

95. De Digitale Werkwijze van ACM langs de lat van de Algemene Verordening Gegevensbescherming (AVG)

MR. S.M. DIELEMANS-GOOSSENS EN MR. M.R. BANEKE

Bij de bedrijfsbezoeken die ACM aflegt, maakt zij veelvuldig gebruik van de bevoegdheid om inzage te vorderen in en kopieën te maken van digitale gegevens. Daarbij handelt ACM volgens de door haar vastgestelde Digitale Werkwijze. Omdat bij de onderzoeken van ACM mogelijk ook privé-gegevens worden ingezien, is de Digitale Werkwijze is al meerde malen voorgelegd aan de rechter met de vraag of deze zich wel verdraagt met het in artikel 8 EVRM neergelegde recht op privacy. Tot nu toe heeft de Digitale Werkwijze deze toets bij de Nederlandse rechter doorstaan. In dit artikel wordt beoordeeld of de Digitale Werkwijze ook stand kan houden als deze wordt getoetst tegen het nieuwe, aangescherpte privacy-kader dat is vastgelegd in de Algemene Verordening Gegevensbescherming (AVG) en dat vanaf 25 mei 2018 van toepassing is. De auteurs menen dat dit niet het geval is en doen in het artikel enkele suggesties voor het 'AVG-proofoen' van de onderzoekspraktijk van ACM.

1. Inleiding

Bij de bedrijfsbezoeken die ACM aflegt, maakt zij veelvuldig gebruik van de bevoegdheid om inzage te vorderen in en kopieën te maken van digitale gegevens. Bij het veiligstellen van de digitale gegevens handelt ACM volgens de door haar vastgestelde Digitale Werkwijze.¹ Omdat bij de onderzoeken van ACM mogelijk ook privé-gegevens (d.w.z. niet-zakelijke bestanden in de zin van artikel 5:17, eerste lid, van de Algemene wet bestuursrecht (Awb)) worden ingezien, is de Digitale Werkwijze is al meerde malen voorgelegd aan de rechter met de vraag of deze zich wel verdraagt met het in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) neergelegde recht op privacy. Inbreuken op dit recht zijn uitsluitend toegestaan voor zover daarin bij wet is voorzien en de inbreuk noodzakelijk en proportioneel is. Tot nu toe heeft de Digitale Werkwijze deze toets bij de Nederlandse rechter doorstaan, meest recent nog in een uitspraak van de voorzieningenrechter van de rechtbank Den Haag van 22 november 2017.² Op het gebied van privacy staat er echter een grote verandering op stapel die maar weinig mensen zal zijn ontgaan: per 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming

(AVG)³ rechtstreeks van toepassing in alle lidstaten. Met de AVG ligt er een aangescherpt privacy-kader waar alle Europese organisaties – ook ACM – vanaf 25 mei 2018 aan moeten voldoen. Voor de weinige ruimte die de AVG biedt voor nadere invulling op nationaal niveau, wordt in Nederland de Uitvoeringswet AVG (UAVG) vastgesteld.⁴ Het wetsvoorstel voor de UAVG is op 12 december 2017 aan de Tweede Kamer gezonden.⁵ Deze ontwikkelingen leiden tot de vraag of de privacy-toetsing van de Digitale Werkwijze aan de AVG anders uitvalt dan de toetsing zoals die tot op heden heeft plaatsgevonden aan artikel 8 EVRM. Wij menen dat dit het geval is en dat de AVG aanpassingen van de Digitale Werkwijze noodzakelijk maakt. In dit artikel beoordelen wij welke bepalingen van de Digitale Werkwijze waarschijnlijk zullen sneuvelen. Ook doen wij enkele suggesties voor het 'AVG-proofoen' van de onderzoekspraktijk van ACM. Wij beginnen echter met een korte beschrijving van de Digitale Werkwijze.

2. Digitale Werkwijze

Het mag geen verbazing heten dat de digitale dossiers en correspondentie van ondernemingen tegenwoordig

1 ACM Werkwijze voor onderzoek in digitale gegevens 2014, Strc. 2014, 3991.
2 ECLI:NL:RBDHA:2017:14150. Zie voor een uitvoerige beschouwing van de toetsing van de praktijk van de bedrijfsbezoeken van ACM aan de artikelen 6 en 8 EVRM ook H.M.H. Speyart, 'Binnen/buiten de reikwijdte discussie en effectieve rechtsbescherming', MP 2017/5, nr. 251.

3 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, PbEU 2016, L119.
4 Bij het van toepassing worden van de AVG en de UAVG vervangen deze de huidige Nederlandse privacyregelgeving, die is neergelegd in de Wet bescherming persoonsgegevens (Wbp).
5 Kamerstukken II, 2017/18, 34 581, nr. 2.

een centrale plek innemen in de onderzoeken van ACM. ACM verzamelt tijdens bedrijfsbezoeken dan ook enorme hoeveelheden digitale bestanden, door forensische kopieën van bestandsmappen en mailboxen te maken en deze veilig te stellen. Hoewel ACM enige richting aanbrengt bij het inzien en veiligstellen van digitale bestanden tijdens een bedrijfsbezoek, is het uiteraard onvermijdelijk dat het integraal kopiëren van complete mailboxen en bestandsmappen gepaard gaat met de nodige "bijvangst" in de vorm van bestanden die niet in het onderzoeksdossier van ACM thuishoren. Meer specifiek gaat het dan om bestanden die buiten de reikwijdte van het onderzoek vallen, privébestanden en geprivilegieerde correspondentie tussen de onderneming en haar advocaat. De Digitale Werkwijze en de daaraan gekoppelde Werkwijze Privilege bevatten een aantal waarborgen voor het doen van digitaal onderzoek door ACM, en het volgen van de daarin vervatte procedures zou moeten resulteren in een dataset die door ACM voor haar onderzoek kan worden gebruikt.⁶ Hieronder volgt een zeer beknopte uiteenzetting van de procedures voor het verzamelen van digitale bestanden die volgen uit de Digitale Werkwijze en de Werkwijze Privilege en de onderzoekspraktijk van ACM.

