Omgevingsdienst regio Utrecht

# BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 580

2 juni 2022

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst regio Utrecht

## Privacybeleleid Omgevingsdienst regio Utrecht 2020

### Hoofdstuk 1 Documenthistorie en goedkeuring

#### Paragraaf 1.1 Documenthistorie

| Versie | Datum | Gewijzigd door | Aard van de wijziging |
|---|---|---|---|
| 0.1 | 08-12-2017 | Dennis Baaten | Eerste opzet |
| 0.2 | 12-12-2017 | Dennis Baaten | Verwerken feedback Phylicia Dest |
| 0.3 | 11-01-2018 | Dennis Baaten | Toevoegen doelbinding bij eisen overeenkomst. Verwerken van impact concept wetsvoorstel Uitvoeringswet AVG op "bijzondere persoonsgegevens". Aanscherpen rechten betrokkenen, encryptie, verwerker |
| 0.4 | 23-01-2018 | Dennis Baaten | Aanscherpen privacy by design en privacy by default. Toevoegen toelichting op gebruik testdata. Aanscherpen DPIA. |
| 0.5 | 24-01-2018 | Dennis Baaten | Tekstuele aanscherping DPIA criteria in hoofdstuk 8.1. |
| 0.6 | 01-02-2018 | Dennis Baaten | Aanscherpen/toevoegen hoofdstuk 9.1 en 9.2 inzake bepalen verwerkerschap. |
| 0.7 | 08-02-2018 | Dennis Baaten | Aanscherpen boetes in hoofdstuk 13. |
| 0.8 | 08-03-2018 | Dennis Baaten | Toevoegen 9.1.2. Toevoegen 9.2.1 n.a.v. afstemming met juristen ODRU. |
| 0.9 | 15-5-2020 | Roseanne de Kloe | Uitgebreide review. Grootste wijzigingen:<br>1. Doel en scope<br>2. Expliciet aangegeven per AVG eis hoe dit geborgd wordt bij de ODRU<br>3. Concrete uitwerking van de algemene beginselen<br>4. Onderscheid tussen gegevensverwerkingen van inwoners en bedrijven<br>5. Uitwerking van de technische en organisatorische maatregelen onder de AVG • Toevoeging van de eisen die de Wet Politie Gegevens (Wpg) stelt boven de AVG |
| 0.10 | 19-5-2020 | Babette BehrensBenne | Review en goedkeuring FG |
| 0.11 | 01-12-2020 | Babette BehrensBenne | Aanpassingen aan instemmingsbrief Ondernemingsraad INT20.1011/3794 |

#### Paragraaf 1.2 Goedkeuring

Voorliggend document is een onderdeel van de gegevensbescherming van de Omgevingsdienst regio Utrecht (ODRU) en is vastgesteld in de vergadering van het dagelijks bestuur d.d. 10 september 2020 bij besluit.

### Hoofdstuk 1 Inleiding

#### Paragraaf 1.1 Achtergrond

De Omgevingsdienst regio Utrecht (ODRU) ondersteunt vijftien gemeenten en andere overheden in de regio Midden-Nederland bij de uitvoering van milieu- en omgevingstaken. Dat doen we met een breed scala aan producten en diensten op het terrein van o.a. bodem, bouw- en woningtoezicht, vergunningen en meldingen, geluid en lucht, klimaat, energie en duurzaamheid, natuur- en milieueducatie, ruimtelijke ordening en toezicht en handhaving. We combineren een klantgerichte, ondernemende werkwijze met vakinhoudelijke expertise en inzicht in het politiek-bestuurlijke speelveld.

#### Paragraaf 1.2 Het belang van privacy

Om haar interne bedrijfsprocessen en gemandateerde milieu- en omgevingstaken uit te kunnen voeren, verwerkt de ODRU persoonsgegevens. Het gaat om persoonsgegevens van en over opdrachtgevers (gemeenten), inwoners, bedrijven, leveranciers en (interne en externe) medewerkers. De ODRU verwerkt deze persoonsgegevens nu nog zowel analoog als digitaal, maar zal deze steeds meer digitaal gaan verwerken.
Privacy is een belangrijk onderdeel van de reguliere bedrijfsprocessen binnen de organisatie en als onderdeel van de dienstverlening aan haar opdrachtgevers (gemeenten). Het is van het grootste belang dat zorgvuldig met deze vertrouwelijke persoonsgegevens wordt omgegaan en dat de privacy gewaarborgd wordt. Inbreuken op de privacy kunnen namelijk schade aanrichten aan de ODRU, gemeenten of diegene van wie de gegevens zijn. Bij schade kan het gaan om onderbreking van de werkzaamheden,

imagoschade, financiële schade en schadeclaims. Ook gaat het om nadelige gevolgen voor personen van wie de gegevens gelekt zijn, zoals imagoschade, stigmatisering en discriminatie. Hoofdstuk 13 gaat dieper in op de risico's als gevolg van privacy inbreuken.

**Paragraaf 1.3 Geldende privacy wet- en regelgeving**

Het privacybeleid is opgesteld in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene verordening gegevensbescherming en overige relevante wet- en regelgeving.

De AVG [1], vervangt de oude Nederlandse Wet bescherming persoonsgegevens (Wbp). De AVG is op 25 mei 2018 van kracht gegaan. Sinds die datum geldt in de hele Europese Unie (EU) dezelfde privacywetgeving. De AVG wordt gehandhaafd door de Nederlandse toezichthouder: de Autoriteit Persoonsgegevens (AP). Organisaties die niet voldoen aan de wet lopen risico's (zie hoofdstuk 13), zoals het riskeren hoge boetes vanuit de AP.
De AVG laat ruimte aan lidstaten om een (strenger) beleid ten aanzien van privacy te voeren. Binnen Nederland gebeurt dit met de nationale wet Uitvoeringswet AVG (UAVG) [2]. Deze nationale wet geeft invulling aan elementen waarover de Europese lidstaten geen consensus konden bereiken in de AVG, en aan zaken die op Europees niveau niet zijn benoemd. Denk bijvoorbeeld aan het BSN-nummer dat binnen Nederland wordt gezien als een identificatienummer dat een bijzondere bescherming toekomt.

Daarnaast bestaat er jurisprudentie ten aanzien van onderwerpen in de AVG. [3] Gedurende de komende jaren zullen rechters steeds vaker bepalen hoe bepaalde zaken uit de AVG het beste geïnterpreteerd en geïmplementeerd kunnen worden. Het beschikbaar komen van jurisprudentie kan wijzigingen in dit beleidsdocument tot gevolg hebben.
De verwerking van persoonsgegevens door boa's viel tot 25 mei 2018 onder de Wet bescherming persoonsgegevens (Wbp). Door de komst van de AVG valt de verwerking van persoonsgegevens rondom strafbare feiten onder een andere Europese wet, namelijk EU-Richtlijn 2016/680. Deze richtlijn is omgezet in de Wet politiegegevens (Wpg) [4], aangevuld met het Bpg (Besluit politiegegevens) [5], en is sinds 1 januari 2019 van kracht. Organisaties die aan de AVG voldoen, voldoen voor het grootste gedeelte aan de Wpg. Hoofdstuk 12 beschrijft de aanvullende maatregelen die door de Wbp vereist worden

**Paragraaf 2.4 Doel van het privacybeleid**

**Artikel**
Het privacybeleid stelt algemene regels op, die betrekking hebben op de manier hoe de ODRU dagelijks omgaat met persoonsgegevens en de privacy van haar medewerkers, bedrijven, inwoners en opdrachtgevers (gemeenten), en wat er wettelijk wel en niet verantwoord is. Het beleid is kaderstellend en wordt aangevuld met beleidsdocumenten en procedures voor privacy op tactisch niveau en werkinstructies op operationeel niveau. Deze documenten zijn terug te vinden in het Privacy Management Systeem op de T:schijf en/of op intranet.

Het primaire doel van het beleid is het minimaliseren van de schade door het voorkomen van datalekken en het minimaliseren van de eventuele gevolgen. Bij schade kan het o.a. gaan om financiële schade, imagoschade, schadeclaims door het niet nakomen van contractuele afspraken en schade voor de privacy voor de betrokkene(n). Deze schade kan betrekking hebben op de ODRU, haar medewerkers, de inwoners, bedrijven, opdrachtgevers of andere betrokkene(n).
Het secundaire doel van het privacybeleid is dat de ODRU voldoet aan de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene verordening gegevensbescherming en overige relevante wet- en regelgeving.

Hoofdstuk 13 beschrijft de risico's wanneer niet voldaan wordt aan de privacydoelstellingen.

**Paragraaf 1.5 Doelgroep en reikwijdte**

Het privacybeleid is van toepassing op alle medewerkers binnen de organisatie en externen die in opdracht van de ODRU een rol vervullen.

1 ) De Europese Algemene Verorderdening Gegevensbescherming (EU-AVG) is hier te raadplegen: https://www.privacyregulation.eu/nl/index.htm
2 ) Uitvoeringswet AVG (AVG) is hier te raadplegen: https://wetten.overheid.nl/BWBR0040940/2018-05-25
3 ) Overzicht met jurisprudentie over de AVG staat op: https://www.recht.nl/nieuws/privacyrecht/173108/kroniek-avg-rechtspraak-juni2018-mei-2019/
4 ) Wet politiegegevens (Wpg) is te raadplegen op: https://wetten.overheid.nl/BWBR0022463/2020-01-01
5 ) Besluit politiegegevens (Bpg) is te raadplegen op: https://wetten.overheid.nl/BWBR0023086/2020-01-01

Het beleid dient te worden toegepast op alle persoonsgegevens (zowel op papier als digitaal), bedrijfsmiddelen die persoonsgegevens bevatten en informatiesystemen die persoonsgegevens verwerken. Daarnaast is het van toepassing op leveranciers die een rol vervullen in onze informatievoorziening. Indirect is de uitwerking van het beleid van invloed op de relatie met partners, klanten en derden.

Het beleid is locatieonafhankelijk. Medewerkers, gedetacheerden en anderen die direct of indirect werkzaam zijn voor de ODRU dienen zich zowel op locaties van de ODRU als daarbuiten aan het beleid te houden.

### Paragraaf 1.6 Eindverantwoordelijkheid

Gelet op de mogelijke impact van inbreuken op de privacy voor de ODRU berust de eindverantwoordelijkheid voor privacy bij de directie van de Omgevingsdienst regio Utrecht.
Hoofdstuk 3 beschrijft de gedelegeerde taken en verantwoordelijkheden op het gebied van privacy.

### Paragraaf 1.7 Evaluatie document

De adviseur informatiebeveiliging en privacy evalueert het privacybeleid minimaal jaarlijks en/of bij grote wijzigingen. Indien noodzakelijk wordt het document bijgesteld. De bevindingen worden gerapporteerd aan de FG, Hoofd Bedrijfsbureau, de directeur en het Dagelijks Bestuur.

### Paragraaf 1.8 Beschikbaarheid document

De adviseur Informatiebeveiliging en Privacy waarborgt dat zowel alle (ingehuurde) medewerkers, dan wel externe partijen die een rol spelen op het gebied van privacy, dit beleid kennen. Het beleid is daarom beschikbaar gesteld in het Privacy Management System op de T:schijf en op intranet. Ook wordt het gecommuniceerd naar relevante externe partijen.

## Hoofdstuk 2 Definities en begrippen

In dit document, maar ook in verschillende wetteksten worden specifieke termen en begrippen gebruikt. In dit hoofdstuk worden deze toegelicht.

**AVG**: de Europese privacywet 'Algemene Verordening Gegevensbescherming' (AVG) is sinds 25 mei 2018 van kracht voor alle lidstaten van de Europese Unie. Deze wet wordt in het Engels ook wel General Data Protection Regulation (GDPR) genoemd.

**Autoriteit Persoonsgegevens (AP)**: de toezichthouder die als taak heeft toe te zien op de verwerking van persoonlijke gegevens krachtens de AVG.

**Baseline Informatiebeveiliging Overheid (BIO)**: [6] De BIO is het gezamenlijk normenkader voor informatiebeveiliging binnen alle overheidsorganisaties. Het normenkader is gebaseerd op de ISO 27002. De BIO vervangt de voorgaande normen (BIWA, BIG, BIR en IBI).

**Betrokkene**: diegene op wie een persoonsgegeven betrekking heeft.

**Beveiliging**: Het samenhangend stelsel van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

**Bijzondere persoonsgegevens**: persoonsgegevens die naar hun aard vertrouwelijker zijn dan 'gewone' persoonsgegevens en verwerking ervan geschiedt op andere gronden dan 'gewone' persoonsgegevens. Het vertrekpunt is dat verwerking van deze categorieën van gegevens verboden is, tenzij aan een aantal voorwaarden is voldaan zoals genoemd in de AVG of de uitvoeringswet.

**Derde**: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.

6 ) De Baseline Informatiebeveiliging Overheid kan geraadpleegd worden via:
https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

**Functionaris voor de Gegevensbescherming (FG)**: De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG) binnen de ODRU.

**Identificeerbare gegevens**: gegevens die zonder onevenredige tijd en moeite aan de betrokkene zijn te koppelen.

**Persoonsgegevens**: dit betreft alle informatie waarmee een natuurlijk persoon direct of indirect kan worden geïdentificeerd. Gegevens waarmee direct kan worden geïdentificeerd zijn identificatoren zoals een naam, identificatienummer en locatiegegevens. Gegevens die mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, en ok gegevens die in combinatie met andere gegevens leiden tot identificeerbaarheid, dienen ook te worden beschouwd als persoonsgegevens. Voorbeelden zijn gegevens over: inkomen, vermogen, beroep, woonplaats en leeftijd.

**Uitvoeringswet AVG**: dit is de Nederlandse nationale wet waarin Nederland invulling geeft aan zaken die op Europees niveau niet zijn benoemd in de AVG.

**Verwerker**: een Verwerker verwerkt persoonsgegevens in opdracht van of ten behoeve van een verwerkingsverantwoordelijke.

**Verwerkingsverantwoordelijke**: een verwerkingsverantwoordelijke is verantwoordelijk voor de verwerking(en) van persoonsgegevens, ook wanneer er sprake is van verwerking door derden. De verwerkingsverantwoordelijke bepaalt zelf het doel van en de middelen voor de verwerking.

**Verwerkersovereenkomst**: wanneer verwerking van persoonsgegevens wordt uitbesteed of wanneer er persoonsgegevens van een andere partij worden verwerkt, moeten er afspraken worden gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Deze afspraken dienen te worden vastgelegd in een zogenaamde verwerkersovereenkomst.

**Verwerkingsregister**: dit is een vanuit de AVG verplicht register wat door organisaties wordt bijgehouden en waarin is vastgelegd wat voor persoonsgegevens zij opslaan of verwerken, van wie deze persoonsgegevens zijn, waar dit wordt opgeslagen en hoe dit is beveiligd.

