WETEN OF VERGETEN?

Handreiking voor het toepassen van de Algemene verordening gegevensbescherming in samenhang met de Archiefwet in de dagelijkse praktijk van het informatiebeheer bij de overheid

Werkgroep AVG

April 2020

Kennisnetwerk
Informatie en Archief

Dit werk is gelicenseerd onder een Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 4.0 Internationaal licentie. Bezoek http://creativecommons.org/licenses/by-nc-sa/4.0/ om een kopie te zien van de licentie of stuur een brief naar Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

INHOUDSOPGAVE

Inleiding

In mei 2018 is de Europese Algemene verordening gegevensbescherming (AVG) in werking getreden in de hele Europese Unie. Deze verordening bepaalt wat je wel en niet mag doen met persoonsgegevens en hoe je deze moet beschermen. De Nederlandse overheid heeft daarnaast te maken met de Archiefwet, die vanuit een ander perspectief richting geeft aan hoe je met informatie, waaronder persoonsgegevens, moet omgaan.

In de praktijk bestaat er nog weleens onduidelijkheid over hoe de AVG en de Archiefwet zich tot elkaar verhouden. Deze handreiking is bedoeld om die onduidelijkheid weg te nemen. Overheden kunnen de verschillende wetten in onderlinge samenhang uitvoeren. De handreiking richt zich in de eerste plaats op medewerkers van overheden die werkzaam zijn binnen het domein van informatiebeheer, ook wel aangeduid als DIV, recordmanagement of informatie- en documentbeheer. Met behulp van deze handreiking kunnen zij hun positie ten opzichte van specialisten binnen het domein van privacy kennen en begrijpen.
De handreiking beperkt zich tot informatie die op grond van de Archiefwet vernietigbaar is en blijvend te bewaren informatie die nog niet is overgebracht naar een archiefbewaarplaats.[1]

Weten of vergeten gaat uit van de nu bestaande inzichten en de huidige wetgeving. Er zullen de komende jaren waarschijnlijk nieuwe richtlijnen en aanpassingen van de Uitvoeringswet AVG volgen, de Archiefwet wordt vernieuwd en ook ontwikkelingen in technologie en samenleving zullen invloed hebben op hoe we naar dit onderwerp kijken. Daarom zal deze handreiking regelmatig worden aangepast.

Om bruikbaar te zijn op de werkvloer van het informatiebeheer, maar ook te kunnen dienen als naslagwerk, is gekozen voor een handreiking in twee delen. Het eerste deel is bedoeld voor toepassing in de praktijk. In dit deel is 'in control komen' het uitgangspunt: sturing geven aan het gedrag van medewerkers en de gewenste cultuur van samenwerking rond informatiebeheer. Hiervoor is allereerst een besef van urgentie nodig op strategisch en tactisch niveau. Vanuit het 'in control komen' is het eenvoudiger om 'compliant' te zijn, dat is het volledig voldoen aan de AVG en de Archiefwet.
Het eerste hoofdstuk biedt een algemene beschrijving en een overzicht van de belangrijkste definities zoals ze in dit document gehanteerd worden. Het tweede hoofdstuk beschrijft de maatregelen die op strategisch niveau vereist zijn: wat is er nodig aan beleid en instrumenten? Het derde hoofdstuk gaat in op tactische aspecten: op welke wijze komen we tot de juiste ontwerpbeslissingen en inrichtingskeuzes? Tot slot gaan we in op operationele aspecten: hoe regelen we het feitelijke beheer, zoals het uitvoeren van daadwerkelijke vernietiging of het behandelen van verzoeken in het kader van het 'recht op vergetelheid' en andere rechten van burgers?
Het tweede deel gaat dieper in op onderwerpen die van belang zijn voor de doelgroep. Dat

[1] Voor informatie die is overgebracht naar een archiefbewaarplaats gelden andere eisen en die brengen andere vraagstukken met zich mee. Informatie daarover is onder meer te vinden op https://kia.pleio.nl/groups/view/48594512/kennisplatform-informatierecht en in de risicoanalyse op de gezinskaarten van het bevolkingsregister, zie: https://vng.nl/sites/default/files/model_risicoanalyse_gezinskaarten_definitief.pdf

gebeurt aan de hand van een juridisch en theoretisch kader en voorbeelden. Dit deel kan als naslagwerk worden gebruikt. Het is mogelijk dat passages in beide delen dubbel zijn. Dit is te verklaren door de verschillende functies van de delen, en is daarom zo gelaten.

De Subwerkgroep Informatiemanagement van de AVG-werkgroep van het Kennisplatform Informatie en Archief (KIA) is in het leven geroepen naar aanleiding van vele vragen uit de praktijk. Ze heeft *Weten of vergeten* opgesteld in opdracht van de beroeps- en brancheverenigingen KVAN/BRAIN.[2] Het concept is voorgelegd aan de Autoriteit Persoonsgegevens en aan het Nationaal Archief. Wij danken beide organisaties voor hun vaak uitgebreide commentaar.

KIA Werkgroep AVG – Subwerkgroep Informatiemanagement
April 2020

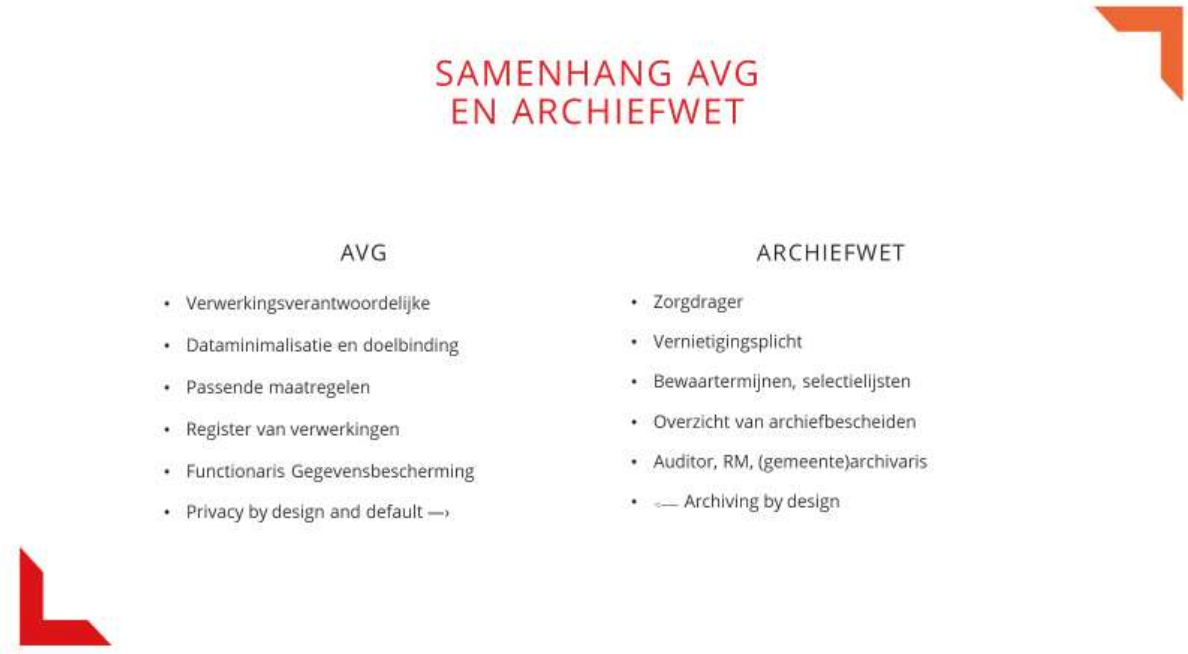
[2] Zie: https://www.kvanbrain.nl/

DEEL 1: PRAKTIJK

1 Introductie en afbakening

1.1 Inleiding

Op het beheer van informatie is verschillende wetgeving van toepassing. De Archiefwet en de AVG hanteren elk een eigen perspectief en soms ook verschillende termen en definities (zie afbeelding). In dit hoofdstuk worden bondig de gehanteerde perspectieven beschreven en de belangrijkste termen en definities toegelicht. Tot slot volgt een opsomming van de thema's die in dit eerste deel worden behandeld.



1.2 Perspectieven

Om de verschillende wetten in samenhang te kunnen toepassen, is het nodig om te begrijpen welke doelen zij dienen. In hoofdlijnen is dit als volgt:

- Archiefwet
    - efficiënte bedrijfsvoering en geheugen
    - authenticiteit en integriteit van (overheids)informatie
    - transparantie van de overheid, afleggen van verantwoording
    - reconstructie van verleden en veiligstellen cultureel erfgoed
- AVG
    - bescherming van persoonsgegevens

Het is belangrijk om te onderkennen dat deze wetten complementair zijn aan elkaar en niet met elkaar concurreren noch elkaar uitsluiten. De AVG gaat als Europese verordening boven de Nederlandse Archiefwet. De AVG laat echter wel ruimte om in nationale wetgeving nadere regels te stellen. Dit is in Nederland onder andere in de Archiefwet gebeurd. Naleving van de Archiefwet betekent dus tevens naleving van bepaalde verplichtingen uit de AVG.

In de Archiefwet wordt de bestuurlijk verantwoordelijke de 'zorgdrager' genoemd; de AVG gebruikt de term 'verwerkingsverantwoordelijke'. Meestal gaat het om hetzelfde bestuur. Des te meer ligt het voor de hand dat beide wetten in samenhang worden uitgevoerd. In de volgende hoofdstukken zal duidelijk worden welke raakvlakken er nog meer zijn en hoe er omgegaan moet worden met schijnbare tegenstellingen.

1.3 Strategisch, tactisch en operationeel niveau

In deze handreiking wordt onderscheid gemaakt tussen strategisch, tactisch en operationeel niveau. Dit onderscheid is gebaseerd op een rolverdeling die bij veel overheidsorganisaties gebruikelijk is, al is dit niet overal als zodanig herkenbaar. In de praktijk zijn er ook organisaties die verschillende niveaus integraal georganiseerd hebben. Voor het goede begrip leggen we daarom eerst uit welke afbakening wij bij het opstellen van dit document hebben gehanteerd:

- **strategisch niveau (richten)**: onder meer het opstellen van organisatiebreed beleid, visievorming, governance en vormgeven van de organisatiestructuur en de sturende processen
- **tactisch niveau (inrichten)**: onder meer het ontwerpen en inrichten van processen en informatiesystemen (privacy by design en archiving by design)
- **operationeel niveau (verrichten)**: het feitelijk beheer van informatie (zoals vernietiging, conversie, overbrenging)

1.4 Belangrijkste termen en definities

In dit document worden de termen 'persoonsgegevens', 'archiefbescheiden', 'documenten' en 'informatie' veel gebruikt. Daarom geven we eerst de definities zoals ze in dit document worden gehanteerd. Er is samenhang tussen de verschillende begrippen. Persoonsgegevens staan niet op zichzelf, maar maken deel uit van archiefbescheiden, documenten of informatie. Handelingen die uit de Archiefwet voortvloeien, zoals het verzamelen, opslaan, beheren en vernietigen van informatie met persoonsgegevens, zijn daarom tevens verwerkingen in de betekenis van de AVG.

Persoonsgegevens

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'). Als zodanig wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een nummer, locatiegegevens, een online identificator, of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.[3]

[3] AVG, artikel 4: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

Verwerking
Alle handelingen met betrekking tot persoonsgegevens, zoals verzamelen, opslaan, ter beschikking stellen, wijzigen, wissen of vernietigen, al dan niet geautomatiseerd.[4] Let op: archivering is ook een verwerking!

Archiefbescheiden
Bescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten.[5]

Document
Een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat.[6] Of: het geheel van samenhangende gegevens, vastgelegd op een of meer gegevensdragers.[7]

De termen 'archiefbescheiden' en 'document(en)' betekenen min of meer hetzelfde. De huidige Archiefwet spreekt van 'archiefbescheiden', het begrip 'document' is in het concept van de nieuwe wet opgenomen. In deze handreiking gebruiken we bij voorkeur de term 'informatie'.

Informatie
In de definitie van NORA is informatie: betekenisvolle gegevens.[8] In deze handreiking gebruiken we 'informatie' als een containerbegrip dat alle typen betekenisvolle informatie op alle mogelijke dragers kan betekenen, bijvoorbeeld: geluidsfragmenten, foto/film, tekstdocumenten, waarden in databases, algoritmen of log-gegevens.

Zie voor overige definities van begrippen het overzicht achterin deze uitgave.

1.5 Eisen

Een aantal thema's op het gebied van informatiebeheer komt terug in zowel de Archiefwet als de AVG:

- bewaren en vernietigen
- overzichten en registers
- openbaarmaking
- toezicht

Bij invulling van deze thema's is het dus noodzakelijk AVG en Archiefwet in samenhang te bekijken. De thema's komen terug in de volgende hoofdstukken.

[4] AVG, artikel 4 onder 2.
[5] Archiefwet art. 1c.
[6] Wob, art. 1: https://wetten.overheid.nl/BWBR0005252/2018-07-28.
[7] Archiefterminologie voor Nederland en Vlaanderen.
[8] NORA: https://www.noraonline.nl/wiki/Informatie.

2 Maatregelen op strategisch niveau

2.1 Inleiding

In dit hoofdstuk volgen enkele suggesties voor maatregelen op strategisch niveau, die bijdragen aan het in samenhang uitvoeren van AVG en Archiefwet. Deze maatregelen zijn nadrukkelijk bedoeld als voorbeelden: er zijn immers meerdere wegen die naar Rome leiden. Voorwaarden voor het realiseren ervan zijn een urgentiebesef op het strategisch niveau van de organisatie en een bereidheid om hierop besluiten te nemen.

2.2 Organisatie van kennis

In veel organisaties is kennis op deelgebieden als informatiebeheer, privacybescherming, informatiebeveiliging en openbaarheid (Wob) bij verschillende functionarissen belegd. Soms werken dezen in verschillende teams of op verschillende afdelingen. Dit brengt het risico met zich mee dat verschillende perspectieven op het informatiebeheer onvoldoende bij elkaar komen. Vanuit strategie kan dit risico worden beperkt. Voorbeelden van dergelijke maatregelen zijn:

- Verschillende rollen die met informatie te maken hebben, worden in de organisatiestructuur dicht bij elkaar gepositioneerd. Bijvoorbeeld door ze in één afdeling onder te brengen. Hierdoor wordt samenwerking vanuit de organisatiestructuur bevorderd.
  De organisatie stelt als beleid vast dat processen op het gebied van informatiebeheer en -toegang zodanig worden ingericht dat de verschillende rollen erbij betrokken worden.

