Gemeente Wassenaar

Privacybeleid Wassenaar

2025-2030

Eenheid Informatie & Datamanagement

Inhoudsopgave

Inleiding

Bij de uitvoering van haar wettelijke taken verwerkt de gemeente een aanzienlijke hoeveelheid persoonsgegevens. Deze gegevens zijn essentieel voor het leveren van diensten aan haar inwoners. Zonder de verwerking van persoonsgegevens is het bijvoorbeeld onmogelijk om aan een inwoner een uitkering te verstrekken of een vergunning te verlenen. De inwoner moet er echter wel op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met zijn persoonsgegevens omgaat. De verwerking van persoonsgegevens kan namelijk risico's met zich meebrengen.

Een onrechtmatige verwerking van persoonsgegevens kan een inbreuk maken op het recht op eerbiediging van de persoonlijke levenssfeer (lees: het recht op privacy) van een betrokkene. De Algemene Verordening Gegevensbescherming (hierna: AVG) van de Europese Unie (hierna: EU) vormt de basis voor dit beleid en stelt richtlijnen op om er zorg voor te dragen dat de verwerking van persoonsgegevens met de nodige zorgvuldigheid plaatsvindt.

In dit beleidsdocument wordt daarom richting gegeven aan de wijze waarop de gemeente om gaat met het recht op privacy in relatie tot de verwerking van persoonsgegevens. Zij toont aan dat zij de privacy waarborgt, beschermt en handhaaft. De inhoud hiervan is van toepassing op de gehele organisatie en alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente waarin persoonsgegevens worden verwerkt.

Het document is ontwikkeld om structuur en beleidskaders te bieden bij de inrichting van de verplichtingen die de AVG aan de gemeente oplegt en om daarover verantwoording af te leggen. Ook helpt het de organisatie bij de beoordeling of zij genoeg maatregelen neemt om een zorgvuldige verwerking van persoonsgegevens te garanderen. Daarnaast is het gericht aan alle inwoners van de gemeente en andere betrokkenen wiens gegevens worden verwerkt, om hen te informeren over de wijze waarop de gemeente met hun persoonsgegevens omgaat.

De onderwerpen die in dit beleidsstuk aan de orde komen zijn het juridische kader waartoe de gemeente zich dient te verhouden, de organisatorische borging van een zorgvuldige verwerking van persoonsgegevens, de omgang met rechten van betrokkenen en algemene kaders ten aanzien van interne regelingen en afspraken op het gebied van gegevensverwerkingen.

Om te garanderen dat gegevensverwerking binnen de gemeente op een rechtmatige wijze plaatsvindt, wordt dit privacybeleid vastgesteld door het college van burgemeester en wethouders (hierna: het college). Dit beleid weerspiegelt de visie en principes van de organisatie op het gebied van privacy en wordt regelmatig beoordeeld en aangepast waar nodig.

1. Uitgangspunten AVG

Bij de uitvoering van al haar wettelijke taken heeft de gemeente te maken met veel informatie die betrekking heeft op personen. Deze persoonsgegevens worden veelvuldig gebruikt om haar inwoners tot dienst te zijn. Zonder gebruik van deze persoonsgegevens is het voor de gemeente vaak niet mogelijk om invulling te geven aan publieke taken.

Het is dan ook gerechtvaardigd dat de gemeente deze persoonsgegevens gebruikt om haar taken uit te voeren, maar het is wel belangrijk dat de gemeente op een zorgvuldige wijze met deze informatie omgaat. De Algemene Verordening Gegevensbescherming - ook wel de AVG genoemd – is wetgeving van de Europese Unie (hierna: EU) die ervoor probeert te zorgen dat ondernemingen en overheidsorganen bij de verwerking van persoonsgegevens deze zorgvuldigheid in acht nemen. Hiermee probeert de AVG tegemoet te komen aan het recht op privacy dat iedere inwoner binnen de EU heeft.

De gemeente dient zich dus aan de regels uit de AVG te houden. Daarnaast zijn er nog andere wetten die relevant zijn bij de verwerking van persoonsgegevens, maar deze zullen later aan bod komen. Er is een aantal uitgangspunten die van belang zijn om te noemen en waar de gemeente zich aan dient te houden. Deze zullen hieronder worden toegelicht.

