Adviesrapport
voorbereiding Archiefsector op de AVG

ICTRECHT

| | |
|---|---|
| Versie: | 1.0 |
| Gemaakt door: | Mr.dr. Mathieu Paapst CIPM<br>ICTRecht B.V. |
| Gemaakt voor: | KVAN/BRAIN |
| Laatste aanpassing gedaan op: | April 2018 |

**ICTRecht B.V.**
Jollemanhof 12
1019 GW Amsterdam

TELEFOON
020 663 1941

E-MAIL
info@ictrecht.nl

INTERNET
ictrecht.nl

KVK
34216164

BTW
NL822330040B01

IBAN
NL07 RABO 0325 2813 78

Overzicht wijzigingen

| Versie | Gemaakt door | Datum | Omschrijving wijzigingen |
|---|---|---|---|
| 1.0 | ICTRecht | 30 april 2018 | Eerste versie |

# Inhoud

# Inleiding

Vanaf 25 mei 2018 zullen in de gehele EU dezelfde privacyregels gelden (de Algemene Verordening Gegevensbescherming, AVG). Deze nieuwe regels zullen de Wet bescherming persoonsgegevens (Wbp) vervangen. Het is van groot belang dat medewerkers van archiverende organisaties kennis hebben van een juiste omgang met persoonsgegevens.

KVAN/Brain heeft ons, ICTRecht, gevraagd om archiverende organisaties te ondersteunen bij de voorbereiding op de Algemene Verordening Gegevensbescherming (AVG). In dit adviesrapport wordt een generiek overzicht gegeven van de huidige stand van zaken met betrekking tot de bescherming van persoonsgegevens bij archiverende organisaties. Wij hebben in de afgelopen maanden een quickscan uitgevoerd bij drie onderling totaal verschillende archiverende organisaties: NIOD, RHC Eindhoven en Haags Gemeentearchief. De gegevens voor de quickscan hebben wij verzameld aan de hand van interviews en de bestaande documenten van de onderzochte organisaties (o.a. beleidsdocumenten over de meldplicht datalekken, privacyreglementen en bruikleenovereenkomsten). Waar wij individueel per organisatie vooral naar hebben gekeken is de vraag of de medewerkers bewust omgaan met persoonsgegevens, bekend zijn met de regels die gelden omtrent de verwerking van persoonsgegevens, bekend zijn met de regels over de meldplicht datalekken en in hoeverre zij de regels van de AVG in praktijk kunnen toepassen (of dat er nog veel onduidelijkheid is) . Op basis van de drie individuele onderzoeken zijn een aantal terugkerende thema's besproken tijdens twee bijeenkomsten met de werkgroep AVG. Deze thema's zijn vervolgens generiek gemaakt omdat wij denken dat deze bij meer archiverende organisaties een rol spelen, en vervolgens opgenomen in dit adviesrapport.

Dit adviesrapport heeft als doel om de generieke bevindingen te presenteren en mogelijke verbeterpunten aan te kaarten. Dit adviesrapport vormt voor archiverende organisaties een goede basis voor vervolgactiviteiten omtrent het afronden van het AVG-implementatietraject. De concrete bevindingen en aanbevelingen worden hierbij uitgewerkt, waarbij de geïnventariseerde generieke risico's op basis van prioriteit worden behandeld.

# Bevindingen en aanbevelingen

Wij adviseren archiverende organisaties om onderstaande punten uit te voeren, teneinde te voldoen aan de wettelijke eisen die gelden voor het verwerken van persoonsgegevens, waarvan sommige niet wettelijk verplicht, maar wel zeer praktisch zijn.

- Bepaal voor de te verwerken persoonsgegevens of je verwerker, verwerkingsverantwoordelijke of mede verantwoordelijke bent, of daarvan onderdeel uitmaakt;
- Stel een verwerkingsregister op en maak (indien de organisatie dit nog niet heeft) een datastroom;
- Controleer het register en de daarbij horende datastroom op regelmatige basis om deze up-to-date te houden.
- Neem na overbrenging de beperkt-openbare archiefbescheiden op in het register.
- Controleer het overzicht van gebruikte applicaties en vul deze aan waar nodig;
- Wijs een persoon in de organisatie aan die verantwoordelijk is om deze lijst up-to-date te houden.
- Controleer het overzicht van derde partijen waar de archiverende organisatie mogelijk mee te maken heeft, en vul deze aan waar nodig;
- Wijs een persoon, of meerdere personen in de organisatie aan die verantwoordelijk is / zijn om deze lijst up-to-date te houden;
- Zorg dat er voor iedere verstrekking van persoonsgegevens inzichtelijk is vanuit welke privacytechnische rol dit plaatsvindt en sluit waar nodig een verwerkersovereenkomst.
- Stel vanuit de sector een uniforme verwerkersovereenkomst op;
- Stuur de verwerkersovereenkomst naar alle leveranciers (eventueel in gezamenlijkheid door middel van een gebruikersvereniging) en draag zorg voor ondertekening van de overeenkomst;
- Pas waar nodig de bruikleen-, bewaargeving-, of schenkingsovereenkomsten aan, rekening houdende met de AVG, en uniformeer deze vanuit de sector.
- Controleer periodiek of gegevens afdoende beveiligd worden en doe dit tevens bij derde partijen waar persoonsgegevens zijn ondergebracht;
- Stel een intern beveiligingsbeleid op waarin wordt vastgelegd welke gegevens op welke manier worden beveiligd;
- Communiceer dit beleid onder de medewerkers en houd de kennis van de medewerkers op peil door bijvoorbeeld trainingen. Controleer tevens periodiek of de maatregelen toegepast worden.
- Stel een plan op waarin de omgang met datalekken wordt omschreven, en informeer de medewerkers over het bestaan van de meldplicht en het calamiteitenplan;
- Houd een register bij waarin alle beveiligingsincidenten worden geregistreerd;
- Vergroot de bewustwording van privacy onder de medewerkers door trainingen of kennissessies;
- Pas het huidige personeelsreglement aan, of stel een apart privacybeleid op, om de normen en waarden op privacyvlak vast te leggen

- Breng in kaart welke gegevens er worden verwerkt en of hiervoor wettelijke bewaartermijnen zijn vastgesteld;
- Stel bewaartermijnen voor diverse gegevens vast indien deze nog niet wettelijk zijn vastgesteld;
- Controleer periodiek of de bewaartermijnen nog niet zijn verstreken.
- Onderzoek of er naast gezinskaarten nog meer archiefbescheiden online (of ter raadpleging op de studiezaal) beschikbaar zijn die bijzondere persoonsgegevens van nog levende personen bevatten.
- Haal (archiefbescheiden bevattende) bijzondere persoonsgegevens van nog levende personen offline voorzover er geen grondslag (meer) is voor de publicatie;
- Registreer de betreffende archiefbescheiden in het verwerkingsregister.
- Leg de omgang met de rechten van betrokkenen –zowel voor als na overbrenging- vast in het interne privacy beleid;
- Zorg dat de identiteit van de aanvrager gecontroleerd wordt voordat gegevens worden verstrekt.
- Denk na over de wijze waarop betrokkenen hun rechten kunnen inroepen voor zowel nieuw over te brengen alsook reeds overgebrachte archiefbescheiden.
- Stel, op basis van het verwerkingsregister, vast welke verwerkingen van persoonsgegevens niet noodzakelijk zijn voor het doel waarvoor ze zijn verkregen, beperk deze verwerkingen en staak de verwerking als er geen rechtmatige grondslag voor is;
- Probeer als sector op een uniforme wijze om te gaan met de bezoekersregistratie: vraag zo weinig mogelijk, en bewaar zo kort mogelijk.
- Voor het bepalen van de noodzakelijkheid voor het opvragen van persoonsgegevens kan navraag worden gedaan bij de diverse afdelingen die doeleinden van de verwerking vaststellen, zodat kan worden nagegaan of het opvragen van persoonsgegevens hiervoor noodzakelijk is;
- Hanteer de Archiefwet als het kader om voor over te brengen archiefbescheiden af te wegen of verdere dataminimalisatie noodzakelijk is.
- Beslis of de functie van FG intern of extern wordt belegd en wijs vervolgens een FG aan;
- Voorkom belangenverstrengeling als de functie intern wordt belegd;
- Maak intern bekend dat er een FG is, en dat dit dus ook de persoon is bij wie alle medewerkers voor privacyvragen terecht kunnen;
- Meld de FG vanaf 25 mei 2018 aan bij de Autoriteit Persoonsgegevens.