De eerste stap in het digitaal onderzoek van ACM, die is neergelegd in artikel 2.1 Digitale Werkwijze, bestaat uiteraard uit het inzien, selecteren en veiligstellen van de bestanden tijdens het bedrijfsbezoek. Zoals hierboven al is opgemerkt gebeurt dit niet op basis van volstrekte willekeur, maar richt ACM zich op het doel en voorwerp van het onderzoek. Indien één of meer personen het uitgangspunt vormen bij de selectie van digitale bestanden, bijvoorbeeld wanneer de mailbox van bepaalde werknemers van de onderneming wordt gekopieerd, dan dient de betrokkenheid van deze personen bij de inbreuk die het doel en voorwerp van het onderzoek vormt te worden vermoed. De verzameling bestanden die tijdens het bedrijfsbezoek wordt veiliggesteld wordt in de Digitale Werkwijze aangeduid als de 'veiliggestelde dataset'. De onderneming krijgt van ACM een overzicht van de gegevens op de veiliggestelde dataset met bijbehorende hashwaarden.⁷

De tweede stap (zie artikel 2.2 Digitale Werkwijze) bestaat uit het bewerken van de veiliggestelde dataset met zoek-

vragen om een dataset vast te stellen met documenten die binnen het doel van het onderzoek vallen, de 'binnen-de-reikwijdte dataset'. Alleen de bestanden die een hit opleveren bij het invoeren van deze zoektermen worden in deze binnen-de-reikwijdte dataset opgenomen. Volgens ACM vallen al deze bestanden hoe dan ook binnen de reikwijdte van haar onderzoek. Hoewel ACM daartoe in de praktijk wel regelmatig bereid blijkt, is een verdere discussie met ACM over het binnen of buiten de reikwijdte vallen van bepaalde bestanden dan ook geen vaststaand onderdeel van deze procedure.⁸ Opmerkelijk is overigens dat de Nederlandse Zorgautoriteit (de NZa) die visie niet deelt. Dat zou althans kunnen worden opgemaakt uit het feit dat, nadat een door de NZa veiliggestelde dataset met zoekwoorden zijn bewerkt, de betrokken onderneming de mogelijkheid heeft om bestanden in die bewerkte dataset niet alleen als privé of geprivilegieerd, maar ook als out of scope te claimen.

Nadat de binnen-de-reikwijdte dataset is vastgesteld, vindt nog één bewerkingsslag plaats om tot de "onderzoeksdataset" te komen. Deze stap bestaat eruit dat de betrokken onderneming de binnen-de-reikwijdte dataset doorzoekt met behulp van een softwareprogramma waarin bestanden als privé of geprivilegieerd kunnen worden geclaimd. Deze claims worden vervolgens beoordeeld door de toezichthoudend ambtenaar waar het om beweerde privébestanden gaat (artikel 2.3 van de Digitale Werkwijze) en door een speciale ACM-ambtenaar, de functionaris verschoningsrecht waar het om beweerde geprivilegieerde gegevens gaat (artikel 2.4 Digitale Werkwijze en de Werkwijze Privilege). Gegevens die uiteindelijk in de onderzoeksdataset komen kunnen door ACM worden toegevoegd aan het onderzoeksdossier (artikel 2.5 Digitale Werkwijze), en kunnen tevens worden hergebruikt voor andere onderzoeken van ACM of aan derden worden verstrekt (artikel 2.6, eerste lid, Digitale Werkwijze). Overige gegevens uit de veiliggestelde dataset worden niet hergebruikt of aan derden verstrekt (artikel 2.6, tweede lid, Digitale Werkwijze). De Digitale Werkwijze beschrijft niet met welke reden en onder welke voorwaarden gegevens uit de onderzoeksdataset aan derden mogen worden verstrekt of aan welke derden deze gegevens mogen worden verstrekt. De Digitale Werkwijze vermeldt uitsluitend dat hiervan een verslag wordt gemaakt (artikel 2.6, derde lid, Digitale werkwijze). Een nadere invulling kan echter worden gevonden in artikel 7 lid 3 van de Instellingswet ACM waaruit blijkt dat ACM gegevens die zij verkrijgt bij de uitvoering van haar wettelijke taken alleen deelt met degene van wie zij die gegevens heeft verkregen en binnen en buitenlandse toezichthouders.

ACM vernietigt de digitale gegevens die zij verzamelt nadat het betreffende onderzoek is afgelopen, met uitzondering van de gegevens in het onderzoeksdossier (artikel 2.6, vierde en vijfde lid, Digitale Werkwijze).

