezichthoudende autoriteiten nader bepalen. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure.

Ter bevordering van een snelle evaluatie en goedkeuring van bindende bedrijfsvoorschriften (lid 1) kan de Commissie modellen en procedures ontwikkelen.

Deze worden voorgelegd aan het artikel 93-comité. Het comité beslist vervolgens met meerderheid van stemmen over een positief of negatief advies. Indien het advies positief is, neemt de Commissie het model of de procedures aan. Ter ondersteuning wordt advies van het Comité ingewonnen (artikel 70 lid 1 punt c). Zie nader *Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)* van het Comité, 17 november 2022 (let wel: dit document is nog in concept, de publieke consultatie sloot 10 januari 2023).

Artikel 48. Niet bij Unierecht toegestane doorgiften of verstrekkingen

Elke rechterlijke uitspraak en elk besluit van een administratieve autoriteit van een derde land op grond waarvan een verwerkingsverantwoordelijke of een verwerker persoonsgegevens moet doorgeven of verstrekken, mag alleen op enigerlei wijze worden erkend of afdwingbaar zijn indien zij gebaseerd zijn op een internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtsbijstand, tussen het verzoekende derde landen en de Unie of een lidstaat, onverminderd andere gronden voor doorgifte uit hoofde van dit hoofdstuk.

Ten tijde van het opstellen van de AVG speelde in de VS een rechtszaak waarin het Amerikaanse concern Microsoft bij gerechtelijk bevel werd verplicht bij haar Europese dochter in Ierland persoonsgegevens te verstrekken van een gebruiker van haar Office 365-dienst. Dit artikel is daar een tegenreactie op. De strekking is dat een Europese entiteit niet mag meewerken aan dergelijke bevelen (hetzij van een rechtbank hetzij van een andere autoriteit).

Verdrag inzake rechtsbijstand. De aangewezen route voor derde landen zoals de VS om in dit soort situaties persoonsgegevens te verkrijgen, is een verdrag inzake rechtsbijstand met de betreffende EU-lidstaat. Nederland heeft bijvoorbeeld sinds 1981 een dergelijk verdrag met de VS.

Cloud Act/Situatie in VS. De hierboven genoemde rechtszaak is inmiddels ingehaald door de in 2018 aangenomen US CLOUD Act (“Clarifying Lawful Overseas Use of Data Act”). Deze wet bepaalt dat een Amerikaanse dienstverlener gehouden is om door de FBI gevorderde data af te geven, ongeacht in welk land ter wereld deze opgeslagen is. Dit botst natuurlijk met dit artikel van de AVG. Het lijkt relevant of de data beheerd wordt door een Europese dochter van de Amerikaanse dienstverlener of niet. Zo’n dochter is dan geen “US based company” en daarmee niet gehouden aan de US CLOUD Act te voldoen. Desalniettemin, is de CLOUD Act van toepassing op organisaties gevestigd in de VS, en data die zij in “possession, custody, or control” (in bezit, bewaring of onder hun controle) hebben. Het kan zo zijn dat een moedermaatschappij toegang of controle heeft over gegevens van hun dochterondernemingen. Om zeker te zijn dat de CLOUD Act niet van toepassing is, moet de Amerikaanse moedermaatschappij geen controle of anderszins gezag hebben over de persoonsgegevens gehouden

door de in de EU gevestigde dochtermaatschappij. Als de moedermaatschappij controle heeft over de persoonsgegevens, of als de dochteronderneming zelf gehouden zou zijn aan de CLOUD Act, ontstaat een onoplosbaar conflict met dit artikel van de AVG. De Europese dochter zou dan de persoonsgegevens in kwestie in het geheel niet kunnen verwerken.

Andere gronden. Wanneer dit hoofdstuk 5 van de AVG een andere grondslag biedt om de persoonsgegevens te verstrekken, blijft deze overeind ondanks dit artikel. Zo zou uitdrukkelijke toestemming van de betrokkene (artikel 49 lid 1 punt a) of doorgifte aan een adequaat derde land (artikel 45) tot de mogelijkheden behoren.

Artikel 49. Afwijkingen voor specifieke situaties

49.1 Bij ontstentenis van een adequaatheidsbesluit overeenkomstig artikel 45, lid 3, of van passende waarborgen overeenkomstig artikel 46, met inbegrip van bindende bedrijfsvoorschriften, kan een doorgifte of een reeks van doorgiften van persoonsgegevens aan een derde land of een internationale organisatie slechts plaatsvinden mits aan één van de volgende voorwaarden is voldaan:

Wanneer doorgifte buiten de EER niet mogelijk is omdat het land niet als adequaat is aangemerkt (artikel 45 lid 3) en ook geen passende waarborgen (artikel 46) of bindende bedrijfsvoorschriften (artikel 47) aanwezig zijn, mag doorgifte alleen als deze onder een van de opties uit dit lid 1 is toegestaan. Er zijn zeven genummerde opties (punten a t/m g) en een om onverklaarbare redenen niet genummerde achtste optie voor niet-repetitieve verwerkingen die noodzakelijk zijn voor dwingende gerechtvaardigde belangen (alineea 2). Zie ook de Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679 van het Comité.

Afdwingbare rechten. Bij een doorgifte op grond van dit lid 1 dient de verwerkingsverantwoordelijke of verwerker gebruik te maken van middelen die de betrokkenen ook na de doorgifte van hun gegevens afdwingbare en bruikbare rechten in de EU verlenen met betrekking tot de verwerking ervan opdat zij de grondrechten en waarborgen kunnen blijven genieten (overweging 114).

49.1(a) de betrokkene heeft uitdrukkelijk met de voorgestelde doorgifte ingestemd, na te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen;

De eerste grondslag voor doorgifte is de uitdrukkelijke toestemming voor doorgifte verleend door de betrokkene. Zie over uitdrukkelijke toestemming nader artikel 9 lid 2 punt a.

Inlichten over risico's. De betrokkene moet apart zijn geïnformeerd over de risico's die deze doorgifte met zich meebrengt. Dit betekent uitleg over wat een niet-adequaat land (artikel 45) is en wat passende waarborgen inhouden, plus natuurlijk waarom desondanks de doorgifte passend is. Deze inlichtingen moeten in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal (artikel 12 lid 1) worden verschaft.

Overheidsinstanties. Een overheidsinstantie mag zich bij uitoefening van haar openbare bevoegdheden niet beroepen op deze grondslag (zie lid 3).

49.1(b) de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen;

Wanneer de doorgifte noodzakelijk is voor een overeenkomst (inclusief precontractuele maatregelen), is de doorgifte ook toegestaan. Een voorbeeld is een verstrekking aan een Amerikaanse creditcardmaatschappij in het kader van een online aankoop. Het moet hier specifiek gaan om een overeenkomst tussen betrokkene en verwerkingsverantwoordelijke. Vergelijk punt c hieronder en zie meer algemeen artikel 6 lid 1 punt b.

Overheidsinstanties. Een overheidsinstantie mag zich bij uitoefening van haar openbare bevoegdheden niet beroepen op deze grondslag (zie lid 3).

49.1(c) de doorgifte is noodzakelijk voor de sluiting of de uitvoering van een in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke persoon of rechtspersoon gesloten overeenkomst;

Naast de overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke (punt b) is ook de overeenkomst in het belang van de betrokkene een grond voor doorgifte.

Overheidsinstanties. Een overheidsinstantie mag zich bij uitoefening van haar openbare bevoegdheden niet beroepen op deze grondslag (zie lid 3).

49.1(d) de doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang;

Een doorgifte die noodzakelijk is wegens gewichtige redenen van algemeen belang is ook toegestaan. Dergelijke belangen zijn bijvoorbeeld (overweging 112): internationale gegevensuitwisselingen tussen mededingingsautoriteiten, belasting- of douanediens, financiële toezichthoudende autoriteiten en diensten met bevoegdheid op het gebied van de sociale zekerheid of de volksgezondheid, bijvoorbeeld in geval van opsporing van contacten in het kader van de bestrijding van besmettelijke ziekten of met het oog op de terugdringing en/of uitbanning van doping in de sport. Ook doorgifte van persoonsgegevens onder de Ver-

dragen van Genève of het humanitair recht bij gewapende conflicten kunnen hieronder vallen. Zie ook artikel 6 lid 1 punt e over dit begrip.

Erkend bij wet. Het algemeen of openbaar belang in kwestie moet zijn erkend bij een Unierechtelijke of nationaalrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is (zie lid 4).

49.1(e) de doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering;

Wanneer een partij een rechtsvordering wil instellen (al dan niet tegen de betrokkene), dan kunnen daar persoonsgegevens bij nodig zijn. Denk aan het opvoeren van bewijs dat een persoon iets gezegd of gedaan heeft. Doorgifte van deze gegevens kan daarbij onvermijdelijk zijn, en moet in dat geval ook toegestaan zijn. Zie meer algemeen artikel 9 lid 2 punt f (grondslag voor bijzondere persoonsgegevens) en artikel 17 lid 3 punt e (geen recht van wissing) over verwerkingen die noodzakelijk zijn voor rechtsvorderingen. Onder een rechtsvordering wordt ook verstaan een administratiefrechtelijke of bestuursrechtelijke procedure, alsook arbitrage (overweging 111).

49.1(f) de doorgifte is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven;

Doorgifte is ook toegestaan wanneer dit nodig is ter bescherming van vitale belangen van de betrokkenen. Dergelijke belangen raken aan het leven, zoals bij medische gegevens in een spoedgeval. Ook doorgifte van persoonsgegevens onder de Verdragen van Genève of het humanitair recht bij gewapende conflicten kunnen hieronder vallen (overweging 112). Zie nader artikel 6 lid 1 punt d over dit begrip. Vereist is wel dat de betrokkene niet in staat is toestemming (punt a) te geven voor doorgifte.

49.1(g) de doorgifte is verricht vanuit een register dat volgens het Unierecht of lidstatelijk recht is bedoeld om het publiek voor te lichten en dat door eenieder dan wel door iedere persoon die zich op een gerechtvaardigd belang kan beroepen, kan worden geraadpleegd, maar alleen voor zover in het geval in kwestie wordt voldaan aan de in Unierecht of lidstatelijk recht vastgestelde voorwaarden voor raadpleging.

Een doorgifte is als laatste ook toegestaan wanneer deze gebeurt vanuit een bij wet ingesteld register dat bedoeld is om het publiek te informeren. Denk bijvoorbeeld aan een openbaar register van leden van gereguleerde beroepen (zoals advocaten of registeraccountants). Een register kan ook beperkt zijn tot personen die een gerechtvaardigd belang hebben om dit te raadplegen, zoals bij het kentekenregister van de Rijksdienst voor het Wegverkeer. Een dergelijke

doorgifte mag geen betrekking hebben op alle persoonsgegevens of volledige categorieën van persoonsgegevens die in het register zijn opgeslagen (zie lid 2).

Wanneer een doorgifte niet op een bepaling van de artikelen 45 of 46, met inbegrip van de bepalingen inzake bindende bedrijfsvoorschriften, kon worden gegrond en geen van de afwijkingen voor een specifieke situatie als bedoeld in de eerste alinea van dit lid van toepassing zijn, mag de doorgifte aan een derde land of aan een internationale organisatie alleen plaatsvinden indien de doorgifte niet repetitief is, een beperkt aantal betrokkenen betreft, noodzakelijk is voor dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke die niet ondergeschikt zijn aan de belangen of rechten en vrijheden van de betrokkene, en de verwerkingsverantwoordelijke alle omstandigheden in verband met de gegevensdoorgifte heeft beoordeeld en op basis van die beoordeling passende waarborgen voor de bescherming van persoonsgegevens heeft geboden. De verwerkingsverantwoordelijke informeert de toezichthouder over de doorgifte. De verwerkingsverantwoordelijke verstrekt de betrokkene naast de in de artikelen 13 en 14 bedoelde informatie, ook informatie met betrekking tot de doorgifte en de door hem nagestreefde dwingende gerechtvaardigde belangen.

Als laatste uitzondering wordt nog toegestaan wat wij maar noemen de incidentele doorgifte: de doorgifte is eenmalig (niet repetitief), betreft een klein aantal betrokkenen en is noodzakelijk voor dwingende belangen van de verwerkingsverantwoordelijke, waarbij die belangen zwaarder wegen dan de belangen van betrokkenen (vergelijk artikel 6 lid 1 punt f). Als dan ook passende waarborgen worden getroffen voor de betrokkenen, is de doorgifte toegestaan.

Informeren toezichthouder. Als de verwerkingsverantwoordelijke zich wil beroepen op deze grond, moet hij de toezichthouder informeren over de doorgifte. De toezichthouder kan dan besluiten corrigerend op te treden, bijvoorbeeld door te bevelen de doorgifte te staken (artikel 58 lid 2 punt d).

Informeren betrokkenen. Als de verwerkingsverantwoordelijke zich wil beroepen op deze grond, moet hij ook betrokkenen hierover informeren (artikel 13 lid 1 punt e en artikel 14 lid 1 punt f).

Belangenafweging. Doorgifte op deze grond vereist een belangenafweging. De verwerkingsverantwoordelijke besteedt (overweging 113) daarbij bijzondere aandacht aan de aard van de persoonsgegevens, het doel en de duur van de voorgestelde verwerking of verwerkingen, alsmede aan de situatie in het land van herkomst, het derde land en het land van de uiteindelijke bestemming en moet voorzien in passende waarborgen ter bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens. Waar het gaat om wetenschappelijk of historisch onderzoek of statistische doeleinden, dient rekening te worden gehouden met de gerechtvaardigde verwachting van de maatschappij dat er sprake is van kennisvermeerdering.

Restgevallen. Doorgifte op deze grond is alleen toegestaan wanneer de overige gronden voor doorgifte niet van toepassing zijn (overweging 113).

Overheidsinstanties. Een overheidsinstantie mag zich bij uitoefening van haar openbare bevoegdheden niet beroepen op deze grondslag (zie lid 3).

Register. De beoordeling en genomen passende waarborgen worden vastgelegd in het verwerkingsregister (zie lid 6).

49.2 Een doorgifte overeenkomstig lid 1, punt g), mag geen betrekking hebben op alle persoonsgegevens of volledige categorieën van persoonsgegevens die in het register zijn opgeslagen. Wanneer een register bedoeld is om door personen met een gerechtvaardigd belang te worden geraadpleegd, kan de doorgifte slechts plaatsvinden op verzoek van die personen of wanneer de gegevens voor hen zijn bestemd.

Een doorgifte vanuit een (semi-)openbaar register is toegestaan (lid 1 punt g), maar daarbij mag niet het gehele register ineens worden doorgegeven. Gaat het om een register dat semi-openbaar is, oftewel uitsluitend te raadplegen door personen met een gerechtvaardigd belang, dan moet de doorgifte gebeuren op verzoek van deze personen of voor hen bestemd zijn. Bij de vraag of de doorgifte gerechtvaardigd is, moet ten volle rekening worden gehouden met de belangen en de grondrechten van de betrokkene (overweging 111).

49.3 Lid 1, eerste alinea, punten a), b) en c) en lid 1, tweede alinea, zijn niet van toepassing op activiteiten die door overheidsinstanties worden verricht bij de uitoefening van hun openbare bevoegdheden.

Overheidsinstanties mogen bij verwerkingen binnen hun openbare bevoegdheden zich niet beroepen op uitdrukkelijke toestemming (lid 1 punt a), uitvoering overeenkomst (lid 1 punt b en c), en de incidentele doorgifte (lid 1 tweede alinea).

49.4 Het in lid 1, punt d), bedoelde openbaar belang moet zijn erkend bij een Unierechtelijke of nationaalrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is.

Op grond van lid 1 punt d) mag doorgifte worden gerechtvaardigd op grond van een algemeen oftewel openbaar belang. Dit belang moet vastgelegd zijn in Unierecht of nationaal recht.

49.5 Bij ontstentenis van een adequaatheidsbesluit kunnen in Unierechtelijke of lidstaatrechtelijke bepalingen of bepalingen om gewichtige redenen van openbaar belang uitdrukkelijk grenzen worden gesteld aan de doorgifte van specifieke categorieën van persoonsgegevens aan een derde land of een internationale organisatie. De lidstaten stellen de Commissie in kennis van dergelijke bepalingen.

Wanneer een land niet als adequaat is aangemerkt onder artikel 45, kan een lidstaat het wenselijk achten dat bepaalde doorgiften naar dat land niet zijn toegestaan, ook niet onder dit artikel 49 lid 1. Dit dient te worden gerechtvaardigd onder gewichtige redenen van openbaar belang, en worden vastgelegd in nationaal recht. Ook de Uniewetgever kan dergelijke grenzen trekken.

49.6 De verwerkingsverantwoordelijke of de verwerker staft de beoordeling en de in lid 1, tweede alinea, van dit artikel bedoelde passende waarborgen in het artikel 30 bedoelde register.

De beoordeling waarom sprake is van een incidentele verwerking (lid 1 tweede alinea) en de bijbehorende passende waarborgen moet worden opgenomen in het register van verwerkingen (artikel 30 lid 1 punt e).

Artikel 50. Internationale samenwerking voor de bescherming van persoonsgegevens

Ten aanzien van derde landen en internationale organisaties nemen de Commissie en de toezichthoudende autoriteiten de nodige maatregelen om:

- a) procedures voor internationale samenwerking te ontwikkelen, zodat de effectieve handhaving van de wetgeving inzake de bescherming van persoonsgegevens wordt vergemakkelijkt;
- b) internationale wederzijdse bijstand te bieden bij de handhaving van de wetgeving inzake de bescherming van persoonsgegevens, onder meer door kennisgeving, doorverwijzing van klachten, bijstand bij onderzoeken en uitwisseling van informatie, voor zover er passende waarborgen voor de bescherming van persoonsgegevens en andere grondrechten en fundamentele vrijheden bestaan;
- c) belanghebbenden te betrekken bij besprekingen en activiteiten om de internationale samenwerking bij de handhaving van de wetgeving inzake de bescherming van persoonsgegevens te bevorderen; en

- d) de uitwisseling en het documenteren van wetgeving en praktijken inzake de bescherming van persoonsgegevens te bevorderen, onder meer betreffende jurisdictiegeschillen met derde landen.

Grensoverschrijdend verkeer van persoonsgegevens brengt risico's met zich mee, zowel voor burgers als voor toezichthouders. Dit afsluitende artikel roept de Commissie en de toezichthouders dan ook op om samen te werken om adequate handhaving en bijstand in deze situaties te realiseren (zie over de samenwerking meer algemeen artikel 61).

Hoofdstuk VI

Onafhankelijke toezichthoudende autoriteiten

Hoofdstuk VI van de AVG bepaalt op welke wijze toezicht wordt uitgeoefend op verwerkingen door verwerkingsverantwoordelijken en verwerkers onder de AVG. Er is gekozen voor een systeem van samenwerkende nationale toezichthouders. Er is geen Europese toezichthouder naast of boven de nationale toezichthouders. Wel is er het Europees Comité voor gegevensbescherming (artikel 68, hierna: “het Comité”) met als taak ervoor te zorgen dat de AVG consequent wordt toegepast door de verschillende toezichthouders.

Afdeling 1 stelt regels over toezichthouders, met name gericht op hun onafhankelijk opereren. In afdeling 2 wordt uitgewerkt wanneer toezichthouders bevoegd zijn en welke taken en bevoegdheden zij hebben.

AFDELING 1. ONAFHANKELIJKHEID

In afdeling 1 worden de nationale toezichthouders ingesteld (artikel 51). Dit dient bij wet te gebeuren (artikel 54) en daarbij dient een aantal voorwaarden in acht te worden genomen (artikel 53). Toezichthouders opereren uiteraard in volgestrekte onafhankelijkheid (artikel 52).

Artikel 51. Toezichthoudende autoriteit

51.1 Elke lidstaat bepaalt dat één of meer onafhankelijke overheidsinstanties verantwoordelijk zijn voor het toezicht op de toepassing van deze verordening, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken.

Iedere lidstaat is verplicht een toezichthouder in te stellen, welke in onafhankelijkheid de naleving van de AVG en meer algemeen de bescherming van de grondrechten van de burger ten aanzien van persoonsgegevens moet controleren. Er is geen overkoepelende Europese toezichthouder (de in artikel 68 genoemde Europese Toezichthouder voor gegevensbescherming heeft, ondanks de naam, slechts een adviserende functie.)

Onafhankelijkheid. De toezichthouder moet bevoegd zijn haar taken en bevoegdheden volstrekt onafhankelijk uit te oefenen (zie nader artikel 52). In Nederland wordt dit gewaarborgd door de toezichthouder als een zelfstandig bestuursorgaan in te richten, zoals onder de Richtlijn met de Autoriteit Persoonsgegevens is gebeurd. De Autoriteit Persoonsgegevens is vanwege de intrekking van de Wbp formeel opnieuw opgericht (artikel 6 Uitvoeringswet).

Meerdere toezichthouders. Sommige landen, met name Duitsland, hebben de behoefte om meerdere toezichthouders in te stellen. De AVG biedt daartoe ruimte als dat in overeenstemming is met de constitutionele, organisatorische en bestuurlijke structuur van een land. Eén van hen dient dan te worden aangewezen (lid 3) als deelnemer aan het Comité (artikel 68).

Taken en bevoegdheden. De toezichthouders hebben brede taken (artikel 57) en bevoegdheden (artikel 58), waaronder de bevoegdheid tot het opleggen van boetes. Tegen besluiten van toezichthouders staat beroep bij de rechter open (artikel 78). Toezichthouders moeten samenwerken (lid 2 en nader artikel 63).

Europese Toezichthouder. De AVG kent geen overkoepelende Europese toezichthouder. In diverse artikelen wordt de Europese Toezichthouder voor gegevensbescherming genoemd. Deze *European Data Protection Supervisor* of EDPS is een onafhankelijke EU-toezichthoudende autoriteit ten aanzien van de verwerking van persoonsgegevens door de EU-instellingen en –organen, met daarnaast adviserende bevoegdheden over EU-beleid en wetgeving met privacy-aspecten en een samenwerkende taak om te zorgen voor een consistente gegevensbescherming. De EDPS is opgericht onder Verordening 45/2001 die verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie regelt. In tegenstelling tot wat de naam suggereert, is de EDPS géén toezichthouder in de zin van de AVG.

Nederland. In Nederland is en blijft de Autoriteit Persoonsgegevens (AP) de Nederlandse toezichthoudende autoriteit (artikel 6 Uitvoeringswet).

- | | |
|------|---|
| 51.2 | Elke toezichthoudende autoriteit draagt bij tot de consequente toepassing van deze verordening in de hele Unie. Daartoe werken de toezichthoudende autoriteiten onderling en met de Commissie samen overeenkomstig hoofdstuk VII. |
|------|---|

Bij meerdere toezichthouders is er de kans op uiteenlopende beslissingen ten aanzien van (on)rechtmatige verwerkingen, handhaving en dergelijke. Ter voorkoming daarvan bepaalt lid 2 dat de toezichthouders consequent moeten handelen en samen moeten werken met elkaar en met de Commissie om tot eenvormige toepassing te komen. Zie nader het coherentiebeginsel uit artikel 63.

- 51.3 Wanneer er in een lidstaat meer dan één toezichthoudende autoriteit is gevestigd, wijst die lidstaat de toezichthoudende autoriteit aan die die autoriteiten in het Comité moet vertegenwoordigen en stelt hij de procedure vast om ervoor te zorgen dat de andere autoriteiten de regels in verband met het in artikel 63 bedoelde coherentiemechanisme naleven.

Het is mogelijk dat een lidstaat meerdere toezichthouders heeft (zie lid 1). In dat geval moet één van hen worden aangewezen als deelnemer aan het Comité voor gegevensbescherming (artikel 68), dit om te voorkomen dat die lidstaat meerdere stemmen krijgt in de besluitvorming van het Comité.

Coherentieprocedure. Het coherentiemechanisme dient ter borging dat de AVG in de gehele EU consequent wordt toegepast (artikel 63). Doel is te zorgen dat toezichthouders geen uiteenlopende beslissingen nemen, met name wanneer een toezichthoudende autoriteit voornemens is betreffende verwerkingsactiviteiten met wezenlijke gevolgen voor een betekenisvol aantal betrokkenen in verscheidene lidstaten een maatregel vast te stellen waarmee rechtsgevolgen worden beoogd (overweging 135).

- 51.4 Elke lidstaat stelt de Commissie uiterlijk op 25 mei 2018 [twee jaar vanaf de datum van inwerkingtreding van deze verordening] in kennis van de wettelijke bepalingen die hij overeenkomstig dit hoofdstuk vaststelt, alsmede, onverwijld, van alle latere wijzigingen daarvan.

Uiterlijk op 25 mei 2018 moest iedere lidstaat bij wet (artikel 54) hebben geregeld dat een toezichthouder wordt opgericht (lid 1), dat diens onafhankelijkheid wordt geborgd (artikel 52), hoe leden worden benoemd (artikel 53) en overige procedurele aspecten (artikel 54). De lidstaat moet dit aan de Commissie melden.

Artikel 52. Onafhankelijkheid van de toezichthouder

- 52.1 Elke toezichthoudende autoriteit treedt volledig onafhankelijk op bij de uitvoering van de taken en de uitoefening van de bevoegdheden die haar overeenkomstig deze verordening zijn toegewezen.

De toezichthouder moet bevoegd zijn haar taken en bevoegdheden volstrekt onafhankelijk uit te oefenen. In Nederland wordt dit gewaarborgd door de toezichthouder als een zelfstandig bestuursorgaan in te richten. Deze onafhankelijkheid houdt echter niet in dat de toezichthouder niet zou mogen worden gecontroleerd op financieel beleid (zie lid 6) of dat er geen rechterlijke toetsing zou mogen plaatsvinden op hun activiteiten (zie artikel 78). Zie over onafhankelijkheid nader HvJ EU, ECLI:EU:C:2010:125, 9 maart 2010 (Commissie v. Duitsland) en HvJ EU, ECLI:EU:C:2012:631, 10 oktober 2012 (Commissie v.

Oostenrijk). De AP valt als toezichthouder in de zin van artikel 5:11 Awb gewoon onder de regels omtrent toezicht in de Algemene wet bestuursrecht.

- 52.2 Bij de uitvoering van hun taken en de uitoefening van hun bevoegdheden overeenkomstig deze verordening blijven de leden van elke toezichthoudende autoriteit vrij van al dan niet rechtstreekse externe invloed en vragen noch aanvaarden zij instructies van wie dan ook.

Teneinde de onafhankelijkheid te garanderen mogen leden van een toezichthouder niet worden onderworpen aan externe invloed of instructies. Gekozen is voor aansluiting bij de Wet rechtspositie rechterlijke ambtenaren om de onafhankelijkheid van de leden van de Autoriteit Persoonsgegevens te borgen (artikel 8 Uitvoeringswet).

- 52.3 De leden van toezichthoudende autoriteiten verrichten geen handelingen die onverenigbaar zijn met hun taken en verrichten gedurende hun ambtstermijn geen al dan niet bezoldigde beroepswerkzaamheden die onverenigbaar zijn met hun taken.

Vanuit het bewaren van onafhankelijkheid mogen leden van een toezichthouder niets doen dat onverenigbaar is met hun werk bij de toezichthouder. Vergelijk artikel 13 van de Kaderwet zelfstandige bestuursorganen over nevenfuncties.

- 52.4 Elke lidstaat zorgt ervoor dat elke toezichthoudende autoriteit beschikt over de personele, technische en financiële middelen, en de bedrijfsruimten en infrastructuur die nodig zijn voor het effectief uitvoeren van haar taken en uitoefenen van haar bevoegdheden, waaronder die in het kader van wederzijdse bijstand, samenwerking en deelname aan het Comité.

De lidstaten moeten zorgen dat de toezichthouders in staat zijn om hun taken uit te oefenen. Daartoe dienen deze te beschikken over de financiële en personele middelen en de bedrijfsruimten en infrastructuur die noodzakelijk zijn voor hun taken. In het bijzonder moet de toezichthouder in staat zijn de taken in het kader van wederzijdse bijstand en samenwerking met andere toezichthoudende autoriteiten uit te kunnen voeren.

- 52.5 Elke lidstaat zorgt ervoor dat elke toezichthoudende autoriteit eigen en zelfgekozen personeelsleden heeft, die onder de exclusieve leiding van het lid of de leden van de betrokken toezichthoudende autoriteit staan.

De toezichthouder selecteert en benoemt zijn eigen personeel, zonder externe invloed of instructies (zie lid 2). In Nederland worden de voorzitter, leden en buitengewone leden van de AP, op voordracht van de minister, benoemd (middels een Koninklijk Besluit) voor een periode van vijf jaar. Herbenoeming kan voor een periode van nogmaals vijf jaar (artikel 7 Uitvoeringswet). Op het personeel zijn de rechtspositieregels die gelden voor de ambtenaren die zijn

aangesteld bij ministeries, van overeenkomstige toepassing (artikel 15 van de Kaderwet zelfstandige bestuursorganen). Artikel 16 van de Kaderwet zelfstandige bestuursorganen bepaalt dat personeel van een zelfstandig bestuursorgaan uitsluitend aan dat orgaan verantwoording aflegt. Daarnaast is er een Raad van advies die de AP adviseert over de algemene aspecten van de bescherming van persoonsgegevens. De leden van deze Raad worden, op voordracht van de AP, benoemd door de minister (artikel 7 lid 6 Uitvoeringswet).

- 52.6 Elke lidstaat zorgt ervoor dat op elke toezichthoudende autoriteit financieel toezicht wordt uitgeoefend zonder dat daarbij de onafhankelijkheid van de toezichthoudende autoriteit in het gedrang komt en dat het een afzonderlijke, publieke jaarbegroting heeft, die een onderdeel kan zijn van de algehele staats- of nationale begroting.

De AVG vereist dat lidstaten financieel toezicht houden op toezichthouders. Uiteraard mag dit hun onafhankelijkheid niet aantasten (lid 1). In Nederland is financieel toezicht op zelfstandige bestuursorganen geregeld in hoofdstuk 4 van de Kaderwet zelfstandige bestuursorganen. De jaarbegroting is apart en openbaar (artikel 29 Kaderwet zelfstandige bestuursorganen).

Artikel 53. Algemene voorwaarden voor de leden van de toezichthoudende autoriteit

- 53.1 De lidstaten schrijven voor dat elk lid van hun toezichthoudende autoriteiten volgens een transparante procedure wordt benoemd door:
- hun parlement;
 - hun regering;
 - hun staatshoofd; of
 - een onafhankelijk orgaan dat krachtens het lidstatelijke recht met de benoeming is belast.

Teneinde de onafhankelijkheid van de toezichthouder te waarborgen, worden leden volgens een transparante procedure benoemd. In Nederland behelst het College van de Autoriteit Persoonsgegevens standaard drie leden (artikel 7 lid 1 Uitvoeringswet), welke worden benoemd middels een Koninklijk Besluit (artikel 7 lid 3 Uitvoeringswet).

- 53.2 Elk lid beschikt over de nodige kwalificaties, ervaring en vaardigheden, met name op het gebied van de bescherming van persoonsgegevens, voor het uitvoeren van zijn taken en het uitoefenen van zijn bevoegdheden.

Uiteraard dienen de leden van de toezichthouder te beschikken over de relevante kwalificaties, ervaring en vaardigheden.

53.3 De taken van een lid eindigen bij het verstrijken van de ambtstermijn, bij ontslag of bij verplichte pensionering overeenkomstig de wetgeving van de lidstaat in kwestie.

Na verstrijken van de ambtstermijn of pensionering van het lid eindigen diens taken. De geheimhoudingsplicht blijft van kracht (artikel 54 lid 2).

53.4 Een lid wordt slechts ontslagen indien het op ernstige wijze is tekortgeschoten of niet langer aan de vereisten voor de uitvoering van de taken voldoet.

Teneinde de onafhankelijkheid van de toezichthouder te borgen, kan ontslag van leden enkel plaatsvinden indien zij de minister hiertoe verzoeken (artikel 7 lid 7 Uitvoeringswet).

Artikel 54. Regels inzake de oprichting van de toezichthoudende autoriteit

54.1 Elke lidstaat regelt al het volgende bij wet:

54.1(a) de oprichting van elke toezichthoudende autoriteit;

54.1(b) de vereiste kwalificaties en voorwaarden om als lid te worden benoemd voor elke toezichthoudende autoriteit;

54.1(c) de regels en procedures voor de benoeming van het lid of de leden van elke toezichthoudende autoriteit;

54.1(d) de ambtstermijn van het lid of de leden van elke toezichthoudende autoriteit, die ten minste vier jaar bedraagt, behoudens de eerste ambtstermijn na 24 mei 2016 [de datum van inwerkingtreding van deze verordening], die korter kan zijn wanneer dat nodig is om de onafhankelijkheid van de toezichthoudende autoriteit door middel van een in de tijd gespreide benoemingsprocedure te beschermen;

54.1(e) of het lid of de leden van elke toezichthoudende autoriteit opnieuw kan of kunnen worden benoemd en zo ja, hoe vaak;

54.1(f) de voorwaarden in verband met de plichten van het lid of de leden en de personeelsleden van elke toezichthoudende autoriteit, de verboden op met die plichten onverenigbare handelingen, werkzaamheden en voordelen tijdens en na de ambtstermijn en de regels betreffende de beëindiging van de ambtstermijn onderscheidenlijk de arbeidsverhouding.

De oprichting, inrichting en werkwijze van een toezichthouder dienen bij wet in formele zin geregeld te worden. Dit waarborgt de onafhankelijkheid van de

toezichthouder. De hier genoemde zaken zijn in Nederland geregeld in de Kaderwet zelfstandige bestuursorganen en worden in de Uitvoeringswet nader benoemd en uitgewerkt.

- 54.2 Ten aanzien van de vertrouwelijke informatie die hun bij de uitvoering van hun taken of de uitoefening van hun bevoegdheden ter kennis is gekomen, geldt voor het lid of de leden en de personeelsleden van elke toezichthoudende autoriteit zowel tijdens hun ambtstermijn als daarna het beroepsgeheim, zulks overeenkomstig Unierecht of lidstatelijk recht. Tijdens hun ambtstermijn geldt het beroepsgeheim met name voor meldingen van inbreuken op deze verordening door natuurlijke personen.

De leden en het personeel van de toezichthouder dienen aan geheimhouding gebonden te zijn inzake hetgeen hen ter kennis komt bij hun werk, maar ook daarna. In Nederland volgt dit beroepsgeheim uit artikel 125a lid 3 Ambtenarenwet, die van overeenkomstige toepassing is op personeel van een zelfstandig bestuursorgaan (artikel 15 lid 1 Kaderwet zelfstandige bestuursorganen).

AFDELING 2. COMPETENTIE, TAKEN EN BEVOEGDHEDEN

Afdeling 2 bepaalt wanneer toezichthouders competent ofwel bevoegd zijn (artikel 55), onder meer in het geval van grensoverschrijdende verwerkingen waarbij meerdere toezichthouders betrokken zijn (artikel 56). Ook taken (artikel 57) en bevoegdheden (artikel 58) worden hier geregeld.

Artikel 55. Competentie van toezichthouders

- 55.1 Elke toezichthoudende autoriteit heeft de competentie op het grondgebied van haar lidstaat de taken uit te voeren die haar overeenkomstig deze verordening zijn opgedragen en de bevoegdheden uit te oefenen die haar overeenkomstig deze verordening zijn toegekend.

Elke toezichthouder dient op het grondgebied van haar lidstaat competent ofwel bevoegd te zijn onder de AVG om op te treden tegen vermoedelijke inbreuken daarop. In Nederland is de AP competent gesteld om de taken en bevoegdheden van de toezichthouders op basis van de AVG uit te oefenen (artikel 14 Uitvoeringswet).

Gronden. Een toezichthouder is competent bij verwerkingen door een vestiging (van een verwerkingsverantwoordelijke of een verwerker) op het grondgebied van de betreffende lidstaat en bij verwerkingen door overheidsinstanties of particuliere organen die optreden in het algemeen belang in die lidstaat. Ook bij verwerkingen elders (zowel binnen als buiten de EU) met gevolgen voor betrok-

kenen op dat grondgebied is de toezichthouder van dat grondgebied competent. Bij verwerkingen vanuit meerdere lidstaten zie de samenwerkingsprocedure van artikel 60.

Competent bij klacht. Als laatste wordt een toezichthouder competent zodra een betrokkene een klacht indient over een verwerking, ongeacht of de toezichthouder volgens een van de andere gronden competent zou zijn voor die verwerking. Als dat niet zo is, dan moet de toezichthouder een wél competente toezichthouder informeren; hij blijft dan wel betrokken (zie de samenwerkingsprocedure van artikel 60).

55.2 In het geval van verwerking door overheidsinstanties of door particuliere organen die handelen op grond van artikel 6, lid 1, punt c) of punt e), is de toezichthoudende autoriteit van de lidstaat in kwestie competent. In dergelijke gevallen is artikel 56 niet van toepassing.

Wanneer sprake is van grensoverschrijdende verwerking (verwerking in meerdere landen of met wezenlijke gevolgen voor betrokkenen in meerdere landen, artikel 4 definitie 23), geldt als hoofdregel dat de toezichthouder van het land van de hoofdvestiging de leiding neemt (artikel 56). Deze hoofdregel geldt niet bij verwerking door overheidsinstanties (artikel 6 lid 1 punt c) of door particuliere organen die handelen in het algemeen belang (artikel 6 lid 1 punt e). In die situatie is alleen de toezichthoudende autoriteit van de lidstaat in kwestie bevoegd.

55.3 Toezichthoudende autoriteiten zijn niet competent toe te zien op verwerkingen door gerechten bij de uitoefening van hun rechterlijke taken.

De AVG is van toepassing op verwerkingen door gerechtelijke instanties, echter zijn de nationale toezichthouders niet bevoegd om op te treden tegen verwerkingen door rechtbanken. Dit in verband met de onafhankelijkheid van de rechterlijke macht (die immers ook besluiten van toezichthouders kan vernietigen).

Het toezicht op die gegevensverwerkingen moet kunnen worden toevertrouwd aan specifieke instanties binnen de rechterlijke organisatie van de lidstaat, zo merkt overweging 20 nog op. Deze zelf in te richten privacytoezichthouders moeten met name de naleving van de regels van deze verordening garanderen, leden van de rechterlijke macht van hun verplichtingen krachtens deze verordening sterker bewust maken, en klachten met betrekking tot die gegevensverwerkingen behandelen.

Uit de jurisprudentie volgt dat deze uitzondering ook reikt tot situaties waarbij door journalisten inzage wordt verzocht in stukken relevant voor een lopende procedure bij de bestuursrechter. Het Hof oordeelt dat ook toezicht van de AP over of dit al dan niet rechtmatig zou zijn, van invloed kan zijn op de onafhankelijkheid van een gerecht (Hv) EU 24 maart 2022, ECLI:EU:C:2022:216).

Artikel 56. Competentie van de leidende toezichthoudende autoriteit

56.1 Onverminderd artikel 55 is de toezichthoudende autoriteit van de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke of verwerker competent op te treden als leidende toezichthoudende autoriteit voor de grensoverschrijdende verwerking door die verwerkingsverantwoordelijke of verwerker overeenkomstig de procedure van artikel 60.

Wanneer een verwerking zich niet beperkt tot één lidstaat, kan een situatie ontstaan dat volgens de hoofdregel (artikel 55) meerdere toezichthouders bevoegd zijn. Omdat deze situatie tot complexiteit of uiteenlopende beslissingen kan leiden, introduceert de AVG een éénloketprocedure (artikel 60) waarbij één toezichthouder de leiding neemt en over de gehele verwerking kan oordelen. De leidende toezichthouder is de toezichthouder die bevoegd is voor het land van de hoofdvestiging van de verwerkingsverantwoordelijke.

Grensoverschrijdende verwerking. Van een grensoverschrijdende verwerking is sprake (artikel 4 definitie 23) als zij plaatsvindt hetzij in vestigingen in meerdere landen, hetzij betrokkenen uit meerdere landen waarschijnlijk wezenlijke gevolgen ondervinden van de verwerking. Enkel het feit dat persoonsgegevens kunnen worden opgevraagd via internet in een andere lidstaat maakt een verwerking nog niet grensoverschrijdend (zie het Lindqvist-arrest, HvJ EU, ECLI:EU:C:2003:596, 6 november 2003).

Vestiging. Een vestiging is iedere duurzame, reële en daadwerkelijke activiteit in een lidstaat, zelfs indien slechts gering (HvJ EU 1 oktober, ECLI:EU:C:2015:639, 2015, Weltimmo). Ook een handelsagent kan als ‘vestiging’ kwalificeren wanneer hij belast is met het innen van gelden in verband met een internetdienst en de verwerkingsverantwoordelijke vertegenwoordigt bij geschillen (idem). De enkele aanwezigheid van een vertegenwoordiger is daarentegen niet voldoende om te kunnen spreken van een vestiging, aldus de richtlijnen van artikel 29 Werkgroep. Zie nader Richtsnoeren 3/2018 over het territoriale toepassingsgebied van de AVG (artikel 3) van het Comité, 12 november 2019.

Wezenlijke gevolgen betrokkenen. Indien het waarschijnlijk is dat betrokkenen uit meerdere landen wezenlijke gevolgen ondervinden van een gegevensverwerking, is er sprake van een grensoverschrijdende verwerking. In de *Guidelines WP 244 for identifying a controller or processor's lead supervisory authority* (alleen beschikbaar in het Engels) van het Comité, 13 december 2016 worden verschillende factoren genoemd welke in acht dienen te worden genomen om te beoordelen of er sprake is van ‘waarschijnlijk wezenlijke gevolgen’. In het algemeen dienen de context van de verwerking, het soort persoonsgegevens en de doeleinden van de verwerking in acht te worden genomen. Het te verwachten negatieve effect voor betrokkenen speelt daarbij een belangrijke rol.

Hoofdvestiging. Wanneer sprake is van een grensoverschrijdende verwerking, is de toezichthouder voor de hoofdvestiging (of enige vestiging) van de verwerkingsverantwoordelijke of verwerker bevoegd. De hoofdvestiging is (artikel 4 definitie 16) de plaats waar de centrale administratie is gelegen dan wel de vestiging waar de beslissingen over de doelstellingen van en de midelen voor de verwerking van persoonsgegevens worden genomen (HvJ EU, ECLI:EU:C:2015:639, 1 oktober 2015). De verwerkingsverantwoordelijke of verwerker dient zelfstandig te identificeren welke vestiging is aan te merken als hoofdvestiging. Het besluit hiertoe kan echter, achteraf, door de desbetreffende toezichthouder worden betwist.

Verwerking buiten EU. Wanneer een verwerkingsverantwoordelijke of verwerker in een land buiten de EU is betrokken, is sprake van doorgifte (artikel 44) en is de toezichthouder bevoegd voor de lidstaat waar de vertegenwoordiger (artikel 27) gevestigd is.

Niet bij overheid. Bij verwerkingen door overheidsinstanties of particuliere organen in het algemeen belang is alleen de toezichthouder uit die lidstaat bevoegd (artikel 55 lid 2).

Verwerkingsverantwoordelijke en verwerker andere toezichthouder. In beginsel is het, ten aanzien van de leidende toezichthouder, niet relevant of een organisatie functioneert als verwerkingsverantwoordelijke of als verwerker. Dit is echter anders, indien een verwerkingsverantwoordelijke en een verwerker onder de autoriteit van een andere toezichthouder vallen. Wanneer dat het geval is, valt de verwerker (ten aanzien van die specifieke gegevensverwerking) eveneens onder de autoriteit van de toezichthouder van de verwerkingsverantwoordelijke (overweging 36). De toezichthouder van de verwerker dient vervolgens wel deel te nemen aan de samenwerkingsprocedure (artikel 60).

- 56.2 In afwijking van lid 1 is elke toezichthoudende autoriteit competent een bij haar ingediende klacht of een eventuele inbreuk op deze verordening te behandelen indien het onderwerp van die zaak alleen verband houdt met een vestiging in haar lidstaat of alleen voor betrokkenen in haar lidstaat wezenlijke gevolgen heeft.

Wanneer een klacht of inbreuk alleen relevant is voor een specifieke lidstaat, is er geen noodzaak de procedure van lid 1 in werking te stellen. Iedere toezichthouder kan deze specifiek nationale situatie dan in beginsel gewoon oplossen. Wel moet (lid 3) een toezichthouder in deze situatie de leidende toezichthouder informeren zodat deze kan besluiten of hij alsnog de procedure in werking wil stellen.

56.3 In de in lid 2 van dit artikel bedoelde gevallen stelt de toezichthoudende autoriteit de leidende toezichthoudende autoriteit onverwijld in kennis van de zaak. Binnen drie weken nadat zij in kennis is gesteld, besluit de leidende toezichthoudende autoriteit of zij de zaak al dan niet zal behandelen, overeenkomstig de in artikel 60 vastgelegde procedure; zij houdt daarbij rekening met het al dan niet bestaan van een vestiging van de verwerkingsverantwoordelijke of de verwerker in de lidstaat van de toezichthoudende autoriteit die haar in kennis heeft gesteld.

Als een toezichthouder meent dat een klacht of inbreuk alleen relevant is voor een specifieke lidstaat, kan deze de klacht of inbreuk zelf onderzoeken en aanpakken (zie lid 5). De leidende toezichthouder heeft echter voorafgaand het recht te beslissen dat de zaak toch breder relevant is.

In kennis stellen. De toezichthouder die meent dat een klacht of inbreuk alleen voor hem relevant is, moet de leidende toezichthouder (zoals bepaald in lid 1) onverwijld van de zaak in kennis stellen. Deze moet dan binnen drie weken besluiten of zij de zaak zal behandelen zoals volgt uit lid 1 of dat ze de zaak laat aan de lokale toezichthouder.

Bestaan van vestiging. Bij het besluit moet de leidende toezichthouder in ieder geval mee laten wegen of er een vestiging is van de verwerkingsverantwoordelijke of de verwerker in de lidstaat waar de lokale toezichthouder bevoegd is, om zo te garanderen dat de beslissing van die toezichthouder feitelijk kan worden geëffectueerd.

56.4 Wanneer de leidende toezichthoudende autoriteit besluit de zaak te behandelen, is de procedure van artikel 60 van toepassing. De toezichthoudende autoriteit die de leidende toezichthoudende autoriteit in kennis heeft gesteld, kan bij deze laatste een ontwerpbesluit indienen. De leidende toezichthoudende autoriteit houdt zo veel mogelijk rekening met dat ontwerp wanneer zij het in artikel 60, lid 3, bedoelde ontwerpbesluit opstelt.

Samenwerking. Conform artikel 60 werkt de leidende toezichthouder samen met de andere betrokken toezichthouders teneinde tot een consensus te komen. De betrokken toezichthouders wisselen alle relevante informatie met elkaar uit.

Ontwerp van besluit. Wanneer de leidende toezichthouder besluit de zaak te behandelen, dient de toezichthouder die haar in kennis heeft gesteld, de mogelijkheid te hebben een ontwerpbesluit in te dienen. De leidende toezichthouder moet daarmee maximaal rekening houden bij het opstellen van het finale besluit (zie ook artikel 60 lid 3 dat “naar behoren” rekening houden vereist). Hiermee zou het zwaarder belang van deze lokale toezichthouder moeten worden gediend.

- 56.5 Indien de leidende toezichthoudende autoriteit besluit de zaak niet te behandelen, wordt deze overeenkomstig de artikelen 61 en 62 behandeld door de toezichthoudende autoriteit die de leidende toezichthoudende autoriteit in kennis heeft gesteld.

Wanneer de leidende toezichthouder besluit de zaak niet te behandelen, komt deze terug bij de toezichthouder die deze als eerste op zijn bordje kreeg. Deze kan de zaak nu naar eigen inzicht afhandelen, zij het dat hij wederzijdse bijstand (artikel 61) kan verlangen van met name de leidende toezichthouder en gezamenlijk op kan treden (artikel 62).

- 56.6 De leidende toezichthoudende autoriteit is voor de verwerkingsverantwoordelijke of de verwerker de enige gesprekspartner bij grensoverschrijdende verwerking door die verwerkingsverantwoordelijke of verwerker.

Om te voorkomen dat verschillende toezichthouders uiteenlopende toezeggingen of mededelingen doen, bepaalt lid 6 dat alleen de leidende toezichthouder gesprekspartner mag zijn van de verwerkingsverantwoordelijke of verwerker.

Artikel 57. Taken

- 57.1 Onverminderd andere uit hoofde van deze verordening vastgestelde taken, verricht elke toezichthoudende autoriteit op haar grondgebied de volgende taken:

De toezichthouder heeft een aantal algemene taken (punten a tot en met v hieronder), en daarnaast een aantal bevoegdheden (artikel 58).

- 57.1(a) zij monitort en handhaaft de toepassing van deze verordening;

De eerste taak van elke toezichthouder is in het algemeen nagaan hoe de AVG wordt nageleefd en natuurlijk het optreden (zie ook artikel 58) tegen schendingen.

- 57.1(b) zij bevordert bij het brede publiek de bekendheid met en het inzicht in de risico's, regels, waarborgen en rechten in verband met de verwerking. Bijzondere aandacht wordt besteed aan specifiek op kinderen gerichte activiteiten;

De tweede taak van de toezichthouder is het informeren van het publiek over omgang met persoonsgegevens, met name over risico's en rechten. Gezien steeds vaker persoonsgegevens van kinderen worden gebruikt, krijgt dit bijzondere aandacht.

57.1(c) zij verleent overeenkomstig het recht van de lidstaat, advies aan het nationale parlement, de regering, en andere instellingen en organen over wetgevings-initiatieven en bestuursmaatregelen in verband met de bescherming van de rechten en vrijheden van natuurlijke personen op het gebied van verwerking;

Een derde taak van toezichthouders is de wetgever en overheidsinstanties te adviseren over nieuwe wetgeving en bestuursmaatregelen en –regelingen. Het is aan de lidstaten om te bepalen of en wanneer dergelijk advies ingewonnen moet worden en wat de wetgever vervolgens hiermee doet. Zie ook artikel 36 lid 4, dat bepaalt dat lidstaten de toezichthouder moeten raadplegen bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel, of een daarop gebaseerde regelgevingsmaatregel in verband met verwerking van persoonsgegevens.

57.1(d) zij maakt de verwerkingsverantwoordelijken en de verwerkers beter bekend met hun verplichtingen uit hoofde van deze verordening;

Een toezichthouder zal verder verwerkingsverantwoordelijken en verwerkers informeren over hun verplichtingen onder de AVG. Dit zal in de praktijk veelal gebeuren door het opstellen van richtsnoeren, aanwijzingen en *best practices*.

