

Boetes onder het regime van de AVG

247

Trefwoorden:

boete, handhaving, AVG

De komst van de Algemene verordening gegevensbescherming (AVG) hield de gemoederen behoorlijk bezig. De angst voor torenhoge boetes zorgde er bij veel organisaties voor dat gegevensbescherming prioriteit kreeg. Bijna anderhalf jaar na het van toepassing worden van de AVG, hebben diverse Europese toezichthouders uiteenlopende boetes opgelegd op grond van de AVG. Zo werd in Frankrijk € 50 miljoen opgelegd aan Google,¹ € 18 miljoen aan de Oostenrijkse Post,² € 150 000 aan PwC in Griekenland,³ € 5000 aan een Duitse chatapp⁴ en € 388 aan een Tsjechische werkgever⁵. De Britse toezichthouder heeft een vooraankondiging van twee monsterboetes gedaan van ruim £ 183 miljoen voor British Airways en ruim £ 99 miljoen voor Marriott.⁶ En op 16 juli 2019 legde de Autoriteit Persoonsgegevens (AP) de eerste AVG-boete in Nederland op van € 460 000 aan het HagaZiekenhuis (Haga).⁷

Over de handhaving van de AVG is veel te zeggen. In dit artikel zal eerst worden ingegaan op de handhavingsmogelijkheden die de AVG de (Nederlandse) privacytoezichthouder biedt. Vervolgens wordt een aantal handhavingsbesluiten van de Nederlandse toezichthouder (onder de AVG en voorheen) en boetes opgelegd door buitenlandse toezichthouders besproken en wordt gekeken in hoeverre voorzichtige lessen uit de eerste AVG-handhavingsbesluiten zijn te trekken.

I Toezichts- en handhavingsmogelijkheden

I.1 AVG

Net als onder de Privacyrichtlijn⁸ legt de AVG het toezicht in de lidstaten neer bij een of meer onafhankelijke toezichthouders.⁹ In de meeste lidstaten is ervoor gekozen om één nationale toezichthouder aan te wijzen, in Nederland de AP.^{10, 11} Alleen Duitsland kent meerdere toezichthouders: naast een federale toezichthouder hebben alle 16 Duitse deelstaten een eigen toezichthoudende autoriteit.¹²

De AVG biedt de nationale toezichthouders – naast diverse adviserings- en toezichtstaken – een breed scala aan handhavingsbevoegdheden (artikel 57 en 58 AVG). Zo kan de toezichthouder onder meer informatie vorderen, toegang verkrijgen tot persoonsgegevens en bedrijfsruimten, waarschuwingen uitdelen, tijdelijke of definitieve verwerkingsbeperkingen opleggen, internationale gegevensstromen opschorten en uiteraard een last onder dwangsom en boetes opleggen.

Ook regelt de AVG de samenwerking tussen toezichthouders bij toezicht op grensoverschrijdende verwerkingen (hoofdstuk VII AVG).¹³

De meest controversiële vorm van samenwerking is het nieuwe één-loketmechanisme (de *onestopshop*). Het

* Herwin Roerdink en Tineke van de Bunt zijn beide advocaat bij Vondst advocaten te Amsterdam. Met dank aan Florent Beurret, student-stagiair bij Vondst, voor zijn onderzoek. De tekst van dit artikel is op 1 oktober 2019 afgesloten. Ontwikkelingen na deze datum zijn in beginsel buiten beschouwing gelaten.

1 Commission Nationale de l'Informatique et des Libertés (CNIL), 21 januari 2019, n°SAN-2019-001.

2 Österreichische Datenschutzbehörde, 28 oktober 2019.

3 Hellenic Data Protection Authority, 30 juli 2019.

4 Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, 21 november 2017.

5 Úřad Pro Ochranu Osobních Údajů, 10 januari 2019, zaaknr. UOOU-08244/18-15.

6 Er was ten tijde van het schrijven van dit artikel in beide gevallen sprake van een 'intention to fine'. Statements ICO van 8 en 9 juli 2019.

7 Autoriteit Persoonsgegevens, 16 juli 2019. Naast een bestuurlijke boete werd ook een last onder dwangsom opgelegd.

8 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

9 Artikel 51 lid 1 AVG. Een lijst met alle toezichthouders is beschikbaar op de website: https://edpb.europa.eu/about-edpb/board/members_en.

10 Onder de toekomstige ePrivacyverordening (EPV) zal in sommige landen ook de telecomtoezichthouder gedeeltelijk bevoegd zijn tot handhaving, zoals in Zweden en Polen. Vgl. de situatie in Nederland ten aanzien van de handhaving van spam- en cookieregels door ACM en AP. Voor een uitvoerige bespreking van de EPV zie H.W. Roerdink, 'Over the top: Het voorstel voor de Europese e-Privacyverordening', *IR* 2017, afl. 5/6 en H.W. Roerdink, 'Over the top: Het voorstel voor de Europese e-Privacyverordening (het vervolg)', *IR* 2019, afl. 1.

11 De verlening van mandaat, machtiging en volmacht binnen de AP is nader geregeld in het Besluit mandaat, volmacht en machtiging Autoriteit Persoonsgegevens van 11 maart 2019, op basis van artikel 15 lid 1 UAVG.

12 De toezichthouders zijn onderdeel van de Datenschutzkonferenz. Zie www.datenschutzkonferenz-online.de/index.html. De federale toezichthoudende autoriteit is de Bundesbeauftragte für Datenschutz und Informationsfreiheit – 'BfDI' (www.bfdi.bund.de).

13 Sinds de inwerkingtreding van de AVG wordt onder meer intensief samengewerkt bij de afhandeling van klachten. Dit blijkt o.a. uit: 'Toezichtkader Autoriteit Persoonsgegevens. Uitgangspunten voor toezicht 2018-2019', mei 2018, beschikbaar op: www.autoriteitper-

voorstel hiervoor stuitte op veel bezwaren bij lidstaten,¹⁴ en het mechanisme was uiteindelijk een van de laatste openstaande punten uit de AVG.¹⁵ Op grond van dit mechanisme wordt een leidende toezichthouder (de *lead authority*) aangewezen die toezicht houdt op verwerkingsverantwoordelijken en verwerkers (i) die persoonsgegevens verwerken in meerdere lidstaten, of (ii) waarvan de gegevensverwerking wezenlijke gevolgen heeft voor betrokkenen in meerdere lidstaten. De European Data Protection Board (EDPB) – het samenwerkingsorgaan van alle nationale toezichthouders – heeft richtsnoeren gepubliceerd, waarin in meer detail wordt uitgelegd op welke wijze de leidende toezichthouder moet worden vastgesteld en hoe het één-loketmechanisme moet worden toegepast.¹⁶ De *onestopshop* was een van de hete hangijzers tijdens de onderhandelingen over de AVG, mede omdat het bepaalt welke toezichthouder uiteindelijk een boete kan incasseren. De boetes komen in de meeste landen toe aan de staatskas. Dat geldt in ieder geval voor Nederland,¹⁷ België, Frankrijk, Denemarken en het Verenigd Koninkrijk. In Duitsland komt de boete toe aan de deelstaat waar de toezichthouder is gevestigd die de boete heeft opgelegd. Een aantal landen kent een regeling waarbij een deel van de boete naar de staatskas gaat en een deel (al dan niet indirect) toekomt aan de nationale toezichthouder, waaronder Oostenrijk (10%), Portugal (40%) en Italië (50%).¹⁸

Uit het Google-boetebesluit van de Franse toezichthouder CNIL kan worden afgeleid dat in ieder geval deze toezichthouder het één-loketmechanisme, in het bijzonder de rol van de leidende toezichthouder, in de praktijk niet al te nauw interpreteert in geval van grove overtredingen van de AVG.¹⁹ De CNIL besloot, kort gezegd, dat zij (en niet de toezichthouder in Ierland waar Google haar Europese hoofdkantoor heeft) bevoegd was en het één-loketmechanisme niet van toepassing was, omdat Google in Ierland geen beslissingsbevoegdheid zou hebben gehad (en dus geen verwerkingsverantwoordelijke was) met betrekking tot de verwerking die leidde tot de boete. Het lijkt erop dat de ICO in het Marriott-boetebe-

sluit wel het één-loketmechanisme heeft toegepast en als *lead authority* heeft opgetreden.²⁰ Over het één-loketmechanisme is het laatste woord nog niet gesproken.

1.2 Nationale wetgeving

De AVG geeft nationale wetgevers de ruimte om in de nationale wetgeving aanvullende bevoegdheden aan de toezichthouder toe te kennen.²¹ In Nederland is dat geregeld in de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) en de Algemene wet bestuursrecht (Awb). De Nederlandse wetgever heeft van de beleidsruimte gebruikgemaakt door de last onder bestuursdwang en last onder dwangsom als handhavingsmiddelen te handhaven (artikel 16 UAVG en titel 5.3 Awb). Met name dit laatste handhavingsmiddel werd onder de voormalige privacywetgeving regelmatig door de AP toegepast als relatief laagdrempelige manier om toezicht te houden.²² Daarnaast is de geboden beleidsruimte benut om de bevoegdheid van de AP tot het betreden van woningen zonder toestemming van de bewoner te handhaven, alsmede de algemene bevoegdheden tot toezicht op de naleving uit titel 5.2 Awb, voor zover noodzakelijk voor een goede uitoefening door de AP van haar taken (artikel 15 UAVG).