1.1. De zes algemene beginselen van de AVG

Bij de verwerking van persoonsgegevens dient de gemeente altijd rekening te houden met de volgende algemene beginselen van de AVG:[1]

1. Rechtmatigheid, behoorlijkheid, transparantie: De gemeente mag alleen persoonsgegevens verwerken wanneer er sprake is van één van de zes grondslagen die worden opgesomd in paragraaf 2.2. Daarnaast dient de gemeente op een behoorlijke manier met persoonsgegevens om te gaan en de betrokkenen hierover op een transparante wijze te informeren. De betrokkenen dienen actief te worden geïnformeerd waarom en welke persoonsgegevens worden verwerkt. De communicatie hierover dient eenvoudig, toegankelijk en begrijpelijk te zijn;
2. Doelbindingsvereiste: Persoonsgegevens mogen enkel voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld, en vervolgens alleen verder worden verwerkt wanneer er sprake is van een verenigbaar doel;
3. Minimale gegevensverwerking (‘dataminimalisatie’): Bij de verwerking van persoonsgegevens mogen deze enkel verwerkt worden voor zover dat strikt noodzakelijk is om het vooraf bepaalde doel te halen. Daarbij dient de gemeente zich ook steeds af te vragen of het doel niet op een minder ingrijpende wijze ook kan worden bereikt. Hiermee wordt bedoeld dat wanneer het mogelijk is om het doel ook te bereiken door minder persoonsgegevens te verwerken of zelfs helemaal niet, voor deze mogelijkheid gekozen dient te worden;

[1] Zie artikel 5 AVG.

4. Juistheidsvereiste: Het is van belang dat voortdurend moet worden nagegaan of de persoonsgegevens die worden verwerkt juist en actueel zijn. Als blijkt dat de gegevens niet meer correct zijn moeten ze door de gemeente gewijzigd of verwijderd worden. Een betrokkene heeft daarom ook het recht om aan de gemeente te verzoeken diens persoonsgegevens te wijzigen. Zie voor meer informatie hierover paragraaf 4.1.;
5. Opslagbeperking: Persoonsgegevens mogen niet langer worden bewaard dan strikt genomen nodig is voor het doel dat door de verwerking bereikt dient te worden;
6. Integriteit en vertrouwelijkheid: De gemeente zorgt voor een goede beveiliging van de persoonsgegevens die zij verwerkt. Hiervoor dient zij passende technische of organisatorische maatregelen te nemen.[2] Meer uitleg over hoe de gemeente dit precies uitvoert, kan worden gevonden in haar Informatiebeveiligingsbeleid.

1.2. De zes rechtmatigheidsgrondslagen van de AVG

Bij de verwerking van persoonsgegevens dient de gemeente zich altijd te baseren op één van de zes juridische grondslagen die in de AVG zijn opgesomd. Als deze grondslag ontbreekt mag de gemeente dus geen persoonsgegevens verwerken voor het bereiken van het beoogde doel. Er kan gebruik worden gemaakt van een van de volgende grondslagen:

1. Toestemming van de betrokkene: De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
2. Uitvoering van een overeenkomst: De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
3. Wettelijke verplichting: De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de gemeente rust;
4. Vitale belangen: De verwerking is noodzakelijk om de vitale belangen van een individu te beschermen;
5. Taak van algemeen belang of openbaar gezag: De verwerking is noodzakelijk 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 gemeente is opgelegd;
6. Gerechtvaardigde belangen van de gemeente: de verwerking is noodzakelijk om tegemoet te komen aan de gerechtvaardigde belangen van de gemeente. De gemeente kan hier geen beroep op doen als het recht op privacy van de betrokkenen zwaarder wegen dan het belang van de gemeente. Ook mag de gemeente geen gebruik maken van deze grondslag wanneer zij uitvoering geeft aan haar normale publieke taken.

Bij de uitvoering van haar publieke taken zal de gemeente voornamelijk een beroep doen op de derde en vijfde grondslag, namelijk dat de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang of openbaar gezag, of wanneer de verwerking noodzakelijk om te voldoen aan een wettelijke verplichting die aan de gemeente is opgelegd. Dit betekent niet dat de andere vier grondslagen niet worden gebruikt door de gemeente, maar deze komen wel veel minder vaak voor.

[2] Zie artikel 25 AVG.

