gemeente Opsterland

GEMEENTEBLAD

Officiële uitgave van de gemeente Opsterland

Nr. 580585

30 december 2022

Privacybeleid 2022 - 2026

1. Inleiding

Binnen de gemeente Opsterland werken we met veel persoonsgegevens van inwoners, ondernemers en medewerkers. Wij verwerken deze gegevens om onze wettelijke taken en verplichtingen uit te voeren. Mensen die hun persoonsgegevens aan onze gemeente toevertrouwen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig omgaat met hun gegevens.

De Algemene verordening gegevensbescherming (hierna: AVG) legt meer verantwoordelijkheden bij organisaties zelf. Van organisaties wordt namelijk verwacht dat zij aan kunnen tonen dat zij persoonsgegevens op een veilige manier verwerken. Dit noemt men in de AVG de 'verantwoordingsplicht'. Organisaties zijn gehouden om aan deze verantwoordingsplicht te voldoen. Zo moet er onder andere worden aangetoond dat een verwerking aan de beginselen van gegevensverwerking voldoet, zoals: rechtmatigheid, transparantie, doelbinding en juistheid. Ook moet een organisatie kunnen laten zien dat passende technische en organisatorische maatregelen zijn genomen om de persoonsgegevens te beveiligen. De AVG verplicht overheidsorganisaties als gemeenten om hiervoor een privacybeleid op te stellen.

Het privacybeleid stelt het kader en de algemene uitgangspunten voor de verwerking van persoonsgegevens bij de gemeente Opsterland. Daarnaast biedt het privacybeleid inzicht in gemaakte keuzes rondom de verwerking van persoonsgegevens, waardoor de gemeente voldoet aan de verantwoordingsplicht die op haar rust. Tot slot blijkt uit het privacybeleid dat de gemeente haar werkzaamheden conform de AVG uitvoert.

Het beleid wordt vastgesteld door het College van Burgemeester en Wethouders (hierna: het college) van de gemeente Opsterland en wordt jaarlijks geëvalueerd en waar nodig geactualiseerd. De penvoerder van het beleid is de Privacy Officer van de gemeente Opsterland. De Functionaris gegevensbescherming bewaakt een tijdige evaluatie en deelt de uitkomsten hiervan met het College, tezamen met een voorstel voor het actualiseren van het privacybeleid.

Indien nodig wordt in het beleid verwezen naar bestaande procedures van de gemeente Opsterland. Ook wordt in het beleid worden verwezen naar documenten of procedures die in de nabije toekomst worden opgemaakt.

2. Uitgangspunten

De gemeente Opsterland is haar bewust van haar voorbeeldfunctie in de regio en hecht grote waarde aan het waarborgen van de privacy van haar inwoners en werknemers.

Alle medewerkers van de gemeente zijn verantwoordelijk voor het correct omgaan met persoonsgegevens, zij zijn bekend met het privacybeleid.

Voor specifieke werkterreinen binnen de gemeente (denk bijvoorbeeld aan het sociaal domein, Human Resource Management, etc.) kunnen aanvullende werkwijzen worden vastgesteld voor wat betreft de omgang met persoonsgegevens.

Voor inwoners en andere betrokkenen is het beleid rondom de verwerking van persoonsgegevens door de gemeente Opsterland op internet te raadplegen in de vorm van de privacyverklaring.

De gemeente besteedt aandacht aan privacy in afspraken met derde partijen. Gemaakte afspraken worden vastgelegd in convenanten en overeenkomsten in het kader van persoonsgegevensverwerking.

De gemeente streeft ernaar aan alle eisen van de wet- en regelgeving in het kader van privacy te voldoen en neemt hiervoor de benodigde maatregelen. Het uitgangspunt van de gemeente is dat zij, met de beschikbare middelen, alle mogelijke en redelijke maatregelen treft om ervoor te zorgen dat alle onderdelen van de persoonsgegevensverwerking conform de privacywetgeving worden uitgevoerd.

Het veilig verwerken van persoonsgegevens is een doorlopend proces. Voor de onderdelen van de persoonsgegevensverwerking die op dit moment nog niet (volledig) voldoen aan de wet- en regelgeving

in het kader van privacy, geldt dat de gemeente de intentie heeft om, zonder onredelijke vertraging, de noodzakelijke maatregelen te nemen voor deze onderdelen.

3. Juridisch kader

3.1 Algemene wetgeving

De belangrijkste eisen rondom privacy en gegevensbescherming zijn opgenomen in de AVG. Dit is een Europese Verordening die rechtstreeks van toepassing is in alle lidstaten van de Europese Unie (hierna: EU). De AVG biedt in sommige gevallen ruimte om nadere wetgeving te maken op nationaal niveau. In Nederland is hieraan invulling gegeven in de Uitvoeringswet AVG (hierna: UAVG).

3.2 Toepasselijkheid Algemene verordening gegevensbescherming

De AVG benoemt twee verschillende toepassingsgebieden op basis waarvan kan worden vastgesteld of de AVG van toepassing is op de betreffende verwerking. Deze toepassingsgebieden zijn het '*materiële toepassingsgebied*' en het '*territoriale toepassingsgebied*'.

Als verwerkingen van persoonsgegevens voldoen aan de eisen van beide toepassingsgebieden geldt dat de AVG van kracht is op deze verwerkingen. De gemeente dient er dan zorg voor te dragen dat deze verwerkingen conform de AVG worden uitgevoerd.

Materieel toepassingsgebied

Het materiële toepassingsgebied stelt dat de AVG van toepassing is op het moment dat persoonsgegevens geheel of gedeeltelijk geautomatiseerd worden verwerkt of wanneer persoonsgegevens in bestanden worden opgenomen of bestemd zijn om in bestanden te worden opgenomen.

Binnen de gemeente worden persoonsgegevens op verschillende manieren geheel of gedeeltelijk geautomatiseerd verwerkt. Denk hierbij bijvoorbeeld aan: het kunnen inloggen op het Citrixportaal, het gebruiken van persoonsgegevens uit de Basisregistratie Personen (hierna: BRP) en het opslaan van persoonsgegevens in het zaaksysteem.

Op basis van deze voorbeelden en een groot aantal andere verwerkingen van persoonsgegevens die binnen de gemeente worden uitgevoerd kan worden vastgesteld dat aan het materiële toepassingsgebied van de AVG wordt voldaan.

Territoriaal toepassingsgebied

Het territoriale toepassingsgebied stelt dat de AVG van toepassing is op het moment dat een verwerkingsverantwoordelijke of verwerker binnen de EU is gevestigd en persoonsgegevens verwerkt.

Aangezien de gemeente voor het uitvoeren van haar werkzaamheden kan worden aangemerkt als verwerkingsverantwoordelijke (uitgelegd in hoofdstuk 3.3), persoonsgegevens verwerkt en binnen de EU is gevestigd voldoet de gemeente ook aan het territoriale toepassingsgebied.

Omdat de gemeente bij de uitvoering van haar werkzaamheden voldoet aan zowel het materiële toepassingsgebied als het territoriale toepassingsgebied, kan worden vastgesteld dat de gemeente dient te voldoen aan de AVG.

3.3 Verwerkingsverantwoordelijke of verwerker

De AVG stelt dat de partij die het doel en de middelen van de verwerking van persoonsgegevens bepaalt, wordt aangemerkt als de partij die verantwoordelijk is voor de verwerking van persoonsgegevens, ofwel: de *verwerkingsverantwoordelijke*.

Naast de verwerkingsverantwoordelijke kent de AVG ook de verwerker. De verwerker is de partij die persoonsgegevens namens de verwerkingsverantwoordelijke verwerkt.

Bij bepaling van de rol (verwerkingsverantwoordelijke of verwerker) waarin de gemeente optreedt bij de verwerkingen van persoonsgegevens die zij uitvoert, zijn de richtlijnen die de AVG hiervoor geeft leidend.

3.4 Specifieke wetgeving

Naast de AVG en de UAVG als algemene wetgeving kan specifieke wetgeving ook bepalen op welke wijze de gemeente omgaat met persoonsgegevens. Voor de gemeente zijn onder andere de volgende specifieke wetten van toepassing voor wat betreft het verwerken en beschermen van persoonsgegevens:

- Wet maatschappelijke ondersteuning 2015 (Wmo);
- Participatiewet;
- Jeugdwet;

- Wet gemeentelijke schuldhulpverlening;
- Wet geneeskundige behandelingsovereenkomst;
- Wet basisregistratie personen (Wet BRP);
- Wet algemene bepalingen burgerservicenummer;
- Wet politiegegevens;
- Archiefwet;
- Telecommunicatiewet;
- Kieswet;
- Wet open overheid (WOO).

