gemeente
Goeree-Overflakkee

Privacybeleid 2024
AVG & Wpg

Versie	1.0
Auteur	Robin Broere
Datum	20 maart 2024

Inhoudsopgave

1. Inleiding

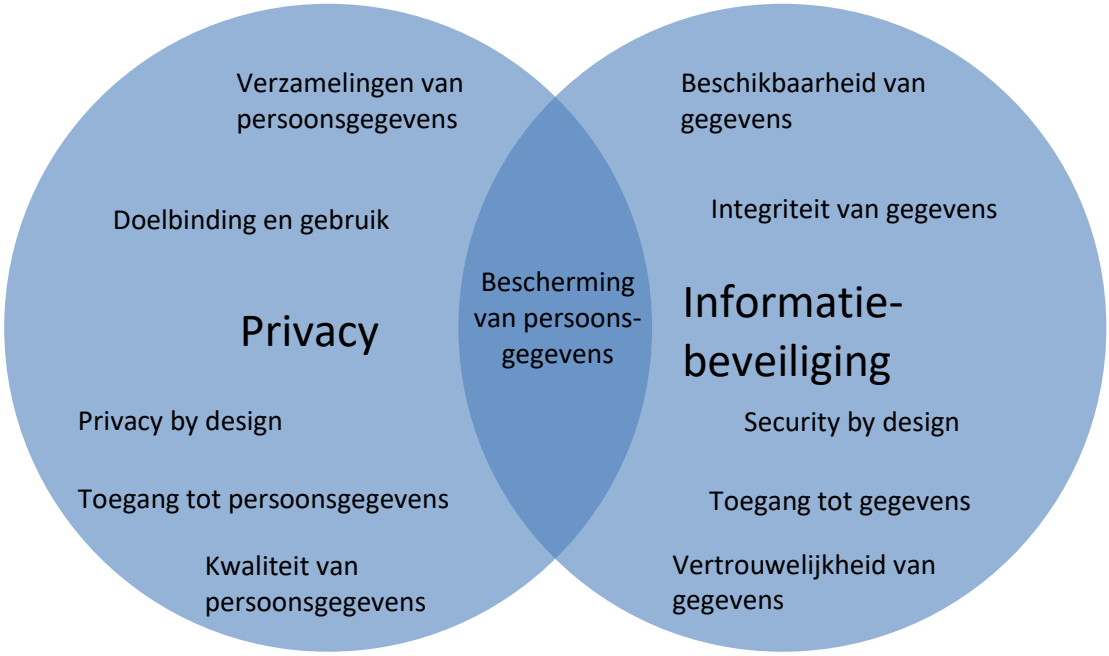
Binnen de gemeente Goeree-Overflakkee wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers, maar kunnen ook via (keten)partner worden verkregen voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat. In deze tijd gaat ook de gemeente mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet altijd onder de Algemene verordening gegevensbescherming (AVG) maar kan ook onder de Wet politiegegevens (Wpg) vallen. De AVG en de Wpg sluiten elkaar wederzijds uit. Op een aantal onderdelen is sprake van overlap.

Het bestuur, Burgermeester en Wethouders en het management spelen een cruciale rol bij het waarborgen van privacy van zowel de AVG als de Wpg. De gemeente Goeree-Overflakkee geeft middels dit beleid, als overkoepelend raamwerk, een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Het privacybeleid van de gemeente Goeree-Overflakkee is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving. Dit beleid wordt ondersteund door verschillende procedures en documentatie die in meer detail beschrijven hoe de principes die in dit beleid worden vermeld, zijn geïmplementeerd en uitgevoerd.

Samenhang privacy en informatiebeveiliging.

Tussen privacy en informatiebeveiliging bestaat een nauwe samenhang, zie figuur 1. Het zijn twee verschillende begrippen maar hebben wel een gemeenschappelijk raakvlak. Privacy gaat over het vertrouwelijk omgaan met persoonlijke gegevens en deze dus ook voldoende beschermen. Informatiebeveiliging gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie. Het privacybeleid kan door deze samenhang niet los worden gezien van het informatiebeveiligingsbeleid.



Figuur 1: Samenhang privacy en informatiebeveiliging

2. Privacy

In dit hoofdstuk wordt eerst de visie van de gemeente met betrekking tot privacy beschreven. Daarna komen de reikwijdte en de wettelijke kaders van dit beleid aan bod.