2.3 Beleid en toezicht

Wat betreft het beleid van een organisatie op het gebied van het informatiebeheer, ligt het voor de hand daarbij de uitvoering van AVG en Archiefwet te integreren. Twee voorbeelden daarvan zijn:

- als uitgangspunt vaststellen dat de selectielijst wordt gehanteerd voor het bepalen van bewaartermijnen van informatie met persoonsgegevens
- besluiten dat de bewaartermijnen in verwerkingsregisters (AVG) en overzichten van informatie (Archiefwet) en in documenten zoals het informatiebeleidsplan op elkaar worden afgestemd

In zowel Archiefwet als AVG zijn toezichthoudende functies voorgeschreven. Op grond van de Archiefwet is binnen de verschillende overheidsniveaus toezicht ingericht. Bij de centrale overheid is dat de Inspectie Overheidsinformatie en Erfgoed; bij de decentrale overheid is het de provincie-, gemeente- of waterschapsarchivaris.[9] Binnen organisaties fungeren vaak

[9] In de huidige Archiefwet is de benoeming van een archivaris niet verplicht, hoewel de meeste decentrale overheden een archivaris hebben aangesteld.

ook auditors of recordmanagers op dit gebied.
Op grond van de AVG is het voor de overheid verplicht een functionaris gegevensbescherming (FG) te benoemen, die toezicht houdt op het domein privacy. Daarnaast kunnen er ook privacyfunctionarissen aangesteld zijn. Vaak zijn er nog andere rollen die binnen de organisatie toezicht uitoefenen, zoals op het terrein van informatiebeveiliging een Chief Information Security Officer (CISO), de Chief Information Officer (CIO) de hoogst verantwoordelijke op het gebied van ICT. Soms is een informatiecommissaris benoemd, vaker is een WOB-functionaris aanwezig. Een regulier overleg tussen deze functionarissen, die alle te maken hebben met informatiebeheer en -management, is zeker aan te bevelen en vaak al praktijk.

Een meer integrale aanpak kan een stimulans krijgen wanneer toezichthoudende functionarissen samen optrekken en integraal rapporteren aan bestuur en/of management. Minimaal zouden zij elkaars rapportages moeten kennen en er onderling naar verwijzen. Eenzelfde stimulans kan uitgaan van integraal beleid waarin de verschillende perspectieven worden omgezet naar samenhangende implementatierichtlijnen voor de organisatie.

2.4 Inrichten van sturende processen

Vanuit de governance is het mogelijk om aan te sturen op een integrale aanpak door werkwijzen vast te stellen waarin zowel de expert(s) op het gebied van privacy als op het gebied van informatiebeheer (plus andere informatiegerelateerde deskundigen) een vaste rol hebben. Voorbeelden van dergelijke maatregelen zijn:

- inrichten van het project- of inkoopproces van software, waarin is vastgelegd wanneer welke rollen aan tafel komen te zitten, bijvoorbeeld voor het opstellen van het programma van eisen ten behoeve van een aanbesteding
- inrichten van het proces voor het controleren van een lijst met te vernietigen informatie (vernietigingslijst), waarin zowel de deskundige of toezichthouder op het gebied van de Archiefwet (bij de decentrale overheden de archivaris) als de toezichthouder op het gebied van privacy (FG) een rol kan krijgen. De toezichthoudende rollen kunnen hierover met elkaar afspraken maken. Dit is vooral aan te bevelen bij afwijkingen van de selectielijst, zoals bij ‘hotspots’. Zie deel 2 hoofdstuk 3.
- afspraken over het proces van behandeling van verzoeken van burgers op grond van hun rechten uit de AVG. Als uitgangspunt kan worden afgesproken dat bij het toetsen van deze aanvraag zowel deskundigheid op het gebied van privacy als op het gebied van archivering, selectie en vernietiging wordt betrokken. Zie deel 2 hoofdstuk 5.

2.5 Bewaren en vernietigen

De AVG stelt dat er niet langer moet worden bewaard dan nodig voor het doel, maar geeft niet aan op welke wijze dat moet gebeuren. Op dit punt is de Archiefwet aanvullend, want daarin is het instrument van de selectielijst verplicht gesteld. In een selectielijst geeft een

overheidsorganisatie aan welke categorieën informatie deze onderkent en welke bewaartermijnen daarbij worden gehanteerd. Daarmee kan de selectielijst tevens worden gezien als het wettelijke instrument voor de overheid om bewaartermijnen in de zin van de AVG vast te stellen.[10] Een voorwaarde daarvoor is dat de uitgangspunten van de AVG zijn meegenomen bij de totstandkoming van die selectielijst. Zo niet, dan zal de lijst aangepast moeten worden.

Soms merken overheidsorganisaties dat de selectielijst zoals die in het verleden is vastgesteld, nog onvoldoende rekening houdt met de AVG. De praktische maatregel die hierbij hoort is het herzien van de selectielijst. Er kan worden nagegaan of de bewaartermijnen niet te lang zijn en er kunnen zo nodig nieuwe, specifieke categorieën informatie worden toegevoegd. Een voorbeeld van een dergelijke nieuwe categorie zou kunnen zijn: 'onrechtmatig verzamelde persoonsgegevens', dus gegevens die (per abuis) verzameld zijn zonder dat hiermee een doelbinding was. In dit geval kan de bewaartermijn bepaald worden als: 'direct vernietigen na ontdekken'.[11]

Persoonsgegevens die uitsluitend op basis van de grondslag 'toestemming' worden verzameld en niet op basis van 'uitvoering van een wettelijke taak' of 'overheidsgezag' zijn ook zo'n geval. Neem de opgave van dieetwensen voor een door de overheid georganiseerde kennisbijeenkomst. Na afloop van de bijeenkomst en ook na intrekking van die toestemming is er geen grond meer om deze gegevens nog te bewaren. De selectielijst kan voor deze variant een generieke categorie bevatten op grond waarvan de persoonsgegevens na afloop van de bijeenkomst of intrekking van de toestemming ook daadwerkelijk snel vernietigd kunnen worden. De meeste persoonsgegevens verwerkt de overheid echter in het kader van een wettelijke taak of openbaar gezag en dan is dit mechanisme niet van toepassing.

Op strategisch niveau is het nodig dat binnen organisaties zowel de FG als de deskundige en/of toezichthouder op het terrein van de Archiefwet zich aan het instrument van de selectielijst committeert. Voor iedereen wordt dan duidelijk dat voldoen aan de Archiefwet op dit punt tevens bijdraagt aan uitvoering van de AVG en het 'in control' komen op de onderdelen informatiehuishouding en privacy.

2.6 Overzichten en registers

Om inzicht te krijgen in te nemen maatregelen, is een nulmeting van de situatie in alle gevallen nodig. De AVG schrijft voor dat er een 'register van verwerkingen' wordt opgesteld

[10] In zijn Kamerbrief van 31 oktober 2019 heeft de minister van Justitie en Veiligheid er expliciet op gewezen dat voor het bepalen van bewaartermijnen van informatie met persoonsgegevens de selectielijsten het geëigende instrument zijn, zie: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/31/tk-voornemens-met-betrekking-tot-de-uavg-en-avg

[11] Voor meer informatie over ontwerpen, vaststellen en actualiseren van selectielijsten, zie: https://www.nationaalarchief.nl/archiveren/waardering-en-selectie

en bijgehouden. De Archiefregeling schrijft voor dat er een 'actueel en compleet overzicht van archiefbescheiden' is. Inhoudelijk zit er overlap tussen beide, omdat persoonsgegevens nu eenmaal deel uitmaken van 'archiefbescheiden' of informatie. Dit stelt overheden voor de strategische keuze of zij twee aparte registers willen bijhouden of juist één integraal overzicht willen realiseren. Overheden zijn vrij om daar zelf de meest geschikte keuze in te maken. Wanneer de keuze uitvalt voor twee aparte registers, is het uiteraard sterk aan te bevelen om te bepalen dat de bewaartermijn die in beide registers staat, gelijkluidend ingevuld wordt. Daarnaast is het aanbevelenswaardig om in beide gevallen te werken vanuit een gemeenschappelijk vastgesteld begrippenkader, dat bij voorkeur aansluit op de referentiearchitectuur. Voorbeelden daarvan zijn EAR[12] voor de centrale overheid en GEMMA[13] voor gemeenten. Werken vanuit eenzelfde begrippenkader en architectuur bevordert een integrale aanpak, vergemakkelijkt onderlinge vergelijking tussen register en overzicht en maakt ook automatisering eenvoudiger.
De overzichten, die het register of de registers bieden, vormen een basis voor risico-analyse en verdere maatregelen.

[12] Zie: https://www.earonline.nl
[13] Zie: https://www.gemmaonline.nl

3 Maatregelen op tactisch niveau

3.1 Inleiding

Ook op tactisch niveau zijn een aantal maatregelen mogelijk die bijdragen aan het in samenhang uitvoeren van de AVG en de Archiefwet. Voor de uitvoering van de maatregelen is naast een nulmeting of overzicht van wat er in huis is, een besef van urgentie en een beslissingsbereidheid en -bevoegdheid bij de verantwoordelijken op dit niveau in de organisatie nodig. In dit hoofdstuk worden enkele suggesties gedaan voor maatregelen.

3.2 Inrichtingsprincipes: 'by design'

Op tactisch niveau is het aan te bevelen de principes van 'privacy by design and default' en 'archiving by design' toe te passen. Dit wil in deze context zeggen dat bij het ontwerp van een proces en/of het daarbij gebruikte informatiesysteem ook meteen de eisen ten aanzien van respectievelijk privacy en archivering worden geformuleerd en geïmplementeerd als standaardinstellingen. In de volgende subparagrafen worden voorbeelden gegeven van inrichtingsprincipes die een overheidsorganisatie daarbij kan hanteren. Sommige daarvan zijn verplicht.

3.2.1 Dataminimalisatie en principes van de Archiefwet

Een belangrijk inrichtingsprincipe is dat van dataminimalisatie of minimale gegevensverwerking: niet meer persoonsgegevens verwerken dan noodzakelijk voor een bepaald doel. De toepassing van dit principe is op grond van de AVG een verplichting. Een voorbeeld van een praktische maatregel die hieruit volgt, is dat in het ontwerp van het datamodel geen ruimte komt voor vastlegging van persoonsgegevens die niet strikt noodzakelijk zijn voor het doel. Dit voorkomt dat in een latere fase vragen ontstaan over archiveren en bewaren van deze persoonsgegevens in verband met de privacy. Speciale aandacht is hierbij nodig voor bijzondere en gevoelige persoonsgegevens, waarvan de verwerking in principe verboden is (met uitzonderingen, zie deel 2 paragraaf 2.1).
Aan de andere kant moeten natuurlijk wel voldoende gegevens worden verwerkt om aan de doelstellingen van de Archiefwet te beantwoorden, zoals bewijsfunctie, reconstrueerbaarheid van een zaak en geschiedschrijving (zie hiervóór 1.2). Toepassing van deze principes van de Archiefwet sluit de toepassing van het beginsel van dataminimalisatie beslist niet uit.

Praktijkvoorbeeld: een organisatie heeft een online-formulier voor het maken van afspraken bij een loket. Op dit formulier staan niet-verplichte velden waarop de burger desgewenst bepaalde persoonlijke informatie kan invullen, zoals BSN en leeftijd. Een burger besluit deze velden leeg te laten, waarna het toch lukt om een afspraak te maken. Deze afspraak verloopt vervolgens zonder problemen. In dit geval hadden de velden 'BSN' en 'leeftijd' dus net zo goed niet in het online-formulier opgenomen kunnen worden, want deze gegevens waren kennelijk niet nodig voor het doel: het maken van een afspraak. Bovendien is het opnemen van een BSN niet toegestaan als dat niet in een wettelijke bepaling is voorgeschreven. Kortom: hier was dataminimalisatie als onderdeel van het principe 'privacy by design' niet toegepast, en waren de gegevens ook niet nodig voor reconstructie van de zaak, zoals de Archiefwet wil.

3.2.2. Bewaartermijn

Een tweede inrichtingsprincipe is dat de bewaartermijnen uit de selectielijst vanaf de start worden toegepast op alle informatie die wordt opgeslagen. Soms zijn er binnen één proces meerdere bewaartermijnen mogelijk, bijvoorbeeld als de termijn afhankelijk is van het resultaat van een zaak (zoals verlenen dan wel afwijzen van een vergunningsaanvraag). Sommige procesgerichte selectielijsten bieden ruimte om deelzaken te benoemen die een kortere bewaartermijn kunnen hebben dan de hoofdzaak. Dit kan een oplossing zijn om persoonsgegevens die alleen tijdens de behandeling relevant zijn, korter te bewaren.

Een voorbeeld hiervan is het noteren van een bankrekeningnummer voor het innen van leges binnen een vergunningsproces. Op het moment dat een betaling heeft plaatsgevonden en dat goed is vastgelegd in de boekhouding, is het in principe niet meer nodig om het bankrekeningnummer ook nog in het vergunningsdossier te bewaren. Een notitie dat de leges zijn betaald met eventueel verwijzing naar de boekhouding is dan voldoende.

3.2.3 Toegangsniveau

Een derde inrichtingsprincipe betreft het toegangsniveau. Overheden kunnen hierin eigen beleid voeren, bijvoorbeeld: 'openbaar, tenzij…' of juist 'need to know'. Welk beleid ook van toepassing is, er wordt bij 'by design' of 'by default' altijd gekeken of in de specifieke situatie de algemene beleidsregel toegepast kan worden of dat hiervan afgeweken moet worden.

Hierbij kunnen verschillende stadia worden onderscheiden: na afronding van een zaak is het vaak niet noodzakelijk dat dezelfde rollen toegang tot hebben de informatie als tijdens behandeling van de zaak. In de ontwerpfase wordt het autorisatiemodel voor de verschillende stadia in de levenscyclus van informatie bepaald. Het is hierbij van belang om verschillende doelgroepen te definiëren. Informatie is primair van belang voor de ambtenaren die een zaak behandelen of die binnen een proces werkzaam zijn. Daarnaast zijn er meer secundaire gebruikers van informatie, zoals medewerkers elders in de keten of medewerkers die audits of toezicht uitvoeren.

