

AVG en privacy bij archieven en bibliotheken

DOOR MIRJAM ELFERINK, MARTIJN KORTIER EN TIJS WEUSTENRAAD¹

1. Inleiding

*"Als wij samen naar de bibliotheek zouden gaan en er zou bij de ingang een man staan met een camera, die permanent zou meelopen. Welk boek je inkijkt, waar je naar zoekt... Nou, die sla je onmiddellijk in elkaar. Althans vrij snel. Nu zit de bibliotheek op internet en gebeurt hetzelfde. En niemand maakt zich er zorgen over. Vind ik raar."*²

Het voorgaande citaat is afkomstig van Aleid Wolfsen, de huidige voorzitter van de Autoriteit Persoonsgegevens. Hij schetst treffend dat een invulling van het begrip 'privacy' kennelijk afhankelijk is van de context.

"Een archief heeft alleen maar nut als je het ook mag inzien."

Deze quote is afkomstig van Marens Engelhard, algemeen rijksarchivaris en tevens directeur van het Nationaal Archief in Den Haag, uit een interview in Trouw.³

Deze quote geeft weer dat bij archieven het belang van de samenleving bij openbaarheid van archieven hoog in het vaandel staat. Ook volledige en integere archivering is van groot belang. Deze instellingen hebben immers als

- 1 Mr. dr. M.H. (Mirjam) Elferink en mr. M.J.M. (Martijn) Kortier zijn beide advocaat en oprichters van Elferink & Kortier Advocaten, een kantoor gespecialiseerd in het adviseren en procederen over intellectueel eigendomsrecht (IE), ICT-recht en privacy. Mr. T. (Tijs) Weustenraad is juridisch medewerker bij Elferink & Kortier Advocaten. De auteurs geven met enige regelmaat cursussen aan informatiespecialisten over o.a. privacy en archieven. Mirjam Elferink promoveerde op het proefschrift "Verwijzingen in wetgeving. Over de publiekrechtelijke en auteursrechtelijke status van normalisatienormen" (Deventer: Kluwer 1998).
- 2 Dit citaat is afkomstig van Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens, 7 oktober 2016.
- 3 Salm, H. (2018, 31 maart). De rijksarchivaris is niet bang voor gerommel in de archieven door de nieuwe privacywet. Geraadpleegd van <https://www.trouw.nl/nieuws/de-rijksarchivaris-is-niet-bang-voor-gerommel-in-de-archieven-door-de-nieuwe-privacywet~b9e613b4/>.

maatschappelijke taak hun collecties voor huidige en komende generaties toegankelijk te maken en te houden, bij voorkeur zo laagdrempelig mogelijk. Zo hebben het Nationaal Archief en de Koninklijke Bibliotheek onder andere als wettelijke taak de archieven van de rijksoverheid, respectievelijk de nationale bibliotheekverzamelingen te beheren en toegankelijk te maken. Daarbij ontkomen zij niet aan het verwerken van persoonsgegevens. Het belang van openbaarheid en dat van volledige en integere archivering staat vaak op gespannen voet met het recht op privacy van betrokkenen. Enerzijds moet de samenleving erop kunnen vertrouwen dat de archieven volledig en integer zijn. Bovendien is het uitgangspunt dat gearhiveerde documenten openbaar zijn. Anderzijds gaat de privacywet- en regelgeving in beginsel uit van een vertrouwelijke behandeling van persoonsgegevens en een zo minimaal mogelijke verwerking daarvan. Hoe verhouden deze uitgangspunten zich tot elkaar? Doordat archieven en bibliotheken vele bronnen van kennis verzamelen en beheren die – veelal – een breed scala aan persoonsgegevens bevatten en hun dienstverlening daarnaast in toenemende mate is gedigitaliseerd, is de belangstelling voor privacy de afgelopen jaren sterk toegenomen.

De komst van de Europese Algemene Verordening Gegevensbescherming⁴ (hierna: ‘AVG’), die op 25 mei 2018 in werking is getreden, brengt voor deze instellingen nieuwe en uitgebreidere verplichtingen met zich mee. Daarnaast regelt de AVG een aantal specifieke zaken voor archieven en bibliotheken. Zo ziet artikel 85 AVG op de verwerking en vrijheid van meningsuiting en van informatie, en artikel 89 AVG op archivering in het algemeen belang. Ook kent de AVG een uitzondering in verband met wetenschappelijk, historisch of statistisch onderzoek. Met welke verdere privacyrechten en -plichten moeten archieven en bibliotheken rekening houden? En welke uitzonderingen op de ‘gewone regels’ gelden voor hen? Archiven hebben doorgaans ook veel gegevens over overledenen in hun collectie. Over de privacybescherming van overledenen bestaan veel misverstanden. De indruk leeft dat verwerking van persoonsgegevens van overledenen zonder meer is toegestaan omdat de AVG daarop niet van toepassing is. Dat ligt echter genuanceerder. In dit artikel gaan wij in op deze vragen en behandelen wij een aantal specifieke regels uit de AVG.

Dit artikel richt zich in het bijzonder op archieven, bibliotheken, gemeenten, samenwerkingsverbanden van gemeenten en onderzoeksinstituten, die in hun dagelijkse werkzaamheden te maken krijgen met vragen over de verwer-

4 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 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, Publicatieblad van de Europese Unie L 119.

king en bescherming van persoonsgegevens bij het verwerken daarvan in (historische) archiefbestanden. Daarbij ligt de focus op verwerking van persoonsgegevens in de bronnen die deze instellingen verwerken. De verwerking van persoonsgegevens bij instellingen die zien op de dagelijkse processen en diensten rondom de verwerking van (historische) archiefbestanden laten wij in dit artikel feitelijk buiten beschouwing. Dat betekent bijvoorbeeld dat de registratie van bezoekers van archiefbewaarplaatsen die bepaalde archiefbescheiden willen inzien of de verwerking van lenersgegevens door een bibliotheek niet zullen worden behandeld.⁵ Dergelijke verwerkingen raken vanzelfsprekend aan de dagelijkse werkzaamheden van medewerkers van archiefinstellingen en bibliotheken. Toch is die verwerking privacy-technisch minder ingewikkeld en in onze ogen derhalve minder interessant om te behandelen in dit artikel. Voor de 'dagelijkse' persoonsgegevensverwerkingen dient men immers de 'normale' regels uit de privacyregelgeving te volgen. Daar bestaat reeds veel literatuur over. De vraag óf men bepaalde persoonsgegevens mag verwerken en zo ja, hoe, kan overigens wel grotendeels worden beantwoord door het stramien van de AVG te doorlopen, zoals wij dat in dit artikel in zijn algemeenheid uitlegen.

In onze ogen verdient de verwerking van persoonsgegevens in de bronnen die de voornoemde instellingen beheren, daarentegen wel nadere uitwerking. Deze verwerking blijkt in de praktijk immers ingewikkeld en zorgt ervoor dat medewerkers van met name archieven voor dilemma's worden geplaatst. Welk recht moet prevaleren? De AVG of de Archiefwet? Geldt het beginsel van openbaarheid of het beginsel van beperking van de verwerking van persoonsgegevens? In dit artikel zoomen wij daar nader op in.

Achtereenvolgens behandelen wij de volgende onderwerpen:

1. het begrip 'privacy';
2. een uitleg over de AVG en diens verhouding met de Archiefwet, Wet openbaarheid van bestuur (Wob) en eventuele andere sectorale wetgeving;
5. De specifieke regels en uitzonderingen voor archieven en bibliotheken ten aanzien van de verwerking van persoonsgegevens in de diverse (archief)bestanden, die wij aanhalen in dit artikel, gelden in principe niet voor verwerkingen van persoonsgegevens die zien op de dagelijkse processen en diensten in het kader van de normale bedrijfsvoering van bijvoorbeeld de archiefinstellingen en bibliotheken. Het voert te ver om in het bestek van dit artikel óók stil te staan bij dergelijke persoonsgegevensverwerkingen. Overigens dienen deze verwerkingen van persoonsgegevens uiteraard wel aan de algemene beginselen en uitgangspunten van de AVG te worden getoetst. De door ons in dit artikel beschreven toelichting op de werking/het stramien van de AVG biedt de kaders voor de beantwoording van de vraag of dergelijke persoonsgegevensverwerkingen in lijn zijn met de AVG.

3. enkele belangrijke begrippen uit de AVG;
4. de werking/het stramien van de AVG;
5. bijzondere persoonsgegevens;
6. de privacy-rollen van de AVG: verwerkingsverantwoordelijke en verwerker;
7. verplichtingen uit de AVG in algemene zin;
8. de Archiefwet en privacy;
9. de Wet openbaarheid van bestuur en privacy;
10. uitzonderingen AVG voor archieven, onderzoekers en bibliotheken;
11. beeldmateriaal en privacy;
12. privacy van overledenen;
13. afronding.

2. Begrip ‘privacy’

Privacy. De term wordt veelvuldig gebezigd. Maar wat betekent dit begrip nu eigenlijk? De Amerikanen Warren en Brandeis definieerden het begrip privacy in 1890 als “the right to be let alone”.⁶ Dit werd ingegeven door een zaak waarin iemands persoonlijke levenssfeer werd aangetast door de roddelpers. Later, met de opkomst van de computer, kwam het besef dat steeds meer informatie over individuen werd opgeslagen in grootschalige informatiesystemen waardoor er een risico op aantasting van de persoonlijke levenssfeer ontstond. Doordat verschillende databestanden aan elkaar gekoppeld kunnen worden, kunnen er persoonsprofielen worden opgesteld van individuen. Dergelijke informatie kan diep ingrijpen in de persoonlijke levenssfeer. Daardoor groeide de behoefte om op enigerlei wijze zeggenschap te krijgen over het gebruik van deze informatie. Deze informationele kant van de persoonlijke levenssfeer werd als eerste gekarakteriseerd door A.F. Westin:

*“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others”.*⁷

In de praktijk blijkt het lastig om een eenduidige definitie van privacy te geven. Een ander voorbeeld:

“Privacy is geen statisch object, maar een concept dat context gerelateerd is. Hierdoor is het onmogelijk om het te definiëren zonder te refereren aan een com-

6 S.D. Warren en L.D. Brandeis, The right to privacy, in: Harvard Law Review, 15 december 1890.

7 A.F. Westin, Privacy and freedom, New York, 1967, p. 7.

*plex geheel van sociale, culturele, religieuze en historische parameters waaraan het zijn betekenis ontleent.*⁷⁸

Er circuleren vele definities van het begrip privacy, maar bovenstaand citaat van hoogleraar privacy, veiligheid en databescherming Serge Gutwirth uit 1998 dekt wat ons betreft eigenlijk wel de lading. Voor iedereen betekent privacy namelijk iets anders. Privacy zal voor onze koning een hele andere lading hebben dan voor een ‘normale’ burger.

Privacy is dus niet voor ieder individu hetzelfde. Privacy heeft bovendien niet op ieder moment dezelfde betekenis. Privacy lijkt op een soort zelfbeschikkingsrecht; het recht om een persoon zelf te laten bepalen wat er met zijn of haar persoonsgegevens gebeurt. In de praktijk worden er echter ook heel veel persoonsgegevens verwerkt zonder dat betrokkenen dat weten of zonder dat zij daar toestemming voor hebben gegeven. Denk bijvoorbeeld aan de verwerking van persoonsgegevens bij gemeentelijke instanties. De interpretatie van privacy als een soort zelfbeschikkingsrecht is wat ons betreft dan ook te eng. Ook als men geen weet heeft van verwerking van de persoonsgegevens of als men daar niet mee instemt, kan het toch zo zijn dat organisaties rechtmatig persoonsgegevens verwerken. Bescherming van deze persoonsgegevens is ook – of misschien wel juist – in die gevallen van belang.

Dat privacy contextafhankelijk is, blijkt alleen al uit het feit dat er tegenwoordig veel meer aandacht voor de bescherming van de persoonlijke levenssfeer is dan vroeger. Blijkbaar is er reden om extra waakzaam te zijn. Maar worden er ook meer persoonsgegevens verwerkt? Nog niet zo lang geleden waren alle adressen en telefoongegevens van alle Nederlanders voor iedereen beschikbaar in de telefoongids. Tegenwoordig worden gegevens op andere manieren verzameld en gaan ze sneller en eenvoudiger de wereld over. Denk daarbij aan het verzamelen van persoonsgegevens via cookies, big data, Facebook, et cetera. Door de digitalisering vliegen persoonsgegevens bijna per definitie de hele wereld over. Verwerking van persoonsgegevens is iets van alle tijden. De wijze waarop en in welk tempo dat gebeurt verschilt echter. De vraag is wat de impact van die verwerking is en hoe die verwerking in goede banen moet worden geleid. Uitgangspunt daarbij zou moeten zijn dat de betrokkene in ieder geval weet wat er met zijn of haar persoonsgegevens gebeurt en welke organisatie erover beschikt. In die zin komen we toch terug bij het eerdergenoemde zelfbeschikkingsrecht; eenieder heeft recht op informatie over de verwerking van zijn of haar persoonsgegevens.

8 S. Gutwirth, *Privacy and the information Age* (R. Casert, Trans), Rowman & Littlefield, 2001, p. 29.

3. De privacy wet- en regelgeving en de verhouding tot overige wetgeving

De AVG is een Europese verordening die regels bevat over de verwerking van persoonsgegevens. De AVG is in april 2016 aangenomen en is sinds 25 mei 2018 effectief van toepassing in de gehele Europese Unie (EU). Verordeningen hebben rechtstreekse werking in de lidstaten van de EU. Dit betekent dat deze direct toepasbaar zijn in de lidstaten en niet eerst hoeven te worden omgezet naar nationaal recht. Ook in Nederland is de AVG dus rechtstreeks van toepassing. De AVG geeft lidstaten de ruimte om een eigen invulling te geven aan bepaalde verplichtingen. Daarvoor kunnen lidstaten aanvullende nationale uitvoeringsregelgeving vaststellen. In Nederland is dat op een aantal onderdelen gebeurd. Deze specifieke regels zijn vastgelegd in de zogeheten ‘Uitvoeringswet Algemene Verordening Gegevensbescherming’ (hierna: ‘UAVG’). De AVG dient in Nederland in samenhang met de UAVG gelezen, beoordeeld en toegepast te worden.

Vóór de AVG gold in Nederland de Wet bescherming persoonsgegevens (hierna: ‘Wbp’). Via de Nederlandse Wbp is de Europese richtlijn bescherming persoonsgegevens (95/46 EG) uit 1995 geïmplementeerd.⁹ Zowel deze richtlijn als de AVG zijn op Europees niveau vastgesteld. Het stramien en delen van de inhoud van de AVG lijken dan ook erg veel op dat van de Wbp. Wel bevat de AVG op diverse onderdelen strengere regels en hogere sancties dan de Wbp. Op die specifieke regels uit de AVG gaan wij verderop in dit artikel nader in.

De AVG en de UAVG bieden een algemeen kader van regels voor iedere verwerking van persoonsgegevens. Daarnaast kunnen echter ook regels uit de toepasselijke sectorspecifieke wet- en regelgeving van invloed zijn op persoonsgegevensverwerkingen. Denk bijvoorbeeld aan de Archiefwet en de Wet openbaarheid van bestuur (hierna: ‘Wob’). De Archiefwet en de Wob hebben als uitgangspunt dat gegevens openbaar zijn. De AVG heeft als uitgangspunt om zo min mogelijk gegevens te verwerken en deze goed te beveiligen. Dit strookt niet altijd met het uitgangspunt van de Archiefwet en de Wob. In het geval er sprake mocht zijn van tegenstrijdige rechten en plichten die voortvloeien uit sectorspecifieke regelgeving, zoals de Archiefwet en/of de Wob, dan zou bij een dergelijke ‘botsing’ formeel genomen de AVG als Europese verordening voorgaan op nationale wetgeving. De AVG bevat echter een aantal afwijkende regels voor onder meer archivering in het algemeen belang en

9 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, Publicatieblad van de Europese Gemeenschappen L 281, 38e jaargang, 23 november 1995.

de verwerking in het kader van de vrijheid van meningsuiting en van informatie. De AVG biedt de lidstaten van de EU daarnaast de ruimte om in nationale regelgeving specifieke regels vast te stellen. De Nederlandse wetgever heeft van die ruimte gebruikgemaakt en getracht in oplossingen te voorzien om dergelijke ‘botsingen’ te beslechten. Zo bevat de UAVG bijvoorbeeld een aantal uitzonderingen voor archivering in het algemeen belang en is de Archiefwet aangepast aan de AVG. Als er persoonsgegevens worden verwerkt, zijn de AVG en UAVG náást de Archiefwet en de Wob van toepassing. Dat betekent dat de verwerking van (persoons)gegevens – naast dat deze moet voldoen aan de regels van de Archiefwet en/of de Wob – ook getoetst moet worden aan de AVG en UAVG. Verderop in dit artikel gaan wij in op deze specifieke regels en de verhouding daarvan met de AVG en UAVG.

4. Enkele belangrijke begrippen uit de AVG

Voor een goed begrip van de AVG en de materie die daarin wordt behandeld, is het van belang om scherp te hebben wat de betekenis is van een aantal begrippen uit de AVG. De belangrijkste begrippen in dat kader zijn:¹⁰

- *Persoonsgegevens*: Alle gegevens die direct of indirect te herleiden zijn tot een bepaalde natuurlijke persoon, zijn aan te merken als persoonsgegevens. Het gaat dan feitelijk om alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dat betekent dat ook gegevens waar niet direct een naam aan gekoppeld is als persoonsgegevens kunnen worden aangemerkt. Dit begrip is derhalve zeer ruim. Te denken valt aan onder meer NAW-gegevens, telefoonnummers, e-mailadressen, maar ook aan inkomensgegevens of het IP-adres. Overledenen vallen in beginsel niet onder het toepassingsbereik van de AVG. Zij zijn volgens de wet immers geen natuurlijke personen meer. Dat neemt niet weg dat de bescherming van de persoonlijke levenssfeer ook in het geval van overledenen nog een rol kan spelen. Daar gaan wij later in dit artikel verder op in.
- *Bijzondere persoonsgegevens*: Persoonsgegevens die naar hun aard gevoelig zijn. Voor deze gegevens geldt in de AVG een bijzonder regime. Het betreft persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens of gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid, blijken.
- *Strafrechtelijke persoonsgegevens*: Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.