2.1. Visie

Inwoners van de gemeente Goeree-Overflakkee kunnen erop vertrouwen dat de gemeente hun privacy respecteert en zorgvuldig omgaat met hun persoonsgegevens. Privacybescherming is een onderwerp dat voor bestuurders en medewerkers een integraal onderdeel van het werk vormt.

2.2. Reikwijdte

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente Goeree-Overflakkee en haar bestuursorganen waarin persoonsgegevens worden verwerkt.

Waar nodig wordt in dit beleid specifiek aandacht besteedt aan AVG of Wpg verwerkingen. Wpg verwerkingen zijn alleen van toepassing op het uitvoeren van een politietaak door boa’s

2.3. Wettelijke kaders voor de omgang met gegevens

Voor de omgang met persoonsgegevens gelden onder andere de volgende wettelijke kaders:

- Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
- Artikel 8 Europees Verdrag voor de Rechten van de mens en de fundamentele vrijheden;
- Artikelen 10 en 13 Grondwet (persoonlijke levenssfeer en briefgeheim);
- Sectorale wetgeving;
- Archiefwet;
- Wet politiegegevens (Wpg);
- Besluit politiegegevens (Bpg);
- Besluit politiegegevens buitengewoon opsporingsambtenaren;
- Regeling periodieke audit politiegegevens;
- Informatiebeveiligingsbeleid;
- Personeelshandboek hoofdstuk Integriteit;
- Interne kaders.

2.4. Privacyverklaring AVG en Wpg

In het kader van transparantie heeft de gemeente een privacyverklaring voor de AVG en de Wpg op haar website gepubliceerd. In deze privacyverklaringen worden personen geïnformeerd over de wijze waarop hun gegevens worden verwerkt, welke categorieën persoonsgegevens worden verwerkt en op basis van welk doel.

3. AVG uitgangspunten

In dit hoofdstuk worden de belangrijkste uitgangspunten van de Algemene verordening gegevensbescherming (AVG) beschreven. Persoonsgegevens worden in overeenstemming met de AVG op behoorlijke en transparante wijze verwerkt.

3.1. Grondslagen

De verwerking van persoonsgegevens is alleen rechtmatig als deze gebaseerd is op een van de wettelijke grondslagen zoals omschreven in AVG artikel 6. In de AVG zijn de volgende grondslagen benoemd:

Toestemming

De betrokkene, degene van wie de persoonsgegevens worden verwerkt, heeft toestemming gegeven voor de verwerking van diens persoonsgegevens voor een of meer specifieke doeleinden. Hierbij mag geen sprake zijn van een afhankelijkheidspositie of wanverhouding waardoor niet volledig aan de eis kan worden voldaan dat de toestemming 'vrijelijk' moet zijn gegeven. Vanwege de verhoudingen tussen betrokkene en de gemeente, kan de gemeente in de meeste situaties niet om toestemming vragen. In uitzonderlijke situaties kan wel om toestemming worden gevraagd, bijvoorbeeld voor het verzenden van een nieuwsbrief. Als er toestemming is gegeven, kan deze te allen tijde worden ingetrokken.

Uitvoering overeenkomst

Wanneer de gemeente een contract aangaat met een ander partij of de betrokkene, verwerkt de gemeente persoonsgegevens voor zover dit nodig is om eventuele (pre-)contractuele verplichtingen met betrekking tot dit specifieke contract na te komen. Hierbij zal de gemeente rekening houden met eventuele beperkingen die voortvloeien uit relevante wet- en regelgeving met betrekking tot het type gegevens dat in de (pre-)contractuele fase mag worden verwerkt. Deze grondslag wordt bijvoorbeeld toegepast indien sprake is van een arbeidsovereenkomst.

Wettelijke verplichting

De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de gemeente rust. De gemeente is verplicht zich te houden aan verschillende wet- en regelgeving die het verzamelen, gebruiken, opslaan en verspreiden van persoonlijke informatie vereist. Een voorbeeld hiervan is de Wet basisregistratie personen. Op basis van deze wet is de gemeente verplicht is om bepaalde persoonsgegevens op te slaan in het basisregister.

Vitale belangen

In uitzonderlijke gevallen kan de gemeente een beroep doen op deze verwerkingsgrondslag, om de vitale belangen van de betrokkene te beschermen als dringende medische zorg nodig is.