57.1(e) zij verstrekt desgevraagd informatie aan iedere betrokkene over de uitoefening van zijn rechten uit hoofde van deze verordening en werkt daartoe in voorkomend geval samen met de toezichthoudende autoriteiten in andere lidstaten;

Betrokkenen kunnen toezichthouders om advies vragen, waar deze kosteloos op in moet gaan (lid 3). Toezichthouders kunnen ook bemiddelen als de betrokkene bij een andere toezichthouder in een andere lidstaat zou moeten zijn.

57.1(f) zij behandelt klachten van betrokkenen, of van organen, organisaties of verenigingen overeenkomstig artikel 80, onderzoekt de inhoud van de klacht in de mate waarin dat gepast is en stelt de klager binnen een redelijke termijn in kennis van de vooruitgang en het resultaat van het onderzoek, met name indien verder onderzoek of coördinatie met een andere toezichthoudende autoriteit noodzakelijk is;

Betrokkenen kunnen klachten indienen bij de toezichthouder (artikel 77). Ook verenigingen en andere organisaties van betrokkenen kunnen dit (artikel 80). De toezichthouder moet deze klachten dan onderzoeken en de klager op de hoogte houden van de voortgang. Zie nader artikel 77 lid 2.

57.1(g) zij werkt samen met andere toezichthoudende autoriteiten, onder meer door informatie te delen en wederzijdse bijstand te bieden, teneinde de samenhang in de toepassing en de handhaving van deze verordening te waarborgen;

Toezichthouders werken met elkaar samen bij grensoverschrijdende handhaving (artikel 60, 61 en 62), en streven daarbij naar een coherente toepassing van de AVG (artikel 63).

57.1(h) zij verricht onderzoeken naar de toepassing van deze verordening, onder meer op basis van informatie die zij van een andere toezichthoudende autoriteit of een andere overheidsinstantie ontvangt;

In het kader van handhaving (zie ook punt a) dient een toezichthouder onderzoek te doen naar mogelijke overtredingen of andere relevante ontwikkelingen (zie ook punt i). Dit kan gebeuren op basis van tips van andere overheidsinstanties.

57.1(i) zij volgt de relevante ontwikkelingen voor zover deze invloed hebben op de bescherming van persoonsgegevens, met name de ontwikkelingen in informatie- en communicatietechnologieën en handelspraktijken;

De toezichthouder moet natuurlijk op de hoogte blijven van ontwikkelingen in de markt, met name waar het gaat om informatie- en communicatietechnologie (ICT) en handelspraktijken die gebruik van persoonsgegevens vergen zoals online reclame.

57.1(j) zij stelt de in artikel 28, lid 8, en artikel 46, lid 2, punt d), bedoelde standaardcontractbepalingen vast;

De toezichthouder kan standaardbepalingen vaststellen voor verwerkersovereenkomsten (artikel 28 lid 8), en ook voor standaardbepalingen inzake gegevensbescherming bij doorgiften naar derde landen (artikel 46 lid 2 punt d). Zie nader artikel 58 lid 3 punt g.

57.1(k) zij stelt een lijst op met betrekking tot het vereiste inzake een gegevensbeschermings-effectbeoordeling overeenkomstig artikel 35, lid 4, en houdt deze lijst bij;

Bij verwerkingen met een hoog risico is een DPIA verplicht (artikel 35 lid 1). Toezichthouders kunnen een zwarte lijst opstellen met verwerkingen waarvoor een DPIA verplicht is (artikel 35 lid 4).

57.1(l) zij verstrekt advies over de in artikel 36, lid 2, bedoelde verwerkingsactiviteiten;

Een verwerking met hoog risico kan inbreuk maken op de AVG, met name wanneer de risico's onvoldoende onderkend of geborgd zijn (artikel 36 lid 2). De toezichthouder moet dan adviseren over hoe hiermee om te gaan.

57.1(m) zij bevordert de opstelling van gedragscodes uit hoofde van artikel 40, geeft advies en keurt, overeenkomstig artikel 40, lid 5, gedragscodes goed die voldoende waarborgen leveren;

Brancheorganisaties en dergelijke kunnen een gedragscode (artikel 40) invoeren over hoe de AVG in hun branche moeten worden toegepast. Dit vereist het advies van de toezichthouder (artikel 40 lid 5). Zie ook artikel 58 lid 3 punt d. Meer algemeen moet de toezichthouder stimuleren dat gedragscodes worden ingevoerd.

57.1(n) zij bevordert de invoering van certificeringsmechanismen voor gegevensbescherming en van gegevensbeschermingszegels en -merktekens overeenkomstig artikel 42, lid 1, en keurt de criteria voor certificering uit hoofde van artikel 42, lid 5, goed;

De toezichthouder kan verwerkingen en mechanismen daarvoor certificeren, en ook criteria voor certificering goedkeuren (artikel 42 lid 5). Zie ook artikel 58 lid 3 punt f. Meer algemeen moet de toezichthouder stimuleren dat certificering wordt gehanteerd.

57.1(o) waar van toepassing verricht zij een periodieke toetsing van de overeenkomstig artikel 42, lid 7, afgegeven certificeringen;

Certificaten voor gegevensverwerking of mechanismen daarvoor worden afgegeven voor maximaal drie jaar (artikel 42 lid 7) en worden in ieder geval bij verlenging getoetst of nog voldaan is aan de eisen voor certificering.

57.1(p) zij zorgt voor het opstellen en het bekendmaken van de eisen inzake de accreditatie van een orgaan voor het toezicht op gedragscodes op grond van artikel 41 en van een certificeringsorgaan op grond van artikel 43;

Brancheorganisaties kunnen gedragscodes opstellen over de invulling van de AVG binnen hun branche (artikel 41). Onderdeel van zo'n gedragscode is het hebben van een onafhankelijk toezichthoudend orgaan (artikel 41 lid 4). Daarnaast kunnen verwerkingen en mechanismen daarvoor worden gecertificeerd (artikel 42). Dit kan door de toezichthouder gebeuren maar ook door een geaccrediteerd certificeringsorgaan (artikel 43). Accreditering van beide organen gebeurt door de toezichthouder. Deze dient dan ook de criteria voor accreditatie te publiceren.

57.1(q) zij zorgt voor de accreditatie van een orgaan voor het toezicht op gedragscodes op grond van artikel 41 en van een certificeringsorgaan op grond van artikel 43;

Zoals bij punt p is opgemerkt, moeten organen voor toezicht op een gedragscode en voor certificering van verwerkingen of mechanismen daarvoor worden geaccrediteerd. Deze accreditatie gebeurt door de toezichthouder.

57.1(r) zij geeft toestemming voor de in artikel 46, lid 3, bedoelde contractuele en andere bepalingen;

De toezichthouder kan toestemming geven voor het hanteren van zelfgemaakte contractbepalingen voor waarborging van doorgifte naar derde landen (artikel 46 lid 3 punt a). Zie ook artikel 58 lid 3 punt h.

57.1(s) zij keurt overeenkomstig artikel 47 bindende bedrijfsvoorschriften goed;

De toezichthouder kan toestemming geven voor door een concern opgestelde bindende bedrijfsvoorschriften voor doorgifte binnen dat concern aan onderdelen buiten de EU (artikel 47). Zie ook artikel 58 lid 3 punt j.

57.1(t) zij levert een bijdrage aan de activiteiten van het Comité;

Elke toezichthouder heeft zitting in het Comité (artikel 68 lid 3), en moet daar dan ook een actieve bijdrage in leveren.

57.1(u) zij houdt interne registers bij van inbreuken op deze verordening en van overeenkomstig artikel 58, lid 2, getroffen maatregelen; en

De toezichthouder documenteert schendingen van de AVG en de bijbehorende corrigerende maatregelen (artikel 58 lid 2). Deze registers zullen terugkomen in het jaarverslag (artikel 59), hoewel natuurlijk vertrouwelijkheid geboden kan zijn (artikel 54 lid 2).

57.1(v) zij verricht alle andere taken die verband houden met de bescherming van persoonsgegevens.

Als laatste wordt nog bepaald dat de toezichthouder al het andere kan en mag doen dat in verband staat met de bescherming van persoonsgegevens.

- 57.2 Elke toezichthoudende autoriteit faciliteert de indiening van klachten als bedoeld in lid 1, punt f), door maatregelen te nemen, zoals het ter beschikking stellen van een klachtenformulier dat ook elektronisch kan worden ingevuld, zonder dat andere communicatiemiddelen worden uitgesloten.

Iedere toezichthouder dient ingericht te zijn op het ontvangen van klachten (lid 1 punt f), en dit dient zo gemakkelijk mogelijk gemaakt te worden. Betrokkenen dienen te kunnen klagen via een elektronisch in te vullen formulier. De toezichthouder mag dus niet bijvoorbeeld eisen dat men schriftelijk klaagt of een kopie per post opstuurt.

- 57.3 Elke toezichthoudende autoriteit verricht haar taken kosteloos voor de betrokkene en, in voorkomend geval, voor de functionaris voor gegevensbescherming.

Alle taken die een toezichthouder verricht ten behoeve van betrokkenen geschieden kosteloos. Slechts bij kennelijk ongegronde of buitensporige verzoeken (lid 4) mag een toezichthouder een vergoeding vragen of de verzoeken afwijzen.

- 57.4 Wanneer verzoeken kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, kan de toezichthoudende autoriteit op basis van de administratieve kosten een redelijke vergoeding aanrekenen, of weigeren aan het verzoek gevolg te geven. Het is aan de toezichthoudende autoriteit om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

Een toezichthouder mag verzoeken van betrokkenen weigeren wanneer ze kennelijk ongegrond of buitensporig zijn. Ook mag de toezichthouder het verzoek alleen in behandeling nemen wanneer een redelijke vergoeding wordt betaald. Hiermee wil men proberen excessen en querulanten aan banden te leggen. De bewijslast dat hiervan sprake is, ligt bij de toezichthouder. Vergelijk artikel 12 lid 5 over buitensporige verzoeken om informatie bij verwerkingsverantwoordelijken.

Kennelijk ongegrond. Een verzoek is kennelijk ongegrond als evident niet is voldaan aan de randvoorwaarden bij een verzoek, of als wordt gevraagd om iets waar men evident geen recht op heeft. Voorbeelden zijn een verzoek tot handhaving bij gegevens van een overleden persoon of om ingrijpen bij een onderneming die inmiddels is opgeheven.

Buitensporig. Een verzoek is buitensporig als er sprake is van een zeer disproportionele last op de toezichthouder, bijvoorbeeld wanneer men wekelijks grote lappen contractuele bepalingen voorlegt ter goedkeuring (lid 3 punt r) of wanneer men dagelijks stapels papieren over triviale overtredingen aandraagt.

Artikel 58. Bevoegdheden van toezichthouders

58.1 Elke toezichthoudende autoriteit heeft alle volgende onderzoeksbevoegdheden om:

Iedere toezichthouder heeft in beginsel drie bevoegdheden: onderzoeksbevoegdheden (dit lid 1), corrigerende bevoegdheden (lid 2) en adviserende bevoegdheden (lid 3).

58.1(a) de verwerkingsverantwoordelijke, de verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke of van verwerker te gelasten alle voor de uitvoering van haar taken vereiste informatie te verstrekken;

De toezichthouder heeft de bevoegdheid te gelasten dat een verwerkingsverantwoordelijke, verwerker of vertegenwoordiger (van een partij buiten de EU, artikel 27) alle vereiste informatie verschaft. Als spiegel bepaalt artikel 31 dat de genoemde partijen desgevraagd samen moeten werken met de toezichthouder. In Nederland bepaalt artikel 5:20 Algemene wet bestuursrecht dat een ieder verplicht is aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden. De last tot het verstrekken van de informatie is aan te merken als een besluit in de zin van de Algemene wet bestuursrecht (artikel 14, lid 4 Uitvoeringswet).

58.1(b) onderzoeken te verrichten in de vorm van gegevensbeschermingscontroles;

Een gegevensbeschermingscontrole is een controle (audit) op de wijze waarop een verwerkingsverantwoordelijke of verwerker de beveiligingseis (artikel 32) bij de verwerking nakomt.

58.1(c) een toetsing te verrichten van de overeenkomstig artikel 42, lid 7, afgegeven certificeringen;

Onder artikel 42 kunnen certificeringen worden afgegeven waarmee kan worden aangetoond dat verwerkingsverantwoordelijken en verwerkers in overeenstemming met de AVG handelen. Wanneer aan de eisen voor de certificering niet of niet meer wordt voldaan, kan het worden ingetrokken (artikel 42 lid 7). De toezichthouder is bevoegd op ieder moment een certificering te toetsen.

58.1(d) de verwerkingsverantwoordelijke of de verwerker in kennis te stellen van een beweerde inbreuk op deze verordening;

Het is mogelijk dat een schending van de AVG als eerste wordt gemeld aan de toezichthouder, bijvoorbeeld omdat de ontdekker daarvan niet binnen de verwerkingsverantwoordelijke de juiste kanalen kan vinden. In dat geval kan de

toezichthouder zelf deze partijen informeren, zodat deze de juiste stappen kan nemen, zoals een waarschuwing geven of een boete opleggen.

58.1(e) van de verwerkingsverantwoordelijke en de verwerker toegang te verkrijgen tot alle persoonsgegevens en alle informatie die noodzakelijk is voor de uitvoering van haar taken; en

De toezichthouder mag in het kader van uitvoering van haar taak toegang vorderen tot persoonsgegevens die de verwerkingsverantwoordelijke en de verwerker verwerken, en meer algemeen alle noodzakelijke informatie verlangen. In Nederland is dit geregeld in artikel 5:17 Algemene wet bestuursrecht (inzage te vorderen van zakelijke gegevens en bescheiden). De AVG staat toe (artikel 90 lid 1) dat lidstaten in het kader van verwerkingen onder beroepsgeheim beperkingen stellen aan deze regel (vergelijk artikel 5:20 Algemene wet bestuursrecht).

58.1(f) toegang te verkrijgen tot alle bedrijfsruimten van de verwerkingsverantwoordelijke en de verwerker, daaronder begrepen tot alle uitrustingen en middelen voor gegevensverwerking, in overeenstemming met het uniale of lidstatelijke procesrecht.

Indien noodzakelijk voor de uitvoering van de taken van de toezichthouder kan deze toegang verlangen tot alle bedrijfsruimten, maar ook alle hulpmiddelen waarmee persoonsgegevens worden verwerkt. Dit zou ook een inspectie van relevante software kunnen omvatten. In Nederland kan de toezichthouder deze toegang verlangen conform artikel 5:15 Algemene wet bestuursrecht (toegang tot bedrijfsruimten) en 5:17 Awb (inzage te vorderen van zakelijke gegevens en bescheiden). De AVG staat toe (artikel 90 lid 1) dat lidstaten in het kader van verwerkingen onder beroepsgeheim beperkingen stellen aan deze regel (vergelijk artikel 5:20 Awb). De AP is daarnaast bevoegd om een woning te betreden zonder toestemming van de bewoner (artikel 15 lid 2 Uitvoeringswet).

58.2. Elke toezichthoudende autoriteit heeft alle volgende bevoegdheden tot het nemen van corrigerende maatregelen:

Naast de in lid 1 genoemde onderzoeksbevoegdheden heeft de toezichthouder ook bevoegdheden tot het nemen van corrigerende maatregelen, zoals waarschuwingen of stakingsbevelen maar ook een bevel tot uitvoeren van een specifieke plicht zoals het wissen van gegevens of het informeren van betrokkenen over een datalek. De maatregelen onder c t/m g en j worden als last opgelegd, welke kan worden versterkt met een dwangsom (artikel 5:32 Algemene wet bestuursrecht). Deze kan hoger zijn dan onder de Awb normaal toegestaan is: artikel 83 lid 6 staat een boete bij niet-nakoming toe van maximaal 20.000.000 euro of 4% van de totale wereldwijde jaaromzet als deze hoger is dan dat bedrag. Aangezien de corrigerende maatregelen worden aangemerkt als een besluit in de zin van de Algemene wet bestuursrecht (met uitzondering van de waarschuwing uit artikel 58, lid 2 punt a AVG), zijn de artikelen 5:4 tot en met 5:10 uit de

Algemene wet bestuursrecht hierbij van overeenkomstige toepassing (artikel 14 lid 4 Uitvoeringswet).

58.2(a) de verwerkingsverantwoordelijke of de verwerker waarschuwen dat met de voorgenomen verwerkingen waarschijnlijk inbreuk op bepalingen van deze verordening wordt gemaakt;

De lichtste corrigerende bevoegdheid is een waarschuwing dat waarschijnlijk inbreuk op de AVG wordt gemaakt. Dit middel kan alleen worden ingezet bij een voorgenomen verwerking. Wanneer uit een DPIA (artikel 35) blijkt dat een voorgenomen verwerking een hoog risico zou opleveren, moet de toezichthouder vooraf worden geraadpleegd (artikel 36 lid 1). De toezichthouder kan dan advies uitbrengen (artikel 36 lid 2). Als de voorgenomen verwerking waarschijnlijk niet door de beugel kan, dan krijgt het advies de vorm van een waarschuwing.

58.2(b) de verwerkingsverantwoordelijke of de verwerker berispen wanneer met verwerkingen inbreuk op bepalingen van deze verordening is gemaakt;

Wanneer de toezichthouder constateert dat sprake is van een overtreding van de AVG, kan in lichte gevallen worden gekozen te volstaan met een waarschuwing. De Awb kent dit instrument niet expliciet. Uit de jurisprudentie blijkt dat als een berisping niet meer is dan een vaststelling dat een overtreding is begaan, er geen sprake is van een besluit en dus ook geen mogelijkheid tot bezwaar en beroep.

58.2(c) de verwerkingsverantwoordelijke of de verwerker gelasten de verzoeken van de betrokkene tot uitoefening van zijn rechten uit hoofde van deze verordening in te willigen;

De toezichthouder kan gelasten dat de verwerkingsverantwoordelijke een verzoek tot uitoefening van rechten van de betrokkenen, zoals inzage (artikel 15), rectificatie (artikel 16), gegevenswissing (artikel 17), beperking (artikel 18) of data-export (artikel 20), inwilligt. De last kan ook aan de verwerker worden gegeven. De verwerker moet de verwerkingsverantwoordelijke (artikel 28 lid 3 punt e) bijstand verlenen bij het uitoefenen van rechten van de betrokkene.

58.2(d) de verwerkingsverantwoordelijke of de verwerker gelasten, waar passend, op een nader bepaalde manier en binnen een nader bepaalde termijn, verwerkingen in overeenstemming te brengen met de bepalingen van deze verordening;

Meer algemeen kan de toezichthouder gelasten dat de verwerkingsverantwoordelijke of de verwerker op een door de toezichthouder te bepalen wijze zijn verwerkingen aanpast om binnen de AVG te blijven.

58.2(e) de verwerkingsverantwoordelijke gelasten een inbreuk in verband met persoonsgegevens aan de betrokkene mee te delen;

Onder artikel 34 moet de verwerkingsverantwoordelijke een datalek melden aan betrokkenen wanneer deze waarschijnlijk een hoog risico inhoudt voor hun privacy. Als deze dat (nog) niet zelf heeft gedaan, kan de toezichthoudende autoriteit hem daartoe verplichten (artikel 34 lid 4), tenzij blijkt dat de gevolgen al zijn beperkt conform artikel 34 lid 3.

58.2(f) een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, opleggen;

De toezichthouder kan een beperking van de verwerking (artikel 18) gelasten of zelfs een verbod op verwerking.

58.2(g) het rectificeren of wissen van persoonsgegevens of het beperken van verwerking uit hoofde van de artikelen 16, 17 en 18 gelasten, alsmede de kennisgeving van dergelijke handelingen aan ontvangers aan wie de persoonsgegevens zijn verstrekt, overeenkomstig artikel 17, lid 2, en artikel 19;

De toezichthouder kan, ook als daar geen verzoek van betrokkenen over ligt, gelasten dat de verwerkingsverantwoordelijke of verwerker persoonsgegevens rectificeert (artikel 16) of wist (artikel 17), of de verwerking beperkt (artikel 18). De verwerkingsverantwoordelijke kan bij wissing gehouden zijn andere verwerkingsverantwoordelijken ook te gelasten de persoonsgegevens te wissen (artikel 17 lid 2). Betrokkenen moeten daarover worden geïnformeerd conform artikel 19.

58.2(h) een certificering intrekken of het certificeringsorgaan gelasten een uit hoofde van de artikelen 42 en 43 afgegeven certificering in te trekken, of het certificeringsorgaan te gelasten geen certificering af te geven indien niet langer aan de certificeringsvereisten wordt voldaan;

Technologieën voor gegevensbescherming kunnen worden gecertificeerd door toezichthouders (artikel 42) om aan te geven dat deze voldoen aan de eisen uit de AVG. Toezichthouders mogen ook derden als certificeringsorgaan aanwijzen (artikel 43). Certificeringen kunnen te allen tijde worden ingetrokken (artikel 42 lid 7) en de toezichthouder mag een certificeringsorgaan gelasten certificering te staken (artikel 43 lid 7).

58.2(i) naargelang de omstandigheden van elke zaak, naast of in plaats van de in dit lid bedoelde maatregelen, een administratieve geldboete opleggen op grond van artikel 83; en

De toezichthouder kan ervoor kiezen een geldboete op te leggen (artikel 83) als dat gezien de aard van de overtreding passend is (zie artikel 83 lid 2) en de boete

doeltreffend, evenredig en afschrikkend is. Deze boete staat los van een eventuele dwangsom op niet-nakoming (vergelijk artikel 83 lid 6).

58.2(j) de opschorting van gegevensstromen naar een ontvanger in een derde land of naar een internationale organisatie gelasten.

De toezichthouder kan bepalen dat doorgifte naar een specifieke ontvanger buiten de EU niet langer toegestaan is, wanneer deze ontvanger niet voldoet aan de eisen uit hoofdstuk V.

58.3 Elke toezichthoudende autoriteit heeft alle autorisatie- en adviesbevoegdheden om:

Als derde heeft iedere toezichthouder de bevoegdheid om bepaalde adviezen te verstrekken en om certificeringen en gedragscodes en dergelijke goed te keuren. De autorisatie- en adviesbevoegdheden worden, met uitzondering van verstrekt advies (lid a) aangemerkt als een besluit in de zin van de Algemene wet bestuursrecht.

58.3(a) de verwerkingsverantwoordelijke advies te verstrekken in overeenstemming met de procedure van voorafgaande raadpleging van artikel 36;

Een verwerkingsverantwoordelijke moet bij verwerkingen met verhoogd risico voorafgaand aan de verwerking de toezichthoudende autoriteit raadplegen (artikel 36). Deze adviseert dan over of de verwerking plaats mag vinden en eventueel onder welke voorwaarden.

58.3(b) op eigen initiatief dan wel op verzoek, aan het nationaal parlement, aan de regering van de lidstaat, of overeenkomstig het lidstatelijke recht aan andere instellingen en organen alsmede aan het publiek advies te verstrekken over aangelegenheden die verband houden met de bescherming van persoonsgegevens;

Een toezichthouder kan aan overheidsinstellingen, maar ook aan het publiek, advies verstrekken over alle aangelegenheden omtrent de bescherming van persoonsgegevens.

58.3(c) toestemming te geven voor verwerking als bedoeld in artikel 36, lid 5, indien die voorafgaande toestemming door het lidstatelijke recht wordt voorgeschreven;

Een lidstaat kan ervoor kiezen een voorafgaande toestemming van de toezichthouder verplicht te stellen bij verwerkingen op grond van het algemeen belang (artikel 36 lid 5), zoals bij sociale zekerheid en volksgezondheid.

58.3(d) overeenkomstig artikel 40, lid 5, advies uit te brengen over en goedkeuring te hechten aan de ontwerpgedragscodes;

Brancheorganisaties en dergelijke kunnen een gedragscode (artikel 40) invoeren over hoe de AVG in hun branche moeten worden toegepast. Dit vereist het advies van de toezichthouder (artikel 40 lid 5).

58.3(e) certificeringsorganen te accrediteren overeenkomstig artikel 43;

Verwerkingen en mechanismen daarvoor kunnen worden gecertificeerd (artikel 42). Dit kan door de toezichthouder gebeuren maar ook door een geaccrediteerd certificeringsorgaan (artikel 43). Accreditatie gebeurt door de toezichthouder.

58.3(f) certificeringen af te geven en certificeringscriteria goed te keuren overeenkomstig artikel 42, lid 5;

De toezichthouder kan verwerkingen en mechanismen daarvoor certificeren, en ook criteria voor certificering goedkeuren (artikel 42 lid 5).

58.3(g) de in artikel 28, lid 8, en artikel 46, lid 2, punt d), bedoelde standaardbepalingen inzake gegevensbescherming aan te nemen;

De toezichthouder kan standaardbepalingen vaststellen voor verwerkersovereenkomsten (artikel 28 lid 8), en ook voor standaardbepalingen inzake gegevensbescherming bij doorgiften naar derde landen (artikel 46 lid 2 punt d).

58.3(h) toestemming te verlenen voor de in artikel 46, lid 3, punt a), bedoelde contractbepalingen;

De toezichthouder kan toestemming geven voor het hanteren van zelfgemaakte contractbepalingen voor waarborging van doorgifte naar derde landen (artikel 46 lid 3 punt a).

58.3(i) toestemming te verlenen voor de in artikel 46, lid 3, punt b), bedoelde administratieve regelingen;

De toezichthouder kan toestemming geven voor doorgifte door overheidsinstanties aan derde landen in het geval deze geen juridisch bindende regelingen treffen (artikel 36 lid 3 punt b).

58.3(j) goedkeuring te hechten aan bindende bedrijfsvoorschriften overeenkomstig artikel 47.

De toezichthouder kan toestemming geven voor door een concern opgestelde bindende bedrijfsvoorschriften voor doorgifte binnen dat concern aan onderdelen buiten de EU (artikel 47).

- 58.4 Op de uitoefening van de bevoegdheden die uit hoofde van dit artikel aan de toezichthoudende autoriteit worden verleend, zijn passende waarborgen van toepassing, daaronder begrepen een doeltreffende voorziening in rechte en een eerlijke rechtsbedeling, zoals overeenkomstig het Handvest vastgelegd in het Unierecht en het lidstatelijke recht.

Uitoefening van de bevoegdheden uit lid 1, 2 of 3 mag uiteraard alleen wanneer dit binnen de fundamentele rechtsorde van de EU plaatsvindt. De aangesproken partij heeft dus onder meer recht op een eerlijk proces, zoals in het Handvest grondrechten EU voor de grondrechten is opgenomen.

- 58.5 Elke lidstaat bepaalt bij wet dat zijn toezichthoudende autoriteit bevoegd is inbreuken op deze verordening ter kennis te brengen van de gerechtelijke autoriteiten en, waar passend, daartegen een rechtsvordering in te stellen of anderszins in rechte op te treden, teneinde de bepalingen van deze verordening te doen naleven.

Toezichthouders zijn bevoegd zelf corrigerende maatregelen te nemen (lid 2) waar dat passend is. Dit lid 5 bepaalt dat het aan de lidstaat is hoe deze maatregelen worden afgedwongen. Ons systeem van bestuursrechtelijke handhaving is een mogelijkheid; het aanbrengen bij de (civiele dan wel straf)rechter en van daaruit de handhaving laten verlopen is ook mogelijk. Zie ook artikel 83 lid 9.

- 58.6 Elke lidstaat kan bij wet bepalen dat zijn toezichthoudende autoriteit, naast de in lid 1, 2 en 3 bedoelde bevoegdheden bijkomende bevoegdheden heeft. De uitoefening van die bevoegdheden doet geen afbreuk aan de doeltreffende werking van hoofdstuk VII.

Een lidstaat mag in nationaal recht aanvullende bevoegdheden opnemen voor zijn toezichthouder. Deze bevoegdheden mogen echter niet de regels omtrent samenwerking en grensoverschrijdende bevoegdheid uit hoofdstuk VII van de AVG doorkruisen.

Artikel 59. Activiteitenverslagen

Elke toezichthoudende autoriteit stelt jaarlijks een verslag over haar activiteiten op, met daarin mogelijk een lijst van de soorten gemelde inbreuken en de soorten maatregelen die overeenkomstig artikel 58, lid 2, worden genomen. Die verslagen worden toegezonden aan het nationale parlement, de regering en elke andere autoriteit die daartoe in het lidstatelijke recht is aangewezen. Zij worden ter beschikking gesteld van het publiek, de Commissie en het Comité.

Iedere toezichthouder moet jaarlijks verslag doen van haar activiteiten. Zij kan ervoor kiezen daarin een lijst van schendingen van de AVG op te nemen en/of een lijst van maatregelen zoals opgelegde waarschuwingen, verboden en geldboetes (artikel 58 lid 2). Zie ook artikel 57 lid 1 punt u.

Toezending. De toezichthouder stuurt het jaarverslag naar alle autoriteiten die daar krachtens het nationale recht belang bij hebben. In Nederland wordt het jaarverslag van een zelfstandig bestuursorgaan toegezonden aan de minister en aan beide kamers der Staten-Generaal (artikel 18 Kaderwet zelfstandige bestuursorganen).

Publicatie. De jaarverslagen worden beschikbaar gesteld voor het publiek, voor de Commissie en het Comité van toezichthouders. Het ligt voor de hand dat dit op de website van het Comité zal gebeuren (vergelijk artikel 70 lid 1 punt y over de publicatie van besluiten van toezichthouders).

Hoofdstuk VII

Samenwerking en coherentie

Bij invoering van de AVG is gekozen voor een systeem van samenwerkende nationale toezichthouders in plaats van één Europese toezichthouder. Hoofdstuk VII regelt hoe de toezichthouders met elkaar samenwerken. Het hoofdstuk kent drie afdelingen.

Afdeling 1 regelt de onderlinge samenwerking. Allereerst is er een vorm van samenwerking waarbij één toezichthouder de leiding neemt en de overige betrokken toezichthouders hem volgen (artikel 60). Daarnaast is er de wederzijdse bijstand (artikel 62) waarbij personeel wordt uitgeleend. Meer algemeen is er de plicht tot informatie-uitwisseling (artikel 61).

Komen toezichthouders er niet uit, dan regelt afdeling 2 hoe men in onderlinge afstemming tot eenvormige beslissingen kan komen, het zogeheten coherentiemechanisme (artikel 63). Het Comité voor gegevensbescherming kan hierbij adviserend optreden (artikel 64) maar uiteindelijk in bepaalde gevallen ook bindend advies (artikel 65) geven.

In afdeling 3 tenslotte wordt het Europees Comité voor gegevensbescherming ("het Comité") als een onafhankelijk orgaan van de EU opgericht (artikel 68) met als takenpakket (artikel 70) het afstemmen van de toezichthouderspraktijk en adviseren aan alle partijen.

AFDELING 1. SAMENWERKING

Toezichthouders kunnen op verschillende manieren samenwerken. Allereerst is er een vorm van samenwerking waarbij één toezichthouder de leiding neemt en de overige betrokken toezichthouders hem volgen (artikel 60). Daarnaast is er de wederzijdse bijstand (artikel 62) waarbij personeel wordt uitgeleend. Meer algemeen is er de plicht tot informatie-uitwisseling (artikel 61).

Artikel 60. Samenwerking tussen de leidende toezichthoudende autoriteit en andere betrokken toezichthoudende autoriteiten

60.1 De leidende toezichthoudende autoriteit werkt overeenkomstig dit artikel samen met de andere betrokken toezichthoudende autoriteiten teneinde tot een consensus proberen te komen. De leidende toezichthoudende autoriteit en de betrokken toezichthoudende autoriteiten wisselen alle relevante informatie met elkaar uit.

Bij verwerkingen in meerdere lidstaten zijn volgens de hoofdregel (artikel 55) meerdere toezichthouders bevoegd. Om uiteenlopende beslissingen te voorkomen, is gekozen voor een éénloketsprocedure waarbij één toezichthouder de leiding neemt en over de gehele verwerking kan oordelen.

Leidende toezichthouder. De toezichthouder die de leiding neemt, is de toezichthouder van de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke of verwerker (artikel 56 lid 1).

Consensus. Doel van de samenwerkingsprocedure is tot consensus te komen. Dit volgt ook uit het coherentiemechanisme (artikel 63), dat inhoudt dat toezichthouders met elkaar en met de Commissie samenwerken, met name om te voorkomen dat uiteenlopende besluiten worden genomen over toegestane of verboden verwerkingen.

Procedure. Conform dit artikel 60 moet de leidende toezichthouder samenwerken met de andere toezichthouders om tot een consensus te komen ten aanzien van een vermeende schending of andere kwestie ten aanzien van een grensoverschrijdende verwerking. Allereerst moet zij besluiten (artikel 56 lid 3) of zij de zaak al dan niet zal behandelen. Als zij dat besluit, moet eveneens conform dit artikel worden samengewerkt om tot een besluit te komen ten aanzien van de verwerking.

Nederland. De AP dient eventuele samenwerkingsprotocollen met andere toezichthouders bekend te maken in de Staatscourant (artikel 19 lid 1 Uitvoeringswet).

60.2 De leidende toezichthoudende autoriteit kan te allen tijde andere betrokken toezichthoudende autoriteiten verzoeken wederzijdse bijstand overeenkomstig artikel 61 te verlenen, en kan gezamenlijke werkzaamheden ondernemen overeenkomstig artikel 62, in het bijzonder voor het uitvoeren van onderzoeken of voor het toezicht op de uitvoering van een maatregel betreffende een in een andere lidstaat gevestigde verwerkingsverantwoordelijke of verwerker.

De leidende toezichthouder kan medewerking van andere betrokken toezichthouders verlangen. Dit kan bestaan uit wederzijdse bijstand (artikel 61), waarbij

men elkaar op de hoogte houdt van relevante zaken en elkaar assisteert, en uit gezamenlijke werkzaamheden (artikel 62), waarbij men gezamenlijk een onderzoek start of handhavingsmaatregelen oplegt.

- 60.3 De leidende toezichthoudende autoriteit deelt onverwijld alle relevante informatie over de aangelegenheid mee aan de andere betrokken toezichthoudende autoriteiten. Zij legt de andere betrokken toezichthoudende autoriteiten onverwijld te hunner beoordeling een ontwerpbesluit voor en houdt naar behoren rekening met hun standpunten.

In het kader van de samenwerking (lid 1) moet de leidende toezichthouder in ieder geval alle relevante informatie delen met de andere betrokken toezichthouders. Ook moeten deze andere toezichthouders betrokken worden bij het nemen van een besluit ten aanzien van de verwerking waar het onderzoek over gaat. Zij kunnen vervolgens bezwaar maken (lid 4).

Ontwerpbesluit door lokale toezichthouder. Wanneer een lokale toezichthouder een zaak heeft doorgegeven aan de leidende toezichthouder, mag deze tevens een ontwerpbesluit aandragen. De leidende toezichthouder moet zo veel mogelijk rekening daarmee houden (artikel 56 lid 4).

- 60.4 Indien één van de andere betrokken toezichthoudende autoriteiten binnen een termijn van vier weken na te zijn geraadpleegd overeenkomstig lid 3 van dit artikel een relevant en gemotiveerd bezwaar tegen het ontwerpbesluit indient, onderwerpt de leidende toezichthoudende autoriteit, indien zij het relevante en gemotiveerde bezwaar afwijst of het niet relevant en niet gemotiveerd acht, de aangelegenheid aan het in artikel 63 bedoelde coherentiemechanisme.

Wanneer de leidende toezichthouder een ontwerpbesluit voorlegt (lid 3), kunnen de andere toezichthouders daar bezwaar tegen maken. Dit bezwaar dient relevant en gemotiveerd te zijn. Als de leidende toezichthouder zich niet kan vinden in het bezwaar, treedt het coherentiemechanisme van artikel 63 in werking. Anders wordt het ontwerpbesluit herzien (lid 5). Indien er geen bezwaren zijn binnen vier weken, wordt het ontwerpbesluit definitief (lid 6).

Relevant en gemotiveerd bezwaar. Een relevant en gemotiveerd bezwaar (zie artikel 4 definitie 24) is een bezwaar over het al dan niet bestaan van een inbreuk op de AVG, of over de vraag of de voorgenomen maatregel strookt met de AVG. Het bezwaar moet duidelijk de omvang van de risico's van het ontwerpbesluit documenten voor de grondrechten van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie. Het Comité kan richtsnoeren opstellen over de invulling van deze criteria (artikel 70 lid 1 punt t). Zie nader Richtsnoeren 9/2020 inzake relevant en gemotiveerd bezwaar overeenkomstig Verordening 2016/679 van het Comité, 9 maart 2021.

- 60.5 Indien de leidende toezichthoudende autoriteit voornemens is het ingediende relevante en gemotiveerde bezwaar te honoreren, legt zij de overige betrokken toezichthoudende autoriteiten te hunner beoordeling een herzien ontwerpbesluit voor. Dat herziene ontwerpbesluit wordt binnen een termijn van twee weken aan de in lid 4 bedoelde procedure onderworpen.

Als de leidende toezichthouder het bezwaar van een andere betrokken toezichthouder overneemt (zie lid 4), moet het ontwerpbesluit worden herzien. Dit wordt dan opnieuw voorgelegd, waarna alle betrokken toezichthouders opnieuw bezwaar kunnen maken conform lid 4.

- 60.6 Indien geen enkele andere betrokken toezichthoudende autoriteit binnen de in de leden 4 en 5 bedoelde termijn bezwaar heeft gemaakt tegen het door de leidende toezichthoudende autoriteit voorgelegde ontwerpbesluit, worden de leidende toezichthoudende autoriteit en de betrokken toezichthoudende autoriteiten geacht met dat ontwerpbesluit in te stemmen en zijn zij daaraan gebonden.

Als er (al dan niet na herziening conform lid 5) geen bezwaren zijn tegen een ontwerpbesluit, wordt het ontwerpbesluit definitief. Alle toezichthouders zijn daar vervolgens aan gebonden. Het besluit kan dan worden opgelegd aan de verwerkingsverantwoordelijke of de verwerker (lid 6).

- 60.7 De leidende toezichthoudende autoriteit stelt het besluit vast en deelt het mee aan de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke of de verwerker, naargelang het geval, en stelt de andere betrokken toezichthoudende autoriteiten, alsmede het Comité in kennis van het besluit in kwestie, voorzien van een samenvatting van de relevante feiten en gronden. De toezichthoudende autoriteit waarbij de klacht is ingediend, stelt de klager in kennis van het besluit.

Na goedkeuring door alle betrokken toezichthouders (lid 6) wordt een ontwerpbesluit definitief. Vervolgens stelt de leidende toezichthouder het besluit formeel vast, waarna het wordt medegedeeld aan de verwerkingsverantwoordelijke of de verwerker die het betreft.

Informatie aan toezichthouders en Comité. Het bestaan van het besluit en een samenvatting daarvan wordt gemeld aan de andere betrokken toezichthouders en aan het Comité. Het Comité kan het besluit vervolgens opnemen in het register (artikel 70 lid 1 punt y).

Informatie aan klager. Indien het besluit genomen is naar aanleiding van een klacht (artikel 57 lid 1 punt f), zal de betrokken toezichthouder (waar de klacht is ingediend) de klager informeren over het besluit.

- 60.8 Ingeval een klacht is afgewezen of verworpen, stelt de toezichthoudende autoriteit waarbij de klacht is ingediend, in afwijking van lid 7, het besluit vast en deelt zij het mee aan de klager en stelt zij de verwerkingsverantwoordelijke ervan in kennis.

Wanneer het besluit is dat de klacht wordt afgewezen, dan wordt dit besluit genomen door de toezichthouder waar de klacht is ingediend en niet door de leidende toezichthouder. Deze toezichthouder meldt het besluit vervolgens aan de klager en aan de verwerkingsverantwoordelijke (of, zo mag men aannemen, de verwerker).

- 60.9 Indien de leidende toezichthoudende autoriteit en de betrokken toezichthoudende autoriteiten het erover eens zijn delen van een klacht af te wijzen of te verwerpen en voor andere delen van die klacht op te treden, wordt voor elk van die laatstgenoemde delen een afzonderlijk besluit vastgesteld. De leidende toezichthoudende autoriteit stelt het besluit vast voor het deel betreffende de maatregelen inzake de verwerkingsverantwoordelijke, en deelt het mee aan de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke of de verwerker op het grondgebied van haar lidstaat, en stelt de klager daarvan in kennis. Voor het deel waarvoor de klacht in kwestie is afgewezen of verworpen, wordt het besluit vastgesteld door de toezichthoudende autoriteit van de klager, en door haar aan die klager medegedeeld, en wordt de verwerkingsverantwoordelijke of de verwerker daarvan in kennis gesteld.

Wanneer een klacht gedeeltelijk terecht is, worden twee besluiten genomen: het eerste betreffende de terechte delen van de klacht, en het tweede betreffende de afgewezen delen daarvan. De besluitprocedure voor het eerste besluit is conform lid 7 (de leidende toezichthouder stelt het vast) en voor het tweede besluit conform lid 8 (de toezichthouder die de klacht ontving, stelt het vast).

- 60.10 De verwerkingsverantwoordelijke of de verwerker treft, na in kennis te zijn gesteld van het besluit van de leidende toezichthoudende autoriteit overeenkomstig de leden 7 en 9, de nodige maatregelen teneinde het besluit wat betreft de verwerkingsactiviteiten binnen al zijn vestigingen binnen de Unie te doen naleven. De verwerkingsverantwoordelijke of de verwerker deelt de door hem met het oog op de naleving van het besluit getroffen maatregelen mee aan de leidende toezichthoudende autoriteit, die de andere betrokken toezichthoudende autoriteiten ervan in kennis stelt.

Wanneer een verwerkingsverantwoordelijke of verwerker een besluit opgelegd krijgt, dient hij natuurlijk zijn verwerkingen aan te passen om te voldoen aan het besluit. Zie nader de corrigerende bevoegdheden uit artikel 58 lid 2 en de algemene medewerkingsplicht uit artikel 31.

60.II Indien, in buitengewone omstandigheden, een betrokken toezichthoudende autoriteit het met reden dringend noodzakelijk acht dat in het belang van bescherming van de belangen van betrokkenen wordt opgetreden, is de in artikel 66 bedoelde spoedprocedure van toepassing.

De werkwijze volgens dit artikel kan tot vertraging leiden in verband met de afstemming en bijbehorend advies van het Comité. Daarom kent de AVG een spoedprocedure (artikel 66), waaronder een toezichthouder een voorlopige maatregel mag opleggen die maximaal drie maanden van kracht is en uitsluitend voor de eigen lidstaat geldt.

60.I2 De leidende toezichthoudende autoriteit en de andere betrokken toezichthoudende autoriteiten verstrekken elkaar langs elektronische weg, door middel van een standaardformulier, de krachtens dit artikel vereiste informatie.

Om informatie-uitwisseling tussen toezichthouders te vergemakkelijken, schrijft de AVG een elektronische verstrekking voor. De Commissie bepaalt hoe dit standaardformulier opgezet en gerealiseerd wordt (artikel 67). Zie nader Richtsnoeren 02/2022 voor de toepassing van artikel 60 AVG van het Comité, 14 maart 2022 .

Artikel 61. Wederzijdse bijstand

61.I De toezichthoudende autoriteiten verstrekken elkaar relevante informatie en wederzijdse bijstand om deze verordening op een consequente manier ten uitvoer te leggen en toe te passen, en nemen maatregelen om doeltreffend met elkaar samen te werken. De wederzijdse bijstand bestrijkt met name informatieverzoeken en toezichtsmaatregelen, zoals verzoeken om voorafgaande toestemming en raadpleging, inspecties en onderzoeken.

In het kader van wederzijdse bijstand en het streven naar consensus (artikel 60) dienen toezichthouders elkaar op de hoogte te houden van relevante zaken en elkaar bijstand te verlenen om tot een consequente toepassing van de AVG te komen.

Informatieverstrekking. Het delen van informatie zal in de praktijk de meest voorkomende manier zijn van samenwerking door toezichthouders.

Wederzijdse bijstand. Toezichthouders staan elkaar bij in de uitvoering van de AVG, zoals bij gezamenlijke acties (zie artikel 62) of in het overleg wanneer één van hen de leidende toezichthouder vormt (artikel 60). Bijstand omvat vooral het verstrekken van informatie, maar ook het samenwerken bij het uitvoeren van toezicht, zoals bij het afhandelen van verzoeken over voorafgaande toestemming (artikel 36) en het uitvoeren van inspecties (artikel 58 lid 1 punten e en f).

Een nadere vorm van bijstand is gezamenlijk onderzoek of handhaving (artikel 62).

- 61.2 Elke toezichthoudende autoriteit neemt alle passende maatregelen die nodig zijn om een verzoek van een andere toezichthoudende autoriteit onverwijld en uiterlijk binnen één maand na ontvangst daarvan te beantwoorden. Hierbij kan het in het bijzonder gaan om toezending van relevante informatie over de uitvoering van een onderzoek.

Verzoeken om informatie of bijstand dienen uiterlijk binnen één maand te worden afgehandeld. Wordt deze termijn niet gehaald, dan wordt de verzoekende toezichthouder bevoegd (lid 8) om een voorlopige spoedmaatregel (artikel 67) te nemen.

- 61.3 Verzoeken om bijstand bevatten alle nodige informatie, waaronder het doel van en de redenen voor het verzoek. De uitgewisselde informatie wordt alleen gebruikt voor het doel waarvoor om die informatie is verzocht.

Verzoeken om informatie dienen alle benodigde informatie te bevatten om ze af te kunnen handelen. De verzoeken, en de antwoorden, mogen alleen worden gebruikt voor het doel waarvoor het verzoek is gedaan.

- 61.4 De toezichthoudende autoriteit waaraan een verzoek om bijstand is gericht, wijst dit verzoek slechts af indien:

61.4(a) zij niet bevoegd is voor het onderwerp van het verzoek of voor de maatregelen die zij verzocht wordt uit te voeren; of

61.4(b) het verzoek inbreuk maakt op deze verordening of met Unierecht of lidstatelijk recht dat van toepassing is op de toezichthoudende autoriteit die het verzoek ontvangt.

Een toezichthouder is in beginsel altijd gehouden om verzoeken in te willigen. Slechts wanneer zij niet bevoegd is de gevraagde informatie of bijstand te verstrekken (artikel 58), of wanneer het verzoek in strijd is met de AVG of ander toepasselijk recht, mag zij het verzoek afwijzen. Deze grond voor afwijzing moet worden gemotiveerd (lid 5).

- 61.5 De toezichthoudende autoriteit tot wie het verzoek is gericht, informeert de verzoekende toezichthoudende autoriteit over de resultaten of, in voorkomend geval, de voortgang van de maatregelen die in antwoord op het verzoek zijn genomen. Indien de toezichthoudende autoriteit tot wie het verzoek is gericht het verzoek op grond van lid 4 afwijst, licht zij de redenen daarvoor toe.

De aangezochte toezichthouder moet de verzoekende toezichthouder informeren over de voortgang en resultaten van hetgeen waarover verzocht is. Een afwijzing van een verzoek (zie lid 4) moet gemotiveerd zijn.

- 6I.6 Toezichthoudende autoriteiten tot wie het verzoek is gericht delen in de regel de door andere toezichthoudende autoriteiten gevraagde informatie langs elektronische weg mee door middel van een standaardformulier.

Verzoeken om informatie en bijstand worden elektronisch afgehandeld, tenzij dit niet mogelijk is. Het is wenselijk dat daarvoor een standaardformulier wordt ontwikkeld. De Commissie bepaalt hoe dit standaardformulier opgezet en gerealiseerd wordt (artikel 67).

- 6I.7 De maatregelen die toezichthoudende autoriteiten tot wie een verzoek is gericht nemen uit hoofde van een verzoek om wederzijdse bijstand, zijn kosteloos. De toezichthoudende autoriteiten kunnen regels overeenkomen om elkaar te vergoeden voor specifieke uitgaven die voortvloeien uit het verstrekken van wederzijdse bijstand in uitzonderlijke omstandigheden.

Toezichthouders mogen elkaar geen kosten in rekening brengen voor het afhandelen van informatieverzoeken of verzoeken om bijstand. Slechts in uitzonderlijke gevallen, bijvoorbeeld bij zeer complexe verzoeken aan een relatief kleine toezichthouder waarvoor extra mankracht moet worden ingeschakeld, zouden afwijkende afspraken kunnen worden gemaakt.

- 6I.8 Wanneer een toezichthoudende autoriteit de in lid 5 bedoelde informatie niet binnen één maand na ontvangst van het verzoek van een andere toezichthoudende autoriteit verstrekt, kan de verzoekende toezichthoudende autoriteit overeenkomstig artikel 55, lid 1, op het grondgebied van haar lidstaat een voorlopige maatregel nemen. In dat geval wordt geacht dat er overeenkomstig artikel 66, lid 1, dringend moet worden opgetreden en dat dit een dringend bindend besluit van het Comité vereist overeenkomstig artikel 66, lid 2.

Een verzoek om informatie of bijstand moet binnen een maand worden afgehandeld (lid 5). Wanneer de reactie in deze periode uitblijft, kan de verzoekende toezichthouder binnen de spoedprocedure (artikel 66 lid 1) een voorlopige maatregel nemen. Deze mag maximaal drie maanden geldig zijn en moet beperkt zijn tot het grondgebied waar deze toezichthouder bevoegd voor is (artikel 55 lid 1). Vervolgens moet het Comité om een bindend besluit worden verzocht over eventueel te nemen definitieve maatregelen (artikel 66 lid 2).

61.9 De Commissie kan door middel van uitvoeringshandelingen het model en de procedures voor de in dit artikel bedoelde wederzijdse bijstand vastleggen, alsmede de regelingen voor de elektronische uitwisseling van informatie tussen toezichthoudende autoriteiten onderling en tussen toezichthoudende autoriteiten en het Comité, waaronder het in lid 6 van dit artikel bedoelde standaardformulier. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure.

Teneinde het afhandelen van informatieverzoeken en verzoeken om bijstand te vergemakkelijken, kan een gestandaardiseerde procedure en een werkmodel worden ingevoerd. Aansluitend is het regelen van elektronische uitwisseling van informatie (zie ook artikel 67). De Commissie maakt hiervoor een ontwerp-regeling en legt dat voor aan het artikel 93-comité. Dat comité beslist vervolgens met meerderheid van stemmen (artikel 93 lid 2). Indien het advies positief is, wordt de regeling ingevoerd.

Artikel 62. Gezamenlijke werkzaamheden van toezichthoudende autoriteiten

62.1 In voorkomend geval voeren de toezichthoudende autoriteiten gezamenlijke werkzaamheden uit, waaronder gezamenlijke onderzoeken en gezamenlijke handavingsmaatregelen, waarbij leden of personeelsleden van de toezichthoudende autoriteiten van andere lidstaten worden betrokken.