1.3. Verschillende soorten persoonsgegevens

Volgens de AVG zijn er verschillende soorten persoonsgegevens. Er zijn namelijk gewone, gevoelige en bijzondere persoonsgegevens. Dit onderscheid is gemaakt, omdat de verwerking van bepaalde persoonsgegevens sneller of een grotere inbreuk maken op de privacy van de betrokkene. Daarom kunnen de regels strenger worden naar gelang de privacy inbreuk groter wordt. Hieronder worden de verschillende soorten toegelicht.

1.3.1. Gewone en bijzondere persoonsgegevens

In de AVG wordt er een onderscheid gemaakt tussen normale en bijzondere persoonsgegevens. Bij normale persoonsgegevens gaat het om alle informatie over een individu, waarmee hij of zij direct of indirect geïdentificeerd kan worden. Het individu in deze context wordt de 'betrokkene' genoemd.[3]

Wanneer er over bijzondere persoonsgegevens wordt gesproken, gaat het om een specifiek aantal gegevens die in de AVG worden opgesomd.[4] Het gaat om de volgende categorieën van persoonsgegevens:

- Ras of etnische afkomst;
- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuigingen;
- Het lidmaatschap van een vakbond blijken;
- Genetische gegevens[5];
- Biometrische gegevens met het oog op identificatie van een persoon[6];
- Gegevens over de gezondheid, of;
- Gegevens met betrekking tot iemands seksuele geaardheid.

Wanneer de gemeente één of meer van deze bijzondere persoonsgegevens wil verwerken zijn er extra eisen en waarborgen waaraan zij dient te voldoen alvorens hiertoe over mag worden gegaan. Volgens de AVG moet de gemeente, naast een juridische grondslag zoals uitgelegd in paragraaf 2.2, ook expliciet een grondslag hebben uit de Uitvoeringswet AVG (hierna: UAVG).

Hierin zijn namelijk de extra eisen en waarborgen uitgewerkt die bij de verwerking van deze bijzondere gegevens nodig zijn.

---

[3] Gegevens over een overleden persoon zijn overigens geen persoonsgegevens. Gegevens over een rechtspersoon wordt in principe ook niet gekwalificeerd als een persoonsgegevens waarvoor de regels van de AVG gelden.

[4] Zie artikel 9 AVG.

[5] Website AP, *Deze persoonsgegevens geven unieke informatie over iemands fysiologie of gezondheid en/of over de gezondheid van familieleden. Dat maakt de informatie zo gevoelig. In de praktijk gaat het hierbij vooral om informatie over erfelijkheid en genetische kenmerken die het resultaat is van een biologisch monster. Bijvoorbeeld informatie uit analyse van het DNA.*

[6] Website AP, *Dit zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking van iemands kenmerken, waarmee eenduidig vast te stellen is wie iemand is. Bijvoorbeeld met een vingerafdrukscan, gezichtsherkenning, een irisscan of een digitale stemopname.*

1.3.2. Gevoelige persoonsgegevens

Er bestaan ook persoonsgegevens die eigenlijk tussen de gewone en bijzondere persoonsgegevens vallen. Alhoewel bij de verwerking van deze gegevens de gemeente niet hoeft te voldoen aan de eisen in de AVG voor verwerking van bijzondere persoonsgegevens, kunnen er toch extra waarborgen gelden. Er kan bijvoorbeeld specifieke wet- en regelgeving zijn waar de gemeente zich aan dient te houden bij de verwerking van gevoelige persoonsgegevens.

De volgende gevoelige persoonsgegevens zijn voor de gemeente relevant:

- Strafrechtelijke gegevens: Dit zijn gegevens over strafrechtelijke veroordelingen, strafbare feiten en veiligheidsmaatregelen die daarmee verband houden. Deze gegevens mogen alleen worden verwerkt onder leiding van een overheidsorgaan en wanneer de verwerking is toegestaan bij wetgeving die ook oog heeft voor de belangen van de betrokkene.[7] Aangezien de gemeente een overheidsorgaan is, mag zij deze gegevens verwerken als de wet dit aan haar voorschrijft. De gemeente (in dit geval gaat het om het bestuursorgaan de burgemeester) moet bijvoorbeeld regelmatig in het kader van handhaving van de openbare orde en veiligheid strafrechtelijke gegevens verwerken. Daarnaast is er specifieke wetgeving dat ziet op de zorgvuldige verwerking van politiegegevens door buitengewoon opsporingsambtenaren (boa's). In paragraaf 5.1 wordt specifiek aandacht besteed aan de verwerking van politiegegevens door de gemeente.
- Burgerservicenummer (BSN): het BSN is een nummer dat speciaal is ontworpen voor de overheid, zodat zij een betrokkene kan identificeren of informatie kan koppelen. Het is daarmee een hulpmiddel voor de gemeente om ervoor te zorgen dat zij de juiste persoon voor zich heeft en de juiste informatie over de betrokkene gebruikt kan worden. Voor gebruik en beheer van het BSN is de Wet algemene bepalingen burgerservicenummer en aanverwante regelgeving in het leven geroepen. De gemeente houdt zich aan deze regelgeving bij de verwerking van het BSN.
- Financiële gegevens: Voor de gemeente is het regelmatig noodzakelijk om financiële gegevens te verwerken voor de uitvoering van publieke taken en natuurlijk ook in relatie tot haar werknemers. De gemeente draagt er zorg voor dat er op een zorgvuldige en veilige manier met deze gegevens om wordt gegaan.