# 1. Bepaal de rol van de archiverende organisatie

**1.1 Gegevensverantwoordelijk**

De AVG spreekt over de verwerkingsverantwoordelijke en de verwerker. Een verwerker is een partij die in opdracht van een ander persoonsgegevens verwerkt, en daarbij niet zelf het doel en de middelen van die verwerking bepaalt. Die ander heet dan met een mond vol de verwerkingsverantwoordelijke, en zoals de naam aangeeft is dat de partij die verantwoordelijkheid draagt voor de verwerking. Deze kiest dus het doel, zoals salarisadministratie, nieuwsbrieven, bezoekersadministratie of beveiliging van het pand. Ook kiest deze de middelen: salarispakket X, collectiebeheersysteem Y, een WhatsApp groep of cameratoezicht. De verwerker voert dit vervolgens netjes uit.
In de praktijk zijn de meeste verwerkers wat actiever. Ze kiezen in ieder geval vaak zelf de middelen, zoals een bepaald softwarepakket of de wijze van opslag of beheer. Een archiverende organisatie zal bijvoorbeeld meestal zelf al te gebruiken software gekozen hebben, en bepaalt vanuit haar expertise op welke wijze inzage kan worden gegeven in archiefstukken. Dat maakt het soms lastig te bepalen of iemand verwerker is of juist verantwoordelijke. Uiteindelijk geeft dan de keuze voor het doel de doorslag: wie beslist er uiteindelijk wat er precies gaat gebeuren. De relevante factoren zijn:

1. Mate van zeggenschap. Hoe meer zeggenschap een partij heeft bij de uitvoering van de opdracht, hoe eerder deze zelf verantwoordelijke is.
2. Gebruik van resultaten. Als een partij de resultaten van een verwerking zelf kan gebruiken, wijst dat eerder op verantwoordelijke-schap.
3. Aard van de dienstverlening. Als de dienstverlening typisch gericht is op één klant of opdrachtgever, en er geen eigen gebruik van de gegevens wordt gemaakt, wijst dat op verwerkerschap.
4. Transparantie van de dienstverlening. Hoe meer inzicht de ene partij heeft in wat er gebeurt bij de andere partij, hoe eerder die andere partij als verwerker te zien is.
5. Grip op de dienstverlening. Hoe meer ruimte de ene partij heeft om een verwerking te laten staken of aanpassen, hoe eerder de andere partij als verwerker te zien is.
6. Contractuele bepalingen. Een contract kan expliciet zeggen of een partij verwerker is of niet. Dit is niet doorslaggevend, maar weegt wel mee.

Indien de archiverende organisatie organisatorisch deel uit maakt van een overheidsorgaan (zorgdrager) dan is dat overheidsorgaan de verwerkingsverantwoordelijke ten aanzien van persoonsgegevens (die in archiefbescheiden opgenomen kunnen zijn). Dat geldt in het bijzonder voor archiefbescheiden zoals bedoeld in art. 1 sub c Archiefwet 1995, met uitzondering van het daar onder punt 3 genoemde. Bij bewaargeving van particuliere archieven en collecties is de archiverende organisatie ten aanzien van die in bewaring te nemen archieven en collecties vooral verwerker. In het geval van bruikleen of schenking ligt het eerder voor de hand dat de ontvanger (mede-) verwerkingsverantwoordelijke gaat worden.
Indien de archiverende organisatie zelfstandig opereert (bijvoorbeeld als Gemeenschappelijke Regeling of als private organisatie, zoals de Stichting Nederlands instituut voor Beeld en Geluid) dan dient expliciet voor die organisatie te worden vastgesteld wie er ten aanzien van welke persoonsgegevens aan te

wijzen is als verwerkingsverantwoordelijke. In het geval van het NIOD is dat bijvoorbeeld de KNAW, en in het geval van het Haags Gemeentearchief is dat het College van burgemeester en wethouders. In het geval van het RHC Eindhoven bestaat er over de bestuurlijke positionering onduidelijkheid.
Dit rapport is geschreven vanuit de rol van de verwerkingsverantwoordelijke.

Aanbevelingen

- Bepaal voor de te verwerken persoonsgegevens of je verwerker, verwerkingsverantwoordelijke of mede verantwoordelijke bent, of daarvan onderdeel uitmaakt;

# 2. Inventarisatie van persoonsgegevens

**2.1 Register**

Voldoen aan privacywetgeving begint met het maken van een overzicht van alle persoonsgegevens die worden verwerkt binnen de organisatie. Het is praktisch om een dergelijk overzicht te hebben, bovendien geldt vanaf 25 mei 2018 de wettelijke plicht om een register bij te houden van alle persoonsgegevens die worden verwerkt in een organisatie.[1] Een dergelijk verwerkingsregister is verplicht voor iedere organisatie die méér dan incidenteel persoonsgegevens verwerkt, of indien er op grote schaal bijzondere persoonsgegevens worden verwerkt/personen worden gemonitord. Aangezien de archiverende organisaties structureel archiefbescheiden (bevattende persoonsgegevens) verwerken, en incidenteel ook bijzondere en strafrechtelijke persoonsgegevens, dient door de verwerkingsverantwoordelijke een verwerkingsregister opgesteld te worden, en kan geen beroep worden gedaan op de uitzonderingsgrond voor kleine organisaties (van minder dan 250 medewerkers). Bovendien zou die uitzondering enkel gelden ten aanzien van incidentele verwerkingen (zoals de bezoekersregistratie van een eenmalig evenement).

Het register dient opgesteld te worden vanuit de rol van verantwoordelijke en dient ten minste de volgende informatie te bevatten:

- naam en contactgegevens van de verwerkingsverantwoordelijke;
- de doeleinden waarvoor gegevens worden verwerkt;
- de categorieën gegevens (zoals NAW-gegevens, contactgegevens);
- de categorieën betrokkenen (bijvoorbeeld bezoekers studiezaal, medewerkers, burgers);
- de categorieën ontvangers (aan wie worden de gegevens verstrekt, denk hierbij aan softwareleveranciers, onderzoekers);
- informatie over eventuele doorgifte van gegevens naar derde landen;
- de bewaartermijnen van de gegevens;
- de manieren waarop gegevens zijn beveiligd.

**2.2 Datastroom**

Naast de plicht om een register bij te houden, is het praktisch om een datastroom te maken. Een datastroom maakt inzichtelijk op welke manier gegevens zich door de organisatie bewegen, en welke producten er ontstaan als gevolg van de interne processen. Het is belangrijk om te weten binnen welke afdeling(en) gegevens zich bevinden, bijvoorbeeld om op de juiste plek toepasselijke beveiligingsmaatregelen toe te kunnen passen. Maar ook om inzichtelijk te krijgen met welke ontvangers de gegevens gedeeld worden, om daarmee vervolgens een passende overeenkomst mee te sluiten.
De datastroom moet duidelijk maken:

- hoe de gegevens de organisatie binnenkomen;
- via welke (IT-)systemen en derden ze verwerkt worden;
- waar de gegevens opgeslagen worden;
- hoe ze uiteindelijk de organisatie weer verlaten.

1 Art. 30 AVG.

Een uitgewerkte datastroom zorgt voor overzicht van alle gegevensverwerkingen en input voor het verplichte register.

Zowel het register als de datastromen dienen continu up-to-date gehouden te worden. Dit is te realiseren door personen van verschillende afdelingen periodiek, bijvoorbeeld eens per kwartaal, naar het register te laten kijken en deze waar nodig aan te passen.