Bepalingen in specifieke wetgeving over de verwerking van persoonsgegevens gaan voor op het algemeen wettelijk kader.

Wijzigingen binnen bestaande (specifieke) wetgeving of toevoeging van nieuwe (specifieke) wetgeving, welke van toepassing is op de verwerking van persoonsgegevens binnen de gemeente, worden continu bewaakt.

4. Bevoegd toezichthoudende autoriteit

De AVG bepaalt dat iedere lidstaat van de EU een nationale toezichthouder instelt. Deze toezichthouder is verantwoordelijk voor het controleren van de naleving van de AVG en treedt hierin volledig onafhankelijk op. In Nederland is dit de Autoriteit Persoonsgegevens (hierna: AP). Het doel van de AP is om op deze manier de grondrechten (bijv. het recht op privacy) en fundamentele vrijheden (bijv. vrijheid van meningsuiting) van mensen te beschermen.

Op het terrein van telecomdiensten is ook de toezichthouder Autoriteit Consumenten en Markt (hierna: ACM) actief. De ACM ziet onder andere toe op het naleven van de wetgeving over het gebruik van cookies op websites.

4.1 De taken van de toezichthoudende autoriteit

De AP heeft de verantwoordelijkheid gekregen om toe te zien op de naleving van de AVG. Maar, dit is niet de enige taak van de AP. Enkele andere taken van de AP worden hieronder opgesomd:

- het informeren van organisaties over hun verplichtingen die volgen uit te wettekst van de AVG;
- het informeren van het brede publiek over risico's op het gebied van verwerking van persoonsgegevens;
- het informeren van betrokkenen over de rechten die zij hebben op grond van de AVG;
- het behandelen van klachten in verband met de verwerking van persoonsgegevens;
- het adviseren van de regering en/of het parlement over nieuwe wet- en regelgeving;
- het adviseren van organisaties over verwerkingen van persoonsgegevens.

Uit bovenstaande volgt dat de AP niet alleen als taak heeft om te controleren op de naleving van de AVG, maar een veel breder takenpakket heeft. Een groot onderdeel van dit takenpakket betreft het informeren en adviseren inzake de toepassing van de AVG en het bekendmaken van de risico's die er bestaan met betrekking tot het verwerken van persoonsgegevens.

4.2 De bevoegdheden van de toezichthoudende autoriteit

De AP heeft drie verschillende soorten bevoegdheden. Deze bevoegdheden kunnen worden onderscheiden in de volgende drie categorieën:

- onderzoeksbevoegdheden;
- de bevoegdheid tot het nemen van corrigerende maatregelen;
- autorisatie- en adviesbevoegdheden.

<u>Onderzoeksbevoegdheden</u>

Onderzoeksbevoegdheden geven de AP de mogelijkheid om binnen een organisatie onderzoek uit te voeren naar de naleving van de AVG. De organisatie waarbinnen het onderzoek plaatsvindt kan worden verplicht alle benodigde informatie aan de AP te verstrekken. Ook dient de AP toegang te verkrijgen tot alle bedrijfsruimten, als zij dit noodzakelijk acht voor het onderzoek.

<u>De bevoegdheid tot het nemen van corrigerende maatregelen</u>

Op het moment dat de AP heeft vastgesteld dat een organisatie in overtreding van de AVG is, kan zij corrigerende maatregelen nemen. De corrigerende maatregel(en) worden opgelegd met als doel de onrechtmatige werkwijze van de organisatie te veroordelen en ervoor te zorgen dat de organisatie zo spoedig mogelijk passende maatregelen neemt om te voldoen aan de AVG. Enkele corrigerende maatregelen worden hieronder opgesomd:

- het geven van een waarschuwing;
- het opleggen van een tijdelijke of definitieve verwerkingsbeperking;
- het opleggen van een administratieve geldboete tot maximaal €20.000.000 of 4% van de totale wereldwijde jaaromzet.

Autorisatie- en adviesbevoegdheden
De autorisatie- en adviesbevoegdheden geven de AP de mogelijkheid om organisaties en de regering en/of het kabinet advies te verstrekken met betrekking tot het naleven van de AVG. De AP heeft, onder andere door deze bevoegdheden, niet alleen een toezichthoudende rol, maar ook een adviserende rol.

5. Governance

De governance beschrijft de wijze waarop de gemeente Opsterland de besturing en besluitvorming rondom privacy heeft georganiseerd en welke rollen zijn belegd. Elke rol heeft specifieke taken, verantwoordelijkheden en bevoegdheden. Het samenspel tussen deze rollen zorgt ervoor dat het privacybeleid is verankerd binnen de gemeente.

5.1 Rollen, taken, verantwoordelijkheden en bevoegdheden

- ***Het college (burgemeester en wethouders)***

Het college is de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens voor een groot aantal gemeentelijke taken en tevens eindverantwoordelijk voor privacy en gegevensbescherming binnen de gemeente Opsterland. Het college legt verantwoording af over de privacy beleidsvoering aan de gemeenteraad. Met het bekrachtigen van het privacybeleid belegt het college de uitvoering en naleving hiervan bij het ambtelijk apparaat.

- ***De bestuurder***

Het collegelid met het beleidsgebied privacy en gegevensbescherming in de portefeuille vertegenwoordigt op dit gebied het College van B&W. Het collegelid heeft over dit gebied veelvuldig overleg met de teammanager bij wie privacy is belegd, met de Functionaris voor gegevensbescherming en met de Chief information security Officer.

- ***Gemeentesecretaris/ eindverantwoordelijkheid op ambtelijk niveau***

De gemeentesecretaris is de hoogste ambtenaar binnen de ambtelijke organisatie, en de eerste adviseur van het college. De gemeentesecretaris vormt de schakel tussen het bestuur en de ambtelijke organisatie en is in het kader van privacy ambtelijk eindverantwoordelijk.

- ***Directieteam***

De gemeentesecretaris vormt samen met de directieleden het directieteam (hierna: DT). Het DT is verantwoordelijk voor de vertaling en uitvoering van het privacybeleid naar de organisatie. Het DT stelt kaders en geeft sturing ten aanzien van privacy op tactisch en operationeel niveau, evalueert beleidskaders en controleert of de uitvoering van de (U)AVG in de organisatie voldoende is geborgd en wordt nageleefd.

Het DT stuurt op risico's, controleert of beveiligingsmaatregelen effectief de persoonsgegevens beschermen, ondersteunt de evaluatie van het privacybeleid en zorgt ervoor dat de Functionaris voor gegevensbescherming tijdig wordt betrokken bij alle aangelegenheden die verband houden met de verwerking, dan wel bescherming van persoonsgegevens.

Het DT is er tevens verantwoordelijk voor dat medewerkers adequaat zijn getraind voor het veilig verwerken van persoonsgegevens en moet dat kunnen aantonen.

- ***Teammanager***

Binnen de afdelingen zijn de teammanagers verantwoordelijk voor de naleving van de privacywetgeving en het privacybeleid op uitvoeringsniveau.

De teammanager voert binnen zijn team regie op de privacy bestendigheid van de werkprocessen en bijbehorende gegevensverwerkingen.

- ***Proceseigenaar***

De proceseigenaar is verantwoordelijk voor een of meer bedrijfsprocessen, zowel op tactisch als operationeel niveau. De proceseigenaar is daarmee ook verantwoordelijk voor de borging van de AVG binnen dat proces en het actueel houden van het verwerkingsregister. De proceseigenaar wordt hierbij ondersteund door de Privacy Officer.

Als procesverantwoordelijke is de proceseigenaar zich bewust van de privacyrisico's die verband houden met de verwerking van persoonsgegevens en voorziet hij/zij in praktische oplossingen waarmee hij/zij die risico's tegengaat. De proceseigenaar voert hiervoor onder andere, gezamenlijk met de Privacy Officer en/of de Functionaris voor gegevensbescherming en de CISO, data protection impact assessments (hierna: DPIA) uit.

De Functionaris voor gegevensbescherming rapporteert aan het directieteam over de privacy activiteiten die binnen het team hebben plaatsgevonden. De Functionaris voor gegevensbescherming wint hiervoor eventueel informatie in bij de proceseigenaar.