Algemeen belang/openbaar gezag

De verwerking is noodzakelijk om een publieke taak van algemeen belang uit te voeren of openbaar gezag uit te oefenen. Deze taken zijn in de wet vastgelegd en relevant voor de gemeente. De gemeente zal voor de vervulling van de publieke taken veelal deze grondslag toepassen. Een voorbeeld hiervan is het plaatsen van camera's op openbare locaties om de openbare orde te handhaven.

Gerechtvaardigd belang

Het kan voorkomen dat het belang van de gemeentelijke organisatie om bepaalde persoonsgegevens te verwerken groter is dan het privacybelang van de betrokkene. Hierbij vindt een belangenafweging plaats tussen enerzijds de belangen van de gemeente en anderzijds de belangen van betrokkenen. Deze afweging moet goed worden onderbouwd.

Deze grondslag geldt niet voor de gemeente als zij persoonsgegevens verwerken in het kader van de uitoefening van publieke taken. Voor de uitoefening van bedrijfsmatige handelingen, zoals het opnemen van telefoongesprekken voor kwaliteitsdoeleinden kan deze grondslag wel worden toegepast.

3.2. Overige uitgangspunten

Doelbinding

Dit beginsel borgt dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld om willekeurig gebruik van de gegevens te voorkomen. De gemeente zorgt er daarom voor dat persoonsgegevens uitsluitend worden verwerkt op basis van vooraf vastgestelde doeleinden. Het is mogelijk dat persoonsgegevens voor meer dan één doel worden verzameld. In een dergelijk geval zal de gemeente een beoordeling van de verenigbaarheid uitvoeren om er zeker van te zijn dat er voldoende aansluiting is op het oorspronkelijke doel en zal hierover duidelijke en transparante communicatie aan betrokkene verstrekken voordat de verdere verwerking wordt uitgevoerd.

Dataminimalisatie

De gemeente verwerkt niet meer gegevens persoonsgegevens dan die nodig zijn voor het vooraf bepaalde doel. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan de wettelijke voorgeschreven termijnen, zoals de Archiefwet. Wanneer de termijnen niet zijn vastgelegd in de wet, dan is het uitgangspunt dat persoonsgegevens niet langer worden bewaard dan nodig is voor het bepaalde doel. De door de gemeente vastgestelde bewaartermijn zijn opgenomen in het verwerkingsregister. De gemeente bewaart de persoonsgegevens in ieder geval in overeenstemming met de Selectielijst archiefbestanden gemeenten en intergemeentelijke organen 2020.

Juistheid

De gemeente heeft de nodige maatregelen getroffen om te waarborgen dat de persoonsgegevens die de gemeente van betrokkenen verwerkt juist en actueel zijn, bijvoorbeeld door periodiek de juistheid, nauwkeurigheid en actualiteit te controleren. Als blijkt dat gegevens niet langer juist en compleet zijn, dan zullen ze worden gewijzigd of verwijderd. Daarnaast is het voor betrokkenen mogelijk om bij de gemeente een verzoek in te dienen op rectificatie of wissing van persoonsgegevens.

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 doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is afgestemd op classificatie van de gegevens in relatie tot de Baseline Beveiliging Overheden (BIO).

Subsidiariteit

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt. De gemeente verzekert zich voor de het verwerken van de persoonsgegevens of verwerking op een andere manier kan plaatsvinden, waardoor minder dan wel geen persoonsgegevens verwerkt hoeven te worden.

Proportionaliteit

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het te dienen doel.

4. Wpg uitgangspunten

Persoonsgegevens die worden verwerkt in het kader van de uitvoering van de politietaak worden in overeenstemming met de Wpg verwerkt. De uitgangspunten van de Wpg zijn grotendeels gelijk aan dat van de AVG. Dit geldt met name voor de overige uitgangspunten zoals benoemd in paragraaf 3.2. In dit hoofdstuk worden de belangrijkste uitgangspunten van de Wet politiegegevens (Wpg) beschreven.

Met ingang van 1 januari 2019 vallen ook de boa's onder de Wpg. Binnen gemeente Goeree-Overflakkee kunnen boa's naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG te maken als met de Wpg. Op basis van de taak vallen de persoonsgegevens onder de AVG óf onder de Wpg. Bij de verwerking van gegevens moet duidelijk zijn welke gegevens er op enig moment worden verwerkt.