**2.3 Constateringen**

Er is onder sommige archiverende organisaties onduidelijkheid of de plicht om een register aan te leggen ook van toepassing is op archiefbescheiden. Het register dient vooral om intern voor een verwerkingsverantwoordelijke duidelijkheid te verkrijgen over welke persoonsgegevens zich waar binnen een werkproces kunnen bevinden, op welke wijze dat beveiligd zou moeten zijn, en of er bijzonderheden zijn met betrekking tot de bewaartermijnen. Voor niet overgebrachte archiefbescheiden is deze plicht onverkort van toepassing. De verwerkingsverantwoordelijke zal dit in de rol van archiefvormer in kaart moeten brengen. Dat hoeft uiteraard niet per individueel document, maar zal per afzonderlijk proces kunnen worden beschreven. De selectielijst kan voor het bepalen van de termijnen gebruikt worden. Het bovenstaande is ook van toepassing indien een archiverende organisatie niet (volledig) onder het regime van de Archiefwet valt (zoals Stichting Beeld en Geluid), en de collecties door hen niet overgebracht zullen gaan worden in de zin van de Archiefwet. Er bestaat voor collecties bestaande uit journalistieke werken, zoals een krantenarchief, overigens een uitzondering op de plicht voor opname daarvan in een verwerkingsregister. Het is dus niet nodig om alle oude kranten door te lezen op zoek naar mogelijke (categorieën van) persoonsgegevens.

Na overbrenging van archiefbescheiden naar een archiefbewaarplaats doet zich een iets andere situatie voor. Waar het gaat om overgebrachte archiefbescheiden (bevattende persoonsgegevens) die op grond van de Archiefwet openbaar zijn geworden, voegt het daarvan opnemen in een art. 30 register niets meer toe. Het is daarom niet nodig om deze archiefbescheiden in het verwerkingsregister op te nemen. Dat is anders waar het gaat om archiefbescheiden waar aan de openbaarheid een beperking is, of moet worden gesteld. Die beperking komt op basis van de Archiefwet over het algemeen op 75 jaar, maar ook langer is mogelijk. De beperking kan binnen de archiefwet bijvoorbeeld worden opgelegd vanwege de bescherming van de persoonlijke levenssfeer. Ook kan de beperking voortvloeien uit andere wetgeving. Denk daarbij aan het vanuit de AVG voortvloeiende verbod om bijzondere persoonsgegevens van nog levende personen te verwerken.
In het verwerkingsregister zouden categorieën van beperkt-openbare archiefbescheiden daarom gewoon moeten worden opgenomen, inclusief de al dan niet uit een speciale wet voortvloeiende beperkingstermijn, aan wie de gegevens mogelijk worden verstrekt (denk aan onderzoekers, of aan een hosting partij) en de wijze waarop deze stukken beveiligd zijn (denk bijvoorbeeld aan autorisatie, of door encryptie). Het moet daarmee voor de verwerkingsverantwoordelijke inzichtelijk worden op welke inventarisnummers een dergelijke beperking rust.

Aanbevelingen

- Stel een verwerkingsregister op en maak (indien de organisatie dit nog niet heeft) een datastroom;
- Controleer het register en de daarbij horende datastroom op regelmatige basis om deze up-to-date te houden.
- Neem na overbrenging de beperkt-openbare archiefbescheiden op in het register.

# 3. Overzicht gebruikte applicaties

**3.1 IT overzicht**

Organisaties maken gebruik van diverse applicaties om persoonsgegevens en archiefbescheiden (bevattende persoonsgegevens) te verwerken. Onder risico 2 is genoemd dat uit een dergelijke datastroom blijkt waar en binnen welke IT-systemen persoonsgegevens zich binnen (of buiten) de organisatie bevinden. Het is belangrijk voor een verwerkingsverantwoordelijke om het volledige IT-landschap in kaart te hebben. Dat is nodig om de noodzakelijke beveiligingsmaatregelen te kunnen treffen en om de juiste juridische afspraken met derde partijen te kunnen over het gebruik van de persoonsgegevens. Dat betekent dat er een uitputtend overzicht moet zijn van gebruikte softwareapplicaties binnen de organisatie, en zeker waar het raakt aan de bedrijfsvoering van de archiverende organisatie. Te denken valt aan:

- Office software inclusief email
- DMS zoals Sharepoint
- Netwerkopslag
- Collectiebeheersysteem
- Opslagvoorzieningen zoals DiVault
- Statistiek software (in het kader van de website)
- Financiële administratie en loonadministratie
- Samenwerkingsplatforms zoals Basecamp of Pleio

Let op dat het hier dus niet uitsluitend hoeft te gaan om software of applicaties aangeschaft en beheerd door de verwerkingsverantwoordelijke. Ook applicaties van derden die “gratis” gebruikt worden dienen in dit overzicht opgenomen te worden zodra er persoonsgegevens worden gedeeld. Hierbij kan gedacht worden aan applicaties zoals Dropbox of Wetransfer.

Aanbevelingen

- Controleer het overzicht van gebruikte applicaties en vul deze aan waar nodig;
- Wijs een persoon in de organisatie aan die verantwoordelijk is om deze lijst up-to-date te houden.

# 4. Overzicht van derde partijen

### 4.1 Overzicht

Naast een overzicht van applicaties is het belangrijk om inzichtelijk te hebben met welke derde partijen persoonsgegevens gedeeld worden. Deze derde partijen kunnen softwareleveranciers zijn, maar het kan ook gaan om dienstverleners die (naast software) diensten aanbieden voor bijvoorbeeld het converteren van bronnen. De lijst met derde partijen met wie persoonsgegevens gedeeld worden, bestaat daarom uit meer partijen dan alleen softwareleveranciers. Om deze reden is het belangrijk deze lijst apart te registreren van het overzicht gebruikte applicaties. Het verkrijgen van dit inzicht is noodzakelijk om te kunnen voldoen aan de AVG. Als verantwoordelijke partij voor de verwerking van persoonsgegevens is het aan de verwerkingsverantwoordelijke om zorg te dragen dat de gegevens die de eigen organisatie verlaten, ook zorgvuldig worden verwerkt bij de ontvangers van persoonsgegevens.

### 4.2 Rolverdeling

Bij het inventariseren van deze derde partijen, en ook applicaties, dient inzichtelijk te zijn hoe de privacytechnische rolverdeling eruitziet.
Privacywetgeving maakt daarin op hoofdlijnen een onderscheid tussen de verantwoordelijke partij en de verwerkende partij. De eerste partij bepaalt wat er met persoonsgegevens dient te gebeuren en waarom dit plaats moet vinden. De tweede partij voert verwerkingen van persoonsgegevens in opdracht van de eerstgenoemde partij uit.
Niet alle derde partijen treden op als verwerker voor de archiverende organisatie. De Belastingdienst ontvangt bijvoorbeeld wel persoonsgegevens van de archiverende organisatie, namelijk betreffende de medewerkers, maar ze verwerken deze gegevens niet voor deze organisatie. Zij verwerken de persoonsgegevens ten behoeve van eigen werkzaamheden en verplichtingen.

Aanbevelingen

- Controleer het overzicht van derde partijen waar de archiverende organisatie mogelijk mee te maken heeft, en vul deze aan waar nodig;
- Wijs een persoon, of meerdere personen in de organisatie aan die verantwoordelijk is / zijn om deze lijst up-to-date te houden;
- Zorg dat er voor iedere verstrekking van persoonsgegevens inzichtelijk is vanuit welke privacytechnische rol dit plaatsvindt en sluit waar nodig een verwerkersovereenkomst.

# 5. Verwerkersovereenkomsten afsluiten

ICTRECHT

**5.1 Verplichting**

Als het overzicht van gebruikte applicaties en derde partijen compleet is kan de volgende stap gezet worden. Dat betreft het maken van juridische afspraken met deze derde partijen. Wanneer een externe partij namens de archiverende organisatie persoonsgegevens (binnen archiefbescheiden) verwerkt, is de archiverende organisatie verplicht om met die derde partij afspraken te maken over de mate waarin en de manier waarop persoonsgegevens worden verwerkt. De derde partij is dan 'verwerker' in opdracht van de archiverende organisatie, die in dit geval 'verwerkingsverantwoordelijke' is.[2] De afspraken over de omgang met persoonsgegevens tussen deze partijen moeten worden vastgelegd, dat gebeurt in een verwerkersovereenkomst. Ook wanneer de archiverende organisatie zelf in opdracht van andere partijen persoonsgegevens verwerkt, zoals in het geval van bruikleen, en als verwerker is aan te merken, moet een verwerkersovereenkomst gesloten worden.