6 Het is overigens maar zeer de vraag of de waarborgen die door de Werkwijze 2014 worden geboden voldoende effectief zijn, gelet op met name het proportionaliteitsbeginsel, dat is neergelegd in artikel 5:13 Awb, en de eisen die aan onderzoeken van toezichthouders worden gesteld door artikel 8 van het Europees Verdrag van de Rechten van de Mens en de rechtspraak van het Europees Hof voor de Rechten van de Mens. Die vraag komt in deze bijdrage echter niet aan de orde. Zie daarvoor Speyart, noot 2, en F. ten Have, Digitale bewijsvergaring door de ACM: herleving van het 'buiten de reikwijdte'-argument, Markt & Mededinging 2017(4). Beide artikelen zijn geschreven naar aanleiding van de uitspraak van de voorzieningenrechter van de Rechtbank Den Haag van 12 juli 2017 in de zaak X/ACM (ECLI:NL:RBDHA:2017:7968).

7 Een hashwaarde is de uitkomst van een wiskundige berekening over de inhoud van het bestand. De hashwaarde van een bestand is altijd uniek en zal na bewerking van het bestand veranderen. Zo kan altijd worden vastgesteld dat aan het bestand iets is gewijzigd, zelfs als dat met het blote oog niet is waar te nemen.

8 Deze redenering van ACM heeft geen stand gehouden in de zaak X/ACM. Zie meer uitgebreid Speyart, noot 2, en Ten Have, noot 6. Het is de vraag hoe ACM met de uitspraak van de voorzieningenrechter zal omgaan.

3. AVG

De AVG bevat regels die natuurlijke personen moeten beschermen bij de verwerking van hun persoonsgegevens. Alle informatie die herleid kan worden naar geïdentificeerde of een (met redelijke middelen) identificeerbaar natuurlijk persoon, is een persoonsgegeven.⁹ Daarbij kan het gaan om voor de hand liggende gegevens als NAW-gegevens en BSN-nummers, maar ook gegevens als e-mailadressen, telefoonnummers, belgegevens, locatiegegevens, IP-adressen, salarisgegevens, kentekens en reisgegevens kunnen – afhankelijk van de context – kwalificeren als persoonsgegevens. De regels van de AVG gelden voor alle verwerkingen van die persoonsgegevens. Van verwerking is snel sprake, aangezien dit begrip zeer ruim is gedefinieerd in de AVG. Uit artikel 4, onder (2), AVG volgt dat het daarbij gaat om verwerking *“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”*.

De verplichtingen van de AVG rusten in hoofdzaak op de ‘verwerkingsverantwoordelijke’. Een term die – praktisch weergegeven – duidt op degene die vaststelt dat hij de betreffende persoonsgegevens gaat verwerken en voor welke doelen en met welke middelen hij dat gaat doen.

Alle ondernemingen in Nederland raken langzaam maar zeker doordrongen van de – soms vergaande – verplichtingen die de AVG stelt aan hun verwerkingen van persoonsgegevens. Dat stuit hier en daar op onbegrip, met name waar het organisaties betreft waarbij het verwerken van data niet centraal staat in hun bedrijfsvoering (anders dan bijvoorbeeld bij tech- of telecombedrijven). Geen enkele organisatie lijkt echter te ontkomen aan de toepasselijkheid van de AVG en de daaraan verbonden eisen. Nagenoeg ieder bedrijf verwerkt namelijk al persoonsgegevens in het kader van HR aspecten (zoals werknemers- en salarisadministratie) en de administratie van contactpersonen. Ook overheidsinstanties behoren uitdrukkelijk tot de werkingssfeer van de AVG.¹⁰ Wat exact overheidsinstanties zijn, moet worden bepaald aan de hand van nationaal recht. In Nederland zal worden aangesloten bij artikel 1:1 Awb en gaat het dus om alle organen van rechtspersonen die krachtens

publiekrecht zijn ingesteld en andere organen of colleges die met enig openbaar gezag zijn bekleed.

De AVG stelt strikte eisen aan de verwerking van persoonsgegevens. Zo moet daarbij een aantal beginselen in acht worden genomen, waaronder die van:

- rechtmatige, behoorlijke en transparante verwerking;
- verzameling en verwerking voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden;
- minimale gegevensverwerking (beperkt tot dat wat noodzakelijk is);
- opslagbeperking; en
- beveiliging.¹¹

Om rechtmatig te kunnen zijn, moet er altijd sprake zijn van een grondslag voor de verwerking van persoonsgegevens. De mogelijke grondslagen zijn limitatief opgesomd in artikel 6 AVG, en omvatten onder meer toestemming van de betrokken persoon en de uitvoering van een overeenkomst met die persoon. Voor de verwerking van persoonsgegevens door overheidsinstanties als de ACM zullen met name de grondslagen ‘noodzakelijk om te voldoen aan een wettelijke verplichting’ en ‘noodzakelijk voor de vervulling van een taak van algemeen belang’ relevant zijn. ACM heeft immers wettelijke toezichtstaken en heeft bij de uitvoering van die taken op grond van artikel 5:17 Awb de bevoegdheid om inzage te vorderen in zakelijke gegevens.

Daarbij ontstaat de situatie dat de Autoriteit Persoonsgegevens (AP) als toezichthouder het optreden van ACM kan toetsen aan de AVG en de UAVG

Onder de AVG is het voor een aantal organisaties waaronder ook overheidsinstanties als ACM verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen die betrokken moet worden bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De FG informeert en adviseert over de verplichtingen onder de AVG en ziet toe op de naleving daarvan

4. ACM en de AGV

ACM valt als overheidsinstantie binnen de werkingssfeer van de AVG en zal vanaf 25 mei 2018 in overeenstemming met de AVG moeten handelen daar waar ACM persoonsgegevens verwerkt. Daarbij ontstaat de situatie dat de Autori-

⁹ Artikel 4, onder (1), AVG.