1.3 Boetebevoegdheid

Het onderdeel van de AVG dat nieuw is en het meeste stof deed opwaaien, is de boetebevoegdheid (artikel 58 lid 2 onderdeel i AVG). De privacyrichtlijn uit 1995, waarop de Wet bescherming persoonsgegevens (Wbp) gebaseerd was, bevatte een dergelijke vergaande bevoegdheid niet.²³

De algemene voorwaarden voor de boetebevoegdheid uit artikel 58 zijn uitgewerkt in artikel 83 AVG. Artikel 83 voorziet in twee boetecategorieën:

- Op grond van lid 4 kunnen toezichthouders een bestuurlijke boete van maximaal € 10 miljoen of tot 2% van de wereldwijde jaaromzet per overtre-

soonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegevens_2018-2019.pdf. Ook meldt het persbericht van de Europese Commissie 'General Data Protection Regulation shows results, but work needs to continue' van 24 juli 2019 dat de teller voor grensoverschrijdende zaken waarin door meerdere toezichthouders wordt samengewerkt eind juni 2019 op 516 zaken staat: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449.

14 Zie bijv. de uiteenzetting van 13 november 2014 over het één-loketmechanisme aan de 'Working Party on Informatie Exchange and Data Protection': www.statewatch.org/news/2014/nov/eu-dp-reg-one-stop-shop-14788-rev1-14.pdf.

15 Dit blijkt bijvoorbeeld uit de mededeling van de Europese Commissie van 11 april 2016, dat de Europese Commissie onder andere het standpunt van de Raad met betrekking tot het één-loketmechanisme aanvaardt: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CONSIL:ST_7805_2016_INIT&from=EN.

16 Richtlijnen voor het bepalen van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of de verwerker (WP 244, rev.01).

17 Artikel 14 lid 6 en artikel 16 lid 3 UAVG bepalen dat de bestuurlijke boete en de verbeurde dwangsom toekomt aan de Staat.

18 Artikel 42 van de Lei Da Proteção De Dados Pessoais en artikel 166 lid 7 van de Decreto Legislativo 30 giugno 2003, n.196.

19 Commission Nationale de l'Informatique et des Libertés, Délibération n°SAN-2019-001 du 21 janvier 2019 (Google LLC). Zie ook L. Moerel, 'CNIL's Decision Fining Google Violates One-Stop-Shop', https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3337478.

20 <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/>.

21 Uit voornoemd persbericht van de Europese Commissie van 24 juli 2019 volgt dat drie lidstaten (i.e. Griekenland, Portugal en Slovenië) hun nationale recht op dit moment nog moeten aanpassen aan de AVG.

22 MvT bij de UAVG, par. 3.4.1.

23 De Wbp bevatte wel een boete voor het niet doen van een melding van € 4500 (artikel 66), die door (destijds) het CBP een aantal malen is opgelegd. Zie o.m. ECLI:NL:RBUTR:2005:AU0980, ECLI:NL:RBSHE:2005:AT0462 en ECLI:NL:RVS:2005:AU4972. Per 1 januari 2016 kon de (inmiddels) Autoriteit Persoonsgegevens op grond van de wet van 4 juni 2015 (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid CBP) een boete van maximaal € 820 000 opleggen wegens overtreding van de Wbp. Deze boetebevoegdheid heeft de Autoriteit Persoonsgegevens voor zover bekend nooit uitgeoefend.

- ding opleggen voor overtreding van de verantwoordingsverplichtingen ('lid 4-boetes'). Het gaat dan bijvoorbeeld om onvoldoende beveiligingsmaatregelen, overtreding van de verplichting om een DPIA uit te voeren, of om een datalek (tijdig) te melden.
- Op grond van lid 5 kunnen toezichthouders een bestuurlijke boete van maximaal € 20 miljoen of tot 4% van de totale wereldwijde jaaromzet per overtreding opleggen voor overtreding van de bepalingen over de principes, rechtsgrondslagen en rechten van betrokkenen ('lid 5-boetes'). Dit omvat overtredingen van de regels die zien op geautomatiseerde besluitvorming, waaronder profilering, en op de internationale doorgifte van persoonsgegevens. In Nederland geldt deze laatstgenoemde sanctie ook bij onrechtmatige verwerking van persoonsgegevens van strafrechtelijke aard (artikel 17 UAVG). Verder kan een lid 5-boete worden opgelegd voor het niet naleven van een bevel van de AP.

In Nederland is ervoor gekozen dat de AP ook boetes kan opleggen aan overheidsinstanties en -organen (artikel 18 UAVG).²⁴ In theorie zou de AP daarmee eveneens boetes aan zichzelf kunnen (en moeten) opleggen. De AP heeft begin dit jaar zelf ook een datalek veroorzaakt: de AP stuurde een persbericht per e-mail aan 38 journalisten, redacties en relaties met de geadresseerden in het cc-veld in plaats van het bcc-veld. De AP heeft dit datalek bij zichzelf gemeld.²⁵ Voor zover bekend heeft deze melding niet tot een nader onderzoek of het opleggen van handhavende maatregelen geleid. Dat had best gekund nu het uitgerekend een datalek van de AP betrof, maar werd niet nodig geacht omdat de e-mail een verwijzing naar een algemeen persbericht betrof, de e-mail was gericht aan zakelijke adressen en het risico voor de betrokkenen gering was.

I.4 Richtsnoeren EDPB

De bepalingen ten aanzien van de boetes in de AVG zijn redelijk abstract geformuleerd. De EDPB heeft richtsnoeren aangenomen om een coherente toepassing en vaststelling van de boeteregels in de diverse lidstaten te bewerkstelligen.²⁶ Deze richtsnoeren bevatten evenwel geen aanknopingspunten voor de concrete berekening van de boetes. Dit was aanleiding voor de AP om zelf boetebeleidsregels te publiceren, zo blijkt uit de toelichting bij deze beleidsregels.²⁷ De boetebeleidsregels zullen door de AP worden gehanteerd totdat er op Europees niveau richtsnoeren zijn aangenomen.

De Duitse privacytoezichthouders hebben op 14 oktober jl. ook een voorstel gedaan voor boetebeleidsregels.²⁸ In het voorstel wordt een vijfstappenmodel geïntroduceerd om de hoogte van de boete te berekenen (op basis van onder meer de grootte van de onderneming en de jaarlijkse omzet).

I.5 Boetebeleidsregels AP

De boetebeleidsregels 2019 van de AP (Bbr) zijn een aangepaste versie van de ingetrokken boetebeleidsregels die in 2016 werden opgesteld met de introductie van de boetebevoegdheid uit de Wet meldplicht datalekken (als onderdeel van de Wbp).²⁹

De beleidsregels gaan bij de beoordeling van de hoogte van de boete uit van categorie-indelingen en boetebandbreedtes. De AVG-overtredingen zijn in bijlagen 1 en 2 Bbr ingedeeld in verschillende boetecategorieën: voor de 'lage' lid 4-boetes bevatten de nieuwe beleidsregels drie boetecategorieën (I-III), voor de lid 5-boetes vier boetecategorieën (I-IV).³⁰ Elke categorie is gekoppeld aan een boetebandbreedte die de AP 'passend en geboden voorkomt'. Per categorie is daaraan een in zwaarte oplopende basisboete verbonden van 50% van de boetebandbreedte, die door de AP als 'startbedrag' wordt genomen bij de berekening van een boete (artikel 2 Bbr).

Categorie	Boetebandbreedte	Basisboete
I	€ 0-200 000	€ 100 000
II	€ 120 000-500 000	€ 310 000
III	€ 300 000-750 000	€ 525 000
IV	€ 450 000-1 000 000	€ 725 000

De meeste lid 4-boetes vallen in categorie I of II; op een enkele uitzondering na vallen de lid 5-boetes in categorie III of IV. De overtreding van de meldplicht datalekken is een van de belangrijkste uitzonderingen op deze categorie-indeling. Hoewel een lid 4-boete, valt deze in categorie III. Onder de beleidsregels uit 2016 viel deze overtreding nog in categorie II.³¹ In de toelichting op de boetebeleidsregels wordt niet verduidelijkt welke overwegingen ten grondslag hebben gelegen aan de ophoging in categorie van de meldplicht datalekken onder de huidige boetebeleidsregels. In plaats daarvan verwijst de AP enkel naar haar algemene toelichting op de systematiek van categorie-indeling in de oude beleidsregels.

Aan de hand van de concrete boete verhogende en boete verlagende factoren berekent de AP de uiteindelijke boete (artikel 7 Bbr). Deze factoren zijn ontleend aan

²⁴ Ook bijvoorbeeld de Zweedse uitvoeringswet kent deze mogelijkheid, zij het dat voor die situatie lagere boetemaxima gelden.