In de verwerkersovereenkomst worden onder andere afspraken gemaakt over verantwoordelijkheden, audits en het melden van incidenten zoals datalekken.[3] Naast de eisen die de AVG aan de overeenkomst stelt kunnen partijen zelf zaken opnemen die zij relevant vinden, bijvoorbeeld over aansprakelijkheid.[4] De verwerkersovereenkomst hoeft geen opzichzelfstaand document te zijn. Het integreren van deze bepalingen in een overeenkomst van opdracht, een bruikleen/bewaargevingsovereenkomst of in een schenkingsovereenkomst is toegestaan.

Aangezien de archiverende organisatie als verantwoordelijke voor verschillende gegevensverwerkingen is aan te merken, is het aan de verantwoordelijke om deze verwerkersovereenkomsten zo spoedig mogelijk te sluiten. Wij adviseren om één persoon binnen de organisatie verantwoordelijk te maken voor het najagen van de status van de verwerkersovereenkomsten.

**5.2 Constateringen**

Er ontbreken bij veel archiverende organisaties nog de verwerkersovereenkomsten met betrekking tot de derde partijen waarmee persoonsgegevens gedeeld (kunnen) worden. In het bijzonder moet daarbij gewezen worden op de Collectiebeheersystemen (zoals Mais-Flexis), waarin bij sommige archiverende organisaties ook de gegevens van de bezoekers van de studiezaal worden geregistreerd. Tevens kan gedacht worden aan extern gehoste systemen zoals -maar niet beperkt tot- Adlib, of beeldbanken zoals Memorix/Picturae.
Ook ontbreken er in veel bruikleen-, bewaargeving-, of schenkingsovereenkomsten specifieke bepalingen over de naleving van de AVG.

[2] De verwerkingsverantwoordelijke is de partij die het doel en de middelen van de verwerking bepaalt, de verwerker is de partij die bij de verwerking van persoonsgegevens in opdracht van de verwerkingsverantwoordelijke handelt (art. 4 onder 7 en 8 AVG).
[3] Onder huidige wetgeving, de Wet bescherming persoonsgegevens (Wbp), wordt er nog gesproken over een 'bewerker' en een 'bewerkersovereenkomst'. In de Algemene Verordening Gegevensbescherming (AVG) wordt gesproken over 'verwerker' en 'verwerkersovereenkomst'. Inhoudelijk verschillen deze begrippen echter niet.
[4] De wettelijke eisen worden opgesomd in art. 28 lid 3 AVG.

Aanbevelingen

- Stel vanuit de sector een uniforme verwerkersovereenkomst op;
- Stuur de verwerkersovereenkomst naar alle leveranciers (eventueel in gezamenlijkheid door middel van een gebruikersvereniging) en draag zorg voor ondertekening van de overeenkomst;
- Pas waar nodig de bruikleen-, bewaargeving-, of schenkingsovereenkomsten aan, rekening houdende met de AVG, en uniformeer deze vanuit de sector.

# 6. Beveiliging van persoonsgegevens

### 6.1 Vereisten

De Wbp en de AVG eisen dat er passende technische en organisatorische maatregelen genomen worden teneinde persoonsgegevens te beschermen tegen verlies of andere onrechtmatige verwerkingen. Omdat de wet technologie onafhankelijk is, worden er geen concrete maatregelen genoemd. De maatregelen dienen een passend niveau van beveiliging te bieden waarbij rekening wordt gehouden met de stand van de techniek, de kosten van de uitvoering, de risico's van de gegevensverwerkingen en de aard van de persoonsgegevens. Deze maatregelen dienen niet alleen te zien op de persoonsgegevens die reeds verzameld zijn, maar tevens op onnodige verzameling van persoonsgegevens. Dat wil zeggen dat bijvoorbeeld een zorgdrager zich continu af dient te vragen of alle gebruikte persoonsgegevens noodzakelijk zijn voor de beoogde doelen.

Alvorens deze maatregelen te kunnen bepalen is het van belang dat de aanwezige gegevens, en de doelen waarvoor de gegevens aanwezig zijn, in kaart zijn gebracht. Mede daarom is de inventarisatie van persoonsgegevens, middels het register en de datastroom van wezenlijk belang. Om de continuïteit van de maatregelen te waarborgen adviseren wij om een intern informatiebeveiligingsplan te hanteren, waarin alle afspraken omtrent veilige omgang met gegevens vastgelegd worden. Dit plan bestaat uit zowel technische als organisatorische maatregelen. Deze twee typen maatregelen worden hieronder uitgelegd.

### 6.2 Technisch

Alvorens de technische beveiligingsmaatregelen ontwikkeld, vastgelegd en gecontroleerd kunnen worden, is het van belang dat de archiverende organisatie een helder beeld heeft van alle softwareapplicaties die worden gebruikt. Vervolgens zal per applicatie beoordeeld moeten worden in hoeverre de persoonsgegevens beveiligd worden en zal dit periodiek gecontroleerd moeten worden. Dit kan bijvoorbeeld door het uitvoeren van een jaarlijkse audit door een externe partij. Dergelijke testen zijn uit te voeren op eigen systemen, maar op het moment dat persoonsgegevens tevens bij derde partijen ondergebracht worden dienen soortgelijke testen daar ook uitgevoerd te worden. Bepalingen over het uitvoeren van deze testen moeten zijn opgenomen in de verwerkersovereenkomsten.

### 6.3 Organisatorisch

Naast de technische kant van de beveiliging is de organisatorische kant minstens zo belangrijk. Een softwareapplicatie kan technisch goed beveiligd zijn, maar dit beschermt de data niet tegen toegang tot gegevens door personen die nog autorisaties hebben maar deze uit hoofde van hun functie niet meer zouden moeten hebben. Hetzelfde geldt voor het afsluiten van opbergkasten met gevoelige documenten, of het vergrendelen van een computerscherm op het moment dat iemand zijn werkplek verlaat.

Het is niet realistisch om alle handelingen van de medewerkers te monitoren, maar het is wel belangrijk om handvatten aan de medewerkers te geven hoe zij om dienen te gaan met de beveiliging van persoonsgegevens.

Uiteraard is het van belang dat er ook controle op de naleving van deze regels uitgevoerd wordt. Daarbij speelt bewustwording binnen de organisatie een grote rol. Alle medewerkers moeten zich bewust zijn van het belang van de binnen de archiverende organisatie aanwezige data en de zorgvuldige omgang daarmee. Bewustwording kan gestimuleerd worden door het geven van training, het communiceren en promoten van het interne beleid, maar ook door bijvoorbeeld een 'nep' phishingmail rond te sturen en te testen hoeveel medewerkers hierop reageren.

Aanbevelingen

- Controleer periodiek of gegevens afdoende beveiligd worden en doe dit tevens bij derde partijen waar persoonsgegevens zijn ondergebracht;
- Stel een intern beveiligingsbeleid op waarin wordt vastgelegd welke gegevens op welke manier worden beveiligd;
- Communiceer dit beleid onder de medewerkers en houd de kennis van de medewerkers op peil door bijvoorbeeld trainingen. Controleer tevens periodiek of de maatregelen toegepast worden.

# 7. Omgang met datalekken

### 7.1 Meldplicht

Sinds 1 januari 2016 zijn organisaties die persoonsgegevens verwerken wettelijk verplicht om incidenten aangaande de beveiliging van persoonsgegevens, zogeheten datalekken, te melden bij de Autoriteit Persoonsgegeven en eventueel bij de betrokkenen (de personen op wie de persoonsgegevens betrekking hebben). Om goed voorbereid te zijn op mogelijke datalekken, is het van belang een calamiteitenplan op te stellen dat invulling geeft aan deze meldplicht. In een dergelijk beleid worden afspraken gemaakt over de omgang met datalekken.