10 In de AVG worden veel definities gebruikt. De definities worden uitgewerkt in artikel 4 AVG.

- *Betrokkene*: De natuurlijke persoon op wie de (persoons)gegevens betrekking hebben.
- *Verwerken van persoonsgegevens*: Alle handelingen met betrekking tot een persoonsgegeven; zowel actief als passief. De AVG duidt 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, aan als verwerkingen van persoonsgegevens. Een organisatie ‘verwerkt’ derhalve al snel. Anders dan het woord ‘verwerken’ doet vermoeden, is een actieve handeling daarvoor niet vereist. Bedenk daarbij dat niet uitsluitend ‘verwerkers’ verwerken, maar dat ook de ‘verwerkingsverantwoordelijke’ verwerkt. De terminologie kan op dit punt voor leken verwarrend zijn. Uitgangspunt is dat iedere partij die iets met de persoonsgegevens ‘doet’ of ‘deze onder zich heeft’, die gegevens aan het ‘verwerken’ is. Vervolgens moet de vraag gesteld worden in welke rol men verwerkt.
- *Bestand*: Elk gestructureerd geheel van persoonsgegevens dat volgens bepaalde criteria toegankelijk is. Daarbij maakt het niet uit of dit geheel gecentraliseerd of gedecentraliseerd is, dan wel op functionele of geografische gronden is verspreid. Dit betekent kort gezegd dat er sprake moet zijn van gegevensverwerkingen of -verzamelingen die onderlinge samenhang vertonen en op systematische wijze toegankelijk moeten zijn. Een (analoge) gegevensverzameling voor een bepaald dossier in een archief zal in principe op grond van deze definitie aangemerkt worden als een ‘bestand’ in de zin van de AVG.
- *Verwerkingsverantwoordelijke*: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, die/dat alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze partij bepaalt het hoe en het waarom van de persoonsgegevensverwerking. Hoe in de praktijk bepaald kan worden of een bepaalde organisatie een verwerkingsverantwoordelijke is, wordt in paragraaf 5 van dit artikel toegelicht.
- *Verwerker*: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Deze partij bepaalt niet het hoe en het waarom ten aanzien van de persoonsgegevensverwerking. Hij verwerkt de persoonsgegevens uitsluitend ten behoeve van een ander – de verwerkingsverantwoordelijke – en bepaalt niet zelf welke persoonsgegevens hij verwerkt, voor welk doel, hoe lang, et cetera. Hoe men in de praktijk bepaalt of men een verwerker is, komt in paragraaf 5 van dit artikel aan de orde.

5. Werking AVG

In de AVG kan een bepaald stramien ontwaard worden dat feitelijk uiteenvalt in de volgende vier stappen:

1. Is de AVG van toepassing?
2. Wat is de rol van de desbetreffende organisatie bij een specifieke soort persoonsgegevensverwerking: ‘verwerkingsverantwoordelijke of verwerker’?
3. Als verwerkingsverantwoordelijke: is het vervolgens toegestaan de persoonsgegevens te verwerken? Is er een doel en een grondslag? En in het geval van verwerking van bijzondere persoonsgegevens: is er een onthefing voor het verwerkingsverbod?
4. Als er op grond van het voorgaande mag worden verwerkt: hoe dan verder? Er moet immers worden voldaan aan de verplichtingen uit de AVG.

Deze stappen in het stramien van de AVG lichten wij in deze paragraaf toe. In paragraaf 7 behandelen wij deze stappen in een praktijkcasus.

5.1. AVG van toepassing?

De AVG is, kort gezegd, van toepassing op de – geheel of gedeeltelijk – geautomatiseerde verwerking van persoonsgegevens, maar ook op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Daarbij wordt aangehaakt bij de definities zoals we die in de vorige paragraaf hebben behandeld. De toepasselijkheid van de AVG vaststellen lijkt op het eerste gezicht makkelijker dan het in de praktijk blijkt te zijn. Wat zijn nu precies persoonsgegevens en is mijn organisatie deze wel aan het verwerken?

Anders dan sommige mensen in een reflex lijken te denken, is het niet zo dat als de AVG van toepassing is, er een verbod bestaat op het verwerken van persoonsgegevens. Dat is zeker niet het geval. De wet verbiedt het verwerken van persoonsgegevens (in beginsel) niet, maar geeft juist de kaders waarbinnen die verwerking plaats moet vinden. In die zin staat de AVG verwerking van persoonsgegevens – onder voorwaarden – juist toe. De AVG beoogt dat betrokkenen erop kunnen vertrouwen dat er goed met hun persoonsgegevens wordt omgegaan.

Als is vastgesteld dat er sprake is van verwerking van persoonsgegevens in de zin van de wet, is alleen nog maar vastgesteld *dát* de AVG van toepassing is op die verwerking. Dat zegt nog niets over de wijze *waarop* de persoonsgegevens worden verwerkt en belangrijker, of ze wel *mogen* worden verwerkt.

5.2. Welke rol?

Voordat we aan beantwoording van die laatste vraag toekomen, moet een organisatie eerst vaststellen wat haar rol in dezen is: met andere woorden; is men een verwerkingsverantwoordelijke of een verwerker? De wet legt aan beide figuren immers verschillende soorten verplichtingen op. Pas als die rol duidelijk is kan de vraag gesteld worden of de persoonsgegevensverwerking toegestaan is. Deze beide rollen – die van verwerkingsverantwoordelijke en verwerker – behandelen wij gezien het belang daarvan afzonderlijk in paragraaf 6.

5.3. Is de verwerking toegestaan?

Bij de beantwoording van de vraag of verwerking van persoonsgegevens is toegestaan, zijn de begrippen ‘doel en grondslag’ van essentieel belang. De verwerkingsverantwoordelijke dient namelijk allereerst een doel en grondslag van de persoonsgegevensverwerking vast te stellen.

De AVG schrijft voor dat persoonsgegevens uitsluitend voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (‘doel’) mogen worden verwerkt. Dat aldus – door de verwerkingsverantwoordelijke – vastgestelde doel is het startpunt van de verwerking van persoonsgegevens. Persoonsgegevens mogen niet op een met dat doel onverenigbare wijze verder worden verwerkt.

Met dat voorschrift als uitgangspunt zou archivering dus niet toegestaan zijn. Persoonsgegevens worden immers nooit initieel voor archiveringsdoeleinden verzameld. Zij worden in eerste instantie verwerkt voor een andere, oorspronkelijke, verwerking. Pas na die oorspronkelijke verwerking worden zij gearchiiveerd, hetgeen evident een ander doel is dan het initiële verwerkingsdoel. De wetgever heeft daarom uitdrukkelijk voorzien in een uitzondering voor verdere verwerking met het oog op archivering in het algemeen belang en voor wetenschappelijk, historisch en statistisch onderzoek. Deze doeleinden worden – blijkens de tekst van de AVG – niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd. Op deze uitzondering zoomen wij verderop in dit artikel verder in.

Heeft de organisatie geen gerechtvaardigd doel voor de verwerking, dan mag zij de persoonsgegevens ook niet verwerken. Let wel, bepaalde verwerkingen zijn mogelijk niet strikt noodzakelijk om een bepaalde dienst te kunnen verlenen, maar de desbetreffende organisatie kan daar wel degelijk een bepaald doel bij hebben. Denk in dat kader bijvoorbeeld aan het online bestellen van een e-book. De leverancier verwerkt het e-mailadres van de klant om het e-

book aan de desbetreffende klant te kunnen toesturen. Daarnaast verwerkt deze organisatie het e-mailadres ook om haar klant periodiek een nieuwsbrief te sturen. Die laatste verwerking is niet strikt noodzakelijk in het kader van haar primaire dienstverlening, maar kan voor de organisatie toch een gerechtvaardigd doel dienen. Immers, daarmee doet de organisatie aan relatiebeheer, brengt zij haar collectie onder de aandacht, werft zij mogelijk nieuwe klanten, et cetera. Of deze verwerking is toegestaan zit hem niet zozeer in het ‘doel’, maar mogelijk meer in de vraag of er een ‘grondslag’ aanwezig is.

Bij iedere persoonsgegevensverwerking dient de verwerkingsverantwoordelijke zich af te vragen of hij een gerechtvaardigd doel voor die verwerking heeft. Dat geldt niet alleen voor nieuwe verwerkingen maar ook voor bestaande. Bij de inwerkingtreding van de AVG hebben veel organisaties hun persoonsgegevensverwerkingen doorgelicht, al dan niet in het kader van de nieuwe verplichting tot het bijhouden van een zogenaamd gegevensverwerkingenregister. In veel gevallen hebben organisaties destijds moeten constateren dat zij ook verwerkingen uitvoeren waarvoor zij niet direct een gerechtvaardigd doel hebben. Daarmee valt voor die organisaties in ieder geval een van de twee kernbegrippen (doel en grondslag) weg. Zij zouden vervolgens moeten concluderen dat zij die desbetreffende persoonsgegevensverwerking niet mochten uitvoeren. Dat hadden zij strikt genomen overigens ook al niet gemogen onder het regime van de Wbp.

Overigens dient de verwerkingsverantwoordelijke op grond van de AVG het doel vast te leggen. Dit is onderdeel van de zogeheten ‘accountabilityplicht’. Dat geldt niet alleen intern, maar feitelijk ook extern. De verwerkingsverantwoordelijke heeft namelijk in beginsel een informatieverplichting richting de betrokkene en daarin dient hij onder meer het doel van de verwerking kenbaar te maken. Op de verplichtingen die verwerkingsverantwoordelijken en verwerkers onder de AVG hebben, gaan wij later in dit artikel dieper in.

Het hebben van een gerechtvaardigd doel alleen is niet voldoende om persoonsgegevensverwerking te kunnen rechtvaardigen. De wet stelt dat er uitsluitend sprake is van een rechtmatige verwerking indien er daarnaast sprake is van een zogenaamde wettelijke ‘grondslag’. In artikel 6 van de AVG zijn zes limitatieve grondslagen opgesomd. Met andere woorden: de verwerkingsverantwoordelijke móét een van deze grondslagen kunnen kiezen. Als dat niet het geval is mag hij de persoonsgegevens – ook al heeft hij een doel – niet verwerken. De zes grondslagen zijn:

- ondubbelzinnige toestemming van de betrokkene;
- de noodzaak om een overeenkomst met de betrokkene uit te voeren;
- de noodzaak om te voldoen aan een wettelijke verplichting;
- de noodzaak om een vitaal belang van de betrokkene te beschermen;

- de noodzaak om een taak van algemeen belang of uitoefening van openbaar gezag te vervullen (voor overheids- of andere publiekrechtelijke organisaties); en
- de noodzaak voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde, waarvoor het belang van de betrokkene op bescherming van diens persoonlijke levenssfeer dient te wijken ('belangenafweging').

In de praktijk merken wij dat men snel geneigd is om toestemming te vragen voor de verwerking van persoonsgegevens. Toestemming betreft de eerste grondslag in artikel 6 AVG. Daarmee ontstaat – ten onrechte – mogelijk de indruk dat toestemming de belangrijkste en meest voor de hand liggende grondslag is. Dat is zeker niet het geval. Wanneer verwerkingsverantwoordelijken uit een van de andere grondslagen kunnen kiezen, en derhalve toestemming niet noodzakelijk is, raden wij aan om ook geen toestemming te vragen. Toestemming moet alleen worden gevraagd als er geen andere grondslag voorhanden is. Toestemming kan bijvoorbeeld immers altijd worden ingetrokken door betrokkenen, hetgeen moeilijkheden met zich mee kan brengen als een andere grondslag meer voor de hand had gelegen. Denk bijvoorbeeld aan een wettelijke verplichting om persoonsgegevens te verwerken. Bovendien hebben betrokkenen een aantal rechten onder de AVG. Denk daarbij aan het recht op verwijdering van persoonsgegevens of het recht op dataportabiliteit. Een aantal van die rechten kan onder andere uitgeoefend worden in het geval de grondslag voor de verwerking toestemming is geweest. Het uitoefenen van die rechten gaat echter niet zonder meer op als de verwerking is gebaseerd op een van de andere grondslagen. Een verwijderingsverzoek gaat vanzelfsprekend niet op als de verwerkingsverantwoordelijke wettelijk verplicht is om te verwerken (denk daarbij bijvoorbeeld aan de wettelijke verplichting voor werkgevers om een kopie van een identiteitsbewijs van hun werknemers op te slaan), maar wel in het geval de verwerking is gebaseerd op toestemming.

De voor de praktijk belangrijkste grondslag is de laatste in het rijtje met grondslagen uit artikel 6 AVG. Als de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke óf van een derde, mogen persoonsgegevens ook worden verwerkt. Die verwerking kan dus geschieden zonder toestemming van betrokkene.

Aan deze laatste grondslag heeft de wetgever echter een belangenafweging verbonden. De grondslag gaat namelijk niet op als de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen dan de belangen van de verwerkingsverantwoordelijke of de desbetreffende derde (in het bijzonder als de betrokkene een kind is). Als de verwerking wordt gebaseerd op deze grondslag, dient men derhalve af te wegen of de persoonsge-

gevensverwerking noodzakelijk is voor het belang van bijvoorbeeld de verwerkingsverantwoordelijke zelf. De impact die de verwerking vervolgens heeft op de betrokkene mag niet zodanig zijn dat die betrokkene onevenredig in haar (privacy)belangen wordt geschaad. Als dat laatste het geval is, dient de afweging in het voordeel van de betrokkene uit te vallen en mag de verwerking dus niet op deze grondslag plaatsvinden. In dat geval zal de verwerkingsverantwoordelijke waarschijnlijk zijn toevlucht moeten zoeken in de grondslag ‘toestemming’. Een goed voorbeeld van de grondslag ‘noodzakelijk voor de behartiging van de belangen van de verwerkingsverantwoordelijke of een derde’ zou bijvoorbeeld het controleren van e-mailcorrespondentie van werknemers in het kader van fraudepreventie kunnen zijn. Er dient in dit voorbeeld overigens wel sprake te zijn van concrete verdenkingen en het middel dient – mede in het kader van de belangenafweging – te voldoen aan proportionaliteits- en subsidiariteitstoetsen.

Bijzondere en strafrechtelijke persoonsgegevens

De verwerking van bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens kan significante risico's meebrengen voor de grondrechten en de fundamentele vrijheden van natuurlijke personen. Het verwerken van bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens is daarom in beginsel verboden op grond van artikel 9 en 10 AVG. Voor verwerking daarvan geldt derhalve een ander stramien dan hiervoor uitgewerkt voor normale persoonsgegevens. Bij normale persoonsgegevens geldt dat ze mogen worden verwerkt indien de verwerkingsverantwoordelijke daarvoor een doel en een grondslag heeft. Voor bijzondere persoonsgegevens (en strafrechtelijke gegevens, die we voor de overzichtelijkheid in dit artikel samenvoegen onder de noemer ‘bijzondere persoonsgegevens’) geldt dat verwerking niet is toegestaan, tenzij de verwerkingsverantwoordelijke voor verwerking een gerechtvaardigd doel heeft, een grondslag heeft én er een van de uitzonderingen op het verbod uit artikel 9 en 10 AVG opgaat. De belangrijkste uitzonderingen in dit kader zijn:

- uitdrukkelijke toestemming van de betrokkene;
- kennelijke openbaarmaking van de persoonsgegevens door de betrokkene;
- de noodzaak van de verwerking met het oog op archivering in het algemeen belang;
- de noodzaak van de verwerking met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden.

Met name de twee laatstgenoemde uitzonderingen zijn voor archieven en bibliotheken van belang. Verderop in dit artikel gaan wij verder in op deze uitzonderingen.

Verwerking BSN

Onder de Wbp was het Burgerservicenummer (hierna ‘BSN’) een bijzonder persoonsgegeven. Onder de AVG zijn BSN’s geen bijzondere persoonsgegevens meer, maar zij behoeven op grond van artikel 46 UAVG nog steeds een bijzondere behandeling. BSN’s mogen alleen worden verwerkt ter uitvoering van een wettelijke verplichting en dan nog uitsluitend indien dit strikt noodzakelijk is. Toestemming van de betrokkene voor verwerking van zijn of haar BSN is derhalve nooit een rechtsgeldige rechtvaardiging voor die verwerking.

5.4. *Hoe moeten de persoonsgegevens verwerkt worden; verplichtingen AVG*

Als men door middel van de ‘doel en grondslag’-vraag heeft vastgesteld of men persoonsgegevens ook daadwerkelijk mag verwerken, komt men toe aan de laatste vraag: op welke wijze mag men die gegevens verwerken? Het voorgaande zegt immers nog niets over de wijze waarop de persoonsgegevens moeten worden verwerkt of over de verplichtingen (bijvoorbeeld informatieverplichtingen jegens de betrokkenen) die de verwerkingsverantwoordelijke vervolgens moet naleven. De AVG legt aan verwerkingsverantwoordelijken en aan verwerkers de nodige verplichtingen op die tot doel hebben om de persoonsgegevens op deugdelijke, transparante en behoorlijke wijze te verwerken en daarnaast om passende (technische en organisatorische) beveiliging van de persoonsgegevens te bewerkstelligen. Omdat wij ons in dit artikel richten op een specifiek deel van verwerkingen van persoonsgegevens, namelijk door archieven en bibliotheken, gaat het te ver om alle verplichtingen en waarborgen die de AVG kent, te behandelen. De belangrijkste lichten wij echter nader toe in paragraaf 8.

6. **Wanneer is een organisatie verwerker en wanneer verwerkingsverantwoordelijke?**

De eerste vraag die men moet beantwoorden, zodra men heeft vastgesteld dat men persoonsgegevens verwerkt, is of men een verwerker of een verwerkingsverantwoordelijke is. In de praktijk is dit een belangrijke vraag waar veel partijen mee worstelen.

In een recente kwestie zien wij dat het in de praktijk niet altijd goed gaat met het vaststellen van welke rol men heeft.¹¹ In deze kwestie merkte de rechtbank

11 Rb. Noord-Nederland 20 december 2018, ECLI:NL:RBNNE:2018:5385.

nota bene zichzelf aan als verwerker voor de procederende partijen, die dan dus verwerkingsverantwoordelijken zouden zijn. Dat lijkt ons echter onjuist. Het feit dat de rechtbank zichzelf kwalificeert als verwerker doet ook in de juridische literatuur de wenkbrauwen fronsen.¹² Het zou zuiverder zijn als de rechtbank zichzelf ook als verwerkingsverantwoordelijke zou aanmerken, naast de procederende partijen die op hun beurt voor hun eigen deel van de verwerking in deze procedure verwerkingsverantwoordelijke zijn. Waarom dat zuiverder zou zijn, lichten we in het hiernavolgende toe.

Waarom is het onderscheid tussen het zijn van verwerkingsverantwoordelijke en/of het zijn van verwerker zo belangrijk? Dat heeft ermee te maken dat beide rollen hele andere verplichtingen met zich meebrengen. Om inzicht te hebben in deze specifieke verplichtingen, moet men dus weten welke positie men heeft.