²⁵ www.computable.nl/artikel/nieuws/crm/6670704/250449/autoriteit-persoonsgegevens-blundert-met-cc-knop.html.

²⁶ Richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten in de zin van Verordening (EU) 2016/679 (WP 253), goedgekeurd op 3 oktober 2017 en aangenomen door EDPB in Endorsement 1/2018 van 25 mei 2018.

²⁷ https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcr-2019-14586_0.pdf.

²⁸ Zie de Engelse vertaling van het voorstel: www.datenschutzkonferenz-online.de/media/pm/20191126_dsk_financing_concept_en.pdf.

²⁹ Zie noot 23.

³⁰ Daarnaast geven de Boetebeleidsregels categorie-indelingen en boetebandbreedtes voor bestuurlijke boetes die kunnen worden opgelegd op grond van onder meer de Telecommunicatiewet, de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.

³¹ Met uitzondering van overtredingen van artikel 33 lid 3 AVG, waarin de vereisten voor de inhoud van een melding aan de toezichthouder zijn opgenomen. Dergelijke overtredingen vallen wel in de tweede categorie.

artikel 83 lid 2 AVG. In feite wordt het bedrag van de relevante basisboete naar boven of naar beneden bijgesteld, binnen de boetebandbreedte die voor de desbetreffende categorie is vastgesteld (artikel 6 en 7 Bbr). De AP kan op grond van de relevante omstandigheden een hogere of lagere categorie en bandbreedte toepassen (artikel 8 Bbr). Op deze manier probeert de AP ervoor te zorgen dat de uiteindelijke boete voldoende afschrikwekkend effect heeft voor zowel de overtreder als voor potentiële overtredders in het algemeen. De boete wordt in beginsel met 50% verhoogd in geval van recidive (artikel 8.2 Bbr).

Opvallend is dat de vastgestelde maximumboetes substantieel lager zijn dan de maximumboetes die de toezichthouder op grond van de AVG zou kunnen opleggen. Een verklaring hiervoor kan zijn dat de boetebeleidsregels basale uitgangspunten bevatten ‘gericht op middelgrote organisaties’, zoals AP-voorzitter Wolfsen in een interview heeft benadrukt.³² Dit is opmerkelijk en blijkt overigens op geen enkele manier uit de beleidsregels. ‘Bij de grote bedrijven kun je heel gemakkelijk naar de hoogste bedragen gaan die onder de AVG kunnen worden opgelegd’, aldus Wolfsen. De beleidsregels geven de AP uitdrukkelijk de ruimte om nog steeds de maximumboetes uit de AVG op te leggen als de boetebandbreedtes in een concreet geval geen passende bestraffing toelaten (artikel 8.3 en 8.4 Bbr). Artikel 4:84 Awb biedt vanwege bijzondere gevallen die niet in de beleidsregels zijn verdisconteerd tevens nog de mogelijkheid om daarvan af te wijken (inherente afwijkingsbevoegdheid). Maar daarbij kan niet enkel de grootte van een organisatie doorslaggevend zijn (en wanneer is een bedrijf ‘groot’?). Wij vermoeden daarom dat de AP in de meeste gevallen de hoogtes uit de boetebeleidsregels zal hantieren.

Zowel de AVG, de richtsnoeren van de EDPB als de boetebeleidsregels zijn bovendien onduidelijk over de jaaromzet die als uitgangspunt moet worden genomen voor de toepassing van de boetemaxima. Betreft dit de omzet van het gehele concern, of alleen de desbetreffende onderneming die de norm heeft overtreden? Er zijn goede argumenten om te betogen dat de AP bij het bepalen van de wereldwijde jaaromzet alleen de (netto-)omzet van de

desbetreffende onderneming als uitgangspunt dient te nemen, en niet die van het gehele concern. De AVG refereert immers aan de omzet van de onderneming, en spreekt niet over het concern. Ook bevat de memorie van toelichting bij de UAVG aanknopingspunten voor deze beperkte uitleg.³³ Daartegenover staat dat in overweging 150 AVG wordt opgemerkt dat het begrip ‘onderneming’ ziet op ‘een onderneming overeenkomstig de artikelen 101 en 102 van het VWEU’. Op basis hiervan zou kunnen worden beargumenteerd dat moet worden aangesloten bij het (ruimere) mededingingsrechtelijke ondernemingsbegrip, maar dit lijkt te verstrekkend. In de AVG zelf komt deze verwijzing echter niet terug.³⁴ Daarbij komt dat het nog onduidelijk is welk percentage wordt genomen. Artikel 83 lid 4 en 5 spreken van een maximaal percentage (‘tot’), hetgeen impliceert dat de toezichthouder ook een lager percentage kan hanteren. De boetebeleidsregels geven op dit punt geen duidelijkheid.

Een ander punt van onduidelijkheid is in hoeverre een verwerkingsverantwoordelijke een aan hem opgelegde boete kan afwentelen op een verwerker, en *visa versa*. Artikel 82 AVG, dat kort gezegd de aansprakelijkheid van verwerkingsverantwoordelijken en verwerkers voor schade als gevolg van AVG-inbreuken regelt, lijkt niet zonder meer van toepassing op (schade als gevolg van) boetes. Het contractueel ‘doorschuiven’ van boetes lijkt daarmee ook onder de AVG mogelijk. De vraag is wel in hoeverre doorschuiven in de praktijk redelijk is. Uit de recent door de AP goedgekeurde Data Pro Code van Nederland ICT kan namelijk worden afgeleid dat de AP boetes in beginsel alleen zal opleggen aan de partij die daadwerkelijk de AVG schendt³⁵ (en daarmee doorgaans ook de (verwerkers)overeenkomst).

1.6 Publicatie van boetebesluiten

In diverse lidstaten is het gebruikelijk dat boetebesluiten worden gepubliceerd. In Nederland vindt openbaarmaking plaats in overeenstemming met de Beleidsregels openbaarmaking.³⁶ De publicatieplicht is niet opgenomen in de UAVG. De AP heeft wel geprobeerd om een speci-

32 E.P.M. Thole, Ö. Zivali & C. Ebbers, “‘Voor diverse zaken is het boetetraject gestart’”. Interview met Aleid Wolfsen, voorzitter van de AP, één jaar na de AVG, *P&I* 2019, afl. 3.

33 *Kamerstukken II* 2017/18, 34851, 3, p. 30 (MvT): ‘Het begrip omzet is niet gedefinieerd in de verordening. In de beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015 met betrekking tot het opleggen van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2016, *Stcrt.* 2016 nr. 2043) wordt hiervoor met betrekking tot het begrip jaaromzet van de rechtspersoon aangesloten bij de netto-omzet, bedoeld in artikel 377, zesde lid, van Boek 2 van het Burgerlijk Wetboek. Het ligt voor de hand dat dit wederom als uitgangspunt zal worden genomen voor het nieuw op te stellen beleid van de Autoriteit Persoonsgegevens.’ Artikel 2:377 lid 6 BW luidt: ‘Onder de netto-omzet wordt verstaan de opbrengst uit levering van goederen en diensten uit het bedrijf van de rechtspersoon, onder aftrek van kortingen en dergelijke en van over de omzet geheven belastingen.’

34 Voor een uitgebreide behandeling van het mededingingsrechtelijke ondernemingsbegrip in het kader van de AVG, zie E. Oude Elferink & J.G. Reus, ‘Handhaving van de Algemene Verordening Gegevensbescherming vanuit Nederlands Perspectief’, *NtER* 2017, afl. 6, p. 157-164.

35 Dit volgt uit de Standaardclausules voor verwerkingen, welke onderdeel zijn van de goedgekeurde Data Pro Code van Nederland ICT. Artikel 2.8 luidt: ‘Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van Data Processor.’ In de (niet door de AP goedgekeurde) toelichting van Nederland ICT bij deze bepaling staat nog vermeld dat de AP als uitgangspunt heeft ‘dat boetes alleen opgelegd moeten worden aan de partij die daadwerkelijk de Avg schendt. Indien een data processor zich niet aan de Avg houdt, zou de boete dus rechtstreeks aan hem en niet aan de verwerkingsverantwoordelijke of opdrachtgever opgelegd moeten worden. Als een boete aan de verwerkingsverantwoordelijke wordt opgelegd, dan betekent dat dus dat hij zich zelf schuldig maakt aan schending van de Avg. In dat geval is het merkwaardig dat hij deze boete eenvoudig zou kunnen “doorschuiven” aan de verwerker.’

36 Beleidsregels openbaarmaking door de Autoriteit Persoonsgegevens van 12 januari 2016, gepubliceerd in *Stcrt.* 2016, 1380.

fieke wettelijke grondslag voor actieve openbaarmaking van handhavingsbesluiten in de AVG te laten opnemen, maar dat lag gelet op het beleidsneutrale karakter van de UAVG, niet voor de hand, aldus de Minister voor Rechtsbescherming.³⁷

Voorafgaand aan publicatie wordt door de AP op grond van artikel 4 Beleidsregels openbaarmaking een voorname tot openbaarmaking gezonden, op grond waarvan de onderzochte (rechts)persoon nog 10 werkdagen wordt gegund om aan te geven of het besluit nog (bedrijfs)vertrouwelijke gegevens bevat en eventueel rechtsmiddelen aan te wenden tegen de openbaarmaking.³⁸ Dat betekent in de praktijk een kortgedingprocedure, want een bezwaarschriftprocedure tegen het boetebesluit schorst de publicatie van het boetebesluit niet. De rechter zal een nadere afweging moeten maken tussen het algemene belang dat door openbaarmaking wordt gediend en het belang van de beboete organisatie om geen onevenredig nadeel te lijden als gevolg van de publicatie. Daarbij wordt aan het algemeen belang een groot gewicht toegekend.