Uit een calamiteitenplan moet duidelijk worden wie de leiding neemt in een dergelijk traject, binnen welke termijn er melding wordt gemaakt en hoe het lek wordt gedicht. In een calamiteitenplan moeten onder andere de volgende onderwerpen worden opgenomen:

1. Hoe worden mogelijke datalekken geconstateerd?
2. Hoe worden mogelijke datalekken geïdentificeerd?
3. Hoe en door wie wordt er bepaald of een datalek gemeld dient te worden?
4. Hoe wordt een datalek gemeld aan de toezichthouder?
5. Hoe wordt een datalek gedocumenteerd?

Met de komst van de AVG dient ieder beveiligingsincident, ongeacht of het als datalek moet worden gemeld bij de Autoriteit Persoonsgegevens, te worden gedocumenteerd inclusief de gevolgen en de genomen maatregelen om eenzelfde situatie in de toekomst te voorkomen. De Autoriteit Persoonsgegevens kan toegang verlangen tot deze documentatie, en de documentatie moet adequaat zijn om de toezichthouder te laten controleren of datalekken daadwerkelijk worden gemonitord en opgevolgd.

### 7.2 Constateringen

Uit de interviews en aangeleverde documenten is gebleken dat medewerkers vaak wel weten dat er –al dan niet vanuit de zorgdrager- een datalekprotocol of een calamiteitenplan beschikbaar is, maar dat het vaak onduidelijk is wie er onder welke omstandigheden verwerkingsverantwoordelijke is, welke afspraken er met verwerkers of subverwerkers zijn gemaakt over het melden van datalekken, en wanneer er binnen de archiverende organisatie überhaupt sprake is van een datalek. Om die laatste vraag te kunnen beantwoorden hebben wij hierna een stappenplan opgenomen dat gevolgd kan worden bij een vermoedelijk datalek.

### 7.3 Stappenplan

Niet alle datalekken moeten gemeld worden aan de toezichthouder. Het moet gaan om een datalek in verband met persoonsgegevens. Een datalek dat wel gemeld dient te worden aan de toezichthouder wordt als volgt omschreven in de AVG:

---

*Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of*

*de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.*

Een inbreuk hoeft niet te worden gemeld wanneer het onwaarschijnlijk is dat deze redelijkerwijs een risico voor betrokkenen met zich meebrengt. Om te inventariseren of iets een datalek is, zullen de volgende vragen in deze volgorde moeten worden beantwoord:

1. Is er sprake van een inbreuk op de beveiliging ('beveiligingsincident')?
2. Zijn er bij de inbreuk persoonsgegevens verloren gegaan? Of
3. Kan er niet worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt?

Iedere vraag is een stap in de beslissing of er sprake is van een datalek. Deze stappen zullen hieronder worden toegelicht.

### 7.3.1 Beveiligingsincident

Van een inbreuk op beveiliging is sprake wanneer zich daadwerkelijk een incident heeft voorgedaan. Alleen een dreiging van een inbreuk op de beveiliging is daarom nog geen incident. Voorbeelden van beveiligingsincidenten zijn:

- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Ontdekt u een beveiligingsprobleem en dicht u dat voordat het is misbruikt, dan is er geen sprake van een datalek. Daarvoor moet u wel te kunnen verifiëren dat het lek niet is misbruikt. Een inbreuk op de beveiliging wordt een datalek wanneer de inbreuk door verlies of onrechtmatige verwerking gevolgen heeft voor de persoonsgegevens.

### 7.3.2 Verlies van persoonsgegevens

Indien er door de inbreuk op de beveiliging (archiefbescheiden bevattende) persoonsgegevens verloren zijn gegaan en er is geen complete en actuele reservekopie meer van, dan is dit altijd te kwalificeren als een datalek.

### 7.3.3 Onrechtmatige verwerking

Het is echter ook mogelijk dat gegevens niet verloren zijn gegaan, maar wel onrechtmatig zijn verwerkt. Dit houdt bijvoorbeeld in dat onbevoegde personen toegang hebben verkregen tot gegevens waar zij geen toegang toe mochten hebben. Denk aan de publicatie zonder beperkingen van beperkt-openbare archiefbescheiden op het internet, of de toegang tot gegevens voor een onderzoeker zonder dat getoetst is of voldaan is aan de voorwaarden die uit art. 24 Uitvoeringswet AVG gelden.
Andere vormen van onrechtmatige verwerking zijn het onrechtmatig wijzigen/aantasten van persoonsgegevens en het al dan niet per ongeluk verstrekken van (archiefbescheiden bevattende) persoonsgegevens aan onbevoegden. Denk bijvoorbeeld ook aan de situatie waarbij iemand met een smartphone een foto maakt van een stuk dat niet gekopieerd mag worden.
Het is in dat geval aan de verwerkingsverantwoordelijke om aan te tonen dat iemand de gegevens niet heeft in kunnen zien, of er niets mee gedaan heeft.
Opgemerkt moet worden dat er ook sprake is van een datalek indien het gaat om

het onrechtmatig wijzigen of aantasten van persoonsgegevens opgenomen in archiefbescheiden die op grond van de Archiefwet al openbaar zijn.

**7.4 Melding maken?**
Op het moment dat er sprake is van een datalek zoals hierboven omschreven, dan is het aan de verwerkingsverantwoordelijke om per vastgesteld datalek te beoordelen of het datalek aan de toezichthouder gemeld moet worden. De toezichthouder stelt dat een datalek *níét* aan haar gemeld hoeft te worden indien "het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen". Hieronder wordt dit criterium nader uitgewerkt.

Kwantitatief ernstig
Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig). Zo zal een datalek waardoor over 50 personen gegevens openbaar zijn gemaakt, kwantitatief ernstig zijn en dus gemeld moeten worden aan de toezichthouder.

Kwalitatief ernstig
Daarnaast kan een lek ook ernstig zijn indien er geen grote hoeveelheden persoonsgegevens gelekt zijn, maar het wel om gevoelige persoonsgegevens gaat (kwalitatief ernstig). Een paar voorbeelden van wat gevoelige persoonsgegevens zijn:

- inloggegevens;
- financiële gegevens;
- kopieën van identiteitsbewijzen;
- strafrechtelijke gegevens;
- bijzondere persoonsgegevens (bijvoorbeeld over levensovertuiging of gezondheid);
- wachtwoord/inlognaam combinatie.

De aard en omvang van het datalek dienen telkens in overweging genomen te worden bij de afweging of een lek met betrekking tot bijzondere persoonsgegevens aan de toezichthouder gemeld dient te worden.

**7.5 Melding aan betrokkenen**
Het kan mogelijk zijn dat een datalek niet alleen aan de toezichthouder, maar ook aan de personen van wie de gegevens zijn gelekt (de betrokkenen) gemeld moet worden. Dit is het geval wanneer het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Hetzelfde geldt uiteraard indien er gegevens van medewerkers of bezoekers zijn gelekt.

De drempel voor het melden van een datalek aan de betrokkene ligt hoger dan voor het melden aan de Autoriteit Persoonsgegevens. Er dient daarom een nieuwe afweging gemaakt te worden voor melding aan de betrokkenen. Hierbij is de kwalificatie van een "Hoog risico" en de genomen beveiligingsmaatregelen van belang.

Hoog risico
Er is sprake van een hoog risico wanneer de te verwachten gevolgen van het datalek zich met grote waarschijnlijkheid voordoen. Er dient dan een melding

gemaakt te worden aan de betrokkenen. Negatieve gevolgen voor de rechten en vrijheden van betrokkenen kunnen bijvoorbeeld het volgende zijn:

- het niet kunnen uitoefenen van hun rechten (zoals wissing of rectificatie);
- identiteitsdiefstal- of fraude;
- financiële verliezen;
- ongedaan making van pseudonimisering en reputatieschade;
- discriminatie;
- verlies van controle over hun persoonsgegevens.