¹⁰ In artikel 4, onder (7) AVG worden overheidsinstanties uitdrukkelijk genoemd als verwerkingsverantwoordelijke. Wel worden in artikel 2 AVG verwerkingen *“door bevoegde autoriteiten met het oog op 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”* uitgesloten van de werkingssfeer van de AVG. Voor deze verwerkingen komt een separaat kader met de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn (EU) 2016/680, PbEU 2016, L119) die in Nederland in een separaat wetsvoorstel zal worden geïmplementeerd. Hoewel ACM punitieve sancties kan opleggen is zij een bestuursrechtelijke toezichthouder en valt zij daarmee niet binnen het separate, strafrechtelijke kader, maar binnen de werkingssfeer van de AVG.

¹¹ Artikel 5 AVG.

teit Persoonsgegevens (AP) als toezichthouder het optreden van ACM kan toetsen aan de AVG en de UAVG.¹²

Wanneer ACM op grond van artikel 5:17 Awb inzage vordert in zakelijke gegevens, waarbij ook persoonlijke gegevens worden gekopieerd (en dus verwerkt in de zin van de AGV) is dat 'noodzakelijk om te voldoen aan een wettelijke verplichting' en is dat 'noodzakelijk voor de vervulling van een taak van algemeen belang', omdat ACM wettelijke toezichtstaken heeft.

Het is evident dat ACM bij de onderzoeken waarbij volgens de Digitale Werkwijze wordt gewerkt ook (al dan niet zakelijke) persoonsgegevens verwerkt. Daarbij gaat het om de persoonsgegevens van de personen op wie het onderzoek zich mede richt, waaronder mogelijk ook hun volledige e-mailmappen en/of de data gegenereerd met hun telefoon, maar ook om de persoonsgegevens van alle mogelijke derden die voorkomen in de bestanden die ACM digitaal doorzoekt, zoals de gegevens van de personen die e-mails hebben verzonden aan de persoon die onderdeel uitmaakt van het onderzoek.

Dit maakt onder meer dat ACM steeds een grondslag moet hebben voor het kopiëren en doorzoeken van de gegevens, dat haar verwerkingen proportioneel moeten zijn, dat de gegevens goed moeten worden beveiligd en dat moet worden gewerkt met zo kort mogelijke bewaartermijnen. Dit zijn onderwerpen waarmee op dit moment in Digitale de werkwijze weinig tot geen rekening mee wordt gehouden. ACM meet zich met de Digitale Werkwijze een ruime vrijheid aan bij het invullen van de bevoegdheid die zij uit hoofde van artikel 5:17 Awb heeft om inlichtingen te vorderen. Vrijheden die in schril contrast lijken te staan tot de verregaande bescherming van de privacy van natuurlijke personen in de AVG, die onder meer tot uitdrukking komt in de beginselen van (i) rechtmatige en transparante gegevensverwerking, (ii) minimale gegevensverwerking (niet meer gegevens verwerken dan strikt noodzakelijk), (iii) doelbinding (uitsluitend verwerken voor het doel waarvoor de gegevens zijn verzameld) en (iv) opslagbeperking (niet langer in een herleidbare vorm bewaren dan noodzakelijk) alsmede in de rechten van de betrokken personen op onder meer informatie over de verwerking van en inzage in de gegevens die van hen worden verwerkt.

Nu zijn de bescherming die de AVG biedt aan de betrokken personen en de verplichtingen die de AVG oplegt aan de verwerkingsverantwoordelijken niet absoluut. Op grond van artikel 23 AVG zijn beperkingen mogelijk van de rech-

ten en gelden ook de beginselen van artikel 5 AVG en de meldplicht bij datalekken van artikel 34 AVG¹³ (die we in Nederland al sinds 1 januari 2016 kennen op grond van artikel 34a Wbp) niet onverkort in onder meer situaties waar toezichtstaken in het algemeen belang worden uitgevoerd. Ook in de UAVG wordt aandacht besteed aan deze uitzondering. Zo is te lezen in de Memorie van Toelichting bij de UAVG¹⁴:

"Voorop staat dat het recht op bescherming van persoonsgegevens nimmer absoluut kan worden geformuleerd. Een samenleving kan niet functioneren wanneer niet onder bepaalde omstandigheden kan worden afgeweken van dit recht. Dit is een belangrijke achterliggende ratio van artikel 23 van de verordening. Tegelijkertijd zijn de in de verordening opgenomen rechten van de betrokkene en verplichting tot melding van een inbreuk belangrijke waarborgen voor bescherming van de persoonlijke levenssfeer, waarvan niet dan indien dit noodzakelijk is mag worden afgeweken."

Het is goed voorstelbaar dat voor het uitoefenen van bevoegdheden door toezichthouders als de ACM een dergelijke beperking van rechten en verplichtingen gerechtvaardigd kan zijn, maar daarvoor moet wel aan een aantal voorwaarden worden voldaan.