**Wet Politiegegevens (Wpg)**: deze wet regelt de verwerking van politiegegevens, i.c. elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt; hieronder valt bijvoorbeeld het verzamelen, wijzigen, raadplegen, verstrekken, afschermen of vernietigen van politiegegevens.

## Hoofdstuk 3 Privacy organisatie

### Paragraaf 3.1 Interne taken en verantwoordelijkheden

Binnen de ODRU zijn de taken en verantwoordelijkheden met betrekking tot privacy als volgt vastgesteld. Deze zijn ook opgenomen in de functieprofielen van de betreffende medewerkers[7].

| | |
|---|---|
| Algemeen Bestuur | Het Algemeen bestuur oefent de controlefunctie uit en kan vanuit die rol controleren of de privacyregels en het privacybeleid worden nageleefd. |
| Dagelijks Bestuur | Bestuurlijk verantwoordelijk voor het naleven van de privacyregels en het privacybeleid. Het dagelijks bestuur stelt het privacybeleid van de ODRU vast. Tenminste een keer per jaar is privacy een agendapunt in de vergadering van het Dagelijks Bestuur. |
| Directie | De directeur is ambtelijk eindverantwoordelijk voor de verwerking van persoonsgegevens binnen de ODRU. Hij draagt zorg dat de organisatie voldoet en blijft voldoen aan de privacyregels en het privacybeleid en draagt zorg voor periodieke evaluatie. De directeur is het aanspreekpunt voor de FG |
| Hoofd Bedrijfsbureau | Het Hoofd Bedrijfsbureau heeft o.a. privacy, informatiebeveiliging, informatiebeheer en ICT in zijn portefeuille. Hij/zij is verantwoordelijk voor een betrouwbare informatievoorziening binnen de ODRU. Hij is verantwoordelijk dat het privacybeleid, de AVG vereisten en de beveiligingsmaatregelen binnen de ODRU geïmplementeerd zijn. Hij legt over privacy verantwoording af aan de directie en in het MT. |
| Afdelingshoofden | De afdelingshoofden zijn verantwoordelijk voor de verwerking van persoonsgegevens overeenkomstig de AVG en het privacybeleid binnen hun afdeling |
| Clustercoördinatoren | Clustercoördinatoren zien toe op het naleven van de privacyregels en het privacybeleid binnen de afdeling. Dit impliceert o.a. de volgende taken: |

7 .)Bron: Personeelshandboek Omgevingsdienst regio Utrecht, vastgesteld op 3 december 2019.

| | |
|---|---|
| | • Bijdragen aan de bewustwording van het belang van gegevensbescherming bij medewerkers onder meer door privacy periodiek tijdens het clusteroverleg aan de orde te stellen;<br>• Signaleren van risico's, zwakke plekken in de beveiliging;<br>• Zorg dragen voor bescherming digitale personele gegevens; Zorg dragen voor de juiste autorisatie medewerkers t.b.v. toegang tot systemen;<br>• Melden van nieuwe verwerkingen bij de adviseur informatiebeveiliging en privacy voordat met de nieuwe verwerking wordt gestart.<br>• Laten beoordelen van de verwerkersovereenkomst door de adviseur informatiebeveiliging en privacy. |
| Systeemeigenaren | De systeemeigenaren dragen zorg voor de passende beveiligingsmaatregelen en signaleren beveiligingsrisico's met betrekking tot de betreffende systemen. |
| Functionaris voor de Gegevensbescherming | De Functionaris voor de Gegevensbescherming (FG) houdt binnen de ODRU toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Zie voor een uitgebreide beschrijving paragraaf 3.2 |
| Adviseur Informatiebeveiliging en Privacy | De Adviseur Informatiebeveiliging en Privacy maakt onderdeel uit van het Cluster Informatiemanagement, Privacy en Informatiebeveiliging. Hij/zij is verantwoordelijk dat de organisatie voldoet aan de Basline Informatiebeveiliging Overheid en de AVG. Hij/zij stelt het privacybeleid (inclusief onderliggende procedures en werkinstructies) op en implementeert dit binnen de organisatie. Ook adviseert de adviseur over de te nemen maatregelen. De adviseur rapporteert over privacy aan de FG. |
| Medewerkers ODRU en externe medewerker [8] | Verantwoordelijk voor het bewust en veilig omgaan met persoonsgegevens. Dit doen zij in lijn met het privacybeleid en de bijbehorende procedures en werkinstructies. |

## Paragraaf 3.2 Functionaris voor de Gegevensbescherming

Een Functionaris voor de Gegevensbescherming (FG), ook wel Data Protection Officer (DPO) genoemd, houdt toezicht op de toepassing en naleving van de AVG binnen een organisatie. Het aanstellen van een FG is verplicht in drie gevallen:

1. Voor overheden en publieke organisaties;
2. Voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen/observeren;
3. Voor organisaties die vanuit hun kernactiviteit op grote schaal bijzondere persoonsgegevens verwerken.

Het hebben van een personeelsbestand voor bijvoorbeeld salarisverwerking of IT helpdesk doeleinden worden gezien als een 'ancillary function' (ondersteunende taak / nevenactiviteit) in plaats van een 'core activity' (kernactiviteit). Hierdoor is het hebben van een personeelsadministratie doorgaans geen argument om verplicht een FG aan te stellen.

De ODRU is verplicht tot het aanstellen van een FG, omdat zij een openbaar lichaam is, en daarmee een onderdeel van de Nederlandse overheid. De ODRU heeft haar FG aangemeld bij de AP.

Ten aanzien van een FG geldt het volgende:
- De wettelijke taken en bevoegdheden van de FG geven hem/haar een onafhankelijke positie in de organisatie;
- De FG moet een natuurlijk persoon zijn;
- De FG dient aangemeld te worden bij de Autoriteit Persoonsgegevens;
- De FG functie kan ook worden bekleed op basis van een dienstverleningsovereenkomst die werd afgesloten met een persoon of een organisatie die niet tot de organisatie van de verwerkingsverantwoordelijke / verwerker behoort;
- Organisaties mogen op vrijwillige basis een FG aanwijzen. Voor een vrijwillige FG gelden na aanstelling dezelfde rechten en plichten dan voor een verplichte FG;
- Een FG is niet persoonlijk verantwoordelijk bij niet-naleving van de AVG;
- Een FG geniet ontslagbescherming, vergelijkbaar met leden van de ondernemingsraad. Beëindiging van de arbeidsovereenkomst in relatie tot de uitvoering van specifieke FG taken, kan alleen middels de kantonrechter.

De ODRU draagt de FG de bij wet voorgeschreven taken op. De taken zijn in de functiebeschrijving vastgelegd.

8 ) Bron: Personeelshandboek Omgevingsdienst regio Utrecht, vastgesteld op 3 december 2019.

De ODRU zorgt ervoor dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De ODRU zorgt ervoor dat de FG zijn plichten en taken onafhankelijk vervult en geen instructies ontvangt met betrekking tot de uitoefening van de functie. Vanuit zijn onafhankelijke toezichthoudende functie dient de FG te beschikken over alle bevoegdheden die hem in staat stellen om zijn taken naar behoren uit te kunnen oefenen. De FG heeft bij twijfel of verschil van mening over de wijze waarop verwerkingen van persoonsgegevens dienen plaats te vinden de doorslaggevende stem.

De ODRU en de personen die bij een verwerking van persoonsgegevens zijn betrokken verstrekken desgevraagd de FG alle inlichtingen en verlenen alle overige medewerking die hij voor de uitoefening van zijn taak behoeft. Hiervoor heeft de FG toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt. Ook is de FG bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen. Hierdoor kan het zijn dat de FG toegang (nodig)
heeft tot dossiers, systemen en apparatuur waarin of waarmee persoonsgegevens worden verwerkt.

De FG brengt rechtstreeks verslag uit aan het MT, Dagelijks Bestuur en Algemeen Bestuur. Daarbij wordt hij ondersteund bij de vervulling van zijn taken en zorgen voor personeel, kantoren, uitrusting en alle andere middelen die nodig zijn voor de vervulling van diens plichten en taken.

### Paragraaf 3.3 Externe taken en verantwoordelijkheden

Het privacybeleid en geldende wet- en regelgeving gelden ook voor opdrachtgevers (gemeenten) en externe partijen waarmee de ODRU samenwerkt en informatie mee uitwisselt.
De ODRU borgt op onderstaande wijze dat taken en verantwoordelijkheden tussen de ODRU en externe samenwerkingspartners helder zijn:

- Tussen de ODRU en opdrachtgevers zijn samenwerkingsafspraken gemaakt. Privacy en informatiebeveiliging zijn hier integraal onderdeel van.

- Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoop Voorwaarden (AIV) van de ODRU, waarin onder meer geheimhouding en aansprakelijkheid is geregeld. In overeenkomsten die met derden worden afgesloten, wordt expliciet verwezen naar het privacy- en informatiebeveiligingsbeleid van de ODRU en de verplichting van het bedrijf om de ODRU op basis van minimaal hetzelfde beveiligingsniveau te helpen betrouwbare diensten te leveren. Ook sluit de ODRU met leveranciers, wanneer zij optreden als Verwerker van de persoonsgegevens, een Verwerkersovereenkomst af waarin de AVG vereisten en de beveiligingsmaatregelen worden afgedwongen. Hoofdstuk 7 gaat uitgebreid in op verwerkersovereenkomsten.

## Hoofdstuk 4 Verwerkingsbeginselen en rechtmatigheid

### Paragraaf 4.1 Algemene beginselen van het verwerken van persoonsgegevens

Alle verwerkingsprocessen die worden uitgevoerd door, binnen of namens de ODRU waarbij persoonsgegevens betrokken zijn, moeten aansluiten op de beginselen van de bescherming van persoonsgegevens die de AVG stelt. De ODRU neemt deze verwerkingsbeginselen in alle verwerkingsprocessen mee. Onderstaande sub paragrafen beschrijven deze algemene beginselen.

*4.1.1 Rechtmatigheid, behoorlijkheid en transparantie*
Persoonsgegevens moeten op een zodanige wijze verwerkt worden dat deze verwerking ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Volgens dit beginsel moeten alle verwerkingen van persoonsgegevens in de eerste plaats rechtmatig en behoorlijk zijn. Dit houdt in dat alle processen waarbij persoonsgegevens verwerkt worden in overeenstemming met de wet moeten zijn. Dit doelt zowel op de AVG zelf alsook op nationaal recht. In de tweede plaats moeten alle verwerkingen transparant zijn. Dit houdt vooral in dat de betrokkene zich van de verwerking bewust is. Processen waarbij persoonsgegevens op een onredelijke of onrechtmatige manier verwerkt worden, bijvoorbeeld indien de betrokkene niet over het verwerken geïnformeerd werd, zijn dus in principe in strijd met dit beginsel.

De ODRU treft de volgende maatregelen om te voldoen aan het beginsel van rechtmatigheid, behoorlijkheid en transparantie:

- Verwerkingsregister, zie voor meer informatie hoofdstuk 7;

- Uitvoeren van DPIA's, zie voor meer informatie hoofdstuk 10;

- Privacyverklaring op de ODRU website.

*4.1.2 Doelbinding*

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Het principe van doelbinding eist dat de doelen van het verwerken voorafgaand aan het verwerken specifiek vastgelegd zijn. Vooral mogen de doeleinden niet te vaag of te breed geformuleerd zijn, en mogen ze na het verzamelen niet meer gewijzigd worden.

Voor de ODRU geldt dat de kaders waarbinnen de doelstelling van de verwerking van persoonsgegevens dient te blijven, zijn:

- Het uitvoeren van de gemandateerde wettelijke taken op het gebied van milieu en omgeving;
- Ondersteuning van de bedrijfsvoering;
- Het aangaan en uitvoeren van arbeidsovereenkomsten met (ingehuurde) medewerkers; Het voldoen aan wettelijke verplichtingen.

*4.1.3 Minimale gegevensverwerking*

In de derde plaats vraagt het beginsel van minimale gegevensverwerking, dat gegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit beginsel houdt in essentie in dat persoonsgegevens alleen verwerkt mogen worden indien het noodzakelijk is dat zij verwerkt worden. Persoonsgegevens die niet noodzakelijk zijn mogen in beginsel niet verzameld worden. Indien een aantal verschillende verwerkingsprocessen uitgevoerd worden, is het beginsel van minimale gegevensverwerking op elke verwerking van toepassing.

Verder houdt het beginsel van minimale gegevensverwerking in, dat alleen medewerkers van de ODRU, die ter uitoefening van hun taken toegang tot bepaalde persoonsgegevens moeten hebben, deze categorieën persoonsgegevens kunnen inzien. Wanneer toegang tot persoonsgegevens niet noodzakelijk is, mag ook geen toegang mogelijk zijn.

De ODRU treft de volgende maatregelen om te voldoen aan het beginsel van dataminimalisatie:

- Verwerkingsregister, zie voor meer informatie hoofdstuk 7;
- Uitvoeren van DPIA's, zie voor meer informatie hoofdstuk 10;
- Kennis en bewustzijn onder de medewerkers over dataminimalisatie;
- Autorisatiebeleid; voor meer informatie hoofdstuk 10

*4.1.4 Juistheid*

Verder moeten gegevens in beginsel juist zijn en zo nodig geactualiseerd worden. Alle redelijke maatregelen moeten worden genomen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

Het beginsel van juistheid houdt vooral in dat alle gegevens over een persoon juist moeten zijn. Indien gegevens onjuist blijken te zijn, moeten deze gegevens zo snel mogelijk verbeterd of aangevuld worden. Dit geldt zowel voor gegevens die bij het verzamelen van gegevens al onjuist waren alsook indien de feitelijke situatie verandert en gegevens daardoor aangepast moeten worden.

De ODRU treft de volgende maatregelen om te voldoen aan het beginsel van juistheid:

- Project datakwaliteit
- Kwaliteitsprocedures en controles op de operationele afdelingen

*4.1.5 Opslagbeperking*

Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is. Echter mogen persoonsgegevens voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, mits passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen.

Indien het wenselijk is om de gegevens niet algeheel te wissen, kunnen gegevens ook geanonimiseerd worden. Omdat het niet mogelijk is om betrokkene aan de hand van geanonimiseerde gegevens te identificeren is opslag in geanonimiseerde vorm wel toegestaan. Ook pseudonimisering is een mogelijkheid om als alternatief toe te passen. Bij pseudonimisering van persoonsgegevens is het echter be-

langrijk dat een veilige methode van pseudonimisering toegepast wordt om het identificeren zo ver mogelijk uit te sluiten.

Er moet wel rekening mee gehouden worden dat pseudonimisering ook een verwerkingsproces is en alle waarborgen, principes en de rechten van betrokkenen ook op pseudonimisering van toepassing zijn.