3.2.4 Openbaarheidsniveau

In het verlengde van het toegangsniveau ligt het openbaarheidsniveau. Informatie van de overheid kan of moet soms actief of passief openbaar worden gemaakt. Bijvoorbeeld: de (online) terinzagelegging van vergunningsaanvragen of publicatie van verslagen van de gemeenteraad. Vanuit privacyperspectief is het (nagenoeg) altijd nodig om alleen informatie te publiceren die ontdaan is van persoonsgegevens. In de ontwerpfase kan hier al rekening mee worden gehouden door te definiëren hoe te publiceren informatie wordt opgebouwd, bijvoorbeeld door in het datamodel vast te leggen welke gegevenselementen wel of niet voor publicatie in aanmerking komen. Dan kan er later op geautomatiseerde wijze gepubliceerd worden, zonder dat er eerst handmatig 'lakwerk' vereist is.
In geval van papieren archief wordt, als het goed is, in het register van verwerkingen vastgelegd of en welke (bijzondere) persoonsgegevens er in welke archieven zijn of worden opgenomen. Dit helpt bij het bepalen welke gegevens weggelaten moeten worden bij eventuele publicatie. Zie ook 3.3.1.

3.2.5 Ontwerpkeuzes documenteren

In de praktijk is het niet altijd mogelijk om de ideale situatie te realiseren. Beperkingen in de techniek dwingen soms pragmatische keuzes af. Een veelvoorkomend knelpunt is bijvoorbeeld dat informatiesystemen over beperkte vernietigingsfunctionaliteit beschikken en leveranciers dit alleen tegen kostbaar meerwerk kunnen aanpassen. Omdat in de praktijk bij de aanschaf van een applicatie naar vele facetten wordt gekeken, waarvan archivering en privacybescherming er slechts enkele zijn, kan het zijn dat er een applicatie wordt gekozen die op bepaalde vlakken minder goed scoort, maar op het totale pakket van eisen toch de meeste punten haalt. Het eerste systeem dat perfect is op het totale spectrum van procesondersteuning, beveiliging, privacybescherming, archivering enzovoort moet nog op de markt komen. Daarom is het niet altijd verstandig om in te zetten op het voldoen aan alle eisen. Te zware eisen kunnen ertoe leiden dat geen enkele leverancier zich inschrijft bij een aanbesteding; het uitvoeren van Plan B – een systeem kiezen dat nog niet aan alle eisen voldoet – blijkt dan het best haalbare.

Het is belangrijk om gemaakte ontwerpkeuzes te documenteren en de consequenties voor zowel privacy als archivering te beschrijven en aan de verantwoordelijke voor te leggen. Deze moet de ontwerpkeuzes kunnen verantwoorden en kunnen aangeven welke

maatregelen worden genomen om ondanks een ontbrekende functie in een systeem toch aan de wetgeving te voldoen.

3.2.6 Omgang met legacy: redesign of uitsterfconstructie?

De meeste overheden werken nog deels of geheel met informatiesystemen die niet voldoen aan de 'by design'-principes waarbij vooraf de eisen uit AVG én Archiefwet zijn ingebouwd, zoals in het voorgaande geformuleerd. Dit noemen we in deze handreiking legacy-systemen. Om te bereiken dat het informatiebeheer toch voldoet aan bescherming van persoonsgegevens en aan de Archiefwet, moet een keuze worden gemaakt tussen herontwerpen van deze systemen of andere maatregelen.[14] Dit kan bijvoorbeeld door middel van een risicoanalyse.[15] Of het zinvol is om de systemen te herontwerpen, is afhankelijk van een aantal factoren die je bij deze risicoanalyse gebruikt, zoals:

- aantal legacy-systemen binnen een organisatie
- de aard (gewoon, bijzonder of gevoelig) van de beheerde persoonsgegevens[16]
- de mate waarin de legacy-systemen al aan AVG en Archiefwet voldoen
- plannen om een of meer legacy-systemen op korte termijn te vervangen
- het gemak waarmee de benodigde aanpassingen zijn door te voeren
- budget en menskracht beschikbaar voor systeemaanpassingen
- urgentiebesef bij de systeemeigenaar
- bestaan van acceptabele workarounds

In sommige gevallen kan het zinvol zijn om een uitsterfconstructie te hanteren en de aandacht te richten op vernieuwing, ofwel: eerst de kraan dicht, dan pas dweilen.

In andere gevallen kan het wél zinvol zijn om een bestaand systeem te herontwerpen. Voorbeeld: een systeem is van centraal belang en bevat de belangrijkste documenten binnen een organisatie. Zie ook deel 2, hoofdstuk 2: Inrichting informatiebeheer.

3.3 Delen en publiceren

Het beheer van informatie zou weinig zin hebben als deze niet werd gebruikt en hergebruikt. Bij de beschikbaarstelling aan derden van informatie met persoonsgegevens zijn maatregelen nodig om te voorkomen dat persoonsgegevens onbedoeld of onbevoegd worden verspreid en geraadpleegd. Omdat onze doelgroep, de medewerkers die zich met informatiebeheer bezighouden, hiermee veel te maken heeft, nemen we dit onderwerp hier op. Zie ook deel 2, hoofdstuk 4: Actieve publicatie van informatie met persoonsgegevens.

---

[14] Zie ook de Richtlijn van de Europese EDPB: Guidelines 4/2019 on Article 25: Dataprotection by Design and by default, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_nl

[15] Zie voor een methode van risico-analyse bijvoorbeeld: Handreiking Dataclassificatie Baseline Informatie Overheid, https://www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/

[16] Zie voor het onderscheid tussen gewone, bijzondere en gevoelige persoonsgegevens deel 2, hoofdstuk 2, paragraaf 1.

3.3.1 Patronen voor beschikbaarstelling

Er is een aantal patronen te onderscheiden als het gaat om beschikbaarstelling van informatie met persoonsgegevens aan derden. Zie ook deel 2 hoofdstuk 4 voor de algemene richtlijnen daarbij.

In principe zijn er twee mogelijkheden:

1. De informatie wordt openbaar, zoals bij de online publicatie op een openbaar platform, bijvoorbeeld de website van de betrokken overheid.
2. De informatie wordt via een niet-openbaar platform of kanaal, zoals bijvoorbeeld MijnOverheid of via e-mail beschikbaar gesteld.

Afhankelijk van platform, doelstelling en gebruiker verwijder je al dan niet de persoonsgegevens, bijvoorbeeld door anonimiseren van een kopie. Er kan daarbij ook onderscheid gemaakt worden tussen gewone en bijzondere of gevoelige persoonsgegevens. Met deze laatste moet nog veel terughoudender worden omgesprongen dan met gewone persoonsgegevens, zie ook deel 2 paragraaf 2.1.

We onderscheiden hier vijf patronen:

1. publiceren van informatie op een openbaar platform
2. publiceren van informatie op een niet-openbaar platform
3. aanbieden van open data
4. genereren van een dataset voor een specifiek doel
5. toesturen of beschikbaar stellen van informatie via een niet-openbaar kanaal

Patroon 1: (bijzondere) persoonsgegevens moeten waar nodig verwijderd zijn uit de gepubliceerde versie, op zo'n manier dat een handige gebruiker de gegevens niet toch tevoorschijn kan halen. Verwijderen kan hier zijn: pseudonimiseren, zie de paragraaf hieronder.

Patroon 2: platforms als MijnOverheid zijn besloten en beveiligd. Daarom kunnen persoonsgegevens, ook bijzondere en gevoelige, er zo nodig worden gepubliceerd.

Patroon 3: er mogen geen persoonsgegevens in de datasets staan. Daarnaast is het belangrijk om te analyseren wat de risico's op profilering door de potentiële hergebruiker zijn, bijvoorbeeld als er uitgebreide datasets aan geografische gegevens zijn gekoppeld. Betrek hierbij altijd een privacyfunctionaris of FG.

Patroon 4: analyseer goed wie de afnemer is, wat diens belang is en welke gegevens voor het specifieke doel van waarde zijn. Dit patroon heeft vaak betrekking op (intern of extern) onderzoek en/of het trainen van een algoritme. De afnemer moet duidelijk kunnen aangeven welke gegevens nodig zijn, de verstrekker moet duidelijk kunnen aangeven wat de kwaliteit van de verstrekte gegevens is. Er is dus een dialoog nodig om te kunnen bepalen welke maatregelen in een specifieke situatie vereist zijn. Betrek ook hierbij altijd een privacyfunctionaris of FG.

Patroon 5: hiervoor geldt hetzelfde als voor patroon 1. Behalve dat er, afhankelijk van de doelstelling en de ontvangende partij, in dit patroon uitzonderingen kunnen voorkomen.

Bijvoorbeeld als documenten tussen overheden worden uitgewisseld, of tussen een overheid en een rechtsprekende instantie in het kader van een juridisch proces. Betrek ook hierbij de privacyfunctionaris of FG.

Bij het beschikbaar stellen van informatie uit papieren archieven gelden bovenstaande principes ook. Meestal zullen digitale kopieën worden gebruikt bij publicatie en andere terbeschikkingstelling. Het verwijderen van persoonsgegevens uit de kopie zal dan vaak handmatig moeten gebeuren.

3.3.2 Anonimiseren of pseudonimiseren

Er zijn twee manieren om processen in te richten waarbij informatie wordt ontdaan van persoonsgegevens, namelijk:

1. **anonimiseren**: persoonsgegevens zijn onherstelbaar uit een bestand verwijderd.
2. **pseudonimiseren**: persoonsgegevens zijn versleuteld en daardoor onherkenbaar gemaakt. Met behulp van de gebruikte sleutel kan dit echter wel hersteld worden. Zie ook deel 2 paragraaf 2.3.

In algemene zin geldt dat het bij het openbaar maken van informatie vaak verstandig is om te pseudonimiseren. Niet door de bron te anonimiseren, want in dat geval is er feitelijk sprake van onrechtmatige archiefvernietiging, maar door een geanonimiseerd nieuw publicatiebestand te creëren. Het is wel belangrijk ervoor te zorgen dat het verwijderde gegeven niet uit de context kan worden opgemaakt. Een voorbeeld: wel de naam weghalen, maar niet het adres. Bij hergebruik van informatie binnen ketens kan het verstandig zijn om een kopie van het origineel te ontdoen van persoonsgegevens, waarbij sommige gebruikers wel en sommige niet over de sleutel beschikken om de persoonsgegevens weer zichtbaar te maken, afhankelijk van hun rol binnen het proces. Een risico van het werken met gepseudonimiseerde kopiebestanden is dat deze gehackt kunnen worden. Als een hacker de sleutel achterhaalt, dan kan de pseudonimisering ongedaan worden gemaakt. Voor de keuze om een dergelijke methodiek te gebruiken, is het verstandig om een risicoanalyse uit te voeren. Natuurlijk is het noodzakelijk om ook daarbij weer deskundigen op het terrein van privacy te betrekken.

3.4 Rechten van burgers met betrekking tot hun persoonsgegevens

Een betrokkene van wie de overheid persoonsgegevens verwerkt, kan op basis van de AVG een verzoek bij die overheid indienen om persoonsgegevens over haar of hem in te zien, te rectificeren, te verwijderen enzovoort. Een uitgebreide beschrijving van deze rechten en de uitzonderingen daarop zijn te vinden in hoofdstuk 5 van dit deel.
Om bij alle verzoeken van betrokkenen een zorgvuldige afweging van belangen te kunnen maken, is het nodig om contactpersonen aan te wijzen en procedures in te richten waarbij deskundigheid op het terrein van zowel de Archiefwet als de AVG wordt betrokken.

3.5 Overbrenging naar een archiefbewaarplaats

Voor de overbrenging van permanent te bewaren archieven of informatie naar een archiefbewaarplaats wordt overlegd tussen de archiefvormer en de beheerder van de bewaarplaats, meestal de archivaris.[17] Daarbij wordt gezamenlijk bepaald welke informatie na overbrenging beperkt openbaar moet blijven. Bijzondere persoonsgegevens in de zin van de AVG – dus van nog levende personen – zijn op grond van Archiefwet artikel 2a sowieso beperkt openbaar. Ook op grond van artikel 15 van de wet kunnen beperkingen worden gesteld op basis van 'eerbiediging van de persoonlijke levenssfeer'.

Bij informatie die volgens het 'by design and default'-principe is ingericht, is het eenvoudig om bij overbrenging onderdelen uit te zonderen van raadpleging of gebruik door ze beperkt openbaar te stellen. Ook is het nuttig als het register van verwerkingen en/of archievenoverzicht duidelijk weergeeft welke digitale informatie en welke papieren archieven (bijzondere) persoonsgegevens bevatten. Zo is bij overbrenging snel te bepalen welke informatie en archieven na overbrenging beperkt openbaar moeten blijven. Het alternatief, handmatig uitzoeken van deze informatie, kan zeer tijdrovend zijn.

[17] Archiefbesluit artikel 9 onder 2 en 3. De beperkende bepalingen worden opgenomen in de verklaring van overbrenging.

4 Maatregelen op operationeel niveau

4.1 Inleiding

Op operationeel niveau hebben overheden te maken met praktische vraagstukken. Bijvoorbeeld als het gaat om verzoeken om informatie die is vastgelegd in legacy-systemen, waarop de 'by design'-principes nog niet zijn toegepast. Of om een specifiek verzoek in het kader van 'het recht op vergetelheid', om daadwerkelijke vernietiging en het opstellen van verklaringen van vernietiging. In dit hoofdstuk worden enkele veelvoorkomende vraagstukken behandeld.

4.2 Delen en publiceren

Bij het delen of publiceren van informatie met persoonsgegevens gaat het vaak om informatie die in bestaande systemen is vastgelegd, waarbij de design-principes zoals beschreven in het vorige hoofdstuk nog niet altijd zijn toegepast. Dit betekent dat het vaak nodig is om informatie handmatig te bewerken voordat deze gedeeld of gepubliceerd kan worden. Bijvoorbeeld het weglakken van persoonsgegevens in documenten die in het kader van een Wob-verzoek worden verstrekt.