Zeggenschap over doel en middelen

Per soort verwerking van persoonsgegevens dient te worden vastgesteld of partijen moeten worden aangemerkt als verwerker of als verwerkingsverantwoordelijke. De voorloper van de 'European Data Protection Board', waarin alle Europese privacy-toezichthouders zijn vertegenwoordigd, heeft de hiervoor genoemde definities van verwerkingsverantwoordelijke en verwerker in een opinie nader toegelicht.¹³ Dat advies is weliswaar gegeven onder de Europese richtlijn bescherming persoonsgegevens (95/46/EG) uit 1995¹⁴, maar is nog steeds relevant nu deze begrippen blijkens de definities in de AVG inhoudelijk niet gewijzigd zijn. Uit het advies volgt dat de verwerkingsverantwoordelijke zeggenschap heeft over welke persoonsgegevens er worden verwerkt, de duur van de opslag alsmede wie er toegang heeft tot de persoonsgegevens. Oftewel, het 'hoe' en 'waarom' ten aanzien van de persoonsgegevensverwerkingen worden bepaald door de verwerkingsverantwoordelijke. Een verwerker verwerkt daarentegen de persoonsgegevens slechts ten behoeve van de verwerkingsverantwoordelijke. Hierbij opereert de verwerker binnen de kaders van het mandaat en de instructies die hij van de verwerkingsverantwoordelijke heeft gekregen, aldus de European Data Protection Board. De verwerker bepaalt per definitie niet het doel en de middelen van de persoonsgegevensver-

12 Rb. Noord-Nederland 20 december 2018, ECLI:NL:RBNNE:2018:5385, *Computerrecht*2019/53, m.nt. M.A.A. Oostveen.

13 WP29, Advies 1/2010 over de begrippen 'verantwoordelijke' en 'verwerker', (WP169), 16 februari 2010, p. 8-24.

14 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, Publicatieblad van de Europese Gemeenschappen L 281, 38e jaargang, 23 november 1995.

werking.¹⁵ Anders gezegd: hij voert ten aanzien van de persoonsgegevens tot op zekere hoogte het beleid uit van de verwerkingsverantwoordelijke.

Eigen keuzes verwerker

Dat neemt niet weg dat een verwerker op enkele punten wel eigen keuzes kan maken. Veelal wordt een verwerker juist ingeschakeld om zijn expertise, bijvoorbeeld een cloudleverancier. De cloudleverancier verzorgt de opslag van persoonsgegevens op zijn servers ten behoeve van de verwerkingsverantwoordelijke. Daarbij heeft hij geen zeggenschap over welke persoonsgegevens voor welke doeleinden worden opgeslagen. In die zin wordt slechts het beleid van de verwerkingsverantwoordelijke uitgevoerd. Echter, de cloudleverancier maakt wel eigen keuzes ten aanzien van bijvoorbeeld de technische wijze van opslag van de persoonsgegevens en de beveiliging van zijn servers. Dat de cloudleverancier ten aanzien van deze zaken keuzes maakt, betekent niet dat hij automatisch zeggenschap heeft over de te verwerken persoonsgegevens en dus verwerkingsverantwoordelijke is. Immers, de cloudleverancier wordt – gelet op zijn expertise – door de verwerkingsverantwoordelijke ingehuurd om de opslag van de persoonsgegevens te verzorgen. Daarmee bepaalt de verwerkingsverantwoordelijke het middel – ‘de cloudleverancier’ – voor de verwerking van persoonsgegevens, waaraan de cloudleverancier in opdracht gevolg geeft.

Aanwijzingen voor verwerkingsverantwoordelijkheid

De Autoriteit Persoonsgegevens geeft, aanvullend op de opinie van de European Data Protection Board, een aantal praktische aanwijzingen waarmee kan worden bepaald of een partij verwerkingsverantwoordelijke is. Volgens de Autoriteit Persoonsgegevens kan de toepasselijkheid van één of meerdere van de volgende criteria erop wijzen dat een betreffende partij verwerkingsverantwoordelijke is:

- het bepalen van de doeleinden voor de gegevensverwerking;
- het bepalen van de middelen die aangewend worden voor de verwerking;
- het bepalen welke gegevens worden verwerkt;
- het bepalen van de bewaartermijnen;
- het hebben van zeggenschap over de toegang tot de gegevens;
- het hebben van zeggenschap over de informatie die wordt verstrekt aan de betrokkene;
- het hebben van zeggenschap over het verstrekken van gegevens aan derden en/of naar partijen in landen buiten de EU;
- de contractuele afspraken over gegevensverwerking tussen partijen.”¹⁶

15 WP29, Advies 1/2010 over de begrippen ‘verantwoordelijke’ en ‘verwerker’, (WP169), 16 februari 2010, p. 24-30.

16 Autoriteit Persoonsgegevens, Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace, (z2014-00944), 13 oktober 2015, p. 36.

Wij zien in de praktijk dat partijen proberen om de verantwoordelijkheid bij een van de partijen neer te leggen door dat uitdrukkelijk in een verwerkersovereenkomst vast te leggen. Dat kan weliswaar een goed aanknopingspunt vormen, maar geeft niet de doorslag wanneer er in de praktijk feitelijk niet naar gehandeld wordt. Contracten en andere formeel-juridische bronnen zijn dus niet allesbepalend.¹⁷ Dit blijkt onder meer uit de Bluetrace-zaak; de kwestie waarin de Autoriteit Persoonsgegevens de hiervoor genoemde criteria heeft geformuleerd. In die zaak heeft een partij zichzelf in de door partijen getekende verwerkersovereenkomst aangemerkt als verwerker. Deze partij bleek echter feitelijk gezien een verwerkingsverantwoordelijke te zijn. Volgens de Autoriteit Persoonsgegevens was deze partij daarom, ondanks de door haar afgesloten verwerkersovereenkomst, geen verwerker en legde haar daarom een last onder dwangsom op voor het niet-naleven van diverse op de verwerkingsverantwoordelijke gerichte verplichtingen.¹⁸ Een last onder dwangsom is overigens niet hetzelfde als een boete. Het is een maatregel, een stok achter de deur, om een partij te bewegen een onrechtmatige situatie op te heffen.

Uitwisseling van persoonsgegevens tussen twee partijen

In de praktijk wordt vaak gedacht dat een partij een verwerker is op het moment dat die partij persoonsgegevens van een andere partij ontvangt. Dat is echter zeker niet altijd het geval. Indien bijvoorbeeld een openbare bibliotheek van een school persoonsgegevens van leerlingen ontvangt in het kader van een onderlinge samenwerking voor educatie-doeleinden, dan is de bibliotheek niet zonder meer een verwerker van de school. Er is dan eerder sprake van uitwisseling van persoonsgegevens tussen twee verwerkingsverantwoordelijken, te weten de bibliotheek en de school. De bibliotheek bepaalt in dat geval immers zelf op welke wijze zij de ontvangen persoonsgegevens zelf verder verwerkt. Zij krijgt daartoe geen specifieke opdracht tot verwerking van persoonsgegevens van de school.

Deze situatie kan voor partijen vreemd aanvoelen. In een dergelijk geval worden door verwerkingsverantwoordelijken, die dus letterlijk verantwoordelijk zijn voor de persoonsgegevens, de betreffende persoonsgegevens gedeeld met derde partijen, zonder dat er aanvullende afspraken (in een verwerkersovereenkomst) worden gemaakt met die partijen. Het maken van afspraken is wel verplicht als die andere partij een verwerker zou zijn. Waarom hoeft dat dan niet als de andere partij zelf een verwerkingsverantwoordelijke is? Het antwoord op die vraag is simpel: op de andere partij – die zelfstandig verwer-

17 Autoriteit Persoonsgegevens, Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace, (z2014-00944), 13 oktober 2015, p. 36.

18 Autoriteit Persoonsgegevens, Last onder dwangsom Bluetrace, (z2015-00981), 30 juni 2016, p. 6 en 7.

kingsverantwoordelijke is – rusten de verplichtingen uit de AVG immers rechtstreeks. In de situatie dat de partij die de persoonsgegevens ontvangt verwerker zou zijn, zouden deze verplichtingen worden opgelegd door middel van een verwerkersovereenkomst. Alhoewel wij het ongemakkelijke gevoel dat partijen hier soms bij kunnen hebben begrijpen, is er formeel-juridisch dus geen sprake van een lacune.

Primaire rol

Een ander element dat een rol speelt bij de vaststelling van de privacy-rol is de aard van de dienstverlening. Bestaat de dienstverlening van een partij primair uit het verwerken van persoonsgegevens of betreft die verwerking slechts een (noodzakelijk) uitvloeisel van een andere primaire dienst? Indien de verwerking van persoonsgegevens voornamelijk een noodzakelijk uitvloeisel van de betreffende dienst is, dan is dit een indicatie dat er géén sprake is van verwerkerschap in de zin van de AVG. Dit komt omdat die partij dan zelf bepaalt op welke wijze zij de persoonsgegevens aanwendt in haar dienstverlening. Denk bijvoorbeeld aan een advocaat die persoonsgegevens van zijn cliënt verwerkt bij de voorbereiding van een procedure voor de rechter. De verwerking van persoonsgegevens is dan een noodzakelijk uitvloeisel van zijn dienstverlening, maar niet het doel op zich. Bestaat de dienstverlening daarentegen primair uit het verwerken van persoonsgegevens – als de dienstverlening zich derhalve primair op ‘verwerken in de zin van de AVG’ richt – dan is dit juist een indicatie voor het zijn van verwerker.¹⁹

Hoe zit het nu met bibliotheken en archiefinstellingen? In beginsel zullen bibliotheken en archiefinstellingen aan te merken zijn als een verwerkingsverantwoordelijke voor de verwerking van de persoonsgegevens van bijvoorbeeld hun leden (in het geval van bibliotheken), of van de persoonsgegevens die zich in het archief bevinden (in het geval van archieven). Als zij delen van de op hun rustende verwerking uitbesteden aan een derde, bijvoorbeeld in het geval van lenersgegevens die in een SaaS-platform worden opgeslagen, dan zijn die derden aan te merken als een verwerker en dient er op grond van de AVG een verwerkersovereenkomst gesloten te worden.

Een archiefinstelling kan daarentegen onder omstandigheden mogelijk wel aangemerkt worden als verwerker. Gedacht kan worden aan de opslag van een particulier archief door de archiefinstelling. De archiefinstelling is dan voor die specifieke verwerking – de opslag van het betreffende particulier archief – een verwerker. In de meeste gevallen zullen archiefinstellingen echter wél zeggenschap hebben over de te verrichten archiefhandelingen, zoals het verschaf-

19 Autoriteit Persoonsgegevens, Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace, (z2014-00944), 13 oktober 2015, p. 36 en 37.

fen van inzage aan derden. In dat geval is de gegevensverwerking een noodzakelijk uitvloeisel uit de dienstverlening van de archiefinstelling en is zij een verwerkingsverantwoordelijke. De archiefinstelling dient daarom per soort verwerking van persoonsgegevens vast te stellen of zij verwerker of verwerkingsverantwoordelijke is.

Tot slot: In het geval er tussen partijen persoonsgegevens worden gedeeld, kent de AVG naast de verwerkingsverantwoordelijke-verwerker-relatie en de figuur van verschillende verwerkingsverantwoordelijken die naast elkaar zelfstandig verantwoordelijk zijn voor hun eigen deel van de verwerking, ook nog een ‘gezamenlijke verwerkingsverantwoordelijkheid’. In dat geval bepalen meerdere partijen gezamenlijk het doel en de middelen voor dezelfde verwerking. Daarvan is in de praktijk echter niet snel sprake en we laten deze figuur in dit artikel voor het overige dan ook buiten beschouwing. Mocht die situatie zich wel voordoen, dan verlangt de AVG dat er tussen partijen wél afspraken gemaakt worden.

7. Praktijkcasus werking AVG

In paragraaf 5 gaven wij aan dat het stramien van de AVG feitelijk in de volgende vier stappen uiteenvalt:

1. Is de AVG van toepassing? De AVG is van toepassing op de ‘verwerking van persoonsgegevens’.
2. Wat is de rol van de desbetreffende organisatie bij een specifieke soort persoonsgegevensverwerking: ‘verwerkingsverantwoordelijke’ of ‘verwerker’?
3. Als verwerkingsverantwoordelijke: is het vervolgens toegestaan de persoonsgegevens te verwerken? Is er een ‘doel’ en een ‘grondslag’? En in het geval van verwerking van bijzondere persoonsgegevens: is er een onthefing voor het verwerkingsverbod?
4. Als er op grond van het voorgaande mag worden verwerkt: hoe dan verder? Er moet immers worden voldaan aan de verplichtingen uit de AVG. Denk daarbij bijvoorbeeld aan het informeren van betrokkenen, het treffen van passende technische en organisatorische beveiligingsmaatregelen en het sluiten van verwerkersovereenkomsten met verwerkers.

Deze stappen in het stramien van de AVG lichten wij in de volgende praktijkcasus nader toe.

*Casus gezinskaarten*²⁰

Gemeenten waren in het verleden wettelijk verplicht om als onderdeel van de bevolkingsadministratie gezinskaarten bij te houden. De kaarten bevatten gegevens zoals de naam, het geslacht, adres(sen), geboortedatum en -plaats, burgerlijke staat, nationaliteit en het beroep. Daarnaast vermelden deze kaarten de ‘kerkelijke gezindte’ van de betrokkene. Op grond van de Archiefwet hebben de gemeenten deze gezinskaarten overgebracht naar een archiefinstelling. Deze archiefinstelling houdt nu een analoge verzameling van gezinskaarten uit de periode 1920-1939 bij. De archiefinstelling heeft daarbij de zeggenschap over het beheer en het bijhouden van deze verzameling. Zij heeft bijvoorbeeld zeggenschap over de vraag of een derde al dan niet deze verzameling kan inzien.

Wat moet de archiefinstelling in deze casus met de AVG? Wat de gemeenten in deze casus met de AVG moeten, laten wij hier – gezien de gekozen toelichting op het stramien van de AVG – buiten beschouwing.

1. Allereerst moet de vraag worden gesteld of de AVG wel van toepassing is. Er moet dan sprake zijn van het verwerken van persoonsgegevens in de zin van de AVG. In dat kader moeten we dus kijken naar de definities zoals die in paragraaf 4 zijn aangehaald. De archiefinstelling verkrijgt persoonsgegevens van de gemeenten en slaat deze op in haar archief. Alle handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen en het opslaan, zijn aan te merken als verwerkingen van persoonsgegevens. Er is derhalve sprake van een verwerking in de zin van de AVG. Zelfs wanneer de archiefinstelling niets actief doet met de persoonsgegevens (al kan dat op zichzelf worden betwist omdat de persoonsgegevens in het archief geordend en bijgehouden moeten worden), neemt dat niet weg dat er wel sprake is van een – alsdan weliswaar passieve – verwerking in de zin van de definitie uit de AVG.

De volgende vraag is of er wel sprake is van ‘persoonsgegevens’. Bij persoonsgegevens hebben we het over alle gegevens die te herleiden zijn tot een bepaalde natuurlijke persoon. Het behoeft geen uitleg dat de gegevens op gezins-

20 Momenteel bestaat in de archiefwereld veel onduidelijkheid over het ter beschikking stellen van gezinskaarten omdat daar persoonsgegevens in kunnen staan van personen die nog in leven zijn. Bovendien bevatten de gezinskaarten vaak bijzondere persoonsgegevens zoals kerkelijke gezindte. De ‘Beroeps- en Brancheverenigingen voor het archiefwezen KVAN-BRAN-werkgroep AVG’ heeft daarvoor in juni 2019 een ‘Model Data Protection Impact Assessment op de gezinskaarten van het bevolkingsregister (1920-1939)’, vastgesteld. Dat model is een hulpmiddel voor (samenwerkingsverbanden van) gemeenten en archiefinstellingen met een risicoanalyse van het openbaar maken van o.a. gezinskaarten van voor 1939.

kaarten persoonsgegevens zijn. Deze gegevens zijn immers te herleiden tot een individu.

Een ander punt van aandacht is dat de gezinskaarten analoog zijn. De persoonsgegevens worden in dit geval dus niet geheel of gedeeltelijk geautomatiseerd verwerkt en die eis wordt wel gesteld bij de toepasselijkheid van de AVG. Zoals eerder in dit artikel dus al is aangehaald, is de AVG óók van toepassing op verwerking van analoge gegevens, voor zover die gegevens in een bestand zitten of bestemd zijn om in een bestand te worden opgenomen. In dit geval betreffen het gegevens die bestemd zijn om in een bestand op te nemen. De gegevens zullen immers op een bepaalde gestructureerde manier toegankelijk zijn voor de medewerkers van de archiefinstelling en in beginsel ook voor derden.

Gezien het voorgaande is er in dit geval sprake van verwerking van persoonsgegevens en daarom is de AVG op deze specifieke verwerking van toepassing.

2. Vervolgens dient de archiefinstelling zich af te vragen wat de rol van haar organisatie in dezen is. Hoewel de archiefinstelling niet degene is die de persoonsgegevens op gezinskaarten initieel van de betrokkenen verzameld heeft, is zij in deze situatie aan te merken als verwerkingsverantwoordelijke. Zij heeft immers vanaf het moment van overbrenging van de gezinskaarten de zeggenschap over het doel en de middelen van de verwerking van persoonsgegevens. Zij heeft onder meer de zeggenschap over op welke wijze de gezinskaarten worden gearcheveerd en in hoeverre derden deze mogen inzien. Dat de gezinskaarten op grond van een wettelijke verplichting moeten worden overgebracht naar de archiefinstelling en door haar gearcheveerd moeten worden, doet daar niets aan af.

3. Nu vaststaat dat de archiefinstelling is aan te merken als een verwerkingsverantwoordelijke, dient zij te onderzoeken of zij de desbetreffende persoonsgegevensverwerking legitiem mag uitvoeren.

In dat kader zijn het gerechtvaardigd doel en de grondslag van belang. Voor de archiefinstelling is haar doel onder meer gelegen in het uitvoeren van haar wettelijke opdracht om haar collecties te beheren en voor huidige en toekomstige generaties toegankelijk te maken en te houden. De grondslag voor het archiveren betreft een wettelijke verplichting. In artikel 3 van de Archiefwet is immers de verplichting vastgelegd om archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren. Overigens dient de archiefinstelling voor elk specifiek deel van de verwerking te beschikken over een gerechtvaardigd doel en deze op een grondslag te baseren. Merk daarbij op dat deze vraag niet hetzelfde is als de vraag of alle gegevens wel noodzakelijk zijn.

Het kan best zo zijn dat de archiefinstelling bepaalde gegevens wil verwerken omdat zij daarbij een bepaald doel voor ogen heeft, maar dat die gegevens strikt genomen niet noodzakelijk zijn om haar doel tot het bijhouden van volledige en integere archieven uit te kunnen voeren. De noodzakelijkheidsvraag komt wel aan bod zodra het doel is vastgesteld. Immers, persoonsgegevens mogen alleen verwerkt worden als dat noodzakelijk is voor dat aldus vastgestelde doel.