Wettelijke grondslag

Op grond van artikel 23 AVG moet voor afwijkingen onder die bepaling sprake zijn van een nationale wettelijke regeling waarbij de rechten en verplichtingen worden beperkt. Ook moet die regeling noodzakelijk zijn en mag deze niet verder gaan dan nodig voor het beoogde doel. In artikel 41 UAVG wordt meer ruimte geboden en krijgt de verwerkingsverantwoordelijke ook de mogelijkheid om zelf te beoordelen of in sommige gevallen een beperking van de rechten en verplichtingen gerechtvaardigd is. Dit is volgens de wetgever nodig in aanvulling op sectorspecifieke wettelijke regeling waarin in beperkingen wordt voorzien:

"Sectorspecifieke bepalingen zijn alleen mogelijk in een situatie waarin voorzienbaar is in welke situatie afwijking noodzakelijk is. Vaak is echter in hoge mate onvoorzienbaar in welke gevallen, en ten aanzien van welke gegevens het noodzakelijk is om af te wijken van de rechten van betrokkene. Hierom is het noodzakelijk om een generieke regeling op te nemen in de Uitvoeringswet, die ruimte biedt aan de praktijk om in de toekomst hierin een belangenafweging te maken. (...) De vraag of in het concrete geval een uitzondering gerechtvaardigd is, zal door de verwerkingsverantwoordelijke zelf moeten worden afgewogen op grond van artikel 41 van de Uitvoeringswet.¹⁵"

12 Uit artikel 55 AVG volgt dat wanneer overheidsinstanties persoonsgegevens verwerken in het kader van de vervulling van een taak van algemeen belang of om te voldoen aan een wettelijke verplichting van de nationale toezichthouder (de AP) altijd competent is, dit in afwijking van artikel 56 op grond waarvan bij grensoverschrijdende verwerkingen ook toezichthouders van andere lidstaten competent kunnen zijn. Voor verwerkingen van persoonsgegevens door gerechten is overigens uitdrukkelijk opgenomen in artikel 55, derde lid, AVG dat de toezichthouders juist niet competent zijn. Dit om de onafhankelijkheid bij de uitoefening van rechterlijke taken te borgen. De gerechten zijn wel onderworpen aan de AVG, maar het toezicht op de naleving moet worden toevertrouwd aan een specifieke instantie binnen de rechterlijke organisatie.

13 Deze meldplicht is voor Nederland niet nieuw en kennen sinds 1 januari 2016 al op grond van artikel 34a Wbp

14 *Kamerstukken II*, 2017/18, 34 581, nr. 3, p. 40.

15 MvT UAVG, p. 40.

Men zou kunnen denken dat we op deze manier – met een eigen afweging van ACM of de inperking van de rechten en verplichtingen noodzakelijk en proportioneel is – weer uitkomen bij de artikel 8 EVRM toets die de Digitale Werkwijze al meerdere malen heeft doorstaan.¹⁶ Maar er lijkt wel degelijk sprake van cruciale verschillen die maken dat de toets aan de AVG anders zal uitvallen. Zo is uiteraard nog niet getoetst of het beperken van alle nieuwe concrete rechten en verplichtingen die in de AVG zijn opgenomen wel noodzakelijk en proportioneel is. Daarnaast kunnen die rechten en verplichtingen onder het systeem van de AVG en de UAVG straks alleen met een categorale regeling worden beperkt, als deze de vorm heeft van een wettelijke regeling. De Digitale Werkwijze omvat wel een categorische beperking¹⁷, terwijl het géén wettelijke regeling is. Alleen al daarom kan de Digitale Werkwijze geen stand houden onder de AVG.

Wettelijke basis of toetsing per individueel geval

Er zijn twee mogelijkheden: ofwel de Digitale Werkwijze wordt vervangen door een wettelijke regeling, ofwel de ACM toetst – op grond van artikel 41 UAVG – *per individueel geval* of een beperking van de rechten en verplichtingen uit de AVG in dat geval gerechtvaardigd is. Dat het bij de afweging van de verwerkingsverantwoordelijke onder artikel 41 UAVG gaat om een vangnet voor individuele gevallen¹⁸ waarin dat incidenteel noodzakelijk is en dat daarop geen categorische beperkingen kunnen worden gebaseerd volgt duidelijk uit de memorie van toelichting bij de UAVG:

"De bepaling biedt dus een mogelijkheid om alleen in individuele zaken af te wijken van de rechten die gelden op grond van de verordening, indien dit strikt noodzakelijk is met het oog op de in artikel 23 van de verordening genoemde belangen. Een categorische beperking van de rechten van betrokkene kan, wanneer dit noodzakelijk en evenredig is in een democratische samenleving, daarentegen niet op artikel 41 worden gebaseerd maar alleen eventueel in sectorspecifieke wetgeving worden opgenomen".¹⁹

Dit geldt uitdrukkelijk ook voor toezichthouders:

"Ook toezichthouders die persoonsgegevens verzamelen in het kader van bestuursrechtelijk toezicht zullen in concrete gevallen een afweging moeten maken of in voorkomende gevallen afgeweken zal moeten worden van de rechten van betrokkene bij verwerking van persoonsgegevens".²⁰

Daarmee lijkt de conclusie gerechtvaardigd dat de Digitale Werkwijze volledig moet wijken bij het van toepassing worden van de AVG

Daarmee lijkt de conclusie gerechtvaardigd dat de Digitale Werkwijze volledig moet wijken bij het van toepassing worden van de AVG, althans dat deze in een wettelijke regeling moet worden vervat. In dat laatste geval lijkt een summier wettelijke basis, met ruimte voor een eigen – daarop gebaseerd – beleid van ACM niet voldoende. De wettelijke regeling moet zodanig zijn vormgegeven dat deze de verwerkingsverantwoordelijke (in dit geval ACM) geen ruimte meer laat om afwegingen per individueel geval te maken, zodat de beperkingen voor de betrokken natuurlijke personen ook voorzienbaar zijn.²¹

Als niet wordt voorzien in een wettelijke regeling, zal ACM per geval steeds moeten beoordelen welke beperkingen gerechtvaardigd, noodzakelijk en proportioneel zijn. Als betrokken personen het niet eens zijn met die afweging, zouden zij zich tot de AP kunnen wenden met een klacht of een verzoek om handhaving. Dit maakt de vraag gerechtvaardigd of de elementen van de huidige Digitale Werkwijze en de vrijheid die ACM zich aanmeet bij het bewaren, doorgeven en verder verwerken van de gegevens straks nog kunnen worden gehandhaafd.