Taken van de proceseigenaren in het kader van privacy zijn:
- het vergroten van het bewustzijn omtrent privacy binnen het team;
- het borgen van de AVG binnen de eigen processen;
- het uitdragen van het privacybeleid op de medewerkers binnen het team;
- het toepassen van het privacybeleid en de daaraan gerelateerde procedures binnen de eigen processen;
- het leveren van input voor wijzigingen op maatregelen en procedures;
- het vroegtijdig betrekken van de Functionaris voor gegevensbescherming of de Privacy Officer bij aanpassingen van bestaande processen of nieuwe processen;
- managen van gesloten overeenkomsten in het kader van het verwerken van persoonsgegevens met derden, zoals: verwerkersovereenkomsten, overeenkomsten gegevensuitwisseling;
- bespreking van privacy incidenten en de mogelijke gevolgen voor beleid en maatregelen.

Wanneer gemeentelijke processen zodanig zijn georganiseerd dat de onderliggende gegevensverwerking onder de verantwoordelijkheid van meerdere proceseigenaren valt, is een door de gemeentesecretaris aan te wijzen proceseigenaar coördinator en procesverantwoordelijke.

- ***Inkoop***

De afdeling Inkoop is betrokken bij de inkoop van diensten en producten. Als er een DPIA is uitgevoerd op de betreffende diensten of producten, gebruikt de afdeling Inkoop de uit het DPIA verkregen informatie. Indien de aard van de samenwerking met de dienstverlener het sluiten van een verwerkersovereenkomst of andere overeenkomst inzake de verwerking van persoonsgegevens verplicht stelt, wordt de PO en eventueel juridische zaken in dit kader benaderd voor advies.

- ***Juridische zaken***

De afdeling Juridische Zaken adviseert bij privacyvraagstukken. Tevens analyseert en interpreteert juridische zaken de wet- en regelgeving op gebied van privacy, maakt de organisatie daarmee bekend en creëert awareness. De afdeling adviseert bij het sluiten van verwerkersovereenkomsten en andere overeenkomsten inzake de verwerking van persoonsgegevens en ICT contracten. Juridische Zaken kan tevens betrokken worden bij de uitvoering van DPIA's.

- ***Chief information security officer (hierna: CISO)***

De CISO ontwikkelt het beleid voor informatiebeveiliging, ondersteunt bij de implementatie van het informatiebeveiligingsbeleid en ziet toe op de naleving van dit beleid. Hij of zij adviseert bij de opzet van technische en organisatorische beheersingsmaatregelen in de DPIA's en ziet erop toe dat deze maatregelen effectief zijn. Tijdens de levensloop van de verwerkingen ziet de CISO toe op de effectieve werking van de maatregelen, legt de bevindingen vast en rapporteert hierover aan de directie. De CISO heeft tevens een rol in het identificeren, analyseren en afhandelen van (mogelijke) datalekken.

- ***Privacy Officer (hierna: PO)***

De PO ondersteunt het DT op haar aandachtsgebied. De PO heeft binnen dat gebied een operationeel uitvoerende rol en is het dagelijkse aanspreekpunt voor medewerkers wat betreft het verwerken van persoonsgegevens. Daar passen taken bij als adviseren over de procedures en de werkprocessen van de afdelingen, over het sluiten van verwerkersovereenkomsten en andere overeenkomsten inzake de verwerking van persoonsgegevens met externe partijen, het beheer van het verwerkingsregister en het coördineren van het proces rondom datalekken. Ook het opstellen, bijstellen, vernieuwen en herzien van het beleid dat de gemeente rondom privacy voert is een taak van de PO.

De PO voert controles uit op de effectieve werking van beheersingsmaatregelen en ondersteunt (eventueel gezamenlijk met de Functionaris voor gegevensbescherming) het DT bij het afleggen van verantwoording over de naleving van de AVG. De PO schakelt de Functionaris voor gegevensbescherming in bij (verplichte) adviestrajecten en legt zo nodig dilemma's voor.

- ***Alle medewerkers***

Het nakomen van het beleid is de verantwoordelijkheid van elke medewerker, ongeacht de positie binnen de gemeente. Bij alle taken moet steeds worden gedacht aan en gehandeld worden naar het belang van degene wiens persoonsgegevens worden verwerkt.

• ***Functionaris voor gegevensbescherming (hierna: FG)***
De FG houdt toezicht op de uitvoering en naleving van de AVG. De AVG stelt het aanstellen van een FG verplicht voor overheidsinstanties en publieke organisaties. De gemeente heeft een FG aangesteld die rapporteert aan het hoogste bestuursorgaan van de gemeente.

De werkzaamheden van de FG, haar positie en bevoegdheden hebben een wettelijke grondslag.

De FG ziet erop toe dat de gemeente voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. De FG toetst onder andere de naleving van de wettelijke eisen, gemeentelijke richtlijnen op het gebied van privacy en het privacy- en het informatiebeveiligingsbeleid. De FG is contactpersoon van de gemeente voor de AP.

De FG houdt toezicht op de uitvoering en naleving van de AVG binnen de gemeente Opsterland, geeft informatie, adviezen en doet aanbevelingen aan de organisatie en het college voor een verdere optimalisering van de privacy bedrijfsvoering en de omgang met persoonsgegevens. De FG ondersteunt en adviseert bij de uitvoering van een DPIA en ziet toe op de juiste procesgang bij het DPIA.

De FG wordt betrokken bij beslissingen die gevolgen hebben voor privacy en gegevensbescherming. Alle relevante informatie wordt tijdig gedeeld met de FG, zodat hij/zij passend advies kan verlenen.

De FG krijgt de nodige ruimte voor een professionele uitvoering van taken.
- Het college, het MT en de proceseigenaren zorgen ervoor dat de FG naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens.
- De FG wordt volledig geïnformeerd over aspecten van de bedrijfsvoering binnen de gemeente waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.
- Het college, het MT en de proceseigenaren ondersteunen de FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.
- De FG mag niet geïnstrueerd worden over invulling van taken, onder druk worden gezet, gestraft of ontslagen voor de uitvoering van zijn taken, tenzij de FG niet functioneert op basis van hetgeen in het kader van haar/zijn functie verwacht mag worden.

De FG brengt jaarlijks rechtstreeks verslag uit aan het college over de uitkomsten van haar toezichtstaak.

5.2 Planning en control
Aantoonbaar voldoen aan de AVG is een continu vereiste om aan de omgekeerde bewijslast van de privacy wet- en regelgeving te voldoen. Om de naleving van de AVG continu te waarborgen heeft de gemeente specifieke maatregelen genomen die ervoor zorgen dat de verwerking van persoonsgegevens blijft voldoen aan de privacywetgeving. Hetgeen ook de basis is voor de jaarlijkse verantwoording van het bestuur en van de FG.

De AVG biedt de gemeente het normenkader voor het voldoen aan de AVG. Gezien de ontwikkelingen in de digitale wereld is (de interpretatie van) de AVG continu in ontwikkeling. De gemeente streeft ernaar de benodigde maatregelen te nemen om de ontwikkelingen met betrekking tot de AVG te borgen. De periode waarbinnen de gemeente de benodigde maatregelen kan realiseren is afhankelijk van de ontwikkelingen binnen het normenkader. Wat in ieder geval geldt is dat de gemeente, met de middelen die zij ter beschikking heeft, haar inzet om zo spoedig mogelijk aan het normenkader te voldoen.

6. Beginselen inzake de verwerking van persoonsgegevens
6.1 Rechtmatigheid, behoorlijkheid en transparantie
Rechtmatigheid
De AVG eist dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag aangewezen dient te kunnen worden. Dit betekent dat een verwerking alleen mag plaatsvinden als één van de onderstaande zes grondslagen van toepassing is in de gegeven situatie:
1. indien de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
2. indien de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene onderdeel is;
3. indien de verwerking noodzakelijk is om aan een wettelijke verplichting te kunnen voldoen die op de verwerkingsverantwoordelijke rust;
4. indien de verwerking noodzakelijk is om de vitale belangen van een betrokkene of andere natuurlijke persoon te beschermen;

5. indien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;[1]
6. indien de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belanden van de verwerkingsverantwoordelijke of van een derde.

De gemeente mag haar, voor de uitvoering van haar publieke taken, niet beroepen op de grondslag 'gerechtvaardigd belang' (de zesde grondslag in bovenstaande opsomming). Voor de uitvoering van verwerkingen die geen betrekking hebben op de publieke taken die op de gemeente rusten, mag de gemeente haar wel beroepen op de grondslag gerechtvaardigd belang.

Een specifiek overzicht van welke grondslag per verwerkingsdoeleinde wordt gehanteerd is te vinden in het verwerkingsregister. Voor het uitvoeren van haar publieke taken beroept de gemeente haar voornamelijk op de vijfde grondslag, 'de noodzakelijkheid van het verwerken van persoonsgegevens voor een taak van algemeen belang'. Afhankelijk van de situatie kan de gemeente haar beroepen op andere grondslagen.