Daarnaast is het van belang dat de op de gezinskaart vermelde religie een bijzonder persoonsgegeven betreft. De verwerking van bijzondere persoonsgegevens is echter in beginsel verboden, tenzij daarvoor een uitzondering bestaat. Voor archiefinstellingen is genoemde uitzondering opgenomen in artikel 2a van de Archiefwet, zodat zij in het kader van hun verplichtingen uit de Archiefwet wel bijzondere persoonsgegevens mogen verwerken. Verderop in dit artikel gaan wij dieper in op deze uitzondering voor het verwerken van bijzondere persoonsgegevens door archiefinstellingen.

4. De archiefinstelling moet vervolgens voldoen aan de eisen die de AVG stelt. Wat die eisen zijn lichten wij toe in de volgende paragraaf.

8. Enkele verplichtingen uit de AVG in vogelvlucht

De meeste verplichtingen uit de AVG rusten op de verwerkingsverantwoordelijke. Het woord zegt het immers al: de verwerkingsverantwoordelijke is in hoofdzaak verantwoordelijk voor de verwerking die onder zijn auspiciën plaatsvindt. In beginsel geldt dat ook voor de verwerking die de verwerker ten behoeve van de verwerkingsverantwoordelijke uitvoert (al heeft de verwerker ook een zelfstandige verantwoordelijkheid). Hierna volgt een aantal belangrijke verplichtingen die rusten op verwerkingsverantwoordelijken.

8.1 *Persoonsgegevens verwerken op rechtmatige, behoorlijke en transparante wijze*

Allereerst geldt als algemeen uitgangspunt dat de verwerkingsverantwoordelijke de persoonsgegevens op een rechtmatige, behoorlijke en transparante wijze dient te verwerken.²¹ Het verwerken van persoonsgegevens dient te allen tijde conform dit algemene beginsel te geschieden. Dit beginsel vormt een ‘kapstokbepaling’, die in de AVG nader wordt geconcretiseerd in andere bepalingen.

21 Artikel 5 lid 1 sub a AVG.

gen. De verwerkingsverantwoordelijke moet onder andere te allen tijde kunnen aantonen dat alle persoonsgegevensverwerkingen onder zijn verantwoordelijkheid in overeenstemming met de AVG geschieden (het verantwoordingsbeginsel).²² Deze verplichting komt in de praktijk neer op een ‘documentatieplicht’ voor de verwerkingsverantwoordelijke. Hij dient vast te leggen op welke wijze hij er zorg voor draagt dat persoonsgegevensverwerking in overeenstemming is met het bepaalde in de AVG. Voor de verwerkingsverantwoordelijke is het derhalve van belang om inzichtelijk te hebben welke (categorieën van) persoonsgegevens hij exact verwerkt. Vervolgens zal moeten worden nagegaan of al deze verwerkingen op rechtmatige wijze en in overeenstemming met de AVG geschieden.

8.2 Register van verwerkingsactiviteiten

Dit inzicht kan in eerste instantie worden verkregen door het aanleggen van een ‘register van verwerkingsactiviteiten’. Middels dit register wordt inzichtelijk gemaakt of de verwerking van persoonsgegevens rechtmatig geschiedt en of er nog specifieke aandachtspunten zijn om conform de AVG te handelen. In de meeste gevallen is een verwerkingsverantwoordelijke verplicht om een register van verwerkingsactiviteiten bij te houden.²³

Dit register dient voor de verwerkingsverantwoordelijke in ieder geval de volgende informatie te bevatten:²⁴

1. de naam en contactgegevens van de verwerkingsverantwoordelijke alsmede van een eventueel aangestelde functionaris voor de gegevensbescherming;
2. de verwerkingsdoeleinden;
3. een beschrijving van de categorieën persoonsgegevens die worden verwerkt en de categorieën van betrokkenen waar die persoonsgegevens betrekking op hebben;
4. de categorieën van ontvangers aan wie de persoonsgegevens worden verstrekt, waaronder ook worden verstaan de verwerkers;
5. indien van toepassing, de doorgiften van persoonsgegevens aan derde landen of internationale organisaties inclusief de vermelding daarvan alsmede de getroffen passende waarborgen;
6. de beoogde bewaartermijnen van persoonsgegevens;
7. een algemene omschrijving van de getroffen technische en organisatorische beveiligingsmaatregelen.

²² Artikel 5 lid 2 AVG.

²³ Artikel 30 AVG.

²⁴ Artikel 30 lid 1 AVG.

Op verzoek dient de verwerkingsverantwoordelijke een dergelijk register aan de Autoriteit Persoonsgegevens ter beschikking te stellen. Deze registerplicht stelt de Autoriteit Persoonsgegevens in staat om haar toezicht uit te oefenen en draagt bij aan het hiervoor genoemde verantwoordingsbeginsel en de hiervoor genoemde documentatieplicht.

Ook de verwerker is zelfstandig verplicht om een dergelijk register bij te houden. De informatie die de verwerker in het register dient op te nemen is gericht op de verwerkingsactiviteiten die zij ten behoeve van verwerkingsverantwoordelijken verricht. Dit register bevat bijvoorbeeld informatie over de categorieën van verwerkingen die ten behoeve van de verwerkingsverantwoordelijke worden uitgevoerd, om welke verwerkingsverantwoordelijken het gaat, et cetera.

8.3 *Verwerking volgens welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden*

Zoals eerder uitvoerig aangehaald, mogen persoonsgegevens slechts worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.²⁵ Deze doeleinden vormen een belangrijke basis voor het rechtmatig verwerken van persoonsgegevens:

- De verzamelde persoonsgegevens mogen enkel worden verwerkt voor zover dat noodzakelijk is om de vooraf vastgestelde doeleinden te behalen. In beginsel is het niet toegestaan om de persoonsgegevens verder te verwerken op een wijze die onverenigbaar is met de vooraf vastgestelde doeleinden ('doelbinding'). Het kan 'handig' zijn om bepaalde persoonsgegevens, die de verwerkingsverantwoordelijke reeds in bezit heeft, te gebruiken voor andere zaken zoals marketing. Dit is echter niet zonder meer toegestaan, bijvoorbeeld in het geval de persoonsgegevens in eerste instantie voor andere doeleinden zijn verkregen.
- De persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is om de vooraf vastgestelde doeleinden te behalen.²⁶ Op het moment dat de persoonsgegevens niet meer nodig zijn om deze doeleinden te behalen, dan dienen zij in beginsel te worden verwijderd ('opslagbeperking'). Dit uitgangspunt geldt tenzij er een wettelijke bewaartermijn geldt. In dat geval dienen de persoonsgegevens bewaard te worden conform die termijn, ook als het oorspronkelijke doel is bereikt.
- De vooraf vastgestelde doeleinden bakenen bovendien af welke persoonsgegevens de verwerkingsverantwoordelijke mag verzamelen en ver-

²⁵ Artikel 5 lid 1 sub b AVG.

²⁶ Artikel 5 lid 1 sub e AVG.

werken. Persoonsgegevens moeten namelijk toereikend zijn, ter zake dienend en beperkt tot datgene wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking' of 'data-minimalisatie').²⁷ Oftewel, indien het niet noodzakelijk is om bepaalde persoonsgegevens te verwerken om een bepaald doeleinde te behalen, dan is het ook niet toegestaan om de betreffende persoonsgegevens te verwerken.

4 Het informeren van betrokkenen over de persoonsgegevensverwerkingen

De verwerkingsverantwoordelijke is verplicht om betrokkenen te informeren over de verwerking van hun persoonsgegevens. Hoe hij dat moet doen is uitgewerkt in de artikelen 12, 13 en 14 van de AVG.

In de praktijk wordt regelmatig gebruikgemaakt van zogenaamde 'privacyverklaringen'. Een AVG-conforme privacyverklaring bevat onder meer een omschrijving van de verwerkingsdoeleinden waarvoor de persoonsgegevens van een betrokkene worden verwerkt en de vermelding van de verwerkingsgrondslagen. Daarnaast dient in een privacyverklaring informatie te worden verstrekt over de eventuele verstrekking van persoonsgegevens van de betrokkene aan een derde en de bewaartermijn die wordt gehanteerd. Bovendien is het van belang om de betrokkene te informeren over zijn rechten, zoals het recht op inzage, rectificatie, vergetelheid en dataportabiliteit (gegevensoverdraagbaarheid). Wanneer de persoonsgegevens niet van de betrokkene zelf zijn verkregen, dient tot slot ook te worden geïnformeerd over de 'bron' waar de persoonsgegevens vandaan komen.²⁸ Overigens bevat de AVG meer voorschriften voor de inhoud van privacyverklaringen. Het voert echter te ver om in het bestek van deze bijdrage al deze verplichtingen te bespreken. De genoemde informatieverplichtingen gelden overigens niet wanneer de betrokkene reeds over de informatie beschikt. Met name in het geval van archieven zijn de persoonsgegevens veelal niet van de betrokkene zelf verkregen en is het in de praktijk vaak vrijwel onmogelijk om de informatie specifiek aan alle betrokkenen te verstrekken. Derhalve voorziet de AVG in een uitzondering voor archieven. Deze uitzondering komt later in dit artikel aan de orde.

²⁷ Artikel 5 lid 1 sub c AVG.

²⁸ Artikelen 12, 15 tot en met 22 AVG.

8.5 *Rechten van betrokkenen*

De AVG kent aan de betrokkenen diverse rechten toe. Betrokkenen kunnen deze rechten uitoefenen jegens de verwerkingsverantwoordelijke. Een greep uit deze rechten:

- Het recht op inzage, waarbij de betrokkene van de verwerkingsverantwoordelijke uitsluitend dient te krijgen of zijn persoonsgegevens worden verwerkt en, indien dat het geval is, om welke persoonsgegevens het gaat.²⁹ De verwerkingsverantwoordelijke dient daarbij de betrokkene onder andere te informeren over de verwerkingsdoeleinden, om welke categorieën persoonsgegevens het gaat, aan welke derden de persoonsgegevens worden verstrekt, et cetera. In beginsel moet de verwerkingsverantwoordelijke een kopie van de persoonsgegevens die worden verwerkt, verstrekken aan de betrokkene.
- Het recht op rectificatie.³⁰ De onjuiste of onvolledige persoonsgegevens dienen op verzoek van de betrokkene onverwijld te worden verbeterd of aangevuld.
- Het recht op ‘vergetelheid’.³¹ De verwerkingsverantwoordelijke dient de persoonsgegevens op verzoek van de betrokkene onder bepaalde omstandigheden te wissen. De betrokkene kan daarom verzoeken in situaties waarin de persoonsgegevens bijvoorbeeld 1) niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld, 2) de betrokkene zijn toestemming voor de verwerking intrekt of 3) als de persoonsgegevens anderszins onrechtmatig worden verwerkt. De wet kent daarnaast nog een aantal andere situaties waarin een verzoek tot verwijdering van persoonsgegevens kan worden gedaan. De betrokkene kan echter niet zonder meer aanspraak maken op de verwijdering van persoonsgegevens. Zo mag het verzoek tot verwijdering niet aan het uitoefenen van het recht op vrijheid van meningsuiting en informatie in de weg staan. Ook als de verwerkingsverantwoordelijke wettelijk verplicht is om te verwerken, gaat een verzoek tot verwijdering niet op. Tevens is voorzien in een uitzondering voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. In dat geval dienen wel extra waarborgen getroffen te worden. Verderop in dit artikel gaan we nader in op deze specifieke uitzondering.
- Het recht op beperking van de verwerking.³² De betrokkene kan in sommige gevallen de verwerking van zijn persoonsgegevens door de verwer-

29 Artikel 15 AVG.

30 Artikel 16 AVG.

31 Artikel 17 AVG.

32 Artikel 18 AVG.

kingsverantwoordelijke beperken. Bijvoorbeeld als hij juistheid van zijn persoonsgegevens betwist. In dat geval dient de verwerkingsverantwoordelijke de verwerking te beperken gedurende de periode waarin hij de juistheid van de persoonsgegevens controleert. Beperking van de verwerking houdt in dat de verwerkingsverantwoordelijke de persoonsgegevens in beginsel, behoudens de loutere opslag, niet mag verwerken.

- Het recht op gegevensoverdraagbaarheid.³³ De betrokkene kan in bepaalde gevallen verlangen dat de persoonsgegevens die hij aan de verwerkingsverantwoordelijke heeft verstrekt aan hem worden overgedragen. Ook kan hij in die gevallen verlangen dat zijn persoonsgegevens rechtstreeks worden overdragen aan een andere verwerkingsverantwoordelijke. De betrokkene heeft dit recht wanneer zijn persoonsgegevens via automatische procedés worden verwerkt en hij daarvoor zijn toestemming heeft gegeven of wanneer de verwerking nodig is voor de uitvoering van de overeenkomst die hij gesloten heeft. De verwerkingsverantwoordelijke dient de persoonsgegevens in een gestructureerd, gangbaar en machineleesbaar formaat over te dragen, dat wil zeggen op een interoperabele wijze, zonder de betrokkene in dat kader te hinderen.
- Het recht op bezwaar.³⁴ De betrokkene kan te allen tijde bezwaar maken tegen de verwerking van persoonsgegevens wanneer de verwerking:
 - wordt gebaseerd op de verwerkingsgrondslag ‘de vervulling van een taak van algemeen belang of het openbaar gezag’ (voor overheids- of andere publiekrechtelijke organisaties); of
 - wordt gebaseerd op de verwerkingsgrondslag ‘het gerechtvaardigd belang’; of
 - geschiedt voor direct marketing.
- De verwerkingsverantwoordelijke dient in dat geval in beginsel de betreffende verwerking te staken. Het recht van bezwaar kan bijvoorbeeld ertoe leiden dat de verwerkingsverantwoordelijke, die de verwerking baseert op gerechtvaardigde belangen, opnieuw een belangenafweging maakt met inachtneming van het gemaakte bezwaar. Ook indien de persoonsgegevens worden verwerkt met het oog op archivering in het algemeen belang of wetenschappelijk, historisch of statistisch onderzoek heeft de betrokkene het recht om bezwaar te maken, tenzij de verwerking wordt gebaseerd op de verwerkingsgrondslag ‘de vervulling van een taak van algemeen belang’.

33 Artikel 20 AVG.

34 Artikel 21 AVG.

8.6 *Beveiliging via passende technische en organisatorische maatregelen*

De verwerkingsverantwoordelijke moet passende technische en organisatorische maatregelen (laten) nemen om de persoonsgegevens te beveiligen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.³⁵ In dit verband rust de plicht om datalekken aan de Autoriteit Persoonsgegevens – en onder omstandigheden óók aan de betrokkene – te melden, dan ook bij de verwerkingsverantwoordelijke.³⁶

De verwerker heeft een zelfstandige plicht om persoonsgegevens die hij onder zich heeft adequaat te beveiligen; derhalve ook de persoonsgegevens die afkomstig zijn van de verwerkingsverantwoordelijke ten behoeve waarvan hij een deel van de verwerking op zich neemt.³⁷

8.7 *Meldplicht datalekken*

De verwerkingsverantwoordelijke heeft op grond van artikel 33 en 34 AVG een meldplicht in geval van een inbreuk in verband met persoonsgegevens (een ‘datalek’). Wanneer er een datalek heeft plaatsgevonden dat waarschijnlijk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dan heeft de verwerkingsverantwoordelijke de plicht om dit zonder onredelijke vertraging te melden aan de Autoriteit Persoonsgegevens. Kan het datalek niet binnen 72 uur na ontdekking daarvan gemeld worden, dan dient de melding vergezeld te gaan met een motivering van de vertraging.

Houdt het datalek een hoog risico in voor de rechten en vrijheden van natuurlijke personen, dan dient de verwerkingsverantwoordelijke het datalek tevens aan de betrokkene(n) te melden, tenzij de betreffende persoonsgegevens onbegrijpelijk zijn gemaakt voor onbevoegden (bijvoorbeeld versleuteld), maatregelen zijn genomen waardoor het hoge risico zich waarschijnlijk niet meer zal voordoen of de mededeling onredelijke inspanningen zou vergen en de betrokkenen via een openbare mededeling of soortgelijke maatregel worden geïnformeerd.

Een melding omvat in ieder geval de aard van de inbreuk, de waarschijnlijke gevolgen, de maatregelen die zijn voorgesteld of genomen om de inbreuk aan te pakken en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt. Tot slot dienen alle datalekken die zich hebben

35 Artikel 5 lid 1 sub f en artikel 32 AVG.

36 Artikelen 33 en 34 AVG.

37 Artikel 32 AVG.

voorgedaan – ook die niet gemeld zijn bij de Autoriteit Persoonsgegevens –, tezamen met de feiten, gevolgen en genomen maatregelen, door de verwerkingsverantwoordelijke te worden gedocumenteerd.

8.8 *Privacy by design / privacy by default*

Op grond van artikel 25 AVG dient de verwerkingsverantwoordelijke bij het ontwerp van zijn diensten en/of producten al rekening te houden met de persoonsgegevensbescherming. Achteraf moet hij ook kunnen aantonen dit te hebben gedaan. Dit wordt *privacy by design* genoemd. Denk hierbij bijvoorbeeld aan het versleutelen van persoonsgegevens of het inbouwen van toegangsbeheer in een systeem. Met dat laatste wordt voorkomen dat medewerkers die daartoe niet bevoegd zijn, inzicht krijgen in bepaalde gegevens. Daarmee wordt invulling gegeven aan de (interne) verplichting tot dataminimalisatie; het niet méér gegevens verwerken dan noodzakelijk.

Daarnaast dient de verwerkingsverantwoordelijke ervoor te zorgen dat de standaardinstellingen van zijn diensten en/of producten altijd zo privacy-vriendelijk mogelijk zijn. Indien de gebruiker bijvoorbeeld kan kiezen hoeveel informatie hij wil delen, dient de standaardinstelling te zijn dat alleen de persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Dit wordt *privacy by default* genoemd. Denk hierbij bijvoorbeeld aan het opstellen van een invulformulier voor het aanvragen van een bepaalde dienst. Vaak wordt het invullen van een aantal velden verplicht gesteld (vaak aangeduid door middel van een ‘*’). Er zouden conform het privacy by default-uitgangspunt niet meer velden verplicht mogen zijn dan strikt noodzakelijk is voor het uitvoeren van verwerkingsdoel. Een ander voorbeeld is het zogenaamde ‘opt-in/out-vinkje’, dat men online veel tegen komt, bijvoorbeeld bij het aanmelden van een nieuwsbrief. Conform het uitgangspunt zou dat vinkje niet al aangezet mogen zijn (opt-out), maar moet de betrokkene de vrije mogelijkheid hebben om dat vinkje zelf te zetten (opt-in).

8.9 *(D)PIA*

Wanneer een soort verwerking waarschijnlijk een hoog privacyrisico inhoudt, dient de verwerkingsverantwoordelijke vóórafgaand aan de verwerking een beoordeling uit te voeren om deze privacyrisico’s in kaart te brengen.³⁸ Dit wordt ook wel een *Data Protection Impact Assessment* (DPIA) genoemd.