De ODRU treft de volgende maatregelen om te voldoen aan het beginsel van opslagbeperking:
- Project autorisaties en opschoning netwerkschijven;
- Integratie van de bewaartermijn en selectielijsten in haar VTH applicatie en Document Management Systeem, zie voor meer informatie hoofdstuk 10

*4.1.6 Integriteit en vertrouwelijkheid*

Het beginsel van integriteit en vertrouwelijkheid bepaalt, dat er passende technische of organisatorische maatregelen worden genomen. Naast een passende beveiliging moeten de persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.
Dit betekent dat de ODRU (en mogelijk ingeschakelde verwerkers) zorgvuldig met persoonsgegevens omgaan. Zorgvuldigheid betekent in de eerste instantie dat medewerkers, die met persoonsgegevens werken, vertrouwelijk met gegevens omgaan. In de tweede plaats betekent zorgvuldigheid dat ODRU technische en organisatorische maatregelen treft, die gegevens verder beveiligen en afschermen.

De ODRU treft de volgende maatregelen om te voldoen aan het beginsel van integriteit en vertrouwelijkheid:
- De ODRU creëert kennis en bewustzijn over persoonsgegevens, integriteit, vertrouwelijkheid en de AVG vereisten onder haar medewerkers;
- Met (ingehuurde) medewerkers worden afspraken gemaakt over geheimhouding;
- Met verwerkers worden afspraken gemaakt over privacy en informatiebeveiliging in een verwerkersovereenkomst, zie voor meer informatie hoofdstuk 8;
- De ODRU implementeert de verplichte technische en organisatorische beveiligingsmaatregelen conform de Baseline Informatiebeveiliging Overheid, zie voor meer informatie hoofdstuk 10.

*4.1.7 Verantwoordingsplicht*

De ODRU is verantwoordelijk voor de naleving van de beginselen en kan deze aantonen. De ODRU moet aantonen, dat de beginselen van gegevensverwerking juist en correct worden nagekomen. Indien de ODRU haar verplichtingen niet (goed) nakomt, is zij aansprakelijk.

De ODRU treft onderstaande maatregelen om te voldoen aan het beginsel verantwoordingsplicht:
1. Doel en context van de verwerking worden binnen de ODRU enerzijds vastgelegd in een verwerkingsregister en anderzijds in overeenkomsten met verwerkers;
2. De FG doet periodiek onderzoek naar de privacy binnen de organisatie en rapporteert hierover aan het bestuur van de ODRU;
3. Er is een FG aangesteld;
4. Er wordt een register bijgehouden van datalekken en beveiligingsincidenten;
5. In het verwerkingsregister wordt, indien van toepassing, ook bijgehouden of er toestemming is gegeven door de betrokkenen om de gegevens te mogen verwerken.

**Paragraaf 4.2 Rechtmatigheid**

De ODRU moet kunnen aantonen dat elk verwerkingsproces op een wettelijke grondslag is gebaseerd. Verwerking van persoonsgegevens is daardoor alleen rechtmatig indien de ODRU aan kan tonen dat een van de voorwaarden uit artikel 6 AVG van toepassing is. Kortom, de verwerking van persoonsgegevens door ODRU is alleen toegestaan, indien de verwerking is gebaseerd op één van onderstaande grondslagen.

De ODRU heeft in haar verwerkingsregister per verwerking onderbouwd op welke grondslag de verwerking gebaseerd is. Zie voor meer informatie hoofdstuk 7.

*4.2.1 Toestemming*

In het geval van toestemming is verwerking van persoonsgegevens alleen rechtmatig indien de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doelen. Toestemming is alleen geldig indien hij geïnformeerd, vrijwillig en specifiek gegeven werd.

Toestemming kan te allen tijde door de betrokkene ingetrokken worden. Intrekken van toestemming heeft geen negatieve gevolgen op de rechtmatigheid van de verwerkingen, die vóór het intrekken van toestemming plaats hebben gevonden. Het verwerken van persoonsgegevens moet uiteraard onverwijld

beëindigd worden zodra toestemming is ingetrokken, tenzij de verwerkingen op een ander rechtsgrond gesteund kunnen worden.

*4.2.2 Uitvoeren van een overeenkomst*
Persoonsgegevens mogen ook verwerkt worden indien verwerking noodzakelijk is om een overeenkomst uit te voeren of om op verzoek van de betrokkene een overeenkomst tot stand te kunnen brengen. Dit is bijvoorbeeld van toepassing op de arbeidsovereenkomst met de (ingehuurde) medewerkers, waarvoor persoonsgegevens verwerkt moeten worden, zowel vóór het tot stand komen van de overeenkomst als ook tijdens het dienstverband.

De ODRU kan alleen een beroep op deze rechtsgrond doen indien de gevraagde persoonsgegevens daadwerkelijk noodzakelijk zijn voor de uitvoering van de overeenkomst. Waar (aanvullende) gegevens niet noodzakelijk zijn, is deze voorwaarde niet van toepassing.

*4.2.3 Wettelijke verplichting*
Uiteraard mag de ODRU gegevens verwerken indien zij wettelijk verplicht is om de verwerkingen uit te voeren. Er bestaan een aantal wettelijke verplichtingen die van toepassing kunnen zijn. De ODRU verwerkt persoonsgegevens om namens haar opdrachtgevers (gemeenten) wettelijke milieu- en omgevingstaken uit te voeren. Daarnaast is de ODRU verplicht om gegevens te verwerken om aan haar wettelijke verplichtingen als werkgever te voldoen en vanwege fiscale verplichtingen.

*4.2.4 Vitale belangen*
Persoonsgegevens mogen verder verwerkt worden indien de verwerking noodzakelijk is om vitale belangen van de betrokkene te beschermen. Een vitaal belang is aan de orde als het over een belang gaat dat essentieel is voor iemands leven of gezondheiden u die persoon niet om toestemming kunt vragen om zijn of haar gegevens te verwerken. Bijvoorbeeld wanneer er acuut gevaar dreigt maar iemand bewusteloos is of mentaal niet in staat is om toestemming te geven. Ter illustratie: bij een grootschalige ramp moet de hulpverlening onmiddellijk op gang komen. In die situatie is het natuurlijk niet te doen om eerst alle betrokken personen te informeren en om toestemming te vragen om hun medische gegevens te verwerken. Ook kan deze grondslag van toepassing zijn indien er sprake is van een epidemie met (mogelijk) grote maatschappelijke gevolgen.

4.2.5 Taak van algemeen belang
Verwerking van gegevens is ook toegestaan indien de ODRU persoonsgegevens verwerkt in verband met de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan haar wettelijk is opgedragen. Deze voorwaarde is alleen van toepassing indien de persoonsgegevens daadwerkelijk noodzakelijk zijn voor de verwerking in verband met de uitoefening van een publiekrechtelijke taak. Het gaat daarbij om taken die in de wet zijn vastgelegd en die relevant zijn voor de organisatie.

*4.2.6 Gerechtvaardigd belang*
Persoonsgegevens mogen verder verwerkt worden indien ODRU een gerechtvaardigd belang aan kan tonen, dat wil zeggen indien de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van ODRU of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen dan de belangen.
Gerechtvaardigde belangen kunnen onder andere bedrijfsbelangen of andere economische belangen betreffen, indien het belang voldoende zwaar weegt. De feitelijke aanwezigheid van een belang is echter niet voldoende. Deze voorwaarde kan alleen toegepast worden indien maatregelen getroffen zijn voor de veiligheid van data en indien de subsidiariteit en de proportionaliteit van de verwerking gewaarborgd is. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt (subsidiariteit), en dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel (proportionaliteit). Wanneer met geen of minder persoonsgegevens hetzelfde doel bereikt kan worden, moet daar altijd voor gekozen worden. De belangen van de Verwerkingsverantwoordelijke en de betrokkene moeten dus voorzichtig afgewogen worden. De afweging van belangen dient gemotiveerd en gedocumenteerd te worden in het verwerkingsregister.
Let op: de grondslag gerechtvaardigd belang mag niet ingezet worden door overheidsorganen in het kader van de uitvoering van hun publieke taak. De taak moet namelijk gewoon wettelijk gecreëerd zijn en kan dus als het goed is altijd terug herleid worden naar bepaalde regelgeving.

## Hoofdstuk 5 Persoonsgegevens en bijzondere categorieën van persoonsgegevens

### Paragraaf 5.1 Persoonsgegevens

Persoonsgegevens betreffen alle informatie waarmee een natuurlijk persoon direct of indirect kan worden geïdentificeerd. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG.

Onderstaand een aantal voorbeelden van informatie die worden gezien als persoonsgegevens. Deze lijst is niet uitputtend.

1. Voornaam en achternaam
2. Adres
3. Burgerservicenummer (BSN)
4. Identificatienummers
   - Personeelsnummer
   - Klantnummer
   - Patiëntnummer
   - Bankrekeningnummer
5. Geboortedatum / leeftijd
6. Locatiegegevens
7. Online identificatoren o IP-adres o MAC-adres
   - Cookies (ook als de naam van de persoon achter het cookie niet bekend is)
   - RFID tag
   - IMEI nummer

8. E-mailadres
9. Vingerafdruk
10. Pasfoto
4. Iemands IQ
5. Gebruikersnaam
6. Persoonskenmerken zoals gewicht, lengte, haarkleur en geslacht

Bij de ODRU worden persoonsgegevens van opdrachtgemeenten, leveranciers, (ingehuurde) medewerkers, inwoners en bedrijven verwerkt. In het verwerkingsregister wordt weergegeven welke persoonsgegevens de ODRU verwerkt. Zie voor meer informatie over het verwerkingsregister hoofdstuk 7.
Let op: persoonsgegevens over bedrijven zijn niet altijd persoonsgegevens. Er is bij bedrijven wel sprake van een persoonsgegeven indien de gegevens herleidbaar zijn naar een persoon, zoals bij een eenmanszaak of indien het gegevens van een individuele bestuurder zijn.

### Paragraaf 5.2 Bijzondere persoonsgegevens

5.2.1 Verwerkingsverbod op bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn bijzonder gevoelig. Deze categorieën persoonsgegevens hebben een bijzondere bescherming, omdat het bekend worden van deze gegevens mogelijk negatieve gevolgen voor de betrokkene kan hebben. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij er aan de voorwaarden van de AVG óf aan de uitzonderingen zoals genoemd in de Uitvoeringswet AVG wordt voldaan.

De volgende gegevens worden gezien als bijzondere persoonsgegevens (artikel 9 lid 1):
1. Ras of etnische afkomst;
2. Politieke opvattingen;
3. Religieuze of levensbeschouwelijke overtuigingen;
4. Lidmaatschap van een vakbond;
5. Genetische gegevens;
6. Biometrische gegevens met het oog op de unieke identificatie van een persoon;
7. Gegevens over gezondheid;
8. Seksueel gedrag of seksuele gerichtheid;
9. Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 10 AVG, artikel 32 en 33 UAVG).

In het memorie van toelichting op het wetsvoorstel van de UAVG[9] staat dat indirecte informatie ook als bijzondere persoonsgegevens worden gezien:
Een persoonsgegeven is niet alleen bijzonder wanneer het direct het desbetreffende bijzondere onderwerp onthult. Ook gegevens die indirect dergelijke informatie onthullen, worden aangemerkt als bijzondere categorieën van persoonsgegevens. Tot de bijzondere categorieën van persoonsgegevens moeten dus niet alleen gegevens worden gerekend die direct betrekking hebben op bijvoorbeeld het lidmaatschap van een vakbond als zodanig, maar ook gegevens waaruit iemands vakbondslidmaatschap indirect valt af te leiden. De administratie van een vakbond, met daarin namen en adressen van de leden, is daarvan een voorbeeld. Noodzakelijk is wel dat er een rechtstreeks verband is. Gegevens die hooguit een indicatie geven dat het om een gevoelig kenmerk zou kunnen gaan, vallen buiten de reikwijdte van de bijzondere regeling voor gevoelige gegevens.

*5.2.2 Uitzonderingen op het verwerkingsverbod*
In beginsel mogen bijzondere categorieën persoonsgegevens dus niet verwerkt worden. Er bestaat echter een aantal uitzonderingen op dit beginsel. Artikel 9 (2) AVG benoemt uitzonderingen, waarvan een aantal ook voor ODRU van belang kan zijn. Indien een van deze uitzonderingen van toepassing is, mogen bijzondere persoonsgegevens bij uitzondering verwerkt worden. Wanneer de ODRU gebruik maakt van de deze uitzondering, wordt dit in het verwerkingsregister onderbouwd.

Het gaat om onderstaande uitzonderingen:
1. De betrokkene heeft uitdrukkelijk toestemming gegeven voor de verweking, tenzij is bepaald dat het verbod niet door de betrokkene kan worden opgeheven;
2. De verwerking is noodzakelijk om wettelijke plichten of rechten te dienen binnen het arbeidsrecht, sociale zekerheidsrecht en sociale beschermingsrecht;
3. Wanneer de verwerking van vitaal belang (levensbelang) is voor de betrokkene, en deze niet in staat is om zelf toestemming te geven;
4. Verwerking vindt plaats door politieke, religieuze, levensbeschouwelijke organisaties of vakbonden, waarbij de verwerking noodzakelijk is voor het onderhouden van contact met leden of voormalige leden;
5. De verwerking heeft betrekking op gegevens die de door de betrokkene zelf openbaar zijn gemaakt;
6. Wanneer de verwerking noodzakelijk is in het kader van gerechtelijke procedures;
7. Wanneer de verwerking noodzakelijk is voor een zwaarwegend algemeen belang dat bij wet is vastgelegd;
8. Wanneer de verwerking noodzakelijk is voor medische redenen, met name in verband met de arbeid (het medisch beroepsgeheim blijft van toepassing);
9. Wanneer de verwerking noodzakelijk is voor archivering in het openbaar belang of voor onderzoek of statistiek;
10. Wanneer de verwerking nodig is in het algemeen belang op het gebied van de volksgezondheid.

Daarnaast benoemd de UAVG in artikel 22 tot en met artikel 33 ook een aantal uitzonderingen die van toepassing zijn op de verwerking van bijzondere persoonsgegevens. Deze uitzonderingen komen grotendeels overeen met de uitzonderingen die in de AVG worden genoemd, maar in een aantal gevallen wijkt de uitzondering af. In dergelijke gevallen is in Nederland de UAVG leidend. De meest opvallende afwijkingen zijn:

*In de UAVG wordt het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken, niet van toepassing verklaard indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Het verwerken voor biometrische gegevens is dus toegestaan zolang dit voor authenticatie of beveiligingsdoeleinden gebeurt.*

De ODRU verwerkt in principe geen bijzondere persoonsgegevens. In haar verwerkingsregister is inzichtelijk welke bijzondere persoonsgegevens zijn verwerkt. Een rechtmatige uitzondering hierop is de verwerking van strafrechtelijke gegevens van inwoners en bedrijven in haar Boa Registratie Systeem. Dit is rechtmatig, aangezien het verwerken van deze strafrechtelijke gegevens in een aantal gevallen wettelijk verplicht is voor het uitvoeren van de wettelijke taken omtrent integraal toezicht en handhaving en horeca vergunningen.
De ODRU treft passende organisatorische en technische maatregelen conform de Baseline Informatiebeveiliging Overheid om deze bijzondere persoonsgegevens te beschermen.