**7.6. Encryptie en hashing**

Een datalek hoeft niet aan de betrokkenen gemeld te worden indien de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Hiervan is bijvoorbeeld sprake als de persoonsgegevens voorzien zijn van een beveiliging die volgens de laatste stand van de techniek als 'veilig' kan worden aangemerkt. Denk hierbij bijvoorbeeld aan algemeen gebruikte vormen van encryptie of hashing.

**7.7. Onevenredige inspanning**

Als het informeren van alle betrokkenen een zware inspanning vereist bijvoorbeeld omdat het om een zeer groot aantal betrokkenen gaat of omdat de betrokkenen lastig te contacteren zijn (omdat bijvoorbeeld geen actuele adressen beschikbaar zijn) dan is een melding aan de betrokkene niet nodig. De betrokkenen worden dan op een andere manier geïnformeerd. Denk hierbij aan een openbare mededeling in landelijke nieuwswebsites of kranten of een persbericht verspreid door de toezichthouder.

**7.8. Maatregelen achteraf om het hoge risico te voorkomen**

Als er direct maatregelen genomen zijn na het datalek om de gevolgen van het datalek te voorkomen dan is het niet meer nodig om de betrokkenen alsnog te informeren. Denk hierbij aan een hacker die data heeft gestolen waarbij de hacker is opgepakt voordat hij de data heeft verspreid. Het datalek heeft al plaatsgevonden maar er zijn dusdanige maatregelen genomen dat er geen risico op verdere verspreiding is.

Aanbevelingen

- Stel een plan op waarin de omgang met datalekken wordt omschreven, en informeer de medewerkers over het bestaan van de meldplicht en het calamiteitenplan;
- Houd een register bij waarin alle beveiligingsincidenten worden geregistreerd;

# 8. Intern beleid inzake persoonsgegevens

Teneinde een zorgvuldige omgang met persoonsgegevens te kunnen bewerkstelligen, is het noodzakelijk om in de gehele organisatie dezelfde privacybeleving te hebben. Iedere werknemer dient op de hoogte te zijn van de waarde van persoonsgegevens en de zorgvuldige omgang daarmee. Daarbij gaat het ook om de gegevens van de eigen medewerkers. Uit het documentonderzoek en de afgenomen interviews bleken sommige archiverende organisaties dit laatste nog niet goed op het netvlies te hebben staan.

Een gedegen en werkbaar intern privacybeleid staat of valt met de privacybeleving bij de medewerkers. In het privacybeleid wordt omschreven hoe de processen met betrekking tot het verwerken van persoonsgegevens zijn ingericht. Resultaat van dergelijk beleid is dat bij nieuwe producten en projecten door de verwerkingsverantwoordelijke rekening wordt gehouden met de principes van 'Privacy by Design' (het implementeren van privacy maatregelen in de ontwikkelfase van een nieuw product en project) en 'Privacy by Default' (producten en projecten zo inrichten dat er standaard gebruik wordt gemaakt van privacyvriendelijke instellingen en configuraties). Beide principes nemen onder de AVG een belangrijke rol in. Medewerkers dienen zich continu bewust te zijn van het feit dat ze met persoonsgegevens werken en dat er vanuit oa de AVG, de Uitvoeringswet AVG, de WOB en vanuit de Archiefwet strikte regels gelden ten aanzien van de omgang met dergelijke gegevens. Trainingen of periodieke bewustwordingssessies kunnen hieraan bijdragen.

Vanwege de mogelijkheid bij archiverende organisaties tot thuiswerken verdient ook het gebruik van eigen hardware aandacht. Wanneer medewerkers hun e-mail bekijken (of andere via internet te benaderen applicaties zoals het collectiebeheersysteem gebruiken) op een privé-pc, -laptop, -tablet of -smartphone, bestaat het risico dat onbevoegden zichzelf toegang verschaffen door malafide software op de privé-hardware van medewerkers.

We adviseren om in het interne privacybeleid een aantal minimale eisen te stellen aan het gebruik van privé-apparatuur. Een voorbeeld is dat er een pincode op een telefoon moet zitten als de zakelijke e-mail erop binnengehaald wordt. Verder kan ook worden gedacht het hebben van adequate antivirussoftware en de meest recente software updates. Daarbij dient ook opgenomen te worden hoe de medewerkers moeten omgaan met verlies van hun eigen apparatuur wanneer hier werkgerelateerde gegevens op staan.

In het interne privacybeleid kan worden opgenomen welke software gefaciliteerd wordt. Zo wordt het voor alle medewerkers duidelijk welke software gebruikt kan worden. Door een dergelijk overzicht op te nemen in een intern beleid, kunnen medewerkers erop aangesproken worden indien blijkt dat ze gebruik maken van niet-toegestane software.

Naast bepalingen omtrent geheimhouding in de arbeidsovereenkomst en het personeelsreglement, of voor ambtenaren in art.2:5 Awb, adviseren wij om ook richting medewerkers te benadrukken dat dit tevens geldt voor beperkt openbare archiefbescheiden, en archiefbescheiden die bijzondere persoonsgegevens bevatten van nog levende personen.

Aanbevelingen

- Vergroot de bewustwording van privacy onder de medewerkers door trainingen of kennissessies;
- Pas het huidige personeelsreglement aan, of stel een apart privacybeleid op, om de normen en waarden op privacyvlak vast te leggen.

# 9. Bewaartermijnen van persoonsgegevens

Voor het bewaren van persoonsgegevens gelden vaak geen vaste bewaartermijnen, tenzij deze ergens in een wet zijn vastgelegd. Indien een dergelijke wettelijke bewaartermijn afwezig is, stelt de AVG dat persoonsgegevens slechts bewaard mogen worden voor zolang dat noodzakelijk is. Dit betekent dat op het moment dat het voor de verwerkingsverantwoordelijke niet meer noodzakelijk is om gegevens te bewaren, deze gegevens verwijderd zouden moeten worden.

Voor verwerkingsverantwoordelijken kan voor de te hanteren bewaartermijn worden aangesloten bij de termijnen genoemd in de selectielijsten. De selectielijsten zijn gebaseerd op een wettelijke verplichting (art. 5 Archiefwet). Dit houdt dus ook in dat voor alle gegevens waarvoor geen wettelijke bewaarplicht geldt, de verwerkingsverantwoordelijke zelf een bewaartermijn vast moet stellen. Deze bewaartermijnen zullen ook gedocumenteerd moeten worden, zodat de verwerkingsverantwoordelijke aan kan tonen welke bewaartermijnen zij –naast de termijnen in de selectielijst- hanteert.
Uiteraard moeten deze bewaartermijnen ook daadwerkelijk nageleefd worden, en zal er (automatisch) gecontroleerd moeten worden of een bewaartermijn al is verlopen of nog niet, en of de gegevens dus verwijderd moeten worden. Verder is het van belang dat op het moment dat er software wordt ontwikkeld of afgenomen, er gecontroleerd wordt of gegevens daadwerkelijk verwijderd kunnen worden uit de betreffende software.

Aanbevelingen

- Breng in kaart welke gegevens er worden verwerkt en of hiervoor wettelijke bewaartermijnen zijn vastgesteld;
- Stel bewaartermijnen voor diverse gegevens vast indien deze nog niet wettelijk zijn vastgesteld;
- Controleer periodiek of de bewaartermijnen nog niet zijn verstreken.