Naast samenwerking onder één leiding (artikel 60) en wederzijdse bijstand (artikel 61) kunnen toezichthouders ook gezamenlijk een onderzoek starten of handavingsmaatregelen opleggen. Hierbij treden leden of personeel van verschillende toezichthouders onder gezag van één van hen op in het kader van een onderzoek of handhaving. Dit verschilt van de samenwerking onder artikel 60, waarbij één toezichthouder de leiding neemt en (weliswaar in overleg) tot een besluit komt ten aanzien van de verwerking.

62.2 Indien de verwerkingsverantwoordelijke of de verwerker vestigingen heeft in meerdere lidstaten, of indien een significant aantal betrokkenen in meer dan één lidstaat waarschijnlijk wezenlijke gevolgen ondervindt van de verwerkingsactiviteiten, heeft van elk van die lidstaten één toezichthoudende autoriteit het recht om aan de gezamenlijke werkzaamheden deel te nemen. De toezichthoudende autoriteit die bevoegd is overeenkomstig artikel 56, lid 1 of lid 4, verzoekt de toezichthoudende autoriteit van elk van die lidstaten om deelname aan de gezamenlijke werkzaamheden in kwestie en beantwoordt onverwijld het verzoek van een toezichthoudende autoriteit om te mogen deelnemen.

In veel gevallen zullen gezamenlijke werkzaamheden uitgevoerd worden omdat sprake is van een grensoverschrijdende verwerking waar vraagtekens bij te stel-

len zijn. In die situatie mag elke betrokken lidstaat deelnemen aan de gezamenlijke werkzaamheden. Dit wordt gecoördineerd door de toezichthouder voor de hoofdvestiging (artikel 4 definitie 16) van de verwerkingsverantwoordelijke of verwerker in kwestie.

Grensoverschrijdend. Van een grensoverschrijdende situatie is sprake wanneer de verwerkingsverantwoordelijke of de verwerker vestigingen heeft in meerdere lidstaten, of wanneer een significant aantal betrokkenen in meerdere lidstaten wezenlijke gevolgen ondervindt van de verwerking. Vergelijk artikel 56 lid 1 dat in dergelijke gevallen de competentie van een leidende toezichthouder aanwijst.

Meerdere toezichthouders. Onder de AVG is het mogelijk dat een EU-lidstaat meerdere toezichthouders heeft (zie artikel 51 lid 1). Eén van hen neemt dan deel aan de gezamenlijke werkzaamheden.

- 62.3 Een toezichthoudende autoriteit kan overeenkomstig het lidstatelijke recht en met toestemming van de ondersteunende toezichthoudende autoriteit, aan de aan gezamenlijke werkzaamheden deelnemende leden of personeelsleden van de ondersteunende toezichthoudende autoriteit bevoegdheden toekennen, onder meer in verband met het voeren van onderzoek, of, voor zover het nationale recht de ontvangende toezichthoudende autoriteit dat toestaat, de leden of de personeelsleden van de ondersteunende toezichthoudende autoriteit toestaan om hun onderzoeksbevoegdheden overeenkomstig het nationale recht van de ondersteunende toezichthoudende autoriteit uit te oefenen. Deze onderzoeksbevoegdheden mogen hierbij uitsluitend worden uitgeoefend onder leiding en in aanwezigheid van leden of personeelsleden van de ontvangende toezichthoudende autoriteit. De leden of de personeelsleden van de ondersteunende toezichthoudende autoriteit zijn onderworpen aan het recht van de lidstaat van de ontvangende toezichthoudende autoriteit.

Bij gezamenlijk optreden treden personeel of leden van een toezichthouder op samen met die van een andere, de ontvangende toezichthouder. Deze laatste mag dit personeel en/of leden bevoegdheden toekennen voor onderzoek (zoals het mogen binnentreden, art. 5:27 lid 1 Awb) of toestaan de bevoegdheden uit hun eigen lidstaat uit te oefenen in de ontvangende lidstaat.

Toezicht. Vereist is wel dat een bevoegd leidinggevende van de ontvangende toezichthouder daarbij aanwezig is en dat een en ander verloopt binnen het recht van de ontvangende lidstaat.

Schade. Wanneer aldus ingezet personeel schade aanricht bij derden, is de lidstaat van de ontvangende toezichthouder daarvoor aansprakelijk (leden 4 en 5).

- 62.4 Wanneer personeelsleden van een ondersteunende toezichthoudende autoriteit overeenkomstig lid 1 actief zijn in een andere lidstaat, neemt de lidstaat van de ontvangende toezichthoudende autoriteit de verantwoordelijkheid voor hun activiteiten, met inbegrip van de aansprakelijkheid voor alle door die personeelsleden bij de uitvoering van hun werkzaamheden veroorzaakte schade, overeenkomstig het recht van de lidstaat op het grondgebied waarvan die personeelsleden actief zijn.

Wanneer een toezichthouder personeel van een andere toezichthouder inzet bij gezamenlijke werkzaamheden onder dit artikel, is deze ontvangende toezichthouder verantwoordelijk en aansprakelijk voor hun handelen. De regels voor aansprakelijkheid zijn die in het algemeen gelden bij schade veroorzaakt door overheidsoptreden. In Nederland zie artikel 8:88 en verder Awb. Indien de ontvangende lidstaat schade moet vergoeden, wordt deze verhaald conform lid 5.

- 62.5 De lidstaat op het grondgebied waarvan de schade is veroorzaakt, vergoedt deze schade onder de voorwaarden die gelden voor door zijn eigen personeelsleden veroorzaakte schade. De lidstaat van de ondersteunende toezichthoudende autoriteit waarvan de personeelsleden op het grondgebied van een andere lidstaat aan iemand schade hebben berokkend, betaalt die andere lidstaat het volledige bedrag terug dat die andere lidstaat voor rekening van die personeelsleden aan de rechthebbenden heeft uitgekeerd.

Schade bij handelen door personeel van een ondersteunende toezichthouder wordt vergoed door de lidstaat van de ontvangende toezichthouder conform de nationale regels van die lidstaat (zie ook lid 4). De lidstaat van de ondersteunende toezichthouder vergoedt deze schade vervolgens aan de lidstaat van de ontvangende toezichthouder. Andere mogelijkheden tot verhaal van schade zijn uitgesloten onder lid 6.

- 62.6 Onverminderd de uitoefening van zijn rechten tegenover derden en met uitzondering van het in lid 5 bepaalde, ziet elke lidstaat er in het in lid 1 bedoelde geval van af het bedrag van de in lid 4 bedoelde schade op een andere lidstaat te verhalen.

Wanneer schade ontstaat bij handelen door personeel van een ondersteunende toezichthouder (zie lid 4), wordt deze alleen vergoed onder de nationale regels van de lidstaat van de ontvangende toezichthouder (lid 5).

- 62.7 Wanneer een gezamenlijke werkzaamheid is gepland en een toezichthoudende autoriteit niet binnen één maand aan de in lid 2, tweede zin, van dit artikel vastgestelde verplichting voldoet, kunnen de andere toezichthoudende autoriteiten een voorlopige maatregel nemen op het grondgebied van de lidstaat waarvoor zij bevoegd zijn overeenkomstig artikel 55. In dat geval wordt geacht dat er overeenkomstig artikel 66, lid 1, dringend moet worden opgetreden en dat dit een dringend advies of een dringend bindend besluit van het Comité vereist overeenkomstig artikel 66, lid 2.

Toezichthouders zijn verplicht met elkaar op verzoek gezamenlijke werkzaamheden te verrichten. Wanneer een toezichthouder niet binnen een maand aan een dergelijk verzoek voldoet, mogen de andere toezichthouders voor hun eigen lidstaat een voorlopige maatregel nemen, zoals een verwerkingsverantwoordelijke een beperking opleggen in een verwerking. Deze maatregel mag maximaal drie maanden geldig zijn en alleen op het eigen grondgebied gelden (artikel 66 lid 1).

AFDELING 2. COHERENTIE

Wanneer toezichthouders niet tot consensus kunnen komen bij gezamenlijk optreden onder de vorige afdeling, dan regelt afdeling 2 hoe men in onderlinge afstemming tot eenvormige beslissingen kan komen, het zogeheten coherentiemechanisme (artikel 63). Het Comité voor gegevensbescherming kan hierbij adviserend optreden (artikel 64) maar uiteindelijk in bepaalde gevallen ook bindend advies (artikel 65) geven.

Artikel 63. Coherentiemechanisme

Teneinde bij te dragen aan de consequente toepassing van deze verordening in de gehele Unie werken de toezichthoudende autoriteiten met elkaar en waar passend samen met de Commissie in het kader van het in deze afdeling uiteengezette coherentiemechanisme.

Om te zorgen dat de AVG in de gehele Unie consequent wordt toegepast, voert dit artikel een coherentiemechanisme in voor samenwerking tussen de toezichthouders. Het coherentiemechanisme houdt in dat toezichthouders met elkaar en met de Commissie samenwerken, met name om te voorkomen dat uiteenlopende besluiten worden genomen over toegestane of verboden verwerkingen.

Toepasselijkheid. Het coherentiemechanisme moet te allen tijde worden toegepast wanneer toezichthouders met elkaar samenwerken of met de Commissie. Gebruik van het mechanisme wordt expliciet vereist bij het opstellen van stan-

daardebepalingen voor verwerkersovereenkomsten (artikel 28 lid 8), het opstellen van lijsten van verwerkingen waarvoor wel dan wel geen DPIA vereist is (artikel 35 lid 6), accreditatie van handhavers van gedragscodes (artikel 41 lid 3), het goedkeuren van contractuele bepalingen voor doorgifte aan derde landen (artikel 46 lid 4), het goedkeuren van bindende bedrijfsvoorschriften (artikel 47 lid 1), het overleg bij bezwaar over een ontwerpbesluit omtrent een grensoverschrijdende verwerking (artikel 60 lid 4)

Meerdere toezichthouders. In landen met meerdere toezichthouders moet de toezichthouder met zitting in het Comité (artikel 68 lid 4) een procedure vaststellen om te zorgen dat zijn collega's zich houden aan het coherentiemechanisme.

Afwijken bij spoed. In spoedgevallen waarbij dringend moet worden opgetreden om de rechten en vrijheden van betrokkenen te beschermen, mag een toezichthouder gemotiveerd afwijken van het coherentiemechanisme om voorlopige maatregelen te nemen die maximaal drie maanden geldig zijn en alleen op het eigen grondgebied gelden (artikel 66 lid 1).

Advies van Comité. Bij de toepassing van het coherentiemechanisme dient het Comité binnen een bepaalde termijn een advies uit te brengen, indien een meerderheid van zijn leden daartoe beslist of indien een betrokken toezichthouder of de Commissie daarom verzoekt (overweging 136).

Onafhankelijkheid Commissie. Het coherentiemechanisme geldt niet in geval van maatregelen die de Commissie kan nemen in de uitoefening van haar overige EU-bevoegdheden (overweging 135).

Voorbeeld. Voorafgaand aan een tweetal boetes uitgedeeld door de Ierse toezichthouder aan Meta op 12 januari 2023, hebben verschillende toezichthouders hun zienswijze gedeeld. Omdat in het geval van beide conceptbeslissingen (de een over Whatsapp, de ander over Instagram en Facebook) tien verschillende toezichthouders substantieel anders oordeelden, was het uiteindelijk aan het Comité om een advies uit te geven, op basis van hun autoriteit tot geschilbeslechting in deze situaties (zie verder artikel 65).

Artikel 64. Advies van het Comité

64.1 Het Comité brengt een advies uit wanneer een bevoegde toezichthoudende autoriteit voornemens is een van onderstaande maatregelen vast te stellen. Hiertoe deelt de bevoegde toezichthoudende autoriteit het Comité het ontwerpbesluit mee indien het:

Het Comité van samenwerkende toezichthouders (zie artikel 68) heeft als belangrijkste taak te zorgen dat de AVG op eenvormige wijze wordt uitgelegd en

gehandhaafd. Wanneer toezichthouders dan ook maatregelen willen nemen die bredere impact hebben, moeten zij het advies van het Comité inwinnen. In principe moet dit advies worden opgevolgd (lid 7), maar als een toezichthouder daar vanaf wil wijken dan is dat mogelijk onder de regels van artikel 64. Voor spoedgevallen is er de spoedprocedure van artikel 65.

64.1(a) de vaststelling beoogt van een lijst van verwerkingen waarvoor de eis inzake een gegevensbeschermingseffectbeoordeling overeenkomstig artikel 35, lid 4, geldt;

Toezichthouders mogen lijsten vaststellen (artikel 35 lid 4) van verwerkingen waarvoor altijd een DPIA (zie artikel 35 lid 1) uitgevoerd moet worden. Zij hebben hierbij het advies nodig van het Comité.

64.1(b) betrekking heeft op de vraag, overeenkomstig artikel 40, lid 7, of een gedragscode of de wijziging of uitbreiding van een gedragscode met deze verordening in overeenstemming is;

Toezichthouders mogen gedragscodes goedkeuren (zie artikel 40 lid 5) waarmee bepaalde branches willen gaan werken. Als de gedragscode verwerkingen in verschillende lidstaten betreft, moet deze voor advies worden voorgelegd aan het Comité (artikel 40 lid 7).

64.1(c) beoogt de eisen inzake accreditatie van een orgaan overeenkomstig artikel 41, lid 3, van een certificeringsorgaan overeenkomstig artikel 43, lid 3, of de criteria voor certificering als bedoeld in artikel 42, lid 5, goed te keuren;

Een gedragscode kan een toezichthoudend orgaan, zoals een geschillencommissie, aanstellen voor de naleving daarvan (artikel 41 lid 1). Zo'n orgaan moet worden geaccrediteerd, en de criteria daarvoor worden door de toezichthouder opgesteld onder advies van het Comité (artikel 41 lid 3). Evenzo kan een certificering van een verwerking of technologie worden verricht door een toezichthouder of door een door hem aangewezen certificeringsorgaan. De criteria voor accreditatie van zo'n certificeringsorgaan worden door de toezichthouder opgesteld onder advies van het Comité (artikel 41 lid 3).

64.1(d) de vaststelling beoogt van de in artikel 46, lid 2, punt d), en artikel 28, lid 8, bedoelde standaardbepalingen inzake gegevensbescherming;

Bij doorgifte van persoonsgegevens naar een niet-adequaat derde land is het mogelijk passende waarborgen te treffen door het gebruiken van zogeheten standaardbepalingen (*model clauses*). Deze kunnen zowel door de Commissie (artikel 46 lid 2 punt c) als door toezichthouders (artikel 46 lid 2 punt d) worden opgesteld. In het laatste geval dient de toezichthouder advies van het Comité in te winnen.

Voor inzet van een verwerker is een verwerkersovereenkomst nodig (artikel 28 lid 3). De toezichthouders mogen daar standaardbepalingen voor opstellen (artikel 28 lid 8). Ook hiervoor dient de toezichthouder advies van het Comité in te winnen.

64.1(e) de toestemming beoogt voor de in artikel 46, lid 3, punt a), bedoelde contractbepalingen; of

Verwerkingsverantwoordelijken of verwerkers kunnen eigen contractuele bepalingen opstellen voor gebruik met ontvangers in derde landen (artikel 46 lid 3 punt a). Dergelijke bepalingen moeten vooraf zijn goedgekeurd door de toezichthouder (artikel 57 lid 1 punt r), en die heeft dan weer het advies nodig van het Comité om die goedkeuring te mogen geven.

64.1(f) de goedkeuring beoogt van bindende bedrijfsvoorschriften in de zin van artikel 47.

Specifiek binnen een concern of groep van ondernemingen is het mogelijk passende waarborgen voor doorgifte te realiseren middels zogeheten bindende bedrijfsvoorschriften (artikel 47). Deze dienen te worden goedgekeurd door de voor het concern bevoegde toezichthouder, en deze heeft daarbij advies van het Comité nodig.

64.2 Een toezichthoudende autoriteit, de voorzitter van het Comité of de Commissie kunnen elk verzoeken dat aangelegenheden van algemene strekking of met rechtsgevolgen in meer dan één lidstaat worden onderzocht door het Comité teneinde advies te verkrijgen, met name wanneer een bevoegde toezichthoudende autoriteit haar verplichtingen tot wederzijdse bijstand overeenkomstig artikel 61, of tot gezamenlijke werkzaamheden overeenkomstig artikel 62, niet nakomt.

Ook bij andere aangelegenheden dan genoemd in lid 1 kan het Comité advies verstrekken. Het moet dan gaan om aangelegenheden van algemene strekking of met rechtsgevolgen in meerdere lidstaten, geen bagatels of lokale aangelegenheden dus. Het meest voorkomende geval zal zijn wanneer een toezichthouder niet meewerkt aan de eis tot wederzijdse bijstand (artikel 61) of samenwerking en informatie-uitwisseling (artikel 62).

64.3 Het Comité brengt in de in de leden 1 en 2 bedoelde gevallen een advies uit over de aan het Comité voorgelegde aangelegenheid, mits het daarover niet eerder advies heeft uitgebracht. Dat advies wordt binnen acht weken vastgesteld met gewone meerderheid van de leden van het Comité. Die termijn kan met zes weken worden verlengd, rekening houdend met de complexiteit van de aangelegenheid. Met het in lid 1 bedoelde ontwerpbesluit, dat overeenkomstig lid 5 onder de leden van het Comité wordt verspreid, wordt een lid dat niet binnen een redelijke, door de voorzitter aangegeven termijn bezwaar heeft aangetekend, geacht in te stemmen.

Het Comité moet binnen acht weken het advies uitbrengen. Bij complexe zaken mag deze termijn met zes weken worden verlengd. Tot dit advies is uitgebracht, mag de toezichthouder geen besluit over de kwestie nemen (lid 6). Het advies wordt aangenomen met gewone meerderheid van stemmen, waarbij stilzwijgen geldt als instemmen.

64.4 De toezichthoudende autoriteiten en de Commissie delen onverwijld langs elektronische weg door middel van een standaardformulier het Comité alle relevante informatie mee, waaronder naargelang het geval een samenvatting van de feiten, het ontwerpbesluit, de redenen waarom een dergelijke maatregel moet worden genomen en de standpunten van andere betrokken toezichthoudende autoriteiten.

Communicatie met het Comité gebeurt zo veel mogelijk elektronisch en door gebruikmaking van standaardformulieren.

64.5 De voorzitter van het Comité stelt onverwijld langs elektronische weg:

64.5(a) de leden van het Comité en de Commissie door middel van een standaardformulier in kennis van alle relevante informatie die het Comité heeft ontvangen. Het secretariaat van het Comité verstrekt indien nodig vertalingen van relevante informatie; en

64.5(b) de, naargelang het geval, in de leden 1 en 2 bedoelde toezichthoudende autoriteit en de Commissie in kennis van het advies en maakt dat advies bekend.

De leden van het Comité en de Commissie moeten zo veel mogelijk op de hoogte worden gehouden van alle relevante informatie omtrent de adviesprocedure. Dit gebeurt zo nodig met vertalingen.

- 64.6 De bevoegde toezichthoudende autoriteit stelt haar in lid 1 bedoelde ontwerpbesluit niet vast binnen de in lid 3 bedoelde termijn.

Zo lang het Comité nog geen advies heeft gegeven, dienen de betrokken toezichthouders te wachten met het nemen van hun besluit. In spoedgevallen is afwijking hiervan mogelijk onder de regels van artikel 66.

- 64.7 De in lid 1 bedoelde bevoegde toezichthoudende autoriteit houdt maximaal rekening met het advies van het Comité en deelt de voorzitter van het Comité binnen twee weken na ontvangst van het advies langs elektronische weg door middel van een standaardformulier mee of zij haar ontwerpbesluit zal handhaven dan wel wijzigen alsmede, in voorkomend geval het gewijzigde ontwerpbesluit.

De toezichthouder in kwestie moet binnen twee weken aan de voorzitter van het Comité aangeven of hij van plan is het advies op te volgen. Zo ja, dan moeten de wijzigingen aan het ontwerpbesluit worden overlegd. Als hij dit niet van plan is, dan moet hij de redenen daarvoor opgeven (lid 8). Het Comité neemt dan een bindend besluit (artikel 65 lid 1 punt c). De reactie van de toezichthouder moet middels een elektronisch standaardformulier de informatie aanleveren.

- 64.8 Wanneer de in lid 1 bedoelde bevoegde toezichthoudende autoriteit de voorzitter van het Comité binnen de in lid 7 van dit artikel bedoelde termijn, onder opgave van de redenen, kennis geeft van haar voornemen het advies van het Comité geheel of gedeeltelijk niet op te volgen, is artikel 65, lid 1, van toepassing.

Wanneer een toezichthouder het advies uit lid 1 niet wenst op te volgen, meldt hij dit aan de voorzitter van het Comité en wel binnen twee weken na ontvangst van het advies (lid 7). In dat geval zal het Comité een bindend besluit vaststellen (artikel 65 lid 1 punt c).

Artikel 65. Geschillenbeslechting door het Comité

- 65.1 Om te zorgen voor de correcte en consequente toepassing van deze verordening in individuele gevallen, stelt het Comité een bindend besluit vast in de volgende gevallen:

Het Comité heeft in drie gevallen de bevoegdheid een bindend besluit te nemen wanneer toezichthouders er onderling niet uitkomen. Zij moet dit besluit binnen een maand nemen met tweederdemeerderheid (lid 2) met een escalatieprocedure als dat niet lukt (lid 3). De toezichthouders moeten hun besluitvorming opschorten gedurende deze tijd (lid 4) maar er is een spoedprocedure (artikel 66). Het besluit wordt door de voorzitter gecommuniceerd (lid 5).

65.1(a) wanneer in een geval als bedoeld in artikel 60, lid 4, een betrokken toezichthoudende autoriteit een relevant en gemotiveerd bezwaar heeft ingediend tegen een ontwerpbesluit van de leidende toezichthoudende autoriteit en de leidende toezichthoudende autoriteit heeft het bezwaar niet gevolgd of heeft het bezwaar afgewezen als zijnde irrelevant of ongemotiveerd. Het bindend besluit heeft betrekking op alle aangelegenheden die onderwerp van het relevante en gemotiveerde bezwaar zijn, en met name op de vraag of inbreuk op de onderhavige verordening wordt gemaakt;

Het eerste geval waarin het Comité de knoop mag doorhakken, is wanneer meerdere toezichthouders onder leiding van één van hen over een grensoverschrijdende verwerking moet besluiten (artikel 60). Iedere toezichthouder kan een relevant en gemotiveerd bezwaar (zie artikel 4 definitie 24) opwerpen, waar de leidende toezichthouder in beginsel in mee moet gaan (artikel 60 lid 5). Doet deze dat niet, dan volgt in eerste instantie de onderlinge samenwerking uit het coherentiemechanisme (artikel 63). Heeft deze geen effect, dan volgt de besluitprocedure van dit artikel.

65.1(b) wanneer er verschillend wordt geoordeeld over de vraag welke betrokken toezichthoudende autoriteit bevoegd is voor de hoofdvestiging;

Het tweede geval waarin het Comité beslist, is wanneer verschillende toezichthouders zich bevoegd achten voor de hoofdvestiging van een verwerkingsverantwoordelijke of verwerker. Dit criterium bepaalt namelijk welke toezichthouder de leiding heeft (artikel 56 lid 1) bij een grensoverschrijdende verwerking. Men kan bijvoorbeeld van mening verschillen waar de feitelijke beslismacht binnen een concern ligt. Zie over de hoofdvestiging artikel 4 definitie 16.

65.1(c) wanneer een bevoegde toezichthoudende autoriteit in de in artikel 64, lid 1, genoemde gevallen het Comité niet om advies vraagt, of het krachtens artikel 64 uitgebrachte advies van het Comité niet volgt. In dat geval kan elke betrokken toezichthoudende autoriteit of de Commissie de aangelegenheid meedelen aan het Comité.

Het derde geval waarin het Comité beslist, is wanneer een bevoegde toezichthouder zich niet kan vinden in het advies van het Comité (artikel 64 lid 1) inzake criteria voor een verplichte DPIA, goedkeuring van een gedragscode, accreditatie van een geschillencommissie bij een gedragscode of een certificeringsorgaan, of goedkeuring van standaard contractuele bepalingen of bindende bedrijfsvoorwaarden. Iedere toezichthouder kan hierover aan de bel trekken bij het Comité.

- 65.2 Het in lid 1 bedoelde besluit wordt binnen één maand na de verwijzing van de aangelegenheid vastgesteld met een tweederdemeerderheid van de leden van het Comité. Deze termijn kan wegens de complexiteit van de aangelegenheid met één maand worden verlengd. Het in lid 1 bedoelde besluit wordt met redenen omkleed en gericht tot de leidende toezichthoudende autoriteit en alle betrokken toezichthoudende autoriteiten, en is bindend.

Het Comité dient binnen een maand een besluit te nemen in de kwesties genoemd in lid 1, en wel met een tweederdemeerderheid van de stemmen. In complexe gevallen mag de termijn naar twee maanden worden verlengd. Het aldus genomen besluit moet worden gemotiveerd en is bindend op de betrokken toezichthouders. Komt men er niet uit, dan volgt de procedure van lid 3. Het besluit wordt conform lid 5 aan de toezichthouders bekendgemaakt.

- 65.3 Indien het Comité niet binnen de in lid 2 genoemde termijn een besluit heeft kunnen vaststellen, stelt het zijn besluit binnen twee weken na het verstrijken van de in lid 2 bedoelde tweede maand vast, met een gewone meerderheid van zijn leden. Bij staking van stemmen onder de leden van het Comité is de stem van de voorzitter beslissend.

Wanneer het Comité er niet uit komt, of geen tweederdemeerderheid kan vinden, vindt een escalatie plaats waarbij men binnen twee weken na de verlengde termijn van twee maanden een besluit moet nemen. Dit besluit wordt met gewone meerderheid genomen en de voorzitter (artikel 73) hakt de knoop door bij het staken der stemmen.

- 65.4 De betrokken toezichthoudende autoriteiten stellen tijdens de in de leden 2 en 3 bedoelde termijn geen besluit over de overeenkomstig lid 1 aan het Comité voorgelegde aangelegenheid vast.

Zo lang het Comité nog geen besluit heeft genomen, dienen de betrokken toezichthouders te wachten met het nemen van hun besluit. In spoedgevallen is afwijking hiervan mogelijk onder de regels van artikel 66.

- 65.5 De voorzitter van het Comité brengt het in lid 1 bedoelde besluit onverwijld ter kennis van de betrokken toezichthoudende autoriteiten. Hij brengt de Commissie daarvan op de hoogte. Het besluit wordt onverwijld bekendgemaakt op de website van het Comité nadat de toezichthoudende autoriteit het in lid 6 bedoelde definitieve besluit ter kennis heeft gebracht.

Wanneer het besluit is genomen, wordt het gemeld door de voorzitter aan de betrokken toezichthouders, en aan de Commissie. Het besluit van het Comité wordt op haar website gepubliceerd, uiteraard pas nadat de bevoegde toezichthouder het onderliggende besluit over de verwerking heeft gemeld aan de betreffende verwerkingsverantwoordelijke of verwerker.

65.6 De leidende toezichthoudende autoriteit of, in voorkomend geval, de toezichthoudende autoriteit waarbij de klacht is ingediend, stelt onverwijld en uiterlijk binnen één maand na de kennisgeving door het Comité een definitief besluit vast op basis van het in lid 1 van dit artikel bedoelde besluit. De leidende toezichthoudende autoriteit of, in voorkomend geval, de toezichthoudende autoriteit waarbij de klacht is ingediend, deelt het Comité de datum mee waarop haar definitieve besluit ter kennis wordt gebracht van respectievelijk de verwerkingsverantwoordelijke of de verwerker en van de betrokkene. Het definitieve besluit van de betrokken toezichthoudende autoriteiten wordt vastgesteld overeenkomstig artikel [60], leden 7, 8 en 9. Het definitieve besluit verwijst naar het in lid 1 van dit artikel bedoelde besluit en geeft aan dat genoemd besluit overeenkomstig lid 5 van dit artikel zal worden bekendgemaakt op de website van het Comité. Het in lid 1 van dit artikel bedoelde besluit wordt aan het definitieve besluit gehecht.

Uiterlijk één maand na de in lid 5 bedoelde kennisgeving stelt de leidende toezichthouder een besluit vast. De definitieve datum waarop dit gebeurt, dient aan het Comité kenbaar gemaakt te worden. Het Comité zal dit besluit op haar website bekendmaken. Het oorspronkelijke en door het Comité vastgestelde besluit worden aan elkaar gehecht.

Artikel 60a. Dit lid 6 verwijst naar een artikel 60a dat niet bestaat. Bedoeld wordt artikel 60.

Artikel 66. Spoedprocedure

66.1 In buitengewone omstandigheden kan een betrokken toezichthoudende autoriteit, wanneer zij van mening is dat er dringend moet worden opgetreden om de rechten en vrijheden van betrokkenen te beschermen, in afwijking van het in de artikelen 63, 64 en 65 bedoelde coherentiemechanisme of van de in artikel 60 bedoelde procedure, onverwijld voorlopige maatregelen met een bepaalde geldigheidsduur van ten hoogste drie maanden nemen die beogen rechtsgevolgen in het leven te roepen op het eigen grondgebied. De toezichthoudende autoriteit deelt die maatregelen met opgave van de redenen onverwijld mee aan de andere betrokken toezichthoudende autoriteiten, het Comité en de Commissie.

Het gekozen stelsel van samenwerkende toezichthouders brengt naar zijn aard mee dat besluitvorming lang kan duren. Op grond van artikel 63 (met procedures in artikelen 64 en 65) moeten toezichthouders met elkaar en met de Commissie samenwerken om uiteenlopende beslissingen te voorkomen, en op grond van artikel 60 moeten toezichthouders met elkaar samenwerken teneinde tot een consensus proberen te komen. In spoedgevallen is het toegestaan hiervan af te wijken.

Buitengewone omstandigheden. Van een spoedgeval is sprake bij buitengewone omstandigheden waarbij grondrechten van betrokkenen dringend moeten worden beschermd. Een dergelijke situatie zou kunnen zijn dat een grensoverschrijdende verwerking op grove schaal de AVG schendt, of dat schokkende onthullingen over een derde land haar geschiktheid voor doorgifte ernstig in twijfel doet trekken. Het niet binnen één maand afhandelen van een verzoek door een toezichthouder wordt aangemerkt als een spoedgeval (artikel 61 lid 8).

Voorbeeld. Voorafgaand aan een tweetal boetes uitgedeeld door de Ierse toezichthouder aan Meta op 12 januari 2023, hebben verschillende toezichthouders hun zienswijze gedeeld en was het uiteindelijk aan het Comité om een advies uit te geven, op basis van hun autoriteit tot geschilbeslechting in deze situaties (zie verder artikel 65 lid 1 punt a). Dit zorgde voor een aanzienlijke verhoging van het boetebedrag, en een ingrijpend andere interpretatie van de AVG.

Voorlopige maatregelen. De toezichthouder mag uitsluitend voorlopige maatregelen opleggen ter bescherming van betrokkenen in het kader van een spoedprocedure. Meest voor de hand ligt het tijdelijk doen beperken (artikel 58 lid 2 punt f) van de verwerking en het opschorten van doorgifte aan een derde land (artikel 58 lid 2 punt j).

Geldigheid. Een voorlopige maatregel mag ten hoogste drie maanden geldig zijn en moet qua werkingssfeer beperkt zijn tot de lidstaat waar de toezichthouder bevoegd voor is.

- 66.2 Wanneer een toezichthoudende autoriteit overeenkomstig lid 1 een maatregel heeft genomen en van mening is dat er dringend definitieve maatregelen moeten worden genomen, kan zij het Comité met opgave van redenen om een dringend advies of een dringend bindend besluit verzoeken.

Het opleggen van definitieve maatregelen kan alleen via de gewone uitoefening van haar bevoegdheden (artikel 58). Wanneer spoed vereist is, kan de toezichthouder het daarvoor benodigde advies (artikel 64) of bindend besluit (artikel 65) van het Comité met spoed laten opstellen.

- 66.3 Een toezichthoudende autoriteit kan het Comité met opgave van redenen, waaronder de redenen waarom er dringend moet worden opgetreden, om een dringend advies of een dringend bindend besluit verzoeken wanneer de bevoegde toezichthoudende autoriteit geen passende maatregel heeft genomen in een situatie waarin er dringend moet worden opgetreden, teneinde de rechten en vrijheden van betrokkenen te beschermen.

Ook andere toezichthouders kunnen in spoedgevallen om een advies (artikel 64) of bindend besluit (artikel 65) van het Comité verzoeken. Zij moeten dit doen onder opgaaf van redenen, met name waarom spoed vereist is.

66.4 In afwijking van artikel 64, lid 3, en van artikel 65, lid 2, wordt een als in de leden 2 en 3 bedoeld dringend advies of dringend bindend besluit binnen twee weken met gewone meerderheid van de leden van het Comité vastgesteld.

Adviezen en besluiten van het Comité zoals hier bedoeld worden in beginsel met tweederdemeerderheid genomen (artikel 64 lid 3 voor adviezen en artikel 65 lid 2 voor besluiten). In spoedgevallen kan met gewone meerderheid worden besloten.

Artikel 67. Uitwisseling van informatie

De Commissie kan uitvoeringshandelingen van algemene aard vaststellen om de regelingen voor de elektronische uitwisseling van informatie tussen toezichthoudende autoriteiten onderling en tussen toezichthoudende autoriteiten en het Comité, met name het in artikel 64 bedoelde standaardformulier, vast te leggen. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure.

Teneinde uitwisseling van informatie tussen toezichthouders, en tussen toezichthouder en het Comité (artikel 68), te vergemakkelijken, kan een gestandaardiseerde wijze van elektronische uitwisseling worden ingevoerd. In het bijzonder geldt dit bij adviezen van het Comité, dat (artikel 64 lid 4) via een elektronisch standaardformulier alle daarvoor relevante informatie moet ontvangen.

Vaststellingsprocedure. De Commissie maakt ter vaststelling van een elektronische uitwisselingsregeling of een standaardformulier een ontwerpregeling en legt dat voor aan het artikel 93-comité. Dat comité beslist vervolgens met meerderheid van stemmen (artikel 93 lid 2). Indien het advies positief is, wordt de regeling ingevoerd.

Standaardformulieren. De AVG roept specifiek op tot het werken met standaardformulieren bij de samenwerking met een leidende toezichthouder (artikel 60 lid 12), het verstrekken van informatie en bijstand (artikel 61 lid 6) en het verstrekken van informatie voor een advies van het Comité (artikel 64 lid 4).

AFDELING 3. EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING

In deze afdeling wordt het Europees Comité voor gegevensbescherming ("het Comité") als een onafhankelijk orgaan van de Unie opgericht (artikel 68). Haar takenpakket (artikel 70) is het afstemmen van de toezichthouderspraktijk en adviseren aan alle partijen. Artikelen 71-75 regelen procedurele aspecten van het Comité en haar samenstelling.

Artikel 68. Europees Comité voor gegevensbescherming

68.1 Het Europees Comité voor gegevensbescherming (het “Comité”) wordt ingesteld als orgaan van de Unie en heeft rechtspersoonlijkheid.

Teneinde een consequente toepassing van de AVG te bevorderen, is een Europees Comité voor gegevensbescherming als een onafhankelijk orgaan van de EU opgericht. Het Comité vervangt de Artikel 29-werkgroep en heeft rechtspersoonlijkheid. Het Comité is onafhankelijk (artikel 69) en heeft adviserende taken (artikel 70) en rapporteert jaarlijks (artikel 71) middels een jaarverslag. Haar documenten zijn openbaar (artikel 76).

Samenstelling en organisatie. Het Comité kent voor elke lidstaat één vertegenwoordiger alsook een vertegenwoordiger van de Europese Toezichthouder voor gegevensbescherming (de Europese Toezichthouder, lid 3). Deze leden kiezen een voorzitter en twee vicevoorzitters (artikel 73). Het Comité maakt haar eigen reglement van orde (artikel 74) en wordt bij haar dagelijkse werkzaamheden ondersteund door een secretariaat (artikel 75).

Artikel 29-Werkgroep. Het Comité is de opvolger van de Artikel 29-Werkgroep van samenwerkende toezichthouders die onder de Richtlijn adviezen en richtsnoeren uitgaf (artikel 94 lid 2).

Artikel 93-comité. Het Comité is niet te verwarren met het artikel 93-comité dat de Commissie adviseert ten aanzien van gedelegeerde handelingen zoals het vaststellen van modelteksten, certificeringsnormen en informatie-uitwisselingsprocedures (zie artikel 93).

68.2 Het Comité wordt vertegenwoordigd door zijn voorzitter.

Het Comité dient door zijn voorzitter te worden vertegenwoordigd. Deze wordt met gewone meerderheid uit haar leden gekozen (artikel 73 lid 1) en is eenmaal herkiesbaar (artikel 73 lid 2). De voorzitter heeft de beslissende stem bij staken der stemmen in het Comité (artikel 65 lid 3) maar heeft geen bijzondere bevoegdheden.

68.3 Het Comité bestaat uit de voorzitter van één toezichthoudende autoriteit per lidstaat en de Europese Toezichthouder voor gegevensbescherming, of hun respectieve vertegenwoordigers.

Het Comité wordt samengesteld uit de voorzitters van elke toezichthouder, alsook de Europese Toezichthouder voor gegevensbescherming (zie artikel 51). Wanneer een lidstaat meerdere toezichthouders heeft (zie artikel 51 lid 3), moet die lidstaat één daarvan aanwijzen om in het Comité zitting te hebben. De Com-

missie mag een vertegenwoordiger bijeenkomsten laten bijwonen (lid 5) maar is geen lid van het Comité.

- 68.4 Wanneer in een lidstaat meer dan één toezichthoudende autoriteit belast is met het toezicht op de toepassing van de bepalingen krachtens deze verordening, wordt overeenkomstig het recht van die lidstaat een gezamenlijke vertegenwoordiger aangewezen.

Een lidstaat kan meerdere toezichthouders hebben (zie artikel 51 lid 3), zoals in Duitsland het geval is. In dat geval moet die lidstaat één daarvan aanwijzen om in het Comité zitting te hebben. Hiermee wordt geborgd dat elke lidstaat één stem heeft bij besluitvorming.

- 68.5 De Commissie heeft het recht deel te nemen aan de activiteiten en, zonder stemrecht, aan de bijeenkomsten van het Comité. De Commissie wijst een vertegenwoordiger aan. De voorzitter van het Comité stelt de Commissie in kennis van de activiteiten van het Comité.

Het Comité is onafhankelijk (artikel 69) en de Commissie heeft dus geen zitting of stemrecht in het Comité. Wel mag de Commissie als observator deelnemen aan activiteiten en bijeenkomsten van het Comité, en wordt zij door de voorzitter geïnformeerd over de activiteiten van het Comité.

- 68.6 In de in artikel 65 bedoelde gevallen heeft de Europese Toezichthouder voor gegevensbescherming uitsluitend stemrecht bij besluiten over op de instellingen, organen en instanties van de Unie toepasselijke beginselen en regels die inhoudelijk met die van de onderhavige verordening overeenstemmen.

Wanneer toezichthouders onderling van inzicht verschillen over te nemen besluiten, zoals welk van hen bevoegd is of welk besluit moet worden vastgesteld bij een grensoverschrijdende verwerking, kan het Comité een bindend besluit dienaangaande nemen om de knoop door te hakken (artikel 65). De Europese Toezichthouder heeft in die gevallen geen stemrecht, tenzij het gaat over besluiten over regels uit Verordening 45/2001 (welke de EDPS als toezichthouder aanmerkt).

Artikel 69. Onafhankelijkheid

- 69.1 Het Comité treedt bij de uitvoering van zijn taken of de uitoefening van zijn bevoegdheden overeenkomstig de artikelen 70 en 71 onafhankelijk op.

Als orgaan van de EU en met name als orgaan boven de samenwerkende toezichthouders dient het Comité uiteraard volstrekt onafhankelijk te opereren bij uitoefening van haar adviserende taken (artikel 70) en verzorging van rapportages (artikel 71).

- 69.2 Onverminderd verzoeken van de Commissie als bedoeld in artikel 70, leden 1 en 2, vraagt noch aanvaardt het Comité bij de uitvoering van zijn taken of de uitoefening van zijn bevoegdheden instructies van wie dan ook.

Deel van de onafhankelijkheid van het Comité is dat anderen haar geen instructies kunnen geven. Hoewel de Commissie wel verzoeken kan doen om advies (artikel 70 lid 1 punt b), al dan niet met spoed (artikel 70 lid 2), is zo'n verzoek niet te zien als een instructie. In theorie kan het Comité weigeren het advies uit te brengen, hoewel dit in de praktijk natuurlijk niet te verwachten is.

Artikel 70. Taken van het Comité

- 70.1 Het Comité zorgt ervoor dat deze verordening consequent wordt toegepast. Daartoe doet het Comité op eigen initiatief of, waar passend, op verzoek van de Commissie met name het volgende:

Het Comité wordt ingesteld als een onafhankelijke toezichthouder op de toezichthouders. Zij heeft geen bevoegdheden naar verwerkingsverantwoordelijken of verwerkers toe. Haar taak is adviseren, bemiddelen, coördineren en uitwerken van informatieve richtsnoeren.

- 70.1(a) toezien op en zorgen voor de juiste toepassing van deze verordening in de in de artikelen 64 en 65 bedoelde gevallen, onverminderd de taken van de nationale toezichthoudende autoriteiten;

Hoewel de toezichthouders onafhankelijk opereren bij hun besluitvorming, heeft het Comité een coördinerende taak. Bij algemene besluiten, zoals het opstellen van lijsten van verwerkingen waarvoor een DPIA verplicht is of de vaststelling van standaardbepalingen inzake gegevensbescherming, is het inwinnen van advies van het Comité verplicht (artikel 64). Bij geschillen tussen toezichthouders, zoals wie bevoegd is of welk besluit moet worden vastgesteld bij een grensoverschrijdende verwerking, heeft het Comité de bevoegdheid een bindend besluit vast te stellen (artikel 65).

- 70.1(b) adviseren van de Commissie over aangelegenheden in verband met de bescherming van persoonsgegevens in de Unie, waaronder alle voorgestelde wijzigingen van deze verordening;

Het Comité heeft een adviserende taak bij alle aangelegenheden betreffende persoonsgegevens en hun bescherming. Dit omvat onder meer het wijzigen van de AVG, maar ook andere verordeningen en richtlijnen die regelingen omtrent persoonsgegevens kennen.

70.1(c) adviseren van de Commissie over het mechanisme en de procedures voor de uitwisseling van informatie wat betreft bindende bedrijfsvoorschriften tussen verwerkingsverantwoordelijken, verwerkers, en toezichthoudende autoriteiten;

Wanneer een land of organisatie niet als adequaat is aangemerkt onder artikel 45, is doorgifte alleen toegestaan wanneer sprake is van passende waarborgen. Specifiek binnen een concern of groep van ondernemingen is het mogelijk dergelijke waarborgen te realiseren middels zogeheten bindende bedrijfsvoorschriften (artikel 47 lid 1). Bij het uitwerken van mechanismes en procedures in dit verband moet de Commissie advies inwinnen bij het Comité.

70.1(d) uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken inzake procedures voor het wisselen van links, kopieën of reproducties van persoonsgegevens uit algemeen beschikbare communicatiediensten als bedoeld in artikel 17, lid 2;

Deel van het recht van gegevenswissing (artikel 17) is de plicht voor een verwerkingsverantwoordelijke die de te wisselen persoonsgegevens openbaar heeft gemaakt, andere verwerkingsverantwoordelijken te informeren over de wissing (artikel 17 lid 2). Deze anderen dienen dan op hun beurt de gegevenswissing te overwegen. Ter assistentie van de markt kan het Comité richtsnoeren, aanbevelingen of *best practices* formuleren over hoe dit wisselen uit te voeren in de context van (met name online) communicatiediensten zoals websites.

70.1(e) onderzoeken, op eigen initiatief of op verzoek van een van zijn leden dan wel op verzoek van de Commissie, van kwesties die betrekking hebben op de toepassing van deze verordening, en uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken om te bevorderen dat deze verordening consequent wordt toegepast;

Om te stimuleren dat de AVG consequent wordt toegepast (zie ook artikel 63) kan het Comité richtsnoeren, aanbevelingen of *best practices* publiceren over hoe dit het beste kan gebeuren. Dit kan over elk onderwerp van de AVG; punten f tot en met m hieronder noemen specifieke onderwerpen waar dergelijke publicaties met name wenselijk zijn.

70.1(f) uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken in overeenstemming met punt e) van dit lid ter verdere specificatie van de criteria en de voorwaarden voor besluiten op basis van profilering krachtens artikel 22, lid 2;

De in het vorige punt genoemde richtsnoeren, aanbevelingen of *best practices* kunnen nader worden uitgewerkt ten aanzien van het onderwerp profilering (artikel 4 definitie 4), met name wanneer profilering wordt ingezet voor geautomatiseerde besluitvorming (artikel 22) en de situaties waarin dat toegestaan is (artikel 22 lid 2).

70.1(g) uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken in overeenstemming met punt e) van dit lid ter vaststelling van inbreuken in verband met persoonsgegevens alsmede van de in artikel 33, leden 1 en 2, bedoelde onredelijke vertraging, en voor de bijzondere omstandigheden waarin een verwerkingsverantwoordelijke of een verwerker verplicht is de inbreuk in verband met persoonsgegevens te melden;

De richtsnoeren, aanbevelingen of *best practices* uit punt e) kunnen tevens nader worden uitgewerkt over het onderwerp datalekken (artikel 33), zoals wat melden zonder onredelijke vertraging betekent en hoe de norm voor wanneer datalekken moeten worden gemeld nader moet worden ingevuld. Zie ook punt h hieronder.

70.1(h) uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken in overeenstemming met punt e) van dit lid ten aanzien van de omstandigheden waarin een inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen, als bedoeld in artikel 34, lid 1;

De richtsnoeren, aanbevelingen of *best practices* uit punt e) kunnen wat betreft datalekken (punt g hierboven) ook worden opgesteld ten aanzien van het mededelen van datalekken aan betrokkenen (artikel 34).

70.1(i) uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken in overeenstemming met punt e) van dit lid ter verdere specificatie van de criteria en de eisen voor doorgiften van persoonsgegevens op basis van bindende bedrijfsvoorschriften voor verwerkingsverantwoordelijken en bindende bedrijfsvoorschriften voor verwerkers, alsmede op basis van verdere noodzakelijke eisen om de bescherming van persoonsgegevens van de betrokkenen in kwestie te garanderen, als bedoeld in artikel 47;

Het Comité kan richtsnoeren, aanbevelingen of *best practices* uitvaardigen over de bindende bedrijfsvoorschriften (artikel 47) waaronder een concern persoonsgegevens mag doorgeven binnen haar organisatie naar onderdelen buiten de Europese Unie.

70.1(j) uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken in overeenstemming met punt e) van dit lid ter verdere specificatie van de criteria en de eisen voor de doorgiften van persoonsgegevens op grond van artikel 49, lid 1;

Het Comité kan richtsnoeren, aanbevelingen of *best practices* uitvaardigen over de gronden waarop persoonsgegevens mogen worden doorgegeven (artikel 49) als het land niet als adequaat is aangemerkt (artikel 45 lid 3) en er ook geen passende waarborgen (artikel 46) of bindende bedrijfsvoorschriften (artikel 47) aanwezig zijn.

70.1(k) opstellen van richtsnoeren voor toezichthoudende autoriteiten betreffende de toepassing van de in artikel 58, leden 1, 2 en 3, bedoelde maatregelen en betreffende de vaststelling van administratieve geldboeten overeenkomstig artikel 83;

Het Comité kan richtsnoeren, aanbevelingen of *best practices* uitvaardigen ten aanzien van de bevoegdheden van de toezichthouder (artikel 58), zowel de onderzoeksbevoegdheden (artikel 58 lid 1), als de corrigerende bevoegdheden (artikel 58 lid 2) en adviserende bevoegdheden (artikel 58 lid 3). Ook kunnen deze worden uitgevaardigd over hoe de administratieve boetes (artikel 83) worden opgebouwd, bijvoorbeeld welke onder- of bovengrenzen worden gehanteerd voor categorieën overtredingen of hoe de diverse boetefactoren (artikel 83 lid 2) moeten worden toegepast).

70.1(l) evalueren van de praktische toepassing van de richtsnoeren, aanbevelingen en beste praktijken;

Naast het uitvaardigen van richtsnoeren, aanbevelingen of *best practices* dient het Comité deze ook te evalueren, in ieder geval de algemene richtsnoeren (punt e) en die betreffende profilering (punt f).

70.1(m) uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken in overeenstemming met punt e) van dit lid, ter vaststelling van gemeenschappelijke procedures waarmee natuurlijke personen inbreuken op deze verordening kunnen melden, als bedoeld in artikel 56, lid 2;

Het Comité kan richtsnoeren, aanbevelingen of *best practices* uitvaardigen over hoe burgers schendingen van de AVG kunnen melden aan een toezichthouder. Het punt verwijst naar artikel 54 maar bedoeld wordt artikel 56 lid 2 dat over klachten van betrokkenen gaat. Artikel 54 lid 2 regelt de geheimhoudingsplicht voor leden van toezichthouders.

70.1(n) bevorderen van het opstellen van gedragscodes en het invoeren van certificeringsmechanismen voor gegevensbescherming en gegevensbeschermingszegels en -merktekens overeenkomstig de artikelen 40 en 42;

Een branche of sector kan de eisen uit de AVG vertalen naar specifieke regels en deze als gedragscode invoeren (artikel 40). Tevens kunnen certificeringsmechanismen worden ontwikkeld vanuit de markt ter ondersteuning van bewijs dat een verwerkingsverantwoordelijke of verwerker voldoet aan de AVG (artikel 42). Het Comité heeft hierbij een stimulerende taak.

70.1(o) goedkeuren van de criteria voor certificering overeenkomstig artikel 42, lid 5, en houden van een openbaar register van certificeringsmechanismen en van gegevensbeschermingszegels en -merktekens overeenkomstig artikel 42, lid 8, en van de geaccrediteerde verwerkingsverantwoordelijken of verwerkers die in derde landen zijn gevestigd, overeenkomstig artikel 42, lid 7;

Certificeringsmechanismen dienen als ondersteuning van bewijs dat een verwerkingsverantwoordelijke of verwerker voldoet aan met name de technische eisen van gegevensbescherming (artikel 42). Certificeringsmechanismen vereisen keuring en bij invoering van het mechanisme kan daartoe een bevoegd orgaan worden aangewezen (artikel 42 lid 5). Deze organen worden geaccrediteerd door de bevoegde toezichthouder of een apart accreditatieorgaan (artikel 43 lid 1), waarbij het Comité krachtens dit punt o een ondersteunende taak heeft. Tevens neemt het Comité de organen en goedgekeurde mechanismen op in een openbaar register (artikel 43 lid 6), net als gecertificeerde verwerkingsverantwoordelijken en verwerkers in derde landen (artikel 42 lid 7).