9 ) Memorie van toelichting op EU AVG, te raadplegen via: https://zoek.officielebekendmakingen.nl/kst-34851-3.html

### Paragraaf 5.3 Gevoelige persoonsgegevens

Bijzondere persoonsgegevens zijn per definitie gevoelige gegevens. Er zijn meer persoonsgegevens die een hogere impact op de privacy hebben dan gewone persoonsgegevens. Dit zijn vooral gegevens die gelet op de inhoud of vanwege hun aard als gevoelig worden aangemerkt, omdat dit bijvoorbeeld iets zegt over de financiële situatie van een persoon, het minderjarigen betreft of het bijvoorbeeld iets zegt over iemands surfgedrag.

De ODRU verwerkt ook gevoelige persoonsgegevens. In haar verwerkingsregister is inzichtelijk welke gevoelige persoonsgegevens de ODRU verwerkt. Een aantal voorbeelden daarvan zijn:

- Financiële gegevens, zoals bankrekeningnummer en salaris van medewerkers
- BSN nummer van inwoners in haar VTH applicatie. De ODRU kan op basis van het BSN controleren of een natuurlijke persoon al bekend is in het systeem. Dit is noodzakelijk voor de ODRU om de milieu- en omgevingstaken die zij voor haar opdrachtgevers (gemeenten) uitvoert efficiënt en effectief uit te kunnen voeren.

De ODRU treft passende organisatorische en technische maatregelen conform de Baseline Informatiebeveiliging Overheid om deze gevoelige gegevens te beschermen.

## Hoofdstuk 6 Rechten van betrokkenen

### Paragraaf 6.1 Algemeen

De privacy rechten van betrokkenen ten aanzien van de verwerkingsverantwoordelijke zijn onder de AVG aanzienlijk versterkt. De betrokkene heeft de volgende privacy rechten:

- Recht op informatie;
- Recht van inzage;
- Recht op rectificatie;
- Recht op gegevenswissing/vergetelheid;
- Recht op beperking van de verwerking;
- Recht op overdraagbaarheid/dataportabiliteit;
- Recht van bezwaar;
- Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profilering.
-

### Paragraaf 6.2 Recht op informatie

De ODRU is verplicht aan de betrokkene bepaalde informatie te verstrekken om de transparantie van verwerkingen te waarborgen. Informatie die in ieder geval aan de betrokkene verstrekt moet worden, zijn:

- De contactgegevens van ODRU;
- De contactgegevens van de FG;
- De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd en de rechtsgrond voor de verwerking;
- In voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- Of persoonsgegevens doorgegeven worden aan een land buiten de Europese Unie of aan een internationale organisatie.
  - Indien gegevens naar een derde land doorgegeven worden moet ook vermeld zijn of er een adequaatheidsbesluit is genomen door de Europese Commissie;
  - Indien gegevens naar een derde land of naar een internationale organisatie doorgegeven worden waar de privacy van betrokkenen door passende of geschikte waarborgen beschermd wordt (artikel 46, 47 of 49 (1) AVG) moet de betrokkene geïnformeerd worden uit welke waarborgen de maatregelen bestaan, en hoe ze toegankelijk zijn.

- De periode gedurende welke de persoonsgegevens zullen worden opgeslagen of, indien dat niet mogelijk is, de criteria ter bepaling van het bewaartermijn.
- Dat de betrokkene het recht heeft om ODRU te verzoeken om inzage, portabiliteit, rectificatie of verwijdering van persoonsgegevens, beperking van en bezwaar tegen verwerking;
- Volgens artikel 21 (4) AVG moet het recht op bezwaar uiterlijk op het moment van het eerste contact met de betrokkene uitdrukkelijk onder de aandacht van de betrokkene gebracht en duidelijk en gescheiden van enige andere informatie weergegeven worden.
- Het recht, toestemming te allen tijde weer in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van verwerkingen op basis van de toestemming vóór de intrekking daarvan
- Dat de betrokkene het recht heeft een klacht in te dienen bij de Autoriteit Persoonsgegevens (de toezichthouder)

- Het bestaan van geautomatiseerde besluitvorming, waaronder profilering, en tenminste in het geval van profilering, nuttige informatie over de onderliggende logica, het belang en de verwachte gevolgen van de verwerking voor de betrokkene.

In het geval dat informatie direct van de betrokkene verzameld wordt, geeft ODRU de volgende aanvullende informatie aan de betrokkene:
- Of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten; en
- Of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt

De informatie moet bij het verzamelen van persoonsgegevens aan de betrokkene verstrekt worden. ODRU deelt de informatie ook aan de betrokkene mee wanneer ODRU het plan vormt om persoonsgegevens voor een ander doel te gebruiken dan waarvoor zij oorspronkelijk zijn verzameld. ODRU licht de betrokkene in vóórdat de verwerking begint.

Indien de informatie niet direct van de betrokkene is verkregen maar uit een ander bron afkomstig is, ligt de situatie iets anders. In dergelijk geval moet de bovengenoemde informatie ook aan betrokkene verstrekt worden, met de aanvulling om welke categorieën van persoonsgegevens het gaat.

Verder dient rekening te worden gehouden met de volgende punten:
- De bovengenoemde informatie wordt binnen een redelijke termijn verstrekt, maar uiterlijk binnen een maand na de verkrijging van persoonsgegevens;
- Indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene;
- Indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de gegevens voor het eerst worden verstrekt.

Indien ODRU van plan is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt zij vóór de verdere verwerking informatie over dat andere doel en alle relevante verdere informatie.
De informatieplicht is niet van toepassing indien en voor zover
- De betrokkene reeds over de informatie beschikt;
- Het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder o Bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de toepasselijke voorwaarden en waarborgen, of
  - Voor zover de verplichting om informatie te verstrekken de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

In dergelijke gevallen neemt ODRU passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;
- Het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven door een wet dat op ODRU van toepassing is en passende maatregelen van toepassing zijn om de gerechtvaardigde belangen van de betrokkene te beschermen;
- De persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Europees of nationaal recht, waaronder een statutaire geheimhoudingsplicht.

**Paragraaf 6.3 Recht op inzage**

De betrokkene kan een verzoek indienen om te weten of persoonsgegevens betreffende hem of haar verwerkt worden en om de persoonsgegevens die bij ODRU over hem of haar opgeslagen zijn in te zien. ODRU is verplicht tot inzage van die persoonsgegevens en zal de volgende informatie moeten verstrekken:

- De verwerkingsdoeleinden;
- De betrokken categorieën van persoonsgegevens;

- De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
- Indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- Dat de betrokkene het recht heeft ODRU te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
- Dat de betrokkene het recht heeft klacht in te dienen bij de AP;
- Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
- Het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor betrokkene;
- Indien persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie er passende waarborgen zijn genomen gelet op de doorgifte van de persoonsgegevens.

ODRU is op verzoek van de betrokkene verplicht om een kopie van de persoonsgegevens die worden verwerkt te verstrekken. De betrokkene dient zich wel eerst te identificeren door een kopie van het identiteitsbewijs (met afgeschermd BSN) op te sturen aan de ODRU. Een volledig overzicht kan op verschillende manieren worden gegeven. Uitgangspunt is dat er (digitale) kopieën van het dossier worden verstrekt. In sommige gevallen kan het ook een optie zijn om de betrokkene de gegevens op locatie te laten inzien. Dit mag echter alleen in overleg met de betrokkene.

Houd er in elk geval rekening mee dat de volgende informatie niet wordt overhandigd bij een inzageverzoek, ook niet als daar uitdrukkelijk om wordt gevraagd:
- Persoonlijke en vertrouwelijke werkaantekeningen en notities. Te denken valt aan interne e-mails voor overleg. Maken de gegevens uit deze e-mails onderdeel uit van het dossier, dan moeten deze gegevens wel worden overhandigd;
- Documenten waarin persoonsgegevens van derden zijn opgenomen. Afschriften van deze documenten mogen alleen worden overhandigd als deze andere persoonsgegevens voldoende zijn afgeschermd. Bijvoorbeeld geanonimiseerd of onleesbaar gemaakt;

Persoonsgegevens die worden gebruikt in het kader van de voorkoming, opsporing en vervolging van strafbare feiten.

**Paragraaf 6.4 Recht op gegevenswissing of correctie**

Na een inzageverzoek kan blijken dat persoonsgegevens onjuist zijn. In dat geval heeft betrokkene het recht om de onjuiste persoonsgegevens te laten corrigeren. Verder heeft betrokkene het recht om onvolledige informatie aan te vullen.

Naast een recht op correctie heeft de betrokkene het recht om van ODRU zonder onredelijke vertraging te verlangen dat persoonsgegevens worden gewist. ODRU is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:
- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt
- De betrokkene trekt toestemming in en er is geen andere rechtsgrond waarop verwerking gebaseerd kan worden
- De betrokkene maakt bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking
- De persoonsgegevens zijn onrechtmatig verwerkt
- De persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op ODRU rust .

Indien ODRU de persoonsgegevens gedeeld heeft, neemt zij redelijke maatregelen om andere verwerkingsverantwoordelijken die de persoonsgegevens verwerken ervan op de hoogte te stellen dat de betrokkene ODRU heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen. Daarbij geldt: hoe belangrijker de wijziging, hoe meer moeite er moet worden gedaan om die andere partijen in te lichten.

De ODRU is niet verplicht om gegevens te wissen en te verwijderen wanneer verwerking nodig is:
- Voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;

- Voor het nakomen van een wettelijke verwerkingsverplichting of voor het vervullen van een taak van algemeen belang of het uitoefenen van openbaar gezag dat aan ODRU is verleend;
- Met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden;
- Voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

**Paragraaf 6.5 Recht op beperking van de verwerking**

De betrokkene heeft een recht op beperking van de verwerking onder de volgende omstandigheden:
- De juistheid van de persoonsgegevens wordt door de betrokkene betwist;
- De verwerking is onrechtmatig en de betrokkene kiest voor beperking van het gebruik van persoonsgegevens in plaats van voor het wissen ervan;
- ODRU heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van ODRU zwaarder wegen dan die van de betrokkene.

Het gevolg van een beperking van de verwerking is dat ODRU persoonsgegevens slechts mag verwerken:
- Indien betrokkene toestemming geeft; of
- Indien het nodig is voor een rechtsvordering; of
- Ter bescherming van de rechten van een andere persoon; of
- Om gewichtige redenen van algemeen belang.

ODRU moet verder iedere ontvanger van persoonsgegevens op de hoogte brengen van de vereiste beperking van verwerking. Indien de beperking van de verwerking weer op wordt geheven, wordt de betrokkene vóór de opheffing door ODRU op de hoogte gebracht.

**Paragraaf 6.6 Recht op dataportibiliteit**

De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij of zij aan ODRU heeft verstrekt, in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen, en het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door ODRU, indien
- De verwerking berust op toestemming én
- De verwerking via geautomatiseerde processen wordt verricht.

Indien het technisch mogelijk is kan de betrokkene verzoeken dat gegevens rechtstreeks van ODRU naar een nieuwe Verwerkingsverantwoordelijke worden doorgezonden.

**Paragraaf 6.7 Recht op bezwaar**

Indien persoonsgegevens verwerkt worden op basis van algemeen belang of gerechtvaardigde belangen van ODRU of van een derde, heeft de betrokkene het recht om vanwege met zijn of haar specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens. ODRU staakt de verwerking van de persoonsgegevens tenzij zij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met een rechtsvordering.

**Paragraaf 6.8 Geautomatiseerde individuele besluitvorming**

De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking (waaronder profilering) gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

Dit recht is niet van toepassing indien het besluit:
- Noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en ODRU; of
- Is wettelijk toegestaan; of
- Berust op de uitdrukkelijke toestemming van de betrokkene

In het geval dat het besluit noodzakelijk is of op toestemming berust treft ODRU passende maatregelen ter bescherming van de rechten en vrijheden van de betrokkene, waaronder ten minste:
- Het recht op menselijke tussenkomst;
- Het recht om zijn standpunt kenbaar te maken en;
- Het recht om het besluit aan te vechten.

Verder mogen deze besluiten niet op bijzondere categorieën van persoonsgegevens gebaseerd zijn, tenzij er passende maatregelen ter bescherming van de belangen van betrokkenen getroffen zijn én:
- De betrokkene uitdrukkelijk toestemming heeft gegeven of;
- De verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang.

### Paragraaf 6.9 Afhandeling rechten van betrokkenen

In de privacyverklaring op de website van de ODRU [10] staat dat betrokkenen een verzoek tot het uitoefenen van hun privacyrechten kunnen sturen naar de FG. Dit kan per post en per e-mail. Vervolgens treedt de uitvoeringsrichtlijn procedure beoordelen en afhandelen rechten van betrokkenen in werking. Wanneer de ODRU optreedt als verwerkingsverantwoordelijke moet zij ervoor zorgen dat betrokkenen zich te allen tijde kosteloos kunnen beroepen op deze rechten, en dat er binnen de wettelijk geldende termijn van één maand dient te worden gereageerd op verzoeken van betrokkenen door de FG. Een verlenging met maximaal twee maanden is mogelijk, mits die binnen één maand wordt gemeld en de extra benodigde tijd goed is onderbouwd.
Wanneer de ODRU optreedt als verwerker van persoonsgegevens kan zij verzoeken van betrokkenen met betrekking tot de persoonsgegevens die ze verwerken in opdracht van verwerkingsverantwoordelijke, afwijzen. De ODRU deelt dan mee dat de ODRU die informatie vanuit haar rol als verwerker niet mag verstrekken, en dat ze zich hiervoor kunnen wenden tot de verwerkingsverantwoordelijke. Wel kan het zo zijn dat de verwerkingsverantwoordelijke aan ODRU vraagt om bepaalde gegevens op te leveren. Vanuit de AVG is de verwerker verplicht om aan dergelijke verzoeken mee te werken.

### Paragraaf 6.10 Privacy klachten

Indien de betrokkene van mening is dat de bepalingen van de AVG en dit privacybeleid niet worden nageleefd of andere redenen heeft tot klagen met betrekking tot de verwerking van persoonsgegevens, kan hij, zoals beschreven in het privacyreglement op de website van de ODRU, ook een klacht indien bij de FG. Dit wordt opgenomen in de uitvoeringsrichtlijn procedure rechten van betrokkenen.