Binnen de gemeente Goeree-Overflakkee zijn boa's voor de volgende domeinen aanwezig:

- Openbare ruimte (domein I)
- Onderwijs (domein III)
- Werk, inkomen en zorg (domein V)

4.1 Grondslagen en bewaartermijn

Om persoonsgegevens onder de Wpg binnen de hierboven genoemde domeinen te mogen verwerken moet een wettelijke grondslag aanwezig zijn. Deze grondslagen gelden voor alle domeinen.

Dagelijkse politietaak

Onder de grondslag dagelijkse politietaak (Wpg artikel 8) worden persoonsgegevens door de boa's verwerkt. De gegevens kunnen zowel over verdachten, slachtoffers als andere betrokkenen gaan. De gegevens mogen tot vijf jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd en verwerkt. Na deze termijn worden de gegevens nog eens vijf jaar bewaard, dit is de bewaartermijn. Daarna moeten de gegevens worden vernietigd. Gedurende de bewaartermijn kunnen de gegevens gebruikt worden voor het afhandelen van klachten, voor audits of een controle door de toezichthouder, de Autoriteit Persoonsgegevens. Verder geldt dat deze gegevens onder bepaalde omstandigheden ter beschikking kunnen worden gesteld voor hernieuwde verwerking in een actueel opsporingsonderzoek. Gegevens in de bewaartermijn mogen ook verwerkt worden voor wetenschappelijk onderzoek en statistiek.

Gerichte verwerkingen

De grondslag voor het verwerken van gegevens die gericht zijn op specifiek personen of gebeurtenissen vallen onder zogenaamde gerichte verwerkingen (Wpg artikel 9). De inbreuk op de persoonlijke levenssfeer van deze personen is groter dan bij het uitvoeren van de dagelijkse politietaak. Denk hierbij aan het plaatsen van gps-bakens of stelselmatige langdurige observatie. Deze gegevens morgen verwerkt worden tot een bepaald is bereikt, hierdoor kunnen gegevens langdurig worden verwerkt, bijvoorbeeld tot er een onherroepelijk vonnis is of tot een verjaringstermijn is bereikt. Hierna mogen de gegevens nog 6 maanden hergebruikt worden, waarna de bewaartermijn van vijf jaar begint. Na de bewaartermijn moeten de gegevens worden vernietigd. Door grote impact van deze verwerking worden in de Wpg specifiek eisen gesteld. Zo moet de organisatie een bevoegd functionaris aanstellen.

Binnen de gemeente kunnen deze werkingen alleen plaatsvinden in het kader van het domein werk, inkomen en zorg (V) bij de sociaal rechercheur. Gezien de zeer beperkte organisatorische omvang van de gemeentelijke sociale recherche wordt de rol van de bevoegd functionaris bij de leidinggevende of de kwaliteitsmedewerker van de sociaal rechercheur belegd.

4.2 Politiegegevens verstrekken en ter beschikking stellen

Binnen de Wpg bestaan verschillende mogelijkheden om gegevens te delen. Politiegegevens die gedeeld worden binnen het Wpg domein worden ter beschikking gesteld aan de boa of politie. Hierbij geldt altijd dat deze gegevens voor de ontvanger nodig zijn voor de taak.

Als Wpg gegevens gedeeld worden buiten het Wpg-domein dan worden gegevens verstrekt. De gegevens verhuizen dan van het Wpg naar het AVG domein. Elke verstrekking moet worden geadministreerd. Voorbeelden aan wie politiegegevens verstrekt kunnen worden zijn HALT bureaus, school en CJIB.

4.3 Overige uitgangspunten

Vanuit de Wpg worden ook organisatorische eisen gesteld aan de verwerking van politiegegevens. Het gaat om het volgende:

Omgang met politiegegevens

Gegevens die op feiten zijn gebaseerd moeten gescheiden worden van feiten die op een persoonlijk oordeel zijn gebaseerd. Ook moet er onderscheid worden gemaakt tussen verschillende betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden.

Audits

De Wpg verplicht boa-werkgevers tot het uitvoeren van audit. Jaarlijks moet een interne Wpg-audit uitgevoerd worden. Elke vier jaar moet een Wpg-audit door een externe gecertificeerde IT-auditor uitgevoerd worden. De rapportage van de externe Wpg-audit moet worden verstrekt aan de toezichthouder, de Autoriteit Persoonsgegevens.

Eventuele geconstateerde tekortkomingen moeten binnen 3 maanden na het uitvoeren van de audit in een verbeterrapport worden opgenomen. Hierop vindt binnen een jaar een her-controle plaats. De her-controle geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de her-controle worden vastgelegd in een rapportage en eveneens verstrekt aan de toezichthouder, uiterlijk 1 jaar na het uitvoeren van de externe audit.