Behoorlijkheid
Het behoorlijkheidsbeginsel is een breed beginsel en vraagt van de gemeente dat er veel maatregelen dienen te worden getroffen om aan te kunnen tonen dat er aan dit beginsel inzake persoonsgegevensverwerking wordt voldaan. De handleiding van de AVG, uitgebracht door het ministerie van Justitie en Veiligheid, stelt dat organisaties van een behoorlijke persoonsgegevensverwerking kunnen spreken als zij voldoen aan art. 24 tot en met art. 43 van de AVG. Enkele voorbeelden hiervan zijn: het opmaken/onderhouden van een verwerkingsregister, het aanstellen van een FG en het implementeren van het Privacy door ontwerp-principe en het Privacy door standaardinstellingen-principe.

De gemeente zal bij het voldoen aan dit beginsel inzake de verwerking van persoonsgegevens bovenstaande richtlijnen uit de handleiding van de AVG aanhouden.

In bijlage 1 van dit document wordt per artikel tussen art. 24 AVG en art. 43 AVG dat van toepassing is op de gemeente verantwoord op welke wijze de gemeente hieraan voldoet.

Transparantie en informatieplicht
Het begrip transparantie richt zich in de AVG voornamelijk op het informeren van betrokkenen over de wijze waarop hun persoonsgegevens worden verwerkt. Het gaat er hierbij voornamelijk om dat het voor betrokkenen duidelijk is dat zijn of haar persoonsgegevens worden verwerkt, welke soorten persoonsgegevens bij de verwerking betrokken zijn, voor welk doeleinde de persoonsgegevens worden verwerkt, welke rechten de betrokkene heeft en op welke manier de gemeente verder omgaat met de persoonsgegevens. De gemeente heeft de plicht om betrokkenen te informeren omtrent de wijze waarop zij de persoonsgegevens van betrokkenen verwerkt.

De gemeente is transparant over de wijze waarop zij persoonsgegevens verwerkt. Voor betrokkenen is het duidelijk op welke wijze de gemeente hun persoonsgegevens verwerkt. Deze informatie is voor betrokkenen namelijk te raadplegen in de privacyverklaring van de gemeente, welke op de website van de gemeente te vinden is. Het informeren van betrokkenen middels de privacyverklaring vindt in beknopte en toegankelijke vorm plaats. Daar komt bij dat de informatie in de privacyverklaring op een begrijpelijke en duidelijk leesbare wijze is geformuleerd.

Tot slot faciliteert de gemeente de mogelijkheid voor betrokkenen om inzage te verkrijgen in de persoonsgegevens die van hen worden verwerkt middels een inzageverzoek. Hierbij wordt de informatie wederom in duidelijke, ondubbelzinnige en leesbare taal aan de betrokkene verstrekt, in het bijzonder wanneer de informatie specifiek voor een kind is bestemd.

6.2 Doelbinding
Volgens de AVG mogen persoonsgegevens alleen verwerkt worden als daarvoor een duidelijk en afgebakend doeleinde is vastgesteld. Het doeleinde moet daarnaast uitdrukkelijk omschreven en gerechtvaardigd zijn.

De persoonsgegevens mogen in beginsel niet voor andere doeleinden verder worden verwerkt, tenzij dat doeleinde verenigbaar is met het doeleinde waarvoor de persoonsgegevens zijn verzameld. Voor de uitvoering van bepaalde wetten, zoals de Jeugdwet, zijn de doeleinden voor de verwerking al in de wet vastgelegd. Net als de persoonsgegevens die opgevraagd en verwerkt mogen worden.

1) Toepassing binnen de gemeente Opsterland: 'Voor de goede vervulling van de gemeentelijke taak'.

Voor het bereiken van het doeleinde waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokkene zoveel mogelijk beperkt.

6.3 Minimale gegevensverwerking
Minimale gegevensverwerking (ook wel: dataminimalisatie genoemd) is een begrip dat centraal staat in de AVG. Om aan dit beginsel te voldoen verwerkt de gemeente alleen persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel.

De gemeente streeft naar minimale gegevensverwerking. Dit houdt in dat de gemeente niet alleen slechts de persoonsgegevens verwerkt die noodzakelijk zijn om het doeleinde te bereiken, maar ook dat de gemeente onder andere de persoonsgegevens niet langer bewaart dan dat noodzakelijk is voor het bereiken van het beoogde doeleinde. Twee begrippen die bij minimale gegevensverwerking een grote rol spelen zijn subsidiariteit en proportionaliteit.

Subsidiariteit
Subsidiariteit houdt in dat er, indien mogelijk, minder of geen persoonsgegevens worden verwerkt om het betreffende doeleinde te bereiken. Het toepassen van verschillende autorisatieniveaus binnen de gemeente maakt dit onder andere mogelijk. De gemeente past deze technische maatregel en andere maatregelen toe om aan het subsidiariteitsbeginsel te voldoen.

Proportionaliteit
Proportionaliteit houdt in dat de inbreuk op de rechten van de betrokkene niet onevenredig mag zijn en in verhouding moet staan tot het doel dat met de verwerking gerealiseerd wordt.

Subsidiariteit en proportionaliteit zijn twee begrippen die tijdens de dagelijkse werkzaamheden van medewerkers vaak toegepast kunnen worden. De gemeente streeft er dan ook naar dat de inhoud waar deze begrippen voor staan bij eenieder die werkzaam is binnen de gemeente bekend zijn.

Het feit dat de gemeente streeft naar minimale gegevensverwerking blijkt voornamelijk uit dit privacybeleid, waar minimale gegevensverwerking als een rode draad doorheen loopt en het feit dat de gemeente voldoet aan haar verplichtingen inzake gegevensbescherming door ontwerp en standaardinstellingen.[2]

6.4 Juistheid en actualisatie
Het beginsel omtrent de juistheid van persoonsgegevens vereist van de gemeente dat zij alle redelijke maatregelen dient te nemen om ervoor te zorgen dat de persoonsgegevens die zij verwerkt juist zijn. Onjuiste persoonsgegevens moeten zo spoedig mogelijk worden gerectificeerd of vernietigd. Wat redelijk is, is situatieafhankelijk en hangt onder andere af van het soort persoonsgegevens die worden verwerkt en de hoeveelheid persoonsgegevens die worden verwerkt. Daarnaast spelen de stand van de techniek en de uitvoeringskosten ook een rol.

Voor bepaalde verwerkingen binnen de gemeente zorgen het systeem en de werkwijze voor een hoge mate van juistheid van de verwerkte persoonsgegevens. Als voorbeeld hiervan kunnen verwerkingen worden genomen waarvoor de BRP wordt geraadpleegd.

Voor andere verwerkingen zorgt voornamelijk een combinatie van technische en organisatorische maatregelen ervoor dat de juistheid van persoonsgegevens wordt gewaarborgd. Waaronder: het inregelen van de (technische) mogelijkheid om aanpassingen te maken binnen systemen en persoonsgegevens te kunnen rectificeren indien noodzakelijk, het hanteren van verschillende autorisatieniveaus, het uitvoeren van audits in het kader van privacy en informatiebeveiliging waarbij onder andere de integriteit en betrouwbaarheid van (persoons)gegevens worden getoetst.

6.5 Bewaartermijn
In beginsel worden persoonsgegevens binnen de gemeente niet langer bewaard dan dat strikt noodzakelijk is. Het bewaren van persoonsgegevens is noodzakelijk om de gemeentelijke taken goed uit te kunnen voeren of om wettelijke verplichtingen na te kunnen komen. Voor gemeenten gelden de Archiefwet of andere wetten om de bewaartermijnen te bepalen. Deze wetten regelen het beheren van archieven en documenten voor de lange termijn zodat deze beschikbaar zijn voor iedereen die er gebruik van moet maken. De Archiefwet houdt daarbij rekening met de privacy door zo nodig de openbaarheid van persoonsgegevens te beperken.

2) Betreffende maatregelen staan in bijlage 1 beschreven.

Om een bewaartermijn te bepalen is kennis nodig van de diverse wetten die hierin voorgaan op de AVG. Per verwerking wordt een bewaartermijn vastgesteld, welke gehandhaafd wordt door middel van genomen technische en organisatorische maatregelen. Dit uit zich bijvoorbeeld door constante doorontwikkeling van het zaaksysteem en andere opslaglocaties, waar gebruikt wordt gemaakt van geautomatiseerde bewaartermijnen.

Het verwerkingsregister van de gemeente geeft overzichtelijk weer welk bewaartermijn voor iedere verwerking van persoonsgegevens wordt gehanteerd.