De originele bron moet op grond van de Archiefwet authentiek en ongewijzigd blijven. De meest praktische oplossing is dus om kopieën te maken van de informatie en die kopieën te anonimiseren. Het kan daarbij verstandig zijn om deze geanonimiseerde versies wel aan het dossier toe te voegen, zodat deze bewerking niet nogmaals uitgevoerd hoeft te worden als dezelfde informatie nog een keer gedeeld of gepubliceerd moet worden. Dit geldt bij zowel digitaal als papieren archief.

4.3 Verzoeken in het kader van rechten van burgers met betrekking tot hun persoonsgegevens

Een burger kan op basis van de AVG hoofdstuk 3 een verzoek indienen om persoonsgegevens over hem in te zien, te rectificeren, te verwijderen enzovoort. Op deze rechten zijn uitzonderingen, die voor de overheid van belang zijn. Het is zaak ervoor te zorgen dat in elk individueel geval de rechten van de burger en de uitzonderingen daarop goed in acht worden genomen en de belangen zorgvuldig tegen elkaar worden afgewogen. Daarvoor is het nodig procedures te volgen die de organisatie, als het goed is, op tactisch niveau heeft ingericht, zie het vorige hoofdstuk.

Zie voor een uitgebreide beschrijving van de rechten van betrokkenen, de uitzonderingen daarop en hoe hiermee om te gaan deel 2 hoofdstuk 5.

4.4 Feitelijke vernietiging

In hoofdstuk 3 is beschreven dat het vernietigingsproces en de vernietigingsfunctionaliteit als onderdeel van de designmethodiek worden ingericht. Dit wordt in praktijk gebracht bij het inrichten van nieuwe informatiesystemen. Een rol in de organisatie wordt dan verantwoordelijk gemaakt voor de tijdige uitvoering van dit proces: het jaarlijks initiëren van

de vernietigingscyclus, inclusief alle interne goedkeuringsstappen die daarbij horen. Gebruikelijk is om deze taak te beleggen bij de afdeling die zich bezighoudt met operationeel informatiebeheer (vaak DIV geheten).

Voorbeeld: Een burger verzoekt om redenen van privacy om zijn uitkeringsdossier, met daarin gegevens over zijn gezinsomstandigheden, te vernietigen. De privacyfunctionaris die dit verzoek behandelt, neemt contact op met de afdeling Informatiebeheer van de gemeente. Deze meldt dat de bewaartermijn uit de selectielijst van het dossier nog niet is verstreken. Gezamenlijk constateert men dat aan het verzoek niet kan worden voldaan, omdat het hier gaat om een verwerking op grond van een wettelijke taak (de Participatiewet) en de wettelijke bewaartermijn nog niet is verstreken. Dit wordt aan de verzoeker medegedeeld. Wel wordt hem verzekerd dat het dossier goed is beveiligd tegen onbevoegde inzage en tijdig zal worden vernietigd

Een aandachtspunt bij de uitvoering van vernietiging is het correct toepassen van de uitzonderingscriteria. Informatie die voor vernietiging in aanmerking komt, mag alleen langer worden bewaard als daar gegronde redenen voor zijn. Denk bijvoorbeeld aan een bijzondere (lokale of landelijke) gebeurtenis ('hotspot'), zaak of persoon. De criteria hiervoor zijn in de selectielijst vastgelegd. De zorgdrager past de criteria toe en bepaalt welke specifieke uitzonderingen er in de organisatie worden gehanteerd (bijvoorbeeld: informatie met betrekking tot de coronacrisis van 2020, die zeker als 'hotspot' aangemerkt kan worden). Deze criteria voor uitzonderingen en de toepassing ervan zullen dus zorgvuldig gecommuniceerd moeten worden met de informatie-eigenaren bij de vakafdelingen én, vanwege het privacy-aspect, met de privacyfunctionaris, privacyjurist of FG. Natuurlijk moeten persoonsgegevens, vooral de bijzondere en gevoelige, ook wanneer zij vanwege zo'n uitzonderingsgrond in de selectielijsten bewaard blijven, goed afgeschermd en beperkt openbaar gesteld worden. Bescherming van persoonsgegevens sluit immers niet uit dat informatie met persoonsgegevens langdurig bewaard mag worden als historische bron.

4.5 Verklaring van vernietiging

Het Archiefbesluit verplicht in artikel 8 tot het opstellen van een 'verklaring van vernietiging' met specificatie van wat is vernietigd. Het Archiefbesluit geeft niet aan welke informatie deze verklaring en specificatie precies moeten bevatten. De praktijk is dan ook dat overheden hier verschillend mee omgaan. Sommige overheden maken uitputtende lijsten met zeer gedetailleerde informatie over de individuele vernietigde dossiers, andere overheden stellen verklaringen op meer geaggregeerd niveau op. Hierin zijn dus verschillende scenario's mogelijk. Het is goed om steeds te blijven bevragen of het principe van minimale gegevensverwerking wel wordt toegepast. Is het in alle gevallen nodig om

uitgebreide beschrijvingen met veel persoonsgegevens te bewaren voor het doel? Dat doel is immers: het bewijs dat informatie is vernietigd.

Een mogelijk scenario is een getrapte aanpak. Het kan voor het interne goedkeuringsproces handig zijn om in eerste instantie een meer gedetailleerd overzicht op te stellen, dat na afloop geaggregeerd wordt tot een formele verklaring waarin details op dossierniveau zijn weggelaten. Op de uiteindelijk te bewaren verklaring staat dan bijvoorbeeld: '150 dossiers van het zaaktype Klachten met afhandelingsdatum in het jaar 2018'. Het eerdere overzicht met uitgebreide beschrijvingen wordt dan vernietigd.

Welke mate van abstractie en minimale gegevensverwerking in een vernietigingslijst volstaat binnen de kaders van de Archiefwet en AVG, kan verschillen per organisatie, proces of taakgebied. Het is raadzaam om af te stemmen met de deskundige op het gebied van informatiebeheer en, bij decentrale overheden, de archiefinspectie én met de FG of privacyfunctionaris over het benodigde detailniveau van vernietigingslijsten. De verklaring van vernietiging mét specificatie moet op grond van alle selectielijsten permanent worden bewaard. Bij overbrenging is het zaak afspraken te maken met de archiefdienst over de mate van openbaarheid. Wanneer er (bijzondere of gevoelige) persoonsgegevens in de specificatie voorkomen, moet de openbaarheid worden beperkt volgens de regels van de Archiefwet, zie ook 3.5.

DEEL 2: VERDIEPING

Inleiding

In dit tweede deel worden de onderwerpen die in het eerste deel als praktijkmaatregel zijn beschreven, uitgediept. De samenloop tussen Archiefwet en AVG wordt in dit deel voorzien van een uitgebreider theoretisch en juridisch kader, met meer voorbeelden.
Ook in dit deel gat het om informatie- en archiefbeheer vanaf het ontstaan tot en met de vernietiging of overbrenging. De omgang met informatie in een archiefbewaarplaats blijft buiten beschouwing.[18]

[18] Informatie daarover is onder meer te vinden op: https://kia.pleio.nl/groups/view/48594512/kennisplatform-informatierecht. Zie ook Archiefwet artikelen 2A en 15 t/m 17 en de risicoanalyse op de gezinskaarten van het bevolkingsregister: https://vng.nl/sites/default/files/model_risicoanalyse_gezinskaarten_definitief.pdf

1 Belang van integraal beheer, basisbegrippen uit Archiefwet en AVG

Persoonsgegevens waarvan de verwerking wordt geregeld in de AVG, maken bij de overheid vrijwel altijd deel uit van 'archiefbescheiden': informatie waarmee de omgang wordt geregeld in de Archiefwet. In het eerste deel van deze handreiking is al duidelijk geworden dat voor de praktijk van het informatiebeheer integrale uitvoering van AVG én Archiefwet nodig is. Hiervoor is binnen overheidsorganisaties samenwerking tussen enerzijds informatiemanagers en -beheerders (zoals DIV'ers) en anderzijds de FG, privacyfunctionarissen en privacyjuristen cruciaal. Alleen dan kan het informatiebeheer voldoen aan beide wetten.[19]
Hieronder volgen enkele basisprincipes uit Archiefwet en AVG die relevant zijn voor informatiebeheer en in relatie tot elkaar invulling in de praktijk zullen krijgen.

1.1 Basisprincipes uit de Archiefwet

Informatie ontstaat bij de overheid tijdens de uitvoering van haar taken. Informatie kan bestaan uit tekstdocumenten, (3D-)tekeningen, video's, foto's, geluidsopnamen, algoritmen, log-gegevens en linked data. Het maakt niet uit welke vorm het heeft: als het ontstaan is uit en tijdens een overheidstaak, valt het onder de Archiefwet.

Overheidsinformatie heeft waarde voor de eigen bedrijfsvoering en het geheugen van de overheid, voor de publieke verantwoording en het maatschappelijk geheugen, voor bewijs en rechtsvinding, en ten slotte voor het historisch onderzoek en als erfgoed. Om al deze redenen is het van belang dat overheidsinformatie voldoende inhoud heeft en context biedt om een zaak te kunnen reconstrueren, dat ze authentiek en integer is, dat wil zeggen dat de informatie is wat ze beweert te zijn, onveranderd blijft en niet gemanipuleerd is.

Op basis van de Archiefwet zijn overheden verplicht om hun informatie in 'goede, geordende en toegankelijke staat' te bewaren en tijdig te vernietigen. Per categorie overheidsinformatie worden **bewaartermijnen** vastgesteld in **selectielijsten.** Dit kan per categorie variëren van één dag tot blijvend. Na afloop van de bewaartermijn is de overheid **verplicht** die informatie te **vernietigen**. Permanent te bewaren informatie is informatie die blijvend van maatschappelijke en historische waarde is. Blijvend te bewaren informatie – een klein deel van het geheel – moet na twintig jaar worden **overgebracht** naar een gemeentelijke, provinciale of rijks**archiefbewaarplaats** en wordt daar in principe openbaar en raadpleegbaar.[20] Na ontstaan van de informatie zijn er op basis van de Archiefwet dus twee mogelijkheden: de informatie wordt bewaard totdat de wettelijke termijn is verstreken, en wordt daarna vernietigd, óf na twintig jaar overgebracht naar een archiefbewaarplaats.

---

[19] In de praktijk is natuurlijk ook samenwerking nodig met functionarissen als de CISO voor informatiebeveiliging en de informatiecommissaris of Wob-functionaris. Deze handreiking beperkt zich echter tot het samengaan van AVG en Archiefwet.

[20] Overbrenging naar een archiefbewaarplaats mag in tijdsblokken gebeuren, waarbij de oudste informatie hoogstens dertig jaar oud mag zijn. Een wijziging van de Archiefwet is in voorbereiding, waarbij de overbrengingstermijn verkort zal worden. Ook voor de bescherming van persoonsgegevens na overbrenging naar een archiefbewaarplaats bestaan wettelijke waarborgen, zie noot 1.

1.2 Basisprincipes uit de AVG

Bij de uitvoering van overheidstaken worden persoonsgegevens verwerkt. Persoonsgegevens zijn alle gegevens die direct of indirect herleidbaar zijn tot een natuurlijke persoon. Onder 'verwerken' verstaat de AVG alle mogelijke handelingen met persoonsgegevens, zoals: verzamelen, opslaan, bewerken, wijzigen, verzenden en vernietigen. Persoonsgegevens staan niet op zichzelf, maar maken meestal deel uit van overheidsinformatie.

Bij de verwerking van persoonsgegevens gelden de volgende principes:
Een verwerking van persoonsgegevens moet **rechtmatig** zijn. Een **rechtmatige grondslag** kan in geval van de overheid bijvoorbeeld zijn: een wettelijke verplichting, een taak van algemeen belang of de uitoefening van openbaar gezag. Niet alles wat de overheid doet, vloeit echter voort uit een wet, uit algemeen belang of overheidsgezag. Denk aan bedrijfsvoering. Dan is een andere grondslag nodig, bijvoorbeeld een overeenkomst of toestemming (AVG artikel 6).[21]
Voor veel overheidsorganisaties zal een grondslag zoals 'wettelijke verplichting' of 'algemeen belang' voldoende basis zijn om persoonsgegevens in hun informatie en archieven te verwerken. Immers, als een overheid de persoonsgegevens nodig heeft voor bijvoorbeeld het uitvoeren van een wettelijke taak, zoals het toekennen van een uitkering of een subsidie, kunnen de gegevens niet worden verwijderd zolang ze nodig zijn voor dat doel. Op dat moment is 'wettelijke verplichting' de grondslag voor het verwerken van de persoonsgegevens, en niet 'archivering in het algemeen belang'. Dat laatste wordt pas een grondslag voor de verwerking wanneer de informatie op den duur blijvend bewaard moet worden op basis van de selectielijst.
Let op: als de primaire verwerking niet rechtmatig was, is het langer bewaren onder de noemer 'archivering in het algemeen belang' ook niet rechtmatig![22] Dit is in 2017 bevestigd in een uitspraak van de Raad van State: archivering is geen excuus om onder alle omstandigheden persoonsgegevens te bewaren die oorspronkelijk niet mochten worden verwerkt.[23]

Samengevat:

- De grondslag voor verwerking van persoonsgegevens in overheidsinformatie die op den duur vernietigbaar is volgens de selectielijst, is wettelijke verplichting, taak van algemeen belang, uitoefening van openbaar gezag, overeenkomst of een andere grondslag zoals genoemd in AVG artikel 6.
- De grondslag voor verwerking van persoonsgegevens in overheidsinformatie die blijvend bewaard moet worden op grond van de selectielijst, is aanvankelijk een van de

[21] Bij de overheid is 'vrije en goed geïnformeerde toestemming' in de zin van de AVG wel problematisch, omdat burgers niet altijd vrij zijn om toestemming te geven aan een overheid waarvan zij afhankelijk zijn.
[22] Zie AVG artikel 5.2.
[23] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2017:2232. Destijds gold de Wbp, maar onder de AVG zijn deze regels onveranderd. Lees ook het artikel: https://www.dirkzwager.nl/kennis/artikelen/raad-van-state-archiefwet-geen-excuus-voor-privacyschending/

bovengenoemde grondslagen. Vervolgens worden zij **verder** verwerkt op grond van 'archivering in het algemeen belang', zoals genoemd in AVG artikelen 5.1 en 89.
- De verwerking ten behoeve van 'archivering in het algemeen belang' wordt in de AVG als verenigbaar beschouwd met de oorspronkelijke verwerking. Er wordt dan van uitgegaan dat bij de oorspronkelijke verwerking de basisprincipes, zoals het uitgangspunt van 'minimale gegevensverwerking', zijn gehanteerd.
- Persoonsgegevens mogen in beginsel niet langer worden bewaard dan nodig is, maar ten behoeve van 'archivering in het algemeen belang' is een langere bewaring wel toegestaan, als dit zo in een selectielijst is vastgelegd. Vanaf het begin van dergelijke verwerkingen is het nodig om rekening te houden met langdurige bewaring.