De betrokkene kan ook de AP verzoeken een onderzoek in te stellen of de wijze van gegevensverwerking door de verantwoordelijke in overeenstemming is met de AVG. Dat kan via deze link.

## Hoofdstuk 7 Verwerkingsregister

Organisaties hebben een documentatieplicht (artikel 30). Dit betekent onder andere dat organisaties moeten kunnen aantonen wat voor informatie zij opslaan of verwerken, van wie deze data is, waar dit wordt opgeslagen en hoe dit is beveiligd. Alle verwerkingen van persoonsgegevens die plaatsvinden bij een organisatie moeten opgenomen worden in het verwerkingenregister. De Autoriteit Persoonsgegevens kan inzage vragen in dit register. Hierin worden in ieder geval de volgende gegevens opgenomen:
- De naam en de contactgegevens van ODRU, eventuele gezamenlijke verwerkingsverantwoordelijken en de FG;
- Doelen van de verwerking;
- Een beschrijving van de categorieën van betrokkenen en van persoonsgegevens;
- De ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- Indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie;
- Bewaartermijnen van de persoonsgegevens;
- Een beschrijving van de technische en organisatorische beveiligingsmaatregelen.

De ODRU heeft een verwerkingsregister opgesteld. De Autoriteit Persoonsgegevens kan inzage vragen in dit register.

10 )Bron: Privacyverklaring Omgevingsdienst regio Utrecht februari 2020, https://www.odru.nl/wpcontent/uploads/2020/02/20200224-Privacyverklaring-website-ODRU-definitief.pdf

De Adviseur Informatiebeveiliging & Privacy zorgt ervoor dat dit register actueel wordt gehouden. Nieuwe verwerkingen worden opgenomen in het register en wijzigingen in bestaande verwerkingen moeten ook worden doorgevoerd. Minimaal halfjaarlijks wordt de actualiteit van het register gecontroleerd. De FG beoordeelt vervolgens de rechtmatigheid van het register.

## Hoofdstuk 8 Verwerker en verwerkersovereenkomst

### Paragraaf 8.1 Definitie

Het komt voor dat derde partijen persoonsgegevens verwerken in opdracht van ODRU. De derde partijen zijn zogenaamde verwerkers. Deze derden voeren dan namens ODRU een proces uit, waarbij ODRU zelf of de derde via ODRU persoonsgegevens verwerkt.
De rollen die de ODRU, vanuit de AVG, kan aannemen zijn:

1. Verwerkingsverantwoordelijke
2. Verwerker
3. Gezamenlijke verwerkingsverantwoordelijke

*Ad 1. Verwerkingsverantwoordelijke (art. 24, AVG)*
Bij deze rol is de organisatie verplicht de AVG na te leven, daarvoor moet zij passende en effectieve maatregelen nemen. Ook moet zij kunnen aantonen dat elke verwerkingsactiviteit past binnen de AVG. De verwerkingsverantwoordelijke is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. (Engelfriet, Chew-Meij & Kager, 2017). Het gaat hierbij om feitelijke invloed op de wijze van en middelen voor het verwerken.

*Ad 2. Verwerker (art. 28, AVG)*
Een partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerkingsverantwoordelijke is namelijk de actor die het doel en de middelen vast stelt.
Doet deze dat toch, dan is de partij geen verwerker maar verwerkingsverantwoordelijke of gezamenlijk verantwoordelijk. (Engelfriet, Chew-Meij & Kager, 2017)

*Ad 3. Gezamenlijk verantwoordelijk (art. 26, AVG)*
Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectievelijke verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van de AVG vast. (Engelfriet, Chew-Meij & Kager, 2017)
In elke rol komt terug wie de verantwoordelijkheid heeft om doelen op te stellen en de middelen te bepalen. Dit zal in elke samenwerking tussen partijen anders zijn, waardoor interpretatieverschil mogelijk is. Bovendien is er nog geen sprake van opgebouwde jurisprudentie.

### Paragraaf 8.2 Bepalen wie Verwerker en (Gezamenlijk) Verwerkingsverantwoordelijke is

De bepaling of een partij een Verwerker of Gezamenlijk Verwerkingsverantwoordelijke is, aan de hand van de feitelijke/werkelijke situatie. Primair is hierbij van belang in welke mate een partij invloed kan uitoefenen op de doelen van de verwerking. Secundair is de invloed van een partij op de middelen van de verwerking.

De feitelijke/werkelijke situatie kan worden geanalyseerd aan de hand van drie factoren:

1. **Mate van beslisbevoegdheid** - de hoeveelheid ruimte die de andere partij krijgt/heeft om zelf te beslissen hoe de verwerking wordt uitgevoerd, is een sterke indicatie van verwerkerschap. Wanneer de andere partij een hoge mate van beslisbevoegdheid heeft, dan neemt de waarschijnlijkheid toe dat deze partij optreed als verwerkingsverantwoordelijke.
   Indicatievragen zijn:
   - Welke mate van zeggenschap heeft de andere partij bij de verwerking?
     - Bepaalt de ODRU volledig hoe de andere partij te werk moet gaan, of neemt de ODRU een dienst af zonder invloed te hebben op hoe dit gaat gebeuren?
   - Wat gebeurt er met de resultaten van de verwerking?

- Worden de resultaten uitsluitend aan de ODRU beschikbaar gesteld, of worden de resultaten door de andere partij ook gebruik voor de eigen dienstverlening en worden er alleen algemene resultaten aan de ODRU gerapporteerd?

- Wat bepaalt het contract tussen de ODRU en de andere partij over eigendom van persoonsgegevens?
  - Blijft de ODRU eigendom van de persoonsgegevens, of worden de persoonsgegevens eigendom van de andere partij?

2. **Mate van inspraak** - de hoeveelheid invloed die de andere partij heeft op de doelen van de verwerking. Als er geen inzicht is in wat de partij met de gegevens gaat doen, dan is een verwerkersrelatie onwaarschijnlijk. Dat maakt een verwerkersrelatie onwaarschijnlijk. Daarbij komt dat u deze partij contractueel noch praktisch zou kunnen stoppen als zij zelfgekozen doelen gaan uitvoeren. Dit is typisch voor een verantwoordelijke.
   Indicatievragen zijn:
   - Hoe kan de verwerking het beste worden omgeschreven?
     Bij bepaalde type verwerkingen is de andere partij doorgaans als verwerkingsverantwoordelijke aan te merken.
     - Uitvoerders van een wettelijke taak. Accountant, notaris, advocaat. Deze uitvoerders mogen niet worden gezien als verwerker, omdat zij zelf bepalen hoe de taak wordt uitgevoerd.
     - PostNL ziet zichzelf ook niet als verwerker: zij vinden dat ze zélf bepalen waar de post heen gaat en wat ze doen met persoonsgegevens, bv. de ontvanger via hun app informeren over de voortgang. Ook kunnen ze dan bijvoorbeeld statistieken over klanten heen uitvoeren, wat waarschijnlijk de achterliggende reden is.
   - In hoeverre is bekend wat de andere partij gaat doen met de persoonsgegevens?
     - Als de ODRU weet wat de andere partij met de persoonsgegevens gaat doen en hier invloed op kan uitoefenen, dan is de andere partij waarschijnlijk verwerker
     - Als de ODRU geen zicht heeft op wat de derde partij met de persoonsgegevens doet en hier ook geen/weinig invloed op kan uitoefenen, dan is de andere partij waarschijnlijk verwerkersverantwoordelijke.
   - Kunnen de door de andere partij gekozen doelen worden tegengehouden of beïnvloed?
     - De ODRU kan hier praktisch noch contractueel iets tegen doen.
     - De andere partij mag niks op eigen initiatief met de persoonsgegevens doen.

3. Positie van de andere partij - het gaat hier om een derde partij, die zelf zijn bedrijfsvoering inricht en waar je als organisatie niet direct zicht op zult hebben. Het is daarmee goed mogelijk dat deze partij toch een verantwoordelijke is. Het contract bepaalt verder nog dat deze partij is, wat een zeer sterke aanwijzing die kant op is maar niet doorslaggevend. Het gaat namelijk uiteindelijk om de werkelijke situatie.
   Indicatievragen zijn:
   - Welke band is er tussen de ODRU en de andere partij?
     – Als de derde partij een zelfstandige organisatie is, die zelf beslist hoe ze haar bedrijfsvoering inricht, is dat een indicatie voor verwerkingsverantwoordelijkheid.

   - Wat bepaalt het contract over verwerkerschap?
     – Wat het contract bepaalt is een indicatie, maar niet doorslaggevend. Het gaat namelijk om de feitelijke/werkelijke situatie.

**Paragraaf 8.3 De ODRU als gezamenlijke regeling: Verwerker of Verwerkingsverantwoordelijke**

De ODRU is een gemeenschappelijke regeling (GR) die taken uitvoert die bij wet aan haar opdrachtgevers (gemeenten) zijn toegekend. Om te bepalen of de ODRU in verhouding tot haar opdrachtgevers als verwerker of verwerkingsverantwoordelijke optreedt, kan in eerste instantie worden gekeken naar de wijze waarop de taken aan de ODRU zijn toegekend.

In het geval van mandaat of machtiging worden de bevoegdheden door de ODRU namens de gemeenten uitgeoefend. In principe blijven de gemeenten in een dergelijke situatie verwerkingsverantwoordelijke (en de ODRU verwerker), maar er kan ook sprake zijn van een gezamenlijke verantwoordelijkheid wanneer de ODRU feitelijk/werkelijk invloed uitoefent op het doel en middelen van de verwerking. Kortom, de feitelijke/werkelijke mate van invloed dient te worden vastgesteld op basis van de criteria

in paragraaf 8.2, zodat op basis van het ontstane inzicht kan worden bepaald of de ODRU richting haar klanten (gemeenten) optreedt als verwerker of verwerkingsverantwoordelijke.

In het geval van delegatie van bevoegdheden is de ODRU zelfstandig bevoegd gemaakt om de overgedragen bevoegdheden uit te oefenen en is de ODRU bestuurlijk verantwoordelijke. Daardoor zijn de gemeenten en de ODRU aangemerkt als Zelfstandig Verwerkingsverantwoordelijken.

Voor het vaststellen van de feitelijke/werkelijke situatie, is gekeken naar de mate van zelfstandigheid waarmee de ODRU uitvoering geeft aan haar taken. Hieruit blijkt dat de ODRU over veel zaken zelfstandige besluiten neemt binnen bepaalde generieke kaders; de operationele bemoeienis van de gemeenten is beperkt en er is sprake van een hoge mate van autonomie. Dit betekent dat de ODRU zeggenschap heeft over het doel en de middelen van de verwerking van persoonsgegevens, en dat impliceert een verwerkingsverantwoordelijkheid. De gemeenten zijn daarnaast ook zelfstandig verwerkingsverantwoordelijke.

De ODRU stelt zich richting haar gemeenten op als Verwerkingsverantwoordelijke.[11] De gemeenten zijn daarnaast ook Zelfstandig Verwerkingsverantwoordelijke.

**Paragraaf 8.4 Verwerkersovereenkomst**

Bij het uitbesteden van een verwerking of bij het verwerken van persoonsgegevens van een andere partij moeten afspraken worden gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Deze afspraken moeten worden vastgelegd in een overeenkomst die de 'verwerkersovereenkomst' wordt genoemd.[12] De verwerkersovereenkomst heeft betrekking op de zorgvuldige omgang met de persoonsgegevens door de verwerker. Dit is een gangbare, maar geen officiële term uit de AVG. De afspraken kunnen ook volgen uit een andere rechtshandeling krachtens Unierecht of lidstatelijke recht. Bij gegevensuitwisseling tussen twee verwerkingsverantwoordelijken is het eveneens aan te bevelen een overeenkomst te sluiten waarin de betrokken partijen afspraken over de gegevensdeling vastleggen, bijvoorbeeld dat de deling van de gegevens rechtmatig is en veilig plaatsvindt. Er moet altijd een geldige grondslag zijn voor het verwerken van de persoonsgegevens. Dit betekent dat persoonsgegevens niet mogen worden gebruikt voor een ander doel dan in de overeenkomst is vastgelegd (bijvoorbeeld een kopie van productiedata in een testomgeving), tenzij de overeenkomst hier expliciet voor wordt aangepast. De ontvangende partij is zelf verantwoordelijk voor de technische en organisatorische maatregelen die voor de beveiliging van de gegevens nodig zijn.
Volgens de AVG wordt in een verwerkersovereenkomst minimaal het volgende geregeld:

- Het doel van de verwerking (doelbinding);
- Persoonsgegevens mogen uitsluiten worden verwerkt op basis van schriftelijke instructies van de verantwoordelijke;
- Personen betrokken bij de verwerking borgen vertrouwelijkheid door bijvoorbeeld het ondertekenen van een NDA of een geheimhoudingsclausule als onderdeel van de arbeidsovereenkomst;
- De technische en organisatorische maatregelen die door de verwerker worden genomen zijn vastgelegd in een bijlage;
- Of er sprake is van algemene of specifieke toestemming voor het inschakelen van sub-verwerkers door verwerker;
- Dat er met de sub-verwerker door verwerker een sub-verwerkersovereenkomst wordt gesloten die voldoet aan de AVG;

- Of en, zo ja, hoe verwerker de verwerkingsverantwoordelijke bijstaat in het geval betrokkenen hun rechten ingevolge de AVG wensen uit te oefenen;

- Hoe verwerker de verwerkingsverantwoordelijke bijstaat bij:
  - Beveiliging van de verwerking;
  - Melding inbreuken aan Autoriteit Persoonsgegevens (datalekken);
  - Mededeling inbreuken aan betrokkenen;
  - Gegevensbeschermingseffectbeoordeling (DPIA);
  - Indien nodig: voorafgaande raadpleging Autoriteit Persoonsgegevens.

- Na afloop van de verwerking worden persoonsgegevens gewist en indien de verwerkingsverantwoordelijke dit wenst, eerst teruggegeven aan de verwerkingsverantwoordelijke;

11 )Advies positie ODRU in relatie tot AVG (aan MT d.d. 27-3-2018)

12 )Een verwerkersovereenkomst vloeit voort uit privacywetgeving. Wanneer er geen persoonsgegevens worden verwerkt, is een verwerkersovereenkomst dus niet nodig.

- Verwerkingsverantwoordelijke stelt alle informatie ter beschikking die nodig is om de nakoming van de verplichtingen onder de AVG aan te tonen;
- De verwerker laat audits door de verwerkingsverantwoordelijke, of door een door verwerkingsverantwoordelijke aangewezen auditor, toe om te controleren of verwerker aan de verplichtingen ingevolgde de AVG en verwerkersovereenkomst voldoet of heeft voldaan;
- De verwerker stelt verwerkingsverantwoordelijke onmiddellijk op de hoogte wanneer verwerker van mening is dat een instructie van de verwerkingsverantwoordelijke in strijd is met de AVG;
- Of verwerker gecertificeerd is, zodat hiermee kan worden aangetoond dat verwerker voldoende garanties biedt.