70.1(p) goedkeuren van de in artikel 43, lid 3, bedoelde eisen met het oog op de accreditatie van certificeringsorganen bedoeld in artikel 43;

Ten behoeve van certificering van mechanismen voor gegevensbescherming worden certificeringsorganen ingesteld (artikel 43). Deze organen moeten aan nader te stellen criteria voldoen (artikel 42 lid 5) en deze criteria worden gespecificeerd door het Comité (artikel 43 lid 3).

70.1(q) uitbrengen van een advies ten behoeve van de Commissie over de in artikel 43, lid 8, bedoelde certificeringseisen;

Onder artikel 43 lid 8 kan de Commissie nadere eisen stellen aan dergelijke certificeringsmechanismen. Hierbij is advies van het Comité nodig.

70.1(r) uitbrengen van een advies ten behoeve van de Commissie over de in artikel 12, lid 7, bedoelde icoontjes;

De verwerkingsverantwoordelijke dient informatie over haar verwerking te verstrekken in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal (artikel 12 lid 1). Lid 7 staat toe dat hierbij gebruik wordt gemaakt van gestandaardiseerde iconen om de herkenbaarheid van verwerkingshandelingen te vergroten. De Commissie is bevoegd (artikel 12 lid 8) om deze iconen vast te stellen, op advies van het Comité.

70.I(s) uitbrengen aan de Commissie van een advies om haar in staat te stellen te beoordelen of het beschermingsniveau in een derde land of een internationale organisatie adequaat is, en om te beoordelen of een derde land, een gebied of één of meerdere nader bepaalde sectoren in dat derde land, of een internationale organisatie geen passend beschermingsniveau meer garandeert. Daartoe verstrekt de Commissie het Comité alle nodige documentatie, met inbegrip van correspondentie met de overheid van het derde land, ten aanzien van derde land, gebied of nader bepaalde sector of met de internationale organisatie.

Wanneer de Commissie voornemens is een land als adequaat voor doorgifte aan te merken (artikel 45 lid 3), is daarbij het advies van het Comité nodig. Het advies documenteert de omgang met persoonsgegevens in het betreffende land of specifieke gebieden of regio's.

70.I(t) uitbrengen van adviezen over ontwerpbesluiten van de toezichthoudende autoriteiten in het kader van het in artikel 64, lid 1, bedoelde coherentiemechanisme over aangelegenheden die overeenkomstig artikel 64, lid 2, ter sprake worden gebracht en uitbrengen van bindende beslissingen overeenkomstig artikel 65, met inbegrip van de in artikel 66 bedoelde gevallen;

Wanneer samenwerkende toezichthouders er onderling niet uitkomen, is inwinnen van het advies van het Comité verplicht (artikel 64). Lukt ook dat niet, dan neemt het Comité een bindend besluit (artikel 65). In spoedgevallen (artikel 66) kan dit anders lopen.

70.I(u) bevorderen van samenwerking en effectieve bilaterale en multilaterale uitwisseling van informatie en beste praktijken tussen de toezichthoudende autoriteiten;

Meer algemeen heeft het Comité als taak de samenwerking tussen toezichthouders te bevorderen.

70.I(v) bevorderen van gemeenschappelijke opleidingsprogramma's en vergemakkelijken van uitwisselingen van personeelsleden tussen de toezichthoudende autoriteiten, en waar passend, met de toezichthoudende autoriteiten van derde landen of met internationale organisaties;

In het kader van haar algemene taak kan het Comité zich inzetten om personeel en leden van toezichthouders op te leiden en uitwisseling in het kader van samenwerking te bevorderen en vergemakkelijken.

70.1(w) bevorderen van de uitwisseling van kennis en documentatie over de wetgeving en de praktijk op het gebied van gegevensbescherming met voor gegevensbescherming bevoegde toezichthoudende autoriteiten van de hele wereld;

Het Comité heeft verder als taak het uitwisselen van kennis en documentatie over privacy en persoonsgegevens met toezichthouders over de gehele wereld.

70.1(x) uitbrengen van adviezen over op Unieniveau opgestelde gedragscodes overeenkomstig artikel 40, lid 9; en

Middels gedragscodes kunnen branches de AVG nader invullen (artikel 40). Dergelijke gedragscodes kunnen algemeen verbindend worden verklaard (artikel 40 lid 9). Dit vereist advies van het Comité (zie ook artikel 64 lid 1 punt b).

70.1(y) houden van een openbaar elektronisch register van besluiten van toezichthoudende autoriteiten en gerechten over in het kader van het coherentiemechanisme behandelde aangelegenheden.

Als laatste taak beheert het Comité een openbaar register, naar verwachting een website, waarin zij besluiten en vonnissen publiceert over kwesties waarbij het coherentiemechanisme (artikel 63) werd ingezet.

70.2 Wanneer de Commissie het Comité om advies vraagt, kan zij een termijn aangeven, rekening houdend met de spoedeisendheid van de aangelegenheid.

Het Comité verstrekt haar advies standaard binnen acht weken (artikel 64 lid 3). Bij een verzoek om advies bedoeld in lid 1 kan de Commissie een gewenste leverdatum aangeven. Dit zal met name spelen bij spoedgevallen, zoals bij een beslissing van de Commissie over of een derde land niet langer adequate waarborgen kent voor doorgifte van persoonsgegevens (artikel 45 lid 5).

70.3 Het Comité zendt zijn adviezen, richtsnoeren, aanbevelingen en beste praktijken toe aan de Commissie en aan het in artikel 93 bedoelde comité en maakt deze bekend.

Adviezen, richtsnoeren, aanbevelingen en *best practices* worden bekend gemaakt aan de Commissie, aan het artikel 93-comité en aan het publiek. Het artikel 93-comité is een comité van vertegenwoordigers van de lidstaten (zie artikel 93), waarmee inspraak op beslissingen van de Commissie mogelijk wordt.

- 70.4 Het Comité raadpleegt, waar passend, de belanghebbende partijen en biedt hun de gelegenheid om binnen een redelijk tijdsbestek commentaar te leveren. Onverminderd artikel 76, maakt het Comité de resultaten van de raadpleging openbaar.

Bij het opstellen van adviezen, richtsnoeren, aanbevelingen en *best practices* (lid 3) worden uiteraard belanghebbende partijen uitgenodigd commentaar te leveren. Artikel 76 verklaart Verordening 1049/2001 (de “Europese Woo”) van toepassing op werk van het Comité. Resultaten van de raadpleging zijn dus voor een ieder openbaar toegankelijk, tenzij een van de daar genoemde uitzonderingen (zoals privacy of bescherming van zwaarwegende zakelijke belangen) opgaat.

Artikel 71. Rapportage

- 71.1 Het Comité stelt een jaarverslag op over de bescherming van natuurlijke personen met betrekking tot de verwerking in de Unie en, in voorkomend geval, in derde landen en internationale organisaties. Het verslag wordt openbaar gemaakt en toegezonden aan het Europees Parlement, de Raad en de Commissie.

Naast de in artikel 70 genoemde taken heeft het Comité tot taak een jaarverslag op te stellen ten aanzien van relevante ontwikkelingen op het gebied van verwerkingen van persoonsgegevens. Dit betreft met name ontwikkelingen in de EU, maar ook ontwikkelingen in derde landen en internationale organisaties. Dit is vooral van belang voor vragen omtrent doorgifte naar deze landen en organisaties (zie hoofdstuk 5).

- 71.2 Het jaarverslag omvat een evaluatie van de praktische toepassing van de richtsnoeren, aanbevelingen en beste praktijken bedoeld in artikel 70, lid 1, punt l), en van de bindende besluiten bedoeld in artikel 65.

Het Comité evalueert jaarlijks de praktische toepassing van richtsnoeren, aanbevelingen en *best practices* die men onder de AVG (artikel 70 lid 1 punt l) heeft uitgevaardigd. Deze evaluatie wordt gepubliceerd in het jaarverslag. Eveneens in het jaarverslag verschijnen bindende besluiten (artikel 65) waarmee het Comité knopen doorhakt in de samenwerking tussen toezichthouders.

Artikel 72. Procedure

- 72.1 Het Comité neemt besluiten met een gewone meerderheid van zijn leden, tenzij anders bepaald in deze verordening.

Besluiten worden genomen met meerderheid van stemmen. De AVG kent twee situaties waarin het Comité met tweederdemeerderheid beslist: het opstellen van het reglement van orde (lid 2) en advies bij het coherentiemechanisme (artikel 63 lid 3) waarin er tussen toezichthouders meningsverschillen bestaan, met name over de vraag of er sprake is van een inbreuk op de AVG en of deze grensoverschrijdend is (artikel 65 lid 1).

- 72.2 Het Comité stelt met een tweederdemeerderheid van zijn leden zijn eigen reglement van orde en zijn eigen werkregelingen vast.

Het Comité dient een reglement van orde op te stellen, en kan daaronder werkregelingen opstellen. Deze moeten met tweederdemeerderheid worden ingevoerd.

Artikel 73. Voorzitter

- 73.1 Het Comité kiest met gewone meerderheid een voorzitter en twee vicevoorzitters uit zijn leden.

Het Comité bestaat uit één toezichthouder per lidstaat (artikel 68 lid 2) en een vertegenwoordiger van de Europese Toezichthouder (zie artikel 68 lid 3). Zij kiezen onderling een voorzitter, die het Comité vertegenwoordigt (artikel 68 lid 2) en organiserende taken heeft (zie artikel 74 lid 1). Bij ontstentenis wordt de voorzitter vervangen door een van de vicevoorzitters. Dit wordt nader geregeld in het reglement van orde van het Comité (artikel 72).

- 73.2 De ambtstermijn van de voorzitter en de vicevoorzitters bedraagt vijf jaar en kan eenmaal worden verlengd.

De voorzitter en de twee vicevoorzitters hebben ambtstermijnen van vijf jaar en mogen daarna eenmaal opnieuw worden gekozen.

Artikel 74. Taken van de voorzitter

De voorzitter heeft de volgende taken:

74.1(a) bijeenroepen van de bijeenkomsten van het Comité en het opstellen van zijn agenda;

74.1(b) ter kennis brengen van de door het Comité overeenkomstig artikel 65 vastgestelde besluiten aan de leidende toezichthoudende autoriteit en de betrokken toezichthoudende autoriteiten;

74.1(c) ervoor zorgen dat de taken van het Comité tijdig worden uitgevoerd, met name wat het in artikel 63 bedoelde coherentiemechanisme betreft.

De taken van de voorzitter volgen logischerwijs uit de functietitel: het organiseren van bijeenkomsten en het vaststellen van de agenda en het toezien op het uitvoeren van de taken van het Comité. Ook communiceert de voorzitter besluiten in het kader van de geschillenprocedure uit artikel 65 en stelt hij de Commissie in kennis van de activiteiten van het Comité (artikel 68 lid 5). Verder kan de voorzitter het initiatief nemen tot adviezen vanuit zijn Comité (artikel 64 lid 2).

74.2 Het Comité stelt in zijn reglement van orde de taakverdeling tussen de voorzitter en de vicevoorzitters vast.

In het reglement van orde (artikel 72 lid 2) wordt uitgewerkt hoe de voorzitter en de twee vicevoorzitters hun taken onderling verdelen.

Artikel 75. Secretariaat

75.1 Het Comité heeft een secretariaat, dat wordt verzorgd door de Europese Toezichthouder voor gegevensbescherming.

Voor de dagelijkse werkzaamheden beschikt het Comité (artikel 68) over een secretariaat. Het secretariaat biedt het Comité analytische, administratieve en logistieke ondersteuning (lid 5). Dit secretariaat wordt verzorgd door de Europese Toezichthouder (zie artikel 68 lid 3).

75.2 Het secretariaat verricht zijn taken uitsluitend volgens de instructies van de voorzitter van het Comité.

De personeelsleden van de Europese Toezichthouder voor gegevensbescherming die betrokken zijn bij de uitvoering van het secretariaatswerk, dienen hun taken uitsluitend te verrichten volgens de instructies van de voorzitter van het

Comité, en zij dienen aan hem verslag uit te brengen (overweging 140). Hiermee blijft de onafhankelijkheid van het Comité gewaarborgd.

- 75.3 De personeelsleden van de Europese Toezichthouder voor gegevensbescherming die betrokken zijn bij de uitvoering van de krachtens deze verordening aan het Comité opgedragen taken vallen onder een andere rapportageregeling dan de personeelsleden die betrokken zijn bij de uitvoering van de aan de Europese Toezichthouder voor gegevensbescherming opgedragen taken.

Net zoals bij de instructiebevoegdheid (lid 3) ligt ook de rapportageplicht voor personeelsleden van de Europese Toezichthouder die in het secretariaat werken uitsluitend bij het Comité.

- 75.4 Waar passend wordt door het Comité en de Europese Toezichthouder voor gegevensbescherming een memorandum van overeenstemming ter uitvoering van dit artikel opgesteld en bekendgemaakt, waarin de voorwaarden van hun samenwerking worden vastgelegd en dat van toepassing is op de personeelsleden van de Europese Toezichthouder voor gegevensbescherming die betrokken zijn bij de uitvoering van de krachtens deze verordening aan het Comité opgedragen taken.

Het zal in de praktijk wenselijk zijn om de voorwaarden van de ondersteuning van het Comité door de EDPS nader uit te werken, alsook om de instructiebevoegdheden (lid 2) en de rapportageplichten (lid 3) vast te leggen. Dit zal gebeuren in een nader te sluiten memorandum.

- 75.5 Het secretariaat biedt het Comité analytische, administratieve en logistieke ondersteuning.

Het secretariaat is ondersteunend op het gebied van administratie, logistiek en aanvullende ondersteunende diensten. Zie nader lid 6.

Het secretariaat is met name belast met:

- 75.6(a) de dagelijkse werking van het Comité;
- 75.6(b) de communicatie tussen de leden van het Comité, zijn voorzitter en de Commissie;
- 75.6(c) de communicatie met andere instellingen en het brede publiek;
- 75.6(d) het gebruik van elektronische middelen voor interne en externe communicatie;
- 75.6(e) de vertaling van relevante informatie;

75.6(f) de voorbereiding en opvolging van de bijeenkomsten van het Comité;

75.6(g) de voorbereiding, opstelling en bekendmaking van adviezen, besluiten inzake beslechting van geschillen tussen toezichthoudende autoriteiten, en andere teksten die het Comité vaststelt.

Lid 6 noemt enkele specifieke werkzaamheden van het secretariaat, met name betreffende de interne communicatie en bekendmaking van informatie.

Artikel 76. Vertrouwelijkheid

76.1 De besprekingen van het Comité zijn vertrouwelijk indien het comité dit noodzakelijk acht, in overeenstemming met zijn reglement van orde.

Het Comité kan bepalen dat besprekingen vertrouwelijk zijn. In zijn reglement van orde moet worden vastgelegd wanneer dit het geval zal zijn.

76.2 Op de toegang tot documenten die aan de leden van het Comité, deskundigen en vertegenwoordigers van derden worden voorgelegd, is Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van toepassing.

Verordening 1049/2001 (de “Europese Woo”) regelt de toegang van het publiek tot de documenten van het Europees Parlement, de Raad en de Commissie. Dergelijke documenten zijn in beginsel voor een ieder toegankelijk. Uitzonderingen gelden onder meer op grond van de persoonlijke levenssfeer en de integriteit van een individu en de commerciële belangen van een natuurlijke of rechtspersoon.

Hoofdstuk VIII

Beroep, aansprakelijkheid en sancties

Hoofdstuk VIII geeft de AVG tanden: toezichthouders kunnen op grond van de artikelen uit dit hoofdstuk boetes opleggen (artikel 83) bij het niet-nakomen van de AVG of het niet voldoen aan de algemene corrigerende maatregelen (artikel 58 lid 2). Deze boetes moeten voldoen aan een aantal randvoorwaarden (artikel 83). Uiteraard staat de gang naar de rechter open tegen een besluit van de toezichthouder (artikel 78).

Betrokkenen kunnen verzoeken om handhaving bij de toezichthouder (artikel 77) maar ook naar de civiele rechter (artikel 79) stappen. Zij kunnen bij beiden nakoming van de AVG eisen, maar ook een schadevergoeding (artikel 82). Lidstaten mogen ook andere sancties invoeren, zoals strafrechtelijke sancties (artikel 84).

Artikel 77. Recht om klacht in te dienen bij een toezichthoudende autoriteit

77.1 Onverminderd andere mogelijkheden van administratief beroep of een voorziening in rechte, heeft iedere betrokkene het recht een klacht in te dienen bij een toezichthoudende autoriteit, met name in de lidstaat waar hij gewoonlijk verblijft, hij zijn werkplek heeft of waar de beweerde inbreuk is begaan, indien hij van mening is dat de verwerking van hem betreffende persoonsgegevens inbreuk maakt op deze verordening.

Toezichthouders kunnen uit eigener beweging optreden, maar zullen in de praktijk vaak op klachten reageren. Dit artikel geeft iedere betrokkene een klachtrecht wanneer hij vermoedt dat sprake is van een hem rakende overtreding van de AVG. Naar Nederlands bestuursrecht zal deze klacht worden gekwalificeerd als een verzoek tot handhaving (art. 4:1 Algemene wet bestuursrecht) waarop de gewone regels van het bestuursrecht van toepassing zijn (Memorie van Toelichting (MvT) Uitvoeringswet AVG (Uitvoeringswet), p. 36). Een betrokkene kan ook een belangenorganisatie namens hem laten optreden (artikel 80).

Bevoegdheid. De betrokkene kan de klacht indienen bij iedere toezichthouder die hem goedgeeft. Voor de hand ligt de toezichthouder voor het land waar de betrokkene gewoonlijk verblijft of zijn werkplek heeft, en de toezichthouder voor het land waar de inbreuk is begaan. De klacht moet wel de betrokkene zelf betreffen.

Competentie. De toezichthouder waar de klacht wordt ingediend, hoeft niet competent te zijn (artikel 55 of 56) voor het onderwerp van de klacht. Als de toezichthouder niet competent is, kan hij op grond van de klacht een wél competente toezichthouder aansporen tot onderzoek over te gaan (artikel 56). De betreffende toezichthouder wordt dan betrokken (artikel 4 definitie 22) bij dit onderzoek. Deze regels gaan boven de algemene bevoegdheidsregels uit het Europese recht, zoals die van Verordening (EU) nr. 1215/2012.

Voorziening in rechte. Een overtreding van de AVG levert een onrechtmatige daad op jegens de betrokkenen in kwestie, die daarop een gerechtelijke procedure kunnen starten. Zie ook artikel 82.

77.2 De toezichthoudende autoriteit waarbij de klacht is ingediend, stelt de klager in kennis van de voortgang en het resultaat van de klacht, alsmede van de mogelijke voorziening in rechte overeenkomstig artikel 78.

De toezichthouder heeft de plicht de klager op de hoogte te houden van de voortgang van de procedure en het resultaat daarvan. Tevens moet de toezichthouder de burger erop wijzen dat hij in bezwaar en beroep kan tegen besluiten van de toezichthouder. Naar Nederlands recht moet een klager in beginsel altijd gelegenheid krijgen zijn zienswijze naar voren te brengen bij de behandeling van zijn klacht (art. 4:7 en 4:8 Awb).

Artikel 78. Recht om een doeltreffende voorziening in rechte in te stellen tegen een toezichthoudende autoriteit

78.1 Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, heeft iedere natuurlijke persoon of rechtspersoon het recht om tegen een hem betreffend juridisch bindend besluit van een toezichthoudende autoriteit een doeltreffende voorziening in rechte in te stellen.

De AVG vereist dat besluiten van toezichthouders getoetst kunnen worden bij een onafhankelijke rechter, los van een eventuele interne beroepsprocedure bij de toezichthouder zelf. In het Nederlands recht wordt hieraan voldaan door het hoger beroep bij de rechtbank dat men kan instellen tegen het besluit op bezwaar dat door de toezichthouder wordt genomen (art. 8:1 Awb).

Geen beroep bij adviezen. Geen mogelijkheid tot voorziening in rechte bestaat bij handelingen van de toezichthouder die niet juridisch bindend zijn, zoals adviezen.

Bevoegdheid. Een vordering tegen een toezichthoudende autoriteit dient te worden ingesteld bij de gerechten van de lidstaat waar de toezichthoudende autoriteit is gevestigd, en dient in overeenstemming te zijn met het procesrecht van

die lidstaat. Volgens art. 8:7 lid 2 Awb is bij een besluit door de Nederlandse toezichthouder de rechtbank bevoegd voor de woonplaats van de klager.

Toetsing. De AVG staat toe dat de rechtbank het besluit van de toezichthouder volledig toetst. In Nederland is de rechter hier terughoudend in en wordt gewoonlijk slechts een marginale toets uitgevoerd of de toezichthouder in redelijkheid dit besluit had kunnen nemen. Dit gebeurde bijvoorbeeld in de zaak aangespannen door VoetbalTV nadat hen een boete werd opgelegd van 575.000 euro, omdat zij geen gerechtvaardigd belang zou hebben gehad om amateurvoetbalwedstrijden online te streamen. De Afdeling Bestuursrecht Raad van State (“de Afdeling”) gaat in op of de AP redelijkerwijs tot dat besluit had mogen komen. De Afdeling legt uit dat voor een gerechtvaardigd belang afweging de driestapentoets (zie artikel 6 AVG) wordt gebruikt. De AP heeft niet alle belangen van VoetbalTV behandeld in vraag 1: “Heeft de partij een gerechtvaardigd belang?”. De AP had dus niet tot het besluit en de boete mogen komen (Afdeling Bestuursrecht Raad van State, ECLI:NL:RVS:2022:2173, 27 juli 2022).

Prejudiciële vragen. Nationale rechtbanken zijn bevoegd (en in hoger beroep verplicht, art 267 VWEU) om prejudiciële vragen te stellen over de uitlegging van het Unierecht, waaronder ook de AVG, in geval van vragen over uitleg of geldigheid daarvan. Dit gebeurde in het vervolg van de hiervoor genoemde zaak ook bij de rechtbank Amsterdam. De Afdeling ging niet in op de inhoudelijke toetsing van het standpunt van de AP dat een gerechtvaardigd belang alleen een tot de wet behorend, wet zijnd, in een wet vastgesteld belang kan zijn, en a priori geen zuiver commercieel belang kan zijn. Na terugverwijzing stelde de rechtbank prejudiciële vragen aan het Hof: hoe moeten we het “gerechtvaardigd belang” interpreteren? Deze zaak is ten tijde van het schrijven van dit boek nog aanhangig.

- 78.2 Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep heeft iedere betrokkene het recht om een doeltreffende voorziening in rechte in te stellen indien de overeenkomstig de artikelen 55 en 56 bevoegde toezichthoudende autoriteit een klacht niet behandelt of de betrokkene niet binnen drie maanden in kennis stelt van de voortgang of het resultaat van de uit hoofde van artikel 77 ingediende klacht.

Naast het recht tegen een besluit in beroep te gaan bij de rechter, bestaat ook het recht in beroep te gaan wanneer een toezichthouder een klacht niet in behandeling neemt, of niet tijdig laat weten hoe de klacht is afgehandeld.

Bevoegde toezichthouder. Iedere betrokkene kan bij iedere toezichthouder een klacht indienen, ongeacht of deze competent is om de klacht af te handelen (zie artikel 77 lid 1). Echter, alleen wanneer een op grond van de hoofdregel (artikelen 55 en 56) bevoegde toezichthouder weigert de klacht op te volgen, kan men naar de rechter.

Verzoek tot handhaving. In Nederland zal een klacht worden opgevat als een verzoek tot handhaving (art. 4:1 Algemene wet bestuursrecht). Op een dergelijk verzoek wordt een besluit genomen, waartegen volgens de normale regels bezwaar en beroep open staat. Dit kan ook bij het niet of niet tijdig nemen van een besluit (artikel 6:12 Awb).

78.3 Een procedure tegen een toezichthoudende autoriteit wordt ingesteld bij de gerechten van de lidstaat waar de toezichthoudende autoriteit is gevestigd.

Hoger beroep tegen een besluit van de toezichthouder is alleen mogelijk bij een rechtbank van de lidstaat waar die toezichthouder is gevestigd. Het nationale recht bepaalt bij welke rechtbank in die lidstaat het beroep wordt ingesteld.

Bevoegde Nederlandse rechtbank. Naar Nederlands recht bepaalt artikel 8:7 lid 2 Awb dat beroep tegen besluiten van de AP open staat bij de rechtbank binnen het arrondissement waarvan de indiener van het beroepschrift zijn woonplaats in Nederland heeft. Bij buitenlandse partijen is bevoegd de rechtbank binnen het rechtsgebied waarvan het bestuursorgaan zijn zetel heeft.

Toetsing. Overweging 143 bepaalt dat de rechtbank volledige rechtsmacht uit moet kunnen oefenen, waaronder rechtsmacht om alle feitelijke en juridische vraagstukken in verband met het bij hen aanhangige geschil te onderzoeken. Dit komt neer op een volledige toetsing, terwijl naar Nederlands bestuursrecht gewoonlijk slechts marginaal wordt getoetst.

78.4 Wanneer een procedure wordt ingesteld tegen een besluit van een toezichthoudende autoriteit waaraan een advies of een besluit van het Comité in het kader van het coherentiemechanisme is voorafgegaan, doet de toezichthoudende autoriteit dat advies of besluit aan de gerechten toekomen.

Om eenvormigheid van de besluitvorming rondom persoonsgegevens en de AVG te stimuleren, moet het Comité adviezen geven over voorgenomen maatregelen van toezichthouders. Deze adviezen dienen ter kennis te komen van de rechtbank wanneer beroep wordt ingesteld tegen die maatregel.

Advies of besluit. Het Comité geeft advies wanneer een toezichthouder maatregelen wil nemen zoals bepalen wanneer een DPIA verplicht is of het goedkeuren van gedragscodes of modelclausules (zie artikel 64). Het Comité besluit over de vraag welke toezichthouder bevoegd is bij een grensoverschrijdende verwerking (zie artikel 65).

Prejudiciële vragen. Wanneer een advies een overwegende rol speelt in de procedure bij de rechtbank, ligt het voor de hand dat de rechtbank prejudiciële vragen stelt aan het Hof van Justitie. Wanneer het gaat om een besluit, is de rechtbank dat zelfs verplicht (artikel 267 VWEU).

Artikel 79. Voorziening in rechte tegen verwerkingsverantwoordelijke of verwerker

- 79.1 Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, waaronder het recht uit hoofde van artikel 77 een klacht in te dienen bij een toezichthoudende autoriteit, heeft elke betrokkene het recht een doeltreffende voorziening in rechte in te stellen indien hij van mening is dat zijn rechten uit hoofde van deze verordening geschonden zijn ten gevolge van een verwerking van zijn persoonsgegevens die niet aan deze verordening voldoet.

Voor de meeste mensen zal een klacht bij een toezichthouder de meest voor de hand liggende route vormen. Echter, dit laat onverlet dat een betrokkene ook naar de rechter kan. Naar Nederlands recht zal de vordering dan op grond van onrechtmatige daad gebaseerd zijn. Tot de mogelijkheden behoren met name een verwerkingsverbod of andere uitoefening van een recht van de betrokkene, maar ook een schadevergoeding (zie artikel 82). Het succesvol aansprakelijk stellen van een verwerkingsverantwoordelijke op basis van onrechtmatige daad gebeurde in de volgende zaak. De eiseres vorderde schadevergoeding op basis van een onrechtmatige daad (art. 6:162 BW) door het schenden van artikel 32 AVG door een ziekenhuis waar ze was behandeld, en de door haar geleden schade die uit die inbreuk op de AVG voortvloeide. De schade kwam voort uit het feit dat de medische gegevens die onttrokken waren uit de eiser haar medische dossier, terugkwamen in een gepubliceerd boek van haar ex. Het ziekenhuis voldeed niet aan NEN7510 en NEN7512 (invulling van artikel 32 AVG voor de zorg) vereisten om toegang tot de dossiers zorgvuldig te loggen (Rb. Zeeland-West-Brabant, ECLI:NL:RBZWB:2022:5457, 21 september 2022), waardoor de schadevergoeding werd toegekend.

Verwerkingsverantwoordelijke én verwerker. In tegenstelling tot de Richtlijn biedt de AVG de mogelijkheid om een verwerker in rechte te betrekken wanneer deze de op hem rustende verplichtingen uit de AVG niet nakomt of rechten van betrokkenen niet respecteert.

Beroepsprocedure bij rechten van betrokkene. Indien een beslissing inzake de rechten van de betrokkene (uit de artikelen 15, 16, 17, 18, 20 of 21) is genomen door een verwerkingsverantwoordelijke of verwerker kan een belanghebbende binnen 6 weken na ontvangst van deze beslissing (of 6 weken na verloop van de termijn indien er niet tijdig is beslist), middels een verzoekschrift (zonder advocaat) beroep instellen tegen dit besluit (artikel 35 Uitvoeringswet). Gedurende deze procedure kan de rechter andere belanghebbenden in de gelegenheid stellen om hun visie kenbaar te maken en partijen verplichten tot het toezenden van nadere stukken. Op deze verzoekschriftprocedure zijn Titel 5, van Boek 2 van het Rv en de artikelen 8:45, lid 2 en 3 en 8:49 van de Awb van overeenkomstige toepassing.

Verzoek tot bemiddeling AP. Een belanghebbende kan gebruik maken van een geschilbeslechtsingsregeling op grond van een goedgekeurde gedragscode (artikel 40, lid 5 AVG), dan wel de AP verzoeken om te bemiddelen in een geschil met een verwerkingsverantwoordelijke. Indien een belanghebbende van deze mogelijkheid gebruik maakt, behoudt deze daarnaast eveneens het recht om, in afwijking van artikel 6:7 van de Awb, binnen 6 weken na ontvangst van een bericht dat de behandeling van de zaak is beëindigd, alsnog beroep in te stellen bij een rechter overeenkomstig artikel 79 AVG (artikel 35 Uitvoeringswet).

Maatregel ter beëindiging of herstel. In de Uitvoeringswet (artikel 35) wordt de rechter de mogelijkheid geboden om, naast sancties, gedrag van de verwerkingsverantwoordelijke of verwerker in strijd met de AVG te verbieden en deze te bevelen maatregelen te treffen tot herstel. Een rechtspersoon (in de zin van artikel 3:305a BW) kan aan een vordering hiertoe geen gegevensverwerking ten grondslag leggen indien de betrokkene hiertegen bezwaar heeft.

- 79.2 Een procedure tegen een verwerkingsverantwoordelijke of een verwerker wordt ingesteld bij de gerechten van de lidstaat waar de verwerkingsverantwoordelijke of de verwerker een vestiging heeft. Een dergelijke procedure kan ook worden ingesteld bij de gerechten van de lidstaat waar de betrokkene gewoonlijk verblijft, tenzij de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie van een lidstaat is die optreedt in de uitoefening van het overheidsgezag.

De betrokkene mag kiezen of hij naar de rechter stapt in het land waar de verwerkingsverantwoordelijke of de verwerker gevestigd is, of naar de rechter in zijn eigen land. Gaat hij naar een ander land, dan volgt welke rechtbank in de betreffende lidstaat bevoegd is uit Verordening 1215/2012/EU (Brussel I).

Bevoegdheid bij overheidsinstanties. Als de betrokken verwerkingsverantwoordelijke of verwerker een buitenlandse overheidsinstantie is die handelt vanuit haar openbare taak, dan moet de betrokkene naar de betreffende lidstaat en kan hij niet naar de rechter in zijn eigen land.

Artikel 80. Vertegenwoordiging van betrokkenen

80.1 De betrokkene heeft het recht een orgaan, organisatie of vereniging zonder winstoogmerk dat of die op geldige wijze volgens het recht van een lidstaat is opgericht, waarvan de statutaire doelstellingen het openbare belang dienen en dat of die actief is op het gebied van de bescherming van de rechten en vrijheden van de betrokkene in verband met de bescherming van diens persoonsgegevens, opdracht te geven de klacht namens hem in te dienen, namens hem de in artikelen 77, 78 en 79 bedoelde rechten uit te oefenen en namens hem het in artikel 82 bedoelde recht op schadevergoeding uit te oefenen, indien het lidstatelijke recht daarin voorziet.

De AVG voorziet in de mogelijkheid van collectieve acties door stichtingen, verenigingen en dergelijke die privacy (mede) tot hun doelstelling rekenen. Nederlandse voorbeelden van dergelijke organisaties zijn de stichting Bits of Freedom ten aanzien van online burgerrechten en de meer algemeen op privacy georiënteerde stichting Privacy First.

Collectieve acties. Collectieve acties zijn in Nederland nu reeds mogelijk (art. 3:305a BW). Een stichting of vereniging met volledige rechtsbevoegdheid kan een rechtsvordering instellen die strekt tot bescherming van gelijksoortige belangen van andere personen, voorzover zij deze belangen ingevolge haar statuten behartigt. Deze vordering mag (lid 3) echter niet strekken tot schadevergoeding te voldoen in geld. De AVG brengt daar geen verandering in. De recent aangenomen Wet afwikkeling massaschade in collectieve actie (TK 34.608) brengt hier verandering in. Iedere betrokkene kan zich onttrekken aan de collectieve actie (artikel 37 Uitvoeringswet).

80.2 De lidstaten kunnen bepalen dat een orgaan, organisatie of vereniging als bedoeld in lid 1 van dit artikel, over het recht beschikt om onafhankelijk van de opdracht van een betrokkene in die lidstaat een klacht in te dienen bij de overeenkomstig artikel 77 bevoegde toezichthoudende autoriteit en de in de artikelen 78 en 79 bedoelde rechten uit te oefenen, indien het, onderscheidenlijk zij, van mening is dat de rechten van een betrokkene uit hoofde van deze verordening zijn geschonden ten gevolge van de verwerking.

Het is ter keuze van de lidstaten of men wil toestaan dat zo'n stichting of andere organisatie bevoegd is een procedure te starten met of zonder machtiging van individuele personen die getroffen zijn door een schending van de AVG. In Nederland is zo'n machtiging in principe niet nodig onder art. 3:305a BW, hoewel in de praktijk de zaak vaak wordt aangespannen door de stichting samen met een individueel getroffen persoon. Wel kunnen getroffen personen bezwaar maken tegen de principiële actie (lid 4).

Artikel 81. Schorsing van de procedure

81.1 Indien een bevoegd gerecht van een lidstaat over informatie beschikt dat bij een gerecht van een andere lidstaat een procedure inzake verwerking betreffende dezelfde aangelegenheid en dezelfde verwerkingsverantwoordelijke of verwerker hangende is, neemt het contact op met dat gerecht in de andere lidstaat om het bestaan van die procedure te verifiëren.

Een mogelijke schending van de AVG kan zowel als administratieve procedure bij de toezichthouder (artikel 77) als procedure bij de rechtbank (artikel 79) worden behandeld. Daardoor kan een zaak aanhangig worden in de ene lidstaat naar aanleiding van een klachtenprocedure bij de toezichthouder, en de andere lidstaat door direct naar de rechter te stappen. Om nu te voorkomen dat dezelfde procedure bij twee rechtbanken komt (litispendentie), met mogelijk uiteenlopende uitspraken, regelt dit artikel 81 hoe deze rechtbanken regelen dat slechts één van hen de zaak behandelt als sprake is van dezelfde aangelegenheid. Vergelijk algemeen Verordening (EU) nr. 1215/2012 (EEX-Verordening).

Dezelfde aangelegenheid. Het criterium voor deze procedure is vrij ruim: het kan gaan om dezelfde verwerking, waarbij het bijvoorbeeld kan gaan om hetzelfde onderwerp van de verwerking, dezelfde activiteiten van de verwerkingsverantwoordelijke of de verwerker, of dezelfde aanleiding (overweging 144). Algemeen is vereist dat er tussen de twee zaken een zo nauwe band bestaat dat een goede rechtsbedeling vraagt om hun gelijktijdige behandeling en berechting, teneinde te vermijden dat bij afzonderlijke procedures onverenigbare beslissingen worden gegeven.

81.2 Indien een procedure inzake verwerking met betrekking tot dezelfde aangelegenheid en dezelfde verwerkingsverantwoordelijke of verwerker hangende is bij een gerecht van een andere lidstaat, kan ieder ander bevoegd gerecht dan dat welk als eerste is aangezocht, zijn procedure schorsen.

Vanuit de algemene regel dat de eerst aangespannen procedure wint, is iedere 'latere' rechtbank bevoegd zijn eigen procedure te schorsen totdat de rechtbank met de eerst aangespannen procedure vonnis heeft gewezen. Een alternatief staat in lid 3: het verwijzen van de zaak naar de eerste rechtbank.

81.3 Indien die procedure in eerste aanleg aanhangig is, kan elk gerecht dat niet als eerste is aangezocht, op verzoek van een van de partijen ook tot verwijzing overgaan, mits het eerst aangezochte gerecht bevoegd is om van de beide procedures kennis te nemen en zijn wetgeving de voeging daarvan toestaat.

Wanneer het nationaal recht daarin voorziet, mag de 'latere' rechtbank de partijen ook verwijzen naar de 'eerdere' rechtbank. Vereist is wel dat die rechtbank bevoegd is om kennis te nemen van de procedure en de procedure uit het ande-

re land kan voegen. In Nederland is verwijzing naar een buitenlandse ‘eerdere’ rechtbank geregeld in artikel 12 Rv.

Artikel 82. Recht op schadevergoeding en aansprakelijkheid

82.1 Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.

Het niet nakomen van een verplichting uit de AVG is krachtens artikel 79 een onrechtmatige daad jegens de betrokkene. Dit geldt zowel voor de verwerkingsverantwoordelijke als voor de verwerker (zie nader lid 2). Wel moet daadwerkelijk schade worden aangetoond; enkele AVG-schending is niet genoeg (HvJ EU 4 mei 2023, ECLI:EU:C:2023:370). Een praktisch probleem hierbij is dat schade als gevolg van een onrechtmatige verwerking zeer lastig te kwantificeren is. De rechtbank zal de schade derhalve moeten schatten (art. 6:106 BW).

Voorbeelden. In een zaak tegen Uitkeringsinstantie UWV heeft de rechtbank Amsterdam geoordeeld dat het UWV een schadevergoeding van 250 euro moest betalen aan een betrokkene vanwege een datalek (ECLI:NL:RBAMS:2019:6490). Een ander voorbeeld is een zaak tegen Bravis ziekenhuis bij de Rechtbank Zeeland West Brabant. De eiseres vorderde schadevergoeding op basis van een onrechtmatige daad (art. 6:106 BW) door het schenden van artikel 32 AVG door het ziekenhuis, en de door haar geleden schade die uit die inbreuk op de AVG voortvloeide. De schade kwam voort uit het feit dat de medische gegevens die onttrokken waren uit de eiser haar medische dossier, terugkwamen in een gepubliceerd boek van haar ex (Rb. Zeeland-West-Brabant, ECLI:NL:RBZWB:2022:5457, 21 september 2022). Anders: RvS 1 april 2020, ECLI:NL:RVS:2020:899.

82.2 Elke verwerkingsverantwoordelijke die bij verwerking is betrokken, is aansprakelijk voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op deze verordening. Een verwerker is slechts aansprakelijk voor de schade die door verwerking is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van deze verordening of buiten dan wel in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld.

De verwerkingsverantwoordelijke en de verwerker zijn hoofdelijk aansprakelijk voor de schade, zij het op verschillende manieren (zie ook lid 4 over meerdere verwerkingsverantwoordelijken of verwerkers). Contractueel kan jegens de betrokkene niet worden afgeweken van deze regeling. Partijen kunnen natuurlijk wel onderling een verhaalsrecht overeen komen (zie ook lid 5 dat een wettelijk verhaalsrecht introduceert).

Verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is in beginsel voor alle schade aansprakelijk, ongeacht of die door hemzelf of door een verwerker is veroorzaakt. Geen aansprakelijkheid bestaat alleen in gevallen van overmacht (lid 3).

Verwerker. De verwerker is aansprakelijk voor alle schade veroorzaakt door een specifiek tot hem gerichte verplichting, zoals het inschakelen van een subverwerker zonder toestemming (artikel 28 lid 2) of het niet op orde hebben van zijn beveiliging (artikel 32), maar ook voor schade veroorzaakt door handelen buiten de instructies.

Inbreuk. Iedere inbreuk ofwel overtreding van de AVG levert in beginsel een grondslag voor een schadeclaim op. Het maakt niet uit of er ook een administratieve boete (artikel 83) op overtreding staat. Ook het overtreden van gedelegeerde handelingen en uitvoeringshandelingen die werden vastgesteld overeenkomstig de AVG, alsmede het lidstatelijke recht waarin afgeleide regels worden gespecificeerd (overweging 146), komt in aanmerking voor een schadeclaim.

- 82.3 Een verwerkingsverantwoordelijke of verwerker wordt van aansprakelijkheid op grond van lid 2 vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

De AVG kent ook bij vorderingen tot schadevergoeding een omgekeerde bewijslast. Een verwerkingsverantwoordelijke of verwerker kan slechts aansprakelijkheid ontlopen door aan te tonen dat het schadebrengende feit hem niet kan worden aangewreven. Dit betreft in eerste instanties gevallen van overmacht (art. 6:75 BW). Ook situaties waarin de betreffende handeling volledig aan een andere partij te wijten is, leveren een vrijstelling van aansprakelijkheid op. Wanneer een verwerker bijvoorbeeld persoonsgegevens verwerkt terwijl de verwerkingsverantwoordelijke geen adequate toestemming (artikel 6 lid 1 punt a) verkregen heeft voor die verwerking, is de verwerker daar niet verantwoordelijk voor te houden.

- 82.4 Wanneer meerdere verwerkingsverantwoordelijken of werkers bij dezelfde verwerking betrokken zijn, en overeenkomstig de leden 2 en 3 verantwoordelijk zijn voor schade die door verwerking is veroorzaakt, wordt elke verwerkingsverantwoordelijke of verwerker voor de gehele schade aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk wordt vergoed.

Wanneer meerdere verwerkingsverantwoordelijken of werkers betrokken zijn, zijn zij allen hoofdelijk aansprakelijk, zij het dat een verwerker iets eerder aan aansprakelijkheid kan ontsnappen (lid 2). De betrokkene kan dus de partij met de diepste zakken aanspreken, ongeacht wie de fout te verwijten is of zelfs maar wie het grootste aandeel had in de fout (vergelijk de groepsaansprakelijkheid uit art. 6:166 BW). Partijen kunnen onderling de schade verhalen (lid 5).

- 82.5 Wanneer een verwerkingsverantwoordelijke of verwerker de schade overeenkomstig lid 4 geheel heeft vergoed, kan deze verwerkingsverantwoordelijke of verwerker op andere verwerkingsverantwoordelijken of werkers die bij de verwerking waren betrokken, het deel van de schadevergoeding verhalen dat overeenkomt met hun deel van de aansprakelijkheid voor de schade, overeenkomstig de in lid 2 gestelde voorwaarden.

Op grond van lid 4 is iedere verwerkingsverantwoordelijke en iedere verwerker hoofdelijk aansprakelijk voor de gehele schade. Dit lid 5 introduceert een verhaalsmogelijkheid voor de aansprakelijk gehouden partij om bij de andere partijen hun deel van de schade gecompenseerd te krijgen.

Hun deel. Vastgesteld moet worden welk deel van de fout ligt bij de aan te spreken partijen. Lid 2 speelt een belangrijke rol: verwerkers zijn alleen aansprakelijk wanneer zij een specifiek tot hen gerichte norm overtreden of buiten de instructies van hun verwerkingsverantwoordelijke treden. Ook lid 3 is relevant: wie kan bewijzen dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit, hoeft niet bij te dragen aan de compensatie. In beginsel zullen de bij te dragen delen van de betrokken partijen van gelijke hoogte zijn, maar als een groter deel van de schade aan één partij toe te rekenen is, dan ligt het voor de hand dat deze meer bijdraagt.

Dwingend recht. Het lijkt geaccepteerd dat partijen in bijvoorbeeld een verwerkersovereenkomst een andere onderlinge verdeling mogen afspreken. Een verwerker zou zijn aansprakelijkheid jegens de verwerkingsverantwoordelijke daarmee kunnen inperken en zo de risico's voor hemzelf beperken. Een verwerkingsverantwoordelijke zal dit echter niet snel accepteren, tenzij de prijs van de dienst navenant laag zal zijn of hij zelf aanvullende schadebeperkende maatregelen kan nemen.

- 82.6 Gerechtelijke procedures voor het uitoefenen van het recht op schadevergoeding worden gevoerd voor de in artikel 79, lid 2, bedoelde lidstaatrechtelijk bevoegde gerechten.

Wanneer een betrokkene schadevergoeding wil claimen, dient hij dit te doen bij een bevoegde rechtbank uit de lidstaat waar de verwerkingsverantwoordelijke of de verwerker een vestiging heeft (artikel 79 lid 2). Tenzij de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie van een lidstaat is, kan hij ook naar een bevoegde rechtbank uit zijn eigen lidstaat stappen (artikel 79 lid 2). Welke rechtbank in de betreffende lidstaat bevoegd is, volgt uit Verordening 1215/2012/EU (Brussel I).

Artikel 83. Voorwaarden aan het opleggen van administratieve geldboeten

83.1 Elke toezichthoudende autoriteit zorgt ervoor dat de administratieve geldboeten die uit hoofde van dit artikel worden opgelegd voor de in de leden 4, 5 en 6 vermelde inbreuken op deze verordening in elke zaak doeltreffend, evenredig en afschrikkend zijn.

Ter afschrikking van overtreding van de AVG hebben de toezichthouders de bevoegdheid om administratieve geldboeten op te leggen aan zowel verwerkingsverantwoordelijken als aan verwerkers. Deze bevoegdheid geldt naast de corrigerende bevoegdheden uit artikel 58 lid 2. De AVG kent twee categorieën: een relatief lage categorie bij overtreding van administratieve bepalingen (lid 4) en een hoge categorie voor meer fundamentele overtredingen (lid 5) of het niet opvolgen van bevelen van toezichthouders (lid 6).

Doeltreffend, evenredig en afschrikkend. Onder het Unierecht moeten sancties in het algemeen doeltreffend, evenredig en afschrikkend zijn. Doeltreffend wil zeggen dat zij het gewenste gedrag (naleving van de AVG) stimuleren, evenredig dat ze niet disproportioneel zwaar (of juist licht) zijn gezien de overtreding en afschrikkend dat ook anderen het gewenste gedrag gaan vertonen (generale preventie). Het Hof van Justitie kan hieraan toetsen. De *Richtlijnen over de toepassing en context van bestuurlijke boetes* (WP 253, 3 oktober 2017) van de Artikel 29-Werkgroep geven aan wanneer een boete opportuun is en wanneer andere sancties gepaster zouden zijn.

Boetes aan ondernemingen. Het opleggen van boetes is met name bedoeld richting ondernemingen. Dit begrip omvat iedere entiteit die een economische activiteit uitoefent (zie artikel 4 definitie 18). Lid 4 en 5 bieden de mogelijkheid de boete te baseren op de wereldwijde jaaromzet van de onderneming. Dit introduceert ook een prikkel tot nakoming bij grote ondernemingen zoals Google-moederbedrijf Alphabet (jaaromzet 2022: € 260 miljard) of Apple (jaaromzet 2022: € 359 miljard).

Boetes aan particulieren. Ook particulieren kunnen de AVG overtreden wanneer hun verwerking de privésfeer ontstijgt (artikel 2 lid 2 punt c). Levert een boete aan een particulier een onevenredige last op (overweging 148), dan ligt een berisping meer voor de hand. Verder moet de toezichthoudende autoriteit bij het bepalen van een passend bedrag voor de geldboete rekening houden met het algemene inkomensniveau in de lidstaat en de economische situatie van de persoon in kwestie. Zo is in België een boete opgelegd aan een stel dat thuis camera's had opgehangen die gericht waren op de openbare weg en de burens.

Boetes aan overheden. Ook overheidsorganen (behalve rechtbanken) zijn onderworpen aan toezicht op hun naleving van de AVG. Boetes kunnen echter alleen aan overheidsorganen worden opgelegd als dat in het nationaal recht uitgewerkt is (zie lid 7). In Nederland is dit mogelijk gemaakt onder artikel 18 Uitvoeringswet.

Zo legde de AP in 2021 een boete aan de Gemeente Enschede op van 600.000 euro voor onrechtmatig gebruik van wifi tracking in de stad, en legde de AP in 2022 een boete van 3,7 miljoen aan de Belastingdienst voor het onrechtmatig gebruik van een zwarte lijst door de Fraude Signalering Voorziening.

Boetebeleid. Toezichthouders kunnen naar eigen inzicht boetebeleid opstellen. Lid 2 biedt een aantal factoren die daarin mee moeten wegen. Het coherentiemechanisme (artikel 63) vereist wel dat toezichthouders hun boetebeleid op elkaar afstemmen, om zo een consequente toepassing van administratieve geldboeten te realiseren. Het Comité kan richtsnoeren opstellen betreffende de vaststelling van administratieve geldboeten overeenkomstig artikel 83 (artikel 70 lid 1 punt k).

Andere straffen. Lidstaten mogen naast de administratieve sancties uit dit artikel ook eigen straffen invoeren ter handhaving van de AVG (artikel 84). Dit zal met name strafrechtelijke sancties betreffen. Doxing, het online publiceren van iemands persoonsgegevens met het doel om die persoon te intimideren, wordt in een (ten tijde van het schrijven van dit boek) recent goedgekeurd wetsvoorstel strafbaar gesteld. Hoewel er niet specifiek gerefereerd wordt aan de AVG voor de strafbaarstelling, was doxing uiteraard al een inbreuk op de AVG welke nu ook strafbaar is gesteld.

Bestuurlijke boete. Administratieve sancties, zoals neergelegd in dit artikel van de AVG worden aangemerkt als bestuurlijke boetes in de zin van artikel 5:40 van de Awb (artikel 14, lid 3 Uitvoeringswet).

Last onder bestuursdwang. Naast de administratieve sancties neergelegd in dit artikel, welke worden aangemerkt als bestuurlijke boetes, wordt het de AP in de Uitvoeringswet ook toegestaan om een last onder bestuursdwang (art. 5:20 lid 1 Awb) op te leggen in dezelfde gevallen (artikel 16 Uitvoeringswet).