Naast het principe van de **rechtmatigheid** zoals hierboven uitgelegd, zijn de volgende principes uit de AVG van belang voor informatiebeheer: **dataminimalisatie** (niet meer gegevens verwerken dan noodzakelijk voor dat doel) en **doelbinding** (de gegevens niet langer en niet voor andere doelen bewaren dan voor het bewuste doel noodzakelijk is). Ook wanneer een verwerking rechtmatig is, moeten dus niet onnodig veel gegevens worden verwerkt en moeten zij niet langer bewaard worden dan strikt nodig voor dat doel. Wie persoonsgegevens beheert moet verder **passende maatregelen** treffen om de privacy te waarborgen. Dit geldt ook voor verwerking van persoonsgegevens op basis van 'archivering in het algemeen belang'.

Op grond van de AVG dient verder onderscheid te worden gemaakt tussen digitale en papieren informatie. Bij **digitale informatie** is doorgaans sprake van 'geautomatiseerde verwerking', bijvoorbeeld opslaan van informatie in een DMS of zaaksysteem met digitale zoekfunctie. Daarvoor geldt de AVG als er persoonsgegevens in voorkomen, en dat is vrijwel altijd zo. Er kan onderscheid worden gemaakt tussen gescande documenten, die bij de huidige stand van de techniek niet altijd geautomatiseerd doorzoekbaar zijn, en digitaal geboren of gescande documenten, die dat wél zijn. In de tweede categorie zijn er meer risico's voor betrokkenen, omdat hun gegevens makkelijker vindbaar zijn. In dat geval gelden alle bepalingen van de AVG en zijn alle mogelijke maatregelen nodig om deze te beschermen.
Papieren archieven vallen alleen onder de AVG als er sprake is van een gestructureerd 'bestand'. In de definitie van de AVG artikel 4.6 is dat het geval als het bestand op naam of op andere (persoons)gegevens toegankelijk is. Voorbeelden: een bestand met personeelsdossiers, subsidiedossiers of dossiers van de sociale dienst, maar ook een serie bouwdossiers, toegankelijk op adres, waarin persoonsgegevens voorkomen.[24]

[24] De AVG schrijft uiteraard meer voor dan in dit hoofdstuk beschreven is: een passende organisatorische en technische beveiliging, het aanstellen van een Functionaris Gegevensbescherming, het opstellen en bijhouden van een register van verwerkingen en het melden van datalekken. Deze aspecten blijven in deze handreiking, die zich concentreert op het beheer van persoonsgegevens in informatie, grotendeels buiten beschouwing. Over deze andere aspecten is informatie te vinden op: https://autoriteitpersoonsgegevens.nl/

2 Inrichting van het informatiebeheer en passende maatregelen

Zoals beschreven in deel 1 is het effectief om AVG-principes als rechtmatige grondslag, dataminimalisatie en doelbinding toe te passen vanaf het ontwerpen van een werkproces. Bijvoorbeeld in een systeem waarin de informatie die het proces ondersteunt, wordt gearchiveerd. Dit is de zogenoemde 'privacy by design and default', die bij voorkeur samengaat met 'archiving by design'.[25]

Voorbeeld: het opnemen van bewaartermijnen volgens de geldende selectielijst draagt bij aan de doelbinding en dataminimalisatie uit de AVG. Wanneer een register van verwerkingen conform de AVG wordt gemaakt, kan dit worden gekoppeld aan het overzicht van alle informatie, dat op grond van de Archiefwet verplicht is.

Voor bestaande systemen, waarbij dit nog niet vanaf het begin is ingeregeld, moeten maatwerkoplossingen worden bedacht. Vragen die de beheerder zich daarbij moet stellen, zijn: welke gegevens worden beheerd, hoe is de toegankelijkheid (tot persoonsgegevens) geregeld, hoe kunnen de bewaartermijnen uit de selectielijst organisatorisch en technisch het beste worden uitgevoerd?
Bij voorkeur gebeurt dit op basis van inventarisatie en risicoanalyse: in welke systemen in de organisatie zitten veel (bijzondere) persoonsgegevens, welke systemen moeten dus het eerst worden bekeken op AVG-compliancy en wat moet er eventueel gebeuren om dat te bereiken?[26]

2.1 Beheer van bijzondere en gevoelige persoonsgegevens

In principe verbiedt de AVG in artikel 9 de verwerking van 'bijzondere persoonsgegevens'. Dit zijn gegevens over gezondheid; biometrische gegevens met het oog op de unieke identificatie van een persoon, zoals vingerafdrukken, irisscans of gegevens gerelateerd aan gezichtsherkenning; genetische gegevens zoals DNA; seksuele gedragingen of voorkeuren; lidmaatschap van een vakbond; politieke opvattingen; religie of levensbeschouwelijke overtuigingen; ras of etnische afkomst. Ook voor het verwerken van strafrechtelijke gegevens gelden strengere regels dan voor gewone persoonsgegevens.[27] Uitzonderingen op het verbod zijn onder meer verwerkingen die noodzakelijk zijn om redenen van 'zwaarwegend algemeen belang', of met het oog op 'archivering in het algemeen belang', en op grond van wetgeving. Een zwaarwegend algemeen belang geldt bijvoorbeeld in geval van medici, die gezondheidsgegevens verwerken en kerken, die ledenlijsten aanleggen.

[25] Privacy by design and default is verplicht op grond van AVG artikel 25. Archiving by design is een meer omvattende, gewenste en efficiënte praktijk.
[26] Dit kan een risicoanalyse zijn, bijvoorbeeld op basis van de 'Handreiking Dataclassificatie Baseline Informatie Overheid', zie: https://www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/
[27] Zie: AVG, artikel 10.

Bijzondere categorieën persoonsgegevens mogen **in een vervolg op de oorspronkelijke verwerking** verder worden verwerkt in het kader van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Vooropgesteld natuurlijk weer dat de primaire verwerking rechtmatig was; zo niet, dan is de vervolgverwerking dat ook niet. Een andere voorwaarde is dat er 'passende maatregelen' worden getroffen voor de bescherming van de privacy (AVG artikel 89).
Bij verwerking van bijzondere persoonsgegevens moet altijd 'de noodzaak en evenredigheid met het nagestreefde doel' worden gewaarborgd, 'de wezenlijke inhoud van het recht op bescherming van persoonsgegevens worden geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene'.[28] De bescherming van deze gegevens moet dus nog van een veel hoger niveau zijn dan bij 'gewone' persoonsgegevens!
Het is dan ook aan te raden om de noodzaak van het verwerken van bijzondere persoonsgegevens zeer goed te verantwoorden en besluiten omtrent het beheer ervan bewust te nemen en te documenteren. Het is van belang om daar in alle fasen een FG of privacyfunctionaris bij te betrekken. In de eerste plaats: weeg bij het ontwerpen en inrichten van een systeem af of het echt nodig is de bijzondere gegevens op te nemen. Ook bij het bepalen van de bewaartermijnen en het toegangsniveau tot informatie met bijzondere persoonsgegevens is het raadzaam in elk geval een privacyfunctionaris of FG te betrekken.
De AVG schrijft voor dat de organisatie in kaart brengt welke bijzondere categorieën persoonsgegevens uit artikel 9 worden verwerkt en in welke informatie die zitten. Daarnaast is het aan te bevelen dat een organisatie voor zichzelf definieert welke 'gevoelige gegevens' en gegevens over kwetsbare personen worden verwerkt. Ook deze verdienen bewuste besluitvorming rond het verzamelen en bewaren van de gegevens, en strenge bescherming van de toegang ertoe, op hetzelfde niveau als bij de bijzondere persoonsgegevens.

Kwetsbare personen zijn: kinderen onder de zestien; hulpbehoevende ouderen; statushouders; mensen met taalachterstand; mensen die een Wmo-voorziening ontvangen; andere kwetsbare individuen waaronder bijstandsgerechtigden, minima; slachtoffers van (huiselijk of seksueel) geweld.

Voorbeelden van gevoelige gegevens zijn:
BSN; kopie paspoort; geboortedatum; locatiegegevens (bijvoorbeeld via navigatie, elefoon, gegevens over reizen in het openbaar vervoer); gegevens over elektronische communicatie (incl. IP-adres, apparaat-ID, MAC-adres, wifiverbindingen); financiële gegevens (inkomensgegevens bankgegevens, rekeningnummer, uitkeringsgegevens).

[28] Zie: AVG, artikel 9, lid 2 onder g.

Verwerking van dit type gegevens valt niet altijd onder artikel 9 van de AVG, maar verdient toch extra bescherming.[29]

2.2 BSN en andere landelijke identificatienummers

Het BSN en andere identificatienummers mogen niet zomaar worden verwerkt, ook niet door de overheid. In artikel 46 van de Uitvoeringswet AVG is bepaald dat het BSN en dergelijke identificatienummers alleen mogen worden gebruikt als dat nadrukkelijk zo in een wettelijke bepaling staat. Aan de verwerking van dit soort identificatienummers zijn significante risico's voor betrokkenen verbonden, zoals het risico op identiteitsfraude. Informatie met BSN's moet dan ook altijd worden behandeld als de categorie gevoelige persoonsgegevens. Bij overbrenging naar een archiefbewaarplaats van informatie die BSN's of dergelijke nummers bevat, moet er bijvoorbeeld speciaal voor worden gewaakt dat de BSN's beperkt openbaar worden.[30]

2.3 'Passende waarborgen' bij het verwerken van persoonsgegevens in overheidsinformatie

Elke verwerkingsverantwoordelijke annex archiefvormer moet 'passende technische en organisatorische maatregelen treffen' om de privacy te waarborgen bij het verwerken van persoonsgegevens (AVG artikel 24). In de AVG wordt deze voorwaarde nog eens specifiek gesteld voor het (langdurig) bewaren van informatie met persoonsgegevens onder het motto 'archivering in het algemeen belang' (AVG artikel 89). Daarbij wordt als expliciete maatregel pseudonimiseren genoemd. Verder worden de passende waarborgen – technische en organisatorische maatregelen – in de AVG niet omschreven. Het is een open norm die nadere invulling vereist. Op het moment van schrijven van deze handreiking, twee jaar na het van kracht worden van de AVG, kunnen we het volgende zeggen over invulling van de norm bij het informatiebeheer.[31] In de praktijk toepasbare maatregelen zijn de volgende:

2.3.1 Anonimiseren

Anonimiseren is het zodanig bewerken van gegevens dat deze niet meer – direct of indirect – herleidbaar zijn tot een persoon.[32] De AVG is dan ook niet van toepassing op informatie met geanonimiseerde persoonsgegevens. Anonimiseren van de brongegevens zelf – in tegenstelling tot kopieën – zal bij de overheid slechts in uitzonderingsgevallen toegepast kunnen worden. Alleen in overeenstemming met een selectielijst en na advies van een archivaris of informatiespecialist kan anonimisering plaatsvinden.
In sommige gevallen, bijvoorbeeld wanneer de gegevens alleen statistisch van belang zijn,

[29] In AVG artikel 8 zijn extra bepalingen opgenomen over gegevens met betrekking tot kinderen onder de zestien.
[30] Onrechtmatig toegevoegde BSN's moeten worden verwijderd. Bij rechtmatig toegevoegde BSN's is verwijdering vóór het einde van de bewaartermijn uit de selectielijst niet mogelijk.
[31] Zie ook het Privacy by Design Framework van Privacy Company: https://www.privacycompany.eu/files/Privacy%20by%20Design%20Framework.pdf
[32] Zie de EU-richtlijn voor anonimiseringstechnieken: https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf

kan anonimisering uitkomst bieden voor de bescherming van persoonsgegevens. Dan is de herleidbaarheid tot specifieke personen immers niet van belang. Maar in de meeste gevallen zal onomkeerbare anonimisering van persoonsgegevens leiden tot verlies van authenticiteit van de informatie, en dus strijdig zijn met de principes van de Archiefwet. Voor blijvend te bewaren archief geldt dat, wanneer de persoonsgegevens eruit zijn verwijderd, het zijn betekenis verliest voor historische onderzoekers (denk aan genealogen). Maar ook in het stadium vóór vernietiging of overbrenging geldt dat geanonimiseerde informatie niet meer bruikbaar is voor de reconstructie van een zaak, als bewijsvoering of als verantwoording naar de samenleving. Daarmee voldoet geanonimiseerde informatie vak niet meer aan de Archiefwet.[33] In die gevallen is het beter om over te gaan tot pseudonimiseren of een andere passende maatregel.[34]
Let op! Bij anonimiseren van persoonsgegevens moet ervoor worden gewaakt dat niet uit de context alsnog het verwijderde gegeven kan worden afgeleid. Bijvoorbeeld wanneer wel de naam, maar niet het adres is verwijderd.