38 Artikel 35 AVG.

Deze verplichting geldt in het bijzonder indien nieuwe technologieën worden gebruikt. De Autoriteit Persoonsgegevens heeft een lijst openbaar gemaakt van het soort verwerkingen waarvoor een DPIA verplicht is. Een DPIA bevat ten minste een beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden, een beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden, een beoordeling van de privacyrisico's en de beoogde maatregelen om de risico's aan te pakken. Het doel van een DPIA is om vooraf de eventuele privacyrisico's te minimaliseren.

8.10 *Functionaris Gegevensbescherming*

De verwerkingsverantwoordelijke en de verwerker kunnen een functionaris voor gegevensbescherming (FG) aanwijzen die onder meer toeziet op naleving van de AVG, nationale wetgeving en het interne privacybeleid, alsmede daarover intern informeert en adviseert. De FG adviseert desgevraagd bij een DPIA en werkt samen met de Autoriteit Persoonsgegevens. In sommige gevallen is het verplicht om een FG aan te wijzen, namelijk indien:³⁹

- de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan (met uitzondering van gerechten bij de uitoefening van hun rechterlijke taken);
- de verwerkingsverantwoordelijke of verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, omvang en/of doeleinden regelmatig en stelselmatige observatie op grote schaal van betrokkenen vereisen;
- de verwerkingsverantwoordelijke of verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere of strafrechtelijke persoonsgegevens.

Lidstaten van de EU kunnen daarnaast ook in nationale regelgeving andere situaties aanwijzen waarvoor het aanstellen van een FG verplicht is. De FG wordt aangewezen op grond van zijn professionele kwaliteiten en zijn deskundigheid ter zake privacybescherming en privacywetgeving, en kan zowel een medewerker als iemand van buiten de organisatie zijn. Let er overigens op dat de FG een bijzondere positie in de organisatie bekleedt en dat hij niet ontslagen of gestraft kan worden in verband met de wijze waarop hij zijn taken uitvoert.⁴⁰

39 Artikel 37 AVG.

40 Artikel 38 lid 3 AVG.

8.11 Verwerkersovereenkomst

Naast de hiervoor genoemde verplichtingen zijn zowel de verwerkingsverantwoordelijke als de verwerker verplicht om een verwerkersovereenkomst aan te gaan, op het moment dat er een verwerker betrokken is bij de verwerking van persoonsgegevens.⁴¹

Uit de AVG volgt dat een verwerkingsverantwoordelijke alleen een verwerker mag inschakelen die ‘afdoende garanties’ kan bieden met betrekking tot de naleving van de AVG.⁴² Deze garanties hebben met name betrekking op de deskundigheid en betrouwbaarheid van de verwerker.

Wanneer biedt een verwerker nu afdoende garanties met betrekking tot de naleving van de AVG? In de praktijk is dit nog niet geheel uitgekristalliseerd. De verwerker kan bijvoorbeeld aansluiten bij gedragscodes, bepaalde NEN-en/of ISO-normen of – in de toekomst – bij certificeringsmechanismes die door de Autoriteit Persoonsgegevens alsdan zijn goedgekeurd.

De verwerkingsverantwoordelijke en de verwerker zijn verplicht om in een overeenkomst of bij een andere bindende rechtshandeling afspraken te maken over de verwerking van de persoonsgegevens. In de praktijk wordt vaak gebruikgemaakt van een verwerkersovereenkomst. De verwerkersovereenkomst dient schriftelijk, al dan niet elektronisch, te zijn.⁴³

De AVG stelt diverse eisen aan de inhoud van de verwerkersovereenkomst. De volgende onderwerpen dienen tenminste in deze overeenkomst te worden geregeld:⁴⁴

1. Een beschrijving van het onderwerp van de persoonsgegevensverwerking, zoals een omschrijving in welk kader de verwerking door de verwerker wordt uitgevoerd. Bijvoorbeeld in het kader van de afname van een IT-systeem.
2. De duur van de verwerking. Voor welke periode wordt gebruikgemaakt van de verwerkingsdiensten van de verwerker?
3. De aard en het doel van de persoonsgegevensverwerking. Welke verwerkingsactiviteiten voert de verwerker uit en wat is het doel van die verwerking?
4. Een omschrijving van het soort persoonsgegevens die de verwerker ten behoeve van de verwerkingsverantwoordelijke zal gaan verwerken. Ook

41 Artikel 28 AVG.

42 Artikel 28 lid 1 AVG.

43 Artikel 28 lid 9 AVG.

44 Artikel 28 lid 3 AVG.

dienen de categorieën van betrokkenen, op wie de persoonsgegevens betrekking hebben, benoemd te worden.

5. De rechten en plichten van de verwerkingsverantwoordelijke.
6. De verplichting voor de verwerker om de persoonsgegevens uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijke te verwerken, tenzij de wet- en regelgeving anders bepalen. Deze verplichting dient eveneens te gelden voor de doorgifte van persoonsgegevens door de verwerker naar landen buiten de Europees Economische Ruimte of aan internationale organisaties die ook vestigingen daarbuiten hebben.
7. De verwerker dient te waarborgen dat enkel de daartoe gemachtigde personen toegang hebben tot de persoonsgegevens alsmede dat zij gebonden zijn om deze vertrouwelijk te behandelen en gebonden zijn aan geheimhouding.
8. De verplichting voor de verwerker om de persoonsgegevens in overeenstemming met de daarvoor geldende eisen uit hoofde van de AVG op een passende, technische en organisatorische wijze te beveiligen.
9. De verwerker dient te allen tijde over een voorafgaande toestemming van de verwerkingsverantwoordelijke te beschikken om sub-verwerkers te mogen inschakelen. Daarnaast dienen de overige eisen die de AVG stelt aan het inschakelen van sub-verwerkers door de verwerker worden vastgelegd in de verwerkersovereenkomst.
10. In de verwerkersovereenkomst dienen diverse bijstandsverplichtingen voor de verwerker worden vastgelegd. Bijvoorbeeld de verplichting om bijstand te verlenen bij de afhandeling van een datalek of om de verwerkingsverantwoordelijke bij te staan bij het beantwoorden van verzoeken van betrokkenen die hun rechten uitoefenen.
11. De verplichting voor de verwerker om na afloop van de verwerkingsdiensten de persoonsgegevens – naar keuze van de verwerkingsverantwoordelijke – te wissen of terug te bezorgen aan de verwerkingsverantwoordelijke, waarbij bestaande kopieën worden verwijderd, tenzij de wet- en regelgeving anders bepalen.
12. De verplichting voor de verwerker om alle nodige informatie aan de verwerkingsverantwoordelijke ter beschikking te stellen om de nakoming van de verwerkersovereenkomst door de verwerker aan te tonen. In dit verband dient de verwerker audits, waaronder inspecties, door of namens de verwerkingsverantwoordelijke mogelijk te maken en eraan bij te dragen.

9. Verhouding AVG tot Archiefwet en Wet openbaarheid van bestuur (Wob)

De AVG is van toepassing als er binnen een archiefinstelling of bibliotheek persoonsgegevens worden verwerkt. Dit neemt niet weg dat daarnaast andere wetgeving van toepassing kan zijn. In deze paragraaf gaan we nader in op de verhouding tussen de algemene privacywet- en regelgeving (de AVG en UAVG) enerzijds en anderzijds de specifieke regels uit hoofde van de Archiefwet en de Wet openbaarheid van bestuur (Wob).

9.1 De Archiefwet en privacy

De Archiefwet 1995 regelt de verplichtingen die overheidsorganen hebben ten aanzien van archiefbescheiden. Het uitgangspunt van de Archiefwet is de openbaarheid van de documenten. De Archiefwet gaat in dit kader uit van een zogenaamd ‘documentenstelsel’ (in plaats van ‘informatiestelsel’ zoals bijvoorbeeld de Wob kent). In beginsel heeft men op basis van de Archiefwet dus recht op inzage in het gehele document of om een kopie daarvan te verkrijgen. Het informatiestelsel zoals de Wob dat kent omvat daarentegen het recht op de informatie, die neergelegd is in de documenten. Het informatiestelsel biedt derhalve – in tegenstelling tot een documentenstelsel – de mogelijkheid om samenvattingen uit of inlichtingen over de informatie uit de betreffende documenten te verstrekken. Ook kan op grond van het informatiestelsel een document eerst geanonimiseerd worden door het ‘weglakken’ van gegevens voordat dit document openbaar gemaakt wordt. Daarin zit het verschil met het openbaarheidsbeginsel uit de Archiefwet, dat niet is gekoppeld aan informatie in de documenten maar aan documenten in het geheel. De archiefbescheiden zijn dus in principe geheel openbaar. In die zin strookt de gedachte achter de Archiefwet niet altijd met het uitgangspunt van de AVG waarin onder andere dataminimalisatie een belangrijk beginsel is. Op voornoemd uitgangspunt zijn echter uitzonderingen mogelijk.

Overheidsorganen zijn verplicht de onder hen berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren alsmede zorg te dragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden.⁴⁵ De term ‘overheidsorgaan’ dient in dit verband ruim te worden opgevat. De Archiefwet is bijvoorbeeld ook van toepassing op universiteiten en (academische) ziekenhuizen. Alle overheidsorganen als bedoeld in de Algemene Wet Bestuursrecht (hierna: ‘Awb’) vallen onder de werking van

45 Artikel 3 Archiefwet.

de Archiefwet. Ook die organen, die juist van de werking van de Awb zijn uitgezonderd.

Overbrenging Archiefbewaarplaats

De Archiefwet legt aan de zogenaamde ‘zorgdrager’ binnen het overheidsorgaan de zorg voor de archiefbescheiden op. De Archiefwet maakt een onderscheid in de zorg voor archieven vóór overbrenging naar een zogenaamde archiefbewaarplaats en de zorg voor de archiefbescheiden ná een dergelijke overbrenging. De archiefbewaarplaats is een bewaarplaats voor de blijvende bewaring van archiefbescheiden. Overbrenging dient in beginsel na 20 jaar te geschieden.⁴⁶ Dat wil echter niet zeggen dat alle bescheiden worden overgedragen naar een zogenaamde archiefbewaarplaats. De zorgdrager is verplicht om op grond van zogenaamde selectielijsten te bepalen welke archiefbescheiden voor overbrenging in aanmerking komen. De archiefbescheiden die niet worden overgedragen worden vervolgens op basis van die selectiecriteria vernietigd.⁴⁷

Na overbrenging zijn de archiefbescheiden op grond van artikel 14 van de Archiefwet in beginsel openbaar. Eenieder is, behoudens de beperkingen die voortvloeien uit Archiefwet, bevoegd de archiefbescheiden kosteloos te raadplegen. Het is overigens ook mogelijk dat particuliere archieven in een archiefbewaarplaats worden opgenomen. Zulks geschiedt vrijwillig op basis van bijvoorbeeld een schenkings- of bruikleenovereenkomst. Men kan in een dergelijke overeenkomst beperkingen op de openbaarheid overeenkomen.

Beperkingen openbaarheid op grond van eerbiediging persoonlijke levenssfeer

Op het moment van overbrenging, dus na 20 jaar, kan de zorgdrager beperkingen aan de openbaarheid stellen, voor een bepaalde termijn.⁴⁸ Dat betekent dat het desbetreffende document voor die periode in principe niet openbaar is. Die termijn is maximaal 75 jaar, tenzij de minister van Onderwijs, Cultuur en Wetenschap, of in voorkomend geval de gedeputeerde staten, anders besluit.⁴⁹ De zorgdrager kan slechts beperkingen aan de openbaarheid stellen voor zover dat noodzakelijk is in het kader van een van de drie, in artikel 15 Archiefwet, genoemde gronden.

46 Artikel 12 Archiefwet.

47 Artikel 5 Archiefwet.

48 Artikel 15 lid 1 Archiefwet.

49 Artikel 15 lid 4 Archiefwet.

In dit artikel zoomen wij in op de beperkingsgrond ‘eerbiediging van de persoonlijke levenssfeer’.⁵⁰ Als de overgebrachte documenten gegevens bevatten die – indien zij openbaar zouden zijn – gevolgen zouden kunnen hebben voor de persoonlijke levenssfeer van de betrokkenen, kan dat een reden zijn om de openbaarheid van de desbetreffende documenten beperken. De eerbiediging van de persoonlijke levenssfeer staat echter niet zonder meer gelijk aan het begrip persoonsgegevens in de AVG. De term ‘persoonlijke levenssfeer’ is ruimer dan het begrip ‘persoonsgegevens’. De persoonlijke levenssfeer omvat onder meer het recht op bescherming van de identiteit, persoonlijke ontwikkeling en het recht om relaties aan te gaan en te ontwikkelen met andere mensen.⁵¹ Weliswaar zal er bij afweging van de vraag of de openbaarheid van een document op grond van de bescherming van de persoonlijke levenssfeer beperkt moet worden, per definitie sprake zijn van verwerking van persoonsgegevens in het desbetreffende document. Nu openbaarheid het uitgangspunt is bij de Archiefwet is het echter niet zo dat het enkele feit dat er sprake is van een persoonsgegeven, dát per definitie een beperking van die openbaarheid zou rechtvaardigen. Dat er persoonsgegevens in het document staan betekent niet zonder meer dat er sprake is van een inbreuk op de persoonlijke levenssfeer van de betrokkene. In paragraaf 5 hebben wij immers toegelicht dat de AVG het verwerken van persoonsgegevens in beginsel niet verbiedt, maar dat er juist kaders worden gesteld waarbinnen deze op rechtmatige wijze verwerkt kunnen worden.

Pas ná overbrenging van archiefbescheiden naar een archiefbewaarplaats, dus na 20 jaar, is het beginsel van openbaarheid op grond van de Archiefwet van toepassing.⁵² De eventuele beperkingen op de openbaarheid op grond van de eerbiediging van de persoonlijke levenssfeer uit hoofde van de Archiefwet spelen derhalve pas na de overbrenging van de archiefbescheiden. Vóór de overbrenging kan informatie eventueel op grond van de Wob openbaar zijn.⁵³ De Wob kent overigens een vergelijkbare mogelijkheid om de openbaarheid te beperken op grond van de eerbiediging van de persoonlijke levenssfeer. In paragraaf 9.2 gaan wij nader in op de Wob. Niettegenstaande de (beperking van de) openbaarheid dient de initiële verwerking van persoonsgegevens vóór de overbrenging uiteraard in lijn te zijn met de eisen die de AVG daaraan stelt. Ook ná de overbrenging dienen de persoonsgegevens in de archiefbewaarplaats in overeenstemming met de AVG verwerkt te worden. De Archiefwet

50 Ten aanzien van milieu-informatie gelden afwijkende regels met betrekking tot het kunnen stellen van beperkingen aan de openbaarheid van archiefbescheiden.

51 CBP Richtsnoeren: Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer, VI, p. 8.

52 Artikel 14 Archiefwet.

53 Artikel 2 Wob.

kent een eigen toets voor de vraag of de openbaarheid van archiefbescheiden al dan niet – bijvoorbeeld op basis van de eerbiediging van de persoonlijke levenssfeer – beperkt moeten worden. Dit is een andere toets dan de vraag of de verwerking van persoonsgegevens rechtmatig is op grond van de AVG.

Bij overbrenging van archiefbescheiden naar een archiefbewaarplaats dient in het kader van privacy dus eerst vastgesteld te worden óf er een inbreuk wordt gemaakt op de persoonlijke levenssfeer van de betrokkene. Daarbij geldt dat een betrokkene erop moet kunnen vertrouwen dat de privacygevoelige gegevens die aan de overheid verstrekt zijn niet zomaar openbaar gemaakt kunnen worden. Van een inbreuk op de persoonlijke levenssfeer kan bijvoorbeeld sprake zijn wanneer de betrokkene reputatieschade of financiële schade zou lijden, dan wel er afbeeldingen of informatie over het gedrag van de betrokkene openbaar gemaakt worden. Daarnaast kan de mate van gevoeligheid van de gegevens in de archiefbescheiden, zoals bijzondere persoonsgegevens als bedoeld in de AVG, een indicatie zijn bij het beperken van de openbaarheid.

Ten aanzien van gegevens over het publieke optreden of het ambtelijk functioneren van een betrokkene kan daarentegen in principe geen beroep worden gedaan op de persoonlijke levenssfeer als weigeringsgrond voor openbaarmaking. De persoonlijke levenssfeer is doorgaans niet in het geding voor zover de gegevens uitsluitend het beroepshalve functioneren van bijvoorbeeld een ambtenaar betreffen. Het gaat daarbij om gegevens die betrekking hebben op het beroepsmatig handelen van een overheidsfunctionaris in de normale uitoefening van de opgedragen taken ten behoeve van het bestuursorgaan. In dit kader dient wel onder andere rekening gehouden te worden met de bekendheid van de betreffende persoon: naarmate een ambtenaar meer bekendheid geniet, zullen zijn persoonsgegevens minder bescherming genieten.⁵⁴ Met andere woorden: aan documenten over een burgemeester zullen minder snel openbaarmakingsbeperkingen mogen worden gesteld, dan aan documenten die persoonsgegevens bevatten over een gemiddelde ambtenaar.

Bij de vraag of er inbreuk wordt gemaakt op de persoonlijke levenssfeer van de betrokkene, dient per document een afweging gemaakt te worden tussen belang van de geheimhouding door de betrokken bestuursorganen en het publieke belang van openbaarheid. Hierbij gaat het om de vraag of er sprake is van een zodanige inbreuk op de persoonlijke levenssfeer dat die een beperking van de openbaarheid rechtvaardigt. Welke van deze belangen in het concrete geval de doorslag behoort te geven, hangt af van alle in onderling verband te beschouwen bijzonderheden van dit geval. Noordam en Ketelaar geven aan dat een

54 CBP Richtsnoeren: Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer, VI, p. 9.

aantal omstandigheden relevant kunnen zijn bij het maken van deze belangenafweging. In de eerste plaats zijn de documenten op het moment van overbrenging in beginsel 20 jaar oud. Tegen die tijd kunnen deze documenten hun administratief belang verloren hebben en zijn privacy-bedreigende aspecten, zoals de koppeling van gegevensbestanden, mogelijk niet meer aan de orde. Archiefbescheiden hebben op dat moment de functie van instrument voor de recht- en bewijszoekende burger en de functie van een cultuur-historisch object voor onderzoek. Deze historische context van informatie maakt volgens Noordam en Ketelaar dat de openbaarheid daarvan niet snel beperkt kan worden.⁵⁵ Dit valt te rijmen met, zoals eerder in deze paragraaf beschreven, dat het enkele feit dat er persoonsgegevens voorkomen in archiefbescheiden, dit niet zonder meer een beperking van de openbaarheid rechtvaardigt. In de juridische literatuur wordt verder wel verdedigd dat de opvatting die een betrokkene heeft over het al dan niet vertrouwelijke karakter van de desbetreffende persoonsgegevens, niet bepalend is voor de openbaarmaking door een bestuursorgaan, maar dat het wel een factor kan zijn die meespeelt. Het voorgaande neemt niet weg dat in de vele rechtspraak over de openbaarheid(sbeperkingen) op grond van de Wob – die een vergelijkbare openbaarheidsbeperking op basis van de eerbiediging van de persoonlijke levenssfeer kent – veelal relatief snel wordt aangenomen dat openbaarmaking een inbreuk op de persoonlijke levenssfeer met zich meebrengt. Daarentegen is een cruciaal verschil tussen de Archiefwet en de Wob dat de ‘leeftijd’ van documenten in archiefbewaarplaatsen in beginsel ouder dan 20 jaar is. Het is daarom de vraag of deze rechtspraak op basis van de Wob een op een ook van toepassing is op archiefbescheiden. Hoe dan ook menen wij dat ten aanzien van archiefbescheiden niet te lichtvaardig moet worden gedacht over het al dan niet stellen van openbaarheidsbeperkingen op grond van de persoonlijke levenssfeer. Een afweging per document in dit kader blijft onzes inziens noodzakelijk.