II AVG-handhaving in Nederland

Naast de hierna te bespreken boetetrajecten is de AP conform haar toezichtskader 2018-2019 ook op andere wijze handhavend opgetreden.

II.1 Controleren naleving AVG: verkennende onderzoeken en pre-AVG-handhaving

Op basis van de verplichting uit artikel 57 lid 1 onderdeel h AVG, kan de AP actief onderzoeken of verwerkingsverantwoordelijken de normen van de AVG naleven. De AP heeft al diverse verkennende onderzoeken ('speldenprikacties', zoals de AP het noemt) uitgevoerd, waaronder naar naleving van de FG-verplichting door diverse ziekenhuizen, (zorg)verzekeraars, banken en overheidsinstellingen, naar het gebruik verwerkersovereenkomsten door (rechts)personen, en naar de naleving van de verplichting een register van verwerkingsactiviteiten bij te houden door private partijen.³⁹ Daarnaast kan de AP steekproefsgewijs onderzoek doen in opvolging van door haar verstuurdte waarschuwingen. Onderzochte

(rechts)personen zijn desgevraagd gehouden om mee te werken aan dergelijke verkennende onderzoeken van de AP (artikel 31 AVG).⁴⁰

Op overtreding van deze medewerkingsverplichting staat een lid 4-boete. In de praktijk zal de soep waarschijnlijk wat minder heet worden gegeten als zij wordt opgediend. Een overtreding van deze verplichting is in de boetebeleidsregels ingedeeld in boetecategorie III. Voor deze categorie is een boetebandbreedte vastgesteld tussen de € 300 000 en € 750 000, en een basisboete van € 525 000.⁴¹ Ook kan de AP bij overtreding een last onder bestuursdwang opleggen (artikel 16 lid 2 AVG).⁴² Een beroep op het zwijgrecht is pas mogelijk op het moment dat een verkennend onderzoek van de AP overgaat in een voornemen van de AP tot het opleggen van een punitieve sanctie.⁴³

Daarnaast heeft de AP het afgelopen jaar aan diverse organisaties een last onder dwangsom opgelegd, voor overtredingen die al waren begonnen voordat de AVG van toepassing was maar daarna nog voortduurden. Zo legde de AP een last onder dwangsom op aan UWV vanwege een gebrekkig beveiligingsniveau van het werkgeversportaal, aan de Nationale Politie vanwege een gebrekkige beveiliging van politiegegevens⁴⁴ en aan Menzis vanwege onbevoegde toegang door werknemers tot medische gegevens. Ten onrechte werd de invordering van deze laatste dwangsom door de AP (o.a. door Menzis zelf) bestempeld als boete. De AP heeft pas recent de besluiten gepubliceerd die ten grondslag liggen aan de laatstgenoemde last onder dwangsom en de invordering ervan,⁴⁵ nu deze onderdeel waren van een gerechtelijke procedure.⁴⁶

In de praktijk blijkt een last onder dwangsom minstens zoveel impact te hebben als een boete: de tijd waarbinnen de last moet worden uitgevoerd is vaak beperkt gezien de benodigde maatregelen, en de dwangsom kan snel oplopen. Zo moest zowel de Nationale Politie als UWV binnen 6 respectievelijk 3 maanden passende beveiligingsmaatregelen treffen met een dreigende dwangsom van € 12 500 per week (met een maximum van € 200 000) en € 150 000 per maand (met een maximum van € 900 000). Uit de website van de AP blijkt overigens dat de AP heeft beoordeeld dat het beide partijen – anders dan Menzis –

37 Zie par. 7.2.4 Openbaarmakingsverplichting in de MvT bij de UAVG.

38 Zie artikel 4 Beleidsregels openbaarmaking door de Autoriteit Persoonsgegevens.

39 Tot op heden is volgens de website van de AP alleen het eerste onderzoek (naar de FG-verplichting) afgerond.

40 Verkennende onderzoeken kunnen tot handhaving leiden in het geval dat er een overtreding wordt geconstateerd, hoewel handhaving niet de primaire insteek is. Zie E.P.M. Thole, Ö. Zivali & C. Ebbers, "Voor diverse zaken is het boetetraject gestart". Interview met Aleid Wolfsen, voorzitter van de AP, één jaar na de AVG, *P&I* 2019, afl. 3.

41 Dit is af te leiden uit de Boetebeleidsregels 2019, inclusief bijlage 1. Onder omstandigheden kan een hogere boete worden opgelegd.

42 Artikel 31 AVG is een *lex specialis* van artikel 5:20 Awb. Opzettelijke niet-naleving van de medewerkingsverplichting uit de Awb is overigens ook strafbaar, bijvoorbeeld op grond van artikel 184 lid 1 Sr.

43 Het zwijgrecht is geregeld in artikel 5:10a Awb. Volgens de Raad van State volgt uit artikel 5:10a Awb dat de cautieplicht bestaat 'wanneer naar objectieve maatstaven door een redelijk waarnemer kan worden vastgesteld dat de betrokkene wordt verhoord met het oog op het aan hem opleggen van een bestraffende sanctie' (ABRvS 27 juni 2018, ECLI:NL:RVS:2018:2115). Het is aannemelijk dat dezelfde systematiek geldt ten aanzien van artikel 31 AVG.

44 Zie respectievelijk https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/last_onder_dwangsom_uwv_werkgeversportaal.pdf en https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/last_onder_dwangsom_nationale_politie_februari_2017.pdf.

45 Zie respectievelijk autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_last_onder_dwangsom_menzis.pdf en autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_invordering_dwangsom_menzis.pdf.

46 https://twitter.com/toezicht_AP/status/1113777423567544320.

wel is gelukt om de bevolen maatregelen binnen de gestelde termijn te treffen.⁴⁷

II.2 Risicogericht toezicht

In het kader van risicogericht toezicht heeft de AP de sectoren overheid, zorg en bedrijven die handelen in persoonsgegevens als aandachtspunten bestempeld. Daarbij wordt extra aandacht besteed aan niet-gemelde datalekken en datalekken die zijn veroorzaakt door ernstige tekortkomingen in de beveiliging. Dit neemt niet weg dat actualiteiten en klachten aanleiding kunnen geven tot optreden in andere sectoren of op andere gebieden, zoals recent de plannen van banken om betaalgegevens te gebruiken voor gepersonaliseerde reclame,⁴⁸ de opslag van medische gegevens in de cloud⁴⁹ en de journalistieke informatie van Trouw en RTL Nieuws dat de Belastingdienst fraude met de kinderopvangtoeslag opspoorde op basis van etnische achtergrond dan wel (tweede) nationaliteit.⁵⁰

In het kader van risicogericht toezicht heeft de AP onder meer eind vorig jaar een verwerkingsverbod opgelegd aan de Minister van Financiën, voor gebruik van het BSN in het btw-identificatienummer van zelfstandigen door de Belastingdienst, omdat dat in strijd is met artikel 46 UAVG en artikel 5 lid 1 onderdeel a en artikel 6 lid 1 AVG.⁵¹

Het lijkt aannemelijk dat het risicogericht toezicht ook heeft geleid tot de boetes van de AP aan Uber en het Haga (zie nader hieronder). Uit de boetebesluiten blijkt dat beide boetes volgen op onderzoek van de AP naar aanleiding van datalekmeldingen door de respectievelijke verwerkingsverantwoordelijken. Een ander aspect dat zal hebben meegespeeld, is dat de datalekken bij Uber en het Haga breed zijn uitgemeten in de media. In die zin leenden de zaken zich goed om aan andere marktpartijen een voorbeeld te stellen.

II.3 AVG-boetes

Sinds de invoering van de AVG zijn in Nederland tot nu toe twee grote boetes opgelegd: aan Uber en het Haga. In het eerder aangehaalde interview met de AP-voorzitter, merkt Wolfsen op dat de AP de boete die zij in augustus 2018 oplegde aan techbedrijf Uber ook aanmerkt als een AVG-boete:

‘Er was sprake van een voortdurende overtreding door Uber, die was weliswaar ontstaan onder de Wbp, maar het niet informeren van de betrokkenen over het datalek door Uber was een voortdurende overtreding, ook nog onder de AVG. Alleen bij de hoogte van de boete hebben we rekening gehouden met de Wbp.’

Hoe dit ook zij, de AP heeft aan Uber een boete opgelegd wegens overtreding van artikel 34a lid 1 en 2 Wet bescherming persoonsgegevens (Wbp) en heeft aangesloten bij het in vergelijking met de AVG ‘gunstiger’ boeteregime onder de Wbp. In het Haga-besluit is daarentegen een boete opgelegd op grond van artikel 32 AVG. Wij houden het er daarom op dat het Haga er met de ‘eer’ van de eerste AVG-boete in Nederland vandoor gaat.