6.6 Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het rechtmatige doeleinde waarvoor de persoonsgegevens zijn verzameld. Daarbij zorgt de gemeente door het nemen van technische en organisatorische maatregelen voor een passend beveiligingsniveau van de persoonsgegevens die zij verwerkt. Een aantal van deze maatregelen staan genoemd in dit beleid. Deze maatregelen zijn een toevoeging op de maatregelen uit het 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid' van de gemeente, welke zijn geïmplementeerd om te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Gezamenlijk vormen deze maatregelen op technisch en organisatorisch vlak voor een passende bescherming van persoonsgegevens.

6.7 Conclusie beginselen inzake de verwerking van persoonsgegevens
Voor alle verwerkingen van persoonsgegevens geldt in beginsel dat de proceseigenaar verantwoordelijk is om ervoor te zorgen dat de verwerking in lijn met de AVG worden uitgevoerd. De PO, FG en CISO kunnen de proceseigenaren hierbij op verschillende manieren ondersteunen.

Alle verwerkingen van persoonsgegevens die binnen de organisatie worden uitgevoerd, worden periodiek getoetst aan de beginselen inzake de verwerking van persoonsgegevens. Op basis van de toetsing wordt bepaald of het noodzakelijk is om aanvullende maatregelen te nemen ten aanzien van de bescherming van de verwerkte persoonsgegevens.

Op kritische bedrijfsprocessen wordt periodiek een DPIA uitgevoerd. Voor niet-kritische bedrijfsprocessen geldt dat periodiek wordt beoordeeld of de huidige werkwijze overeenkomt met de eisen uit de AVG. Op het moment dat verwerkingen niet (meer) conform de AVG worden uitgevoerd, adviseren de FG en/of de CISO in de ontstane situatie. De beoordeling van zowel de kritische bedrijfsprocessen, als de niet-kritische bedrijfsprocessen komt voort uit de verantwoordingscyclus die de gemeente heeft opgemaakt.

Verder heeft de gemeente voor alle overige verplichtingen die voortkomen uit de AVG technische en/of organisatorische maatregelen genomen om ervoor te zorgen dat zij deze naleeft. Hierbij kan onder andere worden gedacht aan: het onderhouden van een verwerkingsregister en een datalekregister, het hanteren van een datalekprotocol, het aanwijzen van een FG, het sluiten van verwerkersovereenkomsten en het informeren van betrokkenen.

Bovenstaande verantwoording leidt tot het feit dat de gemeente alle noodzakelijke technische en organisatorische maatregelen heeft genomen om er zorg voor te dragen dat zij een verwerking van persoonsgegevens voert die in lijn is met de AVG.

7. Rechten van betrokkenen

Betrokkenen hebben verschillende rechten om controle te houden over hun persoonsgegevens. De AVG kent betrokkenen acht verschillende rechten toe, deze rechten zijn:
- recht op (duidelijke) informatie;
- recht op inzage;
- recht op beperking van de verwerking;
- recht op bezwaar;
- recht op rectificatie en aanvulling;
- recht op gegevenswissing (vergetelheid);
- recht op overdraagbaarheid van gegevens (dataportabiliteit);
- recht om niet onderworpen te worden aan geautomatiseerde besluitvorming.

Met deze rechten kunnen betrokkenen de gemeente bijvoorbeeld verzoeken welke persoonsgegevens van hen worden verwerkt, om persoonsgegevens van hen te rectificeren of persoonsgegevens van hen te verwijderen. Een verzoek van een betrokkene wordt in principe binnen één maand afgehandeld. Verlenging is bij uitzondering met maximaal twee maanden mogelijk. De reden van de verlenging wordt

in dat geval binnen één maand nadat de gemeente het verzoek heeft ontvangen aan de betrokkene meegedeeld. Als een verzoek wordt afgewezen stelt de gemeente de verzoeker hier ook binnen één maand gemotiveerd van op de hoogte. Hierbij wordt aangegeven dat de verzoeker het recht heeft op bezwaar/beroep en dat de verzoeker een klacht bij de AP kan indienen.

In sommige gevallen is de gemeente verplicht om een verzoek met betrekking tot de uitoefening van één of meerdere rechten van betrokkenen door te geven aan een derde. Dit kan bijvoorbeeld het geval zijn als de gemeente persoonsgegevens levert aan die derde of wanneer de betreffende derde persoonsgegevens verwerkt voor de gemeente. In dergelijke gevallen zal de gemeente het verzoek zo spoedig mogelijk doorgeven.

Er is een register van verzoeken waarin onder meer de verzoeken van betrokkenen, de datum van ontvangst, de wijze van afhandeling en datum van beantwoording is opgenomen. Ook de doorgifte aan derden inclusief hun bevestiging van ontvangst wordt in het register opgenomen. Documenten die noodzakelijk zijn om bovenstaande aan te tonen kunnen tevens worden opgeslagen. Dit register is onder beheer bij de PO. Indien een verzoek niet of niet tijdig kan worden afgehandeld, wordt direct contact opgenomen met de FG.

De uitoefening van de rechten van betrokkenen is opgenomen in de Procedure 'Uitoefenen rechten van betrokkenen'. Allereerst wordt de identiteit van de verzoeker getoetst, waarna het verzoek inhoudelijk wordt beoordeeld en afgehandeld.

De gemeente vindt het vanuit haar overheidspositie en de voorbeeldfunctie die zij daarmee heeft belangrijk om de rechten van betrokkenen goed en tijdig na te komen. Het voorkomen dat betrokkenen ontevreden zijn met de afhandeling van hun verzoek staat dan ook hoog in de pikorde.

De medewerkers, externe medewerkers en sollicitanten worden in de interne privacyverklaring doorverwezen naar de PO voor de uitoefening van hun rechten. De PO handelt deze verzoeken af met Personeelszaken en houdt hier eveneens een register van bij.

De reden dat er een register bij wordt gehouden met informatie over de verzoeken van betrokkenen omtrent de uitoefening van de rechten die zij op basis van de AVG hebben, is dat de gemeente op deze manier kan verantwoorden dat zij heeft voldaan aan de formele eisen die hierbij van toepassing zijn.

In het geval dat een betrokkene repetitief ongegronde of buitensporige verzoeken omtrent de uitoefening van zijn of haar rechten indient, kan de gemeente eveneens met bovenstaande register haar keuze om kosten in rekening te brengen of weigering om gehoor te geven aan een dergelijk verzoek verantwoorden.

8. Website

8.1 Cookies

De website van de gemeente, www.opsterland.nl, maakt gebruik van cookies. Cookies zijn kleine tekstbestanden met informatie die door de website op de computer, tablet of mobiele telefoon van de gebruiker worden geplaatst. Vervolgens kunnen de cookies weer door de website worden geraadpleegd.

Er bestaan drie soorten cookies:

- **Analytische cookies**: Door deze cookies te plaatsen verkrijgt een organisatie gegevens over het gebruik van haar website. Met deze gegevens kan een organisatie haar website verbeteren, zodat deze beter aansluit op de wensen van de bezoeker. Als er met het gebruik van deze cookiesoort geen persoonsgegevens worden verwerkt, is een organisatie niet verplicht om toestemming te vragen voor het plaatsen van deze cookie.
- **Functionele cookies**: Deze cookies zorgen ervoor dat een website prettig functioneert. Zo kan het zijn dat er gegevens worden onthouden waardoor de gebruiker niet bij ieder bezoek van de website opnieuw moet inloggen. Voor het plaatsen van functionele cookies hoeft geen toestemming te worden gevraagd.
- **Tracking cookies**: Door het plaatsen van tracking cookies kan het gebruikersgedrag op websites worden gevolgd. Dit kan ondersteuning bieden bij het verbeteren van de website en de dienstverlening. Voor het plaatsen van tracking cookies dient een organisatie toestemming aan te vragen.

De website van de gemeente plaatst slechts analytische cookies. De gegevens die met het plaatsen van de analytische cookies worden verzameld zijn niet te herleiden naar een natuurlijke persoon. Voor het anonimiseren van de gegevens die met het plaatsen van de analytische cookies worden verkregen heeft de gemeente gebruik gemaakt van de handleiding die de AP hiervoor heeft aangeboden.

Omdat er geen persoonsgegevens worden verwerkt met het gebruik van de analytische cookies hoeft er geen toestemming van de gebruiker te worden verkregen. Dit maakt dat de gemeente geen gebruik maakt van een zogenaamde 'cookiebanner' op haar website.