# 10. Bijzondere persoonsgegevens (gezinskaarten)

De afgelopen jaren hebben archiverende organisaties diverse archiefbescheiden via het internet openbaar voor een ieder toegankelijk gemaakt, en voor hergebruik beschikbaar gesteld. Soms bevatten deze archiefbescheiden echter bijzondere persoonsgegevens van nog levende personen. De gezinskaarten zijn daar een voorbeeld van. De AVG plaatst zichzelf boven de hergebruikrichtlijn, en geeft aan dat het in beginsel verboden is om bijzondere persoonsgegevens te verwerken.[5] Om deze gegevens wel te mogen verwerken (en eventueel openbaar te mogen maken) moet een nationale wet dat expliciet zo benoemen. Deze uitzondering is voor wetenschappelijk of historisch onderzoek, of voor statistische doeleinden opgenomen in artikel 24 Uitvoeringswet. De uitvoeringswet noemt daarbij als uitdrukkelijke voorwaarde dat bij de uitvoering van het onderzoek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig word geschaad. Niet valt in te zien waarom art 24 Uitvoeringswet door een archiverende organisatie ingeroepen kan worden als grondslag of uitzondering waarmee de gezinskaarten openbaar gemaakt kunnen worden.
Daarnaast is er voor het overbrengen naar een archiefbewaarplaats, en het behouden, bewerken en benutten, een uitzondering opgenomen in artikel 2a Archiefwet. Omdat onder het beheren van deze overgebrachte archiefbescheiden ook de raadpleging en het voor gebruik ter beschikking stellen aan het publiek zou kunnen vallen, is die verwerkingshandeling reeds onder de Wbp uitdrukkelijk in art 2a Archiefwet uitgesloten. De AVG wijzigt deze situatie niet. Dat betekent dat het openbaar maken van archiefbescheiden bevattende bijzondere persoonsgegevens van nog levende personen onder het verbod van de AVG blijft vallen. Als verordening heeft de AVG voorrang op de Archiefwet. Daarom is het niet noodzakelijk om alsnog op grond van de Archiefwet beperkingen te laten opleggen door de zorgdragers. Overgebrachte archiefbescheiden bevattende bijzondere persoonsgegevens van nog levende personen, waarop bij de overbrenging geen beperkte openbaarheid is opgelegd, vallen dus (alsnog) onder het verwerkingsverbod uit de AVG.

Aanbevelingen

- Onderzoek of er naast gezinskaarten nog meer archiefbescheiden online (of ter raadpleging op de studiezaal) beschikbaar zijn die bijzondere persoonsgegevens van nog levende personen bevatten.
- Haal (archiefbescheiden bevattende) bijzondere persoonsgegevens van nog levende personen offline voorzover er geen grondslag (meer) is voor de publicatie;
- Registreer de betreffende archiefbescheiden in het verwerkingsregister.

[5] In beginsel, want de AVG noemt uiteraard wel enige uitzonderingen daarop.

# 11. Rechten van betrokkenen

Betrokkenen hebben diverse rechten. Vanuit de Wbp en de AVG hebben de betrokkenen het recht op informatie en het recht om hun gegevens in te zien, te corrigeren en te verwijderen. De AVG voegt hier het recht op data-export en beperking aan toe. Organisaties moeten ervoor zorgen dat ze aan deze rechten kunnen voldoen, als betrokkenen dat aan hen vragen.

**11.1 Inzagerecht**

Het inzagerecht houdt in dat betrokkenen een aanvraag kunnen indienen om inzicht te krijgen in welke gegevens over hem of haar door de verwerkingsverantwoordelijke verwerkt worden. Indien een dergelijke vraag binnenkomt, dient de verwerkingsverantwoordelijke de volgende informatie te verschaffen aan de betrokkene:

- de doeleinden van de gegevensverwerking (waarvoor worden de persoonsgegevens van de betrokkenen ingezet door de verwerkingsverantwoordelijke?);
- de aard en de herkomst van de persoonsgegevens die verwerkt worden. Dit kunnen bijvoorbeeld de persoonsgegevens zijn die betrokkenen actief hebben verstrekt bij het sluiten van een overeenkomst met de verwerkingsverantwoordelijke;
- De ontvangers van de gegevens. Dit zijn de derde partijen aan wie de verwerkingsverantwoordelijke gegevens verschaft en die deze gegevens voor eigen doeleinden kunnen verwerken.

Het is voor de persoon die een inzageverzoek indient niet toegestaan om inzage in de persoonsgegevens van een ander te verlangen. Of zijn gegevens verwerkt worden, dient binnen vier weken medegedeeld te worden aan de betrokkene. Zodra de gegevens zijn overgebracht naar een archiefbewaarplaats, zijn bovengenoemde informatie verplichtingen niet meer van toepassing en heeft de betrokkene enkel nog het recht om op grond van een gericht verzoek inzage in de archiefbescheiden te verkrijgen.

**11.2 Correctie- en verwijderingsrecht**

Daarnaast hebben betrokkenen het recht om gegevens te laten corrigeren en/of te verwijderen. Dit zal in de meeste gevallen volgen na een inzageverzoek. Correctie of verwijdering mag de betrokkene vragen indien de gegevens feitelijk onjuist zijn, niet nodig zijn om het door de verwerkingsverantwoordelijke vastgestelde doel te behalen, of als de gegevens in strijd met een wettelijk voorschrift worden verwerkt.

Om te voldoen aan een dergelijk verzoek, hoeft er niet per se sprake te zijn van een fout door de verwerkingsverantwoordelijke. Gegevens kunnen ook per ongeluk foutief zijn opgegeven of ingevoerd.

Een verzoek tot correctie of verwijdering van gegevens moet binnen vier weken worden beantwoord. Dit kan een bevestiging zijn dat het verzoek wordt nageleefd, of een weigering, die met redenen omkleed dient te zijn.
Zodra de betreffende persoonsgegevens zijn overgebracht naar een archiefbewaarplaats is het recht tot correctie niet langer inroepbaar. Wel mag de

betrokkene in dat geval zijn eigen lezing aan de desbetreffende archiefbescheiden toevoegen.[6]

Ook het recht van verwijdering is niet onbeperkt. Het is namelijk mogelijk dat de verwerkingsverantwoordelijke een wettelijke bewaartermijn moet naleven. In dat geval is het voor de verwerkingsverantwoordelijke wettelijk gezien niet toegestaan bepaalde gegevens te verwijderen, ook al verzoekt de betrokkene hierom. In dat geval kan de verwerkingsverantwoordelijke aangeven dat zij enkel de gegevens kan verwijderen waar geen wettelijke bewaartermijn voor geldt, en dat de overige gegevens verwijderd zullen worden op het moment dat de wettelijke bewaartermijn is verstreken.
Ook is er in de AVG (art 17 lid 3 sub d) een uitzondering opgenomen voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hierbij gaat het om een afweging waarbij het recht van verwijdering afgewogen moet worden tegen de mogelijke gevolgen voor het archief of het onderzoek van die door de betrokkene gewenste verwijdering. Deze afweging moet overigens ook worden gemaakt nadat archiefbescheiden zijn overgebracht naar een archiefbewaarplaats, hoewel het uiteraard aannemelijk is dat verwijdering in de meeste gevallen de doeleinden van archivering ernstig in het gedrang zal brengen.

De verwerkingsverantwoordelijke zal in alle andere gevallen de gegevens daadwerkelijk moeten verwijderen of, indien verwijderen echt niet mogelijk is, anonimiseren. Dit houdt in dat tevens gegevens die op een digitale back-up staan verwijderd moeten worden.

**11.3 Recht op overdraagbaarheid gegevens**
Een nieuw recht uit de AVG is het recht op dataportabiliteit. Hiermee kan de betrokkene een kopie van zijn persoonsgegevens eisen die bruikbaar is bij een andere, vergelijkbare, dienstverlener. Dit recht is enkel van toepassing wanneer de verwerking is gebaseerd op de grondslag uitvoering van de overeenkomst, of toestemming. Zodra de betreffende persoonsgegevens zijn overgebracht naar een archiefbewaarplaats is dit recht bovendien niet langer inroepbaar.

**11.4 Recht op beperking**
Indien een betrokkene gegronde redenen heeft om te twijfelen aan de legitimiteit van de gegevensverwerking door de verwerkingsverantwoordelijke, heeft de betrokkene het recht om beperking van zijn gegevensverwerking te eisen. Dit houdt in praktische zin in dat de betreffende persoonsgegevens in quarantaine gezet dienen te worden, totdat er opheldering is over de legitimiteit van de gegevensverwerking (bijvoorbeeld of de beveiliging wel passend is en of de bewaartermijnen gehandhaafd worden). Zodra de betreffende persoonsgegevens zijn overgebracht naar een archiefbewaarplaats is dit recht echter niet langer inroepbaar.