Geautomatiseerde systemen

In geautomatiseerde systemen moet logging plaatsvinden 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. Ook moet deze logging periodiek gecontroleerd worden.

Van elke systeem moet een autorisatiematrix zijn vastgesteld wat de basis vormt voor de autorisaties van medewerkers. De matrix en autorisaties moeten periodiek gecontroleerd worden.

3. Rollen en verantwoordelijkheden

Binnen de gemeente zijn verschillende rollen en verantwoordelijkheden belegd om uitvoering te geven aan dit privacybeleid.

Gemeenteraad
De gemeenteraad stelt de gemeentelijke brede kaders en uitgangspunten rondom privacy vast. De gemeenteraad controleert het college van B&W bij de uitvoering van deze kaders.

Burgemeester
De burgemeester is voor zover het haar taakuitoefening betreft verantwoordelijk voor de naleving van de beginselen voor verwerking van persoonsgegevens en de maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.

College van burgemeester en wethouders
Het college van burgemeester en wethouders is verantwoordelijk voor het verwerken van persoonsgegevens binnen de gestelde kaders. Het college stelt hiervoor de beleidskaders en specifieke regelingen en procedures vast. Jaarlijks legt ze verantwoording af aan de gemeenteraad over privacy en de toepassing van het privacybeleid, via de paragraaf bedrijfsvoering in de jaarstukken.

Teamleiders
De teamleiders zijn naar de medewerkers verantwoordelijk voor het sturen op en monitoren van de uitvoering van het beleid. Ze stimuleren bewustwording over privacy bij medewerkers. Het vaststellen van doelen en middelen om persoonsgegevens te verwerken is aan de teamleiders gemandateerd. De teamleiders zijn ook verantwoordelijk voor het afhandelen van datalekken binnen hun afdeling.

Functionaris Gegevensbescherming (FG)
Het college van burgemeester en wethouders stelt een FG aan. De FG houdt vanuit een onafhankelijke positie intern toezicht op de omgang met en naleving van de wetgeving voor zowel de AVG als de Wpg. Hij of zij adviseert en ondersteunt de organisatie rondom privacy. Ook zorgt de FG voor een periodieke rapportage over de naleving van de wetgeving. De FG is contactpersoon voor de Autoriteit Persoonsgegevens.

Chief Information Security Officer (CISO)
De CISO ondersteunt, coördineert en adviseert vanuit een onafhankelijke positie over de te nemen maatregelen voor informatiebeveiliging. Hij of zij rapporteert hierover aan het bestuur, de directie en teamleiders.

Buitengewone Opsporingsambtenaren (boa’s)
De gemeente heeft boa’s in dienst. Afhankelijk van de taak valt de gegevensverwerking van de boa’s onder de AVG of de Wpg. Bij bestuursrechtelijke toezichts- en handhavingstaken worden gegevens onder de AVG verwerkt. Bij opsporingstaken vallen de persoonsgegevens onder de Wpg.

Medewerkers (inclusief inhuur/extern)
Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt, binnen de kaders van zijn rol/functie, voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

Autoriteit Persoonsgegevens (AP)
De Autoriteit Persoonsgegevens is de toezichthoudende instantie.

4. Rechten van betrokkenen

Binnen de AVG en Wpg hebben betrokkenen verschillende rechten. In dit hoofdstuk worden deze rechten behandeld.

Recht op informatie
Betrokkenen worden door de gemeente geïnformeerd op het moment dat zijn/haar persoonsgegevens worden verwerkt.

Recht op inzage
Betrokkenen hebben de mogelijkheid om in te zien of, en op welke manier, zijn/haar gegevens worden verwerkt.

Recht op rectificatie
Als duidelijk wordt dat bepaalde gegevens niet juist zijn, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.

Recht op vergetelheid
Betrokken hebben het recht om persoonsgegevens te laten verwijderen, bijvoorbeeld indien de betrokkene zijn toestemming intrekt of de gegevens niet langer nodig zijn. De gemeente stelt eventuele partners van de gemeente, als deze de gegevens ook hebben, op de hoogte dat de betrokkene ook bij hen ‘vergeten’ moet worden.

Recht op beperking gegevensverwerking
Recht op beperking: De betrokkene heeft het recht om een verzoek in te dienen tot beperking van de gegevensverwerking, bijvoorbeeld wanneer de betrokkene de juistheid van de gegevens betwist.