5. Digitale werkwijze en de AVG

Hoewel steeds van geval tot geval zal moeten worden beoordeeld, menen wij dat de volgende elementen van de Digitale Werkwijze de grootste kans lopen geen stand te kunnen houden:

Grondslag en reikwijdte dataset

Meest in het oog springend is de vraag of ACM wel een grondslag heeft voor alle data die zij kopieert. Onder arti-

16 Zie ook MvT UAVG p. 40: "Gelet op het belang van de rechten van betrokkene, de meldplicht en de beginselen dienen verwerkingsverantwoordelijken alleen van de bevoegdheid om af te wijken gebruik te maken indien dit strikt noodzakelijk is en op proportionele wijze gebeurt. Net als onder artikel 43 van de Wbp geldt voor de toepasselijkheid van deze gronden dus een strikt noodzakelijkheids criterium (vergelijk artikel 8, tweede lid, van het EVRM en artikel 52, eerste lid, van het Handvest)".

17 Dit aangezien sprake is van forse (standaard)beperkingen van de privacy-rechten van betrokken personen door onder meer de ruime bewaartermijnen, de onbeperkte mogelijkheid tot doorgifte van de gegevens aan derde partijen, het standaard verwerken van grote hoeveelheden data en niet informeren van personen wiens gegevens via de persoon op wie het onderzoek zich richt betrokken raken.

18 Wij gaan er daarbij van uit dat de UAVG met 'individuele gevallen' het oog heeft op individuele onderzoeken, en dat niet per individueel persoon wiens gegevens betrokken zijn bij het onderzoek deze afweging moet worden gemaakt. Deze laatste benadering lijkt praktisch onwerkbaar.

19 MvT UAVG, p. 41.

20 MvT UAVG, p. 41.

21 Zie in dit verband ook MvT UAVG, p. 40: "Een voorbeeld van een sectorspecifieke regeling is te vinden in de Wet BRP, die een eigen systematiek kent voor beperking van de rechten van betrokkene. Deze beperkingen worden dwingend voorgeschreven, waardoor de verwerkingsverantwoordelijke hierin zelf geen afweging hoeft te maken, of zelfs mag maken, voor ieder individueel geval. Deze beperkingen zijn hiermee voorzienbaar voor de betrokkene. Een ander voorbeeld van deze categorische afwijking is het huidige artikel 34a, negende en elfde lid, van de Wbp, waarin een aantal specifieke uitzonderingen voor de meldplicht bij een inbreuk op de beveiliging zijn opgenomen. Ook dit is een structurele, categorische afwijking van de hoofdregel, waarvoor het niet opportuun is om de verwerkingsverantwoordelijke telkens zelf een afweging te laten maken".

kel 6 AVG is een grondslag verplicht voor alle verwerkingen, ook het enkele veiligstellen door ACM van data. Dat maakt reeds dat de rechterlijke toets anders kan uitvallen, aangezien de voorzieningenrechter bij een eerdere toets van de Digitale Werkwijze aan artikel 8 EVRM het nog relevant achtte dat bij de eerste selectie van de gegevens nog geen sprake was van ‘inzage’ door ACM.²² Dat onderscheid is bij de toets onder de AVG irrelevant, aangezien zowel de selectie als de inzage vormen van verwerkingen zijn.

De grondslag die ACM kan inroepen zal waarschijnlijk ‘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 verwerkingsverantwoordelijke is opgedragen’. Zijn De Awb biedt in artikel 5:17 een wettelijke basis voor ACM om bij het uitvoeren van haar taken inzage te vorderen in gegevens, maar die basis is beperkt tot zakelijke data. Veel van de data die ACM kopieert valt daar niet onder, met name wanneer ACM integrale kopieën maakt van mobiele telefoons of van e-mail mappen. Inzage in dergelijke privé-gegevens mist dus een wettelijke basis en is daarnaast niet noodzakelijk en proportioneel voor de uitvoering van de taken van ACM. Dat laatste lijkt eveneens te gelden voor gegevens die niet ter zake doende zijn voor het onderzoek in het kader waarvan ACM in een specifiek geval inzage vordert. Het stelsel dat ACM op dit moment hanteert waarbij alle gegevens op basis van (brede) zoektermen als relevant worden aangemerkt en meegenomen en het vervolgens op grond van artikel 2.3 Digitale Werkwijze aan de betrokken onderneming is om aan te geven dat er sprake is van privé-gegevens en vervolgens het oordeel van de toezichthoudend ambtenaar over de houdbaarheid van die claim moet afwachten, is een categorische beperking van de rechten van de betrokken natuurlijke personen die onder de AVG niet langer is toegestaan. Daarbij zal het feit dat deze claim wordt beoordeeld door de toezichthoudend ambtenaar die ook het onderzoek uitvoert eveneens niet als de meest proportionele beperking van de rechten hebben te gelden onder de AVG.²³ Dit werd door de voorzieningenrechter in de al eerder aangehaalde uitspraak van 22 november 2017 waarin aan artikel 8 EVRM werd getoetst ook al als mogelijk knelpunt aangemerkt.²⁴ In die zaak was dit onvoldoende om tot toewijzing van de vordering tot vernietiging van de gekopieerde gegevens althans tot het opleggen van een verbod die gegevens te gebruiken over te gaan, maar onder de AVG lijkt deze wijze van toetsing