Als gezegd, volgden beide boetes op een datalekmelding, maar blijkt uit de boetebesluiten niet waarom de AP er in het geval van Haga voor heeft gekozen de ontoereikende beveiligingsmaatregelen te beboeten, terwijl in het geval van Uber enkel het ontbreken van de melding c.q. de te late melding is beboet en niet (óók) de ontoereikende beveiligingsmaatregelen. Omgekeerd kan de vraag ook worden opgeworpen waarom bij Haga niet ook een overtreding van de meldplicht datalekken onderzocht had moeten worden.⁵²

II.4 (Pre-)AVG-boete Uber

Uit het besluit dat ten grondslag ligt aan de Uber-boete zijn voor de praktijk interessante lessen te leren. Daarom wordt hieronder dieper op enkele aspecten van dit boetebesluit ingegaan.

Op 6 november 2018 heeft de AP aan Uber B.V. en Uber Technologies Inc. gezamenlijk een boete opgelegd van € 600 000 wegens het niet tijdig melden van een datalek met betrekking tot in de VS opgeslagen persoonsgegevens. Het datalek betrof 57 miljoen betrokkenen wereldwijd, waarvan 174 000 uit Nederland.

Uit het procesverloop blijkt dat de boete volgt op ambtshalve onderzoek dat de AP heeft ingesteld naar aanleiding van een datalekmelding van Uber B.V. op 21 november 2017. Opvallend is de snelheid waarmee de AP na de melding in actie is gekomen (temeer nu dit een van de in totaal ruim 10 000 datalekken was die in 2017 werden gemeld bij de AP); slechts twee dagen na de melding heeft de AP Uber al een eerste schriftelijk informatieverzoek verstuurd. En ruim een week na de melding is er al een Europese taskforce opgericht onder leiding van de AP om de onderzoeken van de verschillen-

47 <https://autoriteitpersoonsgegevens.nl/nl/nieuws/nationale-politie-voldoet-aan-last-onder-dwangsom> en <https://autoriteitpersoonsgegevens.nl/nl/nieuws/uwv-heeft-werkwijze-verzuimbeheer-aangepast-na-onderzoek-ap>. De Nationale Politie had overigens aan een eerdere last niet voldaan en een dwangsom van € 40 000 betaald aan de AP.

48 Klachten bij de AP over deze plannen hebben geleid tot een normoverdragende brief van de AP aan de brancheorganisatie, de Nederlandse Vereniging van Banken (NVB) op 3 juli 2019.

49 <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-stelt-geen-onderzoek-naar-opslag-medische-gegevens-cloud>.

50 Vragen van Trouw en RTL Nieuws hebben geleid tot het instellen van onderzoek door de AP naar de verwerking van bijzondere persoonsgegevens zoals nationaliteit bij de Belastingdienst. Dit blijkt uit een persbericht van de AP: <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-doet-onderzoek-naar-verwerking-nationaliteit-bij-belastingdienst>.

51 www.autoriteitpersoonsgegevens.nl/nl/nieuws/belastingdienst-mag-bsn-niet-meer-gebruiken-btw-identificatienummer.

52 Uit het nieuwsitem destijds op de website van het programma ‘EenVandaag’ blijkt dat al sinds half maart een intern onderzoek liep nadat bij routinecontrole was gebleken dat tientallen medewerkers het dossier hadden bekeken die mogelijk niet medisch betrokken waren: <https://eenvandaag.avrotros.nl/item/tientallen-snuffelden-ongeoorloofd-in-medisch-dossier-barbie>.

de toezichthouders naar de datalek bij het Uber concern te onderzoeken.⁵³ Uiteindelijk heeft het wel zo'n halfjaar (en meerdere informatieverzoeken) geduurd totdat de AP tot een voornemen tot opleggen van een boete is gekomen, en bijna een jaar totdat de AP de boete daadwerkelijk heeft opgelegd. De periode vanaf het instellen van een onderzoek tot de oplegging van een sanctie is daarmee een aantal maanden langer dan bij het Haga, maar zo'n vier maanden korter dan in het geval van de last onder dwangsom aan het UWV.⁵⁴

Het Uber-besluit bevat voor de praktijk een aantal interessante onderdelen, onder meer de kwalificatie van Uber B.V. en Uber Inc. als gezamenlijke verwerkingsverantwoordelijken voor de verwerking. Voor nu beperken wij ons tot de wijze waarop de boete tot stand is gekomen. Hoewel voor de berekening van de boete de oude boetemaxima en Boetebeleidsregels 2016 als uitgangspunt zijn genomen, is de gebruikte methodiek dezelfde als die door de AP voor AVG-boetes wordt gebruikt, op basis van de nieuwe Bbr.

Het boetebesluit geeft een goede eerste inkijk in de wijze waarop de AP in de praktijk omgaat met het mechanisme van basisboete, boete verhogende en verlagende factoren, en boetebandbreedte uit de boetebeleidsregels. De wettelijke maximumboete die de AP destijds voor een overtreding van de meldplicht datalekken kon opleggen was € 820 000 per overtreding. In de Boetebeleidsregels 2016 was een overtreding van de meldplicht aan de AP en betrokkenen ingedeeld in categorie II met een bandbreedte van € 120 000 en € 500 000. De AP hanteerde destijds een basisboete op 33% van de bandbreedte, maar gaat in dit geval zonder nadere motivering uit van een hogere basisboete van € 246 500 per overtreding.

Na vaststelling van de basisboete, heeft de AP aan de hand van de ernst van de overtreding, de mate van verwijtbaarheid van Uber en het evenredigheidsbeginsel beoordeeld of er aanleiding is voor verhoging of verlaging daarvan. Dat gebeurt trapsgewijs. De AP achtte de overtreding dusdanig ernstig dat zij de basisboete eerst met een derde heeft verhoogd tot € 327 845 (wat overigens iets minder is dan een derde). De AP nam daarbij in aanmerking dat het lek te laat is gemeld aan de AP en de betrokkenen, betrokkenen door het gebrek aan transparantie geen, of pas laat, voorzorgsmaatregelen hebben kunnen treffen, de AP belemmerd is in haar toezichtstaken, het lek een groot aantal personen in zowel Nederland als daarbuiten heeft getroffen, en het lek een grote hoeveelheid persoonsgegevens betrof. Vervol-

gens heeft de AP de basisboete nogmaals verhoogd met (ook net iets minder dan) een derde tot € 409 190, omdat zij de late melding ernstig verwijtbaar achtte. Daarbij speelde mee dat Uber zich bewust was van de ernst van het lek en de melders een hoge *bounty award*⁵⁵ heeft toegekend in ruil voor geheimhouding. Voor de twee overtredingen (niet melden aan de AP én niet melden aan de betrokkenen) zou de totale boete daarmee uitkomen op € 818 380. Dit totale boetebedrag achtte de AP onevenredig, mede gelet op de omstandigheid dat de strekking van de overtredingen in de kern overeenkomt, en de gedragingen die aan de overtredingen ten grondslag liggende dezelfde zijn. Daarbij speelde een rol dat het datalek de nodige media-aandacht heeft gehad. De AP matigde de boete daarom tot in totaal € 600 000. Deze vermindering lijkt evenwel redelijk willekeurig te zijn vastgesteld en staat in contrast met de gemotiveerdere verhoging van de basisboete door de AP én het boetebedrag dat onder de AVG had kunnen worden opgelegd (begroot op ongeveer € 1 miljoen per overtreding). Wellicht dat de AP in het eerste 'grote' boetebesluit niet te veel risico heeft willen nemen.

II.5 AVG-boete HagaZiekenhuis

De AP legde op 18 juni 2019 de eerste AVG-boete op aan het Haga in verband met het in de pers breed uitgemeten 'Barbie-incident'.⁵⁶ Zo'n 100 medewerkers van het Haga hadden toegang tot het dossier van de Haagse realityster Barbie, terwijl zij geen behandel- of zorgrelatie met haar hadden. De AP heeft het Haga hiervoor een boete van € 460 000 opgelegd. Daarbovenop heeft de AP het Haga een last onder dwangsom opgelegd van € 100 000 voor elke twee weken na 2 oktober 2019 dat zij de beveiliging van haar informatiesysteem niet heeft verbeterd, met een maximum van € 300 000.

Uit het procesverloop dat is beschreven in het boetebesluit, blijkt dat de AP ook in het geval van het Haga ambtshalve onderzoek heeft ingesteld naar aanleiding van de ontvangen datalek melding. Hoewel de AP wat langer heeft gewacht met het versturen van het eerste informatieverzoek dan bij de melding van Uber, heeft zij relatief gezien nog steeds doortastend gehandeld: een kleine drie weken nadat de melding van het datalek op 4 april 2018 was ontvangen is het informatieverzoek uitgestuurd. Opvallend detail is dat het versturen van het informatieverzoek heeft plaatsgevonden drie dagen nadat de Minister voor Medische Zorg en Sport op 20 april 2018 in zijn antwoord op Kamervragen over de ongeoorloofde inzage in het medische dossier van Barbie had benadrukt dat de AP toeziet op naleving van de pri-

53 <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-leidt-taskforce-bij-onderzoeken-datalek-uber>. Ook het onderzoek van Engelse toezichthouder (ICO) heeft geresulteerd in een boete aan Uber op grond van nationale pre-AVG-wetgeving. Dit betrof een boete van £ 385 000, wegens overtreding van de verplichting om persoonsgegevens adequaat te beveiligen: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/>.