83.2 Administratieve geldboeten worden, naargelang de omstandigheden van het concrete geval, opgelegd naast of in plaats van de in artikel 58, lid 2, punten a) tot en met h) en j), bedoelde maatregelen. Bij het besluit over de vraag of een administratieve geldboete wordt opgelegd en over de hoogte daarvan wordt voor elk concreet geval naar behoren rekening gehouden met het volgende:

Bij het opleggen van een boete dient de toezichthouder gemotiveerd aan te geven hoe men aan het betreffende bedrag komt. Dit zal zich vertalen in uitgebreid boetebeleid dat per punt uit dit lid 2 aangeeft hoe het moet worden meegewogen. Dit beleid zal (artikel 63) tussen toezichthouders moeten worden afgestemd. Het Comité kan richtsnoeren opstellen betreffende de vaststelling van administratieve geldboeten overeenkomstig artikel 83 (artikel 70 lid 1 punt k).

Nederland, boetebeleid. Op 19 februari 2019 publiceerde de Autoriteit Persoonsgegevens haar langverwachte boetebeleid (Stc. 14 maart 2019, nr. 14586).

Zij verdeelt de boeteruimte in vier bandbreedtes voor de administratief georiënteerde overtredingen (lid 4) en drie voor de meer principiële overtredingen (lid 5). Een overtreding wordt naar haar ernst eerst in een bandbreedte ingedeeld, waarna het boetebedrag als afwijking van het midden van de bandbreedte wordt gekozen op basis van relevante factoren bij de overtreding.

83.2(a) de aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;

De belangrijkste factoren bij het opleggen van een boete zijn de aard, ernst en duur van de inbreuk. Dit wordt met name gemeten naar het aantal getroffen betrokkenen en de door hen geleden schade. Vergelijk de criteria voor een DPIA uit artikel 35 lid 1.

83.2(b) de opzettelijke of nalatige aard van de inbreuk;

Wanneer de verwerkingsverantwoordelijke of de verwerker opzettelijk of nalatig handelde, zal dit een boeteverhogende omstandigheid opleveren. Zie over deze begrippen nader lid 3.

83.2(c) de door de verwerkingsverantwoordelijke of de verwerker genomen maatregelen om de door betrokkenen geleden schade te beperken;

Een verwerkingsverantwoordelijke of verwerker kan de boete proberen te dempen door maatregelen te nemen om geleden schade te beperken. De mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 25 en 32 zal hierbij zwaar wegen.

83.2(d) eerdere relevante inbreuken door de verwerkingsverantwoordelijke of de verwerker;

Recidive bij een vergelijkbare soort inbreuken zal een boeteverzwarende omstandigheid opleveren.

83.2(e) de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;

Medewerking met de toezichthouder is een boeteverzachtende omstandigheid, hoewel medewerking eigenlijk sowieso al verplicht is (artikel 31).

83.2(f) de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;

Het soort persoonsgegevens is ook een belangrijke factor bij de bepaling van de ernst van de overtreding. Zeker wanneer het gaat om bijzondere persoons-

gegevens (artikel 9) of strafrechtelijke persoonsgegevens (artikel 10) zal dit een boeteverhogende omstandigheid opleveren. Zo werd in 2021 door de AP een boete opgelegd van 725.000 euro aan een onbekend bedrijf voor het gebruik van biometrische gegevens (vingerafdrukken) voor het in- en uitklokken op werk waarbij dat niet noodzakelijk was (Autoriteit Persoonsgegevens, 30 april 2020, Boete vingerafdrukken personeel).

83.2(g) de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke of de verwerker de inbreuk heeft gemeld;

Om een prikkel te bieden om zelf zo snel mogelijk schendingen van de AVG te melden, wordt de wijze van ter kennis komen bij de toezichthouder als mogelijk boeteverlagende omstandigheid opgenomen.

83.2(h) de naleving van de in artikel 58, lid 2, genoemde maatregelen, voor zover die eerder ten aanzien van de verwerkingsverantwoordelijke of de verwerker in kwestie met betrekking tot dezelfde aangelegenheid zijn genomen;

Wanneer een verwerkingsverantwoordelijke of verwerker eerder een corrigerende maatregel (artikel 58 lid 2) opgelegd kreeg, en deze keurig opgevolgd heeft, dan zal dat boeteverlagend kunnen werken. Daar staat tegenover dat het niet naleven van zo'n maatregel natuurlijk boeteverhogend werkt. Er kan zelfs een extra boete worden opgelegd voor dit feit (zie lid 6).

83.2(i) het aansluiten bij goedgekeurde gedragscodes overeenkomstig artikel 40 of van goedgekeurde certificeringsmechanismen overeenkomstig artikel 42; en

Het volgen van gedragscodes of het gebruik van certificeringsmechanismen voorkomt op zich niet dat boetes mogen worden opgelegd. Wel zal dit uiteraard een boeteverlagende omstandigheid opleveren.

83.2(j) elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.

Een toezichthouder mag (en moet) ook alle andere relevante factoren betrekken in het boetebesluit.

83.3 Indien een verwerkingsverantwoordelijke of een verwerker opzettelijk of uit nalatigheid met betrekking tot dezelfde of daarmee verband houdende verwerkingsactiviteiten een inbreuk pleegt op meerdere bepalingen van deze verordening, is de totale geldboete niet hoger dan die voor de zwaarste inbreuk.

Opzettelijk of nalatig handelen is een boeteverzwarende omstandigheid (lid 2 punt b). Lid 3 trekt echter een streep bij een verhoging tot de boete voor de

zwaarste soort inbreuk. Extra opslagen (zoals Amerikaanse *punitive damages*) bij overtredingen uit opzet of nalatigheid zijn dus niet toegestaan.

83.4 Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 10 000 000 EUR of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is:

83.4(a) de verplichtingen van de verwerkingsverantwoordelijke en de verwerker overeenkomstig de artikelen 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 en 43;

83.4(b) de verplichtingen van het certificeringsorgaan overeenkomstig de artikelen 42 en 43;

83.4(c) de verplichtingen van het toezichthoudend orgaan overeenkomstig artikel 41, lid 4.

De AVG kent twee categorieën overtredingen. Lid 4 beschrijft categorie 1, de wat meer administratief georiënteerde verplichtingen. Lid 5 hieronder beschrijft categorie 2, de meer principiële verplichtingen zoals het verkrijgen van toestemming en doorgifte aan derde landen.

83.5 Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is:

83.5(a) de basisbeginselen inzake verwerking, met inbegrip van de voorwaarden voor toestemming, overeenkomstig de artikelen 5, 6, 7 en 9;

83.5(b) de rechten van de betrokkenen overeenkomstig de artikelen 12 tot en met 22;

83.5(c) de doorgiften van persoonsgegevens aan een ontvanger in een derde land of een internationale organisatie overeenkomstig de artikelen 44 tot en met 49;

83.5(d) alle verplichtingen door de lidstaten vastgesteld krachtens hoofdstuk IX;

83.5(e) niet-naleving van een bevel of een tijdelijke of definitieve verwerkingsbeperking of een opschorting van gegevensstromen door de toezichthoudende autoriteit overeenkomstig artikel 58, lid 2, of niet-verlening van toegang in strijd met artikel 58, lid 1.

De hoge categorie boetewaardige overtredingen betreft de meer principiële verplichtingen zoals het naleven van de beginselen (artikel 5), het hebben van een grondslag voor verwerking (artikel 6), het nakomen van de rechten van betrok-

kenen (artikelen 12-22), doorgifte naar buiten de EU (artikelen 44-49), de gedelegeerde bevoegdheden uit hoofdstuk 9 en het niet nakomen van bevelen van een toezichthouder (artikel 58 leden 1 en 2, zie ook lid 6 hieronder). De meer administratief georiënteerde verplichtingen staan hierboven in lid 4.

- 83.6 Niet-naleving van een bevel van de toezichthoudende autoriteit als bedoeld in artikel 58, lid 2, is overeenkomstig lid 2 van dit artikel onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

Onder artikel 58 lid 2 kan een toezichthouder diverse bevelen geven, zoals het inwilligen van verzoeken tot inzage, rectificatie of gegevenswissing, het melden van een datalek, het staken van een verwerking of meer algemeen het herstellen van een tekortkoming bij de nakoming van de AVG. Het niet naleven van zo'n bevel levert een overtreding van dezelfde ernst als de categorie 2-overtredingen van lid 5 op.

- 83.7 Onverminderd de bevoegdheden tot het nemen van corrigerende maatregelen van de toezichthoudende autoriteiten overeenkomstig artikel 58, lid 2, kan elke lidstaat regels vaststellen betreffende de vraag of en in hoeverre administratieve geldboeten kunnen worden opgelegd aan in die lidstaat gevestigde overheidsinstanties en overheidsorganen.

Een toezichthouder kan overheidsorganen corrigerende maatregelen opleggen (artikel 58 lid 2), zoals waarschuwingen, stakingsbevelen of het wissen van persoonsgegevens. Dit geldt niet voor rechtbanken (artikel 55 lid 3). Op grond van dit lid 7 is het opleggen van administratieve boetes aan overheidsinstanties alleen mogelijk als het nationaal recht daarin voorziet.

Nederland. In theorie is het onder de Awb mogelijk dat een overheidsorgaan een bestuursrechtelijke boete opgelegd krijgt. In de praktijk komt dit niet voor.

- 83.8 De uitoefening door de toezichthoudende autoriteit van haar bevoegdheden uit hoofde van dit artikel is onderworpen aan passende procedurele waarborgen overeenkomstig het Unierecht en het lidstatelijke recht, waaronder een doeltreffende voorziening in rechte en een eerlijke rechtsbedeling.

Toezichthouders mogen alleen opereren binnen passende procedurele waarborgen, welke onder meer moeten voorzien in het instellen van beroep bij een onafhankelijke rechter. In Nederland zijn deze waarborgen opgenomen in de procedurele regels uit de Awb.

83.9 Wanneer het rechtssstelsel van de lidstaat niet voorziet in administratieve geldboeten, kan dit artikel aldus worden toegepast dat geldboeten worden geïnitieerd door de bevoegde toezichthoudende autoriteit en opgelegd door bevoegde nationale gerechten, waarbij wordt gewaarborgd dat deze rechtsmiddelen doeltreffend zijn en eenzelfde effect hebben als de door toezichthoudende autoriteiten opgelegde administratieve geldboeten. De boeten zijn in elk geval doeltreffend, evenredig en afschrikkend. Die lidstaten delen de Commissie uiterlijk op [25 mei 2018, twee jaar vanaf de datum van inwerkingtreding van deze verordening] de wetgevingsbepalingen mee die zij op grond van dit lid vaststellen, alsmede onverwijld alle latere wijzigingen daarvan en alle daarop van invloed zijnde wijzigingswetgeving.

De rechtssystemen van Denemarken en Estland kennen geen systeem van administratieve geldboeten. Daarom is voor een creatieve invulling gekozen (overweging 151): de boete wordt in Denemarken ingestoken als een strafrechtelijke sanctie door een bevoegd gerecht, en in Estland in het kader van een procedure voor strafbare feiten door de toezichthoudende autoriteit. Dit moet hetzelfde gevolg hebben als in andere lidstaten waar administratieve geldboeten door de toezichthouders worden opgelegd. De bevoegde Deense en Estse gerechten moeten dan ook rekening houden met de aanbeveling van de toezichthoudende autoriteit die de boete heeft geïnitieerd.

Details van de procedure moeten aan de Commissie worden gemeld. De Commissie kan geen bezwaar maken. Uiteraard dient deze wetgeving wel te voldoen aan de AVG en het Unierecht, anders kan de Commissie deze via de verdragschendingsprocedure (artikel 258 en 259 VWEU) aanvechten.

Artikel 84. Andere sancties

84.1 De lidstaten stellen de regels inzake andere sancties vast die van toepassing zijn op inbreuken op deze verordening, in het bijzonder op inbreuken die niet aan administratieve geldboeten onderworpen zijn overeenkomstig artikel 83, en treffen alle nodige maatregelen om ervoor te zorgen dat zij worden toegepast. Die sancties zijn doeltreffend, evenredig en afschrikkend.

Lidstaten zijn bevoegd om eigen sancties in te voeren bij inbreuken op de AVG. Dit mogen ook strafrechtelijke sancties zijn of winstafracht (overweging 149). Ook deze sancties dienen doeltreffend, evenredig en afschrikkend te zijn (zie artikel 83 lid 1). Deze andere sancties mogen ook aan de verwerker worden opgelegd (artikel 28 lid 10).

Niet onderworpen aan geldboeten. Deze bevoegdheid is met name bedoeld voor situaties waarin de AVG niet zelf een sanctie op inbreuk stelt (zie artikel 83 leden 4 en 5), met name de onbevoegde verwerking van strafrechtelijke persoons-

gegevens (artikel 10) en de algemene verplichtingen van de verwerkingsverantwoordelijke (artikel 24). In Nederland kan de AP voor overtredingen van artikel 10 een bestuurlijke boete opleggen van maximaal 20.000.000 euro, of 4% van de totale wereldwijde jaaromzet (artikel 17 Uitvoeringswet).

Ne bis in idem. Dergelijke sancties aan wél gereguleerde artikelen zijn echter in principe mogelijk, zij het dat daarmee natuurlijk niet het ne-bis-in-idem-beginsel, zoals uitgelegd door het Hof van Justitie (onder meer HvJ EU 26 februari 2013, ECLI:EU:C:2013:105, Åklagaren) mag worden geschonden. Dit gebeurde bij de boete uitgedeeld door de Ierse toezichthouder aan Meta voor onrechtmatig verwerkte persoonsgegevens door hun applicatie WhatsApp op 12 januari 2023. Hoewel WhatsApp (onder andere) het beginsel van transparantie uit artikel 5 schond, was de boete “maar” 5,5 miljoen euro. Het beginsel van transparantie is een principieel beginsel, waarvoor volgens artikel 83 lid 5, relatief hogere boetes mogen worden opgelegd. Omdat de Ierse toezichthouder al eerder een boete hiervoor had opgelegd in 2021 en er niet twee keer een boete voor hetzelfde feit mag worden opgelegd, is de verhoging van de boete op basis van deze schending echter niet meegenomen. Vraagtekens lijken terecht bij of dit de juiste invulling is van het ‘ne bis in idem’ beginsel. Zeker gezien het feit dat boetes corrigerend moeten werken, en op deze wijze en organisatie – twee jaar nadat zij beboet werd – ongestraft door kan gaan met een inbreuk, zonder dat daar repercussies voor bestaan als er geen last onder dwangsom is opgelegd.

Nederland. In Nederland was overtreding van artikelen 4 (onrechtmatige verwerking van Nederlandse persoonsgegevens vanuit het buitenland) en 78 (doorgifte naar land zonder passend beschermingsniveau) van de Wbp een strafbaar feit (artikel 75 Wbp). Gezien de focus op bestuursrechtelijke handhaving ligt het niet voor de hand dat Nederland onder dit artikel 84 bepalingen van strafrecht zal invoeren ter handhaving van de AVG. De Uitvoeringswet bevat geen bepalingen van strafrecht.

84.2 Elke lidstaat deelt de Commissie uiterlijk [25 mei 2018, twee jaar vanaf de datum van inwerkingtreding van deze verordening] de overeenkomstig lid 1 vastgestelde wetgevingsbepalingen mee, alsook onverwijld alle latere wijzigingen daarvan.

Nadat een lidstaat eigen sanctieregels heeft ingevoerd, moeten deze worden gemeld aan de Commissie. Deze mededeling is informatief; de Commissie kan niet onder de AVG bezwaar maken. Uiteraard dient deze wetgeving wel te voldoen aan de AVG en het Unierecht, anders kan de Commissie deze via de verdragsschendingsprocedure (artikel 258 en 259 VWEU) aanvechten.

Hoofdstuk IX

Specifieke verwerkingen

Tijdens de totstandkoming van de AVG kon men het op een aantal punten niet eens worden. Er is voor gekozen om deze punten open te laten in de AVG en de lidstaten de bevoegdheid te geven om eigen wettelijke regelingen te treffen om zo hun eigen keuzes vast te leggen.

Voor al de relatie tot de informatievrijheid (art. 11 Handvest, art. 10 EVRM) bleek een heikel punt. Artikel 85 biedt de bevoegdheid om van de AVG afwijkende regels op te nemen als dat nodig is om de uitingsvrijheid of informatievrijheid te beschermen (artikel 85) of om openbaarheid van bestuur en toegang tot openbare registers te borgen (artikel 86). Lidstaten mogen ook eigen nadere waarborgen en afwijkingen treffen in verband met archivering in het algemeen belang en voor wetenschappelijk of historisch onderzoek of statistische doeleinden (artikel 89).

Ook bij andere wetgeving kunnen botsingen ontstaan, zoals ten aanzien van het nationaal identificatienummer (artikel 87), verwerking van persoonsgegevens in het arbeidsrecht (artikel 88) en wettelijke geheimhoudings- en verschoningsrechten (artikel 90). Als laatste is opgenomen dat bestaande gegevensbeschermingsregels van kerken en religieuze verenigingen in stand blijven (artikel 91).

Artikel 85. Verwerking en vrijheid van meningsuiting en van informatie

85.1 De lidstaten brengen het recht op bescherming van persoonsgegevens overeenkomstig deze verordening wettelijk in overeenstemming met het recht op vrijheid van meningsuiting en van informatie, daaronder begrepen de verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen.

Ook een journalistieke, academische, artistieke of literaire uiting kan persoonsgegevens bevatten. Denk aan een online nieuwsartikel, een kunstcollage met iemands portret of een doorzoekbaar krantenarchief. Denkbaar is dat een strikte uitleg van de AVG dan oplevert dat de verwerking onrechtmatig is. Bij dergelijke uitingen wordt immers zelden adequaat geïnformeerd, beveiliging is afwezig en recht van correctie of wissing wordt niet gegund. Staken van de verwerking levert echter een inperking op van de vrijheid van meningsuiting, net als privacy een grondrecht (artikel 11 Handvest grondrechten EU). Met dit artikel 85 hebben lidstaten de mogelijkheid nadere wetgeving te treffen om hier een betere balans te treffen in te perken.

Journalistieke doeleinden. Men verwerkt voor journalistieke doeleinden indien de verwerking als enig doel heeft de bekendmaking aan het publiek van informatie, meningen of ideeën, ongeacht het overdrachtsmedium. Deze activiteiten zijn niet voorbehouden aan mediaondernemingen en kunnen een winstoogmerk hebben (HvJ EU 16 december 2008, ECLI:EU:C:2008:727, Satamedia). Ook online media, zoals blogs, kunnen dus journalistiek verwerken (HR 18 januari 2013, ECLI:NL:HR:2008:BB3210, Van Gasteren/Hemelrijk). Het concept ‘uitingsvrijheid’ en al daarmee samenhangt moet ruim worden uitgelegd (overweging 153).

Botsende grondrechten. Het spanningsveld tussen de privacy en de uitingsvrijheid is een klassiek voorbeeld van botsende grondrechten. Grondrechten zijn gelijkwaardig (Hoge Raad 18 januari 2008, ECLI:NL:HR:2008:BB3210, Van Gasteren/Hemelrijk) en de rechter moet een botsing beoordelen aan de hand van alle omstandigheden van het geval. De botsing kan bijvoorbeeld worden opgelost door de uitingsvrijheid horizontaal door te laten werken in bijvoorbeeld de toets voor een eigen dringend belang (artikel 6 lid 1 punt f). Ook kunnen rechten van betrokkenen (zoals rectificatie) buiten toepassing worden gelaten als de uitingsvrijheid dit vereist.

“Data protection is the new libel.” Een concrete zorg geuit bij invoering van de AVG is dat de regels over persoonsgegevens zeer streng zijn (zeker vanwege de hoge boetes) en daarmee een afschrikwekkende optie zouden bieden om onwelgevallige uitingen te doen verwijderen. Een beroep op bijvoorbeeld een inadequate beveiliging of een recht van correctie of verwijdering passeert de inhoudelijke belangenafweging die bij een onrechtmatige perspublicatie hoort, zodat de journalist op achterstand zou staan. In Nederland is deze zorg niet aan de orde; al in 2011 bepaalde het Gerechtshof 's-Hertogenbosch dat de Wbp geen extra grondslag biedt om de rechtmatigheid van een perspublicatie mee aan te vechten wanneer deze onder de ‘gewone’ belangenafweging rechtmatig is (1 februari 2011, ECLI:NL:GHSHE:2011:BP3921, Kleintje Muurkrant). Zie ook EHRM 16 juli 2013, zaaknr. 33846/07 (Wegrzynowski).

- 85.2 Voor verwerking voor journalistieke doeleinden of ten behoeve van academische, artistieke of literaire uitdrukkingvormen stellen de lidstaten uitzonderingen of afwijkingen vast van hoofdstuk II (beginselen), hoofdstuk III (rechten van de betrokkene), hoofdstuk IV (de verwerkingsverantwoordelijke en de verwerker), hoofdstuk V (doorgifte van persoonsgegevens naar derde landen of internationale organisaties), hoofdstuk VI (onafhankelijke toezichthoudende autoriteiten), hoofdstuk VII (samenwerking en coherentie) en hoofdstuk IX (specifieke gegevensverwerkingssituaties) indien deze noodzakelijk zijn om het recht op bescherming van persoonsgegevens in overeenstemming te brengen met de vrijheid van meningsuiting en van informatie.

Wanneer lidstaten eigen wetgeving willen invoeren ter versterking van de uitingsvrijheid binnen het kader van de AVG, zijn in beginsel afwijkingen op elk

artikel van de AVG mogelijk. Te denken valt aan een nadere invulling van de grondslag van de eigen dringende noodzaak (artikel 6 lid 1 punt f) of een uitzondering voor journalistieke verwerking van strafrechtelijke persoonsgegevens (artikel 10). Lidstaten zouden ook kunnen bepalen dat de toezichthouder niet of beperkt bevoegd is om op te treden bij journalistieke verwerkingen (artikel 58).

Uitzonderingen. Uitzonderd zijn hoofdstukken I en VIII (en X en XI, maar die hebben geen relevantie voor de uitingsvrijheid). Lidstaten kunnen dus niet bijvoorbeeld de journalistieke verwerking als geheel buiten de AVG plaatsen, aangezien dat strijd met artikel 2 AVG (uit hoofdstuk I) oplevert. Ook kunnen lidstaten niet opnemen dat journalistieke verwerkingen niet mogen worden beboet (artikel 83, hoofdstuk VIII).

Gegevenswissing. Het recht op gegevenswissing, ook wel het vergeetrecht (artikel 17) bevat al een eigen beperking ten aanzien van journalistieke verwerkingen: wanneer een verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie, kan geen beroep op dit recht worden gedaan (artikel 17 lid 3 punt a). Dit is in lijn met EHRM-jurisprudentie over het belang van archieven (EHRM 10 maart 2009, gevoegde zaken 3002/03 en 23676/03, *Times* en EHRM 16 juli 2013, zaaknr 33846/07, *Węgrzynowski*).

Nederland. In de Uitvoeringswet (artikel 43) wordt een groot aantal onderdelen uit de AVG uitgezonderd ten behoeve van de verwerking van persoonsgegevens voor academische, artistieke of literaire uitdrukingsvormen. Met name worden uitgezonderd: het recht om toestemming in te trekken (artikel 7 lid 3), de verwerking van bijzondere persoonsgegevens (artikel 9), de verwerking van strafrechtelijke gegevens (artikel 10), het verstrekken van aanvullende gegevens ter identificatie (artikel 11 lid 2), rechten van de betrokkene (hoofdstuk III), de bepalingen ten aanzien van de verwerkingsverantwoordelijke en de verwerker (hoofdstuk IV, met uitzondering van artikelen 24, 25, 28, 29 en 32), de bepalingen betreffende de doorgifte van persoonsgegevens aan derde landen of internationale organisaties (hoofdstuk V), de bepalingen omtrent toezichthoudende autoriteiten (hoofdstuk VI) en de bepalingen betreffende samenwerking en coherentie tussen toezichthoudende autoriteiten (hoofdstuk VII).

85.3 Elke lidstaat deelt de Commissie de overeenkomstig lid 2 vastgestelde wetgevingsbepalingen mee, alsook onverwijld alle latere wijzigingen daarvan.

Nadat een lidstaat eigen sanctieregels heeft ingevoerd, moeten deze worden gemeld aan de Commissie. Deze mededeling is informatief; de Commissie kan niet onder de AVG bezwaar maken. Uiteraard dient deze wetgeving wel te voldoen aan de AVG en het Unierecht, anders kan de Commissie deze via de verdragsschendingsprocedure (artikel 258 en 259 VWEU) aanvechten.

Artikel 86. Verwerking en recht van toegang van het publiek tot officiële documenten

Persoonsgegevens in officiële documenten die voor de uitvoering van een taak van algemeen belang in het bezit zijn van een overheidsinstantie, een overheidsorgaan of een particulier orgaan, mogen door de instantie of het orgaan in kwestie worden bekendgemaakt in overeenstemming met het Unierecht of het lidstatelijke recht dat op de overheidsinstantie of het orgaan van toepassing is, teneinde het recht van toegang van het publiek tot officiële documenten in overeenstemming te brengen met het recht op bescherming van persoonsgegevens uit hoofde van deze verordening.

Een overheidsinstantie of -orgaan kan in het algemeen belang het publiek toegang bieden tot officiële documenten waarin persoonsgegevens zijn opgenomen. Dit betreft zowel toegang tot registers zoals het Handelsregister of het BIG-register voor zorgverleners als meer algemene overheidsdocumenten. Dit is toegestaan onder de AVG wanneer het Europees of nationaal recht een wettelijke regeling kent over deze toegang. Deze wettelijke regeling moet de AVG nader uitwerken (zie nader artikel 6 lid 1 punt e over het begrip ‘algemeen belang’.)

Balans tussen privacy en openbaar belang. Een dergelijke regeling moet een balans treffen tussen het openbaar belang gediend bij die openbaarheid en de privacy van betrokkenen. In de praktijk wordt dit meestal geregeld door toegang als hoofdregel te stellen, en een uitzonderingsgrond met belangenafweging op te nemen wanneer persoonsgegevens aan de orde zijn. In Nederland bepaalt artikel 5,1 lid 1 punt d Wet open overheid bijvoorbeeld dat het verstrekken van overheidsinformatie achterwege blijft voor zover het gaat om persoonsgegevens, tenzij de betrokkene uitdrukkelijk toestemming gaf voor de openbaarmaking of de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt. De Archiefwet bevat in artikel 2a een beperkte uitzondering op het verbod tot verwerken van bijzondere persoonsgegevens (artikel 9) voor zover noodzakelijk voor beheer en bewaring van archiefstukken.

Openbaarheid van bestuur. Naast toegang tot registers ziet dit artikel 86 ook op toegang tot overheidsinformatie in het algemeen: openbaarheid van bestuur. Deze toegang is met name geregeld in Richtlijn 2003/98/EG inzake hergebruik van overheidsinformatie (in Nederland geïmplementeerd als de Wet hergebruik van overheidsinformatie). De AVG stelt zichzelf boven deze Richtlijn (overweging 154) en alle inzage en hergebruik moeten dus binnen het kader van de AVG worden beoordeeld. Inzage en hergebruik geldt niet voor documenten die uitsluitend persoonsgegevens bevatten, maar ook niet voor documenten met andere informatie wanneer deze tevens persoonsgegevens bevatten en wettelijk is vastgelegd dat daarvan geen hergebruik is toegestaan.

De overheidsinstantie die toegang wil verlenen tot documenten met persoonsgegevens, moet aantonen (1) dat er toestemming is van de betrokkenen of een andere wettelijke grondslag (artikel 6), (2) dat de toegang noodzakelijk en proportioneel is (artikel 5), (3) dat de betrokkene vooraf wordt geïnformeerd over deze verstrekking zodat hij bezwaar kan maken (artikel 21). Daarnaast moet de verzoeker van de informatie aantonen dat een belangenafweging in het voordeel van openbaarmaking uitvalt. Zie nader de *Bavarian Lager*-zaak (HvJ EU, ECLI:EU:C:2010:378, 29 juni 2010).

Overheidsinstanties. De verwijzing naar overheidsinstanties en -organen verwijst naar alle autoriteiten en andere organen die onder nationaal recht het publiek toegang moeten geven tot hun informatie. In Nederland betreft dit dus alle bestuursorganen en alle onder de verantwoordelijkheid van een bestuursorgaan werkzame instelling, dienst of bedrijf (artikel 2.1 jo. 4.1 lid 1 Wet open overheid). Dit artikel 86 geldt echter ook voor particuliere instanties die informatie bezitten die het algemeen belang dient, zoals de Stichting Internet Domeinregistratie Nederland (SIDN) die het houderregister van .nl-domeinnamen beheert.

Artikel 87. Verwerking van het nationaal identificatienummer

De lidstaten kunnen de specifieke voorwaarden voor de verwerking van een nationaal identificatienummer of enige andere identificator van algemene aard nader vaststellen. In dat geval wordt het nationale identificatienummer of enige andere identificator van algemene aard alleen gebruikt met passende waarborgen voor de rechten en vrijheden van de betrokkene uit hoofde van deze verordening.

Vrijwel alle lidstaten kennen een of ander nationaal identificatienummer voor haar burgers. In Nederland is dit bijvoorbeeld het Burgerservicenummer (BSN). Lidstaten mogen nadere regels stellen over de verwerking van dit nummer, dat immers ook een persoonsgegeven vormt.

BSN als persoonsgegeven. De Wet algemene bepalingen burgerservicenummer (Wabb) stelt in artikel 2: *“Het burgerservicenummer bevat geen informatie over de persoon aan wie het is toegekend.”* Abusievelijk wordt daardoor vaak gedacht dat een BSN geen persoonsgegeven is. Dit is onjuist; zowel onder de Wet bescherming persoonsgegevens (Wbp) als onder de AVG is een BSN een persoonsgegeven. Het nummer is immers altijd te koppelen aan informatie over de burger in kwestie, en is daarmee een persoonsgegeven (artikel 4 definitie 1).

Geen bijzonder persoonsgegeven. Onder de Wbp werd het BSN aangemerkt als een bijzonder persoonsgegeven. De AVG doet dit niet. In de praktijk zal het BSN in de context van haar gebruik vaak toch een bijzonder persoonsgegeven opleveren, bijvoorbeeld in de zorg (zie artikel 4 definitie 15).

Gebruik BSN. In de Uitvoeringswet (artikel 46) is bepaald dat het BSN enkel mag worden verwerkt indien dit is gebaseerd op een wettelijke grondslag. Voor de verwerking van een BSN door de overheid is deze wettelijke grondslag neergelegd in artikel 10 Wabb. Voor overige instellingen, welke geen beroep kunnen doen op de Wabb, dient het gebruik van een BSN te zijn voorgeschreven in sectorale wetgeving. De Uitvoeringswet introduceert geen nadere regelgeving ten aanzien van het BSN (MvT Uitvoeringswet, p. 59).

Artikel 88. Verwerking in het kader van de arbeidsverhouding

88.1 Bij wet of bij collectieve overeenkomst kunnen de lidstaten nadere regels vaststellen ter bescherming van de rechten en vrijheden met betrekking tot de verwerking van de persoonsgegevens van werknemers in het kader van de arbeidsverhouding, in het bijzonder met het oog op aanwerving, de uitvoering van de arbeidsovereenkomst, met inbegrip van de naleving van wettelijke of uit collectieve overeenkomsten voortvloeiende verplichtingen, het beheer, de planning en de organisatie van de arbeid, gelijkheid en diversiteit op het werk, gezondheid en veiligheid op het werk, bescherming van de eigendom van de werkgever of de klant dan wel met het oog op de uitoefening en het genot van de met de arbeidsverhouding samenhangende individuele of collectieve rechten en voordelen, en met het oog op de beëindiging van de arbeidsverhouding.

Lidstaten kunnen op hun grondgebied eigen nadere regels stellen over de omgang met persoonsgegevens binnen de arbeidsverhouding. Te denken valt aan persoonsgegevens die werkgevers aan de overheid moeten verstrekken, zoals in Nederland onder de Wet op de identificatieplicht in het kader van bestrijding van zwartwerken.

Wet of collectieve overeenkomst. De lidstaten kunnen deze nadere regels in een wet (in materiële zin) vastleggen, maar ook een collectieve arbeidsovereenkomst (cao) mag dergelijke regels stellen.

Doel van de regeling. Lid 1 staat in beginsel elke soort regeling toe, zolang deze maar niet in strijd is met de AVG. De genoemde grondslagen zoals organisatie van de arbeid, gelijkheid en diversiteit zijn illustratieve voorbeelden.

88.2 Die regels omvatten passende en specifieke maatregelen ter waarborging van de menselijke waardigheid, de gerechtvaardigde belangen en de grondrechten van de betrokkene, met name wat betreft de transparantie van de verwerking, de doorgifte van persoonsgegevens binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen en toezichtsystemen op het werk.

De nadere regels mogen afwijken van de AVG. Zo is het bijvoorbeeld toegestaan te bepalen dat werkgevers ter promotie van diversiteit op de werkvloer

bijzondere persoonsgegevens mogen verwerken zoals ras, etnische afkomst of seksuele gerichtheid. De regels moeten wel binnen de beginselen (artikel 5) van de AVG blijven.

Nederland, gezondheidsgegevens. In de Uitvoeringswet wordt het werkgevers toegestaan in beperkte mate gegevens over gezondheid te verwerken (artikel 30) als dat noodzakelijk is voor een goede uitvoering van wetten of regelingen over re-integratie of gezondheid van werknemers.

88.3 Elke lidstaat deelt de Commissie uiterlijk op [25 mei 2018, twee jaar vanaf de datum van inwerkingtreding van deze verordening] de overeenkomstig lid 1 vastgestelde wetgevingsbepalingen mee, alsook onverwijld alle latere wijzigingen daarvan.

Nadat een lidstaat regels heeft gesteld over persoonsgegevens bij arbeidsovereenkomsten, moeten deze regels worden gemeld aan de Commissie. Deze mededeling is informatief; de Commissie kan niet direct bezwaar maken. Uiteraard dient deze wetgeving wel te voldoen aan de AVG en het Unierecht, anders kan de Commissie deze via de verdragsschendingsprocedure (artikel 258 en 259 VWEU) aanvechten. Regelingen in cao's hoeven niet te worden gemeld.

Artikel 89. Waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden

89.1 De verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met deze verordening voor de rechten en vrijheden van de betrokkene. Die waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt.

Het uitvoeren van wetenschappelijk, historisch of statistisch onderzoek en het beheer van archieven in het algemeen belang is van groot belang voor de maatschappij. Vandaar dat een speciale positie in de AVG wordt gecreëerd voor deze activiteiten. Deze zijn in beginsel mogelijk, zij het dat er passende waarborgen moeten worden getroffen om betrokkenen te beschermen. Natuurlijk moet er nog wel een passende grondslag (zoals toestemming) zijn voor het onderzoek. Nationaal en Europees recht mag wetgeving introduceren waarbij wordt afgeweken van de rechten van betrokkenen (lid 2 en 3).

Passende waarborgen. Verwerkingen onder het kopje van onderzoek en archivering dienen onderworpen te zijn aan passende waarborgen voor de rechten en vrijheden van de betrokkenen. Zie artikel 24 voor de algemene norm voor dergelijke waarborgen. Het accent ligt echter bij het beginsel van gegevensminimalisering (artikel 5 lid 1 punt c).

Minimale gegevensverwerking. Het beginsel van dataminimalisatie (artikel 5 lid 1 punt c) betekent dat niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is voor het doel. Dit beginsel geldt onverkort voor onderzoek en archivering. Zodra het mogelijk is het onderzoeks- of archiveringsdoel te halen met ontkoppelde gegevens (die dus niet langer persoonsgegevens zijn), moet deze ont koppeling worden uitgevoerd. Als tussenvorm mag worden gewerkt met pseudonimisering (artikel 4 definitie 5) waarbij koppeling nog wel mogelijk is, maar de daarvoor benodigde informatie niet direct beschikbaar is.

Verenigbaarheid. Het beginsel van doelbinding (artikel 5 lid 1 punt b) vereist dat persoonsgegevens niet verder mogen worden verwerkt voor een doel dat onverenigbaar is met het originele doel. Echter, de verwerkingen bedoeld in dit artikel 89 worden per definitie als niet onverenigbaar aangemerkt.

Informeren van betrokkenen. Onderzoekers en archivariissen hoeven betrokkenen niet te informeren onder artikel 14 over de verkregen persoonsgegevens wanneer dit onmogelijk blijkt of onevenredig veel inspanning zou vergen (artikel 14 lid 5 punt b). Wel moeten zij dan langs andere weg de betreffende informatie openbaar maken (bijvoorbeeld middels een privacyverklaring), zodat betrokkenen deze langs die weg kunnen verkrijgen.

Opslagtermijn. Het beginsel van opslagbeperking (artikel 5 lid 1 punt e) vereist dat gegevens niet langer mogen worden bewaard in identificeerbare vorm dan noodzakelijk is voor het doel. Echter, wanneer persoonsgegevens uitsluitend nog worden bewaard voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, dan geldt dit vereiste niet.

Bijzondere persoonsgegevens. Voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden mogen ook bijzondere persoonsgegevens worden gebruikt als dat noodzakelijk is voor deze doeleinden (artikel 9 lid 2 punt j).

Big data. Bij statistisch onderzoek wordt veel gebruikt gemaakt van big data, waarbij zeer grote hoeveelheden data worden onderzocht op onvermoede correlaties, die vervolgens voor allerlei doeleinden kunnen worden aangewend. Big data betreft vaak persoonsgegevens, zoals koopgedrag of websitebezoek. Big data-onderzoek staat op gespannen voet met de AVG vanwege het ontbreken van een duidelijk en vooraf gemeld doel (zie ook hieronder bij “Toestemming als grondslag”) en vanwege het feit dat de resultaten van big data-onderzoek vaak worden ingezet voor persoonsgebonden profilering of beslissingen (artikel 21).

Toestemming als grondslag. Een grondslag voor onderzoek of archivering kan toestemming zijn (artikel 6 lid 1 punt a), hoewel toestemming natuurlijk op ieder moment kan worden ingetrokken (artikel 7 lid 3). Dit kan lastig werkbaar zijn bij onderzoek. Een bijkomend probleem is dat het vaak niet mogelijk is om al op het moment waarop de persoonsgegevens worden verzameld, het doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven. Toestemming is dan niet mogelijk aangezien niet aan de informatieplicht is voldaan. Overweging 33 maakt echter ruimte voor een generiekere toestemming voor bepaalde terreinen van wetenschappelijk onderzoek waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen. Betrokkenen moeten dan wel de gelegenheid krijgen om hun toestemming alleen te geven voor bepaalde onderzoeksterreinen of onderdelen van onderzoeksprojecten, voor zover het voorgenomen doel zulks toelaat. Wanneer de toestemming ziet op deelname aan wetenschappelijke onderzoeksactiviteiten in klinische proeven, geldt (overweging 161) het toestemmingsvereiste uit artikel 2 lid 21 van Verordening 536/2014.

Eigen belang als grondslag. Een grondslag voor onderzoek of archivering kan zijn de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde (artikel 6 lid 1 punt f). Onderzoek kan gemakkelijk als zo'n belang worden gezien. Natuurlijk moet de verwerkingsverantwoordelijke dan wel een afweging maken tussen dat belang en de privacybelangen van de betrokkenen, net zoals bij ieder beroep op deze grondslag. Betrokkenen hebben dan het recht om met hun specifieke situatie verband houdende redenen bezwaar te maken tegen deze verwerking, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang (artikel 21 lid 6).

Archivering in het algemeen belang. Openbare archieven zijn van groot belang voor de maatschappij. Het Nationaal Archief verwijst bijvoorbeeld naar zichzelf als het “nationaal geheugen” van Nederland. Dergelijke archieven verdienen dan ook een beschermde positie binnen de AVG; het is niet wenselijk als daar al te makkelijk persoonsgegevens worden gewist (artikel 17) of aangepast (artikel 16). Overweging 157 noemt nog het voorbeeld van wetenschappelijk onderzoek gebaseerd op openbare registers zoals de Basisregistratie Personen (voorheen het GBA): onderzoeksresultaten die door middel van zulke registers worden verkregen, leveren solide kennis van hoge kwaliteit op, die kan worden gebruikt om een op kennis gebaseerd beleid te ontwikkelen en te implementeren, de levenskwaliteit van een deel van de bevolking te verbeteren en sociale diensten efficiënter te maken. Het koppelen van gegevens uit registers kan bijvoorbeeld kennis geven over veel voorkomende medische aandoeningen zoals hart- en vaatziekten, kanker en depressie, of over de wisselwerking op lange termijn van sociale factoren zoals werkloosheid en onderwijs met andere levensomstandigheden.

Wetenschappelijk onderzoek. De term “wetenschappelijk onderzoek” moet ruim worden opgevat gezien de onderzoeksdoelstelling uit artikel 179 VWEU.

Zij omvat bijvoorbeeld technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek (overweging 159). Ook studies op het gebied van de volksgezondheid in het algemeen belang moeten hieronder worden gerekend.

Historisch onderzoek. Historisch onderzoek is gericht op het achterhalen van gebeurtenissen uit het verleden, bij voorkeur op basis van primaire bronnen zoals archieven. Onder historisch onderzoek wordt tevens onderzoek voor genealogische doeleinden (zoals stamboomonderzoek) begrepen, zij het dat de AVG natuurlijk niet geldt voor gegevens over overleden personen (zie ook artikel 4 definitie 11).

Statistisch onderzoek. Statistisch onderzoek wil zeggen dat persoonsgegevens worden geaggregeerd tot uitspraken over groepen, bijvoorbeeld over gezondheid of economisch gedrag (“Mannen tussen 18 en 35 kijken zelden meer televisie” of “Kopers van televisies op afbetaling die woonachtig zijn te Amsterdam, blijken significant vaak wanbetaler”). Deze resultaten mogen vrij worden gebruikt omdat het geen persoonsgegevens meer betreft. Echter, wanneer dergelijk onderzoek leidt tot maatregelen of beslissingen gericht op een specifiek persoon, dan kan men zich niet beroepen op dit artikel 89 (zie nader artikel 22).

Officiële statistieken. Brongegevens voor officiële statistieken zoals in Nederland geproduceerd door het Centraal Bureau voor de Statistiek of binnen de Europese Unie door het Bureau voor de Statistiek van de Europese Gemeenschappen moeten worden beschermd (art. 338 VWEU). Zie nader Verordening 223/2009 over de statistische geheimhoudingsplicht voor Europese statistieken.

89.2 Wanneer persoonsgegevens met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, kan in het Unierecht of het lidstatelijke recht worden voorzien in afwijkingen van de in de artikelen 15, 16, 18 en 21 genoemde rechten, behoudens de in lid 1 van dit artikel bedoelde voorwaarden en waarborgen, voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

Bij wetenschappelijk, historisch of statistisch onderzoek is het niet altijd wenselijk dat betrokkenen hun rechten van inzage (artikel 15), rectificatie (artikel 16), beperking (artikel 18) of bezwaar (artikel 21) uitoefenen. Rectificatie, bezwaar en beperking kunnen de betrouwbaarheid van de brondata aantasten. Inzage kan onwenselijk zijn omdat toekomstige analyses vertekend worden wanneer de betrokkenen weten waar de onderzoekers naar kijken. Bij medisch onderzoek zou de betrokkene op deze manier gezondheidsinformatie ontvangen op een ongecontroleerde manier. Dergelijke situaties zijn onwenselijk.

Het is mogelijk bij een wettelijke regeling zoals onder lid 1 te voorzien in een inperking van deze rechten. Wel moet bij de inperking worden aangetoond dat het uitoefenen van deze rechten een ernstige bedreiging vormt voor het onderzoek. Ook moeten (conform lid 1) dan andere waarborgen worden opgevoerd om de privacy van betrokkenen te beschermen. In plaats van het recht van inzage zou bijvoorbeeld toegang tot de onderzoeksresultaten kunnen worden geboden.

Geen wissing of bezwaar. Het recht van wissing is niet genoemd in dit lid 2. Het artikel bevat zelf al een beperking van gelijke strekking (artikel 17 lid 3 punt d). Hetzelfde geldt voor het recht van bezwaar: dit is niet van toepassing bij onderzoek in het algemeen belang (artikel 21 lid 6).

Nederland. In de Uitvoeringswet (artikel 44) is bepaald dat indien er door een verwerkingsverantwoordelijke de nodige voorzieningen zijn getroffen om te kunnen verzekeren dat persoonsgegevens enkel worden verwerkt ten behoeve van statistische en wetenschappelijke doeleinden het recht op inzage (artikel 15 AVG), rectificatie (artikel 16 AVG) en beperking (artikel 18 AVG) buiten toepassing kunnen worden gelaten.

89.3 Wanneer persoonsgegevens met het oog op archivering in het algemeen belang worden verwerkt, kan in het Unierecht of het lidstatelijke recht worden voorzien in afwijkingen van de in de artikelen 15, 16, 18, 19, 20 en 21 genoemde rechten, behoudens de in lid 1 van dit artikel bedoelde voorwaarden en waarborgen, voor zover die rechten het verwezenlijken van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

Bij archivering in het algemeen belang geldt net als bij onderzoek (zie lid 2) dat het niet altijd wenselijk is dat betrokkenen hun rechten onder de AVG kunnen uitoefenen. Dit kan immers de integriteit van de archieven aantasten, en dat staat op zeer gespannen voet met de uitingsvrijheid (EHRM 10 maart 2009, gevoegde zaken 3002/03 en 23676/03, Times en EHRM 16 juli 2013, zaaknr. 33846/07, Wegrzynowski). Ook kan inzage of overdracht van gegevens een grote belasting vormen voor het archief. Daarom staat dit lid 3 toe dat bij wet afwijkingen op de AVG worden getroffen ten behoeve van archieven in het algemeen belang.

Afwijkingen. De nationale of Uniewetgever kan afwijken van de rechten van inzage (artikel 15), rectificatie (artikel 16), beperking (artikel 18), kennisgeving (artikel 19), overdraagbaarheid (artikel 20) of bezwaar (artikel 21). De afwijkingen moeten noodzakelijk zijn voor een goede uitvoering van de archivering en het onbeperkt uitoefenen van deze rechten moet die archiveringstaak onmogelijk maken of ernstig belemmeren.

Overweging 158 noemt nog de optie dat lidstaten mogen bepalen dat persoonsgegevens voor archiveringsdoeleinden verder mogen worden verwerkt, bijvoor-

beeld met het oog op het verstrekken van specifieke informatie over het politiek gedrag onder voormalige totalitaire regimes, over genocide, misdaden tegen de menselijkheid, met name de Holocaust, of over oorlogsmisdaden.

Archiveren in algemeen belang. De afwijkingen uit dit artikel mogen alleen worden ingevoerd ten behoeve van archivering in het algemeen belang. Zie nader artikel 6 lid 1 punt e over dit begrip. Voor archieven onderhouden voor private doeleinden gelden de rechten van betrokkenen dus onverkort en zal binnen het betreffende recht zelf een weigeringsgrond of beperking moeten worden gevonden, zoals een wettelijke bewaarplicht die het recht van wissing pareert.

Nederland. In de Uitvoeringswet (artikel 45) zijn een aantal artikelen uitgezonderd ten behoeve van de archivering in het algemeen belang (archiefbescheiden in de zin van artikel 1 sub c Archiefwet 1995, opgeslagen voor blijvende bewaring in een archiefbewaarplaats in de zin van artikel 1 sub f Archiefwet 1995). Uitgezonderd zijn het recht op inzage (artikel 15 AVG) indien het verzoek hier toe zodanig ongericht is dat deze in redelijkheid niet kan worden ingewilligd, rectificatie (artikel 16 AVG), beperking indien de juistheid wordt betwist (artikel 18 lid 1 punt a AVG) en overdraagbaarheid (artikel 20 AVG). Aan de andere kant behoudt de betrokkene het recht om in het geval van onjuiste persoonsgegevens, zijn eigen lezing aan de desbetreffende archiefbescheiden toe te voegen (artikel 45 lid 3 Uitvoeringswet). Een en ander zal met zich meebrengen dat de Archiefwet 1995 zal worden geactualiseerd (artikelsgewijze toelichting MvT Uitvoeringswet, p. 91).

- 89.4 Wanneer verwerking als bedoeld in de leden 2 en 3 tegelijkertijd ook een ander doel dient, zijn de afwijkingen uitsluitend van toepassing op verwerking voor de in die leden bedoelde doeleinden.

Een afwijking op grond van onderzoek (lid 2) of archivering (lid 3) moet beperkt worden geformuleerd, zodat deze alleen voor die gronden geldt. Het mag niet zo zijn dat de verwerking an sich legaal wordt verklaard omdat deze óók onderzoeks- of archiveringsaspecten kent.

Artikel 90. Geheimhoudingsplicht

90.1 Wanneer dit noodzakelijk en evenredig is om het recht op bescherming van persoonsgegevens in overeenstemming te brengen met de geheimhoudingsplicht kunnen de lidstaten specifieke regels vaststellen voor de in artikel 58, lid 1, punten e) en f), bedoelde bevoegdheden van de toezichthoudende autoriteiten in verband met de verwerkingsverantwoordelijken of verwerkers die krachtens het Unierecht, het lidstatelijke recht of door nationale bevoegde instanties vastgestelde regelgeving, aan het beroepsgeheim of aan een andere gelijkwaardige geheimhoudingsplicht onderworpen zijn. Die regels gelden uitsluitend met betrekking tot persoonsgegevens die de verwerkingsverantwoordelijke of de verwerker in het kader van een onder die geheimhoudingsplicht vallende activiteit heeft ontvangen of verkregen.

Voor bepaalde beroepen, zoals de advocatuur en de medische sector, geldt een wettelijk beroepsgeheim. Dit beroepsgeheim kan op punten botsen met de regels uit de AVG, met name waar het gaat over het recht van de toezichthouder om inzage in informatie te vorderen (artikel 58 lid 1 punt e) en om toegang te verkrijgen tot alle bedrijfsruimten, uitrustingen en middelen voor gegevensverwerking (artikel 58 lid 1 punt f).

Om het beroepsgeheim te beschermen mag de nationale wetgever nadere regels stellen over hoe de toezichthouder moet handelen in dergelijke situaties. In Nederland bepaalt art. 5:20 Awb dat personen die uit hoofde van hun ambt of beroep of wettelijk voorschrift verplicht zijn tot geheimhouding, niet verplicht zijn medewerking aan een toezichthouder te verlenen, voor zover dit uit hun geheimhoudingsplicht voortvloeit.

90.2 Elke lidstaat deelt de Commissie uiterlijk op [25 mei 2018, twee jaar vanaf de datum van inwerkingtreding van deze verordening] de regels mee die hij heeft vastgesteld overeenkomstig lid 1, alsmede onverwijld alle wijzigingen daarvan.