2.3.2 Pseudonimiseren

Pseudonimiseren is volgens de AVG 'het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder gebruikmaking van aanvullende gegevens'. Bij pseudonimiseren staat voorop dat de koppeling van de informatie met specifieke personen weer hersteld kan worden door toepassing van bijvoorbeeld de sleutel. Het is dan een voorwaarde dat alleen

Als er in een bepaald stadium van gebruik van de informatie wordt gekozen voor pseudonimisering, moet dit ongedaan kunnen worden gemaakt wanneer de informatie nodig is als bewijs, als verantwoording of bij overbrenging naar een archiefbewaarplaats.
Als gegevens van administratief of blijvend belang voorgoed verloren gaan bij pseudonimisering, verliest de informatie immers zijn waarde voor bewaring in het algemeen belang. (AVG, artikel 6 en artikel 89, lid 1)

[33] Zie ook de Kamerbrief van de minister van Veiligheid en Justitie over de toepassing van selectielijsten als het aangewezen instrument voor bewaren en vernietigen van persoonsgegevens in overheidsarchieven, punt 1.3.5 van de brief en bijlage: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/31/tk-voornemens-met-betrekking-tot-de-uavg-en-avg

[34] Zie de Richtlijn van de Europese EDPB: Guidelines 4/2019 on Article 25: Dataprotection by Design and by default, met name onder 52 en 75 ev. Anonimisering wordt daar gelijkgesteld aan vernietiging. Bij de Nederlandse overheid geldt echter het stelsel van selectielijsten op basis van de Archiefwet. Anonimisering kan daardoor alleen worden toegepast als dit overeenstemt met een selectielijst. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_nl

bevoegde personen die sleutel hebben, en dat de twee datasets gescheiden bewaard worden.[35]

Voorbeelden van pseudonimisering zijn het gebruik van verschillende toegangen, encryptie, hashen en polymorfe pseudonimisering:

- **Verschillende toegangen op analoge of digitale informatie**: er kunnen verschillende versies van een toegang op informatie bestaan; een met herleidbare persoonsgegevens en een waarbij de persoonsgegevens zijn weggelaten of gecodeerd. De versie met herleidbare persoonsgegevens is dan alleen door bevoegde personen in te zien.
- **Encryptie**: toepassing van een geheime sleutel. Hierbij staan de persoonsgegevens nog steeds in de dataset, maar in gecodeerde vorm. De partij die over de sleutel beschikt, kan de dataset en de desbetreffende persoonsgegevens eenvoudig decoderen.
- **Hashen**: hierbij worden de ingevoerde persoonsgegevens, ongeacht de omvang/grootte ervan (de invoer) vervangen door een 'uitvoer' van een vaste grootte, bijvoorbeeld een cijfer (hashtag).

Voorbeeld: in een bestand met papieren uitkeringsdossiers komen persoonsgegevens voor van burgers, zoals hun naam, adres, e-mailadres, telefoonnummer en persoonlijke omstandigheden. Alleen voor de behandelende ambtenaren is het nodig om over al deze gegevens te beschikken. Voor andere gebruikers en voor bijvoorbeeld een jaarverslag is het voldoende om algemene informatie te hebben, zoals een overzicht van aantallen verleende en afgewezen uitkeringen en de daaraan verbonden bedragen. Eén exemplaar van de toegang tot de dossiers mét de dossiernummers, namen en andere persoonsgegevens wordt bewaard en is alleen toegankelijk voor de behandelaren. Voor ander gebruik wordt een lijst met alleen de nummers gebruikt, die slechts bepaalde medewerkers kunnen herleiden tot personen.

- **Polymorfe pseudonimisering**: versleuteling waarbij specifieke pseudoniemen voor een gebruiker worden gevormd per ontvangende partij, zonder dat de vormende partij het specifieke pseudoniem kan herleiden of de identiteit van de gebruiker bij gebruik hoeft te kennen.

NB: ook bij pseudonimiseren moet goed worden opgelet of uit de context niet toch het versleutelde persoonsgegeven kan worden afgeleid.

[35] Zie ook: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens#wat-is-pseudonimiseren-6129

2.3.3 Dataminimalisatie

Dit is strikt genomen geen passende waarborg, maar wordt hier toch opgenomen omdat, wanneer dit principe goed wordt toegepast, er minder andere maatregelen nodig zijn. Bij het toepassen van het principe van minimale gegevensverwerking gaat het erom dat niet meer persoonsgegevens worden verzameld en vastgelegd dan nodig voor het doel (perspectief van de betrokkene), maar wel voldoende om het doel van de archivering te bereiken (perspectief van de organisatie). Bij het laatste gaat het dan om de vraag: kan de zaak worden gereconstrueerd aan de hand van de vastgelegde informatie? Idealiter worden deze principes bij de inrichting van systemen al toegepast ('privacy by design and default' en 'archiving by design'), zie het eerste deel.

2.3.4 Bewaartermijnen en tijdige vernietiging

Een belangrijke maatregel voor bescherming van persoonsgegevens is het toepassen van de juiste bewaartermijnen uit de geldende selectielijst en het tijdig vernietigen zodra die termijn is verstreken. Dit geldt voor de informatie als geheel, waar persoonsgegevens deel van uitmaken. Tijdige vernietiging op grond van de selectielijst draagt bij aan het principe 'doelbinding' uit de AVG: niet langer bewaren dan nodig voor het doel. Wanneer een selectielijst niet aan dit principe voldoet, moet deze worden gewijzigd. Zie paragraaf 3.1.

2.3.5 Privacy 'by default': beperking van de toegang door toegangsautorisaties, logging en monitoring

De AVG verplicht in artikel 25 tot het nemen van maatregelen om persoonsgegevens te beschermen bij ontwerp en standaardinstellingen van informatiesystemen. Dit betekent beperking van de toegang tot informatie en systemen met persoonsgegevens. Dit kan via autorisaties en andere vormen van toegangsbeheer tot alleen bevoegde personen die voldoen aan het principe 'need to know'.

Een voorbeeld daarvan is het beperken van inzagerechten in een RMA/DMS, zaaksysteem of andere applicatie tot die personen die dat inzagerecht op basis van hun functie of rol nodig hebben. Binnen applicaties kan de autorisatie verder beperkt blijven of worden uitgebreid, al naar gelang de functie of rol. Voorbeeld: alle medewerkers hebben toegang tot het personeelssysteem, maar zij kunnen alleen hun eigen personeelsdossier inzien. De medewerkers van Personeelszaken kunnen alle dossiers zien, maar alleen sommigen van hen krijgen ook de gevoelige gegevens te zien. Zeker als het gaat om bijzondere en gevoelige persoonsgegevens is deze ingebouwde privacy aan te bevelen. Ook logging en monitoring van wie, wat, wanneer heeft ingezien is een waarborg tegen ongeoorloofde inzage en bevordert bescherming van persoonsgegevens.
Bij analoge archieven zijn maatregelen als het vermijden van persoonsgegevens in zichtbare en herkenbare doos- en mapopschriften, afsluiten van archiefruimten en sleutelbeheer door een beperkt aantal daarvoor aangewezen medewerkers effectief.

2.3.6 Faciliteren van rechten van betrokkenen

Op grond van de AVG hebben burgers rechten met betrekking tot het verwerken van hun persoonsgegevens, zoals het recht op inzage, rectificatie, wissen van gegevens en andere rechten. Bij de overheid kunnen uitzonderingen op deze rechten van toepassing zijn, zie hoofdstuk 5. Er zal bij elke aanvraag een degelijke afweging van belangen moeten plaatsvinden. Het is dus raadzaam procedures in te richten voor verzoeken van burgers, waarbij deskundigheid op het terrein van zowel de AVG als de Archiefwet wordt ingeroepen.

2.3.7 Informatiebeveiliging

Beveiliging volgens de geldende normen, inclusief audits, is onmisbaar voor de bescherming van persoonsgegevens. Informatiebeveiliging moet een continu cyclisch proces zijn. Dit kan bijvoorbeeld aan de hand van risicoanalyse en dataclassificatie, zoals beschreven in de 'Handreiking Dataclassificatie Baseline Informatie Overheid'.[36] Daarin wordt rekening gehouden met bescherming van persoonsgegevens op basis van de AVG én met de bewaartermijnen uit de selectielijsten op basis van de Archiefwet. Binnen de organisatie is het nodig dat CISO, Informatiemanagement/Informatiebeheer en FG of privacyfunctionaris een samenwerking aangaan om op de juiste wijze informatie met persoonsgegevens te beveiligen.

[36] Zie: https://www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/. In deze handreiking gaan we ervan uit dat de organisatie beschikt over een professionele aanpak van informatiebeveiliging, zodat er niet verder inhoudelijk op wordt ingegaan.

3 Bewaartermijnen en archivering in het algemeen belang

3.1 Bewaren en vernietigen van persoonsgegevens bij de overheid

Ook bij het bewaren en vernietigen van persoonsgegevens moeten de AVG en de Archiefwet in onderlinge samenhang worden uitgevoerd. Persoonsgegevens vormen onderdeel van 'archiefbescheiden', de term uit de Archiefwet die informatie, ongeacht de vorm, aanduidt. Net als de AVG bevat de Archiefwet zelf geen concrete bewaartermijnen. Wel leggen overheidsorganisaties op basis van de Archiefwet de bewaartermijnen voor overheidsinformatie vast in zogeheten selectielijsten. De lijsten worden vastgesteld via besluiten in de zin van de Algemene Wet Bestuursrecht (Awb), waarvoor de in deze wet bepaalde uniforme openbare voorbereidingsprocedure geldt. Daarmee worden burgers geacht op de hoogte te zijn van de bewaartermijnen van hun persoonsgegevens, en kunnen zij daartegen bezwaar maken, zie ook hierna 5.1.
Overheidsinformatie – inclusief de persoonsgegevens die erin voorkomen – wordt in de selectielijsten aangemerkt als blijvend te bewaren of als te vernietigen op termijn: zo lang of kort als nodig wordt geacht. Bij het maken van deze keuze vindt een weging plaats van het administratieve, juridische, maatschappelijke en historisch-wetenschappelijke belang van informatie en ook wordt rekening gehouden met privacybescherming. In de procedure voor het vaststellen van de bewaartermijnen zijn verschillende belangen vertegenwoordigd.[37] In de selectielijsten worden ook bewaartermijnen meegenomen die in andere wetgeving zijn bepaald.[38]
Persoonsgegevens die onderdeel zijn van informatie van de overheid, worden doorgaans in de selectielijsten niet apart benoemd. Toch wordt wel degelijk rekening gehouden met bescherming van persoonsgegevens en met de bepalingen van de AVG. In zijn Kamerbrief van 31 oktober 2019 heeft de minister van Justitie en Veiligheid er nog eens expliciet op gewezen dat voor het bepalen van bewaartermijnen van informatie met persoonsgegevens de selectielijsten het geëigende instrument zijn.[39] Het kan natuurlijk voorkomen dat er in een vastgestelde selectielijst nog onvoldoende rekening is gehouden met de bescherming van persoonsgegevens. In dat geval zal de selectielijst geactualiseerd moeten worden.[40]

Bijzondere aandacht verdienen de uitzonderingen op vernietiging. Het komt voor dat informatie die in een selectielijst is aangewezen als vernietigbaar, van vernietiging uitgezonderd kan worden omdat het over bijzondere (lokale) gebeurtenissen ('hotspots'), zaken of personen gaat.[41] Archiefvormer en archivaris overleggen over deze uitzonderingen, die vervolgens door de verantwoordelijke zorgdrager worden benoemd. Voorbeelden zijn bij het ministerie van Defensie de informatie over het gebruik van chroom-6 of in de gemeente

[37] Archiefbesluit, artikel 2.
[38] Bijvoorbeeld in het Wetboek van Koophandel wordt een termijn van ten minste zeven jaar voor financiële gegevens bepaald.
[39] Zie punt 1.3.5 van de brief en bijlage: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/31/tk-voornemens-met-betrekking-tot-de-uavg-en-avg
[40] Voor meer informatie over ontwerpen, vaststellen en actualiseren van selectielijsten, zie: https://www.nationaalarchief.nl/archiveren/waardering-en-selectie
[41] Zie: Archiefbesluit, artikel 5 onder e.

Oss informatie over het ongeluk met de Stint. Het is dus belangrijk om de selectie en vernietiging niet helemaal automatisch te laten verlopen, maar altijd te blijven nadenken over bijzondere omstandigheden. Daarbij moet de bescherming van persoonsgegevens steeds worden afgewogen tegen het (blijvende) maatschappelijk-historische belang van de informatie.

Doelbinding en dataminimalisatie betekenen niet dat bewaartermijnen per definitie kort moeten zijn. Het gaat erom dat de duur van de bewaartermijn zorgvuldig wordt bepaald en te verantwoorden is. Persoonsgegevens, ook bijzondere persoonsgegevens, kunnen voor blijvende bewaring in een archiefbewaarplaats worden aangemerkt.[42]

3.1.1 Register van verwerkingen

Op basis van de AVG leggen overheidsorganisaties bewaartermijnen voor persoonsgegevens vast in het register van verwerkingen. Op basis van de Archiefwet zijn organisaties verplicht om een overzicht te hebben van de informatie die ze in huis hebben. Een organisatie kan ervoor kiezen twee verschillende registers of overzichten aan te leggen, of dit te combineren. Het is in alle gevallen belangrijk dat er niet verschillende termijnen voor het bewaren van persoonsgegevens in dezelfde processen worden gehanteerd: een termijn in de selectielijst en overzicht van informatie en een andere in het register van verwerkingen. Er moet worden voorkomen dat een van beide, óf de AVG óf de Archiefwet, niet wordt nageleefd – en dat het niet meer duidelijk is hoe lang overheidsinformatie bewaard moet blijven. Het is dus noodzakelijk in registers, overzichten en systemen dezelfde bewaartermijnen te hanteren voor dezelfde informatie.

3.1.2 Vernietiging

Verwijdering van persoonsgegevens is pas definitief bij vernietiging. Doorgaans vindt vernietiging van een informatieobject als geheel plaats. Voor vernietiging gelden de volgende bepalingen uit de Archiefwet:

- Zonder vastgestelde selectielijst, of buiten de selectielijst om, mag overheidsinformatie niet worden vernietigd (Archiefwet, artikelen 3 en artikel 5, Archiefbesluit, artikelen 2 t/m 5).
- Vernietiging is verplicht, maar mag niet te vroeg plaatsvinden, pas na afloop van de in de selectielijst vastgestelde bewaartermijn (Archiefwet, artikelen 3 en 5).
- Vernietiging wordt gedocumenteerd (Archiefbesluit, artikel 8).