54 Zie noot 44.

55 Dit is een vergoeding of premie die aan een partij, vaak een (ethical) hacker, wordt uitgekeerd, als deze partij een kwetsbaarheid in het systeem van een bedrijf vindt en deze aan het bedrijf rapporteert. Doorgaans zijn aan zo'n vergoeding voorwaarden verbonden met betrekking tot geheimhouding van de gevonden kwetsbaarheid, die zijn neergelegd in een 'responsible-disclosure'-beleid.

56 Zie bijvoorbeeld: <https://eenvandaag.avrotros.nl/item/tientallen-snuffelden-ongoorloofd-in-medisch-dossier-barbie/> en www.nrc.nl/nieuws/2018/04/09/barbie-zaak-toont-zwakke-epd-a1598782.

vacysregels.⁵⁷ Een andere afwijking ten opzichte van het Uber onderzoek, is dat er bij het Haga een (aangekondigd) onderzoek ter plaatse heeft plaatsgevonden. Een voor de hand liggende verklaring hiervoor is dat het onderzoek bij Uber zich concentreerde op de overtreding van de meldplicht zelf, terwijl in het geval van het Haga enkel de getroffen beveiligingsmaatregelen onder de loep zijn genomen.

In de boetebeleidsregels is voor de onderhavige lid 4-boete een boetebandbreedte van tussen de € 120 000 en € 500 000, en een basisboete van € 310 000 vastgesteld.

Bij de hoogtebepaling is door de AP bij beoordeling van de eerste factor – de aard, ernst en duur van de overtreding – ook de categorie van persoonsgegevens meegewogen, waardoor deze vervolgens niet afzonderlijk redenen geven om de boete te verhogen of verlagen. De vraag is of deze aanpak van de AP strikt genomen juist is, gelet op de tekst van artikel 83 lid 2 onderdeel a AVG. Voor de bepaling van de aard, ernst en duur van de inbreuk moet volgens onderdeel a namelijk rekening worden gehouden met de aard, de omvang of het doel van de verwerking, het aantal getroffen betrokkenen en de omvang van de door hen geleden schade, en dus niet met de categorie van persoonsgegevens.

De ernst en structurele aard van de overtreding, alsook het feit dat de overtreding nog voortduurt, ondanks het Barbie-incident, waren voor de AP aanleiding om de basisboete met € 75 000 te verhogen, naar € 385 000. De AP woog onder andere mee dat er sprake is van een situatie waarin het vertrouwen van patiënten in een zorgvuldige verwerking van hun gegevens in hoge mate is beschaamd, gelet op de grote omvang van het aantal betrokken patiënten opgenomen in het systeem en de gevoeligheid van de gegevens. Onduidelijk is waarom de AP de basisboete overigens met ongeveer een kwart en niet met een derde verhoogt, zoals zij deed in het hiervoor besproken Uber-boetebesluit.

De AP verhoogde de boete vervolgens nogmaals met € 75 000, naar in totaal € 460 000, gelet op (bijzondere) nalatigheid van het Haga in het treffen van adequate beveiligingsmaatregelen, bestaand uit de tweefactor-authenticatie en regelmatige controle van logbestanden. Wederom is onduidelijk waarop dit bedrag van € 75 000 is gebaseerd. Volgens de AP had van het Haga mogen worden verlangd dat zij zich op de hoogte had gesteld van de juiste implementatie van de geldende normen in het licht van de aard en omvang van de verwerking. De argumenten van het Haga, dat zij onvoldoende tijd en middelen beschikbaar had om passende maatregelen te treffen, bijvoorbeeld om frequenter steekproeven uit te voeren, werden door de AP van de hand gewezen.

Naar aanleiding van het Barbie-incident had het Haga uit eigen initiatief een intern onderzoeksrapport laten opstellen, waarin diverse beveiligingsmaatregelen werden

aanbevolen. De AP constateerde dat het Haga een deel van deze maatregelen inmiddels heeft geïmplementeerd, maar een ander deel niet. Dit laatste werd het Haga relatief zwaar aangerekend, in de zin dat de basisboete geheel niet werd verlaagd in het licht van de genomen maatregelen.

Ten slotte waren er volgens de AP geen overige omstandigheden die tot verhoging of verlaging van de boete kunnen leiden. De gevoelige aard van de persoonsgegevens waarop de overtreding betrekking heeft, resulteert niet tot een verdere verhoging, omdat deze aard al als boete verhogende omstandigheid was meegewogen. Ook zag de AP op grond van de concept jaarrekening van het Haga geen aanleiding om de boete te matigen op grond van het evenredigheidsbeginsel (artikel 3:4 en 5:46 Awb). Daarmee blijft het boetebedrag steken op € 460 000.

Gelet op de voortdurende overtreding bleef het niet bij een bestuurlijke boete voor het Haga, maar is ook een last onder dwangsom opgelegd van € 100 000 voor iedere twee weken dat de overtreding na afloop van de begunstigingstermijn van 15 weken voortduurt. De dwangsom is gemaximeerd op € 300 000. De AP heeft bij het vaststellen van de begunstigingstermijn rekening gehouden met de planning van het Haga voor het uitvoeren van de maatregelen.

III AVG-handhaving in Europa

In de andere EU-lidstaten hebben de toezichthouders evenmin stilgezeten. Een groot aantal Europese toezichthouders heeft inmiddels boetes opgelegd op grond van de AVG.

De beboete partijen zijn actief in een keur aan sectoren. De meeste boetes zijn opgelegd aan partijen uit de bankensector, de publieke sector (bijv. politie en gemeenten) en de financiële sector (bijv. incassobureaus), gevolgd door de zorgsector en de horecasector.

Wij hebben globaal onderzoek gedaan naar de boetebesluiten die online te vinden zijn. Weliswaar bepleit de EDPB dat ‘een consequente handhaving van gegevensbeschermingsregels centraal [staat] in een geharmoniseerde gegevensbeschermingsregeling’,⁵⁸ maar van uniformiteit lijkt vooralsnog geenszins sprake:

- Allereerst moet worden opgemerkt dat niet alle boetebesluiten openbaar toegankelijk zijn. Zo zijn de boetebesluiten van Duitse, Griekse, Poolse en Roemeense toezichthouders niet openbaar beschikbaar, anders dan bijvoorbeeld de boetebesluiten van de Nederlandse, Spaanse, Oostenrijkse, Franse en Tsjechische toezichthouders.
- In sommige gevallen worden boetebesluiten alleen samengevat in een kort persbericht.
- Ook worden alle boetebesluiten en de persberichten alleen gepubliceerd in de officiële taal van de lidstaat. Menigeen zal daardoor niet alle uitspraken kunnen lezen, anders dan via een vertaling. Bij hoge

⁵⁷ Antwoord op vragen van het Kamerlid Dijkema (PvdA) over het bericht ‘Tientallen snuffelen ongeoorloofd in medisch dossier Barbie’ (2018Z06397), 20 april 2018, beschikbaar op: https://eenvandaag.avrotros.nl/fileadmin/user_upload/beantwoording-kamervragen-over-het-bericht-27tientallen-snuffelden-ongeorloofd-in-medisch-dossier-barbie.pdf.

⁵⁸ Zie noot 26.

- uitzondering worden het boetebesluit en het persbericht – naast de officiële taal van de lidstaat – in de Engelse taal gepubliceerd.
- Anders dan andere toezichthouders is de Britse toezichthouder ICO op grond van de UK Data Protection Act 2018 gehouden om voorafgaand aan het opleggen van een boete eerst een schriftelijke ‘*notice of intent*’ te geven, zoals is gebeurd in relatie tot het Marriott en British Airways.⁵⁹ De ICO zal het verweer van de onderzochte partijen en de andere betrokken toezichthouders beoordelen voordat zij een definitief besluit neemt.
 - De boetebesluiten van de verschillende toezichthouders die wél integraal zijn gepubliceerd, hebben ieder een eigen vorm en wijken in omvang, motivering en diepgang erg af. Het is hierdoor maar zeer de vraag of bijvoorbeeld in een Nederlandse AVG-handhavingprocedure met succes kan worden verwezen naar een boetebesluit of uitspraak in bezwaar of beroep uit een ander EU-land, ondanks de beoogde harmonisatie.

Op basis van de gevonden boetebesluiten kunnen de volgende algemene inzichten worden verkregen.