De ODRU treft de volgende maatregelen om passende privacyafspraken te maken met haar Verwerkers:
- De ODRU heeft in het inkoopproces geborgd dat wanneer een partij persoonsgegevens verwerkt voor de ODRU dat er een Verwerkersovereenkomst getekend wordt.
- De ODRU heeft een standaard verwerkersovereenkomst format. Hierin zijn de eisen vanuit de AVG geborgd. Ook worden er beveiligingseisen gesteld aan de verwerker, overeenkomstig de eisen die de Baseline Informatiebeveiliging stelt. Eén van deze eisen is dat de Verwerker een passend beveiligingsniveau moet hebben, conform de ISO 27001 of een vergelijkbare informatiebeveiligingsnorm.

Wanneer de ODRU zelf optreedt (dit zal incidenteel zijn) als Verwerker, dan sluit de Verwerkingsverantwoordelijke met de ODRU een Verwerkersovereenkomst.
Wanneer een partij geen Verwerker is en er dus geen Verwerkersovereenkomst nodig is, maakt de ODRU wel afspraken over persoonsgegevens. Het is belangrijk om afspraken te maken over o.a. datalekken, geheimhouding en informatiebeveiliging.

### Paragraaf 8.5 Inhuurkrachten

Inhuurkrachten (zoals bijvoorbeeld ZZP'ers) worden vanuit de AVG ook gezien als leveranciers. Om te voorkomen dat met dergelijke partijen een verwerkersovereenkomst dient te worden afgesloten, zonder dat er expliciet opdracht is gegeven tot het verwerken van persoonsgegevens, zal er een contractuele grondslag moeten bestaan waarmee inhuurkrachten als interne medewerkers kunnen worden behandeld. Deze grondslag ontstaat door het opnemen van de onderstaande passage in overeenkomsten met inhuurkrachten.

*"Aan Opdrachtnemer is niet de expliciete opdracht verstrekt tot verwerking van persoonsgegevens. Indien en voor zover in het kader van de uitvoering van de overeenkomst toch persoonsgegevens worden verwerkt, dan is Opdrachtnemer verwerker in de zin van de AVG, en zal met hem een verwerkingsovereenkomst worden gesloten overeenkomstig de AVG."*

Als vanzelfsprekend houdt de inhuurkracht zich dan aan de dezelfde normen en afspraken als de eigen medewerkers (denk aan geheimhouding/gedragscode). Dit betekent dat de inhuurkracht geen andere toegang heeft tot, of afwijkend gebruik maakt van, persoonsgegevens dan de eigen medewerkers van de ODRU.

Wanneer een inhuurkracht expliciet de opdracht krijgt om a) iets te doen met persoonsgegevens (bijvoorbeeld database maken of opschonen) of b) persoonsgegevens verwerkt anders dan de eigen medewerkers van de ODRU (met een soortgelijke rol of functie), dan dient er wél een verwerkersovereenkomst te worden afgesloten.

De ODRU borgt dat de genoemde passage is opgenomen in overeenkomsten met inhuurkrachten.
De ODRU sluit alsnog een verwerkersovereenkomst met een inhuurkracht af wanneer er expliciet opdracht wordt gegeven tot het verwerken van persoonsgegevens of wanneer de verwerking van persoonsgegevens afwijkt van de eigen medewerkers van de ODRU.

## Hoofdstuk 9 Persoonsgegevens buiten Europa

Persoonsgegevens mogen in principe niet worden geëxporteerd naar een land buiten de Europese Economische Ruimte (EER). Binnen de EER geldt het uitgangspunt van 'free flow of information/ personal data'. Het exporteren van persoonsgegevens naar andere EER-lidstaten is onder dezelfde voorwaarden toegestaan als binnen Nederland.

Onder exporteren wordt o.a. verstaan: het buiten de EU/EER opslaan (bijvoorbeeld in de cloud) of het ter beschikking stellen van persoonsgegevens. Hieronder valt niet het via internet zichtbaar maken van persoonsgegevens aan personen buiten de EU.
Onder bepaalde omstandigheden mogen persoonsgegevens wel worden geëxporteerd naar buiten de EU/EER, zoals wanneer er in het exportland een passend beschermingsniveau is. De Europese Commissie kan besluiten dat een land een passend beschermingsniveau heeft d.m.v. een adequaatheidsbesluit ('adequacy decision') of wanneer door de Europese Commissie goedgekeurde standaardcontracten worden gebruikt.

De ODRU heeft als uitgangspunt dat de data binnen de EER verwerkt wordt. De datacenters van de ODRU staan in Nederland. Daarnaast vereist de ODRU dat haar Verwerkers data ook binnen de EER verwerken.
Wanneer zij persoonsgegevens laat verwerken door organisaties buiten Europa gelden de volgende eisen:

- Dat er een Europees modelcontract is afgesloten, of
- In het geval van Amerikaanse bedrijven, dat deze bedrijven zijn opgenomen in het EUU.S. Privacy Shield (adequaatheidsbesluit)

## Hoofdstuk 10 Technische en organisatorische maatregelen

### Paragraaf 10.1 Informatiebeveiligingsbeleid

**Artikel**
De AVG stelt (artikel 32): "Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:"

De ODRU heeft een, op de NEN/ISO 27002 gebaseerd, basisbeveiligingsniveau voor alle informatie en informatiesystemen van de ODRU; de zogenaamde baseline informatiebeveiliging. Deze eigen baseline is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).
De ODRU heeft een informatiebeveiligingsbeleid dat gebaseerd is op de BIO. Het beleid heeft als hoofddoel om te voorzien in een betrouwbare informatievoorziening, waarbij er tegen een acceptabel kostenniveau bescherming wordt geboden tegen interne en externe dreigingen.
De subdoelen zijn:

- Het waarborgen van de continuïteit van de bedrijfsvoering van de ODRU;
- Het voorkomen van beveiligingsincidenten en datalekken;
- Het minimaliseren van de schade door de negatieve gevolgen van beveiligingsincidenten en datalekken. Deze schade kan betrekking hebben op onze eigen organisatie, onze (interne of externe) medewerkers, de opdrachtgevers, inwoners, bedrijven of andere betrokkenen veroorzaakt door de gevolgen van beveiligingsincidenten.

Op basis van een onderliggend stelsel van technische, fysieke en organisatorische maatregelen garandeert het informatiebeveiligingsbeleid, rekening houdend met de hedendaagse technologische mogelijkheden en de kosten van implementatie, een passend beveiligingsniveau gelet op de risico's die op de informatievoorziening van de ODRU van toepassing zijn.

Een aantal technische en organisatorische maatregelen wordt expliciet benoemd in de AVG. Deze maatregelen worden in de volgende paragrafen nader toegelicht.

### Paragraaf 10.2 Data protection impact assessment (DPIA)

*10.2.1 Introductie*
Een Gegevensbeschermingseffectbeoordeling (GEB; Engels: DPIA; en in de praktijk vaak ook Privacy Impact Assessment (PIA) genoemd) is verplicht voor risicovolle verwerkingen van persoonsgegevens. Organisaties zijn verplicht tot het uitvoeren van een DPIA wanneer er iets wijzigt in de verwerking van persoonsgegevens, of wanneer zij van plan zijn om persoonsgegevens te gaan verwerken en dit waarschijnlijk een hoog risico voor de betrokkene inhoudt (artikel 35). De achterliggende gedachte is dat de DPIA inzicht geeft in de privacy risico's waardoor de juiste maatregelen genomen kunnen worden om de risico's tot een acceptabel niveau te verlagen.

*10.2.2 Criteria hoog risico verwerking*
Artikel 35, lid 3 uit de AVG geeft enkele voorbeelden van wanneer een verwerking "waarschijnlijk een hoog risico inhoudt" [13]:

- Geautomatiseerde beoordeling van personen - een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen.

- Grootschalige verwerking van bijzondere persoonsgegevens - grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.
- Grootschalig monitoren van openbare ruimtes - stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

De AVG geeft niet aan wat er verstaan wordt onder 'op grote schaal'. De werkgroep van Europese privacytoezichthouders, de WP29, geeft hier handvatten voor [14]. Zij beschrijft de volgende criteria:

- Het aantal betrokkenen (bijvoorbeeld de hoeveelheid klanten van wie de organisatie gegevens verwerkt);
- De hoeveelheid soorten persoonsgegevens die de organisatie verwerkt (is er bijvoorbeeld sprake van verwerking van bijzondere persoonsgegevens (o.a. medische, politieke gegevens, gegevens over strafrechtelijke feiten));
- De duur van de gegevensverwerking (hoeveel maanden, weken, jaren worden de gegevens verwerkt);

- De frequentie waarmee de verwerkingen worden uitgevoerd (hoe vaak wordt de verwerking gedaan).

De 'werkgroep artikel 29' (WP29) concretiseert dit en noemt negen criteria om te beoordelen of een verwerking een "waarschijnlijk hoog risico" inhoudt. WP29 geeft aan dat het voldoen aan twee van de negen criteria vaak al betekent dat een DPIA dient te worden uitgevoerd.

1. Evaluatie of scoretoekenning – onder andere profielbepalingen en voorspelling in het kader van kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene.
2. Geautomatiseerde besluitvorming met rechtgevolg of vergelijkbaar wezenlijk gevolg – verwerkingen die gericht zijn op het nemen van beslissingen met betrekking tot betrokkenen "waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden" of die "de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen".
3. Stelselmatige monitoring - verwerkingen die worden gebruikt voor het observeren, monitoren of controleren van betrokkenen, inclusief via netwerken verzamelde gegevens of stelselmatige monitoring van openbaar toegankelijke ruimten.
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard (bijzondere persoonsgegevens) - dit omvat speciale categorieën persoonsgegevens zoals omschreven in artikel 9 (bijvoorbeeld informatie over de politieke opvattingen van personen), evenals persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten zoals omschreven in artikel 10.
5. Op grote schaal verwerkte gegevens
6. Matching of samenvoeging van datasets – bijvoorbeeld datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd op een wijze die de redelijke verwachtingen van de betrokkene zou overschrijden.
7. Gegevens met betrekking tot kwetsbare betrokkenen – verwerkingen van dit soort gegevens is een criterium vanwege de toegenomen machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke, wat betekent dat de natuurlijke personen mogelijk niet in staat zijn om gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Kwetsbare betrokkenen kunnen kinderen omvatten, werknemers, kwetsbaardere segmenten van de bevolking die speciale bescherming behoeven (bijvoorbeeld geesteszieken, asielzoekers, bejaarden, patiënten), maar ook ander situaties waarin een oneven-

13) Voor deze verwerkingen geldt dat het een kernactiviteit dient te zijn van de organisatie
14 *Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_on_data_protection_impact_assessment_dpia.pdf*

wichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.

8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen – bijvoorbeeld het combineren van het gebruik van vingerafdrukken en gezichtsherkenning voor een betere fysieke toegangscontrole. In de AVG wordt duidelijk gesteld (artikel 35, lid 1) dat het gebruik van een nieuwe technologie aanleiding kan geven tot de noodzaak om een DPIA uit te voeren. Dit komt omdat het gebruik van dergelijke technologie nieuwe vormen van het verzamelen en gebruiken van gegevens kan inhouden, mogelijk met een hoog risico voor de rechten en vrijheden van natuurlijke personen. De persoonlijke en sociale gevolgen van het gebruik van een nieuwe technologie kunnen immers onbekend zijn.

9. Wanneer als gevolg van de verwerking zelf betrokkenen een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst (artikel 22) – bijvoorbeeld verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst of de mogelijkheid van betrokkenen om een overeenkomst aan te gaan, toe te staan, te wijzigen of te weigeren.

De Autoriteit Persoonsgegevens heeft daarnaast een lijst opgesteld met 16 verwerkingen waarvoor het uitvoeren van een DPIA verplicht is vóórdat de organisatie met verwerken begint. [1]
Voorbeelden hiervan zijn verwerking van gezondheidsgegevens, locatiegegevens, zwarte lijsten, cameratoezicht en creditscores.

10.2.3 Eisen aan een DPIA
De DPIA moet in ieder geval het volgende bevatten:

1. Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan.
2. Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen.
3. Een beoordeling van de privacyrisico's voor de betrokkenen.
4. De beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat de organisatie aan de AVG voldoet.

De ODRU volgt de volgende stappen op het gebied van een DPIA;

- Bij iedere nieuwe verwerking moet de Verwerkingsverantwoordelijke een eerste beoordeling maken van de risico's die daarbij kunnen bestaan (classificatie);
- Wanneer uit de eerste beoordeling blijkt dat er sprake is van een hoog risico, dan dient een uitgebreide DPIA worden uitgevoerd;
- Wanneer uit de DPIA blijkt dat het hoge risico niet kan worden beperkt met redelijke middelen, dan moet de AP eerst worden geraadpleegd.
- De ODRU hanteert voort het uitvoeren van een DPIA de procedure en het format Gegevensbeschermingseffectbeoordeling Rijksdienst. [1]
- Indien een DPIA uitgevoerd wordt, gaat de ODRU in op de verwerkingen en de bijbehorende doelen. De DPIA zal ook een beoordeling bevatten van de noodzaak en proportionaliteit van de verwerking, de risico's van de verwerking en de beoogde mitigerende maatregelen voor deze risico's. Ten slotte voert ODRU een toets uit om te bepalen of de verwerking overeenkomstig de aanbevelingen en conclusies van de DPIA wordt uitgevoerd. De DPIA dient altijd voorgelegd te worden aan de FG ter advies en akkoord.

**Paragraaf 10.3 Privacy by design en privacy by default**

De AVG verplicht Verwerkingsverantwoordelijken om invulling te geven aan de begrippen privacy by design en privacy by default (artikel 25). Privacy by design betekent dat bij nieuwe projecten, diensten of services privacy meegenomen dient te worden bij de ontwerpkeuzes en criteria.

Privacy by default betekent dat standaard de meest strikte privacy settings moeten worden toegepast wanneer er een nieuw product of service wordt geïntroduceerd, zodat standaard zo min mogelijk persoonsgegevens worden verwerkt.

1 ) Autoriteit Persoonsgegevens, Data protection impact assessment (DPIA), geraadpleegd op 13 mei 2020, https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-apvoor-een-verplichte-dpia-6667

1 ) Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA), geraadpleekg op 13 mei 2020, https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

Volgens artikel 25 AVG moeten er door het hele proces van het verwerken van persoonsgegevens technische en organisatorische maatregelen genomen worden om aan de beginselen te voldoen. Zulke technische en organisatorische maatregelen zijn bijvoorbeeld:

- Het pseudonimiseren van persoonsgegevens;
- Het minimaliseren van de hoeveelheid persoonsgegevens;
- Transparantie met betrekking tot de functies en de verwerking van de persoonsgegevens;
- Het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking en;
- Het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren.