[42] AVG artikel 9 lid 2 onder j

3.1.3 Vernietiging uit een dossier of document

In sommige gevallen, als de selectielijst het toestaat, is het mogelijk om binnen bepaalde **dossiers** of **zaken** (een deel van) de persoonsgegevens eerder te vernietigen dan de overige informatie. Het is belangrijk dat de keuze voor vernietigen of bewaren dan zo goed mogelijk wordt gemotiveerd, op basis van de geldende selectielijst, en dat de integriteit van het dossier behouden blijft. Het moet immers mogelijk blijven de zaak te reconstrueren aan de hand van het dossier. In het algemeen is het niet mogelijk om gegevens te vernietigen uit een **document**. Documenten met 'gaten' zijn niet meer authentiek. Raadpleeg bij twijfel de informatiespecialist of archivaris en stem af met de FG of privacyfunctionaris!

Voorbeeld: bij het aanvragen van een invalidenparkeerplaats is een medische verklaring verplicht. In het dossier is deze verklaring niet meer nodig, zodra de vergunning is verleend. In de selectielijst is de medische verklaring niet apart genoemd. Na het verlenen van de vergunning kan worden volstaan met een aantekening dat de medische verklaring is gezien door de verantwoordelijke ambtenaar. De verklaring zelf hoeft dan niet meer te worden bewaard.

3.2 Archivering in het algemeen belang

Het maatschappelijke belang van archivering wordt in de AVG en de UAVG erkend. Daarvoor is een aantal bepalingen opgenomen.
Het verder verwerken van persoonsgegevens omwille van 'archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden' beschouwt de AVG als rechtmatig (artikel 5.1b). Het bewaren van persoonsgegevens voor langere tijd, zelfs permanent, blijft dan ook onder de AVG mogelijk. De AVG noemt dit een 'verdere verwerking' van persoonsgegevens die oorspronkelijk voor een ander rechtmatig doel, zoals een wettelijke verplichting, een taak van algemeen belang of de uitoefening van openbaar gezag zijn verzameld. Let wel: persoonsgegevens die niet primair op een dergelijke rechtmatige grondslag zijn verzameld en verwerkt, mogen dus ook niet louter omwille van 'archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden' verder worden verwerkt.[43] Verder stelt de AVG dat, wanneer verwijderen van persoonsgegevens bijvoorbeeld door anonimisering of pseudonimisering het doel van de bewaring niet in de weg staat, de gegevens verwijderd moeten worden.[44] Er zijn echter weinig gevallen te bedenken waarbij persoonsgegevens uit overheidsinformatie voorgoed weggehaald kunnen worden door anonimisering, zonder te tornen aan beginselen van de Archiefwet zoals reconstrueerbaarheid van een zaak, authenticiteit en integriteit van

[43] Organisaties zoals het CBS verzamelen gegevens puur om wetenschappelijke/statistische redenen, maar dit heeft een wettelijke grondslag en is dus rechtmatig.
[44] Zie: AVG, artikel 89 lid 1.

informatie. Het zou bijvoorbeeld wel kunnen in gevallen waarbij uit een **dossier** (niet uit een **document**) vernietigd kan worden, als de selectielijst het toestaat, zoals in het voorbeeld van de invalidenparkeerplaats in de vorige paragraaf. Het is in die gevallen wel aan te bevelen, mocht de selectielijst hierover onduidelijk zijn, deze te verduidelijken of aan te vullen.
Ook als langdurige bewaring op grond van de AVG wél is toegestaan, geldt dat er 'passende waarborgen voor de rechten en vrijheden van de betrokken burgers' moeten worden getroffen, zoals artikel 89.1 van de AVG voorschrijft. Zie de artikelen 2A en 15 t/m 17 van de Archiefwet en paragraaf 2.3 in dit deel voor de invulling van die norm.

4 Actieve publicatie van informatie met persoonsgegevens

Bij het publiceren van informatie met persoonsgegevens in de fase vóór vernietiging of overbrenging naar een archiefbewaarplaats is er geen relatie met de Archiefwet. Toch wordt dit in deze handreiking opgenomen, omdat onze doelgroep, de medewerkers van afdelingen die zich met informatiebeheer bezighouden, hier vaak mee te maken hebben.

4.1 Persoonsgegevens van burgers

In het kader van het 'publiceren uit eigen beweging', bijvoorbeeld in het kader van de Wob of na inwerkingtreding de WOO, zetten overheden hun informatie actief online. Voorzichtigheid is daarbij geboden als het gaat om persoonsgegevens van burgers. Deze gegevens kunnen bijvoorbeeld zijn opgenomen in aanvragen, bezwaarschriften, gemeenteraadsstukken, besluiten, onderzoeken, rapporten en andere informatie die wordt gepubliceerd. (Online) publicatie van namen, (e-mail)adressen, telefoonnummers, BSN's en andere persoonsgegevens van betrokkenen is uit den boze. Al helemaal als het bijzondere of gevoelige persoonsgegevens betreft! Wel moeten deze gegevens in het oorspronkelijke, niet-gepubliceerde document bewaard blijven om de integriteit van de informatie te behouden. Zie hiervoor onder meer de richtlijn 'Publicatie van persoonsgegevens op internet' en de brief van de Autoriteit Persoonsgegevens aan de VNG uit 2017.[45] Ook de anonimiseringsrichtlijn van de Raad voor de Rechtspraak kan behulpzaam zijn.[46]

4.2 Persoonsgegevens van bestuurders en ambtenaren

Professionele gegevens, zoals functie, werktelefoonnummer en e-mailadres van bestuurders en ambtenaren, moeten in de originele informatiebestanden en documenten intact blijven om de integriteit van de informatie te borgen. Of de persoonsgegevens van bestuurders en ambtenaren kunnen worden gepubliceerd, met name online, hangt ervan af of een dergelijke publicatie noodzakelijk is. Bij een actueel onderwerp is het zinvol om contactgegevens bekend te maken, zodat de burger in staat wordt gesteld te reageren en te participeren.[47] In zo'n geval zullen dan ook waar nodig persoonsgegevens van de desbetreffende bestuurder of de behandelend ambtenaar bekendgemaakt worden. Als daarentegen documenten uit wat oudere zaken online worden gepubliceerd, is het niet nodig om de contactgegevens van de behandelend ambtenaar te publiceren. De gegevens zijn bovendien vaak niet meer actueel. Niet-publicabele gegevens dienen wel altijd in het originele bestand bewaard te blijven. Voor de namen en andere professionele gegevens van bestuurders tijdens hun bestuursperiode geldt, dat die op grond van het openbare karakter van het ambt vrijwel

[45] Zie hiervoor: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-wijst-gemeenten-op-privacyregels-bij-publicatie-persoonsgegevens-burgers. In de brief van de Autoriteit aan de VNG van 13 oktober 2017 wordt hier nog eens aan herinnerd. De richtsnoeren zijn te vinden onder: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf

[46] https://www.rechtspraak.nl/Uitspraken/paginas/anonimiseringsrichtlijnen.aspx

[47] Uitspraak van de Raad van State afdeling Bestuursrechtspraak: *Volgens vaste jurisprudentie van de Afdeling dienaangaande is de persoonlijke levenssfeer van personen in het algemeen niet in het geding voor zover het uitsluitend hun beroepshalve functioneren betreft*. Zie: ECLI:NL:RVS:2002:AF2070 dd 18-12-2002

altijd openbaar zijn. Privégegevens van bestuurders en ambtenaren, te onderscheiden van hun professionele gegevens, moeten niet anders worden behandeld dan de gegevens van andere natuurlijke personen. Dus vooral als het gaat om bijzondere persoonsgegevens dienen deze uitgezonderd te zijn van publicatie.
Bij externen, die voor een overheid werken en bijvoorbeeld een rapport aanleveren, moet eventuele publicatie van hun persoonsgegevens vooraf geregeld worden en in de overeenkomst opgenomen zijn.
Het is wel steeds zaak de publicatie van persoonsgegevens te beperken tot het hoogst noodzakelijke, volgens het beginsel van minimale gegevensverwerking.

5 Rechten van betrokkenen en uitzonderingen daarop

Omdat afdelingen als Informatiebeheer/DIV van overheidsorganisaties veel te maken hebben met verzoeken van burgers op basis van de AVG, behandelen we in dit hoofdstuk de rechten én de uitzonderingen. Het is belangrijk om intern procedures in te richten waarbij deskundigheid op het terrein van zowel de AVG als de Archiefwet betrokken is.

Betrokkenen hebben op grond van de AVG rechten bij de verwerking van persoonsgegevens over hen: het recht op informatie, inzage, rectificatie en andere rechten. Op deze rechten is in de AVG en Uitvoeringswet AVG ook een aantal uitzonderingen geformuleerd. Voor de overheid zijn vooral van belang de uitzonderingen omwille van wetgeving, van het uitoefenen van een taak van algemeen belang en van overheidsgezag, en ook omwille van 'archivering in het algemeen belang'.
De uitzonderingen zijn nooit absoluut. Er zijn altijd voorwaarden aan verbonden en er moet altijd ruimte zijn voor invulling en afweging van belangen in specifieke gevallen. Het is ook belangrijk te bedenken dat niet alle verwerkingen bij de overheid voortvloeien uit wetgeving, algemeen belang of overheidsgezag! In die gevallen gelden de uitzonderingen niet altijd.
De rechten én de uitzonderingen erop gelden voor informatie met persoonsgegevens vanaf de aanmaak daarvan. Immers, wanneer betrokkenen bij de archiefvormer verwijdering van hun gegevens kunnen eisen en verkrijgen, dan is er later geen informatie meer beschikbaar die omwille van 'archivering in het algemeen belang', historisch of wetenschappelijk belang bewaard had moeten blijven.
Persoonsgegevens in overheidsinformatie mogen net zo lang bewaard blijven als die overheidsinformatie zelf. Hoe lang overheidsinformatie bewaard dient te blijven, is vastgelegd in selectielijsten en die worden vastgesteld op basis van de Archiefwet. Zie hiervoor hoofdstuk 3 in dit deel. Persoonsgegevens van natuurlijke personen verdienen in elk geval gedurende de bewaartermijn bescherming, of die nu lang of kort is. Zie hiervoor hoofdstuk 2 in dit deel. Hieronder wordt per recht van betrokkenen uit de AVG toegelicht welke rechten en uitzonderingen er zijn die relevant zijn voor de overheid.

5.1 Het recht op informatie

De AVG verplicht de verwerkingsverantwoordelijke annex archiefvormer om de betrokkenen te informeren over de verwerking van persoonsgegevens over hem/haar en in welke details (artikelen 13 en 14). Zij moeten onder meer worden geïnformeerd over de periode dat hun persoonsgegevens zullen worden bewaard.

Er is verschil tussen verwerkingen waarbij de informatie van de betrokkene zelf komt, zoals bij het invullen van een formulier, en informatie die niet van de betrokkene komt.

Een verantwoordelijke overheid kan, als het gaat om informatie die van de burger zelf is verkregen, algemene informatie geven over de verwerking in het kader van de Archiefwet. Dit kan worden opgenomen in het privacystatement, in een informatiebrochure of een

mededeling op de website, in de trant van 'uw gegevens worden tevens verwerkt in het kader van de Archiefwet. Dit kan ook betekenen dat ze blijvend worden bewaard…'

In het geval dat de informatie niet van de persoon zelf komt, zijn er uitzonderingen op deze verplichting, namelijk:

- indien het informeren onmogelijk blijkt
- indien het onevenredig veel inspanning zou vergen en/of de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig te belemmeren, in het bijzonder met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden (AVG art. 14 lid 5)

Ook archivering is een verwerking. Wanneer persoonsgegevens (verder) worden verwerkt vanwege 'archivering in het algemeen belang', geldt de terinzagelegging van de selectielijsten als een adequate praktijk om de betrokken personen te informeren over de verwerkingen van hun gegevens. De selectielijst – met bijbehorende mogelijkheid tot het indienen van zienswijze en beroep – informeert de burger voldoende over de persoonsgegevens die worden bewaard op basis van de Archiefwet en de duur van deze bewaring.[48] Het zou onevenredig veel inspanning betekenen wanneer elke burger geïnformeerd zou moeten worden over archivering van zijn persoonsgegevens.

5.2 Het recht op inzage

De betrokkene kan op grond van AVG artikel 15 bij de archiefvormer annex verwerkingsverantwoordelijke vragen om:

- informatie over de vraag of persoonsgegevens over hem/haar worden verwerkt
- inzage in deze verwerkte persoonsgegevens
- informatie over de verwerking. Dit houdt onder meer in:
    - de periode waarin de gegevens worden bewaard
    - de bijbehorende rechten van de betrokkene
    - informatie over doorgifte van de gegevens aan andere landen of internationale organisaties

Het recht op inzage geldt voor alle informatie met persoonsgegevens vóór vernietiging of overbrenging. Het recht is niet van toepassing op bij de wet ingestelde openbare registers, als voor die registers een aparte procedure voor de verwerking van gegevens is geregeld (UAVG, artikel 47).
Het recht op inzage van persoonsgegevens over de betrokken burger geldt niet onverkort voor archieven die naar een archiefbewaarplaats zijn overgebracht.[49]

[48] Zie de Memorie van Toelichting op de Wet bescherming persoonsgegevens (Wbp). Deze is weliswaar ingetrokken, toch kan worden aangesloten bij de praktijk onder de Wbp: https://zoek.officielebekendmakingen.nl/kst-25892-3.html

[49] Zie: UAVG, artikel 45 lid 2: Betrokkene heeft het recht om inzage te verkrijgen in de archiefbescheiden, tenzij verzoeken om inzage zodanig ongericht zijn dat deze in redelijkheid niet kunnen worden ingewilligd. Overigens zijn naar een archiefbewaarplaats overgebrachte archieven in principe openbaar toegankelijk en kosteloos aadpleegbaar, met uitzonderingen onder meer vanwege de privacy (Archiefwet, artikelen 14 t/m 17).

5.3 Het recht op rectificatie

Het recht op rectificatie kan worden toegepast op informatie bij de archiefvormer, dus voorafgaand aan vernietiging of overbrenging naar een archiefbewaarplaats. Het recht geldt volgens AVG artikel 16 voor rectificatie van onjuiste of onvolledige feitelijke en objectieve gegevens die over de betrokkene zelf gaan. Op grond van artikel 19 moeten derden, die eerder de onjuiste persoonsgegevens hebben ontvangen, van de rectificatie op de hoogte worden gesteld, tenzij dit onevenredige inspanning vergt.