Recht op data portabiliteit
Recht op overdraagbaarheid: Betrokkene heeft het recht op overdraagbaarheid van zijn/haar persoonsgegevens in een gangbaar bestandsformaat ofwel dataportabiliteit. Dit houdt in dat betrokkene zijn gegevens op zo’n manier ontvangt dat hij/zij deze weer gemakkelijk door kan geven aan een ander.

Recht op bezwaar
Betrokkene heeft het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens.

Recht op verzet
Betrokkene heeft het recht aan de gemeente te vragen om zijn/haar persoonsgegevens niet meer te gebruiken.

Om te voldoen aan de vereisten met betrekking tot de rechten van betrokkenen, heeft de gemeente een procedure voor de rechten van betrokkenen opgesteld waarin is beschreven op welke wijze verzoeken worden afgehandeld, wie daarbij welke verantwoordelijkheid heeft en welke uitzonderingen van toepassing zijn. Deze procedure waarborgt een tijdige afhandeling van de verzoeken.

5. Verplichtingen

In de AVG en Wpg zijn verplichtingen opgenomen. In dit hoofdstuk worden wettelijke verplichtingen beschreven. Een aantal verplichtingen heeft een documentaire neerslag.

5.1. Register van verwerkingsactiviteiten

De gemeente houdt een register van hun verwerkingsactiviteiten bij voor zowel de AVG als de Wpg. Hierin wordt een overzicht gegeven van de verschillende processen die bij de gemeente worden uitgevoerd en welke soorten persoonsgegevens worden verwerkt. Dit register wordt periodiek gecontroleerd door de FG. Het register wordt ook gebruikt door de gemeente om te voldoen aan verschillende andere AVG vereisten met betrekking tot verantwoording, door onder meer de juridische gronden te documenteren.

5.2. Datalekken

Op basis van de meldplicht datalekken, worden datalekken gemeld aan de Autoriteit Persoonsgegevens wanneer de inbreuk waarschijnlijk een (hoog) risico vormt voor de rechten en vrijheden van degenen wiens persoonsgegevens bij de inbreuk betrokken waren. Deze melding moet onmiddellijk, maar uiterlijk binnen 72 uur nadat de FG kennis heeft genomen van het datalek, te worden gemeld bij de AP. Als deze termijn niet wordt gehaald, dan wordt de vertraging gemotiveerd bij de melding. In het kader van transparantie meldt de gemeente het datalek ook aan betrokkenen.

De gemeente houdt een register bij van alle beveiligingsincidenten en datalekken. Hierin is vastgelegd of een beveiligingsincident heeft geleid tot een datalek . Als dat het geval is wordt geregistreerd, of het datalek is gemeld en welke corrigerende maatregelen zijn getroffen om de risico’s van het datalek te mitigeren.

De gemeente heeft een proces datalekken geïmplementeerd. In deze procedure is beschreven op welke wijze datalekken worden afgehandeld, wie daarbij welke verantwoordelijkheid heeft en hoe datalekken worden geregistreerd. De bewustwording hieromtrent is een terugkerend onderwerp tijdens awareness sessies en e-learning modules.

5.3. Gegevensbeschermingseffectbeoordeling/data protection impact assessment

Een gegevensbeschermingseffectbeoordeling (GEB) of data protection impact assessment (DPIA) houdt in dat voorafgaand aan een gegevensverwerking de privacyrisico’s in kaart worden gebracht. Voor de gemeente geldt dat voor iedere nieuwe verwerking of een wijziging in een bestaande verwerking een DPIA zal worden uitgevoerd, waarbij sprake is van een waarschijnlijk hoog privacy risico.

Op basis van een DPIA kunnen maatregelen worden getroffen om de risico’s te minimaliseren of uit te sluiten. Ook kan het voorkomen dat het hoge privacyrisico niet kan worden gemitigeerd. In dat geval kan de verwerking van persoonsgegevens niet plaats vinden.

De gemeente heeft een DPIA procedure opgesteld waarin het proces voor het uitvoeren van een DPIA is opgenomen. In deze procedure wordt onder meer besproken welke partijen betrokken moeten worden en aan welke verplichtingen een DPIA moet voldoen.