9. Bewustwording en training

Enkel het doorvoeren van Beleid en (technische) maatregelen zijn niet voldoende om risico's in verband met privacy uit te sluiten. Privacy is voor een belangrijk deel een zaak van bewustwording en cultuur. Alle medewerkers van de gemeente moeten zich tijdens de uitvoering van hun werkzaamheden voortdurend bewust zijn van het belang van privacy.

Het waarborgen van de privacy van betrokkenen is niet een belang dat geldt als een aanvulling is op de werkzaamheden van iedere werknemer, maar integraal opgenomen dient te zijn binnen de werkzaamheden van de werknemer. Het is essentieel dat de proceseigenaren het belang van het waarborgen van privacy uitdragen binnen de teams. Daarnaast is het de taak van de gemeente haar visie omtrent persoonsgegevensverwerking kenbaar te maken en daarbij de benodigde maatregelen te nemen. Om er op deze manier voor te zorgen dat persoonsgegevens op een veilige manier worden verwerkt.

Iedere nieuwe werknemer ontvangt aan het begin van zijn of haar dienstverband informatie omtrent de wijze waarop de werknemer om dient te gaan met persoonsgegevens. Deze informatie wordt op een heldere en duidelijke manier overgebracht op de werknemer. De informatie is algemeen van aard en daarom van toepassing op vrijwel alle functies die binnen de gemeente worden uitgevoerd.

De gemeente streeft ernaar ieder kalenderjaar ten minste één campagne binnen de organisatie uit te voeren waarbij het bewustzijn van verschillende essentiële onderwerpen rondom het veilig verwerken van (persoons)gegevens en informatiebeveiliging centraal staan.

Daarnaast bevordert het college samen met het management een privacy bewuste organisatiecultuur via voorbeeldgedrag en door te voorzien in de middelen voor bewustwording en training van medewerkers.

10. Inwerkingtreding

Dit beleid is vastgesteld door het college op 20 december 2022 en treedt in werking op de dag na die van publicatie ervan in het Gemeenteblad.

gemeente Opsterland

BIJLAGE 1 – Verantwoording behoorlijkheidsbeginsel

Het behoorlijkheidsbeginsel is een breed beginsel en vraagt van de gemeente dat er veel maatregelen dienen te worden getroffen om aan te kunnen tonen dat er aan dit beginsel inzake persoonsgegevensverwerking wordt voldaan.

Zoals in hoofdstuk 6.1 van dit document staat omschreven is hieronder een uitwerking te vinden van de wijze waarop de gemeente voldoet aan het behoorlijkheidsbeginsel uit artikel 5 lid 1 van de AVG.

- ***Verantwoordelijkheid van de verwerkingsverantwoordelijke (art. 24 AVG)***

De gemeente neemt alle passende technische en organisatorische maatregelen om ervoor te zorgen dat de verwerking van persoonsgegevens die zij uitvoert, plaatsvindt volgens de AVG. In dit beleid verantwoord de gemeente de technische en organisatorische maatregelen die zij heeft genomen om zorg te dragen voor een veilige verwerking van persoonsgegevens. In aanvulling op het privacybeleid waarborgt de gemeente de beveiliging van de persoonsgegevens die zij verwerkt door te voldoen aan de eisen die aan haar worden gesteld op het gebied van informatiebeveiliging, waarbij het normenkader van de Baseline Informatiebeveiliging Overheid (BIO) de meest prominente rol speelt in het bepalen van het beveiligingsniveau. Aanpalende wetgeving op het gebied van privacy en informatiebeveiliging wordt tevens meegenomen bij de bepaling van het beveiligingsniveau.

Ieder jaar wordt geëvalueerd of het bestaande privacybeleid voldoende dekkend is en worden, waar nodig, delen van het privacybeleid aangevuld, aangepast of op een andere manier gewijzigd om een veilige en behoorlijke verwerking van persoonsgegevens te waarborgen.

- ***Gegevensbescherming door ontwerp en door standaardinstellingen (art. 25 AVG)***

Gegevensbescherming door ontwerp
Gegevensbescherming door ontwerp houdt in dat tijdens de ontwikkeling van beleid, het ontwerpen/in gebruik nemen van nieuwe systemen waarmee persoonsgegevens worden verwerkt, privacy en informatiebeveiliging een duidelijke rol spelen. Op deze manier wordt de inbreuk op de persoonlijke levenssfeer van de persoon wiens persoonsgegevens worden verwerkt geminimaliseerd.

De gemeente voldoet door het nemen van verschillende maatregelen aan haar verplichtingen in het kader van gegevensbescherming door ontwerp. Eén van de maatregelen die de gemeente hiervoor heeft genomen is het uitvoeren van DPIA's. Voor specifieke verwerkingen is het uitvoeren van een DPIA verplicht gesteld door de gemeente. Het uitvoeren van het DPIA vindt normaliter voor de ingebruikname van een systeem of applicatie plaats en komt vervolgens periodiek terug.

Een tweede voorbeeld van een maatregel die de gemeente in dit kader heeft genomen, is de controle van derde partijen. Voordat een derde partij werkzaamheden voor de gemeente uitvoert en daarbij persoonsgegevens verwerkt, wordt gecontroleerd of de derde partij een passend beveiligingsniveau waarborgt.

Onder andere door het nemen van bovenstaande maatregelen zorgt de gemeente ervoor dat zij voldoet aan haar verplichtingen inzake gegevensbescherming door ontwerp.

Gegevensbescherming door standaardinstellingen
Gegevensbescherming door standaardinstellingen beschrijft dat voor het bereiken van elk specifiek doeleinde slechts de persoonsgegevens dienen te worden verwerkt die strikt noodzakelijk zijn om dat betreffende doeleinde te bereiken. Hierbij spelen enkele voorwaarden een rol: de hoeveelheid persoonsgegevens die worden verwerkt voor het bereiken van het beoogde doeleinde, de mate waarin deze persoonsgegevens worden verwerkt, de bewaartermijn die voor de persoonsgegevens wordt gehanteerd en de toegankelijkheid ervan.

De gemeente heeft een procedure opgemaakt waarin per verwerking wordt getoetst of aan alle beginselen inzake de verwerking van persoonsgegevens wordt voldaan. De toetsing wordt periodiek uitgevoerd waardoor continu een passend beveiligingsniveau wordt gewaarborgd.

Bovenstaande procedure houdt in dat op kritische bedrijfsprocessen periodiek een DPIA wordt uitgevoerd. Verder geldt voor niet-kritische bedrijfsprocessen dat periodiek wordt beoordeelt of de huidige werkwijze overeenkomt met de eisen uit de AVG. Op het moment dat verwerkingen niet (meer) conform de AVG worden uitgevoerd, adviseren de FG en/of de CISO in de ontstane situatie.

Bovenstaande werkwijze zorgt er onder andere voor dat de gemeente voldoet aan haar verplichtingen inzake gegevensbescherming door standaardinstellingen. Dit heeft vervolgens tot gevolg dat persoonsgegevens niet overbodig worden verwerkt.

- ***Gegevensuitwisseling tussen zelfstandige verwerkingsverantwoordelijken***

De gemeente kan ook persoonsgegevens uitwisselen met andere verwerkingsverantwoordelijken. Als de gemeente gegevens deelt met een andere organisatie die de persoonsgegevens voor haar eigen doeleinden gebruikt, dan is sprake van uitwisseling van persoonsgegevens tussen twee zelfstandige verwerkingsverantwoordelijken. Alvorens de uitwisseling van de gegevens kan plaatsvinden, wordt vastgesteld of deze derde partij de persoonsgegevens mag ontvangen. Deze beoordeling wordt eventueel uitgewerkt en beoordeeld in een DPIA. Idealiter sluit de gemeente een gegevensuitwisselingsovereenkomst af met de andere verwerkingsverantwoordelijke. De gegevensuitwisselingsovereenkomst van de gemeente is bij voorkeur leidend.

- ***Gezamenlijke verwerkingsverantwoordelijken (art. 26 AVG)***

Van gezamenlijke verwerkingsverantwoordelijkheid is sprake als de gemeente en een andere of meerdere verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen. Alvorens de samenwerking wordt aangegaan wordt vastgesteld of de derde partij de persoonsgegevens mag ontvangen. In geval van een dergelijk samenwerkingsverband sluit de gemeente een overeenkomst gezamenlijke verwerkingsverantwoordelijkheid met de betreffende partij. In deze overeenkomst worden de verantwoordelijkheden met betrekking tot de nakoming van de AVG onderling geregeld. Indien nodig wordt de samenwerking uitgewerkt en beoordeeld in een DPIA.