De openbaarheidsbeperkingen kan de zorgdrager in principe alleen op het moment van overbrenging, dus na 20 jaar, vaststellen. Na het moment van overbrenging kunnen geen beperkingen aan de openbaarheid van het betreffende document meer gesteld worden.⁵⁶ Dit is alleen anders indien zich na overbrenging omstandigheden hebben voorgedaan die, waren zij op dat tijdstip bekend geweest, tot het stellen van openbaarheidsbeperkingen zouden hebben geleid. Volgens Noordam en Ketelaar zou hiervan sprake kunnen zijn wanneer privacygevoelige archiefbescheiden worden aangetroffen, die op grond van de dossier- of inventarisomschrijvingen niet verwacht hadden mogen worden.⁵⁷

55 Noordam en Ketelaar, Privacybescherming, p. 3540-65.

56 Artikel 15 lid 2 Archiefwet.

57 Noordam en Ketelaar, Privacybescherming, p. 3540-63.

Opheffing openbaarheidsbeperkingen

Nadat er openbaarheidsbeperkingen aan een bepaald document zijn gesteld op grond van de eerbiediging van de persoonlijke levenssfeer, kan de zorgdrager, na overleg met degene op wiens last dit document is overgebracht, deze beperkingen in het geheel opheffen of ten aanzien van een specifieke verzoeker buiten beschouwing laten.⁵⁸ De zorgdrager dient in dit kader een belangenafweging uit te voeren. Om de beperking geheel op te heffen dient het belang op openbaarheid van het betreffende document in het algemeen zwaarder te wegen dan de beperking op grond van de eerbiediging van de persoonlijke levenssfeer. Gaat het om het buiten beschouwing laten van de beperking ten aanzien van een specifieke verzoeker, dan dient het belang van deze verzoeker om het document te kunnen raadplegen of te gebruiken zwaarder te wegen.⁵⁹ Een reden om de openbaarheidsbeperkingen geheel op te heffen kan bijvoorbeeld zijn dat alle betrokkenen die genoemd worden in het betreffende document inmiddels overleden zijn. Wetenschappelijk onderzoek kan een grond vormen om de openbaarheidsbeperkingen ten aanzien van de betreffende onderzoeker buiten beschouwing te laten. In het kader van de belangenafweging om de onderzoeker het document in te laten zien of te gebruiken, kan de zorgdrager zorgvuldigheidseisen stellen. Bijvoorbeeld door het ondertekenen van een verklaring waarin eisen zijn gesteld aan het gebruik en de publicatie van de geraadpleegde gegevens door de onderzoeker. Daarnaast kan een direct persoonlijk belang ook een reden zijn om de openbaarheidsbeperkingen ten aanzien van de betreffende verzoeker buiten beschouwing te laten.⁶⁰ Dit vergt afweging tussen dergelijke belangen en het eerder in deze paragraaf beschreven belang van eerbiediging van de persoonlijke levenssfeer.

Toekomstige aanpassing Archiefwet

De Archiefwet wordt overigens binnenkort waarschijnlijk aangepast. De minister van Onderwijs, Cultuur en Wetenschap heeft in de zomer van het jaar 2018 de Tweede Kamer geïnformeerd over een voorgenomen modernisering van de Archiefwet. Deze modernisering ziet met name op het laten aansluiten van de Archiefwet op de verschuiving van papieren archieven naar digitale archieven. De minister wil onder andere de huidige overbrengingstermijn van 20 jaar verkorten naar 10 jaar en de wettelijke begrippen laten aansluiten op de digitale praktijk. Daarnaast wil de minister eventueel een regeling opnemen over de omgang met de vernietiging van digitale kopieën en back-ups die niet naar een archiefbewaarpplaats worden overgebracht alsmede de mogelijk-

58 Artikel 15 lid 3 Archiefwet.

59 Ten aanzien van milieu-informatie die betrekking heeft op emissies in het milieu dient de zorgdrager de beperking ten aanzien van een specifieke verzoeker zonder meer buiten beschouwing te laten.

60 Noordam en Ketelaar, Privacybescherming, p. 3540-64.

heid om digitale archiefbewaarplaatsen op te zetten ('e-depots'). Naar verwachting wordt binnenkort een voorstel voor aanpassing van de Archiefwet aan de Tweede Kamer voorgelegd.⁶¹

9.2 De Wet openbaarheid van bestuur (Wob) en privacy

Hiervoor hebben wij reeds aangestipt dat vóór de overbrenging van archiefbescheiden naar een archiefbewaarplaats het openbaarheidsregime van de Archiefwet nog niet van toepassing is. Vóór de overbrenging kan echter wel het openbaarheidsregime van de Wet openbaarheid van bestuur (Wob) mogelijk van toepassing zijn. De Wob is van toepassing op bepaalde documenten – of delen daarvan – tot aan het moment van overbrenging daarvan naar een archiefbewaarplaats in de zin van de Archiefwet.⁶² Dergelijke documenten kunnen derhalve vóór de overbrenging op grond van de Wob reeds openbaar zijn. De Wob kent een vergelijkbaar regime ten aanzien van de openbaarheid en de eventueel daaraan te stellen beperkingen als de Archiefwet. Daarnaast zijn documenten die op grond van de Wob openbaar zijn in principe ná overbrenging naar een archiefbewaarplaats ook openbaar.

De Wob regelt de openbaarheid van informatie zoals is neergelegd in documenten die bestuursorganen onder zich houden en van informatie zoals is neergelegd in documenten die bij bestuursorganen behoren te berusten. Het gaat daarbij om schriftelijke documenten, maar ook om digitale documenten, foto's, geluidsopnames, e-mails, et cetera. Te denken valt aan informatie over het beleid – met inbegrip van de voorbereiding en uitvoering daarvan – of aan informatie die betrekking heeft op bestuurlijke aangelegenheden. Dergelijke overheidsinformatie is in beginsel openbaar.⁶³ Bestuursorganen zijn enerzijds verplicht om overheidsinformatie uit eigen beweging openbaar te maken voor zover dit in het belang is van een goede en democratische bestuursvoering.⁶⁴ Anderzijds kan iedereen een Wob-verzoek indienen om inzage te krijgen in bepaalde overheidsinformatie.⁶⁵

Beperking openbaarheid o.g.v. eerbiediging van de persoonlijke levenssfeer

Net zoals onder de Archiefwet kan de openbaarheid van overheidsinformatie beperkt worden. De Wob kent meer gronden om de openbaarheid te kunnen beperken dan de Archiefwet. In het kader van privacy is in de Wob eveneens

61 *Kamerstukken II*, 2017–2018, 29 362, nr. 272.

62 *Kamerstukken II*, 1986–1987, 19 859, nr. 3, p. 11.

63 Artikel 2 Wob.

64 Artikel 8 Wob.

65 Artikel 3 Wob.

de ‘eerbiediging van de persoonlijke levenssfeer’ opgenomen als grond om de openbaarheid te beperken.⁶⁶ Dit vergt ook een afweging tussen het belang van openbaarheid en het belang op de eerbiediging van de persoonlijke levenssfeer. Deze te maken afweging is min of meer vergelijkbaar met die van de Archiefwet, met dien verstande dat er een belangrijk verschil zit in de ‘leeftijd’ van de gegevens. Bij de Archiefwet zijn de gegevens ná overbrenging immers in beginsel ouder dan 20 jaar (of na voornoemde wetswijziging mogelijk 10 jaar). De rechtspraak over de openbaarheid(sbeperkingen) op basis van de Wob laat zien dat er relatief snel sprake is van een inbreuk op de persoonlijke levenssfeer, waardoor de openbaarheid beperkt dient te worden.⁶⁷ Het bestuursorgaan heeft dan ook de plicht om inbreuken op de persoonlijke levenssfeer te vermijden dan wel zo beperkt mogelijk te houden.⁶⁸ Aangezien de Wob uitgaat van het informatiestelsel (waar de Archiefwet het documentenstelsel hanteert) hebben bestuursorganen daar ook veel meer mogelijkheden voor. Zij kunnen bijvoorbeeld informatie met privacygevoelige gegevens anonimiseren of ‘weglakken’. Ook kunnen bestuursorganen alleen samenvattingen of inlichtingen over overheidsinformatie verstrekken, om zodoende geen inbreuk te maken op de persoonlijke levenssfeer.

Daarnaast kent de Wob een bijzondere grond om de openbaarheid te beperken. Wanneer er sprake is van bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens of BSN’s geldt dat deze in principe niet openbaar zijn op grond van de Wob.⁶⁹ Dit is alleen anders wanneer er kennelijk geen sprake is van een inbreuk op de persoonlijke levenssfeer. Het verstrekken van dergelijke informatie is dus verboden, tenzij ondubbelzinnig vaststaat dat de verstrekking geen inbreuk maakt op de persoonlijke levenssfeer. Daarover mag redelijkerwijs geen twijfel bestaan.⁷⁰ In de praktijk komt dit erop neer dat dergelijke gegevens in principe niet openbaar zijn.

Om de openbaarheid van overheidsinformatie op grond van de Wob al dan niet te beperken dient – net zoals ten aanzien van de Archiefwet – een afzonderlijke toets uitgevoerd te worden. Een andere toets is de vraag of het openbaar maken c.q. verstrekken van overheidsinformatie geoorloofd is op basis van de AVG. De AVG beantwoordt immers de vraag of het verwerken van persoonsgegevens is toegestaan. De AVG kent geen verplichting tot het ver-

66 Artikel 10 lid 2 sub e Wob.

67 Zie bijv. ABRvS 19 september 2007, zaak no. 200608266/1; ABRvS 9 juni 2004, zaak no. 200305162/1; ABRvS 15 juni 2006, zaak no. 200601804/1.

68 CBP Richtsnoeren: Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer, VI, p. 15-16.

69 Artikel 10 lid 1 sub d Wob.

70 *Kamerstukken II*, 1998-1999, 26 410, nr. 3, p 4-5.

werken van persoonsgegevens. Oftewel, indien de verwerking op basis van de AVG is toegestaan, wil dat nog niet zeggen dat de betreffende gegevens op basis van de Wob verstrekt moeten worden. De Wob hanteert immers haar eigen toets: overheidsinformatie is openbaar, tenzij er sprake is van een inbreuk op de persoonlijke levenssfeer of als er sprake is van bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens of BSN's.⁷¹ Wij beschreven eerder in dit artikel al dat het enkele feit dat er persoonsgegevens worden verwerkt, niet zonder meer met zich meebrengt dat er sprake is van een inbreuk op de persoonlijke levenssfeer.

10 Uitzonderingen AVG voor archieven, onderzoek en bibliotheken

De AVG stelt diverse eisen en verplichtingen aan het verwerken van persoonsgegevens. Deze eisen en verplichtingen kunnen in de praktijk implicaties voor archieven in de zin van de Archiefwet, onderzoekers en bibliotheken met zich meebrengen. Er is een spanningsveld tussen enerzijds de bescherming van persoonsgegevens en anderzijds het belang en de taak van archieven in de zin van de Archiefwet, onderzoekers en bibliotheken. Het verwerken van gegevens in het kader van 'wetenschappelijk, historisch of statistisch onderzoek', de verwerking voor 'journalistieke, academische artistieke of literaire doeleinden' en de 'archivering van gegevens in het algemeen belang' zijn niet altijd te rijmen met de strikte bescherming van persoonsgegevens. De AVG en andere regelgeving voorzien echter in uitzonderingen om onder voorwaarden ook deze specifieke verwerkingen te faciliteren.

10.1 Archivering in het algemeen belang en wetenschappelijk, historisch en statistisch onderzoek

Beginselen verwerking persoonsgegevens – verdere verwerking en opslag

Een belangrijk beginsel in de AVG is dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld. Persoonsgegevens mogen normaliter niet verder worden verwerkt dan voor de doeleinden waarvoor zij oorspronkelijk verzameld zijn. Daarnaast mogen de persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij oorspronkelijk zijn verzameld. In paragraaf 5 hebben wij toegelicht dat met dit uitgangspunt archiveren niet toegestaan zou zijn. Ook zou het dan niet toegestaan zijn om persoonsgege-

⁷¹ *Kamerstukken II*, 1998-1999, 26 410, nr. 3, p 5.

vens verder te gebruiken voor bijvoorbeeld wetenschappelijk onderzoek. Dit knelt met de gerechtvaardigde verwachting van de maatschappij dat er sprake is van kennisvermeerdering.⁷² Persoonsgegevens worden immers in principe niet initieel voor dergelijke doeleinden verzameld en worden in dat kader vaak verwerkt voor andere, dan de oorspronkelijke, doeleinden. In het kader van ‘archivering in het algemeen belang en wetenschappelijk, historisch of statistisch onderzoek’ zijn er daarom uitzonderingen geformuleerd op de hiervoor genoemde hoofdregel.

De AVG staat de verdere verwerking en het langer bewaren van persoonsgegevens toe voor archivering in het algemeen belang en wetenschappelijk, historisch of statistisch onderzoek.⁷³ Het verder verwerken van persoonsgegevens wordt in dat geval als verenigbaar met de oorspronkelijk vastgestelde doeleinden beschouwd. De verwerkingsverantwoordelijke hoeft hiervoor derhalve geen nieuw, separaat, doeleinde vast te stellen. De AVG verbindt hieraan wel de voorwaarde dat er passende waarborgen moeten zijn getroffen.⁷⁴ Denk onder meer aan waarborgen als de verplichting om technische en organisatorische (beveiligings)maatregelen te nemen, waarmee wordt voldaan aan de dataminimalisatieplicht. Deze maatregelen kunnen pseudonimisering omvatten, indien dit niet aan het behalen van de doeleinden van archivering en onderzoek in de weg staat. Ook moeten, waar mogelijk, de persoonsgegevens op een zodanige wijze verder verwerkt worden dat de identificatie van de betrokkenen achterwege blijft.

Bijzondere en strafrechtelijke persoonsgegevens

In archieven kunnen bijzondere persoonsgegevens (en strafrechtelijke gegevens, die we in dit artikel samenvoegen onder de noemer ‘bijzondere persoonsgegevens’) voorkomen. Ook in het kader van wetenschappelijk, historisch en statistisch onderzoek kunnen dergelijke persoonsgegevens verwerkt worden. Uitgangspunt onder de AVG is dat het verwerken van bijzondere persoonsgegevens verboden is.⁷⁵ Dit verbodsbeginsel knelt eveneens met de belangen om gegevens te archiveren of om deze te verwerken voor bijvoorbeeld wetenschappelijk onderzoek. Archiven kunnen bijvoorbeeld niet meer volledig zijn wanneer dergelijke persoonsgegevens niet gearhiveerd mogen worden. De AVG voorziet in dit kader daarom in een uitzondering op het verbod om bijzondere persoonsgegevens te mogen verwerken.⁷⁶ De verwerking van derge-

72 Overweging 113 AVG.

73 Artikel 5 sub b en e AVG.

74 Artikel 89 lid 1 AVG.

75 Artikel 9 lid 1 en artikel 10 AVG.

76 Artikel 9 lid 2 sub j AVG.

lijke persoonsgegevens dient in dat kader door de specifieke wet- en regelgeving te worden toegestaan en/of voorgeschreven.

‘Archivering in het algemeen belang’ ziet op het behoud van historisch belangwekkende informatie. Dit is een erkend publiek belang dat dient te worden afgewogen tegen de bescherming van de persoonlijke levenssfeer. Daarom is in de Archiefwet bepaald dat bijzondere persoonsgegevens kunnen worden verwerkt indien deze verband houden met:⁷⁷

- a. de vervanging van archiefbescheiden;
- b. de overbrenging van archiefbescheiden naar een archiefbewaarplaats;
- c. de opnemng van archiefbescheiden in een archiefbewaarplaats;
- d. het beheer van archiefbescheiden die in een archiefbewaarplaats rusten, met uitzondering van het ter raadpleging of gebruik beschikbaar stellen van zodanige archiefbescheiden. Het beschikbaar stellen van bijzondere persoonsgegevens ter raadpleging of gebruik is dus in beginsel wel verboden, tenzij een beroep kan worden gedaan op een andere uitzondering om deze gegevens hiervoor beschikbaar te stellen (bijvoorbeeld de uitdrukkelijke toestemming van de betrokkene).

Merk daarbij op dat in sub d uitdrukkelijk wordt vermeld dat deze specifieke uitzondering op het verwerkingsverbod van bijzondere persoonsgegevens, in beginsel niet opgaat voor het ‘ter raadpleging of gebruik’ beschikbaar stellen van archiefbescheiden. Dat betekent dat – voor zover documenten met bijzondere persoonsgegevens al geen beperkingen op de openbaarheid kennen, hetgeen vanwege de gevoeligheid van de gegevens hoogstwaarschijnlijk in de regel het geval zal zijn – voor het geven van inzage in de documenten, sprake moet zijn van een andere uitzondering op het verwerkingsverbod.

Ten aanzien van ‘wetenschappelijk, historisch of statistisch onderzoek’ kan het ook noodzakelijk zijn om bijzondere persoonsgegevens te verwerken. Denk bijvoorbeeld aan historisch onderzoek naar het koloniale verleden van Nederland, waarbij de afkomst van de slaven – en daarmee indirect het ras (een bijzonder persoonsgegeven) – wordt vastgelegd. Met het oog op wetenschappelijk, historisch of statistisch onderzoek kunnen bijzondere persoonsgegevens worden verwerkt, mits aan de volgende cumulatieve voorwaarden wordt voldaan:⁷⁸

- a. De verwerking is noodzakelijk voor het wetenschappelijk, historisch of statistisch onderzoek waarbij de eerder in deze paragraaf toegelichte passende waarborgen⁷⁹ zijn getroffen.

⁷⁷ Artikel 2a Archiefwet.

⁷⁸ Artikel 24 en artikel 32 sub f UAVG.

⁷⁹ Artikel 89 lid 1 AVG.