De Nederlandse Uitvoeringswet AVG geeft een aantal uitzonderingen op het recht op rectificatie. Wanneer persoonsgegevens door instellingen of diensten uitsluitend voor wetenschappelijk onderzoek of statistiek worden verwerkt, hoeft rectificatie niet toegepast te worden, en evenmin geldt het voor 'bij de wet ingestelde openbare registers', die al eigen procedures kennen voor aanpassing van persoonsgegevens. Ook is het recht op rectificatie niet van toepassing als het gaat om 'archivering in het algemeen belang', maar de UAVG beperkt dit tot archieven na overbrenging naar een archiefbewaarplaats. Het recht op rectificatie is dus wel van toepassing bij informatie die uiteindelijk wordt vernietigd of vóór overbrenging. Na overbrenging kan de betrokkene alleen zijn/haar eigen lezing aan de volgens hem/haar onjuiste persoonsgegevens toevoegen, de gegevens zelf worden niet gewijzigd (UAVG artikelen 44, 45 en 47).

5.4 Het recht op bezwaar

Burgers hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens, zelfs als dat door de overheid gebeurt in het kader van een publieke taak. Ook op dit recht zijn uitzonderingen geformuleerd, bijvoorbeeld wanneer de openbare veiligheid, de landsverdediging of de opsporing van strafbare feiten in het geding is.[50] De specifieke belangen van de bezwaarde moeten altijd worden afgewogen tegen het algemene belang. Dit geldt ook wanneer bezwaar gemaakt wordt tegen archivering van de gegevens.

5.5 Het recht op beperking van de verwerking

De betrokkene kan ook beperking van de verwerking vragen, bijvoorbeeld als gegevens onjuist zijn, wanneer hij of zij betwist of de verwerking rechtmatig is en/of gedurende de tijd dat zijn bezwaar nog loopt (AVG artikel 18).

5.6 Het recht op vergetelheid

Het recht op vergetelheid betekent het op verzoek van de betrokkene voorgoed wissen van zijn/haar persoonsgegevens. Dit recht geldt niet in twee situaties die relevant zijn voor uitvoering bij de overheid:[51]

[50] Recht op bezwaar: AVG artikel 21, uitzonderingen daarop: AVG artikel 23 en UAVG artikel 41.
[51] Zie AVG artikel 17 derde lid, met name onder b en d

1. Als een organisatie gegevens verwerkt in het kader van een wettelijke verplichting, een taak van algemeen belang, overheidsgezag of een andere rechtmatige grondslag die de AVG in artikel 6 noemt. Zolang wettelijke bewaartermijnen nog niet zijn verlopen – uit de selectielijst[52] en uit diverse wetten – geldt het recht op vergetelheid in principe niet. De uitzondering geldt niet alleen voor blijvend te bewaren informatie, maar ook voor uiteindelijk te vernietigen informatie. Voorwaarde is wel dat de persoonsgegevens waar het om gaat, noodzakelijk zijn om de doelen van de bewaring te verwezenlijken. Wanneer de gegevens niet rechtmatig zijn verzameld en bewerkt, of de gegevens niet nodig zijn voor dat bewuste doel, geldt de uitzondering niet.

Voorbeelden: het BSN is onterecht gebruikt bij een taak waar dat niet wettelijk is voorgeschreven; geboortedata zijn verwerkt waar dat niet strikt nodig is voor die taak; gegevens zijn langer bewaard dan de selectielijst toelaat. In die gevallen moeten de desbetreffende persoonsgegevens op verzoek van de burger over wie de gegevens gaan, worden verwijderd.

2. Als informatie in een selectielijst is aangemerkt als blijvend te bewaren. Hierbij stelt de AVG wel een voorwaarde om niet in te gaan op een verzoek: het vernietigen van de gegevens dreigt het doel van het bewaren onmogelijk te maken of ernstig te verhinderen (artikel17.3d). Alleen dan is vernietigen niet toegestaan.
De doelen waarvoor informatie blijvend worden bewaard, zijn eerder in deze handreiking

Voorbeelden: wanneer van dossiers een aselecte steekproef is bewaard, kan een dossier op verzoek van een betrokkene eventueel worden vernietigd. Dit zal namelijk meestal niet het doel van de bewaring 'in ernstige mate verhinderen', zoals de AVG in artikel 89.3 stelt. Wanneer het gaat om een specifiek dossier dat juist wordt bewaard om een bepaalde reden – zoals: de zaak was spraakmakend – wordt dat lastiger. De zaak als zodanig is in dat geval van maatschappelijk en historisch belang.

geformuleerd als: geheugen van de overheid, publieke verantwoording en maatschappelijk geheugen, bewijs en rechtsvinding, zie in dit deel paragraaf 1.1. Als de gegevens die iemand wil laten vernietigen, nodig zijn om deze doelen te bereiken, moeten we ervan uitgaan dat vernietigen geen optie is, want strijdig met de Archiefwet.

[52] Hierbij speelt weer de vraag of in de desbetreffende selectielijst wel voldoende rekening is gehouden met de bescherming van persoonsgegevens. Zo niet, dan zal de selectielijst geactualiseerd moeten worden.

Wanneer iemand in genoemde twee gevallen aan een overheid verzoekt persoonsgegevens over hem/haar te vernietigen, kan dit verzoek dus niet zonder meer worden afgewezen. De belangen moeten in ieder specifiek geval goed tegen elkaar worden afgewogen. Al met al is de toepasbaarheid van het recht op vergetelheid op overheidsinformatie dus beperkt, maar niet onmogelijk.

5.7 Het recht op overdraagbaarheid van gegevens

In artikel 20 van de AVG is het recht neergelegd van betrokkenen om hun gegevens over te dragen van de ene naar de andere verwerkingsverantwoordelijke, indien technisch mogelijk direct van de ene naar de andere.

Dit recht geldt niet voor persoonsgegevens die worden verwerkt in het kader van een taak van algemeen belang of de uitoefening van openbaar gezag (artikel 20 lid 3). Dit overdragen van gegevens zal bij de overheid dus niet vaak voorkomen. Dit recht is meer toepasselijk bij verwerking van persoonsgegevens door bedrijven waar men klant is, om overstappen mogelijk te maken. Krachtens UAVG artikel 45 geldt de overdraagbaarheid in elk geval niet voor archieven die naar een archiefbewaarplaats zijn overgebracht.

5.8 Geautomatiseerde individuele besluitvorming, waaronder profilering

De overheid gebruikt vele informatiesystemen met gegevens van burgers, en mag daar geen misbruik van maken. Een burger heeft het recht om niet te zijn onderworpen aan besluiten van de overheid die hem aanzienlijk treffen en die uitsluitend op geautomatiseerde verwerking gebaseerd zijn. Met andere woorden: daar moet ook menselijk handelen aan te pas komen. Dit recht uit artikel 22 van de AVG geldt voor persoonsgegevens in alle informatiesystemen, en betrokkenen kunnen er dus ook bij de overheid een beroep op doen. Er zijn uitzonderingen wanneer het gaat om een wettelijke verplichting of een taak van algemeen belang. In dat geval moet de verwerkingsverantwoordelijke wel altijd ‘passende maatregelen’ nemen om de rechten en vrijheden van de betrokkene te beschermen (UAVG artikel 40).[53]

5.9 Houd altijd rekening met rechten van betrokkenen

In dit hoofdstuk zijn een aantal uitzonderingen beschreven op de rechten van personen met betrekking tot gegevens die de overheid over hen heeft. Dat laat onverlet dat een betrokken altijd een verzoek kan indienen op basis van deze rechten. De verantwoordelijke overheid zal dan steeds moeten afwegen of het belang van de verzoeker opweegt tegen andere te beschermen maatschappelijke belangen, zoals dat van geheugen van de samenleving, verantwoording door de overheid en historie.
Ook het vormgeven van de behandeling van verzoeken van burgers is onderdeel van de

[53] Zie ook de uitspraak van de rechtbank Den Haag van 5-2-2020 in de SyRi zaak: de overheid handelde hier in strijd met het privacy-artikel 8 van het Europees Verdrag voor de Rechten van de Mens, omdat bij het vastleggen van persoonsgegevens in combinatie met een algoritme burgers ‘bij voorbaat verdacht’ waren: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865

uitvoering van de AVG. Daarbij is samenwerking tussen FG's en privacyfunctionarissen enerzijds en informatiemanagers en -beheerders/DIV-ers anderzijds onontbeerlijk. Zeker als het gaat om informatie die op grond van een selectielijst voor blijvende bewaring in aanmerking komt, is het raadzaam om ook de archivaris te raadplegen. Het is belangrijk om hiervoor verantwoordelijke contactpersonen aan te wijzen en procedures in te richten. Daarnaast is het aan te bevelen om overlegvormen in het leven te roepen of bestaande vormen te gebruiken om onderling tips, ervaringen en **best practices** uit te wisselen.

'Weten of vergeten' is geen wiskunde, geen geval is hetzelfde en in elk individueel geval zullen belangen afgewogen moeten worden. Daarom is het belangrijk om kennis en ervaringen op te doen en te blijven delen. We hopen met deze handreiking daaraan te kunnen bijdragen.

6 Begrippen

archiefbescheiden (Bron: Archiefwet 1995, artikel 1c)
Bescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten.

archiefvormer (Bron: Archiefterminologie voor Nederland en Vlaanderen)
Persoon, groep personen of organisatie die zelfstandige archiefvorming als een van zijn of haar activiteiten heeft**.**

archiefvorming (Bron: Archiefterminologie voor Nederland en Vlaanderen)
Geheel van procedures en handelingen waarbij archiefbescheiden tot stand komen en in een archief worden opgenomen.

betrokkene (Bron: AVG, artikel 4)
De geïdentificeerde of identificeerbare natuurlijke persoon, van wie gegevens worden verwerkt.

data (Bron: NORA 3.0, Principes voor samenwerking en dienstverlening)
Zie: Gegeven. Het meervoud van digitale gegevens.

dataminimalisatie (Bron: AVG, artikel 5)
Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking).

document (Bron: Archiefterminologie voor Nederland en Vlaanderen)
Geheel van samenhangende gegevens, vastgelegd op een of meer gegevensdragers;
een logisch geheel van documenten die gaan over dezelfde zaak.

(Bron: Wet openbaarheid van bestuur, artikel 1)
Een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat.

(Bron: Conceptwetsvoorstel Archiefwet, november 2019, artikel 1.1)
Schriftelijk stuk of ander geheel van vastgelegde gegevens dat:
a. door een overheidsorgaan is opgemaakt of ontvangen, dat naar zijn aard verband houdt met de publieke taak van dat overheidsorgaan en is bestemd om onder dat overheidsorgaan te berusten;
b. is opgemaakt of ontvangen door instellingen of personen, waarvan de rechten of functies op een overheidsorgaan zijn overgegaan;
c. door een niet-overheidsorgaan is opgemaakt of ontvangen en voor blijvende bewaring is opgenomen door het Nationaal Archief of een decentrale archiefdienst.

doelbinding (Bron: AVG, artikel 5)
Persoonsgegevens mogen alleen op grond van een welomschreven en gerechtvaardigd doel worden verwerkt. Ze mogen niet verder voor een ander doel dat onverenigbaar is met het oorspronkelijke doel worden verwerkt, dus niet langer bewaard dan nodig voor het doel. Archivering in het algemeen belang noemt artikel 5 AVG als 'niet onverenigbaar met het oorspronkelijke doel'.

dossier (Bron: Archiefterminologie voor Nederland en Vlaanderen)
Een logisch geheel van documenten die gaan over dezelfde zaak.

gegeven (Bron: NORA 3.0, Principes voor samenwerking en dienstverlening)
De weergave van een feit, begrip of aanwijzing, geschikt voor overdracht, interpretatie of verwerking door een persoon of apparaat. Synoniem meervoud: data (gegevens).

informatie (Bron: NORA 3.0, Principes voor samenwerking en dienstverlening, NEN-ISO 9000)
Betekenisvolle gegevens. In deze handreiking wordt 'informatie' gebruikt als een containerbegrip dat alle typen betekenisvolle informatie op alle mogelijke dragers kan betekenen, bijvoorbeeld: geluidsfragmenten, foto/film, tekstdocumenten, waarden in databases, algoritmes of log-gegevens.

informatieobject (Bron: NORA 3.0, Principes voor samenwerking en dienstverlening)
Een op zichzelf staand geheel van gegevens met een eigen identiteit. Bijvoorbeeld: document, databasegegeven, e-mailbericht (met bijlagen), (zaak) dossier, internetsite (of een deel ervan), foto/afbeelding, geluidsopname, wiki, blog et cetera.

persoonsgegevens: (Bron: AVG, artikel 4.1)
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd. Voorbeelden: naam, adres, woonplaats, telefoonnummer, geboorteplaats, geboortedatum et cetera.

schonen (Bron: selectielijst gemeenten en intergemeentelijke organen 2017)
De archiefbescheiden die niet van wezenlijk belang zijn voor reconstructie van de zaak mogen worden verwijderd c.q. opgeschoond.

vernietigen (Bron: NEN ISO 15489)
Proces van verwijderen of wissen van archiefbescheiden zonder dat zij weer gereconstrueerd kunnen worden.

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

verwerkingsverantwoordelijke (Bron: AVG, art. 4)
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 verwerking van persoonsgegevens vaststelt.

zaak (Bron: Archiefterminologie voor Nederland en Vlaanderen)
Een in de tijd begrensd complex van handelingen betreffende een bepaald geval.

zorgdrager (Bron: Archiefwet, artikel 1d)
Degene die bij of krachtens de wet belast is met de zorg voor de archiefbescheiden.

Samenstelling werkgroep

De subwerkgroep Informatiemanagement van de werkgroep AVG wordt gevormd door vertegenwoordigers van:

- Inspectie Overheidsinformatie en Erfgoed
- Tweede Kamer der Staten-Generaal
- Rijkswaterstaat
- KVAN/BRAIN, beroeps- en brancheverenigingen voor het archiefwezen
- Gemeente Amsterdam
- Gemeentearchief Rotterdam
- Haags Gemeentearchief