**11.5 Recht van bezwaar**
Wanneer een verwerkingsverantwoordelijke zich beroept op de grondslag “taak van algemeen belang” of “gerechtvaardigd eigen belang”, dan kan een

[6] Art 45 lid 3 UAVG

betrokkene tegen die verwerking bezwaar indienen.[7] Bij een bezwaar dient de verwerking in beginsel gestaakt te worden, tenzij de verwerkingsverantwoordelijke aan kan tonen dat zijn dwingende gerechtvaardigde belangen zwaarder wegen dan de grondrechten van de betrokkene. Dit recht om bezwaar te maken is ook inroepbaar nadat de desbetreffende archiefbescheiden zijn overgebracht naar een archiefbewaarplaats.

**11.6 Identificatie**

Wat bij het behandelen van een van de bovenstaande verzoeken te allen tijde noodzakelijk is, is dat vóórdat er gegevens aan de betrokkene worden verschaft, de identiteit van de betrokkene wordt vastgesteld. Er moet voorkomen worden dat er persoonsgegevens worden verstrekt aan iemand die zich voordoet als een ander. Zo kan er bijvoorbeeld besloten worden dat er telefonisch geen persoonsgegevens verstrekt worden en dat de betrokkene eerst een kopie van zijn identiteitsbewijs dient aan te leveren (waar foto en BSN zijn afgeschermd).

**11.7 Waarborgen bij overbrenging**

Zoals is aangegeven zijn een aantal rechten van betrokkenen ook na overbrenging naar een archiefbewaarplaats nog steeds van toepassing. Bovendien gelden waar het bijzondere persoonsgegevens betreft de verbodsregels vanuit de AVG. De archiverende organisatie doet er daarom verstandig aan om bij overbrenging te controleren danwel bevestigd te krijgen dat de over te brengen archiefbescheiden (bevattende persoonsgegevens) voorkomen in het register met verwerkingsactiviteiten van de zorgdrager. En ook in het geval van schenking of bruikleen van particuliere collecties is een controle op de inhoud en herkomst van de persoonsgegevens aan te bevelen.

Aanbevelingen

- Leg de omgang met de rechten van betrokkenen –zowel voor als na overbrenging- vast in het interne privacy beleid;
- Zorg dat de identiteit van de aanvrager gecontroleerd wordt voordat gegevens worden verstrekt.
- Denk na over de wijze waarop betrokkenen hun rechten kunnen inroepen voor zowel nieuw over te brengen alsook reeds overgebrachte archiefbescheiden.

[7] Het gerechtvaardigd eigen belang (art 6 lid 1 sub f AVG) mag vanaf 25 mei 2018 niet langer door overheidsorganisaties ingeroepen worden als grondslag.

# 12 Gebrek aan data-minimalisatie

Persoonsgegevens moeten worden beperkt tot wat noodzakelijk is voor het doel van de verwerking. Dit beginsel van data-minimalisatie is vastgelegd in de AVG en het richt zich tot de verwerkingsverantwoordelijke, zoals de zorgdragers.[8] Minimalisatie betekent overigens ook geen tekort aan data, want de verwerking moet volgens de AVG ook toereikend en 'ter zake dienend' zijn. Hieruit volgt onder meer dat de noodzaak van de verwerking degelijk onderbouwd moet zijn. [9]

Uit de aangeleverde documenten en de interviews is niet gebleken dat het uitgangspunt van data-minimalisatie strikt wordt nageleefd door zorgdragers, archiverende organisaties en/of derde partijen die persoonsgegevens verwerken in opdracht van de archiverende organisatie. Daarbij gaat het bijvoorbeeld om zaken als bezoekersregistraties. Waar bij de ene archiverende organisatie vrijwel niets geregistreerd wordt van bezoekers van de studiezaal, slaat een andere archiverende organisatie van de bezoekers zelfs het nummer en de geldigheidsduur van een identiteitsbewijs op.
Het verwerken van gegevens omdat ze alleen maar 'nuttig' zijn, voldoet niet aan het vereiste van data-minimalisatie. Voor het verwerken (en uitwisselen) van persoonsgegevens is het vereist dat de noodzaak ervan is onderbouwd op basis van (1) een persoonsgegeven, (2) legitiem doel en (3) rechtmatige grondslag.

Aanbevelingen

- Stel, op basis van het verwerkingsregister, vast welke verwerkingen van persoonsgegevens niet noodzakelijk zijn voor het doel waarvoor ze zijn verkregen, beperk deze verwerkingen en staak de verwerking als er geen rechtmatige grondslag voor is;
- Probeer als sector op een uniforme wijze om te gaan met de bezoekersregistratie: vraag zo weinig mogelijk, en bewaar zo kort mogelijk.
- Voor het bepalen van de noodzakelijkheid voor het opvragen van persoonsgegevens kan navraag worden gedaan bij de diverse afdelingen die doeleinden van de verwerking vaststellen, zodat kan worden nagegaan of het opvragen van persoonsgegevens hiervoor noodzakelijk is;
- Hanteer de Archiefwet als het kader om voor over te brengen archiefbescheiden af te wegen of verdere dataminimalisatie noodzakelijk is.

[8] Art. 5 lid 1 sub c AVG.
[9] Art. 5 en 6 AVG.

# 13. Functionaris voor Gegevensbescherming

De FG is een 'interne toezichthouder'. Hij ziet binnen de organisatie toe op de omgang met persoonsgegevens en controleert of de organisatie voldoet aan de AVG en eventuele andere toepasselijke privacyregelgeving. Onder de Wbp was het nog een vrijwillige keuze om een aanspreekpunt voor privacy te benoemen. Op grond van de AVG is het in de volgende gevallen verplicht om een FG aan te wijzen:[10]

- de verwerking vindt plaats door een overheidsinstantie- of orgaan;
- de verwerkingsverantwoordelijke is hoofdzakelijk belast met verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisten; of
- de verwerkingsverantwoordelijke is hoofdzakelijk belast met grootschalige verwerking van bijzondere categorieën van gegevens.

Voor archiverende organisaties is het vrijwel altijd verplicht om een FG aan te wijzen. Maakt de archiverende organisatie onderdeel uit van een zorgdrager, dan zal de zorgdrager een FG moeten aanwijzen. Deze FG zal dus ook toezicht moeten houden op de wijze waarop de archiverende organisatie voldoet aan de AVG. Maakt de archiverende organisatie deel uit van een Gemeenschappelijke Regeling, dan dient de GR zelf een eigen FG aan te wijzen. Het al dan niet overgebracht zijn van archiefbescheiden speelt hierbij geen enkele rol. De FG houdt dus ook toezicht op de omgang met persoonsgegevens die voor kunnen komen in beperkt openbare archiefbescheiden.
Een FG moet onafhankelijk kunnen functioneren als privacyvraagbaak in een organisatie. Zijn contactgegevens moeten worden medegedeeld aan de Autoriteit Persoonsgegevens. Onafhankelijk houdt in dat de FG geen instructies van bovenaf mag ontvangen voor de uitvoering van zijn taken. Om die reden heeft de FG een vergelijkbare ontslagbescherming als leden van een ondernemingsraad. De FG rapporteert rechtstreeks aan het hoogste management van de organisatie, maar kan van dat management geen onderdeel zijn. In een dergelijk geval is er sprake van belangenverstrengeling, want de FG controleert dan mogelijk zijn eigen beleid. Daarbij dient het privacybelang bij een FG als hoogste in het vaandel te staan, en mag dit dus geen persoon zijn die vanuit zijn/haar functie bijvoorbeeld organisatorische of financiële belangen belangrijker vindt. Een FG kan intern of extern aangewezen worden.

Aanbevelingen

- Beslis of de functie van FG intern of extern wordt belegd en wijs vervolgens een FG aan;
- Voorkom belangenverstrengeling als de functie intern wordt belegd;
- Maak intern bekend dat er een FG is, en dat dit dus ook de persoon is bij wie alle medewerkers voor privacyvragen terecht kunnen;
- Meld de FG vanaf 25 mei 2018 aan bij de Autoriteit Persoonsgegevens.

[10] Zie ook art. 37 AVG.