Nadat een lidstaat regels heeft gesteld over handelen van de toezichthouder bij geheimhouders, moeten deze regels worden gemeld aan de Commissie. Deze mededeling is informatief; de Commissie kan niet direct bezwaar maken. Uiteraard dient deze wetgeving wel te voldoen aan de AVG en het Unierecht, anders kan de Commissie deze via de verdragsschendingsprocedure (artikel 258 en 259 VWEU) aanvechten.

Artikel 91. Bestaande gegevensbeschermingsregels van kerken en religieuze verenigingen

- 91.1 Wanneer kerken en religieuze verenigingen of gemeenschappen in een lidstaat op het tijdstip van de inwerkingtreding van deze verordening uitgebreide regels betreffende de bescherming van natuurlijke personen in verband met verwerking toepassen, kunnen die regels van toepassing blijven, mits zij in overeenstemming worden gebracht met deze verordening.

Artikel 17 van het Verdrag betreffende de werking van de Europese Unie bepaalt dat de status die kerken en religieuze verenigingen en gemeenschappen volgens het nationaal recht in de lidstaten hebben, wordt geëerbiedigd door de Europese Unie. De AVG is een verordening en nationale regelingen op hetzelfde gebied zijn dus in principe nietig. Echter, vanwege artikel 17 VWEU is bepaald dat regelingen van dergelijke religieuze organisaties in stand mogen blijven mits zij niet in tegenspraak zijn met de AVG.

SILA-stip. In Nederland is de bekendste regeling omtrent persoonsgegevens de zogeheten ‘SILA-stip’, waarmee vanuit de Basisregistratie Personen (voorheen Gemeentelijke Basisadministratie) op een privacyvriendelijke manier verhuizingen en dergelijke van kerkleden automatisch werden verstrekt aan de betreffende kerken. In maart 2016 werd een motie (TK 25.764-95) aangenomen een einde te maken aan deze uitzondering voor kerkgenootschappen. Deze motie lijkt niet tot daadwerkelijke stappen ter beëindiging van de SILA-regeling te hebben geleid. Op 14 juli 2022 publiceerde de overheid een ontwerpbesluit “experimenten bijhouding basisregistratie personen”, waarin de overheid uiteenzet hoe bij nieuwe personen die aansluiten bij de SILA toestemming gevraagd zal worden voor de doorgifte van de informatie aan de kerk vanuit de Basisregistratie Personen. In het wetgevingsadvies van de AP van 19 juli 2022 maakt zij duidelijk dat onduidelijk is welk algemeen belang gediend wordt bij deze verstrekking en adviseert de procedure niet voort te zetten.”

Religieuze persoonsgegevens. Religieuze organisaties mogen daarnaast van hun leden het bijzondere persoonsgegeven omtrent religieuze of levensbeschouwelijke overtuigingen verwerken op grond van artikel 9 lid 2 punt d.

- 91.2 Kerken en religieuze verenigingen die overeenkomstig lid 1 uitgebreide regels hanteren, zijn onderworpen aan toezicht door een onafhankelijke toezichthoudende autoriteit, die specifiek kan zijn, op voorwaarde dat de autoriteit voldoet aan de voorwaarden die zijn vastgesteld in hoofdstuk VI van deze verordening.

Ook religieuze organisaties zijn voor wat betreft persoonsgegevens onderworpen aan toezicht. De hiervoor verantwoordelijke toezichthouder kan een andere zijn dan de gewone nationale toezichthouder. Inhoudelijk moet deze wel voldoen aan de eisen die daarvoor gelden (zie artikelen 51-59).

Hoofdstuk X

Gedelegeerde handelingen

In hoofdstuk 10 wordt uitgewerkt op welke wijze de AVG bepaalde uitvoeringshandelingen delegeert aan de Europese Commissie (Commissie) en welke rol een comité van lidstaten speelt bij het nemen van besluiten tot deze handelingen. Artikel 92 beschrijft de voorwaarden waaronder de Commissie uitvoeringshandelingen mag delegeren, en artikel 93 werkt uit hoe de lidstaten inspraak hebben bij deze uitvoeringshandelingen.

Artikel 92. Uitoefening van de bevoegdheidsdelegatie

92.1 De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

Dit artikel regelt de procedure omtrent de twee bevoegdheden (informatie-iconen, artikel 12 lid 8, en certificering van organisaties, artikel 43 lid 8) die onder de AVG zijn gedelegeerd aan de Commissie. Bij het uitoefenen van die bevoegdheid moeten de voorstellen worden voorgehangen aan het Europees Parlement (lid 4).

92.2 De in artikel 12, lid 8, en artikel 43, lid 8, bedoelde bevoegdheidsdelegatie wordt aan de Commissie toegekend voor onbepaalde tijd met ingang van 25 mei 2016 [de datum van inwerkingtreding van deze verordening].

Er zijn onder de AVG twee te delegeren bevoegdheden: het opstellen van informatie-iconen ten behoeve van informeren van betrokkenen, en de te hanteren eisen bij certificering van verwerkingen of verwerkingsmechanismen.

Informatie-iconen. Artikel 12 lid 8 delegeert de bevoegdheid vast te stellen welke informatie de verplichte informatie-iconen dienen weer te geven en via welke procedures de gestandaardiseerde iconen tot stand dienen te komen.

Certificeringsmechanismen. Artikel 43 lid 8 delegeert invulling van de in aanmerking te nemen eisen voor de certificering van verwerkingen of van mechanismen (zoals beveiligingsmiddelen) voor een veilige verwerking. Zie nader artikel 42 over certificering.

92.3 Het Europees Parlement of de Raad kan de in artikel 12, lid 8, en artikel 43, lid 8, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

De gegeven delegatie kan te allen tijde worden ingetrokken door een besluit daartoe dat in het Publicatieblad van de Europese Unie wordt gepubliceerd. Uiteraard heeft dat geen terugwerkende kracht.

92.4 Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

Een voorgenomen gedelegeerde handeling moet worden gemeld aan het Europees Parlement en de Raad van Ministers. Zij kunnen vervolgens binnen drie maanden (lid 5) bezwaar daartegen maken.

92.5 Een overeenkomstig artikel 12, lid 8, en artikel 43, lid 8, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van drie maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of van de Raad met drie maanden verlengd.

Een gedelegeerde handeling moet voorgehangen worden (lid 4) aan het Europees Parlement en de Raad. Zij hebben vervolgens drie maanden om bezwaar te maken, en kunnen daarbij drie maanden uitstel vragen alvorens hun bezwaren uit te spreken. Wordt geen bezwaar gemaakt, dan wordt de handeling geacht te zijn goedgekeurd.

Artikel 93. Comitéprocedure

93.1 De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.

Waar de Commissie een taak heeft onder de AVG, wordt zij daarin bijgestaan door een comité van vertegenwoordigers van lidstaten, zoals geregeld in Verordening 182/2011. Dit comité heeft een zware stem. Bij de uitvoering kunnen twee procedures worden gevolgd: de raadplegingsprocedure of de onderzoeksprocedure. De AVG bepaalt dat alleen de onderzoeksprocedure kan worden ge-

volgd (uitgewerkt in lid 2 van dit artikel) met een uitzondering voor spoedzaken (lid 3).

Controlerend comité. Verordening 182/2011 is algemeen Unierecht dat algemene voorschriften en beginselen bepaalt die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren. Kort gezegd wordt er een comité ingesteld dat uit vertegenwoordigers van de lidstaten bestaat en door de Commissie wordt voorgezeten. Dit comité controleert dan de uitvoering van – in dit geval – de AVG.

Comité versus Comité. Het artikel 93-comité uit dit artikel is niet te verwarren met het Europees Comité voor gegevensbescherming dat in artikel 68 wordt ingesteld. Dit laatste Comité heeft als taak toezien op en zorgen voor de juiste toepassing van de AVG (artikel 70) en adviseren over een en ander. Ter voorkoming van verwarring spreekt dit boek van het Comité en het artikel 93-comité.

93.2 Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 5 van Verordening 182/2011 regelt de zogeheten onderzoeksprocedure. De Commissie legt hierbij een voorgenomen uitvoeringshandeling voor aan het artikel 93-comité, dat vervolgens met meerderheid van stemmen beslist over een positief of negatief advies. Indien het advies positief is, neemt de Commissie de ontwerpuitvoeringshandeling aan.

De onderzoeksprocedure wordt toegepast bij:

- de vaststelling van standaardbepalingen voor verwerkersovereenkomsten (artikel 28 lid 7);
- goedkeuring van sectorale of branchebrede gedragscodes (artikel 40 lid 9);
- goedkeuring van technische normen en mechanismen voor certificering (artikel 43 lid 9);
- de vraag of een derde land of internationale organisatie buiten de EU een passend beschermingsniveau biedt (artikel 45 lid 3);
- goedkeuring van standaardbepalingen inzake gegevensbescherming (artikel 46 lid 2);
- het uitwerken van modellen en procedures voor de elektronische uitwisseling van informatie tussen verwerkingsverantwoordelijken, verwerkers en toezichthoudende autoriteiten wat bindende bedrijfsvoorschriften betreft (artikel 47 lid 3);
- het opstellen van modellen en procedures voor wederzijdse bijstand tussen toezichthoudende autoriteiten onderling en tussen toezichthoudende autoriteiten en het Comité (artikel 61 lid 9); en
- het opstellen van regelingen voor de elektronische uitwisseling van informatie tussen toezichthoudende autoriteiten onderling en tussen toezichthoudende autoriteiten en het Comité (artikel 67).

93.3 Wanneer naar dit lid wordt verwezen, is artikel 8 van Verordening (EU) nr. 182/2011, in samenhang met artikel 5 van die verordening, van toepassing.

Artikel 8 van Verordening 182/2011 wordt ingezet bij bijzondere gevallen waarbij sprake is van “om naar behoren gemotiveerde redenen van urgentie”. De Commissie mag dan zonder voorafgaande voorlegging aan het artikel 93-comité een uitvoeringshandeling nemen die gedurende ten hoogste zes maanden van kracht blijft. Binnen 14 dagen moet het artikel 93-comité de handeling voorgelegd krijgen voor advies. Indien het advies negatief is, trekt de Commissie de betreffende uitvoeringshandeling onmiddellijk in.

De enige in de AVG genoemde plaats waarin naar dit lid wordt verwezen is artikel 45 lid 5: het “om naar behoren gemotiveerde dwingende redenen van urgentie” intrekken, wijzigen of schorsen van een aanwijzing als veilig derde land. De urgentie is dan hierin gelegen dat doorgifte van persoonsgegevens naar een dergelijk land kennelijk niet veilig is en derhalve onverwijld moet stoppen.

Hoofdstuk XI

Slotbepalingen en overgangsrecht

Het slothoofdstuk van de AVG bevat overgangsrecht en regels omtrent evaluatie en herziening. Artikel 94 trekt de Richtlijn uit 1995 in (en daarmee de Wbp), artikel 95 regelt de relatie tot de E-privacyrichtlijn en artikel 96 de besluiten inzake derde landen (zie artikel 45). Artikel 97 werkt een vierjaarlijkse evaluatieprocedure uit van de AVG zelf en artikel 98 bevat een toetsingsinstructie omtrent andere wetgeving rondom privacy en persoonsgegevens.

Artikel 99 tenslotte bepaalt dat de verordening op 25 mei 2016 in werking treedt en twee jaar later, dus op 25 mei 2018 van kracht wordt. De twee jaar hiertussen geldt als implementatieperiode met bijbehorend overgangsrecht.

Artikel 94. Intrekking van Richtlijn 95/46/EG

94.1 Richtlijn 95/46/EG wordt met ingang van 25 mei 2018 [twee jaar vanaf de datum van inwerkingtreding van deze verordening] ingetrokken.

Omdat de AVG de Richtlijn vervangt, dient de Richtlijn te worden ingetrokken. Daarmee verliezen nationale wetten zoals de Wbp hun grondslag. De intrekking gebeurt twee jaar na inwerkingtreding van de AVG. De AVG trad in werking op 25 mei 2016, de twintigste dag na haar bekendmaking in het Publicatieblad van de Europese Unie (zie artikel 99 hieronder). Er geldt een implementatieperiode van twee jaar, dus de Verordening is van toepassing vanaf 25 mei 2018.

Overgangsrecht. De AVG eist dat reeds lopende verwerkingen binnen het regime van de AVG worden gebracht. De periode van twee jaar vanaf haar inwerkingtreding is bedoeld als overgangstermijn om dit te kunnen faciliteren.

Intrekking Wbp. De Wbp wordt in de Uitvoeringswet (artikel 51) ingetrokken.

Hernieuwde toestemming. Toestemming onder de Richtlijn is aan lichtere eisen gebonden dan toestemming onder de AVG (zie artikel 4 definitie 11). Wanneer een 'oude' toestemming niet voldoet aan de eisen uit de AVG, moet deze opnieuw worden verkregen om als grond te kunnen dienen voor een verwerking onder de AVG. Slechts wanneer toestemming op een manier is verkregen die aan de voorwaarden van de AVG voldoet, mag men onder deze grondslag blijven verwerken.

94.2 Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar deze verordening. Verwijzingen naar de groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, die bij artikel 29 van Richtlijn 95/46/EG is opgericht, gelden als verwijzingen naar het bij deze verordening opgerichte Europees Comité voor gegevensbescherming.

Waar andere wetgeving verwijst naar de Richtlijn (of de Wbp), moet vanaf nu dus een verwijzing naar de AVG worden gelezen. Zo verwezen bijvoorbeeld de Telecommunicatiewet en de Wet politiegegevens voor het begrip ‘persoonsgegeven’ en ‘toestemming’ naar de definitie daarvan uit de Wbp.

Nieuwe betekenis. Begrippen uit de Richtlijn krijgen nu dus de betekenis uit de AVG. Dit lijkt een formaliteit maar heeft inhoudelijke gevolgen: zo is de definitie van persoonsgegeven (artikel 4 definitie 1) breder dan onder de Richtlijn, is toestemming onder de AVG (zie artikel 4 definitie 11) met meer eisen omkleed, en gelden zwaardere informatieplichten (zie artikelen 12-15).

Comité. De Artikel 29-Werkgroep wordt opgevolgd door het Comité voor gegevensbescherming (zie artikel 68).

Artikel 95. Verhouding tot Richtlijn 2002/58/EG

Deze verordening legt natuurlijke personen of rechtspersonen geen aanvullende verplichtingen op met betrekking tot verwerking in verband met het verstrekken van openbare elektronischecomunicatiediensten in openbare communicatienetwerken in de Unie, voor zover zij op grond van Richtlijn 2002/58/EG onderworpen zijn aan specifieke verplichtingen met dezelfde doelstelling.

Richtlijn 2002/58/EG, ook wel de E-Privacyrichtlijn, betreft de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie. In Nederland is deze met name geïmplementeerd in hoofdstuk 11 van de Telecommunicatiewet. Hierin wordt onder meer geregeld onder welke voorwaarden elektronische communicatie vertrouwelijk is, hoe mag worden omgegaan met klantgegevens en wanneer voor cookies en andere informatie opslag en -uitlezen toegestaan is. Deze regels blijven als *lex specialis* gehandhaafd en de regels uit de AVG zijn daarop niet van toepassing, behalve waar de AVG expliciet anders vermeldt (zoals in artikel 25 lid 5). Wel worden verwijzingen uit deze regels naar de Richtlijn of Wbp vervangen door verwijzingen naar de AVG (zie artikel 94 lid 2).

ePrivacy Verordening. Al jarenlang buigt de Europese Commissie zich over het aanpassen van de huidige e-privacy richtlijn. Gestreefd wordt naar een ePrivacy Verordening, zodat dezelfde regels over onder andere cookies zullen gelden binnen de verschillende EU-lidstaten. Op 11 januari 2017 publiceerde de Commissie een concept ePrivacy Verordening. Dit document is tot op het moment van het schrijven van dit boek nog niet finaal, en ligt voor het Europees Parlement.

Artikel 96. Verhouding tot eerder gesloten overeenkomsten

Internationale overeenkomsten betreffende de doorgifte van persoonsgegevens aan derde landen of internationale organisaties die door de lidstaten zijn gesloten vóór 25 mei 2018 [de datum van inwerkingtreding van deze verordening], en die in overeenstemming zijn met het vóór 25 mei 2018 [de datum van inwerkingtreding van deze verordening] toepasselijke Unierecht, blijven van kracht totdat zij worden gewijzigd, vervangen of ingetrokken.

De Commissie kon onder de Richtlijn besluiten dat derde landen of internationale organisaties een veilige haven bieden voor persoonsgegevens. Deze besluiten blijven in stand totdat zij worden gewijzigd, vervangen of ingetrokken. Dit betekent met name dat besluiten omtrent doorgifte van persoonsgegevens naar derde landen, in stand blijven (zie ook artikel 45 lid 1). Er zal dus geen herziening hoeven plaats te vinden enkel omdat de Europese regels nu aangescherpt worden.

Artikel 97. Evaluatie Commissieverslagen

97.1 Uiterlijk 25 mei 2022 [4 jaar na de inwerkingtreding van deze verordening] en om de vier jaar daarna, dient de Commissie een verslag in bij het Europees Parlement en de Raad over de evaluatie en de toetsing van deze verordening. De verslagen worden openbaar gemaakt.

Teneinde de effectiviteit van de AVG te kunnen vaststellen, zal elke vier jaar een evaluatie en toetsing plaats dienen te vinden. Hiermee kunnen knelpunten en mogelijkheden voor verbetering worden geïdentificeerd. Lid 2 bepaalt hierbij enkele belangrijke aandachtspunten.

97.2 In het kader van de in lid 1 bedoelde evaluaties en toetsingen beoordeelt de Commissie met name de toepassing en de werking van:

De vierjaarlijkse evaluatie moet gericht zijn op twee onderwerpen:

97.2(a) hoofdstuk V betreffende de doorgifte van persoonsgegevens aan derde landen of internationale organisaties, in het bijzonder met betrekking tot krachtens artikel 45, lid 3, van deze verordening vastgestelde besluiten en op grond van artikel 25, lid 6, van Richtlijn 95/46/EG vastgestelde besluiten;

De vierjaarlijkse evaluatie zal in ieder geval gericht moeten zijn op de status van veilige derde landen. De Commissie kan tot deze status besluiten onder artikel 45. Besluiten genomen onder de Richtlijn (zoals het Privacy Shield-besluit voor de VS) blijven van kracht onder de AVG (artikel 96) en worden hiermee op dezelfde wijze geëvalueerd.

97.2(b) hoofdstuk VII betreffende samenwerking en coherentie.

Hoofdstuk VII regelt samenwerking tussen de verschillende toezichthouders en de rol van het Comité. Ook deze samenwerking wordt vierjaarlijks geëvalueerd.

97.3 Voor het in lid 1 vermelde doel kan de Commissie zowel de lidstaten als toezichthoudende autoriteiten om informatie verzoeken.

De voor de evaluatie benodigde informatie zal worden verkregen bij de lidstaten en de verschillende toezichthouders.

97.4 Bij de uitvoering van de in de leden 1 en 2 vermelde evaluaties en toetsingen neemt de Commissie de standpunten en bevindingen van het Europees Parlement, van de Raad, en van andere relevante instanties of bronnen in aanmerking.

Naast lidstaten en toezichthouders zullen ook het Europees Parlement, de Raad van Ministers en andere relevante bronnen om input worden gevraagd.

97.5 Indien nodig dient de Commissie passende voorstellen in teneinde deze verordening te wijzigen, met name in het licht van de ontwikkelingen in de informatietechnologie en de stand van zaken in de informatiemaatschappij.

Wanneer uit de evaluatie blijkt dat de AVG niet langer goed aansluit bij de praktijk, bijvoorbeeld door privacyaspecten van nieuwe technologieën of ontwikkelingen, kan de Commissie besluiten de AVG aan te passen. Gezien het buitengewoon heftige lobbywerk dat bij het aannemen van de AVG werd gevoerd, zal dit niet lichtvaardig gebeuren.

Artikel 98. Toetsing van andere Unierechtshandelingen inzake gegevensbescherming

Indien passend dient de Commissie wetgevingsvoorstellen in teneinde andere Unierechtshandelingen betreffende de bescherming van persoonsgegevens te wijzigen en aldus een uniforme en consequente bescherming van natuurlijke personen te garanderen in verband met verwerking. Het gaat hierbij met name om de regels betreffende de bescherming van natuurlijke personen in verband met verwerking door instellingen, organen en instanties van de Unie, en betreffende het vrije verkeer van die gegevens.

Dit artikel biedt een algemene instructie aan de Commissie om nadere wetgeving aan te nemen wanneer blijkt dat huidige wetgeving over persoonsgegevens niet in lijn is met de AVG. Speciale aandacht daarbij krijgt verwerking van persoonsgegevens door Unie-instellingen. Hierop is nu Verordening (EG) nr. 45/2001 van toepassing (zie artikel 2 lid 3). Ook hier zullen “de specifieke behoeften van de kleine, middelgrote en micro-ondernemingen” (overweging 13) in aanmerking genomen moeten worden.

Artikel 99. Inwerkingtreding en toepassing

99.1 Deze verordening treedt in werking op 25 mei 2016 [de twintigste dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie].

De AVG werd bekendgemaakt in OJ L 119 van 4 mei 2016, p. 1–88 (online: <http://data.europa.eu/eli/reg/2016/679/oj>). Inwerkingtreding geschiedde twintig dagen later, derhalve op 25 mei 2016.

99.2 Zij is van toepassing met ingang van 25 mei 2018 [twee jaar na de inwerkingtreding van deze verordening].

De AVG is van toepassing twee jaar na de inwerkingtreding, derhalve met ingang van 25 mei 2018. Vanaf dat moment moeten alle verwerkingen van persoonsgegevens voldoen aan het regime van de AVG. Dit geldt dus ook voor verwerkingen die legaal waren onder de Richtlijn (of Wbp), zie ook artikel 95.

**UITVOERINGSWET
ALGEMENE VERORDENING
GEGEVENSBECHERMING**

Hoofdstuk 1

Algemene bepalingen

De Uitvoeringswet is in Nederland ingevoerd om uitvoering te geven aan een aantal gedelegeerde bevoegdheden waar de AVG ruimte voor biedt, en om verplichte nummers uit de AVG uit te voeren (zoals het oprichten van de Autoriteit Persoonsgegevens). Daarnaast worden in de Uitvoeringswet een aantal nationale kwesties uitgewerkt.

De Uitvoeringswet is opgezet in vijf hoofdstukken. Hoofdstuk 1 van de Uitvoeringswet regelt de materiële en territoriale toepasselijkheid van deze wet (artikelen 2, 3 en 4) en regelt het specifieke punt van verwerkingen van minderjarige betrokkenen (artikel 5).

Artikel 1. Definities

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

De Uitvoeringswet introduceert drie definities die voor de praktijk van belang zijn.

bijzondere categorieën van persoonsgegevens: de categorieën van persoonsgegevens, bedoeld in artikel 9, eerste lid, van de verordening

Deze definitie introduceert formeel de term “bijzondere persoonsgegevens” voor de categorieën persoonsgegevens opgenomen in artikel 9 AVG. De AVG kent hiervoor zelf geen verkorte term.

Onze Minister: Onze Minister voor Rechtsbescherming;

De uitvoering van de AVG, en dus ook de Uitvoeringswet, valt onder Franc Weerwind, minister van Rechtsbescherming, een minister zonder portefeuille. Zijn post valt onder het ministerie van Justitie en Veiligheid.

persoonsgegevens van strafrechtelijke aard: persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag;

Deze definitie introduceert een verkorte term voor de “persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen” die in artikel 10 AVG zijn geïntroduceerd en waarvoor een zeer streng regime geldt.

verordening: verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

Deze derde definitie bepaalt dat de term ‘verordening’ verwijst naar de AVG. Dit boek gebruikt echter de term AVG om consequent te blijven.

Artikel 2. Materiële reikwijdte

- 2.1 Deze wet en de daarop berustende bepalingen zijn van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

De Uitvoeringswet is materieel van toepassing in dezelfde situaties als waarin de AVG zelf van toepassing is (artikel 2 AVG).

- 2.2 In afwijking van het eerste lid, is deze wet niet van toepassing op de verwerking van persoonsgegevens voor zover daarop de Wet basisregistratie personen, de Kieswet of de Wet raadgevend referendum van toepassing is.

De verwerking van persoonsgegevens voor de basisregistratie personen, verkiezingen en referenda is apart uitgewerkt in deze wetten. Daarmee is de Uitvoeringswet daarop niet van toepassing. De AVG zelf is wél van toepassing op deze drie verwerkingen (zie onze toelichting bij artikel 2 lid 2 punt a AVG).

- 2.3 Behoudens het bepaalde in artikel 3, is deze wet niet van toepassing op de verwerking van persoonsgegevens, bedoeld in artikel 2, tweede lid, van de verordening.

Artikel 2 lid 2 AVG sluit de toepasselijkheid van de AVG uit voor, kort gezegd, verwerkingen voor nationale veiligheid, Europees buitenlands- en veiligheidsbeleid, zuiver huishoudelijke verwerkingen en het strafprocesrecht. Op diezelfde situaties is de Uitvoeringswet dus ook niet van toepassing. Zie echter artikel 3 dat voor bepaalde specifieke verwerkingen voor de krijgsmacht en de inlichtingen- en veiligheidsdiensten de Uitvoeringswet weer wel van kracht verklaart.

Artikel 2a. Inachtneming behoeften kleine, middelgrote en micro-ondernemingen

De Autoriteit persoonsgegevens neemt bij de toepassing van de verordening de specifieke behoeften van kleine, middelgrote en micro-ondernemingen als bedoeld in artikel 2 van de bijlage bij Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PbEU 2003 L124) in aanmerking.

In overweging 13 van de AVG beveelt de Europese Unie (de EU) uitdrukkelijk om bij toepassing van de verordening rekening te houden met de omvang van bedrijven en organisaties. Dit artikel sluit hierbij aan, zodat de behoeften van deze categorie bedrijven door de Autoriteit Persoonsgegevens (AP) nadrukkelijk meegenomen moeten worden genomen bij toepassing van de AVG.

Midden- en kleinbedrijf. Het midden- en kleinbedrijf (MKB) betreft bedrijven en organisaties die minder dan 250 werknemers bevatten, een jaaromzet van minder dan 50 miljoen euro draaien of onder een balanstotaal van 43 miljoen euro zitten (Aanbeveling 2003/361/EG).

Administratieve lasten. De implicatie is met name dat geen onnodige administratieve of andere lasten aan dergelijke kleine ondernemingen moeten worden opgelegd. Helaas betekent dit niet dat de verplichting tot het voeren van een register van verwerkingen (artikel 30 AVG) vervalt voor het MKB.

Artikel 3. Schakelbepaling verwerkingen buiten werkingssfeer verordening

3.1 Deze wet en de daarop berustende bepalingen zijn mede van toepassing op de verwerking van persoonsgegevens:

Nadat in artikel 2 de Uitvoeringswet buiten toepassing is verklaard voor een aantal categorieën verwerkingen binnen de overheid, schakelt dit artikel 3 dit weer om voor specifieke verwerkingen daarbinnen. Het betreft:

3.1(a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;

Zoals bij artikel 2 lid 2 AVG is opgemerkt, betreft dit een beperkte categorie verwerkingen die met name gaat over nationale veiligheid en het werk van inlichtingendiensten. Geheel duidelijk is de afbakening van deze categorie niet. Daarom bepaalt dit artikel 3 lid 1 dat de Uitvoeringswet weer wél geldt voor deze categorie verwerkingen.

- 3.1(b) door de krijgsmacht bij de uitvoering van activiteiten die binnen de werksfeer van titel V, hoofdstuk 2, van het Verdrag betreffende de Europese Unie vallen.

Ook voor de situatie dat de krijgsmacht persoonsgegevens verwerkt, wordt ter voorkoming van onduidelijkheden bepaald dat de Uitvoeringswet wel van toepassing is. Lid 3 sluit daarvan dan weer uit de verwerkingen door de krijgsmacht bij de inzet ter verdediging en bescherming van de belangen van het Koninkrijk (artikel 97 Grondwet).

- 3.2 De verordening is van overeenkomstige toepassing op de verwerking van persoonsgegevens, bedoeld in het eerste lid.

Omdat de Uitvoeringswet zonder de AVG weinig voorstelt, is de AVG zelf van overeenkomstige toepassing op de in lid 1 bedoelde verwerkingen.

- 3.3 Het eerste en het tweede lid zijn niet van toepassing op:

Om een en ander nog onduidelijker te maken introduceert lid 3 weer een aantal uitzonderingen op de toepasselijkheid van Uitvoeringswet en AVG op de in lid 1 genoemde verwerkingen.

- 3.3(a) de verwerking van persoonsgegevens door de krijgsmacht, voor zover Onze Minister van Defensie daartoe beslist met het oog op de inzet of het ter beschikking stellen van de krijgsmacht ter uitvoering van de in artikel 97 van de Grondwet omschreven taken;

Bij inzet van de krijgsmacht “ter verdediging en bescherming van de belangen van het Koninkrijk”, zoals bij militaire civiele missies en politiemijsies krachtens het Gemeenschappelijk Buitenlands en Veiligheidsbeleid, kan en mag de verwerking van persoonsgegevens buiten de reikwijdte van de AVG en Uitvoeringswet blijven (artikel 39 VEU).

- 3.3(b) de verwerking van persoonsgegevens voor zover daarop de Wet op de inlichtingen- en veiligheidsdiensten 2017 van toepassing is.

Omdat de verwerking van persoonsgegevens door inlichtingen- en veiligheidsdiensten al in de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) geregeld is, is het niet nodig dat hier ook de AVG en Uitvoeringswet op van toepassing zijn.

- 3.4 Van een besluit als bedoeld in het derde lid, onderdeel a, wordt zo spoedig mogelijk mededeling gedaan aan de Autoriteit persoonsgegevens.

Het ministerie van Defensie zal de toezichthouder zo spoedig mogelijk informeren over militaire missies en andere situaties vallend onder artikel 97 Grondwet. De toezichthouder is immers niet competent om daarover te oordelen en moet dan ook weten dat deze bestaan.

Artikel 4. Territoriale reikwijdte

- 4.1 Deze wet en de daarop berustende bepalingen zijn van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in Nederland.

De AVG is territoriaal van toepassing bij verwerkingen in de Europese Unie (artikel 3 lid 1). De Uitvoeringswet sluit daarbij aan, zij het natuurlijk specifiek voor Nederland.

Nederlandse verwerker. Een Nederlandse verwerker moet zich dus aan de Uitvoeringswet houden, ook wanneer zijn verwerkingsverantwoordelijke dat niet hoeft.

Nederlandse verwerkingsverantwoordelijke. Een Nederlandse verwerkingsverantwoordelijke moet zich aan de Uitvoeringswet houden. Hij hoeft zijn buitenlandse verwerkers niet te binden aan de Uitvoeringswet.

- 4.2 Deze wet en de daarop berustende bepalingen zijn van toepassing op verwerking van persoonsgegevens van betrokkenen die zich in Nederland bevinden door een niet in de Europese Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:

4.2(a) het aanbieden van goederen of diensten aan deze betrokkenen in Nederland, ongeacht of een betaling door de betrokkenen is vereist; of

4.2(b) het monitoren van hun gedrag, voor zover dit gedrag in Nederland plaatsvindt.

De AVG is ook territoriaal van toepassing bij het aanbieden van goederen of diensten aan betrokkenen in de Unie, of bij het monitoren van hun gedrag binnen de Unie (artikel 3 lid 2). De Uitvoeringswet sluit wederom hierbij aan, zij het beperkt tot Nederland.

Artikel 5. Toestemming van wettelijk vertegenwoordiger

- 5.1 Indien artikel 8 van de verordening niet van toepassing is, is in de plaats van de toestemming van de betrokkene die van zijn wettelijk vertegenwoordiger vereist indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt.

Artikel 8 AVG bepaalt dat minderjarigen tot zestien jaar niet zelfstandig toestemming kunnen geven voor verwerkingen bij internetdiensten. Toestemming van hun ouders of vertegenwoordigers is dan vereist. Dit artikel 5 Uitvoeringswet breidt dit ouderlijktoestemmingsvereiste uit tot álle verwerkingen, ook wanneer het geen internetdiensten betreft.

Bevoegdheid. Het is niet duidelijk welk artikel in de AVG Nederland toestaat te bepalen dat minderjarigen niet zelfstandig toestemming mogen geven. Wij gaan er maar vanuit dat dit in de praktijk geen rechtsvragen op zal roepen.

Lagere leeftijd. Artikel 8 lid 3 AVG staat lidstaten toe een lagere leeftijd dan zestien jaar te hanteren. Nederland heeft van deze mogelijkheid geen gebruik gemaakt.

- 5.2 Indien de betrokkene onder curatele is gesteld, dan wel ten behoeve van de betrokkene een bewind of mentorschap is ingesteld, is, voor zover het een aangelegenheid betreft waarvoor de betrokkene onbekwaam dan wel onbevoegd is, in de plaats van de toestemming van de betrokkene die van zijn wettelijk vertegenwoordiger vereist.

Voor betrokkenen die onder curatele of onder bewind zijn gesteld, geldt dezelfde situatie als voor minderjarigen onder de zestien.

- 5.3 Toestemming kan door de wettelijk vertegenwoordiger van de betrokkene te allen tijde worden ingetrokken.

Artikel 7 lid 3 AVG bepaalt dat een betrokkene te allen tijde zijn gegeven toestemming kan intrekken. Dit lid 3 bevestigt dat intrekking net als het geven van toestemming door de vertegenwoordiger moet gebeuren.

- 5.4 De rechten van de betrokkene, bedoeld in hoofdstuk III van de verordening, worden ten aanzien van betrokkenen die de leeftijd van zestien jaren nog niet hebben bereikt, ten aanzien van onder curatele gestelden en ten aanzien van betrokkenen ten behoeve van wie een bewind of mentorschap is ingesteld, uitgeoefend door hun wettelijk vertegenwoordigers, voor zover het een aangelegenheid betreft waarvoor de betrokkene onbekwaam dan wel onbevoegd is.

Wanneer een betrokkene nog geen zestien is of juridisch onbekwaam of onbevoegd is om zijn rechten onder de AVG uit te oefenen, mogen zijn wettelijk

vertegenwoordigers in zijn of haar plaats zijn rechten uitoefenen die hij onder de AVG bezit, zoals inzage, correctie of verwijdering.

- 5.5 Dit artikel is niet van toepassing op hulp- en adviesdiensten die rechtstreeks en kosteloos aan een minderjarige of een onder curatele gestelde worden aangeboden.

Overweging 38 AVG bepaalt dat ouderlijke toestemming voor minderjarigen niet vereist is bij preventieve- of adviesdiensten gericht op deze personen. In Nederland is dat bijvoorbeeld de Kindertelefoon. Dit lid 5 verklaart dezelfde situatie van toepassing voor andere verwerkingen die onder de grondslag toestemming plaatsvinden. Hiermee kunnen ouders dus ook geen inzage- of ander recht uitoefenen (lid 4) bij deze categorie verwerkingen.

Hoofdstuk 2

De Autoriteit persoonsgegevens

Hoofdstuk 2 is gewijd aan instelling en regeling van bevoegdheden van de Autoriteit persoonsgegevens (AP), de toezichthouder in Nederland. Het hoofdstuk kent twee paragrafen: paragraaf 2.1 regelt de oprichting en wijze van inrichting van de AP, en paragraaf 2.2 gaat in op de taken en bevoegdheden van de AP in Nederland, met name gericht op de bestuursrechtelijke kant van haar opereren.

PARAGRAAF 2.1. OPRICHTING EN INRICHTING VAN DE AUTORITEIT PERSOONSgegevens

Artikel 6. Oprichting en aanwijzing als toezichthoudende autoriteit

6.1 Er is een Autoriteit persoonsgegevens. De Autoriteit persoonsgegevens bezit rechtspersoonlijkheid.

Formeel is de AP als toezichthouder opgeheven met de intrekking van de Wet bescherming persoonsgegevens. Met dit artikel wordt zij opnieuw opgericht als bestuursorgaan.

6.2 De Autoriteit persoonsgegevens is de toezichthoudende autoriteit, bedoeld in artikel 51, eerste lid, van de verordening.

Hiermee wordt de AP formeel aangewezen als de nationale toezichthouder van Nederland.

6.3 Onverminderd artikel 57 van de verordening, heeft de Autoriteit persoonsgegevens tot taak toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de verordening of de wet bepaalde.

Hiermee wordt de taak van de AP vastgesteld in aanvulling op hetgeen de AVG (artikel 57) bepaalt aan taken van toezichthouders. Met name voegt dit toe dat de AP de Uitvoeringswet kan handhaven. Zie ook artikel 14.

- 6.4 Ter uitvoering van een bindende EU-rechts-handeling kunnen, gehoord de Autoriteit persoonsgegevens, bij regeling van Onze Minister aan de Autoriteit persoonsgegevens taken worden opgedragen.

De minister kan nadere taken opdragen aan de AP wanneer daar aanleiding toe is vanuit een Europese rechtshandeling, zoals bij een adequaatheidsbesluit (artikel 45 AVG).

Artikel 7. Samenstelling

- 7.1 De Autoriteit persoonsgegevens bestaat uit een voorzitter en twee andere leden.

Net zoals onder de Wbp kent de AP een voorzitter en twee leden.

- 7.2 Bij de Autoriteit persoonsgegevens kunnen voorts buitengewone leden worden benoemd. Bij de benoeming van buitengewone leden wordt spreiding over de onderscheidene sectoren van de maatschappij nagestreefd.

Het is mogelijk om bij de AP buitengewone leden te benoemen.

- 7.3 De voorzitter, de andere leden en de buitengewone leden van de Autoriteit persoonsgegevens worden bij koninklijk besluit, op voordracht van Onze Minister, benoemd.

De voorzitter en leden worden bij koninklijk besluit benoemd, om zo de onafhankelijkheid van dit bestuursorgaan te waarborgen. De normale regeling uit artikel 12 Kaderwet zelfstandige bestuursorganen (zbo's) is niet van toepassing (zie lid 8).

- 7.4 De voorzitter voldoet aan de bij of krachtens artikel 5 van de Wet rechtspositie rechterlijke ambtenaren gestelde vereisten voor benoembaarheid tot rechter in een rechtbank.

Om de kwaliteit en onafhankelijkheid van de AP te borgen, moet de voorzitter voldoen aan dezelfde eisen als een rechter.

- 7.5 De benoeming, bedoeld in het derde lid, geldt voor een tijdvak van vijf jaar.

- 7.6 De voorzitter, de andere leden en de buitengewone leden van de Autoriteit persoonsgegevens kunnen eenmaal worden herbenoemd voor een tijdvak van vijf jaar.

De benoeming van de voorzitter en leden is voor vijf jaar, met de eenmalige mogelijkheid tot herbenoeming.

- 7.7 Op eigen verzoek worden de voorzitter, de andere leden en de buitengewone leden van de Autoriteit persoonsgegevens door Onze Minister ontslagen.

Ontslag is mogelijk op eigen verzoek. Daarnaast kunnen niet-functionerende leden (of de voorzitter) worden ontslagen net zoals rechters (Wet rechtspositie rechterlijke ambtenaren, artikel 8 hieronder).

- 7.8 Artikel 12 van de Kaderwet zelfstandige bestuursorganen is niet van toepassing.

Normaal worden bij zbo's de voorzitter en leden door de minister benoemd (artikel 12 Kaderwet zbo's). Deze regeling geldt niet bij de AP.

- 7.9 Er is een Raad van advies die de Autoriteit persoonsgegevens adviseert over algemene aspecten van de bescherming van persoonsgegevens. De leden zijn afkomstig uit de onderscheidene sectoren van de maatschappij en worden benoemd door Onze Minister, op voordracht van de voorzitter van de Autoriteit persoonsgegevens. De leden worden benoemd voor ten hoogste vier jaar. Herbenoeming kan tweemaal en telkens voor ten hoogste vier jaar plaatsvinden. Bij ministeriële regeling wordt de vergoeding van de kosten aan de leden van de Raad van advies vastgesteld.

Al onder de Wbp kende de AP een Raad van Advies. Deze blijft net als de AP zelf gehandhaafd en dient de AP van (niet-bindend) advies.

Artikel 8. Disciplinaire maatregelen voorzitter en andere leden

De artikelen 46c, 46d, tweede lid, 46f, 46g, 46i, met uitzondering van het eerste lid, onderdeel c, 46j, 46l, eerste en derde lid, 46m, 46n, 46o en 46p van de Wet rechtspositie rechterlijke ambtenaren zijn van overeenkomstige toepassing op de voorzitter en de andere leden van de Autoriteit persoonsgegevens, met dien verstande dat:

- a. de disciplinaire maatregel bedoeld in artikel 46c, eerste lid, ten aanzien van de andere leden van de Autoriteit persoonsgegevens door de voorzitter van de Autoriteit persoonsgegevens wordt opgelegd;
- b. het in artikel 46c, eerste lid, onderdeel b, genoemde verbod zich in een onderhoud of een gesprek in te laten met partijen of hun advocaten of gemachtigden of een bijzondere inlichting of schriftelijk stuk van hen aan te nemen, niet op de voorzitter en de andere leden van de Autoriteit persoonsgegevens van toepassing is;
- c. de disciplinaire maatregel bedoeld in artikel 46c, eerste lid, ten aanzien van de voorzitter van de Autoriteit persoonsgegevens door de president van het gerechtshof Den Haag wordt opgelegd.

De Wet rechtspositie rechterlijke ambtenaren regelt in de genoemde artikelen de mogelijkheden tot berisping, schorsing en ontslag van rechters. Deze regeling is van overeenkomstige toepassing op de leden van de AP, met enkele specifieke aanpassingen gezien het karakter en de positie van de AP.

Artikel 9. Rechtspositie voorzitter, andere leden en buitengewone leden

De rechtspositie van de voorzitter, de andere leden en de buitengewone leden wordt geregeld bij of krachtens algemene maatregel van bestuur.

Nadere regelingen over de rechtspositie van de voorzitter en leden worden bij algemene maatregel van bestuur genomen. Hiermee komt de AP als toezichthouder op grotere afstand van de minister te staan dan onder de Wbp. Deze liet dit namelijk aan een ministeriële regeling over.

Artikel 10. Secretariaat

- 10.1 De Autoriteit persoonsgegevens heeft een secretariaat, waarvan de ambtenaren door de Autoriteit persoonsgegevens worden aangesteld, bevorderd, disciplinair gestraft, geschorst en ontslagen.

Het secretariaat ondersteunt de leden van de AP. Hun toezicht en discipline wordt intern geregeld. Zie artikel 52 lid 5 AVG.

- 10.2 Ten aanzien van de tot het secretariaat behorende ambtenaren worden de bij of krachtens de Ambtenarenwet aan het bevoegd gezag toegekende bevoegdheden uitgeoefend door de Autoriteit persoonsgegevens, met uitzondering van de bevoegdheid om regels of nadere regels te stellen.

De personen werkzaam bij het secretariaat zijn ambtenaren in de zin van de Ambtenarenwet.

Artikel 11. Begroting, verantwoording en vertegenwoordigingsbevoegdheid

- 11.1 De Autoriteit persoonsgegevens stelt jaarlijks voorafgaand aan het desbetreffende begrotingsjaar een ontwerpbegroting op.

- 11.2 In de departementale begroting, bedoeld in artikel 2.1, zesde lid, van de Comptabiliteitswet 2016, kent Onze Minister jaarlijks aan de Autoriteit persoonsgegevens een budget toe ten laste van de rijksbegroting.

- 11.3 De Autoriteit persoonsgegevens stelt de begroting vast in overeenstemming met het budget, bedoeld in het tweede lid.

De AVG vereist (artikel 52 lid 6) dat de AP een eigen begroting heeft. Deze wordt jaarlijks in concept opgesteld en goedgekeurd (of niet) door het parlement.

- 11.4 De Autoriteit persoonsgegevens wordt in en buiten rechte vertegenwoordigd door de voorzitter en de andere leden, dan wel door een van hen.

- 11.5 De leden stellen een verdeling van taken vast en betrekken hierbij zoveel mogelijk de buitengewone leden.

De voorzitter en de leden kunnen individueel de AP vertegenwoordigen. Er is op dit moment geen specifieke verdeling van taken vastgesteld. Deze was er onder de Wbp overigens ook niet.

Artikel 12. Beperking inlichtingenplicht jegens minister

Artikel 20 van de Kaderwet zelfstandige bestuursorganen is niet van toepassing indien de Autoriteit persoonsgegevens de informatie van derden heeft verkregen onder de voorwaarde dat het geheime karakter daarvan wordt gehandhaafd.

In beginsel kan de minister van een zbo zoals de AP informatie opeisen onder artikel 20 Kaderwet zbo's. Deze bevoegdheid geldt echter niet wanneer de AP deze informatie heeft verkregen onder geheimhouding van verwerkingsverantwoordelijken of andere derden. Dit waarborgt mede haar onafhankelijkheid (overweging 117 AVG).

Artikel 13. Uitzonderingen bevoegdheden inzake beleidsregels, vernietiging en taakverwaarlozing

13.1 De artikelen 21 en 22 van de Kaderwet zelfstandige bestuursorganen zijn niet van toepassing op de Autoriteit persoonsgegevens.

13.2 Artikel 23 van de Kaderwet zelfstandige bestuursorganen vindt slechts toepassing ten aanzien van het door de Autoriteit persoonsgegevens gevoerde financiële beheer en de administratieve organisatie.

Onder artikel 21 Kaderwet zbo's mag de minister beleidsregels opstellen voor een zbo zoals de AP. Artikel 22 staat de minister toe besluiten van een zbo te vernietigen. Deze twee artikelen moeten buiten toepassing blijven gezien het onafhankelijke karakter van de AP (overweging 117 AVG). De taakverwaarlozing (artikel 23 Kaderwet) geldt alleen bij financiële en administratieve verwaarlozing.

PARAGRAAF 2.2. DE UITOEFENING VAN DE TAKEN EN BEVOEGDHEDEN VAN DE AUTORITEIT PERSOONSgegevens**Artikel 14. Taken en bevoegdheden**

14.1 De Autoriteit persoonsgegevens is bevoegd om de taken uit te voeren en de bevoegdheden uit te oefenen die bij of krachtens de verordening zijn toegekend aan de toezichthoudende autoriteit.

Hiermee wordt de taak van de AP vastgesteld in aanvulling op hetgeen de AVG (artikel 57) bepaalt aan taken van toezichthouders. Met name voegt dit toe dat de AP de Uitvoeringswet kan handhaven. Ook wordt hier geregeld hoe de bevoegdheden van de AP – die volgen uit Europese regels – passen binnen het Nederlandse speelveld van de Algemene wet bestuursrecht (Awb).

- 14.2 Op de voorbereiding van een besluit omtrent goedkeuring van een gedragscode, dan wel de wijziging of uitbreiding daarvan, als bedoeld in artikel 40, vijfde lid, van de verordening is afdeling 3.4 van de Algemene wet bestuursrecht van toepassing.

De toezichthouder is bevoegd gedragscodes (artikel 40 AVG) goed te keuren. In Nederland geldt hierbij dan de openbare voorbereidingsprocedure (afdeling 3.4 Awb). Een ontwerpbesluit over zo'n gedragscode moet dan ter inzage worden gelegd, waarna belanghebbenden (niet per se alleen betrokkenen) zienswijzen kunnen inbrengen. Ook beroep is dan mogelijk tegen het eenmaal genomen besluit.

- 14.3 De Autoriteit persoonsgegevens kan in geval van overtreding van het bepaalde in artikel 83, vierde, vijfde of zesde lid, van de verordening een bestuurlijke boete opleggen van ten hoogste de in deze leden genoemde bedragen.

Het kunnen opleggen van boetes is een bevoegdheid die direct uit de AVG zelf volgt (artikel 83 AVG). Echter, op grond van artikel 5:46 Awb moet “de wet” – dus de Nederlandse wet – bepalen of en welke boetes een toezichthouder kan opleggen. Deze schakelbepaling lost dit probleem op.

- 14.4 De artikelen 5:4 tot en met 5:10a de Algemene wet bestuursrecht zijn van overeenkomstige toepassing op corrigerende maatregelen als bedoeld in artikel 58, tweede lid, onderdelen b tot en met j van de verordening.

Artikel 58 AVG geeft de toezichthouder corrigerende bevoegdheden, zoals een berisping of het doen staken van een verwerking. Dit lid 4 regelt dat een dergelijke bevoegdheid gezien moet worden als een bestuurlijke sanctie in de zin van de Awb, met alle waarborgen en randvoorwaarden van dien (art. 5:4 t/m 5:10a Awb). De waarschuwing (artikel 58 lid 2 punt a AVG) is geen sanctie en valt daarmee niet onder dit regime.

- 14.5 Onverminderd artikel 4:15 van de Algemene wet bestuursrecht kan de Autoriteit Persoonsgegevens de termijn voor het geven van een beschikking opschorten voor zover dit noodzakelijk is in verband met het naleven van op de Autoriteit Persoonsgegevens rustende verplichtingen op grond van de artikelen 60 tot en met 66 van de verordening. Het derde en vierde lid van artikel 4:15 van de Algemene wet bestuursrecht zijn op deze opschorting van overeenkomstige toepassing.

De AVG kent een aantal beslistermijnen voor de toezichthouder, maar regelt niet hoe deze mogen worden opgeschort of verlengd. Hierop is weliswaar artikel 4:15 Awb van toepassing, maar dit artikel gaat niet op bij de verplichtingen rondom samenwerking en coherentie (artikelen 60-66 AVG). Daarom regelt dit lid 5 apart hoe dit geval uit moet pakken.

14.6 De bestuurlijke boete komt toe aan de Staat.

In afwijking van de hoofdregel uit het bestuursrecht komt de boete niet toe aan de AP zelf (artikel 1:1 lid 4 Awb) maar aan de Staat. Dit in verband met de onafhankelijke positie van de AP.

Artikel 15. Toezicht op de naleving

15.1 Met het toezicht op de naleving van de verordening en op de verwerking van persoonsgegevens overeenkomstig het bij of krachtens de wet bepaalde zijn belast de leden en buitengewone leden van de Autoriteit persoonsgegevens, de ambtenaren van het secretariaat van de Autoriteit persoonsgegevens, alsmede de bij besluit van de Autoriteit persoonsgegevens aangewezen personen.

Met dit lid 1 worden de bestuursrechtelijke toezichthoudende bevoegdheden formeel opgedragen aan de leden van de AP, haar ambtenaren van het secretariaat en eventuele nader aangewezen personen.