III.1 Aantal en hoogte boetes

Het totaal aantal boetes dat is opgelegd is niet met zekerheid vast te stellen. De eerdergenoemde onlinebronnen gaan uit van al zeker 97 boetes sinds het moment dat de AVG van toepassing werd tot en met september 2019.⁶⁰ Daaronder zijn 10 Duitse boetes meegenomen, maar het lijkt erop dat het aantal opgelegde boetes in Duitsland vele malen hoger is. Zo spreekt *Die Welt* al in mei 2019 van ten minste 81 AVG-boetes in Duitsland.⁶¹

Uit de geraadpleegde bronnen blijkt dat verder de meeste boetes zijn opgelegd in Hongarije (10), Spanje (10) en Tsjechië (9). Bulgarije (8), Oostenrijk (8) en Roemenië (7) volgen daar kort achter.

De overgrote meerderheid van de boetes is opgelegd aan rechtspersonen en overheidsinstellingen. Ten minste zes boetes zijn opgelegd aan natuurlijke personen: een Oostenrijkse voetbalcoach die vrouwelijke spelers onder de douche filmde (€ 11 000), een Belgische burgemeester voor misbruik van gegevens voor campagnedoelinden (€ 2000), een Duitse politieagent voor het ongeoorloofd gebruiken van gegevens uit het Federale verkeersinformatiesysteem (€ 1400), een Duitse spammer (€ 2000), een Oostenrijker wegens het gebruik van een CCTV-systeem mede gericht op openbare ruimte (€ 2200) en een Oostenrijkse autobezitter wegens onrechtmatig gebruik van een dashcam (€ 300).

De hoogste vijftien boetes zijn opgelegd in de volgende landen:⁶²

Lidstaat	Hoogte	Opgelegd door	Opgelegd aan	Datum
Verenigd Koninkrijk ⁶³	£ 183 390 000	ICO	British Airways	8 juli 2019
Verenigd Koninkrijk ⁶⁴	£ 99 200 396	ICO	Marriott International, Inc.	9 juli 2019
Frankrijk	€ 50 000 000	CNIL	Google Inc.	21 januari 2019
Oostenrijk	€ 18 000 000	Datenschutz-behörde (DSB)	Österreichische Post	23 oktober 2019
Duitsland	€ 14 500 000	Data Protection Authority Berlin	Property company	30 oktober 2019
Bulgarije	€ 2 600 000	KZLD	National Revenue Agency	28 augustus 2019

⁵⁹ Data Protection Act 2018, Section 155, Schedule 16.

⁶⁰ Er is online geen uitputtende database van boetebesluiten, maar er zijn wel verschillende overzichten van AVG-boetes te vinden: zie o.m. https://edpb.europa.eu/news/national-news/2019/first-significant-fine-was-imposed-breaches-general-data-protection_e_fr, www.enforcementtracker.com/#_www.nathantrust.com/gdpr-fines-penalties, en www.helpnetsecurity.com/2019/02/07/gdpr-numbers-january-2019/. De websites geven overigens een verschillend beeld van het aantal boetes, wisselend van in totaal 64 tot 91 boetes. Wij hebben geen exacte data over het aantal boetes dat binnen de EU door privacytoezichthouders is opgelegd. Niet alle boetebesluiten worden overigens gepubliceerd. Het is dan ook de vraag of de gepubliceerde overzichten uitputtend zijn. Voor zover bekend is er nog geen beslissing in bezwaar of beroep van een van de boetebesluiten.

⁶¹ Zie www.welt.de/finanzen/article193326155/DSGVO-Verstoesse-Bundeslaender-ziehen-Bussgeld-Bilanz.html.

⁶² Stand per 30 oktober 2019.

⁶³ Zie noot 6.

⁶⁴ Zie noot 6.

Polen	€ 644 780	Polish National Personal Data Protection Office (UODO)	Morele.net	10 september 2019
Bulgarije	€ 511 000	KZLD	DSK Bank	28 augustus 2019
Nederland	€ 460 000	AP	HagaZiekenhuis	18 juni 2018
Portugal	€ 400 000	CNPD	Hospital	17 juli 2018
Frankrijk	€ 400 000	CNIL	Sergic	28 mei 2019
Spanje	€ 250 000	AEPD	Professional Football League (Laliga)	11 juni 2019
Polen	€ 219 538	UODO	Private company working with data from publicly available sources	26 maart 2019
Noorwegen	€ 203 000	Norwegian Supervisory Authority (Datatilsynet)	Oslo Municipal Education Department	29 april 2019
Denemarken ⁶⁵	€ 200 850	Datatilsynet	ID design A/S	3 juni 2019

III.2 Aard van overtredingen

Op basis van een eerste beoordeling is een zeer globaal inzicht te geven in de aard van de overtredingen.

- De meeste boetes betreffen lid 5-boetes (met een boetemaximum van € 20 miljoen). Een substantieel kleiner deel betreft lid 4-boetes (met een boetemaximum van € 10 miljoen). In een aantal gevallen is sprake van zowel een lid 4-boete als een lid 5-boete.
- Ongeveer de helft van de lid 5-boetes is opgelegd op basis van een overtreding van de algemene beginselen uit artikel 5.⁶⁶ Een derde van de boetes is gebaseerd op overtreding van de rechtmatigheidsgronden uit artikel 6. De overige lid 5-boetes zien met name op informatieverplichtingen (artikel 12, 13 en 14) en het recht op inzage (artikel 15).
- Verreweg de meeste lid 4-boetes zijn opgelegd voor overtreding van de beveiligingsverplichtingen (artikel 32). Daarnaast zijn enkele lid 4-boetes opgelegd wegens overtreding van de bepalingen ten aanzien van *privacy by design* (artikel 25), verwerkersovereenkomsten (artikel 28), de meldplicht datalekken (artikel 33 en 34). Ook zijn twee boetes opgelegd van

wege het ontbreken van een PIA (artikel 35)⁶⁷ en voor het niet aanwijzen van een FG (artikel 37).⁶⁸

III.3 Berekening van de boetes

De verschillende boetebesluiten geven een wisselend beeld over de wijze waarop de hoogte van de boete tot stand is gekomen.

Vooropstaat dat artikel 83 bepaalt dat een boete in elke zaak doeltreffend, evenredig en afschrikwekkend moet zijn. Voor de vaststelling van de hoogte van de boete noemt lid 2 van artikel 83 een aantal omstandigheden waarmee rekening moet worden gehouden. De uitwerking daarvan door de verschillende toezichthouders verschilt. Wij geven hieronder een aantal voorbeelden.

- Op 8 en 9 juli 2019 kondigde de Britse toezichthouder een *'intention to fine'* aan ten aanzien van British Airways en Marriott. Uit de door de ICO gepubliceerde verklaringen is enkel op te maken dat het twee datalekken betrof waarbij respectievelijk 500 000 en 339 miljoen mensen uit verschillende landen betrokken waren. In het laatste geval waren bijvoorbeeld hotelgasten uit 31 verschillende landen van de EER betrokken. Dit leidde ertoe dat de ICO als

⁶⁵ Het rechtssysteem van Denemarken (en Estland) laat de in de AVG beschreven administratieve geldboeten niet toe. De regels over administratieve geldboeten kunnen op een zodanige wijze worden toegepast dat de boete in Denemarken als een strafrechtelijke sanctie door een bevoegd gerecht wordt opgelegd, op voorwaarde dat deze toepassingen van de regels in die lidstaten eenzelfde werking hebben als administratieve geldboeten die door toezichthoudende autoriteiten worden opgelegd. Daarom dienen de bevoegde nationale gerechten rekening te houden met de aanbeveling van de toezichthoudende autoriteit die de boete heeft geïnitieerd (overweging 151 AVG).

⁶⁶ Overigens kunnen overtredingen van meerdere artikelen de grondslag voor de boete vormen.

⁶⁷ Zweden 20 augustus 2019.

⁶⁸ Oostenrijk augustus 2019.