De ODRU heeft de principes privacy by design en privacy by default als volgt geborgd:
De FG en de Adviseur Informatiebeveiliging & Privacy zijn aangesloten bij projecten om te adviseren en borgen dat er passende maatregelen worden getroffen.
De ODRU heeft een standaard set aan privacy en informatiebeveiligingseisen die zij stelt aan nieuwe diensten en services waarbij persoonsgegevens gegevens worden verwerkt. Deze zijn geborgd in de standaard Verwerkersovereenkomst en zijn conform de AVG en BIO.

**Paragraaf 10.4 Bewaartermijn**

Er is op grond van de AVG geen concrete bewaartermijn voor persoonsgegevens. Organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren. Hierbij kijken zij naar hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld of worden gebruikt.

In verschillende Nederlandse wetten worden er wel specifieke bewaartermijnen bepaald. Hierbij kan het gaan om minimale en maximale bewaartermijnen. Bijvoorbeeld op grond van belastingwetgeving

Is de bewaartermijn van persoonsgegevens voorbij of zijn de gegevens niet meer noodzakelijk? Dan moeten organisaties de gegevens vernietigen. Zijn persoonsgegevens bestemd voor historische, statistische of wetenschappelijke doeleinden? Dan mogen organisaties de persoonsgegevens in een archief bewaren.

Voor persoonsgegevens in een archief geldt geen bewaartermijn. Op deze regel bestaat een uitzondering: als de Archiefwet of een andere wet van toepassing is, geldt wel een bewaartermijn. De organisatie moet de gegevens vernietigen als ze niet meer nodig zijn voor het doel van het archief.

De ODRU heeft in haar verwerkingsregister per verwerking vastgesteld wat het bewaartermijn is. Ook is daarin vastgesteld voor achiefwaardige informatie of deze vernietigd of bewaard moeten worden na verstrijken van het bewaartermijn.

**Paragraaf 10.5 Anonimisering en pseudonimisering**

Anonimiseren, ook wel datamasking genoemd, is een methode waarbij persoonsgegevens zodanig worden bewerkt dat deze niet meer gebruikt kunnen worden om een persoon te identificeren. Deze bewerking is onomkeerbaar. De AVG is daarom niet van toepassing op geanonimiseerde persoonsgegevens.

Anonimisering kan op een aantal verschillende manieren worden gerealiseerd:
1. Gegevens kunnen geheel willekeurig in andere data worden vertaald.
2. Gegevens binnen een dataset kunnen worden verschoven. Achternamen kunnen bijvoorbeeld worden verwisseld.
3. Bepaalde gegevens, zoals de eerste cijfers van een nummer, kunnen worden gewist.
4. Alle dag- of maandnummers kunnen worden vervangen door hetzelfde getal, bijvoorbeeld een nul of één.
5. Gegevens kunnen (deels) worden vervangen door willekeurige, fictieve gegevens uit een andere gegevensverzameling.
6. Gegevens kunnen via vooraf gedefinieerde regels worden vervangen.

Bij pseudonimisering ligt dat anders. Pseudonimisering zorgt er namelijk voor dat gegevens niet kunnen worden herleid tot een individu zolang de gegevens geïsoleerd worden beschouwd. Dit betekent dat de herleidbaarheid is beperkt, maar niet voorgoed onmogelijk is gemaakt. Met behulp van “aanvullende informatie” zijn gepseudonimiseerde gegevens wederom te herleiden naar persoonsgegevens. Om

deze reden worden pseudonieme persoonsgegevens door de AVG gezien als persoonsgegevens, waardoor de AVG op dergelijke gegevens onverminderd van toepassing is. Overigens worden beide methoden door de AVG gezien als belangrijke maatregel om persoonsgegevens te beschermen.

Voor de ODRU is anonimisering met name relevant bij testdata. Het selecteren en gereed maken van datasets met testdata is tijdrovend. Testdata moet juist, volledig en identiek aan de productie zijn, zodat uitgevoerde testen met deze data ook representatief zijn. Aanvullend stelt de AVG dat testdata niet zomaar een kopie van de productie-data mag zijn, omdat er anders sprake kan zijn van een 'onrechtmatige verwerking' (er wordt dan voorbij gegaan aan het doel en de grondslag van de verwerking) en/of een 'verhoogd risico op datalekken'. Uitsluitend in die gevallen waarin aantoonbaar geen alternatief is, is verwerking toegestaan. De noodzakelijkheid van de verwerking van persoonsgegevens moet aangetoond kunnen worden. Dit kan bijvoorbeeld middels een DPIA.

Onder de AVG mogen ook Verwerkers geen productiedata als testdata gebruiken. De doelen voor de gegevensverwerking worden namelijk geformuleerd binnen de context van primaire bedrijfsprocessen. Dit betekent dat de persoonsgegevens niet zomaar door de Verwerker mag worden gebruikt voor ondersteunende processen (zoals testen). Het door Verwerkingsverantwoordelijke opnemen van 'testen' als onderdeel van het doel van de verwerking mag niet onder de AVG. De AVG vereist van de verwerkingsverantwoordelijke dat deze kan aantonen dat de verwerking zoveel als mogelijk wordt beperkt (privacy by design en privacy by default), waardoor het moeilijk is om te verdedigen dat het testen door verwerker wordt gezien als doel van de verwerking vanuit de verwerkingsverantwoordelijke.

Omdat het gebruiken van persoonsgegevens in test- of acceptatieomgeving doorgaans buiten het doel van de verwerking vallen, dienen persoonsgegevens in dergelijke omgevingen te worden geanonimiseerd of gepseudonimiseerd. De ODRU heeft als uitgangspunt dat er geen persoonsgegevens in de test- of acceptatieomgeving gebruikt worden. Indien dit wel noodzakelijk is, omdat er geen privacy vriendelijk alternatief is, moet dit onderbouwd worden en goedgekeurd worden door de FG.
De ODRU heeft in haar standaard Verwerkersovereenkomst opgenomen dat Verwerkers geen productiedata als testdata gebruiken.

**Paragraaf 10.6 Beschikbaarheid**

Het is belangrijk om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen. Redundantie binnen fysieke systemen verhoogt de beschikbaarheid, het hebben van een betrouwbare back-up vergezeld met het uitvoeren van reguliere restore tests verzekert het tijdig kunnen herstellen van persoonsgegevens.

De ODRU heeft de volgende maatregelen getroffen op het gebied van beschikbaarheid:
1. De backups zijn redunant uitgevoerd
2. Betrouwbare back-ups
3. Reguliere restore tests

**Paragraaf 10.7 Encryptie**

Met encryptie worden gegevens versleuteld. Het is vervolgens enkel mogelijk deze gegevens te ontsleutelen door degene die in het bezit is van de sleutel. Gebruik van encryptie voor het beveiligen van persoonsgegevens is, in geval van sterke encryptie, een uiterst effectieve manier om persoonsgegevens onherleidbaar te maken voor derden. Een derde die de gegevens onderschept, is niet in staat om de inhoud van de versleutelde gegevens te raadplegen.

Op grond van het doel en de toepassing kan een onderscheid worden gemaakt in encryptie van data in transit en data at rest.
1. Encryptie van 'data in transit', dat wil zeggen encryptie van data dat zich beweegt over het internet of een besloten netwerk, zoals mailverkeer, gebruik van een webapplicatie etc. Deze vorm van encryptie wordt veelvuldig toegepast, immers data in transit is kwetsbaar voor ongeoorloofde toegang. De regel is dat alle vertrouwelijke informatie 'in transit' encrypt moet zijn.
2. Encryptie van 'data at rest', dat wil zeggen encryptie van data dat is opgeslagen in een database, op een (deel van) een disk, in een 'filesystem' etc. Afhankelijk van de technische mogelijkheden is het belangrijk om encryptie zo goed mogelijk toe te passen op vertrouwelijke informatie 'at rest'.

Artikel 34 van de AVG geeft aan dat een melding aan de betrokkenen niet verplicht is als de gelekte persoonsgegevens op de juiste wijze zijn versleuteld (encrypted) en daardoor voor onbevoegden onbegrijpelijk zijn geworden. Een verloren usb-stick met persoonsgegevens die met de juiste encryptie is

beveiligd hoeft niet gemeld te worden aan de betrokken personen (wel aan de Autoriteit Persoonsgegevens).

De ODRU dient te borgen dat zij op de juiste plekken encryptie toepast om zodoende een passende vertrouwelijkheid en integriteit van persoonsgegevens te realiseren. De ODRU past o.a. de volgende encryptie toe:
1. Beveiligde (https) websites
2. Het verzenden van bestanden via Secure FTP
3. Het versturen van versleutelde e-mail berichten en het versleutelen van e-mailbijlagen. Versleutelen van de database en de backups
4. Versleutelen van de laptops

### Paragraaf 10.8 Toegangscontrole

Artikel 32 stelt ook beperkingen aan de toegang tot persoonsgegevens. Die mogen alleen toegankelijk zijn voor personen die van de 'verwerkingsverantwoordelijke' de opdracht hebben gekregen om ze te verwerken.

De ODRU heeft onderstaande processen voor autorisatie en authenticatie geïmplementeerd voor een veilige toegang:
1. Medewerkers krijgen op basis van hun rol rechten toegewezen waarmee ze wel of niet toegang hebben tot persoonsgegevens.
2. Wachtwoordbeleid
3. Twee factor authenticatie
4. Logging en monitoring van onbevoegde toegang

De ODRU dwingt in de Verwerkersovereenkomsten vergelijkbare maatregelen af voor haar Verwerkers.

De ODRU treft diverse organisatorische maatregelen om er voor te zorgen dat persoonsgegevens zorgvuldig worden verwerkt. Medewerkers, waaronder inhuur en externen, hebben een geheimhoudingsplicht. Ook is het van belang dat alleen geautoriseerde medewerkers werken met persoonsgegevens. Waarbij zij tevens weten wat hun verantwoordelijkheid is ten aanzien van de omgang met deze persoonsgegevens en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Het is dus belangrijk dat de medewerkers van de ODRU zich bewust zijn van de regels en gedragsnormen rondom privacy. Deze organisatorische maatregelen dragen ook bij aan een bewustwording binnen de organisatie. Denk hierbij aan het ontwikkelen van specifieke privacy protocollen en afwegingskaders. Organisatorische maatregelen die de ODRU neemt, bestaan onder meer uit het vergroten van het privacy bewustzijn van de medewerkers en personen werkzaam bij of voor de ODRU. Het vergroten van het privacy bewustzijn wordt onder meer bereikt door het ondersteunen van de medewerkers door privacy trainingen en kennissessies. De medewerkers moeten zich bewust zijn van het belang van privacy. Zo moeten zij persoonsgegevens verwerken zoals is bepaald in het privacybeleid en de bijbehorende documentatie.

### Paragraaf 10.9 Aantonen door certificering

Volgens de AVG is certificering of het aansluiten bij een erkende certificering één van de middelen om te laten zien dat een organisatie passende technische en organisatorische maatregelen heeft genomen. Het is op moment van schrijven echter nog niet duidelijk welke certificeringen er worden gezien als voldoende.

De ODRU heeft een, op de NEN/ISO 27002 gebaseerd, basisbeveiligingsniveau voor alle informatie en informatiesystemen van de ODRU; de zogenaamde baseline informatiebeveiliging. Deze eigen baseline is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). De BIO biedt een raamwerk om passende maatregelen te treffen om compliant te zijn aan de AVG.

### Paragraaf 10.10 Evaluatie

De AVG dwingt organisaties om te controleren of de geïmplementeerde maatregelen effectief genoeg zijn. Dit kan onder andere door het uitvoeren van in- en externe audits en penetratietesten.

De ODRU evalueert de privacy en informatiebeveiligingsmaatregelen als volgt:
1. Periodiek worden externe security audits uitgevoerd;
2. De FG en Adviseur Informatiebeveiliging en Privacy voert periodiek een interne audit uit

De ODRU dwingt in de Verwerkersovereenkomsten vergelijkbare maatregelen af voor haar Verwerkers.

## Hoofdstuk 11 Datalekken

### Paragraaf 11.1 Definitie van een datalek

Een datalek is iedere inbreuk op de beveiliging waarbij persoonsgegevens verloren zijn gegaan, of ongeoorloofd zijn gewijzigd, verstrekt of ingezien. Er wordt dan ook wel gesproken van een "onrechtmatige verwerking".

- Er is sprake van onbedoeld verlies van persoonsgegevens
  Dit houdt in dat de ODRU deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan. Bijvoorbeeld als een USB-stick met persoonsgegevens erop kapot is gegaan en er geen back-up van deze gegevens is.

- Er is sprake van onrechtmatige aanpassing of beschadiging van persoonsgegevens
  Bijvoorbeeld als een bankrekeningnummer van een medewerker ten onrechte is aangepast in de salarisadministratie.

- Er is sprake van onrechtmatige toegang tot persoonsgegevens
  Hieronder vallen bijvoorbeeld e-mails die aan de verkeerde persoon zijn gestuurd of persoonsgegevens die per ongeluk zijn gepubliceerd.

Er is nadrukkelijk geen sprake van een datalek wanneer redelijkerwijs kan worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt. Bijvoorbeeld:
- Wanneer er na een hack expliciet kan worden vastgesteld dat de aanvaller geen toegang heeft gehad tot die specifieke database met klantgegevens.
- Wanneer de gegevens op een gestolen USB-stick of harde schijf van een gestolen laptop versleuteld zijn.

Wanneer een onrechtmatige verwerking niet kan worden uitgesloten dient er een datalek te worden gemeld. Zie ook het onderstaande schema opgesteld door de Autoriteit Persoonsgegevens.
Onder de Algemene Verordening Gegevensbescherming (AVG) is het verplicht om datalekken met ernstige gevolgen voor personen wiens persoonsgegevens het betreft binnen 72 uur na ontdekking te melden bij de Autoriteit Persoonsgegevens (AP). In een aantal gevallen dient het ook aan de betrokkene (de persoons wiens persoonsgegevens het betreft) gemeld te worden Voor de beoordeling van het datalek wordt de Richtsnoer Datalekken gevolgd. [15]

De ODRU heeft de volgende maatregelen getroffen op het gebied van datalekken:
1. Er is een werkinstructie en procedure voor het melden van datalekken beschikbaar gesteld op intranet.
2. De ODRU beschikt over middelen om vast te stellen of er sprake is van datalekken. Denk bijvoorbeeld aan logging en monitoring.
3. De ODRU maakt afspraken met Verwerkers over datalekken in de verwerkersovereenkomst.
4. Datalekken worden geanalyseerd en er worden passende maatregelen getroffen, zodat herhaling van het datalek voorkomen wordt.