15.2 De in het eerste lid bedoelde personen zijn bevoegd een woning te betreden zonder toestemming van de bewoner.

De leden en secretariële ambtenaren van de AP zijn bevoegd woningen te betreden als dat nodig is voor hun werk als toezichthouder. Dit in aanvulling op artikel 5:15 Awb, dat weliswaar een binnentreedbevoegdheid kent maar niet voor woningen zonder toestemming. Op dit betreden is natuurlijk wel de Algemene wet op het binnentreden van toepassing.

15.3 De in het eerste lid bedoelde personen behoeven voor de uitoefening van de in het tweede lid omschreven bevoegdheid de uitdrukkelijke en bijzondere volmacht van de Autoriteit persoonsgegevens, onverminderd het bepaalde in artikel 2 van de Algemene wet op het binnentreden.

Voor het mogen binnentreden moet een bijzondere en uitdrukkelijke volmacht gegeven worden.

15.4 Geen beroep is mogelijk op een geheimhoudingsplicht, voor zover inlichtingen of medewerking wordt verlangd in verband met de eigen betrokkenheid bij de verwerking van persoonsgegevens.

Verwerkingsverantwoordelijken en verwerkers opereren vaak onder geheimhouding, hetzij wettelijk (zoals het beroepsgeheim voor advocaten), hetzij contractueel (een geheimhoudingscontract of -beding, bijvoorbeeld in de verwerkersovereenkomst). Om iedere discussie daarover te vermijden bepaalt dit lid

4 expliciet dat dergelijke verplichtingen niet kunnen worden ingeroepen als de toezichthouder geheime informatie nodig heeft.

Geheimhouding door AP. De AP is zelf aan geheimhouding gebonden over wat zij in het uitoefenen van haar werkzaamheden tegenkomt (artikel 2:5 Awb).

- 15.5 Dit artikel en titel 5.2 van de Algemene wet bestuursrecht zijn van overeenkomstige toepassing voor zover dit noodzakelijk is voor een goede uitoefening van de taken die de Autoriteit persoonsgegevens uitvoert in het kader van hoofdstuk VII van de verordening.

Wanneer de AP in samenwerking met andere toezichthouders opereert (hoofdstuk VII AVG) is zij niet zelf een toezichthouder in de zin van de Awb. Dit lid 5 maakt het desondanks mogelijk de bevoegdheden voor toezichthouders (titel 5.2 Awb) in te zetten in die situaties.

Artikel 16. Last onder bestuursdwang

- 16.1 De Autoriteit persoonsgegevens kan een last onder bestuursdwang opleggen ter handhaving van de bij of krachtens de verordening of deze wet gestelde verplichtingen.

Dit lid 1 legt formeel vast dat de AP een last onder bestuursdwang kan opleggen bij uitoefening van haar bevoegdheden uit de AVG of Uitvoeringswet.

- 16.2 De te betalen geldsom van een verbeurde dwangsom komt toe aan de Staat.

In afwijking van de hoofdregel uit het bestuursrecht komen eventuele dwangsommen niet toe aan de AP zelf (artikel 1:1 lid 4 Awb) maar aan de Staat.

Artikel 17. Boete bij onrechtmatige verwerking persoonsgegevens strafrechtelijke aard

- 17.1 De Autoriteit persoonsgegevens kan in geval van overtreding van het bepaalde in artikel 10 van de verordening of in artikel 31 van deze wet een bestuurlijke boete opleggen van ten hoogste 20.000.000 euro of, voor een onderneming, ten hoogste 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar indien dit bedrag hoger is.

17.2 Artikel 83, eerste tot en met derde lid, van de verordening zijn van overeenkomstige toepassing.

De AVG stelt geen boetes op overtreding van het verbod op verwerking van strafrechtelijke persoonsgegevens (artikel 10 AVG). Dit moet in nationaal recht worden geregeld. In Nederland is gekozen dit met even zware boetes te bestraffen als de verwerking van bijzondere persoonsgegevens (artikel 9 jo. 83 lid 5 AVG).

17.3 De bestuurlijke boete komt toe aan de Staat.

In afwijking van de hoofdregel uit het bestuursrecht komt de boete niet toe aan de AP zelf (artikel 1:1 lid 4 Awb) maar aan de Staat. Dit in verband met de onafhankelijke positie van de AP.

Artikel 18. Bestuurlijke boete aan overheden

18.1 De Autoriteit persoonsgegevens kan in geval van overtreding van het bepaalde in artikel 83, vierde, vijfde of zesde lid, van de verordening door een overheidsinstantie of een overheidsorgaan een bestuurlijke boete opleggen van ten hoogste de in deze leden genoemde bedragen.

18.2 Artikel 83, eerste tot en met derde lid, van de verordening zijn van toepassing.

De AVG bepaalt (artikel 83 lid 7) dat lidstaten zelf mogen bepalen of overheidsorganen administratieve boetes (artikel 83 AVG) kunnen worden opgelegd. Nederland heeft deze keuze gemaakt voor zowel de administratieve (artikel 83 lid 4 AVG) als de materiële (artikel 83 lid 5 AVG) overtredingen. Voor wat betreft strafrechtelijke persoonsgegevens zie artikel 17.

18.3 De bestuurlijke boete komt toe aan de Staat.

In afwijking van de hoofdregel uit het bestuursrecht komt de boete niet toe aan de AP zelf (artikel 1:1 lid 4 Awb) maar aan de Staat. Dit maakt het opleggen van de boete vooral symbolisch, wat nog steeds belangrijk is gezien de signaalfunctie die voor de maatschappij uitgaat van het beboeten van een overheidsorgaan voor schenden van een wet.

Artikel 19. Samenwerking met andere toezichthouders

- 19.1 De Autoriteit persoonsgegevens is bevoegd om in het belang van een efficiënt en effectief toezicht op de verwerking van persoonsgegevens afspraken te maken met andere toezichthouders en daartoe gezamenlijk met deze toezichthouders samenwerkingsprotocollen vast te stellen. Een samenwerkingsprotocol wordt bekendgemaakt in de Staatscourant.

De AP mag samenwerken met andere toezichthouders, maar moet daarvoor wel een samenwerkingsprotocol of convenant opstellen met deze andere partijen. Dit protocol wordt dan in de Staatscourant gepubliceerd. Reeds bestaande convenanten gelden bijvoorbeeld met de Autoriteit Consument & Markt, het Agentschap Telecom en de Nederlandse Zorgautoriteit. Sinds 22 oktober 2022 is er ook een samenwerking met De Nederlandsche Bank N.V. in verband met de naleving van de AVG, de Wet op het financieel toezicht (Wft) en de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft).

- 19.2 De Autoriteit persoonsgegevens en de toezichthouders, bedoeld in het eerste lid, zijn bevoegd uit eigen beweging en desgevraagd verplicht aan elkaar de gegevens betreffende de verwerking van persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van hun taak of om te kunnen voldoen aan een op hen rustende wettelijke verplichting.

Wanneer toezichthouders een convenant met elkaar aangaan, zijn zij vervolgens verplicht om elkaar informatie te verstrekken die noodzakelijk is voor het werk van de ander.

Artikel 20. In rechte optreden tegen inbreuken op verordening inzake doorgifte naar derde land

- 20.1 Indien de Autoriteit persoonsgegevens in een onderzoek betreffende de doorgifte van persoonsgegevens naar een land buiten de Europese Unie of naar een internationale organisatie, ingesteld op verzoek van een belanghebbende, gegronde redenen heeft om aan te nemen dat een door de Europese Commissie ten aanzien van het desbetreffende land of de desbetreffende internationale organisatie genomen adequaatheidsbesluit als bedoeld in artikel 45, eerste lid, van de verordening of een door de Europese Commissie genomen besluit met betrekking tot het vaststellen of goedkeuren van standaardbepalingen als bedoeld in artikel 46, tweede lid, onderdelen c en d, van de verordening onvoldoende waarborgen biedt voor een passend niveau van gegevensbescherming, kan de Autoriteit persoonsgegevens bij de Afdeling bestuursrechtspraak van de Raad van State een verzoek indienen om voor recht te verklaren dat het desbetreffende besluit geldig is.

Dit artikel 20 regelt de bevoegdheid van de AP om een door de Europese Commissie (de Commissie) genomen besluit tot adequaat verklaren van een land

(artikel 45 AVG) te toetsen. Deze bevoegdheid volgt uit het *Schrems*-arrest (HvJ EU 6 oktober 2015, ECLI:EU:C:2015:650 (Schrems I)).

Kort gezegd kan de AP dan een procedure starten bij de Afdeling bestuursrecht-spraak Raad van State (de Afdeling) om een verklaring voor recht te krijgen dat het besluit geldig is. Wanneer de Afdeling twijfels heeft over die geldigheid, is zij als hoogste nationale rechter verplicht prejudiciële vragen te stellen over het besluit aan het Hof van Justitie. Deze hakt daarmee feitelijk de knoop door.

20.2 Het verzoekschrift wordt ondertekend en bevat ten minste:

20.2(a) de dagtekening;

20.2(b) de gronden van het verzoek;

20.2(c) de namen van de belanghebbende en de partij die voorwerp is van het onderzoek, bedoeld in het eerste lid.

20.3 Bij het verzoekschrift wordt een afschrift overgelegd van het verzoek van de belanghebbende om handhaving van bij of krachtens wet bepaalde regels inzake de bescherming van persoonsgegevens, waarop het in het tweede lid bedoelde verzoekschrift van de Autoriteit persoonsgegevens betrekking heeft en worden andere op de zaak betrekking hebbende stukken meegezonden.

Het verzoekschrift vereist dat ten minste één betrokkene zich heeft gemeld. Relevante informatie hierover moet beschikbaar gesteld worden. Verder moet de AP motiveren op welke gronden zij de geldigheid wil laten toetsen. Afgezien van dat deze gronden “gegronde redenen” moeten bevatten, zijn er geen inhoudelijke eisen.

20.4 Onverminderd artikel 4:15 van de Algemene wet bestuursrecht wordt de termijn voor het geven van een beschikking op het verzoek om handhaving opgeschort gerekend vanaf de dag na die waarop de Autoriteit persoonsgegevens de verzoeker mededeelt dat toepassing is gegeven aan het eerste lid, tot de dag waarop de Afdeling bestuursrechtspraak van de Raad van State een uitspraak als bedoeld in het zesde lid heeft gedaan.

De beslistermijn op de onderliggende aanvraag van de betrokkene kan worden opgeschort, analoog aan artikel 4:15 Awb tot het moment dat de Afdeling een eindoordeel heeft geveld.

- 20.5 Op de behandeling van het verzoek zijn de titels 8.1 en 8.2 van de Algemene wet bestuursrecht van overeenkomstige toepassing, met uitzondering van de artikelen 8:1 tot en met 8:10, 8:41, de afdelingen 8.2.2a en 8.2.4a en de artikelen 8:70, 8:72 en 8:74. De in het tweede lid, onderdeel c, bedoelde partijen worden als partijen in het geding aangemerkt.

Op de verzoekschriftprocedure wordt de Awb van overeenkomstige toepassing verklaard.

- 20.6 Indien de Afdeling bestuursrechtspraak van de Raad van State, al dan niet na prejudiciële verwijzing op grond van artikel 267 van het Verdrag inzake de werking van de Europese Unie aan het Hof van Justitie van de Europese Unie, tot het oordeel komt dat het aan haar voorgelegde besluit van de Europese Commissie geldig is, dan verklaart zij dat voor recht. Komt zij, na prejudiciële verwijzing aan het Hof van Justitie van de Europese Unie, tot het oordeel dat het aan haar voorgelegde besluit ongeldig is, dan wijst zij het verzoek af.

Het eindoordeel van de Afdeling bestuursrechtspraak moet natuurlijk geënt zijn op de uitspraak van het Hof van Justitie van de Europese Unie (het Hof).

- 20.7 De Afdeling bestuursrechtspraak van de Raad van State kan besluiten het verzoek aan te houden als er bij het Hof van Justitie van de Europese Unie al een prejudiciële vraag omtrent de geldigheid van het desbetreffende besluit aanhangig is.

- 20.8 Tegen het aanhouden van het verzoek door de Afdeling bestuursrechtspraak van de Raad van State, staat geen voorziening open.

De Afdeling bestuursrechtspraak mag het verzoek aanhouden als er reeds andere procedures lopen bij het Hof over hetzelfde adequaatheidsbesluit. Het is niet mogelijk om bezwaar of beroep aan te tekenen tegen dergelijk aanhouden.

Artikel 21. Aanwijzing accrediterende instantie

Bij ministeriële regeling wordt of de Autoriteit persoonsgegevens of de Raad voor Accreditatie of worden zij beide aangewezen als accrediterende instantie als bedoeld in artikel 43 van de verordening.

Om het werk van de toezichthouder te verlichten, kunnen onder artikel 43 AVG andere instanties worden aangewezen die het proces van certificering (artikel 42 AVG) kunnen uitvoeren. Dergelijke instanties moeten zijn geaccrediteerd. De AVG laat daarbij de mogelijkheid open dat een land kiest voor hetzij de toezichthouder als accrediterende instantie (certificeringsorganen), hetzij de reeds

bestaande nationale accrediterende instantie, in Nederland de Raad voor Accreditatie. Nederland laat deze keuze aan de minister. Deze heeft vooralsnog geen keuze gemaakt.

Artikel 21a. Toezicht op naleving PSD II

21a.1 De taak van de Autoriteit persoonsgegevens, bedoeld in artikel 6, derde lid, omvat mede het toezicht op de naleving van de krachtens artikel 3:17, zevende lid, van de Wet op het financieel toezicht gestelde verplichtingen met betrekking tot de toegang van betaaldienstverleners tot de persoonsgegevens van betaaldienstgebruikers.

Dit artikel breidt de taakstelling van de AP uit naar de Wft. Artikel 3:17 lid 7 hiervan schrijft voor dat een betalingsdientaanbieder alleen met de uitdrukkelijke toestemming van de betalingsdienstgebruiker toegang mag krijgen tot persoonsgegevens. Gebruik daarvan moet dan beperkt zijn tot wat noodzakelijk is voor het aanbieden van betalingsdiensten.

PSD II. Dit vereiste is afkomstig uit de Payment Services Directive II (PSD, Richtlijn (EU) 2015/2366), en geldt bovenop de eisen die de AVG stelt aan de verwerking van persoonsgegevens. Voor het verwerken van persoonsgegevens ten behoeve van het verlenen van betaaldiensten moet zowel aan het vereiste in artikel 94 tweede lid van de PSD II, als aan de eisen uit de AVG worden voldaan.

Titel. Artikel 21a heeft in de officiële wetstekst geen titel. Wij hebben dit alternatief aangedragen.

21a.2 Met betrekking tot het toezicht, bedoeld in het eerste lid, vindt de samenwerking en uitwisseling van informatie met De Nederlandsche Bank N.V. en andere relevante toezichthouders plaats overeenkomstig artikel 26 van de richtlijn betaaldiensten, bedoeld in artikel 1:1 van de Wet op het financieel toezicht.

Bij financiële dienstverleners houden ook De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten toezicht. De AP moet als nieuwe toezichthouder samenwerken met deze partijen.

- 21a.3 De Autoriteit persoonsgegevens kan in geval van overtreding van de krachtens artikel 3.17, zevende lid, van de Wet op het financieel toezicht gestelde verplichtingen aan de overtreder een last opleggen om waar passend, op een nader bepaalde manier en binnen een nader bepaalde termijn, verwerkingen in overeenstemming te brengen met het daar bepaalde. Artikel 16 is van overeenkomstige toepassing.

Bij toezicht onder de Wft kan de AP een bindende aanwijzing oftewel last opleggen. Vergelijk artikel 16 voor de last onder bestuursdwang voor het naleven van de AVG.

- 21a.4 De Autoriteit persoonsgegevens kan in geval van een overtreding van de krachtens artikel 3.17, zevende lid, van de Wet op het financieel toezicht gestelde verplichtingen aan de overtreder een bestuurlijke boete opleggen van ten hoogste 20.000.000 euro of, indien dit meer is, ten hoogste 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar. Artikel 83, tweede en derde lid, van de verordening is van overeenkomstige toepassing.

De boetebevoegdheid van de AP wordt hiermee uitgebreid naar artikel 3.17 Wft. De omvang van de boete is gelijk aan de hoogste categorie uit de AVG (artikel 83 lid 5 AVG).

- 21a.5 De bestuurlijke boete en de te betalen geldsom van een verbeurde dwangsom komen toe aan de Staat.

In afwijking van de hoofdregel uit het bestuursrecht komt de boete niet toe aan de AP zelf (artikel 1:1 lid 4 Awb) maar aan de Staat. Dit maakt het opleggen van de boete vooral symbolisch, wat nog steeds belangrijk is gezien de signaalfunctie die voor de maatschappij uitgaat van het beboeten van een overheidsorgaan voor schenden van een wet.

Hoofdstuk 3

Bepalingen ter uitvoering van de verordening

Hoofdstuk 3 regelt de omgang met en uitzonderingen op een aantal verwerkingsverboden, met name rondom bijzondere persoonsgegevens (paragraaf 3.1), de strafrechtelijke persoonsgegevens (paragraaf 3.2) en de rol van de AP en de rechter bij conflicten (paragraaf 3.3).

PARAGRAAF 3.1. BIJZONDERE CATEGORIEËN VAN PERSOONSgegevens

Artikel 22. Verwerkingsverbod bijzondere categorieën persoonsgegevens en algemene uitzonderingen uit verordening

22.1 Overeenkomstig artikel 9, eerste lid, van de verordening zijn verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid verboden.

Dit lid 1 herhaalt het algemene verwerkingsverbod uit de AVG (artikel 9) voor bijzondere persoonsgegevens.

22.2 Overeenkomstig artikel 9, tweede lid, onderdelen a, c, d, e en f, van de verordening is het verbod om bijzondere categorieën van persoonsgegevens te verwerken niet van toepassing, indien:

22.2(a) de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden;

22.2(b) de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;

22.2(c) de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;

22.2(d) de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt; of

22.2(e) de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.

Dit lid 2 herhaalt de algemene en direct werkende uitzonderingen op het algemene verwerkingsverbod uit de AVG (artikel 9) voor bijzondere persoonsgegevens.

Artikel 23. Nationaalrechtelijke algemene uitzonderingen

Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om bijzondere categorieën van persoonsgegevens te verwerken niet van toepassing, indien:

Onder artikel 9 lid 2 punt g AVG mogen lidstaten aanvullende uitzonderingen introduceren op het verwerkingsverbod van bijzondere persoonsgegevens. Nederland heeft in drie gevallen een dergelijke uitzondering gemaakt.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 9 lid 2 punt g AVG.

a. de verwerking noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting;

De eerste uitzondering is wanneer de noodzaak voor de verwerking voortvloeit uit een verdrag of andere volkenrechtelijke verplichting.

- b. de gegevens worden verwerkt door de Autoriteit persoonsgegevens of een ombudsman als bedoeld in artikel 9:17 van de Algemene wet bestuursrecht, en voor zover de verwerking noodzakelijk is voor de uitvoering van de hun wettelijk opgedragen taken, onder voorwaarde dat bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad; of

De tweede uitzondering is wanneer de AP of de Nationale Ombudsman de bijzondere persoonsgegevens nodig heeft in de uitoefening van haar taak. Gezien de aard van de werkzaamheden van deze twee instanties ligt het voor de hand dat zij regelmatig bijzondere persoonsgegevens zullen verwerken van belanghebbenden.

- c. de verwerking noodzakelijk is in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard voor de doeleinden waarvoor deze gegevens worden verwerkt.

De derde uitzondering is wanneer de verwerking noodzakelijk is voor een verwerking van strafrechtelijke persoonsgegevens. Voor die laatste is dan al een grondslag (en uitzondering onder artikel 10 AVG).

Artikel 24. Uitzonderingen voor wetenschappelijk of historisch onderzoek of statistische doeleinden

Gelet op artikel 9, tweede lid, onderdeel j, van de verordening, is het verbod om bijzondere categorieën van persoonsgegevens te verwerken niet van toepassing, indien:

Vanwege het belang van wetenschappelijk of historisch onderzoek of statistische doeleinden bevat de AVG (artikel 89) een aparte regeling daarvoor, die in nationale wetgeving kan worden uitgewerkt. In Nederland geldt daarbij dat het toegestaan is voor dergelijk onderzoek bijzondere persoonsgegevens te verwerken als aan vier voorwaarden is voldaan.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 9 lid 2 punt j AVG.

- a. de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid, van de verordening;

Allereerst moet de verwerking natuurlijk redelijkerwijs noodzakelijk zijn voor het onderzoek. Zie artikel 89 AVG over de reikwijdte van dit begrip.

- b. het onderzoek, bedoeld in onderdeel a, een algemeen belang dient;

Ten tweede moet het onderzoek een algemeen belang dienen. Een zelf opgezet onderzoek van een bedrijf zal hier natuurlijk niet aan voldoen, maar een veldonderzoek van een universiteit of hogeschool in veel gevallen wel.

- c. het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en

Ten derde moet vaststaan dat het vragen van uitdrukkelijke toestemming (de voor de hand liggende manier om het verwerkingsverbod op te heffen, artikel 9 lid 2 punt a AVG) niet haalbaar is.

- d. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Ten vierde moet de verwerkingsverantwoordelijke maatregelen hebben genomen (en hebben uitgewerkt) om te voorkomen dat de privacy van betrokkenenodeloos wordt geschaad.

Artikel 25. Uitzonderingen inzake verwerking persoonsgegevens waaruit ras of etnische afkomst blijkt

Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om persoonsgegevens te verwerken waaruit ras of etnische afkomst blijkt, niet van toepassing, indien de verwerking geschiedt:

In Nederland kan het verbod op verwerken van persoonsgegevens omtrent etnische afkomst in twee specifieke situaties worden opgeheven, naast de algemene uitzonderingen uit artikel 9 lid 2 AVG.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 9 lid 2 sub g AVG.

- a. met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is; of

Allereerst is het toegestaan om bijzondere persoonsgegevens omtrent etnische afkomst te gebruiken als dat onvermijdelijk is voor identificatie van de betrokkene. Een foto is niet per se een bijzonder persoonsgegeven, maar wel wanneer het beoogde gebruik identificatie of authenticatie is (overweging 51 AVG). Een foto op een identiteitskaart valt onder die definitie, maar met deze regeling is zo'n kaart dus geen probleem. Dit geldt overigens zowel bij nationale identiteitsbewijzen als bij private identiteitskaarten zoals werknemerspassen.

- b. met het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen teneinde feitelijke nadelen, verband houdende met de grond ras of etnische afkomst, op te heffen of te verminderen, en slechts voor zover:
 - b(1) de verwerking voor dat doel noodzakelijk is;
 - b(2) de gegevens betrekking hebben op het geboorteland van de betrokkene, diens ouders of diens grootouders, dan wel op andere, bij wet vastgestelde criteria op grond waarvan op objectieve wijze vastgesteld kan worden of iemand tot een bepaalde etnische of culturele minderheidsgroep behoort; en
 - b(3) de betrokkene tegen de verwerking geen schriftelijk bezwaar heeft gemaakt.

Ten tweede is het toegestaan om bijzondere persoonsgegevens omtrent etnische afkomst te gebruiken wanneer dat nodig is voor wat populair heet “positieve discriminatie” of iets netter “voorkeursbeleid”. De gegevens moeten dan beperkt blijven tot geboorteland of -regio of andere wettelijk vastgestelde criteria omtrent de etnische groep.

Bezwaar. De betrokkene kan bezwaar maken tegen dergelijk gebruik van zijn of haar persoonsgegevens. Dit bezwaar moet worden gehonoreerd.

Artikel 26. Uitzonderingen inzake verwerking persoonsgegevens waaruit politieke opvattingen blijken voor vervulling openbare functies

Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om persoonsgegevens te verwerken waaruit politieke opvattingen blijken, niet van toepassing, indien de verwerking geschiedt met het oog op de eisen die met betrekking tot politieke opvattingen in redelijkheid kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges.

Voor bepaalde functies in bestuursorganen en adviescolleges is de politieke gezindheid van de persoon van groot belang. Denk aan burgemeestersbenoemingen. Het verwerkingsverbod is dan ook opgeheven voor deze specifieke situaties.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 9 lid 2 punt g AVG.

Artikel 27. Uitzonderingen inzake verwerking persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken voor geestelijke verzorging

27.1 Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om persoonsgegevens te verwerken waaruit religieuze of levensbeschouwelijke overtuigingen blijken, niet van toepassing, indien de verwerking geschiedt door andere instellingen dan de instellingen, bedoeld in artikel 22, tweede lid, onderdeel c, en voor zover de verwerking noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene, tenzij deze daartegen schriftelijk bezwaar heeft gemaakt.

Een religieuze of levensbeschouwelijke organisatie mag persoonsgegevens dienaangaande verwerken van haar leden of betrokkenen (artikel 9 lid 2 punt d AVG). Voor andere instellingen die bijdragen aan geestelijke verzorging (bijvoorbeeld een verzorgingstehuis voor ouderen) creëert dit artikel 27 een vergelijkbare ontheffing.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 9 lid 2 punt g AVG.

27.2 In de gevallen, bedoeld in het eerste lid, worden geen persoonsgegevens aan derden verstrekt zonder toestemming van de betrokkene.

Het gebruik van die persoonsgegevens moet echter beperkt blijven tot de instelling zelf. Verstrekking aan anderen is niet toegestaan zonder (uitdrukkelijke) toestemming van de betrokkene.

Artikel 28. Uitzonderingen inzake genetische gegevens

28.1 Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om genetische gegevens te verwerken niet van toepassing, indien deze verwerking plaatsvindt met betrekking tot de betrokkene bij wie de desbetreffende gegevens zijn verkregen.

Het verwerken van genetische gegevens van een betrokkene kan ertoe leiden dat informatie over familieleden van de betrokkene bekend wordt. Het verwerkingsverbod uit de AVG voor deze categorie persoonsgegevens wordt dan ook maar beperkt opgeheven in Nederland: alleen voor zover het gaat om verwerking omtrent de betrokkene zelf. Een DNA-analyse mag dus geen informatie geven over anderen dan de aanvrager die zijn of haar eigen DNA-materiaal verstrekke.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 9 lid 2 punt g AVG.

28.2 In andere gevallen dan bedoeld in het eerste lid, is het verbod om genetische gegevens te verwerken uitsluitend niet van toepassing, indien:

28.2(a) een zwaarwegend geneeskundig belang prevaleert; of

28.2(b) de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek dat een algemeen belang dient of ten behoeve van statistiek, indien:

1°. de betrokkene uitdrukkelijke toestemming heeft gegeven; en

2°. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

28.3 Toestemming als bedoeld in het tweede lid, onderdeel b, is niet vereist, indien het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning vergt.

In andere gevallen dan bedoeld in lid 1, bijvoorbeeld bij DNA-onderzoek waarbij ook familie in beeld komt, is er geen sprake van een categorische onthefing. Er moet dan sprake zijn van een zwaarwegend geneeskundig belang (zoals een ernstige ziekte) of een onderzoek van algemeen belang. In dat laatste geval moet uitdrukkelijke toestemming van de betrokkene verkregen zijn en moeten bijzondere waarborgen zijn genomen om de privacy van alle betrokkenen te beschermen.

Artikel 29. Uitzonderingen inzake biometrische gegevens

Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

Het is in Nederland toegestaan om biometrische gegevens te verwerken voor authenticatie- of beveiligingsdoeleinden. Wel moet de noodzaak van deze wijze van authenticeren of beveiligen zijn aangetoond; zijn werkelijk geen alternatieven zoals pincodes of pasjes mogelijk?

Grondslag. De AVG staat deze nationale regeling toe onder artikel 9 lid 2 punt g AVG.

Artikel 30. Uitzonderingen inzake gegevens over gezondheid

30.1 Gelet op artikel 9, tweede lid, onderdeel b, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing, indien de verwerking geschiedt door bestuursorganen, pensioenfondsen, werkgevers of instellingen die te hunnen behoeve werkzaam zijn, en voor zover de verwerking noodzakelijk is voor:

30.1(a) een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene; of

30.1(b) de re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.

Het verbod op verwerking van persoonsgegevens omtrent gezondheid wordt opgeheven wanneer deze gegevens nodig zijn bij een bestuursorgaan, werkgever of pensioenfonds. De noodzaak volgt dan uit het feit dat de betrokkene een recht uitoefent waarbij de gezondheid relevant is, zoals een ziekmelding of een aanvullend pensioen vanwege een gezondheidsprobleem.

Grondslag. Dit artikel levert tevens de grondslag uitvoering wettelijke plicht op (artikel 6 lid 1 punt c AVG).

30.2 Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing, indien de verwerking geschiedt door:

30.2(a) scholen, voor zover de verwerking met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is;

30.2(b) een reclasseringsinstelling, een bijzondere reclasseringsambtenaar, de raad voor de kinderbescherming, de gecertificeerde instelling, bedoeld in artikel 1.1 van de Jeugdwet, of de rechtspersoon, bedoeld in artikel 256, eerste lid, of artikel 302, tweede lid, van Boek 1 van het Burgerlijk Wetboek, voor zover de verwerking noodzakelijk is voor de uitvoering van de aan hen opgedragen wettelijke taken; of

30.2(c) Onze Minister en Onze Minister van Justitie en Veiligheid voor zover de verwerking in verband met de tenuitvoerlegging van vrijheidsbenemende maatregelen noodzakelijk is.

Het verbod op verwerking van persoonsgegevens omtrent gezondheid wordt opgeheven wanneer deze gegevens nodig zijn bij scholen, reclassering of Jus-

titie voor taken waarbij gezondheid relevant is. Bij scholen is dat beperkt tot begeleiding of speciale voorzieningen die nodig zijn voor de leerlingen om deel te nemen aan het onderwijs.

Grondslag. Dit artikel levert tevens de grondslag uitvoering wettelijke plicht op (artikel 6 lid 1 punt c AVG).

30.3 Gelet op artikel 9, tweede lid, onderdeel h, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing indien de verwerking geschiedt door:

30.3(a) hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk; of

30.3(b) verzekeraars als bedoeld in artikel 1:1 van de Wet op het financieel toezicht of financiële dienstverleners die bemiddelen in verzekeringen als bedoeld in artikel 1:1 van die wet, voor zover de verwerking noodzakelijk is voor:

1. de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt; of

2. de uitvoering van de overeenkomst van verzekering dan wel het assisteren bij het beheer en de uitvoering van de verzekering.

Het verbod op verwerking van persoonsgegevens omtrent gezondheid wordt opgeheven wanneer deze gegevens nodig zijn voor een goede verzorging van de betrokkene, of wanneer een verzekeraar deze gegevens nodig heeft om een goede risico-inschatting te maken. Denk bij het laatste bijvoorbeeld aan een overlijdensrisicoverzekering.

Grondslag. Dit artikel levert tevens de grondslag uitvoering geneeskundige behandelovereenkomst dan wel verzekeringsovereenkomst op (artikel 6 lid 1 punt b AVG).

- 30.4 Indien toepassing wordt gegeven aan het eerste, tweede of derde lid, worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verwerkingsverantwoordelijke persoonlijk gegevens verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die krachtens het eerste, tweede of derde lid bevoegd zijn tot verwerking daarvan.

Gegevens inzake gezondheid mogen alleen worden behandeld door partijen die aan het medisch beroepsgeheim zijn gebonden. De regels uit dit beroepsgeheim gaan daarbij boven die uit de AVG.

Persoonlijk verwerken. Een kleine zelfstandige zou zelf gegevens over gezondheid van personeel kunnen verwerken. Dit mag voor zover noodzakelijk voor het werk, maar hierop geldt dan wel een strenge geheimhoudingsplicht. Denk bijvoorbeeld aan een medewerker die epilepsie heeft, wat voor de zelfstandige van belang is om rekening te houden met situaties waarin acuut gehandeld dient te worden.

- 30.5 Het verbod om andere bijzondere categorieën van persoonsgegevens te verwerken is niet van toepassing, indien de verwerking noodzakelijk is in aanvulling op de verwerking van gegevens over gezondheid, bedoeld in het derde lid, aanhef en onderdeel a, met het oog op een goede behandeling of verzorging van de betrokkene.

Wanneer andere bijzondere persoonsgegevens nodig zijn voor een goede medische behandeling of verzorging van de betrokkene, mogen partijen die bevoegd zijn die behandeling of verzorging te geven ook die andere persoonsgegevens verwerken. Een voorbeeld is een verzorgingstehuis dat de religie van bewoners bijhoudt om zo ook geestelijke verzorging op maat te kunnen bieden. Het registreren van etnische afkomst om zo medicatie of psychiatrische behandeling aan te passen zou hier ook onder vallen.

- 30.6 Bij algemene maatregel van bestuur kunnen omtrent de toepassing van het eerste lid en het derde lid, aanhef en onderdeel b, nadere regels worden gesteld.

Omtrent de omgang met gezondheidsgegevens door werkgevers en pensioenfondsen (lid 1) en verzekeraars (lid 3 punt b) kunnen bij Algemene Maatregel van Bestuur (AMvB) nadere regels worden gesteld.

PARAGRAAF 3.2. PERSOONSgegevens VAN STRAFRECHTELIJKE AARD

Artikel 31. Uitzonderingen op de verplichting tot verwerking onder overheidstoezicht

Onverminderd artikel 10 van de verordening mogen persoonsgegevens van strafrechtelijke aard alleen worden verwerkt voor zover dit krachtens de artikelen 32 en 33 is toegestaan.

De verwerking van persoonsgegevens van strafrechtelijke aard (artikel 10 AVG) is alleen toegestaan als dit bij Unierecht of nationaal recht is geregeld. Dit artikel 31 werkt deze mogelijkheid nader uit, maar beperkt de reikwijdte meteen door te bepalen dat alleen artikel 32 (algemene uitzonderingsgronden) en artikel 33 (overige uitzonderingen) dergelijke mogelijkheden bieden. Andere wetten die lijken te gaan over strafrechtelijke persoonsgegevens, kunnen dus niet worden ingezet als nationale regeling bedoeld in artikel 10 AVG.

Artikel 32. Algemene uitzonderingsgronden inzake gegevens van strafrechtelijke aard

Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt, indien:

De algemene uitzonderingsgronden zijn geformuleerd analoog aan artikel 9 lid 2 AVG, dat algemene uitzonderingsgronden bevat voor het verwerkingsverbod van bijzondere persoonsgegevens.

Grondslag. In tegenstelling tot artikel 9 lid 2 AVG, dat slechts het verwerkingsverbod opheft, geeft artikel 32 Uitvoeringswet een grondslag voor verwerking van de strafrechtelijke persoonsgegevens als aan de genoemde randvoorwaarden is voldaan.

- a. de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden;

De eerste uitzondering op het verbod om strafrechtelijke persoonsgegevens te verwerken is de uitdrukkelijke toestemming van de betrokkene. Zie ook artikel 9 lid 2 punt a AVG.

- b. de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;

Een verwerking van strafrechtelijke persoonsgegevens is ook toegestaan als deze noodzakelijk is voor een vitaal belang (levensbelang). De betrokkene moet dan niet in staat zijn om toestemming te geven. Vergelijk artikel 9 lid 2 punt c AVG.

- c. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;

Een andere uitzondering is wanneer de betrokkene de strafrechtelijke persoonsgegevens kennelijk (evident) zelf openbaar heeft gemaakt. Het moet dan gaan om een spontane handeling van de betrokkene waardoor het persoonsgegeven kenbaar wordt voor anderen. Vergelijk artikel 9 lid 2 punt e AVG.

- d. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid;

De verwerking van strafrechtelijke persoonsgegevens is daarnaast toegestaan indien dat noodzakelijk is in het kader van gerechtelijke procedures, bijvoorbeeld omdat een bewijsstuk moet worden overlegd waarin relevante doch bijzondere persoonsgegevens zijn opgenomen. Vergelijk artikel 9 lid 2 punt f AVG.

- e. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang als bedoeld in artikel 23, onderdelen a en b; of

De verwerking van bijzondere persoonsgegevens is niet verboden (artikel 23) wanneer dit noodzakelijk is voor een volkenrechtelijke verplichting (artikel 23 punt a) of voor verwerking door de toezichthouder dan wel de Nationale Ombudsman (artikel 23 punt b). Dezelfde uitzonderingen gelden voor strafrechtelijke persoonsgegevens.

- f. de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid, van de verordening, en is voldaan aan de voorwaarden, bedoeld in artikel 24, onderdelen b tot en met d.

Als laatste grond kan verwerking van strafrechtelijke persoonsgegevens toegestaan zijn als dat noodzakelijk is voor archivering in het openbaar belang of voor onderzoek of statistiek (artikel 89 AVG). Wel moeten passende waarborgen worden genomen om de basis van het grondrecht privacy en de belangen van de betrokkene te beschermen. Vergelijk artikel 9 lid 2 punt j AVG.

Voorbeeld. Het hof gaat al deze leden af in een zaak van Ziggo tegen Brein van 10 oktober 2022. Brein had in deze zaak onderzoek gedaan en de IP-adressen vergaard via welke onrechtmatig auteursrechtelijk beschermde werken werden gedownload. Brein verzocht hierbij Ziggo, die de adressen van de bijbehorende IP-adressen onder zich heeft, een waarschuwingsbrief te sturen aan hen. Het hof oordeelt dat dit strafrechtelijke gegevens zijn (omdat auteursrechtinbreuk strafbaar is gesteld), en Ziggo geen grond heeft op basis van artikel 32 Uitvoeringswet om deze gegevens te verstrekken. De rechter loopt langs alle leden, en stelt dat de enige mogelijk toepasselijke situatie hier zou zijn dat Ziggo een

vergunning van de AP voor de verstrekking krijgt. Aangezien die er niet was, zou een verstrekking onrechtmatig zijn (Gerechtshof Arnhem-Leeuwarden 11 oktober 2022, ECLI:NL:GHARL:2022:8676).

Artikel 33. Overige uitzonderingsgronden inzake gegevens van strafrechtelijke aard

33.1 Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt, indien:

Naast de algemene uitzonderingen van artikel 32 biedt dit artikel 33 een aantal specifieke grondslagen voor het verwerken van strafrechtelijke persoonsgegevens.

33.1(a) de verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, dan wel door verwerkingsverantwoordelijken die deze hebben verkregen krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens;

Allereerst mogen deze persoonsgegevens worden verwerkt door alle actoren betrokken bij het strafrecht, zoals de politie en het Openbaar Ministerie of partijen die onder de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens toegang krijgen tot die gegevens.

33.1(b) de verwerking geschiedt door en ten behoeve van publiekrechtelijke samenwerkingsverbanden van verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken, indien:

1°. de verwerking noodzakelijk is voor de uitvoering van de taak van deze verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken; en

2°. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad; of

Ten tweede mogen deze persoonsgegevens worden verwerkt binnen samenwerkingsverbanden tussen overheidsinstanties, als dit noodzakelijk is voor hun werk en adequate waarborgen zijn getroffen. Deze verwerking moet natuurlijk tot een specifieke wettelijke regeling te herleiden zijn.

33.1(c) de verwerking noodzakelijk is in aanvulling op de verwerking van gegevens over gezondheid, bedoeld in artikel 30, derde lid, aanhef en onderdeel a, met het oog op een goede behandeling of verzorging van de betrokkene.

Ten derde mogen deze persoonsgegevens worden verwerkt door partijen in het veld van de gezondheidszorg als dit noodzakelijk is om de betrokkene te behandelen.

33.2 Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de verwerkingsverantwoordelijke die deze gegevens ten eigen behoeve verwerkt:

Lid 2 voegt een aantal specifieke uitzonderingsgronden toe voor verwerkingsverantwoordelijken om voor zichzelf strafrechtelijke persoonsgegevens te verwerken.

33.2(a) ter beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren; of

Allereerst mag een verwerkingsverantwoordelijke deze persoonsgegevens verwerken als dat nodig is om een verzoek van de betrokkene om een beslissing of een prestatie (zoals een levering of dienstverlening) af te handelen. Natuurlijk mag het verkrijgen van deze persoonsgegevens geen doel op zich zijn van de verwerkingsverantwoordelijke.

33.2(b) ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn.

Ten tweede mag een verwerkingsverantwoordelijke deze persoonsgegevens verwerken om bewijs rondom een strafbaar feit vast te leggen waar hij zelf bij betrokken is. Denk aan een bedrijf dat overvallen wordt.

33.3 Persoonsgegevens van strafrechtelijke aard over personeel in dienst van de verwerkingsverantwoordelijke mogen uitsluitend worden verwerkt, indien dit geschiedt overeenkomstig regels die zijn vastgesteld in overeenstemming met de procedure bedoeld in de Wet op de ondernemingsraden.

Wanneer het gaat om strafrechtelijke persoonsgegevens van personeel, moet daarbij aanvullend de Wet op de ondernemingsraden (Wor) worden gevolgd (zie artikel 27 lid 1 sub k Wor).

33.4 Persoonsgegevens van strafrechtelijke aard mogen ten behoeve van derden worden verwerkt:

33.4(a) door verwerkingsverantwoordelijken die optreden krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus;

33.4(b) indien deze derde een rechtspersoon is die in dezelfde groep is verbonden als bedoeld in artikel 24b van Boek 2 van het Burgerlijk Wetboek; of

33.4(c) indien de Autoriteit persoonsgegevens met inachtneming van het vijfde lid een vergunning voor de verwerking heeft verleend.

Het verwerken van strafrechtelijke persoonsgegevens voor anderen is eigenlijk alleen toegestaan door particuliere beveiligings- en recherchebureaus, en daaraan verbonden organisaties, of aan organisaties die een specifieke vergunning hebben verkregen van de AP.

33.5 Een vergunning als bedoeld in het vierde lid, onderdeel c, kan slechts worden verleend, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Aan de vergunning kunnen voorschriften worden verbonden.

De vergunning om strafrechtelijke persoonsgegevens te verwerken wordt alleen verleend in gevallen waarin een zwaarwegend belang bestaat en adequate waarborgen zijn getroffen.

Zwarte lijsten. Dit lid 5 gaat met name over situaties waarin samenwerkende bedrijven een gezamenlijke zwarte lijst willen aanleggen van bijvoorbeeld wanbetalers of overlastgevende bezoekers.

PARAGRAAF 3.3. RECHTSBESCHERMING

Artikel 34. Toepasselijkheid Algemene wet bestuursrecht bij beslissing van bestuursorganen

Een schriftelijke beslissing op een verzoek als bedoeld in de artikelen 15 tot en met 22 van de verordening wordt genomen binnen de in artikel 12, derde lid, van de verordening genoemde termijnen en geldt, voor zover deze is genomen door een bestuursorgaan, als een besluit in de zin van de Algemene wet bestuursrecht.

Wanneer een bestuursorgaan een verzoek ontvangt tot uitoefening van rechten onder de AVG (artikelen 15 tot en met 22), wordt een dergelijk verzoek behandeld onder de Awb. Dit betekent onder meer dat de reactie op het verzoek wordt gezien als een besluit, maar ook dat bij het niet tijdig nemen van een besluit de burger dwangsommen kan incasseren bij het bestuursorgaan. Bij andere werkingsverantwoordelijken geldt artikel 35 hieronder.

Artikel 35. Toepasselijkheid burgerlijk recht bij beslissing van niet-bestuursorganen

- 35.1 Indien de beslissing op een verzoek als bedoeld in artikel 34 is genomen door een ander dan een bestuursorgaan, kan de belanghebbende zich tot de rechtbank wenden met het schriftelijk verzoek de verwerkingsverantwoordelijke te bevelen het verzoek als bedoeld in de artikelen 15 tot en met 22 van de verordening alsnog toe of af te wijzen.

Wanneer een verwerkingsverantwoordelijke een verzoek ontvangt tot uitoefening van rechten onder de AVG en daarbij geen bestuursorgaan is (zie artikel 34), kan de betrokkene bij een negatieve reactie een verzoekschriftprocedure bij de burgerlijke rechter starten om alsnog zijn recht te halen.

- 35.2 Het verzoekschrift wordt ingediend binnen zes weken na ontvangst van het antwoord van de verwerkingsverantwoordelijke. Indien de verwerkingsverantwoordelijke niet binnen de in artikel 12, derde lid, van de verordening genoemde termijnen heeft geantwoord, is de indiening van het verzoekschrift niet aan een termijn gebonden.

De termijn voor het indienen van een verzoekschrift is zes weken na ontvangst van de reactie van de verwerkingsverantwoordelijke. Komt er in het geheel geen reactie, dan is er ook geen deadline voor het verzoekschrift.

- 35.3 De rechtbank wijst het verzoek toe, voor zover zij dit gegrond oordeelt. Alvorens de rechtbank beslist, stelt zij zo nodig de belanghebbenden in de gelegenheid hun zienswijze naar voren te brengen.

In de verzoekschriftprocedure zal de rechtbank de belanghebbenden hun zienswijze laten geven, om vervolgens een gemotiveerde beschikking over het verzoek te geven.

- 35.4 De indiening van het verzoekschrift behoeft niet door een advocaat te geschieden.

Bij een verzoekschriftprocedure mag men in persoon procederen. Gezien de aard van de onderliggende conflicten (inzage en correctie in persoonsgegevens) is ook geen bijzondere juridische kennis vereist.

- 35.5 De derde afdeling van de vijfde titel van het Tweede Boek van het Wetboek van Burgerlijke Rechtsvordering is van overeenkomstige toepassing.

De rechtbank mag haar beschikking versterken met een dwangsom, te betalen door de verwerkingsverantwoordelijke als niet alsnog gehoor wordt gegeven aan het uitgeoefende recht.

- 35.6 De rechtbank kan partijen en anderen verzoeken binnen een door haar te bepalen termijn schriftelijke inlichtingen te geven en onder hen berustende stukken in te zenden. De verwerkingsverantwoordelijke en belanghebbende zijn verplicht aan dit verzoek te voldoen. De artikelen 8:45, tweede en derde lid, en 8:29 van de Algemene wet bestuursrecht zijn van overeenkomstige toepassing.

In het kader van de procedure kan de rechtbank partijen vragen informatie en stukken aan te leveren om zo een grondig voorbereide beschikking uit te spreken.

Artikel 36. Geschilbeslechting door Autoriteit persoonsgegevens of via gedragscode

- 36.1 De belanghebbende kan zich ook binnen de termijn bepaald voor het instellen van beroep op grond van de Algemene wet bestuursrecht, dan wel die, bedoeld in artikel 35, tweede lid, tot de Autoriteit persoonsgegevens wenden met het verzoek te bemiddelen of te adviseren in zijn geschil met de verwerkingsverantwoordelijke, dan wel gebruik maken van een geschillenbeslechtsingsregeling als bedoeld in artikel 40, tweede lid, onderdeel k, van de verordening, op grond van een goedgekeurde gedragscode als bedoeld in artikel 40, vijfde lid, van de verordening. In dat geval kan het beroep in afwijking van artikel 6:7 van de Algemene wet bestuursrecht nog worden ingesteld dan wel de procedure ingevolge artikel 35 nog aanhangig worden gemaakt nadat de belanghebbende van de Autoriteit persoonsgegevens bericht heeft ontvangen dat de behandeling van de zaak is beëindigd of ingevolge de geschillenbeslechtsingsregeling, bericht heeft ontvangen dat de behandeling van de zaak is beëindigd, doch uiterlijk zes weken na dat tijdstip.

Een belanghebbende die met een conflict omtrent de omgang met persoonsgegevens zit, kan de AP verzoeken om te bemiddelen of te adviseren in dat conflict. Valt die omgang onder een gedragscode, dan kan hij tevens de geschillenbeslechting daaruit inroepen. In deze gevallen wordt de termijn voor het instellen van beroep (artikel 6:7 Awb) opgeschort totdat deze stappen zijn uitgevoerd.

- 36.2 Tijdens de behandeling van het beroep en de procedure, bedoeld in het eerste lid, kunnen de instanties die zijn belast met de behandeling van het geschil, advies van de Autoriteit persoonsgegevens inwinnen.

Bestuursorganen kunnen advies inwinnen bij de AP over hoe het conflict inzake persoonsgegevens moet worden opgelost.

Artikel 37. Vertegenwoordiging van betrokkenen

Een verwerking kan niet ten grondslag worden gelegd aan een vordering als bedoeld in artikel 3:305a BW of een beroep ingesteld in een bestuursrechtelijke procedure door een belanghebbende in de zin van artikel 1:2, derde lid, van de Algemene wet bestuursrecht, voor zover degene die door deze verwerking wordt getroffen, daartegen bezwaar heeft.

Onder artikel 80 AVG kunnen collectieve acties worden ingesteld tot handhaving van de AVG tegen een verwerkingsverantwoordelijke. Hierop is de algemene regeling van artikel 3:305a BW van toepassing. Een betrokkene die er bezwaar tegen heeft dat hij of zij 'meegenomen' wordt in zo'n actie, kan daartegen bezwaar maken. Zijn verwerking blijft dan buiten de collectieve actie.

Collectieve eis tot schadevergoeding. Zeer recent is de Wet afwikkeling massaschade in collectieve actie (TK 34.608) aangenomen. Deze maakt het mogelijk om in collectieve acties schadevergoeding in geld te vorderen. Er gelden wel hoge eisen aan de rechtspersoon die de actie voert, onder meer dat de bestuursleden geen direct winstoogmerk hebben bij de actie en dat de organisatie een duidelijke band met Nederland heeft.

Artikel 38. Opschortende werking bezwaar en beroep

De werking van de beschikking tot oplegging van de bestuurlijke boete wordt opgeschort totdat de bezwaar- of beroepstermijn is verstreken of, indien bezwaar is gemaakt of beroep is ingesteld, totdat op het bezwaar of het beroep is beslist.

Hoofddregel in het bestuursrecht is dat een opgelegde boete moet worden betaald, ook als ondertussen bezwaar of beroep is ingesteld. Met dit artikel wordt dat omgedraaid voor de AVG: een opgelegde boete hoeft niet te worden betaald zolang deze procedures nog lopen.

PARAGRAAF 3.4. DE FUNCTIONARIS VOOR GEGEVENSBESCHERMING**Artikel 39. Geheimhoudingsplicht**

De functionaris voor gegevensbescherming, bedoeld in de artikelen 37 tot en met 39 van de verordening, is verplicht tot geheimhouding van hetgeen hem op grond van een klacht of een verzoek van betrokkene is bekend geworden, tenzij de betrokkene in bekendmaking toestemt.

De FG is gebonden aan geheimhouding met betrekking tot de uitvoering van zijn taken (artikel 38 lid 5 AVG). Dit kan tot problematische situaties leiden wanneer een betrokkene een klacht indient of een verzoek doet en bekendmaking van relevante informatie aan derden noodzakelijk is. Dit artikel 39 schept de mogelijkheid dat de betrokkene dan instemt met de bekendmaking.