- lead authority* optrad en met verschillende Europese toezichthouders optrok. Beide partijen hebben weliswaar meegewerkt met het onderzoek en verbeteringen doorgevoerd in hun beveiliging, maar dat weerhield de ICO er niet van om ongekend hoge boetes op te leggen. Het ligt voor de hand dat de hoogte van de boetes is bepaald aan de hand van de jaaromzet van beide partijen. British Airways doet het qua omzet net iets beter dan het Marriott en het lijkt erop dat er inderdaad percentages van 1,5 tot mogelijk 4% zijn gehanteerd. Het zal interessant zijn om de uiteindelijke boetebesluiten in te zien. Niet alleen vanwege de vraag of deze monsterboetes daadwerkelijk zijn opgelegd, maar met name of er inderdaad gebruik is gemaakt van een percentage van de jaaromzet en op welke manier deze jaaromzet wordt berekend.
- De Bulgaarse toezichthouder legde een boete op van € 2 600 000 aan de National Revenue Agency. Het betrof een datalek waarbij inzage kon worden verkregen in gegevens van ruim 6 miljoen natuurlijke personen (waaronder bijna 2 miljoen overleden personen).
 - De Litouwse toezichthouder legde een boete van € 61 500 op aan MisterTango, een Litouws fintech-bedrijf voor overtreding van artikel 5 en een datalek. Bij het bepalen van het bedrag van de boete heeft de Litouwse toezichthouder onder meer rekening gehouden met het feit dat er op niet-transparante wijze gegevens werden verwerkt, dat het bedrijf in grotere mate en langer dan nodig gegevens heeft verwerkt om het doel te bereiken, dat er systematisch sprake was van een onrechtmatige verwerking, dat er sprake was van onvoldoende beveiliging op het moment van het lek, dat het lek niet werd gemeld, en dat de gegevens onder het bankgeheim vielen en werden verwerkt zonder encryptie en toegangscontrole. Uit het persbericht blijkt verder dat de jaarlijkse wereldwijde omzet van de onderneming in aanmerking is genomen bij het opleggen van de administratieve boete.
 - Een van de Duitse toezichthouders (Baden-Württemberg) die een boete oplegde aan het Duitse media-platform Knuddels.de liet bij de hoogte van de boete onder meer de ‘zeer goede samenwerking’ met de toezichthouder, de ‘voorbeeldige transparantie’ van het bedrijf en het feit dat de kosten (inclusief de beveiligingsmaatregelen die het bedrijf heeft moeten nemen) inmiddels een getal met 6 cijfers besloeg meewegen. De boete kwam uit op € 20 000.
 - Door de Zweedse toezichthouder werd in het onderzoek naar het gebruik van facial-recognition-camera’s door een school bij de hoogte van de boete rekening gehouden met het feit dat er meerdere artikelen uit de AVG waren geschonden, het feit dat het gevoelige persoonsgegevens betrof over kinderen die een afhankelijkheidspositie hebben ten opzichte van het bestuur van de school en opzettelijk gebruik is gemaakt van gezichtsherkenning. Ook is rekening gehouden met het feit dat de verwerking via informatie in de media bij de toezichthouder is gekomen. Als verzachtende omstandigheid speelde evenwel mee dat de pilot slechts drie weken aan de gang was en 22 studenten omvatte. Dit leidde uiteindelijk tot een beperkte boete van zo’n € 18 000. Daarbij speelde een rol dat het een overheidsinstantie betrof en in Zweden de hoogte van boetes die kan worden opgelegd aan overheidsinstanties is beperkt tot € 500 000 (voor lid 4-boetes) en € 1 000 000 (voor lid 5-boetes).⁶⁹ Het is aannemelijk dat de boete substantieel hoger zou zijn als het geen overheidsinstantie betrof.
 - De Franse toezichthouder CNIL legde begin januari 2019 Google een boete op van € 50 miljoen wegens een gebrek aan transparantie en het ontbreken van een wettelijke basis voor verwerking ten behoeve van gepersonaliseerde reclame. De CNIL concludeert in haar besluit⁷⁰ (dat wel integraal is gepubliceerd) kortweg dat onder meer vanwege de omvang van de gegevensverwerking, het aantal betrokkenen (Google had destijds 27 miljoen gebruikers in Frankrijk), de voortdurende schendingen en het bedrijfsmodel van Google (met name de plaats van gegevensverwerking voor reclamadoeleinden) volgt dat een boete van € 50 miljoen gerechtvaardigd is. Hoewel er wel gehint wordt op de mogelijkheid van de berekening op basis van een percentage van 4% van de jaaromzet, motiveert de CNIL de boetehoogte verder niet. De CNIL merkt in het feitenrelaas wel op dat de omzet van Google LLC, een 100%-dochteronderneming van ALPHABET, in 2017 € 96 miljard bedroeg en dat de Franse vestiging ongeveer € 325 miljoen omzette. De omzet in combinatie met een mogelijke boete van 4% valt daarmee niet te rijmen (de boete zou dan immers hoger moeten uitvallen). We kunnen hier evenmin uit afleiden of de CNIL de boete heeft gebaseerd op de omzet van Google LLC of van de Franse vestiging van Google. Google is in beroep gegaan tegen het boetebesluit bij de Conseil d’Etat. Het is te hopen dat de Conseil d’Etat meer openheid zal geven over de bepaling van de hoogte van de boete. Andere boetebesluiten van de CNIL geven op dit punt overigens ook niet meer duidelijkheid: vastgoedbedrijf Sergic kreeg een boete van € 400 000, terwijl de geschatte omzet € 43 miljoen was.⁷¹
 - Ten slotte wordt in een Hongaars boetebesluit rekening gehouden met de toekomstige jaaromzet van

69 Op grond van de Zweedse uitvoeringswet Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

70 www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1.

71 Commission Nationale de l’Informatique et des Libertés, Délibération n°SAN-2019-005 du 28 mai 2019.

de beboete partij ter beoordeling van proportionaliteit van de hoogte van de boete.⁷² Het betrof een boete aan een politieke partij voor het niet melden van een datalek aan de autoriteit en de betrokkenen en voor het onvoldoende documenteren van alle datalekken (artikel 33 lid 5). De hoogte van de boete (ongeveer € 34 000) werd proportioneel geacht gezien de omzet van het afgelopen jaar (ruim € 800 000) én – opmerkelijk genoeg – de verwachte omzet voor het komende jaar (ruim € 1 260 000). Dat laatste zou bij de beoordeling van de hoogte van de boete geen rol moeten spelen.

IV Bevindingen

Weliswaar is het nog erg vroeg om op basis van het globale onderzoek specifieke en valide conclusies te trekken uit de boetes die Europese toezichthouders hebben opgelegd, niettemin valt een aantal zaken op.

Er is sinds de AVG van toepassing is actief toezicht gehouden op de naleving daarvan door de Europese toezichthouders. Het nieuwe handavingsinstrument, de bestuurlijke boete, is daarbij in 21 van de (nu nog) 28 lidstaten van de EU en Noorwegen ingezet. Alleen de toezichthouders in Estland, Finland, Ierland, Kroatië, Luxemburg, Slovenië en Slowakije legden voor zover bekend nog geen boete op. Met name Ierland is in dit rijtje het meest opvallend: in Ierland is een groot aantal ‘techreuzen’ gevestigd en men zou verwachten dat de Ierse toezichthouder voorloper zou zijn in handavingsmaatregelen. De Ierse *Data Protection Commissioner* Helen Dixon heeft overigens wel aangekondigd dat de eerste boetebesluiten in concept gereed zijn, en na feedback van de betrokken partijen en nationale toezichthouders zullen worden gepubliceerd.

De meeste boetes zijn opgelegd wegens overtreding van de algemene beginselen en rechtmatigheid van de verwerking en de beveiliging van persoonsgegevens. Bij meerdere overtredingen is niet duidelijk waarom de toezichthouder de ene overtreding wel verder onderzoekt en beboet, en de andere zonder nadere motivering laat rusten.

De hoogte van de boetes die zijn opgelegd door de toezichthouders loopt sterk uiteen. Ten dele is dit te verklaren omdat de boetes zijn opgelegd aan overheidsinstanties of natuurlijke personen, maar voor een groot deel lijkt dit te worden veroorzaakt doordat de boetes in de bepalingen in de AVG redelijk abstract zijn geformuleerd en er verder geen houvast wordt gegeven voor de berekening. Ook de richtsnoeren van de EDPB bevatten geen aanknopingspunten voor de concrete berekening van de boetes.

Weliswaar heeft de AP zelf boetebeleidsregels opgesteld, maar ook de toepassing daarvan leidt – op basis van de twee gepubliceerde boetebesluiten van de AP, waarvan één op basis van de geldende beleidsregels – tot

onvoorspelbare uitkomsten. In die zin hebben de boetebeleidsregels vooralsnog niet tot meer rechtszekerheid voor overtreders geleid.

Uit de boetebesluiten blijkt dat de jaaromzet van de beboete onderneming veelal wordt meegewogen bij de berekening van de boete. De wijze waarop verschilt per boetebesluit en is niet altijd transparant. In een enkel geval is de hoogte van de boete – overigens zonder duidelijke toelichting – gebaseerd op een percentage van de omzet.

Het verlenen van medewerking aan het onderzoek van de toezichthouder lijkt geen boete verlagend effect te hebben, maar substantiële investeringen door de overtreder in het spoedig oplossen van de overtreding kunnen dat wel hebben. Bovendien kan daar in Nederland mee worden voorkomen dat naast een boete een last onder dwangsom wordt opgelegd.

Over het één-loketmechanisme zal nog de nodige discussie worden gevoerd. Waar de Britse toezichthouder ICO het mechanisme in het Marriott-boetebesluit wel lijkt te hebben toegepast, zet de Franse toezichthouder CNIL het mechanisme in het Google besluit opzij.

Bij al deze bevindingen plaatsen wij de kanttekening dat tegen diverse boetebesluiten bezwaar of beroep is ingesteld, en het laatste woord over zowel de onderbouwing van de boete als de hoogte ervan nog niet is gesproken. Het moge duidelijk zijn dat vooralsnog geen sprake is van de zo gewenste consequente handhaving en dat aan het doel van een geharmoniseerde gegevensbeschermingsregeling in de Europese Unie nog hard moet worden gewerkt.

⁷² Boete van de Hongaarse toezichthouder Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) van 5 april 2019. Zie www.naih.hu/files/NAIH-2019-2668-hatarozat.pdf.