- ***Verwerker en aankoop producten (art. 28 AVG)***

Als persoonsgegevens uitgewisseld worden met een derde partij of worden verwerkt door een derde partij, dan wordt, voorafgaand aan de uitwisseling of de verwerking, beoordeeld of dit is toegestaan op grond van de AVG. Dit is een overleg tussen de afdeling, inkoop, de PO en de CISO waarbij de FG om advies kan worden gevraagd.

Verwerker

De gemeente maakt gebruik van verwerkers voor de verwerking van persoonsgegevens. Deze verwerkers kunnen op hun beurt de verwerkingen weer uitbesteden aan subverwerkers. De gemeente blijft verantwoordelijk en aansprakelijk voor de verwerking in de gehele keten, ongeacht hoeveel verwerkers en subverwerkers worden ingeschakeld. De gemeente mag alleen verwerkers inschakelen die afdoende garanties bieden met betrekking tot het toepassen van technische en organisatorische maatregelen, zodat de verwerkingen aan de vereisten van de AVG voldoen en daarmee de bescherming van de rechten van de betrokkenen voldoende is gewaarborgd.

Alvorens de gemeente een verwerking uitbesteedt, bepaalt de gemeente of de verwerker zich kan houden aan de eisen zoals deze in de AVG zijn benoemd. Hiervoor heeft de gemeente de procedure ‘inschakelen derde’ opgemaakt. Onderdeel van deze procedure is allereerst het kwalificeren van de derde om vast te stellen dat de verwerking daadwerkelijk door een verwerker wordt uitgevoerd en niet door een andere verwerkingsverantwoordelijke. Tevens kan het uitvoeren van een DPIA ook een onderdeel van deze procedure zijn. In het DPIA wordt afgewogen of de nieuwe verwerking binnen de wettelijke kaders en het beleid van de gemeente past. De verwerker moet kunnen aantonen dat aan alle eisen kan worden voldaan en mag alleen subverwerkers inschakelen die hieraan ook voldoen. Afspraken met verwerkers worden vastgelegd in een verwerkersovereenkomst. Ook tijdens de uitbesteding moet de verwerker steeds aantonen dat effectief aan de eisen wordt voldaan, inclusief de verdere uitbesteding aan subverwerkers.

De gemeente staat in principe niet toe dat persoonsgegevens door (sub)verwerkers worden verwerkt in landen buiten de EER[3]. Indien de verwerking buiten de EER plaatsvindt, moet worden vastgesteld of het land een passend beschermingsniveau biedt of andere maatregelen heeft genomen om een passend beschermingsniveau te waarborgen. De FG en de CISO stellen in overleg vast of het betreffende land een passend beschermingsniveau waarborgt. Hierbij is het voldoen aan de AVG en het voeren van een informatiebeveiligingsbeleid door het derde land dat ten minste van vergelijkbaar niveau is als dat van de gemeente essentieel.

De proceseigenaar is verantwoordelijk voor het sluiten van de verwerkersovereenkomst en betrekt de PO in dit proces. De PO kan voor de beoordeling en invulling van een verwerkersovereenkomst de FG, CISO en juridische zaken benaderen. De verwerkersovereenkomst van de gemeente is bij voorkeur leidend. Na afstemming met de PO, en eventueel advies van juridische zaken kan de verwerkersovereenkomst worden aangepast.

Aankoop producten

3) Bij de Europese Economische Ruimte (EER) horen alle EU-landen plus Liechtenstein, Noorwegen en IJsland.

De gemeente mag bij de verwerking van persoonsgegevens alleen systemen en applicaties gebruiken die voldoen aan de AVG. Voorafgaand aan het in gebruik nemen van nieuwe systemen en applicaties moet de gemeente kunnen vaststellen op welke wijze de leverancier de effectieve werking van privacy door ontwerp en privacy door standaardinstellingen heeft ingebouwd in het systeem of de applicatie. Tevens moeten de rechten van betrokkenen en de facilitering daarvan aantoonbaar zijn gewaarborgd door de leverancier. Voorafgaand aan het in gebruik nemen van een nieuw systeem of applicatie worden de PO en de CISO benaderd voor advies. Tevens maken zij de afweging of er een DPIA moet worden uitgevoerd.

- **Register van verwerkingsactiviteiten (art. 30 AVG)**

Een organisatie dient een verwerkingsregister bij te houden als:
- o de verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen;
- o de verwerking van persoonsgegevens niet incidenteel is;
- o de verwerking betrekking heeft op bijzondere persoonsgegevens.

Voor de verwerking van persoonsgegevens die door de gemeente wordt uitgevoerd, zijn al deze drie voorwaarden van toepassing. Dit leidt tot het feit dat de gemeente verplicht is een verwerkingsregister op te stellen en te onderhouden.

Een nieuwe versie van het verwerkingsregister zal volgens het tactisch uitvoeringsbeleid worden opgemaakt in Q3 2022. Hierin worden alle verwerkingen van persoonsgegevens beschreven die op dat moment worden uitgevoerd binnen de gemeente.

De verantwoordingscyclus draagt er zorg voor dat het verwerkingsregister wordt onderhouden en een representatief beeld biedt van de verwerkingen van persoonsgegevens die door de gemeente worden uitgevoerd.

- ***Medewerking met de toezichthoudende autoriteit (art. 31 AVG)***

Op het moment dat de AP, voor het vervullen van haar taken, om medewerking van de gemeente vraagt, gaat de gemeente hierin mee en zal zij alle noodzakelijke handelingen verrichten om in een correcte afhandeling van de betreffende zaak te voorzien.

De FG is in bovenstaande situaties het eerste aanspreekpunt met de AP.

- ***Beveiliging van de verwerking (art. 32 AVG)***

De beveiliging van de persoonsgegevens die de gemeente verwerkt wordt gewaarborgd door het handhaven van wet- en regelgeving die in het kader van informatiebeveiliging op de gemeente van toepassing is. Deze wet- en regelgeving is voor de gemeente de Baseline Informatiebeveiliging Overheid.

De verplichte interne en externe audits die in het kader van bovenstaande wetgeving uitgevoerd dienen te worden, dragen er zorg voor dat de doeltreffendheid van de technische en organisatorische maatregelen die de gemeente heeft genomen om een passend beveiligingsniveau te waarborgen, naar behoren is.

- ***Melding van een inbreuk in verband met persoonsgegevens (artt. 33 en 34 AVG)***

Van een datalek is sprake als er een inbreuk op de beveiliging van persoonsgegevens plaatsvindt, die leidt tot enige ongeoorloofde verwerking daarvan. Het kan hierbij bijvoorbeeld gaan om een diefstal van een laptop, een in de trein vergeten usb-stick of een e-mail die naar de verkeerde persoon is verstuurd. Datalekken moeten worden gemeld bij de toezichthouder binnen 72 uur na ontdekking daarvan. In sommige gevallen moeten ook de personen die zijn getroffen door het datalek (= de betrokkenen) worden ingelicht.

Een datalek moet zonder onredelijke vertraging, maar in ieder geval binnen 72 uur, worden gemeld aan de AP. Echter, als het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, hoeft het datalek niet te worden gemeld aan de AP.

Op het moment dat het datalek een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen, dienen de betrokkenen op wie het datalek effect heeft ook op de hoogte te worden gesteld van het datalek.

De gemeente voldoet aan de eisen rondom datalekken die op haar van toepassing zijn door middel van de procedure ‘Datalekken’ die is vastgesteld. In deze procedure staat in detail weergegeven welke handelingen uitgevoerd dienen te worden op het moment dat er een datalek plaatsvindt.

Tijdens het doorlopen van de procedure wordt de ernst van het datalek beoordeeld, hierbij staan de volgende twee onderwerpen centraal:
- de ernst van de waarschijnlijke gevolgen van het datalek;
- de waarschijnlijkheid dat de gevolgen van het datalek zich zullen voordoen.

De gegevens met betrekking tot de twee bovenstaande onderwerpen zullen de doorslag geven over het wel of niet melden van het datalek bij de AP en/of de betrokkene(n). Gezien een datalek binnen 72 uur dient te worden gemeld bij de AP, wordt bovenstaande beoordeling binnen deze termijn gemaakt.

Alle inbreuken in verband met persoonsgegevens worden vastgelegd in het datalekregister, ongeacht of de inbreuk heeft geleid tot een melding aan de AP en/of aan de betrokkene(n). In het datalekregister worden eveneens de afwegingen opgenomen die hebben geleid tot de beslissing om wel of niet een melding te doen bij de AP en/of de betrokkenen.

Datalekken bij (sub)verwerkers meldt de verwerker zo spoedig mogelijk aan de contactpersoon van de gemeente. Vervolgens bepaalt de gemeente conform de procedure 'Datalekken' of de AP en/of de betrokkenen moeten worden ingelicht.