### Paragraaf 11.2 Inbreukenregister

De AVG verplicht verwerkingsverantwoordelijke tot het documenteren van alle inbreuken in verband met persoonsgegevens, inclusief de gevolgen en de genomen maatregelen om dit in de toekomst te voorkomen (artikel 33 lid 5). Ook wanneer deze inbreuken nadrukkelijk niet hebben geleid tot een datatalek. De Autoriteit Persoonsgegevens kan toegang verlangen tot deze documentatie (artikel 58 lid 1 punt a), en de documentatie moet adequaat zijn om de toezichthouder te laten controleren of datalekken daadwerkelijk worden gemonitord en opgevolgd.
Onder ‘inbreuk in verband met persoonsgegevens’ wordt verstaan; wanneer persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt. Zie ook artikel 4 lid 12 voor de definitie in de AVG.

De ODRU beschikt over een inbreukenregister waarin alle inbreuken in relatie tot persoonsgegevens worden vastgelegd. Dit inbreukenregister is conform de eisen die de AVG hieraan stelt.
De FG rapporteert periodiek over datalekken aan het MT en het bestuur van de ODRU.

## Hoofdstuk 12 Aanvullende maatregelen vanuit de Wet Politiegegevens

### Paragraaf 12.1 Achtergrond van de Wpg

De verwerking van persoonsgegevens door boa’s viel tot 28 mei 2018 onder de Wet bescherming persoonsgegevens (Wbp). Met de komst van de AVG valt de verwerking van persoonsgegevens voor voorkoming van, onderzoek naar, opsporing van en vervolging van strafbare feiten onder een andere Europese wet, namelijk de EU-Richtlijn 2016/680. Deze richtlijn is omgezet in een nationale wet, namelijk de Wet politiegegevens (Wpg). Deze wet is aangevuld met het Besluit politiegegevens (Wpg). Deze wet en bijbehorend besluit zijn sinds 1 januari 2019 van kracht. Vanaf dat moment is er één wettelijk regime

15 Zie voor meer informatie de Guidelines Meldplicht Datalekken, geraadpleegd op 12-05-2020:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf

voor de verwerking van persoonsgegevens in de strafrechtelijke keten. Daarvoor bestond de situatie dat voor delen van de keten de Wbp en voor andere delen de Wpg van kracht was. Per 9 maart 2019 is tevens het Besluit politiegegevens buitengewoon opsporingsambtenaren van kracht geworden. Daarin staan bepalingen inzake de overeenkomstige toepassing van de Wpg op de verwerking van persoonsgegevens door personen die als buitengewoon opsporingsambtenaar zijn belast met de opsporing van strafbare feiten.

**Paragraaf 12.2 Wat blijft hetzelfde onder de Wpg?**

De werkgever van de boa blijft verantwoordelijk voor de verwerking van persoonsgegevens volgens de Memorie van Toelichting bij de wetswijziging. Verder is in de EU-richtlijn 2018/680, waarop de Wpg is gebaseerd, aansluiting gezocht bij de AVG. Dat betekent dat organisaties die de AVG hebben geïmplementeerd voor een belangrijk deel ook voldoen aan de eisen die de Wpg stelt. Denk hierbij aan de volgende verplichtingen: de meldplicht datalekken, het uitvoeren van DPIA's en het aanstellen van een Functionaris Gegevensbescherming (FG).

Daarnaast blijven onderstaande verplichtingen die ook onder de Wpb al gelden van kracht [16]:

1. Politiegegevens worden alleen aan geautoriseerde politieambtenaren in andere organisaties beschikbaar gesteld voor zover nodig voor de uitvoering van hun taak. Wel kan een werkgever besluiten om specifieke verwerkingen uit te laten voeren door niet-Boa's;
2. In de dagelijkse uitvoering van taken wordt alleen toegang verleend tot gegevens ouder dan 1 jaar op basis van een relatie met actuele gegevens;
3. Bij verstrekking van onjuiste of onrechtmatig verkregen gegevens moet de ontvanger worden geïnformeerd;
4. Gegevens uit de dagelijkse uitvoering van taken moeten na 5 jaar worden vernietigd;
5. Gegevens ten behoeve van een onderzoek moeten na maximaal een halfjaar worden verwijderd als ze niet langer nodig zijn voor het onderzoek, maar ze mogen pas na 5 jaar worden vernietigd;
6. Er bestaat een verplichting tot privacy-audits met rapportage aan de Autoriteit Persoonsgegevens (AP), te weten twee jaar na inwerkingtreding en daarna elke 4 jaar;
7. Er moet een privacyfunctionaris worden benoemd, niet te verwarren met de FG

**Paragraaf 12.3 Wat verandert er onder de Wpg?**

Onderstaand overzicht beperkt zich tot de afwijkingen van en aanvullingen op de AVG. Het gaat in hoofdlijnen om het volgende:

1. De boa heeft bijna altijd ook bestuursrechtelijke toezichts- en handhavingstaken. Een boa krijgt daarom bij het verwerken van persoonsgegevens zowel met de AVG te maken als met de Wpg. In de verwerking van gegevens moet dus duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg.
2. Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd. (Wpg 4.3)
3. Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden. (Wpg 6b)
4. Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens. (Wpg 32a, Bpg 6:1a.3g)
5. Er worden specifieke eisen gesteld aan de informatiebeveiliging die in het aangepaste Besluit politiegegevens zijn opgenomen.
6. Belangrijk is dat zaken – vaak nog meer dan in het verleden - gedocumenteerd moeten worden binnen de Wpg, namelijk:
   - doelen van onderzoeken
   - verstrekking of doorgifte
   - afwijzing van verzoeken om inzage
   - inbreuk op de beveiliging
   - doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens
   - melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens

16 Bron: https://www.bmc.nl/binaries/content/assets/bmcnl/pdfs/bmc-folderwet-politiegegevens-2019_lr.pdf

### Paragraaf 12.4 Waar moet de ODRU volgens de Wet politiegegevens aan voldoen?

De ODRU moet volgens de Wet politiegegevens (Wpg) aan een aantal vereisten voldoen bij de verwerking van gegevens. Voor de verwerking van politiegegevens stelt de Wpg net als de AVG een aantal algemene criteria. Dit betreft criteria over noodzakelijkheid, rechtmatigheid, juistheid, proportionaliteit, subsidiariteit en volledigheid. Daarnaast moet de Verwerkingsverantwoordelijke een aantal technische en organisatorische maatregelen nemen. [17]

1. Inspanningsverplichting verwerkingsverantwoordelijke
   De ODRU moet zorgen voor procesinrichting voor verwerking van verschillende soorten gegevens waarmee opzet, bestaan en werking aangetoond wordt (artikel 4a Wpg).

2. Beveiliging
   De ODRU moet technische en organisatorische beveiligingsmaatregelen voor onder andere het verlenen van toegang tot politiegegevens opstellen. Deze toegang kan worden verleend aan personen die gelet op hun functie, de aard van de verwerking van politiegegevens en het doel ervan, noodzakelijkerwijs moeten werken met deze gegevens. Dit kan gaan om fysieke maatregelen zoals toegangszonering of digitale maatregelen als autorisatiebeheer, identiteitsmanagement, beheer van toegangs- en gebruikersrechten (zie ook artikel 4a Wpg).

3. Gegevensbeschermingseffectbeoordeling (GEB)
   De Wpg stelt een GEB verplicht op verwerkingen van politiegegevens die een hoog risico inhouden voor de privacy van burgers. Dit geldt met name voor verwerkingen waarbij nieuwe technologieën worden ingezet (zie artikel 4c Wpg).

4. Rechten betrokken burgers
   Burgers hebben mogelijk recht op informatie over verwerking van politiegegevens. Dit kan een actieve informatieplicht zijn waarbij de gemeente initiatief moet nemen om betrokken burgers te informeren, maar kan ook gaan om een passieve informatieplicht op verzoek van een burger. Dergelijke verzoeken kunnen geheel of gedeeltelijk worden afgewezen als dit de opsporing en vervolging belemmert (artikel 24a t/m 28 Wpg).

5. Registerplicht
   De registerplicht houdt in dat de gemeente – net als onder de AVG – voorziet in het beschrijven van alle verwerkingsactiviteiten in algemene zin, om dit vervolgens op te nemen in een register (artikel 31d Wpg).

6. Meldplicht datalekken
   Er is – net als onder de AVG – een meldplicht voor datalekken bij de Autoriteit Persoonsgegevens. Deze melding kan worden uitgesteld, beperkt of achterwege worden gelaten als dat bijvoorbeeld opsporing, vervolging of berechting belemmert (artikel 33a Wpg).

7. Documentatieplicht
   De documentatieplicht staat voor documentatie van belangrijke verwerkingen, zoals verstrekking politiegegevens aan derden, redenen voor afwijzing inzage- of correctieverzoek en alle inbreuken op de beveiliging van persoonsgegevens (artikel 32 Wpg).

8. Voorwarden ICT-systeem
   Als een bestaand ICT-systeem wordt gebruikt voor de verwerking van politiegegevens, moet dit systeem 'Wpg-proof' zijn. Vereisten zijn een autorisatiestelsel, termijnbewaking van gegevens, onderscheid kunnen maken tussen soorten politiegegevens (gegevens verdachten, slachtoffers, getuigen of contactpersonen) en een op komst zijnde loggingsverplichting.

## Hoofdstuk 13 Non compliance risico

De AP kan boetes opleggen bij overtredingen van de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet van de AVG. De AP kan ook bij overtredingen op grond van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens een boete opleggen.
Bij het vaststellen van (de hoogte van) de boete houdt de AP in eerste instantie rekening met het maximale bedrag van de boete dat in de wet is vermeld. De AVG kent twee categorieën van overtredingen en bijbehorende maximale boetes.

17 Bron: https://www.stimulansz.nl/de-wet-politiegegevens/

1. Verantwoordelijken, degenen die persoonsgegevens verwerken, hebben onder de AVG bepaalde verplichtingen, zoals de verplichting van het bijhouden van een verwerkingsregister. Komt een verantwoordelijke (een van) deze verplichtingen niet na? Dan kan de AP een boete opleggen van maximaal 10 miljoen euro. Of een boete van maximaal 2% van de wereldwijde jaaromzet van een onderneming, mocht dat bedrag hoger uitkomen.
2. Overtreedt een verantwoordelijke de beginselen of grondslagen van de AVG? Of de privacyrechten van de betrokkenen? Dan kan de AP een boete opleggen van maximaal 20 miljoen euro. Of een boete van maximaal 4% van de wereldwijde jaaromzet van een onderneming, mocht dat bedrag hoger uitkomen.

Een boete door de handhavende instantie is echter niet het enige risico als volg van onzorgvuldige omgang met persoonsgegevens. In de volgende paragrafen volgen nog een aantal voorbeelden van mogelijke risico's binnen een AVG context.

*13.1 Voorbeelden van organisatierisico's*

1. Negatieve publiciteit en imagoschade;
2. Dwangmaatregelen of boetes opgelegd door de toezichthouder wegens het niet naleven van de wetgeving;
3. Schadeclaims door betrokkenen;
4. Hogere kosten bij het achteraf nemen van privacy maatregelen;
5. Slechte datakwaliteit leidt tot slechtere performance van de business;
6. Datalekken leiden tot wantrouwen.

*13.2 Voorbeelden van juridische risico's*

1. Niet naleving van privacy regelgeving
2. Niet naleving van sectorale regelgeving;
3. Niet naleving van mensenrechten.

*13.3 Voorbeelden van risico's voor de betrokkene*

1. De mogelijkheid om anoniem gebruik te make van bepaalde diensten wordt gefrustreerd;
2. Persoonsgegevens worden gedeeld en gebruikt op onrechtmatige wijze;
3. Persoonsgegevens worden gebruikt voor doeleinden waar de betrokkenen niet van op de hoogte zijn;
4. Het koppelen van systemen kan ertoe leiden dat meer persoonsgegevens worden gebruikt dan noodzakelijk;
5. Kwetsbare groepen personen worden eerder het slachtoffer van oneigenlijk gebruik van hun persoonsgegevens en kunnen hierdoor gevolgen van ondervinden als uitsluiting, discriminatie of stigmatisering.
6. Persoonsgegevens worden niet of onjuist gemanaged waardoor er een wildgroei aan bestanden met persoonsgegevens ontstaat; hierdoor stijgen de veiligheidsrisico's.

## Hoofdstuk 14 Bronnen

Bij het opstellen van dit privacybeleid zijn de onderstaande bronnen geraadpleegd.

1. CIP Privacy Baseline v3.0: https://www.cip-overheid.nl/wpcontent/uploads/2017/05/20170509%20Privacy%20Baseline%20v3_0.pdf
2. Boek: "De Algemene Verordening Gegevensbescherming Editie 2017" door Arnoud Engelfriet, Lisette Meij, Peter Kager. ISBN: 9789082083446. Eerste druk.
3. Whitepaper AVG – GDRP van Stimmt B.V.
4. Factsheet meldplicht datalekken: https://ictrecht.nl/factsheets/impact-van-de-meldplichtdatalekken/
5. PIA vragenlijst door Norea: https://www.norea.nl/download/?id=522
6. https://www.baaten.com/kennis/wet-en-regelgeving-informatiebeveiliging/europese-privacywetavg/
7. https://ictrecht.nl/2017/01/05/artikel-29-werkgroep-richtlijnen-functionarisgegevensbescherming-fg/
8. Guideline on Data Protection Officers: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243_rev01_enpdf_0.pdf

9. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/functionarisvoor-de-gegevensbescherming-fg
10. https://www.baaten.com/kennis/wet-en-regelgeving-informatiebeveiliging/persoonsgegevensbuiten-europa/
11 http://dirkzwagerieit.nl/2017/12/13/uitvoeringswet-avg-uavg-gepubliceerd-eerste-analyse/
12 Wetsvoorstel Uitvoeringswet Algemene Verordening Gegevensbescherming
13 Memorie van toelichting op het wetsvoorstel van de Algemene Verordening Gegevensbescherming
14 Ontslagbescherming: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-dege-gevensbescherming
15 https://cms.law/nl/NLD/Publication/Privacy-de-begrippen-verantwoordelijke-en-bewerker-nader-uitgelegd
16 Opinion 1/2010 on the concepts of "controller" and "processor" – http://ec.europa.eu/justice/da-taprotection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
17 https://www.it-jurist.nl/nieuws/testen-met-productie-data-mag-dat
18 https://www.nederlandict.nl/news/avg-uitgelegd-deel-3-privacy-by-design-privacy-by-default/
19 Guidelines DPIA door WP29- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/fi-les/wp248_rev.01_nl.pdf
20 https://www.kneppelhout.nl/actueel/wanneer-is-een-data-protection-impact-assessment-dpiavereist
21 https://www.vijverbergjuristen.nl/publicaties/gemeenschappelijke-regelingverwerkingsverantwoor-delijke-of-verwerker-als-bedoeld-in