Hoofdstuk 4

Uitzonderingen en beperkingen

Hoofdstuk 4 van de Uitvoeringswet bevat uitzonderingen op de regels uit de AVG. Ieder van deze uitzonderingen moet tot een specifieke grondslag daarvoor in de AVG te herleiden zijn; EU-lidstaten mogen bij een Verordening immers niet zelfstandig afwijkende bepalingen introduceren.

De Nederlandse uitzonderingen op de AVG betreffen met name een regeling over geautomatiseerde besluitvorming (artikel 40), privacy versus nationale veiligheid (artikel 41), datalekken bij financiële organisaties (artikel 42), journalistiek (artikel 43), wetenschappelijk onderzoek (artikel 44), archieven (artikel 45), het bsn (artikel 46) en openbare registers (artikel 47).

Artikel 40. Uitzonderingen op verbod geautomatiseerde individuele besluitvorming

40.1 Artikel 22, eerste lid, van de verordening geldt niet indien de in die bepaling bedoelde geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang.

In beginsel verbiedt artikel 22 AVG geautomatiseerde individuele besluitvorming, waaronder profilering. Wie immers geraakt wordt door een automatisch besluit, staat vaak met lege handen en zonder zelfs maar duidelijkheid over het waarom dan. In Nederland is dergelijke besluitvorming echter desondanks mogelijk wanneer dit noodzakelijk is voor een wettelijke plicht of overheidstaak. Voorbeelden zijn geautomatiseerde verkeersboetes of het toekennen dan wel intrekken van toeslagen vanuit de Belastingdienst.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 22 lid 2 punt b AVG.

40.2 Bij de geautomatiseerde individuele besluitvorming, bedoeld in het eerste lid, treft de verwerkingsverantwoordelijke passende maatregelen die strekken tot bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene.

- 40.3 Indien de verwerkingsverantwoordelijke geen bestuursorgaan is, dan zijn passende maatregelen als bedoeld in het tweede lid, in ieder geval getroffen indien het recht op menselijke tussenkomst, het recht voor betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten, zijn geborgd.

Bij dergelijke vormen van besluitvorming is wel vereist dat de verwerkingsverantwoordelijke passende maatregelen neemt om de betrokkenen adequaat te beschermen.

Private organisaties. Voor private organisaties zijn passend het recht op menselijke tussenkomst, het recht om gehoord te worden en een mogelijkheid het besluit aan te vechten. Let op dat deze rechten hier dwingendrechtelijk toegekend worden en dus niet bijvoorbeeld in gebruiksvoorwaarden of aanvragen buiten werking kunnen worden verklaard.

Overheidsorganen. Voor overheidsorganen zijn op geautomatiseerde besluitvorming de regels uit de Algemene wet bestuursrecht van toepassing. Specifieke aandacht daarbij verdient de eis tot motivatie en uitleg van de totstandkoming van het geautomatiseerd besluit (zie Afdeling Bestuursrecht Raad van State 17 mei 2017, ECLI:NL:RVS:2017:1259).

Artikel 41. Uitzonderingen op rechten betrokkene en plichten verwerkingsverantwoordelijke

- 41.1 De verwerkingsverantwoordelijke kan de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34 van de verordening, buiten toepassing laten voor zover zulks noodzakelijk en evenredig is ter waarborging van:

41.1(a) de nationale veiligheid;

41.1(b) landsverdediging;

41.1(c) de openbare veiligheid;

41.1(d) de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;

41.1(e) andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

41.1(f) de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;

41.1(g) de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscode voor geregelende beroepen;

41.1(h) een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;

41.1(i) de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of

41.1(j) de inning van civielrechtelijke vorderingen.

Met dit artikel geeft de Nederlandse wetgever invulling aan sectorspecifieke behoeften (en specifieke overheidsbehoeften) inzake de vrije omgang met persoonsgegevens. De genoemde partijen en instanties kunnen (maar moeten niet) een afweging maken of zij bepaalde rechten van betrokkenen buiten toepassing willen laten. De verwerkingsverantwoordelijke die hierop een beroep wil doen, moet dit zorgvuldig afwegen en motiveren (lid 2).

Grondslag. De AVG staat deze nationale regeling toe onder artikel 23 AVG.

41.2 Bij de toepassing van het eerste lid houdt de verwerkingsverantwoordelijke rekening met in ieder geval, voor zover van toepassing:

41.2(a) de doeleinden van de verwerking of van de categorieën van verwerking;

41.2(b) de categorieën van persoonsgegevens;

41.2(c) het toepassingsgebied van de ingevoerde beperkingen;

41.2(d) de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;

41.2(e) de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;

41.2(f) de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;

41.2(g) de risico's voor de rechten en vrijheden van de betrokkenen; en

41.2(h) het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

De verwerkingsverantwoordelijke die zich wil beroepen op de vrijstelling, moet dit vooraf hebben uitgewerkt voor de specifieke voorgenomen verwerking(en). Het is dus niet mogelijk om eenvoudigweg te zeggen “onze doelstellingen zijn belangrijk dus we vallen buiten de AVG” (lid 1 punt e). In beginsel moeten betrokkenen worden geïnformeerd (punt h en artikel 13 AVG) maar hierop zijn uitzonderingen mogelijk als dat het doel van de vrijstelling zou aantasten.

Artikel 42. Uitzondering op meldplicht datalekken aan de betrokkene

Artikel 34 van de verordening is niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.

Op grond van dit artikel is een mededeling van datalekken aan betrokkenen (artikel 34 AVG) niet verplicht voor financiële ondernemingen. De Wet op het financieel toezicht (Wft) kent geen eigen formele mededelingsplicht. Onder de Wft vallende ondernemingen hebben in beginsel wel een mededelingsplicht aan betrokkenen op grond van hun zorgplicht als professioneel dienstverlener. De meldplicht aan de toezichthouder (artikel 33 AVG) geldt wél voor dergelijke financiële ondernemingen.

Artikel 43. Uitzonderingen inzake journalistieke doeleinden of academische, artistieke of literaire uitdrukkingen

43.1 Deze wet, met uitzondering van de artikelen 1 tot en met 4 en 5, eerste en tweede lid, is niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden en ten behoeve van uitsluitend academische, artistieke of literaire uitdrukkingen.

Om een evenwicht tot stand te brengen tussen de bescherming van persoonsgegevens enerzijds en de informatievrijheid anderzijds, draagt de AVG (artikel 85) de lidstaten op passende wettelijke maatregelen te treffen. Dit artikel geeft daar invulling aan door voor journalistiek, academisch onderzoek, kunst en literatuur de AVG en de Uitvoeringswet gedeeltelijk buiten toepassing te laten.

Beperkte toepasselijkheid Uitvoeringswet. Van de Uitvoeringswet zijn alleen artikelen 1 (definities), 2, 3 en 4 (materiële en territoriale toepasselijkheid) en leden 1 en 2 van artikel 5 (toestemming bij minderjarigen) van toepassing op deze categorieën verwerkingen.

Journalistieke doeleinden. Men verwerkt voor journalistieke doeleinden indien de verwerking als enig doel heeft de bekendmaking aan het publiek van informatie, meningen of ideeën, ongeacht het overdrachtsmedium. Deze activiteiten zijn niet voorbehouden aan mediaondernemingen en kunnen een winstoogmerk hebben (HvJ EU 16 december 2008, ECLI:EU:C:2008:727, Satamedia).

De Autoriteit Persoonsgegevens vermeldt op haar site dat bij internetpublicaties hiervan sprake is als aan vier kenmerken is voldaan:

1. Objectieve informatieverzameling. Er moet duidelijk onderscheid zijn tussen feiten, beweringen en meningen. Kan iedere websitebezoeker vrijuit reageren of is er controle op de reacties?
2. Regelmatige bezigheid. Een weblog met een paar verouderde bijdragen kan zich minder snel beroepen op de journalistieke uitzondering dan een website waarop regelmatig iets nieuws verschijnt.
3. Maatschappelijke strekking. De publicatie moet een maatschappelijk belang dienen. Bijvoorbeeld het bekendmaken van misdragingen van een volksvertegenwoordiger of directeur van een bekend of groot bedrijf. De publicatie moet hierbij wel voldoende onderbouwd zijn.
4. Recht van repliek. Dat houdt in dat betrokkenen het recht hebben te reageren op onjuiste, onvolledige of overbodige informatie. Ook hebben zij recht op rectificatie (verbetering) van deze informatie.

Met name het vierde kenmerk vindt geen steun in de Nederlandse praktijk of jurisprudentie rondom journalistieke activiteiten.

Academisch, artistiek of literair. De AVG, noch de jurisprudentie kent een definitie van deze begrippen.

43.2 De navolgende hoofdstukken en artikelen van de verordening zijn niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukingsvormen:

43.2(a) artikel 7, derde lid, en artikel 11, tweede lid;

43.2(b) hoofdstuk III;

43.2(c) hoofdstuk IV, met uitzondering van de artikelen 24, 25, 28, 29 en 32;

43.2(d) hoofdstuk V;

43.2(e) hoofdstuk VI; en

43.2(f) hoofdstuk VII.

Van de AVG zelf worden onder meer de hoofdstukken gericht op de toezicht-houders (hoofdstuk VI en VII) buiten toepassing verklaard. Ook gelden een aantal belangrijke inhoudelijke bepalingen niet:

Toestemming niet intrekbaar. Toestemming gegeven voor journalistieke, academische, artistieke of literaire verwerkingen is niet intrekbaar (artikel 7 lid 3 AVG). Hiermee is het dus niet mogelijk achteraf bijvoorbeeld een journalistieke publicatie weer te verwijderen. Voor fotografen is dit van belang bij de zogeheten quitclaim of model release, die dus gewoon voor de eeuwigheid gegeven kan worden.

Rechten van betrokkenen. Een betrokkene kan bij een journalistieke, academische, artistieke of literaire verwerking geen rechten uitoefenen, aangezien heel hoofdstuk III (Rechten van betrokkenen) buiten toepassing is.

Verplichtingen verwerkingsverantwoordelijke. Een journalistiek, academisch, artistiek of literair opererende verantwoordelijke moet wel passende maatregelen treffen ten behoeve van ‘zijn’ betrokkenen (artikel 24 AVG), rekening houden met privacy by design and by default (artikel 25 AVG), uitsluitend zorgvuldig opererende verwerkers inschakelen (artikel 28 AVG), toezicht houden op hulppersonen (artikel 29 AVG) en passende beveiliging tegen datalekken en misbruik hanteren (artikel 32 AVG).

Doorgifte. Bij een journalistieke, academische, artistieke of literaire verwerking geldt het verbod op doorgifte (hoofdstuk V) niet, en dus ook niet de verplichting om bijvoorbeeld een standaardcontract met een buitenlandse verwerker te sluiten of andere passende waarborgen te treffen.

Boetes en sancties. Hoofdstuk VIII met diverse sancties blijft van kracht, zij het dat de bepalingen gericht op de toezichthouder niet ingeroepen kunnen worden omdat de toezichthouder niet bevoegd is (lid 1 van dit artikel). Een betrokkene kan wel zelf naar de rechter stappen met een eis tot staking van verwerking (artikel 79 AVG) dan wel een schadevergoeding (artikel 82 AVG). Deze actie kan ook collectief worden ingesteld (artikel 80 AVG).

Grondslag. De AVG staat deze nationale regeling toe onder artikel 85 AVG.

- 43.3 De artikelen 9 en 10 van de verordening zijn niet van toepassing voor zover de verwerking van de in die artikelen bedoelde gegevens noodzakelijk is voor het journalistieke doel of de academische, artistieke of literaire uitdrukingsvorm.

Wanneer de verwerking van bijzondere of strafrechtelijke persoonsgegevens (artikelen 9 en 10 AVG) noodzakelijk is voor journalistieke, academische, artistieke of literaire verwerkingen geldt daarop het gewone verwerkingsverbod niet. Een strafrechtjournalist mag dus bijvoorbeeld publiceren over misdrijven waar levende personen bij betrokken zijn.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 85 AVG.

Artikel 44. Uitzonderingen inzake wetenschappelijk onderzoek en statistiek

Indien een verwerking wordt verricht door instellingen of diensten voor wetenschappelijk onderzoek of statistiek, en de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische of wetenschappelijke doeleinden kunnen worden gebruikt, kan de verwerkingsverantwoordelijke de artikelen 15, 16 en 18 van de verordening buiten toepassing laten.

Bij wetenschappelijk of statistisch onderzoek ontstaat een spanningsveld ten aanzien van de integriteit van de brongegevens versus de privacy van betrokkenen. Dit wordt met dit artikel opgelost voor wetenschappelijke instellingen of statistische onderzoeksbureaus. Zij mogen de rechten van inzage (artikel 15 AVG), correctie (artikel 16 AVG) en beperking (artikel 18 AVG) buiten toepassing laten wanneer zij voorzieningen hebben getroffen om te zorgen dat de gegevens ook werkelijk alleen voor hun onderzoeksdoeleinden worden gebruikt.

Optioneel. Het artikel zegt dat de verwerkingsverantwoordelijke deze rechten buiten toepassing *kan* laten. Het moet dus niet. De verwerkingsverantwoordelijke zal daarom expliciet moeten communiceren dat een betrokkene deze rechten niet heeft. De AVG verplicht standaard verwerkingsverantwoordelijken immers om expliciet mensen te wijzen op hun rechten (artikel 13 lid 2 punt b AVG).

Recht van bezwaar. De AVG staat toe dat een nationale regeling ook artikel 21 (recht van bezwaar) buiten toepassing stelt, maar Nederland heeft hier niet voor gekozen. Dit recht bestaat dus onverkort, zij het dat de betrokkene natuurlijk wel met zijn specifieke situatie verband houdende redenen moet stellen (artikel 21 AVG) en de verwerkingsverantwoordelijke dan een afweging moet maken.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 89 lid 2 AVG.

Artikel 45. Uitzonderingen inzake archivering in het algemeen belang

45.1 Bij de verwerking van persoonsgegevens die deel uitmaken van archiefbescheiden als bedoeld in artikel 1, onderdeel c, van de Archiefwet 1995, die berusten in een archiefbewaarplaats als bedoeld in artikel 1, onderdeel f, van die wet, zijn de artikelen 15, 16, 18, eerste lid, onderdeel a, en 20 van de verordening niet van toepassing.

Dit artikel stelt het algemene kader voor omgang met persoonsgegevens in archieven die onder de Archiefwet vallen. De betrokkene heeft in die gevallen geen recht van inzage (artikel 15 AVG), correctie (artikel 16 AVG), beperking (artikel 18 AVG) en data-export (artikel 20 AVG).

Recht van verwijdering. Ook verwijdering (artikel 17 AVG) is in principe niet mogelijk in deze gevallen, zie artikel 17 lid 3 punt d AVG.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 89 lid 3 AVG.

45.1 Betrokkene heeft het recht om inzage te verkrijgen in de archiefbescheiden, tenzij verzoeken om inzage zodanig ongericht zijn dat deze in redelijkheid niet kunnen worden ingewilligd.

Om de betrokkene toch enigszins tegemoet te komen, wordt een afgezwakt recht van inzage geïntroduceerd: inzage mag tenzij dit redelijkerwijs niet haalbaar is. Archiven kunnen om allerlei redenen immers moeilijk toegankelijk zijn.

Geen kopie. De betrokkene heeft onder dit zwakke recht geen recht op een kopie, in tegenstelling tot artikel 15 AVG.

45.1 Betrokkene heeft het recht om, in geval van onjuiste persoonsgegevens, zijn eigen lezing aan de desbetreffende archiefbescheiden toe te voegen.

Het recht van correctie uitoefenen jegens een archiefstuk zou ertoe kunnen leiden dat de geschiedenis wordt herschreven. Tegelijkertijd is het laten bestaan van onjuiste stukken in officiële archiven onwenselijk omdat daardoor mensen in problemen kunnen komen, denk aan fouten in geboortekten. Daarom introduceert dit lid een zwak correctierecht: men mag een “eigen lezing” toevoegen aan de stukken. Hiermee kan de ontvanger van het stuk zelf een afweging maken hoe het stuk te waarderen.

Artikel 46. Verwerking nationaal identificatienummer

- 46.1 Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald.

Dit artikel stelt het algemene kader voor de omgang met het burgerservicenummer (BSN). In de kern komt dit kader erop neer dat een wet moet bepalen waar het BSN voor nodig is, en dat ander gebruik (ook indien doelbinding van toepassing zou zijn) niet toegestaan is als het ander doel niet ook in een wet staat.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 87 AVG.

Bij wet bepaald. De formulering “bij wet bepaald” wijst erop dat het moet gaan om een wet in formele zin. De formele wetgever mag geen gedelegeerde bevoegdheid hieromtrent creëren, en een lagere wetgever (zoals een gemeente) mag geen regelingen invoeren over gebruik van het BSN.

- 46.2 Bij algemene maatregel van bestuur kunnen andere dan in het eerste lid bedoelde gevallen worden aangewezen waarin een daarbij aan te wijzen nummer als bedoeld in het eerste lid, kan worden gebruikt. Daarbij kunnen nadere regels worden gegeven over het gebruik van een zodanig nummer.

Uitzondering op het bovenstaande is in bijzondere gevallen mogelijk. De formele wetgever moet dit in een algemene maatregel van bestuur uitwerken.

Artikel 47. Uitzonderingen op rechten betrokkene bij openbare registers

- 47.1 De artikelen 15, 16, 18 en 19 van de verordening zijn niet van toepassing op bij de wet ingestelde openbare registers, indien bij of krachtens die wet een bijzondere procedure voor de verbetering, aanvulling, verwijdering of afscherming van gegevens is geregeld.

Bij openbare registers die bij wet zijn ingesteld, heeft de betrokkene geen rechten van inzage (artikel 15 AVG), correctie (artikel 16 AVG), beperking (artikel 18 AVG) of data-export (artikel 20 AVG). Vereist is dan wel dat het register een eigen procedure voor correctie, verwijdering of beperking heeft.

Recht van verwijdering. Het recht van verwijdering (artikel 17 AVG) is naar zijn aard niet van toepassing op een vermelding in een openbaar register, aangenomen dat de persoonsgegevens natuurlijk terecht in dat register zijn opgenomen.

Grondslag. De AVG staat deze nationale regeling toe onder artikel 23 AVG.

47.2 Artikel 21 van de verordening is niet van toepassing op bij de wet ingestelde openbare registers.

Ook het recht van bezwaar wordt buiten werking gesteld bij openbare registers die wettelijk zijn ingesteld.

Hoofdstuk 5

Overgangs- en slotbepalingen

Hoofdstuk 5 van de Uitvoeringswet bevat afsluitende regelingen, met name gericht op overgangsrecht (artikelen 48 en 48a), samenloop met andere wetgeving (artikel 49) en inwerkingtreding van de wet (artikelen 50-54).

Artikel 48. Overgangsrecht

48.1 Degene die voorafgaand aan de inwerkingtreding van deze wet is benoemd als lid van het College bescherming persoonsgegevens, is van rechtswege benoemd als lid van de Autoriteit persoonsgegevens.

Bij inwerkingtreding van de AVG verviel de Wbp, en daarmee ook (op papier) de AP, voorheen het College bescherming persoonsgegevens. De AP wordt bij de Uitvoeringswet opnieuw ingesteld (artikel 6) en vanwege de continuïteit worden haar leden van rechtswege per direct opnieuw lid van de AP.

48.2 Degene die voorafgaand aan de inwerkingtreding van deze wet is benoemd als voorzitter van het College bescherming persoonsgegevens, is van rechtswege is benoemd als voorzitter van de Autoriteit persoonsgegevens.

Hetzelfde als voor de leden (lid 1) geldt voor de voorzitter.

48.3 Voor het bepalen van het tijdvak van de benoeming, bedoeld in artikel 7, vijfde lid, geldt het tijdvak, vervuld als voorzitter van het College bescherming persoonsgegevens, voorafgaand aan de inwerkingtreding van deze wet als een tijdvak, vervuld als voorzitter van de Autoriteit persoonsgegevens.

Vanwege de continuïteit van de taakvervulling wordt het tijdvak van de benoeming van de leden van de AP berekend vanaf de datum waarop zij feitelijk zijn begonnen met het werk, immers onder de Wbp.

- 48.4 Op de leden van het College bescherming persoonsgegevens die zijn benoemd of herbenoemd voor 1 januari 2014, blijft artikel 53, derde lid, eerste, tweede en derde volzin, van de Wet bescherming persoonsgegevens van toepassing, zoals dat luidde voor dat tijdstip.

De reeds benoemde leden kunnen meerdere malen herbenoemd worden, dit was zo geregeld onder artikel 53 lid 3 Wbp en dit verworven recht moet worden gerespecteerd.

- 48.5 De ambtenaar die voorafgaand aan de inwerkingtreding van deze wet is benoemd in het secretariaat van het College bescherming persoonsgegevens, is van rechtswege benoemd als ambtenaar in het secretariaat van de Autoriteit persoonsgegevens.

De ambtenaren werkzaam bij het secretariaat van de 'oude' AP/Cbp zijn van rechtswege nu werkzaam bij de 'nieuwe' AP.

- 48.6 Besluiten die voorafgaand aan de inwerkingtreding van deze wet zijn genomen door het College bescherming persoonsgegevens gelden van rechtswege als besluiten, genomen door de Autoriteit persoonsgegevens.

Besluiten die de 'oude' AP heeft genomen, worden behandeld als besluiten van de 'nieuwe' AP. Inhoudelijk is op dergelijke besluiten het recht ten tijde van de Wbp van toepassing (zie lid 8).

- 48.7 In wettelijke procedures en rechtsgedingen waarbij het College bescherming persoonsgegevens voorafgaand aan de inwerkingtreding van deze wet is betrokken, treedt de Autoriteit persoonsgegevens van rechtswege in de plaats van het College bescherming persoonsgegevens.

Bij procedures en bestuursrechtelijk optreden dat geïnitieerd is ten tijde van de Wbp maar nu nog niet is afgerond, wordt de 'nieuwe' AP als het bestuursorgaan gezien. Hiermee is bijvoorbeeld beroep tegen een besluit van de 'oude' AP mogelijk – de oude AP bestaat immers niet meer.

- 48.8 Op wettelijke procedures en rechtsgedingen waarbij het College bescherming persoonsgegevens voorafgaand aan de inwerkingtreding van deze wet is betrokken, is het recht van toepassing zoals dit gold voorafgaand aan de inwerkingtreding van deze wet.

Bij besluiten, procedures en optredens zoals bedoeld in leden 6 en 7, geldt het recht van de Wbp. De regels van de AVG zijn dus niet van toepassing op de afhandeling daarvan, ook niet bijvoorbeeld bij een beroep op bezwaar of een procedure bij de rechtbank daarover.

- 48.9 In samenwerkingsprotocollen treedt op het tijdstip van inwerkingtreding van deze wet de Autoriteit persoonsgegevens van rechtswege in de plaats van het College bescherming persoonsgegevens.

De ‘nieuwe’ AP neemt bestaande samenwerkingen met andere bestuursorganen (zoals de Autoriteit Consument & Markt) van rechtswege over.

- 48.10 Op schriftelijke verzoeken als bedoeld in artikel 46 van de Wet bescherming persoonsgegevens, rechtsgedingen op basis van artikel 49 van de Wet bescherming persoonsgegevens en vorderingen op basis van artikel 50 van de Wet bescherming persoonsgegevens, die op het moment van inwerkingtreding van deze wet reeds aanhangig zijn bij de rechtbank is het recht van toepassing zoals dit gold voorafgaand aan de inwerkingtreding van deze wet.

Bij procedures die reeds bij de rechtbank lopen, is de ‘nieuwe’ AP van rechtswege het bestuursorgaan dat tegenover de betrokkene staat. Het gaat dan om procedures over inzageverzoeken bij een verantwoordelijke (artikel 46 jo. 30 Wbp), een schadeclaim (artikel 49 Wbp) of een verwerkingsverbod (artikel 50 Wbp).

- 48.11 Een verklaring van rechtmatigheid van de gegevensverwerking die voorafgaand aan de inwerkingtreding van deze wet is afgegeven op grond van artikel 32, vijfde lid, in samenhang met artikel 22, vierde lid, onder c, van de Wet bescherming persoonsgegevens, geldt van rechtswege als een vergunning in de zin van artikel 33, vierde lid, onder c, van deze wet.

Onder artikel 32 Wbp moesten voor bepaalde gevoelige verwerkingen van persoonsgegevens (zoals heimelijke observatie of structurele verwerking van strafrechtelijke gegevens) voorafgaande verklaringen van rechtmatigheid gevraagd worden bij het Cbp. De AVG kent deze specifieke constructie niet (maar vergelijk artikel 36 AVG, de voorafgaande raadpleging) en daarom bevat dit lid een overgangsregeling waarbij de vergunningsprocedure uit artikel 33 lid 4 van toepassing wordt verklaard.

- 48.12 Voor zover deze wet daarin niet voorziet, kunnen bij algemene maatregel van bestuur regels of nadere regels worden gesteld omtrent de invoering van de verordening of deze wet.

Mogelijk duiken later situaties op waarin de overgang van of verhouding tussen Wbp en AVG niet goed geregeld is. De minister kan dan met gedelegeerde reparatiewetgeving dit probleem oplossen, al moet hij daar terughoudend gebruik van maken.

Artikel 48a. Overgangsrecht II

48a.1 [Wijzigd deze wet.]

Dit lid wijzigde artikel 6 op niet-inhoudelijke wijze.

48a.2 [Wijzigd deze wet.]

Dit lid wijzigde artikel 11 op niet-inhoudelijke wijze.

48a.3 Op het tijdstip van inwerkingtreding van dit artikel zijn de ambtenaren van het secretariaat, bedoeld in artikel 10, eerste lid, van wie naam en functie zijn vermeld op een door Onze Minister in overleg met de Autoriteit persoonsgegevens vastgestelde lijst, van rechtswege ontslagen en aangesteld als ambtenaar in dienst van de Autoriteit persoonsgegevens. De overgang van de in de vorige volzin bedoelde ambtenaren vindt plaats met een rechtspositie die als geheel ten minste gelijkwaardig is aan die welke voor elk van hen gold op de dag voor de datum van inwerkingtreding van dit artikel.

De ambtenaren werkzaam bij de 'oude' AP zijn van rechtswege nu werkzaam bij de 'nieuwe' AP.

48a.4 Onze Minister bepaalt in overeenstemming met Onze Minister van Financiën welke vermogensbestanddelen van de Staat worden toebedeeld aan de Autoriteit persoonsgegevens.

48a.5 De in het vierde lid bedoelde vermogensbestanddelen gaan op het tijdstip van inwerkingtreding van dit artikel onder algemene titel over op tegen een door Onze Minister in overeenstemming met Onze Minister van Financiën te bepalen waarde.

48a.6 Ingeval krachtens het vierde en het vijfde lid registergoederen overgaan, doet Onze Minister van Financiën de overgang van die registergoederen onverwijld inschrijven in de openbare registers, bedoeld in afdeling 2 van titel 1 van Boek 3 van het Burgerlijk Wetboek. Artikel 24, eerste lid, van Boek 3 van het Burgerlijk Wetboek is niet van toepassing.

Deze formele bepaling regelt dat het vermogen van de 'oude' AP kan worden overgedragen aan de 'nieuwe' AP.

48a.7 In wettelijke procedures en rechtsgedingen, waarbij de Autoriteit persoonsgegevens is betrokken, treedt op het tijdstip van inwerkingtreding van dit artikel de Autoriteit persoonsgegevens in de plaats van de Staat dan wel Onze Minister.

Bij lopende procedures waar de ‘oude’ AP was betrokken, neemt de ‘nieuwe’ AP deze over.

48a.8 In zaken waarin voor het tijdstip van inwerkingtreding van dit artikel aan de Nationale ombudsman is verzocht een onderzoek te doen dan wel de Nationale ombudsman een onderzoek heeft ingesteld naar een gedraging die kan worden toegerekend aan de Autoriteit persoonsgegevens, treedt de Autoriteit persoonsgegevens op dat tijdstip als bestuursorgaan in de zin van de Wet Nationale ombudsman in de plaats van Onze Minister.

Bij lopende onderzoeken van de Nationale Ombudsman waar de ‘oude’ AP was betrokken, neemt de ‘nieuwe’ AP deze over.

Artikel 49. Samenloop

[Wijzigd deze wet.]

Dit artikel wijzigde artikel 3 op ondergeschikte punten.

Artikel 50. Evaluatie

Onze Minister zendt binnen drie jaar na de inwerkingtreding van deze wet, en vervolgens telkens na vier jaar, aan de Staten-Generaal een verslag over de effecten van deze wet in de praktijk en over de uitvoering van de wet in de praktijk.

De Uitvoeringswet is met enige haast opgesteld en ingevoerd, omdat men deze op dezelfde datum wilde invoeren als wanneer de AVG van kracht zou worden (25 mei 2018). Derhalve was behoefte aan regelmatige evaluatie van de Uitvoeringswet. De eerste evaluatie is drie jaar na inwerkingtreding, zodat deze een jaar na de eerste evaluatie van de AVG (vier jaar na inwerkingtreding, dus 2020) plaatsvindt. De vierjaarlijkse evaluatie daarna zorgt er voor dat steeds de eveneens vierjaarlijkse evaluatie van de AVG een jaar eerder is geweest (artikel 97 AVG). Op 2 december 2022 is het voorstel tot wijziging van de Uitvoeringswet ingediend, dit ligt ten tijde van het schrijven van dit boek nog bij de Tweede Kamer (TK 36264).

Artikel 51. Intrekking Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens wordt ingetrokken.

Dit artikel is de logische consequentie van artikel 94 lid 1 AVG, dat Richtlijn 95/46/EG intrekt. Daarmee ontvalt de rechtsbasis voor de Wbp. Verwijzingen naar de Wbp in andere wetten en regelingen moeten worden gelezen als verwijzingen naar de AVG (artikel 94 lid 2 AVG).

Artikel 52. Citeertitel verordening

Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) wordt in overige wetgeving aangehaald als: Algemene verordening gegevensbescherming.

De citeertitel van de AVG in andere wetgeving is formeel in Nederland de Algemene verordening gegevensbescherming, maar mag worden afgekort als AVG.

Artikel 53. Inwerkingtreding

De artikelen van deze wet treden in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

De Uitvoeringswet is in werking getreden op 25 mei 2018, tegelijk met de AVG zelf (Staatsblad 144 van 16 mei 2018). Omdat de invoering van de Uitvoeringswet nogal haastwerk was omdat men de AVG-datum wilde halen, werd een gefaseerde inwerkingtreding achter de hand gehouden. Hiervan is uiteindelijk geen gebruik gemaakt.

Artikel 54. Citeertitel wet

Deze wet wordt aangehaald als: Uitvoeringswet Algemene verordening gegevensbescherming.

De citeertitel van de Uitvoeringswet is formeel de Uitvoeringswet Algemene verordening gegevensbescherming maar de afkortingen Uitvoeringswet en UAVG zijn algemeen gangbaar. Dit boek spreekt van 'Uitvoeringswet'.

Index

De nummers verwijzen naar de artikelen uit de AVG.

*Het **vetgedrukte** artikelnummer betreft het hoofdartikel over dat onderwerp.*

- Aansprakelijkheid verwerker 82, **82(2)**, 82(3)
Aansprakelijkheid verwerkingsverantwoordelijke 82, **82(2)**, 82(3)
Administratieve boetes **83**
Adequaat derde land 13(1)(e), 14(1)(f), **45(1)**
Advies van Comité 28(8), 35(4), 40(7), 41(3), 43(3), 46(2)(d), 46(3), 47, 57(1), **64(1)**
Anonimisering van gegevens **4(1)**, 89
Arbeidsrecht **9(2)(c)**, 9(2)(h), 88
Archivering in algemeen belang 6(1)(f), 9(2)(j), **89**
Artikel 29-Werkgroep zie Europees Comité voor gegevensbescherming
Artikel 93-comité 28(7), 40(9), 43(9), 45(3), 45(5), 46(2), 47(3), 61(9), 67, **93**
Audit op verwerking **28(3)(h)**, 39(1)(b)
Autoriteit Persoonsgegevens **51**
- Beginnelsen 5
Beperken van verwerking 4(3), **18**
Beroepsgeheim 9(2)(i), 38(5), **90**
Bestand **4(6)**
Betrokken toezichthouder **4(22)**, 56(1), 60
Beveiliging van verwerking 32
Bevoegdheidsdelegatie **92**
Bewaartermijnen **5(1)(e)**
Bewerker zie Verwerker
Bewerkersovereenkomst zie Verwerkersovereenkomst
Bijzondere persoonsgegevens **9(1)**
Bindende bedrijfsvoorschriften **4(20)**, 46(1), 47, 57(1)(s)
Binding corporate rules zie Bindende bedrijfsvoorschriften
Biometrische persoonsgegevens **4(14)**, 9(4)
Boetes, hoge categorie 5, 6, 7, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 44, 45, 46, 47, 48, 49, 58(1), 58(2), **83(5)**, 83(6)
Boetes, lage categorie 8, 10, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 41(4), 42, 43, **83(4)**
Burgerservicenummer 9(1), **87**
- Certificeringsmechanisme 24(3), **42**
Certificeringsmechanismen 24(3), 28(5), 25(3), 32(3), **42**, 43, 83(2)(j), 83(4)(b)
Coherentiemechanisme 28(8), 35(6), 41(3), 46(4), 47(1), 60(4), **63**, 66(1)
Collectieve actie **80**
Comité zie Europees Comité voor gegevensbescherming

Competentie toezichthouder 55, 56, 60

Computer says no zie Geautomatiseerde besluitvorming

Concern 4(19)

Data protection officer zie Functionaris voor gegevensbescherming

Data security policy zie Gegevensbeschermingsbeleid

Data-export 15(3), 20

Datalek zie Inbreuk in verband met persoonsgegevens

Dataminimalisatie 5(1)(c)

Dataportabiliteit 20

Derde 4(10)

Derde land 44(1), 45, 46, 47, 48, 49, 50

Dienst van de informatiemaatschappij 4(25), 8(1)

Direct marketing 6(1)(f), 21(2), 21(3)

Doel AVG 1

Doelbinding 5(1)(b)

Doorgifte van persoonsgegevens 44, 45, 46, 47, 48, 49, 50

Doorgifte, adequaatheidsbesluiten 45(1)

Doorgifte, bindende bedrijfsvoorschriften 46(2)(b)

Doorgifte, certificeringsmechanisme 46(2)(f)

Doorgifte, gedragscode 46(2)(e)

Doorgifte, gerechtelijke uitspraak derde land 48

Doorgifte, model clauses zie Doorgifte, standaardbepalingen

Doorgifte, noodzakelijk overeenkomst 49(1)(b), 49(1)(c)

Doorgifte, openbaar register 49(1)(g)

Doorgifte, passende waarborgen 46(1)

Doorgifte, specifieke situaties 49

Doorgifte, standaardbepalingen 46(2)(c), 46(2)(d)

Doorgifte, uitdrukkelijke toestemming 49(1)(a)

Dringend eigen belang 6(1)(f)

Eénloketprocedure 56(1), 60

European Data Protection Supervisor zie Europese Toezichthouder voor gegevensbescherming

Europees Comité voor gegevensbescherming 64(1), 65, 68, 69, 70, 71, 72, 73, 74, 75, 76

Europees Comité voor gegevensbescherming, advies 28(8), 35(4), 40(7), 41(3), 43(3), 46(2)(d), 46(3), 47, 57(1), 64(1)

Europees Comité voor gegevensbescherming, geschillenbeslechting 56(1), 60(4), 65, 66

Europees Comité voor gegevensbescherming, taken 68, 70

Europees Comité voor gegevensbescherming, werkwijze 70, 71, 72, 75

Europese Toezichthouder voor gegevensbescherming 68(3), 68(5), 75(1)

- Foto als persoonsgegevens 9(1)
 Fraudepreventie 6(1)(f)
 Functionaris voor gegevensbescherming 37, 38, 39
- Geautomatiseerde besluitvorming 22
 Gedelegeerde bevoegdheden 92
 Gedragscode 24(3), 40, 41
 Gegevensbescherming door ontwerp 15, 24, 25
 Gegevensbescherming door standaardinstellingen 24, 25
 Gegevensbeschermingsbeleid 24(2)
 Gegevensbeschermingseffectbeoordeling (DPIA) 35
 Gegevensminimalisatie 5(1)(c)
 Geheimhouding 9(2)(i), 38(5), 90
 Genetische persoonsgegevens 4(13), 9(4)
 Gerechtvaardigde belangen 6(1)(f)
 Geschillenbeslechting door Comité 56(1), 60(4), 65, 66
 Gezondheidspersoonsgegevens 4(15), 9(4)
 Grensoverschrijdende verwerking 4(23)
- Historisch onderzoek 21(6), 89
 Hoofdvestiging 4(16), 56(1), 60
- Identificator 4(1)
 Inbreuk in verband met persoonsgegevens 4(12), 33, 34
 Inbreuk, AVG 79
 Inbreuk, beveiliging 4(12), 32, 33, 34, 40(2)(i), 70(1)(g)
 Informatieplichten 12, 13, 14, 19, 21(4)
 Internationale organisatie 4(26), 44, 45, 46, 47, 48, 49, 50
 Inwerkingtreding AVG 99
 Inzagerecht 15, 20
- Journalistieke verwerking 6(1)(f), 85(1)
 Juisheidsbeginsel 5(1)(d)
- Kennelijk openbaar gemaakt 9(2)(e)
 Kennisgevingsplicht 19
 Klacht bij toezichthouder 77(1), 78
 Klachtrecht 79
- Leidende toezichthouder 56(1), 60
 Litispendentie 81
- Medische persoonsgegevens 4(15), 9(4)
 Meldplicht datalekken zie Inbreuk in verband met persoonsgegevens
 Minimale gegevensverwerking 5(1)(c), 25(2)
 Monitoren gedrag 3(2)

Nationaal identificatienummer 9(1), 87

Netwerkbeveiliging 6(1)(f), 32

Onafhankelijkheid toezichthouder 52, 53(4)

Onderneming 4(18)

Onderzoeksprocedure 28(7), 40(9), 43(9), 45(3), 46(2), 47(3), 61(9), 67, 93(2)

Ontvanger 4(9)

Openbaar gezag 6(1)(e)

Openbaarheid van bestuur zie Toegang tot officiële documenten

Opslagbeperking 5(1)(e)

Opsporing strafbare feiten 2(d), 23(1)(d)

Opt-in bij e-mail 7(1)

Opzettelijk of nalatig handelen 83(3)

Overgangsrecht 94

Passende beveiliging 31(1), 32(2)

Passende maatregelen 24(1)

Patiëntnummers 4(15)

Persoonlijke en huishoudelijke activiteiten 2(c)

Persoonsgegevens 4(1)

Persoonsgegevens bij rechtsvorderingen 9(2)(f), 18(2), 23(2)(j), 49(1)(e)

Persoonsgegevens, bijzonder 9(1)

Persoonsgegevens, biometrisch 4(14), 9(4)

Persoonsgegevens, genetisch 4(13), 9(4)

Persoonsgegevens, gezondheid 4(15), 9(4)

Persoonsgegevens, religieus 9(1), 91

Persoonsgegevens, strafrechtelijk 10

Precontractuele maatregelen 6(1)(c)

Privacy by default zie Gegevensbescherming door standaardinstellingen

Privacy by design zie Gegevensbescherming door ontwerp

Privacy impact assessment zie Gegevensbeschermingseffectbeoordeling

Privacy Shield 44, 45(1), 96

Privacyverklaring 12, 13

Profilering 4(4), 21, 22(1)

Pseudonimisering 4(5), 25(1), 32(1)(a)

Recht op beperking 4(3), 18

Recht op gegevensoverdracht zie Dataportabiliteit

Recht op gegevenswissing 17

Recht op vergetelheid zie Recht op gegevenswissing

Recht van bezwaar 21

Recht van data-toegang 15(3), 20

Recht van inzage 15, 20

Recht van rectificatie 16

Rechtmatigheid 5(1)(a), 6(1)

Rechtmatigheid, behoorlijkheid en transparantie 5(1)(a)

- Rechtsvordering bij inbreuk 79
- Rectificatie van persoonsgegevens 16
- Register van verwerkingsactiviteiten 30
- Relevant en gemotiveerd bezwaar 4(24), 60(4)
- Richtlijn 2002/58/EG 25(5), 95
- Richtlijn 95/46/EG 94

- Safe Harbor zie Privacy Shield
- Sancties 58, 83
- Samenwerkende toezichthouders 56(3), 56(4), 60, 61, 62, 63, 67
- Schadevergoeding 79, 82
- Statistische doeleinden 21(6), 89
- Strafrechtelijke persoonsgegevens 10
- Sub-bewerker zie Sub-verwerker
- Sub-verwerker 28(2)

- Taak van algemeen belang 6(1)(e), 9(2)(g), 23(1)(e), 49(1)(d)
- Toegang tot officiële documenten 86
- Toepasselijkheid, materieel 2
- Toepasselijkheid, territoriaal 3
- Toestemming 4(11), 6(1)(a), 7
- Toestemming, afgedwongen bij dienst 7(4)
- Toestemming, intrekken 7(3)
- Toestemming, kinderen bij internetdienst 8
- Toestemming, uitdrukkelijk 4(11), 9(2)(a)
- Toezichthouder 4(21), 51, 52,
- Toezichthouder, betrokken 4(22), 56(1), 60
- Toezichthouder, bevoegdheden 58, 83
- Toezichthouder, boetebevoegdheid 58(2)(i), 83
- Toezichthouder, competentie 55, 56, 60
- Toezichthouder, gezamenlijke werkzaamheden 60, 62
- Toezichthouder, klachten 77(1), 78
- Toezichthouder, leidend 56(1), 60
- Toezichthouder, onafhankelijkheid 52, 53(4)
- Toezichthouder, samenwerking 56(3), 56(4), 60, 61, 62, 63, 67
- Toezichthouder, wederzijdse bijstand 60(2), 61
- Toezichthouder, werkwijze 52, 53, 54, 57, 58, 59

- Uitdrukkelijke toestemming 4(11), 9(2)(a),
- Uitingsvrijheid 6(1)(f), 85(1)
- Uitvoering overeenkomst 6(1)(b)
- Urgentieprocedure 45(5), 93(3)

- Verantwoordelijke zie Verwerkingsverantwoordelijke
- Verantwoordingsplicht 5(2)
- Verenigbaarheid 5(1)(b), 6(4)

- Vergeetrecht zie Recht op gegevenswissing
- Verhaalsrecht bij verwerker 82(5)
- Versleuteling 32(1)(a), 34(3)(a)
- Vertegenwoordiger 4(17), 27
- Verwerker 4(8), 28
- Verwerker, aansprakelijkheid 82, 82(2), 82(3)
- Verwerker, verhaalsrecht 82(5)
- Verwerkersovereenkomst 28(3), 28(6), 28(9)
- Verwerking 4(2), 5, 6
- Verwerking, grensoverschrijdend 4(23)
- Verwerking, historisch onderzoek 21(6), 89
- Verwerking, statistische doeleinden 21(6), 89
- Verwerking, wetenschappelijk onderzoek 21(6), 89
- Verwerkingsverantwoordelijke 4(7)
- Verwerkingsverantwoordelijke, aansprakelijkheid 82, 82(2), 82(3)
- Verwerkingsverantwoordelijke, gezamenlijk 26
- Vestiging 3(1)
- Vestiging 4(16)
- Vitale belangen 6(1)(d), 9(2)(c), 49(1)(f)
- Volksgezondheid 9(2)(i)
- Voorafgaand onderzoek verwerking 36
- Vormvereisten verwerkersovereenkomst 28(9)

- Wetenschappelijk onderzoek 21(6), 89
- Wettelijke verplichting 6(1)(c)
- Wezenlijke gevolgen 56(1)

Bijlage 1

Referentietabel artikelen AVG

Artikel AVG	Overwegingen	Artikel Richtlijn	Artikel Wbp
01	1 t/m 14	01	-
02	14 t/m 21	03	02
03	22 t/m 25	04	04
04	26 t/m 38	02	01
05	39	06	06,07,09-11, 15
06.01	40,41, 44 t/m 50	07	08
06.04-04	40,41, 44 t/m 50	05	-
07	42 t/m 43	-	-
08	38	-	-
09	51 t/m 56	08	03, 16-21,23
10	19	08.05	22
11	57	-	-
12	58 t/m 59	-	-
13	60 t/m 62	10	33
14	-	11	34
15	63 t/m 64	12	35
16	-	12.b	36

Artikel AVG	Overwegingen	Artikel Richtlijn	Artikel Wbp
17	65 t/m 66	12.b	36
18	67	-	-
19	-	12.c	38
20	68	-	-
21	69 t/m 70	14	40, 41
22	71	15	42
23	72 t/m 73	13	43, 44
24	74 t/m 77	-	-
25	78	-	-
26	79	-	-
27	80	04.2	04.03
28	81	17	13, 14
28.03.b	-	16	12
29	-	-	-
30	82	-	-
31	-	-	660305
32	83	17	13, 14
33	85, 87 t/m 89	-	-
34	86 t/m 88	-	34a
35	84, 90 t/m 93	-	-
36	95 t/m 96	-	-
36.04	-	28.02	51.02

Artikel AVG	Overwegingen	Artikel Richtlijn	Artikel Wbp
36.05	-	20	31, 32
37	97	-	-
38	-	-	-
39	-	18.02	64
40	98 t/m 99	27	25
41	-	-	-
42	100	-	-
43	-	-	-
44	101 t/m 102	25	76, 78
45	103 t/m 107, 114	25.06	76, 78
46	108 t/m 109	26.02	-
47	110	26.02	-
48	-	-	-
49	111 t/m 115	26.01	77
50	116	-	-
51	117, 123	28.01	51
52	118, 120	28.01	52.02
53	121	-	-
54	-	-	-
55	122, 124	28.06	-
56	125 t/m 128	-	-
57	129	-	-

Artikel AVG	Overwegingen	Artikel Richtlijn	Artikel Wbp
58	-	28.03	61, 65
59	-	28.05	58
60	130 t/m 131	-	-
61	132 t/m 133	28.06	-
62	134	-	-
63	135	-	-
64	136	-	-
65	-	-	-
66	137 t/m 138	-	-
67	-	-	-
68	139	-	-
69	-	-	-
70	-	-	-
71	-	-	-
72	-	-	-
73	-	-	-
74	-	-	-
75	140	-	-
76	-	-	-
77	141	28.04	60
78	143	28.03	45-48
79	145	22	45-48

Artikel AVG	Overwegingen	Artikel Richtlijn	Artikel Wbp
80	142	-	-
81	144	-	-
82	146	23	49, 50
83	147,148,150-152	-	65-75
84	149	24	49, 50
85	153	9	03.01
86	154	-	-
87	-	08.07	24
88	155	-	-
89	156 t/m 163	32.03	-
90	164	-	-
91	165		
92	166 t/m 167	-	-
93	168 t/m 170	-	-
94	171	-	-
95	-	-	-
96	-	-	-
97	-	33	-
98	-	-	-
99	-	-	-

Bijlage 2

Omnummeringstabel Richtlijn → AVG

Artikel Richtlijn	Artikel AVG	Artikel Wbp
01	01	-
03	02	02
04	03	04
02	04	01
06	05	06,07,09-II, 15
07	06.01	08
05	06.04-04	-
-	07	-
-	08	-
08	09	03, 16-21,23
08.05	10	22
-	11	-
-	12	-
10	13	33
11	14	34
12	15	35
12.b	16	36

Artikel Richtlijn	Artikel AVG	Artikel Wbp
12.b	17	36
-	18	-
12.c	19	38
-	20	-
14	21	40, 41
15	22	42
13	23	43, 44
-	24	-
-	25	-
-	26	-
04.2	27	04.03
17	28	13, 14
16	28.03.b	12
-	29	-
-	30	-
-	31	66.03
17	32	13, 14
-	33	-
-	34	34a
-	35	-
-	36	-
28.02	36.04	51.02

Artikel Richtlijn	Artikel AVG	Artikel Wbp
20	36.05	31, 32
-	37	-
-	38	-
18.02	39	64
27	40	25
-	41	-
-	42	-
-	43	-
25	44	76, 78
25.06	45	76, 78
26.02	46	-
26.02	47	-
-	48	-
26.01	49	77
-	50	-
28.01	51	51
28.01	52	52.02
-	53	-
-	54	-
28.06	55	-
-	56	-
-	57	-

Artikel Richtlijn	Artikel AVG	Artikel Wbp
28.03	58	61, 65
28.05	59	58
-	60	-
28.06	61	-
-	62	-
-	63	-
-	64	-
-	65	-
-	66	-
-	67	-
-	68	-
-	69	-
-	70	-
-	71	-
-	72	-
-	73	-
-	74	-
-	75	-
-	76	-
28.04	77	60
28.03	78	45-48
22	79	45-48

Artikel Richtlijn	Artikel AVG	Artikel Wbp
-	80	-
-	81	-
23	82	49, 50
-	83	65-75
24	84	49, 50
9	85	03.01
-	86	-
08.07	87	24
-	88	-
32.03	89	-
-	90	-
	91	
-	92	-
-	93	-
-	94	-
-	95	-
-	96	-
33	97	-
-	98	-
-	99	-

Bijlage 3

Lijst van afkortingen

Afkringing	Betekenis
de Afdeling	Afdeling bestuursrechtspraak Raad van State
AMvB	Algemene Maatregel van Bestuur
AP	Autoriteit Persoonsgegevens
Artikel 93-comité	Het comité in het leven geroepen door artikel 93 AVG
AVG	Algemene verordening gegevensbescherming
Awb	Algemene wet bestuursrecht
BW	Burgerlijk Wetboek
de Commissie	Europese Commissie
het Comité	Europees Comité voor gegevensbescherming
DNB	De Nederlandsche Bank
DPIA	Data protection impact assessment (gegevensbeschermingseffectbeoordeling)
de e-commercerichtlijn	Richtlijn 2000/31/EG
EER	Europese Economische Ruimte
EHRM	Europese Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FG	Functionaris voor de gegevensbescherming

Handvest grondrechten EU	Handvest van de grondrechten van de Europese Unie
HR	Hoge Raad
HvJ EU	Hof van Justitie van de Europese Unie
Mkb	Midden- en kleinbedrijf
MvT	Memorie van Toelichting
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
Rv	Wetboek van Burgerlijke Rechtsvordering
VWEU	Verdrag betreffende de Werking van de Europese Unie
Wbp	Wet bescherming persoonsgegevens
Wet BRP	Wet basisregistratie personen
Wft	Wet financieel toezicht
Wiv	Wet op de inlichtingen en veiligheidsdiensten
Woo	Wet open overheid
Wor	Wet op de ondernemingsraden
Wwft	Wet ter voorkoming van witwassen en financiering van terrorisme
Zbo's	Zelfstandige bestuursorganen