- b. Het onderzoek dient een algemeen belang.
- c. Het vragen van uitdrukkelijke toestemming aan de betrokkene blijkt onmogelijk te zijn of kost een onevenredige inspanning.
- d. Er is bij de uitvoering van het onderzoek voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Welke waarborgen er getroffen moeten worden is afhankelijk van het concrete geval. Er kunnen bijvoorbeeld maatregelen getroffen worden met betrekking tot de toegang tot de persoonsgegevens, geheimhouding en ter zake de resultaten die openbaar zullen worden gemaakt.

Naast de hiervoor genoemde uitzonderingen kunnen bijzondere persoonsgegevens ook verwerkt worden indien een beroep kan worden gedaan op een andere uitzondering, zoals de uitdrukkelijke toestemming van de betrokkene.⁸⁰ Indien de betrokkene uitdrukkelijk toestemming heeft gegeven, dan kunnen zijn bijzondere persoonsgegevens verwerkt worden. In dit verband bepaalt de AVG met betrekking tot wetenschappelijk onderzoek uitdrukkelijk dat de betrokkene ook toestemming moet kunnen geven voor bepaalde terreinen van wetenschappelijk onderzoek.⁸¹ Op het moment van verzameling van persoonsgegevens is het immers vaak niet mogelijk om het doel voor de verwerking voor het wetenschappelijk onderzoek te omschrijven. Normaliter dient de betrokkene echter precies te weten waarvoor hij toestemming geeft (dat wordt ook wel *informed consent* of geïnformeerde toestemming genoemd). Daarom biedt de AVG de mogelijkheid om in het kader van wetenschappelijk onderzoek een wat meer algemenere toestemming te geven voor bepaalde onderzoeksterreinen of onderdelen van onderzoeksprojecten, voor zover het voorgenomen doel dit toelaat. Hierbij geldt als voorwaarde dat de erkende ethische normen voor wetenschappelijk onderzoek in acht genomen worden.

Overigens betekent opheffing van het verbod op het verwerken van bijzondere persoonsgegevens niet dat de betreffende gegevens zonder meer mogen worden verwerkt. Er dient vervolgens namelijk nog steeds aan de algemeen geldende vereisten uit de AVG, zoals wij in paragraaf 5 hebben toegelicht, te worden voldaan om te waarborgen dat de verwerking rechtmatig is. De verwerkingsverantwoordelijke dient derhalve bijvoorbeeld de verwerking te baseren op een verwerkingsgrondslag uit de AVG en bijvoorbeeld te voldoen aan het beginsel van dataminimalisatie.

80 Artikel 9 lid 2 sub a AVG.

81 Overweging 33 AVG.

Informatieplichten

De verwerkingsverantwoordelijke is verplicht om de betrokkenen te informeren over de verwerkingen van persoonsgegevens. Eerder in dit artikel hebben wij toegelicht wat deze informatieverplichting inhoudt. Archieven, culturele erfgoedinstellingen en onderzoekers verkrijgen echter niet altijd de persoonsgegevens van de betrokkene zelf. Onder meer gezien de aard van hun verwerkingen is het in de praktijk in dergelijke gevallen vaak vrijwel onmogelijk om deze betrokkenen te informeren. Om die reden zijn in de AVG specifieke regels vastgelegd over het informeren van betrokkenen in deze situaties.

De verplichting tot het informeren van de betrokkene geldt niet wanneer de persoonsgegevens van een ander dan de betrokkene zijn verkregen en het verstrekken van de informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, of wanneer deze verplichtingen het doel van de verwerking onmogelijk dreigen te maken of ernstig in het gedrang dreigen te brengen.⁸² In dat geval dienen echter wel passende waarborgen te worden getroffen om de rechten, vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen. Het voorgaande neemt niet weg dat de hoofdregel van de AVG is dat de betrokkenen bij de verkrijging van persoonsgegevens geïnformeerd moeten worden over de verwerking van hun persoonsgegevens. Dat geldt, tenzij er sprake is van een uitzondering. Indien de persoonsgegevens bijvoorbeeld wel rechtstreeks van de betrokkene verkregen worden, dan is er geen enkele reden om niet aan deze informatieverplichting te kunnen voldoen. Daarnaast wil de omstandigheid dat er niet specifiek geïnformeerd kan worden, niet zeggen dat er niet in zijn algemeenheid geïnformeerd kan worden. Zo zou bijvoorbeeld in het geval van archivering, het overheidsorgaan dat de oorspronkelijke verwerking initieert, bij het verzamelen van de persoonsgegevens al in zijn algemeenheid kunnen informeren over haar archiveringsverplichting en wat dat zou betekenen voor de persoonsgegevens van de betrokkenen. Ook de archiefinstelling zelf kan een algemene privacyverklaring opstellen en bijvoorbeeld op haar website plaatsen, waarin zij uitlegt hoe zij omgaat met persoonsgegevens, met de uitoefening van de rechten van de betrokkene, met openbaarheid van de archiefbescheiden én de beperkingen op die openbaarheid, et cetera.

Afwijking rechten van betrokkenen

De betrokkenen hebben, zoals in paragraaf 8 van dit artikel besproken, op grond van de AVG diverse rechten. Zo heeft de betrokkene het recht op inzage, rectificatie en wissing van persoonsgegevens. Daarnaast heeft de betrokkene het recht op beperking van de verwerking, het recht op gegevensoverdraagbaarheid en het recht om bezwaar te maken tegen de gegevensverwerking. Tot

82 Artikel 14 lid 5 sub b AVG.

slot heeft de betrokkene het recht om niet onderworpen te worden aan uitsluitend op geautomatiseerde verwerkingen, waaronder profilering, gebaseerde besluiten die voor hem gevolgen hebben. Deze rechten kunnen voor archieven en onderzoekers op wetenschappelijk, historisch of statistisch terrein implicaties opleveren. Zo kan een collectie in een archief bijvoorbeeld niet meer compleet zijn als een verzoek tot verwijdering van persoonsgegevens ingewilligd moet worden. Met het oog op archivering in het algemeen belang en wetenschappelijk, historisch of statistisch onderzoek zijn er daarom diverse afwijkingen en uitzonderingen op deze rechten van betrokkenen geformuleerd.

In de UAVG is bepaald dat ingeval de persoonsgegevens voor archivering in het algemeen belang worden verwerkt, de betrokkene het ‘recht op inzage, rectificatie, beperking van de verwerking – uitsluitend in geval van betwisting van de juistheid van persoonsgegevens – en de overdraagbaarheid van de persoonsgegevens’ niet kan afdwingen.⁸³ De verwerkingsverantwoordelijke is echter niet verplicht om van deze rechten af te wijken. De verwerkingsverantwoordelijke kan er derhalve voor kiezen om alsnog een verzoek van een betrokkene tot uitoefening van zijn rechten in te willigen. Daarentegen heeft de betrokkene wel het recht op inzage in de betreffende archiefbescheiden en, wanneer hij vervolgens van oordeel is dat de persoonsgegevens onjuist zijn, om een eigen lezing aan de betrokken archiefbescheiden toe te voegen.⁸⁴

Ten aanzien van de verwerking van persoonsgegevens ten behoeve van wetenschappelijk, historisch of statistisch onderzoek is in de UAVG vastgelegd dat de betrokkene het recht op inzage, rectificatie en beperking van de verwerking niet kan afdwingen.⁸⁵ De verwerkingsverantwoordelijke is in dit kader eveneens niet verplicht om van deze rechten af te wijken.

Daarnaast geldt voor de verwerking van persoonsgegevens ten behoeve van zowel archivering in het algemeen belang als wetenschappelijk, historisch of statistisch onderzoek dat de verwerkingsverantwoordelijke niet hoeft te voldoen aan een verzoek tot ‘wissing van persoonsgegevens’.⁸⁶ Doch, dat geldt uitsluitend indien dat verzoek de verwezenlijking van de betreffende doeleinden onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. Het is nog niet geheel duidelijk wat met deze laatste voorwaarde in de AVG wordt beoogd. Het verwijderen van persoonsgegevens strookt immers per definitie niet met het doel van archivering en onderzoek. Archivering en onderzoek zijn gericht op het behoud van gegevens en kennisvermeerdering. In die

83 Artikel 45 lid 1 UAVG.

84 Artikel 45 lid 2 en 3 UAVG.

85 Artikel 44 UAVG.

86 Artikel 17 lid 3 sub d AVG.

zin zal in de praktijk geen sprake zijn van verwijderen van persoonsgegevens uit (met name) archieven omdat dat in de regel gevolgen zal hebben voor de integriteit van het archief. Op basis van jurisprudentie onder de – inmiddels door de AVG vervangen – Wet bescherming persoonsgegevens is het volgens ons verdedigbaar dat deze uitzondering op het recht op wissing van persoonsgegevens vrij snel van toepassing is.⁸⁷ Met andere woorden, onzes inziens is de verwezenlijking van de doeleinden voor archieven en onderzoekers relatief snel onmogelijk dan wel komt het in het gedrang, als het verzoek tot wissing van persoonsgegevens ingewilligd moet worden. De betrokkene heeft dus in het kader van archivering in het algemeen belang en wetenschappelijk, historisch of statistisch onderzoek in principe geen recht op wissing van gegevens. Dat zou mogelijk anders kunnen zijn indien het verwijderingsverzoek ziet op informatie die niet gearhiveerd had mogen worden.

De betrokkene heeft ten slotte geen ‘recht van bezwaar’ ten aanzien van persoonsgegevens die worden verwerkt in het kader van archivering in het algemeen belang en wetenschappelijk, historisch of statistisch onderzoek.⁸⁸

10.2 Vrijheid van meningsuiting en informatie; journalistiek en academische, artistieke of literaire uitdrukkingen

Bibliotheken, musea en universiteiten kunnen gegevens verwerken ten behoeve van ‘academische, artistieke of literaire doeleinden’. Voor de regels in het kader van de AVG worden gegevensverwerkingen voor academische, artistieke of literaire doeleinden gelijkgesteld met de verwerking voor ‘journalistieke doeleinden’ (hierna gezamenlijk voor het overzicht ook wel gemakshalve te noemen ‘de vrijheid van meningsuiting en informatie’). De gegevensverwerkingen in het kader van het recht op vrijheid van meningsuiting en informatie kunnen echter ‘botsen’ met het doel van de AVG om persoonsgegevens te beschermen. Er kan sprake zijn van een botsing tussen twee grondrechten: enerzijds het recht op vrijheid van meningsuiting en informatie, anderzijds het recht op bescherming van de privacy.⁸⁹ Uitgangspunt is dat er geen rangorde bestaat tussen deze grondrechten. Gezien dit uitgangspunt is er in de AVG een aantal uitzonderingen geformuleerd met betrekking tot verwerkingen voor

87 Zie bijvoorbeeld de uitspraak van de rechtbank Amsterdam van 31 maart 2010, ECLI:NL:RBAMS:2010:BM4462, en de uitspraak van de rechtbank Amsterdam van 19 februari 2010, ECLI:NL:RBAMS:2010:BL5458, waarin met het oog op de functie van archieven werd geoordeeld dat het verzoek om persoonsgegevens te wissen terecht afgewezen is.

88 Artikel 21 lid 6 AVG.

89 Respectievelijk artikel 10 en artikel 8 EVRM.

journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen.

Gelet op het hiervoor bedoelde spanningsveld bepaalt de AVG dat de Europese lidstaten verplicht zijn om het recht op bescherming van privacy in overeenstemming te brengen met de vrijheid van meningsuiting en informatie.⁹⁰ De wetgever dient derhalve buitengewoon terughoudend te zijn met het stellen van beperkingen aan de vrijheid van meningsuiting en van informatie.⁹¹ Dit is overigens niets nieuws onder de AVG; ook uit eerdere jurisprudentie volgt dat een beperking op de vrijheid van meningsuiting en informatie slechts in uitzonderlijke omstandigheden kan worden gegeven. In het kader van bijvoorbeeld een beoordeling van de vraag of een perspublicatie rechtmatig is, kan het recht van vrijheid van meningsuiting derhalve niet zonder meer buiten spel gezet worden door louter een beroep te doen op de bescherming van privacy.⁹² De rechter moet hier steeds een belangenafweging maken tussen beide grondrechten. Illustratief voor de verhouding tussen het grondrecht op bescherming van privacy en het grondrecht op vrijheid van meningsuiting en van informatie is de zaak Buivids, waarover het Europees Hof van Justitie recentelijk een arrest heeft gewezen.⁹³

De heer Buivids diende op een politiebureau van de Letse nationale politie een verklaring af te leggen in het kader van een procedure wegens een overtreding. Buivids heeft een video-opname gemaakt van zijn verklaring. Op deze video zijn politieagenten en hun werkzaamheden op het politiebureau te zien. Buivids heeft deze video-opnamen vervolgens op YouTube gepubliceerd. De Letse privacytoezichthouder heeft zich op het standpunt gesteld dat Buivids daarmee inbreuk maakte op de Letse Wet bescherming persoonsgegevens. Buivids deed echter een beroep op zijn vrijheid van meningsuiting. Uiteindelijk werd deze zaak voorgelegd aan het Europees Hof van Justitie.

Het Hof stelt allereerst voorop dat het fundamentele recht op de bescherming van de privacy tot op zekere hoogte verzoend moeten worden met het fundamentele recht van de vrijheid van meningsuiting. Gezien het belang van vrijheid van meningsuiting voor elke democratische samenleving, dienen de daarmee samenhangende begrippen – zoals journalistiek – ruim uitgelegd te worden. ‘Journalistieke activiteiten’ zijn derhalve activiteiten die de bekendmaking aan het publiek van informatie, meningen of ideeën tot doel hebben, ongeacht het overdrachtsmedium. De omstandigheid dat Buivids niet aan te

90 Artikel 85 AVG.

91 *Kamerstukken II*, 2017-2018, 34 851, nr. 3, p. 49.

92 Rb. Amsterdam 12 april 2019, IEPT20190412 (*Talpa*).

93 HvJEU 14 februari 2019, nr. C-345/17 (*Buivids*).

merken is als professioneel journalist, betekent niet dat het fundamentele recht op vrijheid van meningsuiting – en derhalve de journalistieke doeleinden – niet voor de door hem op YouTube gedeelde video-opnamen gelden.

Er dient volgens het Hof te allen tijde een evenwichtige afweging tussen de bescherming van de privacy en de vrijheid van meningsuiting gemaakt te worden. Gezien dit evenwicht dienen de uitzonderingen en beperkingen op het fundamentele recht op de bescherming van de privacy beperkt te blijven tot het strikt noodzakelijke.

Dit oordeel van het Europees Hof van Justitie laat zien dat de bescherming van privacy niet zonder meer de vrijheid van meningsuiting en informatie van tafel veegt. Daarnaast geeft het Hof aan dat de begrippen die samenhangen met het recht op vrijheid van meningsuiting en informatie ruim uitgelegd dienen te worden. Dit is in lijn met de AVG die een ruime uitleg van de begrippen ‘journalistieke doeleinden’ en ‘academische, artistieke of literaire uitdrukkingvormen’ voorschrijft.⁹⁴ Het Hof heeft in een eerder arrest ook al geoordeeld dat activiteiten die de bekendmaking aan het publiek van informatie, meningen of ideeën tot doel hebben, ongeacht het overdrachtsmedium, onder het begrip journalistiek dienen te vallen.⁹⁵ In een andere zaak oordeelde de rechtbank Amsterdam dat daaronder niet alleen het aan de kaak stellen van misstanden in de samenleving en wereldnieuws valt, maar ook ‘entertainmentnieuws’.⁹⁶

De Nederlandse wetgever heeft in de UAVG het spanningsveld tussen de bescherming van privacy en de vrijheid van meningsuiting en informatie onderkend.⁹⁷ Daarin zijn diverse verplichtingen uit de AVG en de UAVG buiten toepassing verklaard voor verwerkingen ten behoeve van uitsluitend journalistieke doeleinden of academische, artistieke of literaire uitdrukkingvormen. Onder meer de volgende verplichtingen zijn uitgezonderd:

- Het verbod om bijzondere en strafrechtelijke persoonsgegevens te mogen verwerken is niet van toepassing (artikel 9 en 10 AVG).
- De betrokkene heeft niet het recht om te allen tijde diens toestemming weer in te kunnen trekken (artikel 7 lid 3 AVG).
- De verwerkingsverantwoordelijke heeft geen verplichting om de betrok-

94 Overweging 153 AVG. De rechtbank Amsterdam van 31 januari 2019, ECLI:NL:RBAMS:2019:645, volgt eveneens deze lijn.

95 HvJEU 16 december 2008, C-73/07, EU:C:2008:727 (*Satakunnan Markkinapörssi en Satamedia*).

96 Rb. Amsterdam 12 oktober 2018, ECLI:NL:RBAMS:2018:7397.

97 Artikel 43 UAVG.

kenen te informeren over de verwerking van persoonsgegevens (artikelen 13 en 14 AVG).

- De betrokkene kan diens rechten niet afdwingen, zoals het recht op inzage, verwijdering of overdracht van de persoonsgegevens (hoofdstuk III AVG).
- De verwerkingsverantwoordelijke is niet verplicht om een register van verwerkingsactiviteiten bij te houden (artikel 30 AVG).
- De regels rondom het melden van datalekken zijn niet van toepassing (artikelen 33 en 34 AVG).

Daarnaast bevat de AVG een expliciete uitzondering voor het recht van de betrokkene op gegevenswissing. De verwerkingsverantwoordelijke hoeft op grond van de AVG geen gehoor te geven aan het verzoek van een betrokkene tot wissing van diens persoonsgegevens indien dat verzoek in de weg staat aan het uitoefenen van het recht op vrijheid van meningsuiting en informatie.⁹⁸

Vóórdat de AVG van toepassing werd diende op grond van vaste jurisprudentie een ‘belangenafweging’ te worden gemaakt tussen enerzijds het belang van de betrokkene die diens rechten wil uitoefenen, bijvoorbeeld het recht op gegevenswissing, en anderzijds het belang bij het recht op vrijheid van meningsuiting en informatievrijheid. De AVG en de bijbehorende UAVG zonderen echter de rechten van betrokkenen uit bij verwerkingen van persoonsgegevens ten behoeve van uitsluitend journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen. Het is dan ook de vraag in hoeverre onder de AVG nog een dergelijke belangenafweging tussen de beide rechten gemaakt dient te worden. In een zaak uit 2018 – nadat de AVG van toepassing werd – maakte de rechtbank Amsterdam een belangenafweging tussen enerzijds het recht op vrijheid van meningsuiting en informatie en anderzijds het recht op gegevenswissing van de betrokkene.⁹⁹ Opvallend genoeg overweegt de rechtbank Amsterdam in een andere uitspraak – zonder daarbij een belangenafweging te maken – dat de betrokkene diens rechten uit hoofde van de AVG niet kan uitoefenen ingeval van de verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden.¹⁰⁰ In weer een andere zaak overweegt de rechtbank Zeeland-West-Brabant dat een betrokkene geen beroep kan doen op zijn rechten uit hoofde van de AVG als gevolg van de exceptie voor de vrijheid van meningsuiting en informatie. De rechtbank maakte hierbij geen belangenafweging.¹⁰¹ Kortom, op basis van recente jurisprudentie bestaat nog geen uitsluitsel over de vraag of de belangenafweging uit de vaste rechtspraak

98 Artikel 17 lid 3 sub a AVG.

99 Rb. Amsterdam 12 oktober 2018, ECLI:NL:RBAMS:2018:7397.

100 Rb. Amsterdam 31 januari 2019, ECLI:NL:RBAMS:2019:645.

101 Rb. Zeeland-West-Brabant 5 juli 2018, ECLI:NL:RBZWB:2018:4139.

van vóór de AVG nog steeds een rol speelt in het kader van de uitzonderingen op de verplichtingen uit de AVG met betrekking tot de vrijheid van meningsuiting en informatie.