Naast de afhandeling van het datalek gaat de procedure ook in op het voorkomen van een soortgelijk datalek in de toekomst.

- ***Data protection impact assessment en voorafgaande raadpleging (artt. 35 en 36 AVG)***

Doel DPIA
Een DPIA, ook wel een gegevensbeschermingseffectbeoordeling genoemd, is een instrument om een analyse uit te voeren naar de risico's die zich in een (voorgenomen) verwerking kunnen voordoen en inbreuk kunnen maken op de privacyrechten van betrokkenen. Het is ook een instrument waarmee de gemeente zich kan verantwoorden dat een verwerking conform de wetgeving wordt uitgevoerd.

Verplichtstelling DPIA
Een DPIA is in ieder geval verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen wiens persoonsgegevens worden verwerkt. Deze beoordeling is aan de gemeente.

In de AVG is vastgesteld dat er in ieder geval een DPIA moet worden uitgevoerd als de gemeente:
- systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten baseert die rechtsgevolgen hebben voor mensen;
- op grote schaal bijzondere persoonsgegevens verwerkt of strafrechtelijke gegevens verwerkt;
- op grote schaal en systematisch mensen monitort in een publiek toegankelijk gebied (bijvoorbeeld het houden van toezicht op een openbaar plein door middel van camera's).

Tevens heeft de AP een lijst met verwerkingen van persoonsgegevens vastgesteld waarvoor het verplicht is om een DPIA uit te voeren. De meest recente versie van deze lijst is op 27 november 2019 gepubliceerd in de Staatscourant. Deze lijst is ook te raadplegen op de website van de AP.

Daarnaast heeft het European Data Protection Board (hierna: EDPB) een lijst met 9 criteria opgesteld om te bepalen of een verwerking van persoonsgegevens een hoog privacyrisico oplevert.

Tot slot heeft de gemeente in het kader van continuïteit en het kunnen voldoen aan haar verplichtingen inzake gegevensbescherming door ontwerp en standaardinstellingen vastgesteld dat DPIA's ook periodiek op kritische bedrijfsprocessen worden uitgevoerd.

De gemeente houdt rekening met alle bovenstaande factoren bij het bepalen of een DPIA dient te worden uitgevoerd.

Uitvoering van het DPIA
De proceseigenaar is verantwoordelijk voor het uitvoeren van een DPIA. Voor het uitvoeren van een DPIA stelt de gemeente een procedure beschikbaar. In deze procedure staat in detail uitgelegd welke handelingen moeten worden genomen om een DPIA op de juiste manier uit te voeren. Bij voorkeur wordt het format van de gemeente gebruikt voor het uitvoeren van een DPIA.

Voorafgaand aan het aftekenen van een DPIA wordt de FG te allen tijde geraadpleegd om te toetsen of de uitkomsten van het DPIA op een correcte wijze tot stand zijn gekomen. Daarnaast wordt de CISO benaderd voor een beoordeling van de maatregelen die zijn genomen op het gebied van informatiebeveiliging. De FG en de CISO adviseren inzake hun bevindingen.

Nadat het DPIA op een correcte wijze is uitgevoerd, wordt het document afgetekend door de proceseigenaar. Vervolgens worden uitgevoerde DPIA's periodiek opnieuw uitgevoerd om continu een passend beveiligingsniveau te waarborgen.

Voorafgaande raadpleging
Het kan voorkomen dat uit het DPIA blijkt dat een verwerking een hoog risico oplevert voor de rechten en vrijheden van betrokkenen en de gemeente geen maatregelen kan nemen om het risico te beperken. Als de gemeente de verwerking, ondanks het risico, toch uit wil voeren dient zij hieromtrent eerst de AP te raadplegen. De AP brengt vervolgens een advies uit omtrent de situatie, welke de gemeente meeneemt in haar beslissing om de verwerking wel of niet uit te voeren.

- **Functionaris voor gegevensbescherming (artt. 37, 38 en 39 AVG)**

De AVG bepaalt dat het aanstellen van een Functionaris Gegevensbescherming in drie verschillende situaties verplicht is. Eén van deze verplichte situaties is: "de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan". Omdat de gemeente een overheidsorgaan betreft, is zij verplicht om een FG aan te stellen.

Ten tijde van het vaststellen van dit beleid heeft de gemeente een FG aangesteld. Op het moment dat de functie van FG door een andere medewerker binnen de gemeente of externe medewerker van de gemeente wordt ingevuld, meldt de gemeente de wijziging bij de AP.

De verantwoording omtrent de positie en de taken van de FG zijn eerder in dit document in hoofdstuk 5.1 behandeld.

- **Conclusie behoorlijkheid verwerking van persoonsgegevens**

Bovenstaande verantwoording inzake de behoorlijkheid van de verwerking van persoonsgegevens die de gemeente uitvoert, leidt tot het feit dat de gemeente alle noodzakelijke, passende technische en organisatorische maatregelen heeft genomen om ervoor te zorgen dat zij een behoorlijke verwerking van persoonsgegevens voert.

BIJLAGE 2 - DEFINITIES

Algemene Verordening Gegevensbescherming
Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt niet meer. De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

Anonimiseren
Anonimiseren betekent verwisseling van persoonsgegevens in gegevens die niet langer gebruikt kunnen worden om een natuurlijk persoon te identificeren, daarbij in ogenschouw nemende 'alle middelen die hiervoor redelijkerwijs gebruikt kunnen worden' door zowel een verantwoordelijke als een derde partij. Een belangrijke factor hierbij is dat de Verwerking onomkeerbaar moet zijn.

Betrokkene
Dit is de natuurlijke persoon wiens persoonsgegevens worden verwerkt.

Bijzondere persoonsgegevens
Persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religieuze of levensbeschouwelijke overtuiging, het lidmaatschap van een vakbond of seksueel gedrag of seksuele gerichtheid blijkt.

Cookies
Cookies zijn kleine bestanden die de aanbieder van een website op de apparatuur van een bezoeker plaatst. Bijvoorbeeld op een computer, telefoon of tablet. Met cookies kan informatie worden verzameld of opgeslagen over het websitebezoek of over (het apparaat van) de gebruiker.

Datalek
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Data Protection Impact Assessment (DPIA)
Een Data Protection Impact Assessment is een wettelijk voorgeschreven instrument om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken. Kortgezegd: een proces voor het verwezenlijken en aantonen van naleving van de AVG. De risico's worden bepaald vanuit het oogpunt van de betrokkene.

Derde
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Functionaris voor gegevensbescherming (FG)
Een FG is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG). De Engelse benaming is Data Protection Officer, afgekort DPO.

Gezondheidsgegevens
Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

Inbreuk in verband met persoonsgegevens (ook wel: Datalek)
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. In het dagelijks leven spreken we over een 'datalek'.

Ontvanger
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, als dan niet een derde, aan wie/ waaraan de persoonsgegevens worden verstrekt.

Persoonsgegevens

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

Profilering
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesse, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Pseudonimisering
Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. Pseudonimisering is omkeerbaar mits gebruik van de juiste sleutel.

Strafrechtelijke gegevens
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de AVG, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.

Toestemming van de betrokkene
Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.

Toezichthoudende autoriteit
Een door een lidstaat ingevolge artikel 51 AVG ingestelde onafhankelijke overheidsinstantie. In Nederland is dat de Autoriteit Persoonsgegevens, afgekort: AP.

Uitvoeringswet AVG (UAVG)
De AVG is rechtstreeks van toepassing in Nederland. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de UAVG.

Verwerker
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerkingsverantwoordelijke
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

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

Verwerkingsregister
Het verwerkingsregister (ook wel: register van de verwerkingsactiviteiten) bevat een opsomming van alle verwerkingen van persoonsgegevens die binnen een organisatie worden uitgevoerd. Aanvullend hierop worden er ook enkele gegevens met betrekking tot de verwerking van persoonsgegevens in het register besproken. Hierbij kan worden gedacht aan: het doeleinde van de verwerking en het bewaartermijn van de persoonsgegevens die betrokken zijn bij de verwerking.

Verantwoordingsplicht

De wettelijke plicht om aan te tonen dat de verwerking van persoonsgegevens voldoet aan de wet- en regelgeving van de AVG.

Materiële toepassingsgebied
Het materiële toepassingsgebied bepaalt op welk type verwerkingen van persoonsgegevens de AVG van toepassing is.

Territoriale toepassingsgebied
Het territoriale gebied bepaalt binnen welke territoriale grenzen de AVG van toepassing is op de verwerking van persoonsgegevens.