van claims van betrokkenen geen stand te kunnen houden vanuit het proportionaliteitsoogpunt. Dit geldt evenzeer voor de mogelijkheid voor ACM om afhankelijk van haar eigen inschattingen de optie van artikel 2.3 Digitale Werkwijze van het aanmerken van gegevens al privé in voorkomende gevallen in het geheel niet te bieden. Uit de Digitale Werkwijze blijkt niet dat er een mogelijkheid is om bezwaar te maken tegen die inschatting van ACM. In dat geval is er geen enkele waarborg meer voor het beschermen van privé-gegevens. Dit lijkt voorshands onverenigbaar met het vereiste van artikel 23 AVG dat eventuele beperkingen van de rechten van personen evenredig moeten zijn.

Een mogelijkheid om zakelijke gegevens aan te merken als niet relevant ontbreekt in het geheel in de Digitale Werkwijze. Onzes inziens zou er (als ACM al zo breed zou mogen kopiëren als zij nu doet) minimaal een mogelijkheid moeten zijn om aan te geven dat gegevens *out-of-scope* zijn om aan de noodzakelijkheidstoets van de AVG te kunnen voldoen. Die waarborg ontbreekt op dit moment, maar zou kunnen worden ingebouwd in een soort tweede controleslag die over de gegevens wordt gemaakt voordat het onderzoeken van die gegevens start. Daarenboven lijkt het hoe dan hoe ook lastig houdbaar om het kopiëren van voor ACM gebruikelijke aantallen van meer dan honderd-duizend documenten als proportioneel te zien. Als na het van toepassing worden van de AVG niet wordt voorzien in een wettelijke regeling waarbij de rechten en verplichtingen onder de AVG categorisch worden beperkt, zal ACM onder artikel 41 UAVG steeds per geval moeten beoordelen wat er wel en niet noodzakelijk en proportioneel is gezien de specifieke omstandigheden van dat geval, zowel qua de hoeveelheid en soort data die wordt gekopieerd en onderzocht, als qua waarborgen die worden ingebouwd voor de betrokkenen.

Bewaartermijnen

Zoals hierboven al is beschreven worden digitale gegevens die wel door ACM zijn veiliggesteld, maar niet zijn opgenomen in het dossier, bewaard uiterlijk totdat het onderzoek is afgerond (artikel 2.6, vierde lid, Digitale Werkwijze). Gegevens die wel zijn opgenomen in het dossier, worden bewaard overeenkomstig de Archiefwet 1995 (artikel 2.6, vijfde lid, Digitale Werkwijze).

Voor zover het daarbij gaat om niet-zakelijke of *out-of-scope* persoonsgegevens is er geen enkele grondslag of noodzaak voor ACM om deze gegevens te bewaren en moeten deze direct worden vernietigd

Onder de AVG is het uitgangspunt dat de opslagperiode van persoonsgegevens wordt beperkt tot een strikt mini-

22 ECLI:NL:RBDHA:2017:14150. In r.o. 4.8 overweegt de voorzieningenrechter: “de eerste selectie vindt automatisch plaats. Van daadwerkelijke inzage in alsdan niet-geselecteerde gegevens is derhalve geen sprake”

23 De separate werkwijze inzake geprivilegieerde gegevens waarbij de beoordeling wordt verricht door een andere functionaris – de functionaris verschoningsrecht – laten we in dit artikel buiten beschouwing.

24 ECLI:NL:RBDH:2017:14150. In r.o. 4.10 overweegt de voorzieningenrechter: “Wel stelt de voorzieningenrechter vast dat, anders dan bij een claim ter zake geprivilegieerde gegevens, een claim ter zake niet-zakelijke gegevens wordt beoordeeld door de onderzoeksleider. Dit kan tot gevolg hebben dat de onderzoeksleider kennis neemt van stukken waarvan achteraf komt vast te staan dat hiervoor geen grondslag aanwezig was. Het valt op voorhand echter niet in te schatten in hoeverre dit probleem zich daadwerkelijk voor zal doen”.

mum.²⁵ Bewaren mag niet langer dan noodzakelijk en op grond van artikel 13 AVG moeten de concrete bewaartermijnen of de criteria voor het vaststellen daarvan worden gecommuniceerd. Dit leidt op zijn minst tot een aanpassing van de regeling voor gegevens die niet in het dossier worden opgenomen. Voor zover het daarbij gaat om niet-zakelijke of *out-of-scope* persoonsgegevens is er geen enkele grondslag of noodzaak voor ACM om deze gegevens te bewaren en moeten deze direct worden vernietigd. Voor persoonsgegevens die zakelijk en relevant voor het onderzoek zijn, lijkt een bewaartermijn tot het einde van het onderzoek wel verdedigbaar onder de AVG.²⁶ Tot welke concrete bewaartermijn de toepassing van de Archiefwet leidt voor de gegevens die wel onderdeel uitmaken van het dossier maakt ACM niet duidelijk, ook niet in de door ACM vastgestelde Archiefbeheersregeling ACM 2013.²⁷ Dit moet onder de AVG wel. De Archiefwet verplicht overigens ook tot zorgdragen voor vernietiging van daarvoor in aanmerking komende archiefbescheiden. ACM kan dus ook na het van toepassing worden van de AVG nog altijd in overeenstemming met die wet handelen, maar zal steeds goed moeten beoordelen welke gegevens op welk moment niet langer noodzakelijkerwijs moeten worden bewaard en daarmee voor vernietiging in aanmerking komen. Daarbij dient ook een belangenafweging worden gemaakt tussen het belang van ACM bij bewaren en de belangen van de betrokken personen. Bij de afweging speelt mee dat gegevens die zich onder de ACM bevinden binnen het bereik van de Wet openbaarheid bestuur kunnen vallen, en ook onder de Archiefwet openbaarheid het uitgangspunt is.