5.4. Privacy by Design en Privacy by Default

Op grond van de AVG moeten bij de verwerking van persoonsgegevens het Privacy by Design en Privacy by Default principe worden toegepast. Privacy by Design houdt in dat al bij het ontwerpen van producten en diensten persoonsgegevens goed worden beschermd. Bij de inrichting van een proces of de bouw van een systeem worden bijvoorbeeld alleen de persoonsgegevens verwerkt die noodzakelijk zijn voor het doeleinde (dataminimalisatie). Ook wordt gekeken naar de benodigde beveiligingsmaatregelen om de persoonsgegevens te beschermen en wie toegang heeft tot de persoonsgegevens.

Privacy by Default is onderdeel van Privacy by Design en houdt in dat de standaardinstellingen van een programma ingesteld moeten worden op de meeste privacyvriendelijke manier. De gemeente zorgt er voor dat programma's niet meer persoonsgegevens van betrokkenen kunnen verzamelen dan nodig voor het specifieke doeleinde en maakt gebruik van opt-in mogelijkheden.

5.5. Toegangscontrole en logging

Binnen de Wpg domeinen wordt met specifieke systemen gewerkt. Voor zover deze systemen als dienst worden afgenomen geven leveranciers doormiddel van een accountantsverklaring[1] aan te voldoen aan de wettelijke eisen van de Wpg. De gemeente als gebruikersorganisatie is zelf verantwoordelijk voor de inrichting van de applicatie. Dit doet de gemeente door het vaststellen van rollen in een autorisatiematrix. Functionarissen worden op basis van deze autorisatiematrix geautoriseerd. Het gebruik van de applicatie wordt gelogd. Hierdoor is controleren wie wanneer, welke (persoons)gegevens heeft verwerkt. De gemeente heeft hiervoor processen vastgesteld.

5.6. Doorgifte van persoonsgegevens

In het geval van samenwerking met externe partijen, waarbij persoonsgegevens worden verwerkt, maakt de gemeente afspraken over de eisen waaraan de gegevensuitwisseling moet voldoen. Deze afspraken worden door de gemeente vastgelegd in overeenkomsten en zijn overeenkomstig wet- en regelgeving. De gemeente kan voor het uitoefenen van haar taken de verwerking van persoonsgegevens uitbesteden aan verwerkers. Daarbij maakt de gemeente alleen gebruik van verwerkers die voldoende technische en organisatorische maatregelen hebben getroffen en zodoende voldoen aan de AVG en Wpg vereisten. Hiervoor wordt gebruik gemaakt van het model verwerkersovereenkomst van de Vereniging van gemeenten (VNG).

Het kan voorkomen dat de gemeente met een andere partij gezamenlijk verwerkingsverantwoordelijke is, bijvoorbeeld door een samenwerking aan te gaan met een andere gemeente. In dat geval sluit de gemeente een overeenkomst af waarin de verplichtingen en verantwoordelijkheden voor beide partijen zijn opgenomen.

In het register van verwerkingsactiviteiten van de gemeente is per verwerking inzichtelijk of de persoonsgegevens zijn gedeeld met derden, hoe deze derden worden gekwalificeerd en of hiermee een overeenkomst is aangegaan. De kwaliteitsmedeweker controleert de overeenkomsten en de daarin vastgestelde afspraken jaarlijks.

Met betrekking tot doorgifte van persoonsgegevens buiten de Europese Economische Ruimte (EER), geldt het uitgangspunt dat de persoonsgegevens niet worden doorgegeven. Dit uitgangspunt is niet van toepassing op een aantal derde landen, of sectoren binnen die landen, waarvoor een adequaatheidsbesluit is genomen door de Europese Commissie (EC). De EC geeft daarmee aan dat deze landen een passend beschermingsniveau van persoonsgegevens waarborgen conform de AVG. Voorts kan de doorgifte van persoonsgegevens naar landen/organisaties buiten de EER plaatsvinden indien een wettelijke uitzondering of een rechtmatige overdrachtsmechanisme zoals omschreven in de AVG van toepassing is. Voornoemde doorgifte zal iedere keer binnen de voorwaardelijke kaders van wet- en regelgeving plaatsvinden.

[1] Derdenverklaring, ook wel Third Party Mededeling (TPM) genoemd.

6. Actualisatie beleid

Dit privacybeleid wordt minimaal één keer per 3 jaar geactualiseerd, of eerder als dat is nodig vanwege strategische ontwikkelingen, ontwikkelingen in de samenleving of verplichtingen voortvloeiend uit wet- en regelgeving.