In tegenstelling tot hetgeen het voorgaande doet vermoeden, worden niet alle verplichtingen uit de AVG buiten toepassing verklaard voor verwerkingen ten behoeve van uitsluitend journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen. Zo zal de verwerkingsverantwoordelijke onder andere onverminderd moeten beschikken over een gerechtvaardigd doeleinde en een verwerkingsgrondslag, alsmede moeten voldoen aan de andere beginselen uit de AVG om de persoonsgegevens te mogen verwerken. Daarnaast blijven de verplichtingen rondom het inschakelen van verwerkers en het beveiligen van persoonsgegevens onverkort van toepassing. *Last but not least*: voor verwerkingen van persoonsgegevens die niet uitsluitend zien op journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen, gelden in principe de verplichtingen uit de AVG onverkort.

11. Beeldmaterialen en privacy

Archieven en bibliotheken beschikken vaak over veel beeldmateriaal. Wanneer personen op deze beeldmaterialen herkenbaar in beeld zijn, zal er in principe sprake zijn van een verwerking van persoonsgegevens. Deze beelden zijn dan immers herleidbaar tot een bepaalde persoon. Ook wanneer personen niet-volledig in beeld zijn kan er toch sprake zijn van persoonsgegevens. Zo is bijvoorbeeld het silhouet van prinses Beatrix voor de meeste mensen toch herkenbaar. Daarmee is dat silhouet een persoonsgegeven. Met de moderne technologieën van tegenwoordig zal over het algemeen in principe snel sprake zijn van identificeerbaarheid.¹⁰² Op beeldmaterialen zijn voorts allerlei (fysieke) kenmerken van de betrokkenen zichtbaar. Bijvoorbeeld het feit dat iemand een hoofddoek of een bril draagt of welke huidskleur hij heeft. Dergelijke kenmerken betreffen bijzondere persoonsgegevens, in voornoemd voorbeeld achtereenvolgens de religie, de visuele gezondheid en het ras van de betrokkene. Dit zou betekenen dat – alleen al vanwege bijvoorbeeld het zichtbare ras – alle camerabeelden en foto's van personen per definitie bijzondere persoonsgegevens zijn. Op grond van de AVG is het in beginsel verboden om bijzon-

102 Autoriteit Persoonsgegevens, *Beleidsregels cameratoezicht*, Den Haag: 28 januari 2016, p. 15. Geraadpleegd van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf. Deze beleidsregels zijn weliswaar onder de Wbp opgesteld, maar de uitleg die de Autoriteit Persoonsgegevens daarin verschaft kan ook onder de AVG nog steeds relevant zijn aangezien er een vergelijkbaar stramien is met de Wbp.

dere persoonsgegevens te verwerken. Strikt genomen zouden archieven, bibliotheken en culturele erfgoedinstellingen dan ook helemaal geen beeldmaterialen van personen mogen verwerken, tenzij zij deze verwerking kunnen baseren op een van de uitzonderingen die de AVG biedt, zoals de uitdrukkelijke toestemming van de betrokkene.¹⁰³

Een dergelijke praktijk is onwenselijk. Het verwerken van beeldmaterialen hoeft op zichzelf niet onaanvaardbaar te zijn. De AVG bepaalt daarom ook dat de verwerking van foto's niet systematisch als verwerking van bijzondere persoonsgegevens mag worden beschouwd. Een foto is volgens de AVG alleen een biometrisch gegeven – hetgeen een bijzonder persoonsgegeven is – wanneer zij wordt verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van de betrokkene mogelijk maken.¹⁰⁴

De AVG zet daarmee de lijn voort die de Autoriteit Persoonsgegevens had vóórdat de AVG van toepassing werd. De Autoriteit Persoonsgegevens zette in haar beleidsregels uiteen dat beeldmaterialen niet als bijzondere persoonsgegevens beschouwd mogen worden indien:¹⁰⁵

- het doeleinde van de verwerking niet gericht is op het verwerken van bijzondere persoonsgegevens, dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven;
- het voor de verwerkingsverantwoordelijke redelijkerwijs niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid op grond van een bijzonder persoonsgegeven; en
- de verwerking van die bijzondere persoonsgegevens onvermijdelijk is bij die verwerking.

Kortom, beeldmaterialen van personen zijn in beginsel geen bijzondere persoonsgegevens, tenzij de verwerking van die beeldmaterialen bedoeld is om personen gericht te identificeren, al dan niet aan de hand van (bijzondere) kenmerken. Van dat laatste is bijvoorbeeld sprake ingeval een pasfoto die op bedrijfspasjes geplaatst wordt waarmee de betrokkene toegang tot de bedrijfsgebouwen heeft.

Let wel, indien beeldmateriaal niet als een bijzonder persoonsgegeven is aan te merken, betekent dat nog niet dat de verwerking daarvan ook rechtmatig is.

103 Autoriteit Persoonsgegevens, *Beleidsregels cameratoezicht*, Den Haag: 28 januari 2016, p. 25-26. Geraadpleegd van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf.

104 Overweging 51 AVG.

105 Autoriteit Persoonsgegevens, *Beleidsregels cameratoezicht*, Den Haag: 28 januari 2016, p. 26. Geraadpleegd van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf.

Persoonsgegevens mogen immers alleen in overeenstemming met de AVG verwerkt worden, behoudens de eventuele in de AVG geformuleerde uitzonderingen zoals de in de vorige paragraaf beschreven vrijheid van meningsuiting en informatie, journalistiek en academische, artistieke of literaire uitdrukkingen. In principe houdt dit in dat er onder meer een gerechtvaardigd doel en een geldige verwerkingsgrondslag voor de verwerking dienen te bestaan.

Portretrecht

Naast de AVG kunnen bij beeldmaterialen ook portretrechten (zoals bedoeld in artikel 19-21 van de Auteurswet) van de geportretteerde van toepassing zijn. Onder een 'portret' wordt verstaan een afbeelding waarop een persoon herkenbaar is afgebeeld. Daarvoor hoeft het hoofd van de persoon niet te zijn afgebeeld; voldoende is dat een persoon herkend kan worden en daarbij kan een typerende lichaamshouding een rol spelen.¹⁰⁶ Een portret kan een foto of video zijn, maar ook een illustratie, schilderij of grafische weergave.

Bij het portretrecht wordt een onderscheid gemaakt tussen portretten die 'in opdracht' zijn gemaakt en portretten die 'niet in opdracht' zijn gemaakt. Wanneer een portret in opdracht is gemaakt, zoals een pasfoto of trouwfoto, dan is voor de openbaarmaking daarvan in beginsel toestemming van de geportretteerde vereist. Dit toestemmingsvereiste geldt tot tien jaar na diens overlijden, waarbij na overlijden de toestemming van alle nabestaanden verkregen moet worden.¹⁰⁷ Is het portret daarentegen niet in opdracht gemaakt, dan is in beginsel geen toestemming vereist voor de openbaarmaking daarvan. Van niet in opdracht gemaakte portretten is bijvoorbeeld sprake wanneer er een foto van het straatbeeld wordt gemaakt en de geportretteerde toevallig daarop wordt vastgelegd. In dat geval is het uitgangspunt dat het portret openbaar gemaakt mag worden, tenzij een redelijk belang van de geportretteerde of diens nabestaanden zich hiertegen verzet.¹⁰⁸ Daarbij kunnen zowel persoonlijke (privacy)belangen als commerciële belangen in aanmerking worden genomen.¹⁰⁹ Een redelijk 'persoonlijk belang' kan bijvoorbeeld de bescherming van de privacy zijn of ongewenste associatie met een product of dienst door gebruik van het portret in reclame.¹¹⁰ Redelijke persoonlijke belangen zouden voorts de inbreuk op de strikt intieme sfeer, gevaar voor represailles, bespot-

106 Visser, in: *T&C Intellectuele eigendom* 2016, art. 21 Auteurswet, aant. 2. Zie ook HR 30 oktober 1987, ECLI:NL:HR:1987:AD0034, *NJ*1988/277 (*Naturiste*) en HR 2 mei 2003, ECLI:NL:HR:2003:AF3416, *NJ*2004/80 (*Breekijzer*).

107 Artikel 20 juncto artikel 25a Auteurswet.

108 Artikel 21 Auteurswet.

109 Visser, in: *T&C Intellectuele eigendom* 2016, art. 21 Auteurswet, aant. 1 en HR 14 juni 2013, ECLI:NL:HR:2013:CA2788 (*Cruifff/Tirion*), r.o. 3.4.

110 HR 2 mei 1997, ECLI:NL:HR:1997:ZC2364, *NJ*1997/661 (*Discodanser*).

ting, et cetera kunnen zijn. Ook bekende personen kunnen een redelijk persoonlijk belang hebben; niet alleen met betrekking tot hun privé-activiteiten, maar ook ten aanzien van hun professionele of zakelijke activiteiten.¹¹¹ Een redelijke ‘commercieel belang’ kan bijvoorbeeld de mogelijkheid zijn om het portret zelf te exploiteren of om mee te delen in de voordelen van de exploitatie.¹¹² De literatuur is overigens verdeeld over de vraag of op commerciële belangen geënte portretrechten vatbaar zijn voor overdracht of vererving, respectievelijk de vraag of aan nabestaanden eigen commerciële belangen kunnen worden toegekend. Het bestaan van een persoonlijk of commercieel belang hoeft overigens niet direct aan openbaarmaking van een portret in de weg te staan. Dit belang dient ook afgewogen te worden tegen andere belangen zoals de vrijheid van meningsuiting, de vrijheid van informatie, de persvrijheid en het recht op privacy.

12. Privacy van overledenen

Archieven en bibliotheken en andere organisaties kunnen persoonsgegevens verwerken van overleden personen. Vooral in archieven bevinden zich veelal gegevens over overledenen. Omdat de AVG van toepassing is op verwerking van persoonsgegevens van ‘natuurlijke personen’, is de wet niet van toepassing op overledenen.¹¹³ Voor onder meer archieven en bibliotheken heeft dit praktisch een groot voordeel. Diverse verplichtingen uit de AVG zijn immers lastig toe te passen wanneer de betrokkene overleden is.

Aan de andere kant is het ook niet wenselijk om helemaal géén regels te hebben over de verwerking van persoonsgegevens van overledenen. Voor nabestaanden kan het pijnlijk zijn als er bijvoorbeeld persoonsgegevens van een verloren dierbare op het internet worden geplaatst. Normaliter maakt de betrokkene uit hoofde van de AVG zelf aanspraak op de bescherming van zijn gegevens. De betrokkene wordt bijvoorbeeld geïnformeerd over en dient in sommige gevallen zijn toestemming te geven voor de verwerking. Na zijn overlijden kan de betrokkene echter niet zelf opkomen voor de bescherming van zijn privacy. Het is dan op zich ook geen vreemde gedachte dat na iemands overlijden diens nabestaanden namens de overledene aanspraak kunnen

111 HR 14 juni 2013, ECLI:NL:HR:2013:CA2788 (*Cruiff/Tirion*), r.o. 3.4; EHRM 24 juni 2004, ECLI:NL:XX:2004:AQ6531, *NJ2005/22 (Caroline von Hannover I)*; EHRM 5 oktober 2010, ECLI:NL:XX:2010:BP3541, *NJ2011/566 (Köpke)* en EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800, *NJ1993/400 (Niemietz)*.

112 HR 14 juni 2013, ECLI:NL:HR:2013:CA2788 (*Cruiff/Tirion*), r.o. 3.4 en HR 19 januari 1979, ECLI:NL:PHR:1979:AC6461, *NJ1979/383 (t Schaep)*.

113 Overweging 27 AVG.

maken op de bescherming van diens privacy. Nabestaanden zouden in dat geval bijvoorbeeld rechten op grond van de AVG kunnen uitoefenen ten aanzien van gegevens die op social media worden verwerkt.

De AVG biedt lidstaten de mogelijkheid om in de nationale wet- en regelgeving regels vast te stellen over de verwerking van persoonsgegevens van overledenen. In dat opzicht zouden lidstaten onder andere kunnen vastleggen wat de rechten van de nabestaanden zijn met betrekking tot de persoonsgegevens van de overledene. Ondanks het advies van de Autoriteit Persoonsgegevens is in Nederland in de UAVG ervoor gekozen om in dit kader geen aanvullende regels vast te stellen.¹¹⁴ Het is echter een misvatting om er dan van uit te gaan dat wanneer iemand overlijdt diens persoonsgegevens geheel ‘vogelvrij’ zijn. Deze gegevens kunnen onder bepaalde omstandigheden aan regelgeving onderworpen zijn.

In de eerste plaats kunnen de gegevens van een overledene eveneens direct of indirect iets zeggen over een andere – nog levende – persoon. Bijvoorbeeld gegevens over het woonadres van een overledene, waar diens nabestaanden nog steeds wonen, of een foto van de overledene met het hele gezin. In dat geval zijn de gegevens van de overledene herleidbaar tot de nabestaanden. De gegevens van de overledene zijn in dat geval ook persoonsgegevens van de betreffende nabestaande. Ten aanzien van die persoonsgegevens is de AVG uiteraard ten opzichte van de betreffende nabestaande wel van toepassing.¹¹⁵

Voorbeeld

Op het internet zijn veel stamboomonderzoeken te vinden, zowel in archieven als in gepubliceerde onderzoeken van (amateur-)genealogen. De AVG is niet van toepassing op overleden personen. Vanuit de AVG zijn er dus weinig bezwaren tegen het publiceren van stambomen op internet. Echter, vanuit het standpunt van volledigheid bevatten veel stambomen ook informatie over nog levende personen, zoals de geboortedatum. Sommige stambomen vermelden zelfs ziekten waaraan mensen zijn overleden. Dergelijke informatie kan betrekking hebben op nabestaanden en dus een persoonsgegeven zijn. Bijvoorbeeld als het gaat om erfelijke ziekten waarmee de kinderen kunnen zijn belast. Dat kan het geval zijn bij een moeder die aan hemofilie leed. Deze ziekte is gebonden aan een gen in het X-chromosoom. Daarom geeft zij de ziekte in

114 *Kamerstukken II*, 2017-2018, 34 851, nr. 3, p. 81.

115 Ministerie van Justitie en Veiligheid (2018), *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet algemene verordening gegevensbescherming*, p. 26. Geraadpleegd van <https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming>.

ieder geval door aan haar zonen. De AVG is dan wel van toepassing op dergelijke gegevens die herleidbaar zijn tot nog levende personen.¹¹⁶

In de tweede plaats kunnen ingeval van beeldmaterialen de regels rondom het portretrecht van toepassing zijn, zoals in de vorige paragraaf reeds toegelicht is. Het portretrecht is van toepassing op beeldmaterialen waarop iemand herkenbaar afgebeeld staat, ook na diens overlijden. Voor in opdracht gemaakte portretten is voor de openbaarmaking daarvan tot tien jaar na het overlijden toestemming van alle nabestaanden vereist.¹¹⁷ Ten aanzien van niet in opdracht gemaakte portretten kunnen na het overlijden van de geportretteerde diens nabestaanden met redelijke belangen zich verzetten tegen de openbaarmaking van het portret.¹¹⁸ In dit verband kan in bepaalde omstandigheden bijvoorbeeld gedacht worden aan het redelijke belang van een nabestaande om een onverstoorde nagedachtenis aan de overledene te hebben.

Ten derde kan het onzorgvuldig omgaan met gegevens van overledenen leiden tot een civiele vordering uit onrechtmatige daad.¹¹⁹ Er kan bijvoorbeeld sprake zijn van een onrechtmatige daad wanneer de eer of de goede naam van de overledene of diens nabestaanden geschonden worden. Nabestaanden kunnen op basis hiervan een immateriële schadevergoeding eisen.¹²⁰ Denk hierbij aan het voorbeeld van nabestaanden van een NSB'er die het verleden van hun overleden vader wordt nagedragen.

Kortom, de bepaling dat de AVG niet van toepassing is op persoonsgegevens van overledenen is niet het hele verhaal. Archiven, bibliotheken en culturele erfgoedinstellingen kunnen alsnog gebonden zijn aan de regels van de AVG indien de gegevens óók betrekking hebben op nog levende personen. Daarnaast kunnen zij te maken hebben met de regels rondom het portretrecht en de maatschappelijke zorgvuldigheidseisen met betrekking tot onder meer de eer en de goede naam van de overledene. Tot slot bevatten de Archiefwet en de Wob een eigen toets voor de eerbiediging van de persoonlijke levenssfeer bij het al dan niet stellen van openbaarheidsbeperkingen en de opheffing daar-

116 CBP Richtsnoeren (2007), *Publicatie van persoonsgegevens op internet*, p. 11. Geraadpleegd van https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf.

117 Artikel 20 juncto 25a Auteurswet.

118 Artikel 21 Auteurswet.

119 Artikel 6:162 BW.

120 Artikel 6:106 lid 1 sub c BW. De memorie van toelichting bij de Wet bescherming persoonsgegevens geeft voorts expliciet aan dat een schadevergoeding op basis van onrechtmatige daad mogelijk is wanneer onzorgvuldig omgegaan wordt met gegevens van overledenen (*Kamerstukken II*, 1997-1998, 25 892, nr. 3, p. 50).

van. Deze toets, zoals eerder in dit artikel besproken is, is niet per se gerelateerd aan de AVG. Hoewel de AVG dus niet van toepassing is, zal er toch rekening gehouden moeten worden met de eerbiediging van de persoonlijke levenssfeer, zoals de eer en de goede naam, van de overledene.

13. Afronding

In dit artikel gingen wij in op de verhouding tussen de AVG enerzijds en de Archiefwet, Wob anderzijds. Daarbij behandelden wij ook de diverse uitzonderingen die de wetgeving kent voor verwerking van persoonsgegevens door archieven en bibliotheken, maar ook ten behoeve van onderzoek en journalistiek. In dit artikel hebben wij ons in het bijzonder gericht op archieven, bibliotheken, gemeenten, samenwerkingsverbanden van gemeenten en onderzoeksinstellingen, die in hun dagelijkse werkzaamheden te maken krijgen met vragen over de verwerking en bescherming van persoonsgegevens bij het verwerken van (historische) archiefbestanden.