Hergebruik en derden

Onder de AVG mogen gegevens alleen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Verder gebruik van de gegevens voor andere doelen dan die oorspronkelijke doelen is maar beperkt mogelijk, namelijk voor zover dat verdere gebruik daarmee verenigbaar is. Ook voor het verstrekken van gegevens aan derden moet er een grondslag bestaan en moet de betrokken persoons daarover worden geïnformeerd. Artikel 2.6 Digitale Werkwijze houdt daar op dit moment nog geen rekening mee en stelt slechts:

“Gegevens opgenomen in de onderzoeksdataset kunnen worden hergebruikt in een ander onderzoek en extern worden verstrekt”.

Of dat houdbaar is zal ACM straks onder artikel 41 UAVG steeds per individueel geval moeten afwegen.

Daarnaast ontbreekt in de Digitale Werkwijze op dit moment een waarborg voor de gegevens van natuurlijke personen op wie het onderzoek zich niet richt, maar wiens gegevens (zonder dat zij dit weten) wel worden verwerkt. Als ACM bijvoorbeeld integrale kopieën maakt van mobiele telefoons, is er sprake van het verwerken door ACM van (gevoelige) persoonsgegevens van vele derden deel uitmaken van die bestanden (waaronder uitgewisselde berichten en belgegevens). Uit de Digitale Werkwijze volgt nu nog op geen enkele wijze dat ACM rekening houdt met de belangen van deze derden wiens gegevens zich kunnen bevinden in de gekopieerde bestanden.

In het verlengde hiervan doemt de vraag op hoe ACM om zal gaan met deze persoonsgegevens in situaties waarin het onderzoek tot handhavingsmaatregelen leidt, en bijvoorbeeld in een situatie van een procedure tegen een boetebevel wordt omgegaan met de mogelijke toegang van derde partijen tot het dossier en de daarin opgenomen persoonsgegevens.

Beveiliging

Daarnaast stelt de AVG eisen aan de beveiliging van persoonsgegevens. De verplichtingen inzake de beveiligingseisen zijn opgenomen in de artikel 24, 25 en 32 AVG en kunnen niet worden beperkt onder artikel 23 AVG en/of artikel 41 UAVG. Het is niet duidelijk op welke wijze ACM op dit moment alle bestanden die zij kopieert en onderzoekt beveiligt, maar uit de toelichting bij de Digitale Werkwijze volgt dat de toezichthoudend ambtenaren “voor zover mogelijk gebruik [maken] van industriestandaard programmatuur en producten”. Dat lijkt volstrekt onvoldoende gezien de grote hoeveelheden data die ACM verwerkt. Onder de AVG zal ACM een beveiligingsbeleid moeten hebben met de passende technische en organisatorische maatregelen die ACM treft. In lijn met artikel 32 AVG zal ACM ook maatregelen moeten doorvoeren als het pseudonimiseren en versleutelen van persoonsgegevens en evaluatie- en testmaatregelen. Als uitgangspunt zal steeds de minimale gegevensverwerking centraal moeten staan. Artikel 25, tweede lid, AVG vat het mooi samen: Als verwerkingsverantwoordelijke moet ACM vanaf 25 mei 2018 zorgen voor:

“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 termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan”.

Op al die fronten lijkt er nog aardig wat werk aan de winkel voor ACM

Op al die fronten lijkt er nog aardig wat werk aan de winkel voor ACM.

²⁵ Zie ook overweging 39 van de considerans van de AVG.

²⁶ Daarbij lijkt eveneens goed verdedigbaar dat onder het einde van het onderzoek moet worden begrepen ofwel het afsluiten van het onderzoek zonder het nemen van handhavingsmaatregelen, ofwel het definitief worden van handhavingsmaatregelen na het eventueel doorlopen van bezwaar- en/of beroepsprocedures daartegen.

²⁷ *Stcr.* 2013, 9715.

6. Tot slot

Het is niet onbegrijpelijk dat niet alle rechten en verplichtingen die onder de AVG gelden voor de bescherming van persoonsgegevens onverkort van toepassing zijn in onderzoeken door toezichthouders als ACM. ACM zal echter wel werk moeten maken van een handelwijze die werkelijk kan volstaan als een solide basis voor de noodzakelijke en proportionele beperkingen die ACM wil aanbrengen in die rechten en verplichtingen. Dat kan na het van toepassing worden van de AVG niet in een categorale regeling als de Digitale Werkwijze, tenzij deze werkwijze in een wettelijke regeling wordt vastgelegd. Bij het uitblijven van een wette-

lijke regeling moet ACM per individueel geval een concrete afweging maken van de beperkingen die in dat specifieke geval noodzakelijk en proportioneel zijn. Wellicht kan ACM daarbij de hulp inroepen van de eigen FG. Als de Digitale Werkwijze illustratief is voor de ruime wijze waarop ACM omgaat met haar grondslagen voor de verwerking van persoonsgegevens, dan heeft deze FG genoeg te doen.

Over de auteurs

Mr. S.M. (Stephanie) Dielemans-Goossens

Advocaat bij Stek.

M.R. (Mattijs) Baneke

Advocaat bij Stek.