2. Verantwoordelijkheden binnen de gemeente

In dit hoofdstuk wordt aandacht besteed aan de wijze hoe de AVG de verantwoordelijkheid over de verwerking van persoonsgegevens verdeelt en hoe de gemeente zowel intern als extern hier invulling aan geeft.

2.1. Verwerkingsverantwoordelijke

In de AVG wordt nadruk gelegd op de verantwoordelijkheid van organisaties en instanties (in de AVG aangeduid als 'verwerkingsverantwoordelijken') om te kunnen aantonen dat zij zich aan de wet

[7] Zie artikel 10 AVG en paragraaf 3.2 van de UAVG.

houden (accountability). De verwerkingsverantwoordelijke is degene die alleen of samen met anderen het *doel van en de middelen voor* de verwerking vaststelt.

Het college van burgemeester en wethouders (hierna: het college), de burgemeester en de gemeenteraad (hierna: de raad) zijn de verantwoordelijke bestuursorganen die, ieder voor zover het hun taakuitoefening betreft, invulling geven aan de taken en verantwoordelijkheden die door verschillende wet- en regelgeving aan hen zijn toebedeeld. Zij zijn dus de verwerkingsverantwoordelijken voor de gegevensverwerking volgens de AVG. Als in dit beleidsdocument gemakshalve wordt gesproken van de 'de gemeente' wordt daarmee bedoeld de drie bestuursorganen die de gemeente bezit.

De verantwoordingsplicht van de gemeente brengt met zich mee dat zij niet alleen de geldende privacyregels moet naleven, maar ook kan aantonen dat deze regels zijn nageleefd. Dit houdt bijvoorbeeld in dat de gemeente kan aantonen dat een verwerking van persoonsgegevens voldoet aan de belangrijkste uitgangspunten van de AVG (zie hoofdstuk 1) en dat zij de juiste technische en organisatorische maatregelen heeft getroffen om de persoonsgegevens te beveiligen.

Er rust dus een verplichting op de gemeente om actief te sturen en te bewijzen dat zij haar *privacyhuishouden* op orde heeft. In dit kader worden in ieder geval de volgende maatregelen genomen:

- Het hebben van een privacybeleid dat openbaar wordt gemaakt;
- Het hebben van een informatiebeveiligingsbeleid dat openbaar wordt gemaakt;
- Een actueel en volledig register van verwerkingen bijhouden en het publiceren van een abstract van het register;
- Er wordt verantwoording afgelegd over de verwerking van persoonsgegevens en informatiebeveiliging in het jaarverslag en de jaarrekening van de gemeente;
- De gemeente houdt een register van datalekken bij;
- Data Protection Impact Assessments (hierna: DPIA) worden uitgevoerd bij nieuwe gegevensverwerkingen met een hoog risico. De lijnmanager ondertekent de risicoanalyse af als deze is afgerond;
- De gemeente heeft een algemene privacyverklaring die op haar website is te raadplegen;
- Applicaties worden ingekocht mede op basis van de oplossingen die zij bieden met betrekking tot *privacy by design and default*.
- Bij het inzetten van verwerkers sluit de gemeente een verwerkersovereenkomst af volgens het model van de VNG (zie hiervoor paragraaf 7.2).

2.2. Lijnmanagement

Het eigenaarschap van de processen en systemen waarmee wordt gewerkt, is belegd bij de eenheidsmanagers. Een zorgvuldige verwerking van persoonsgegevens is daar onderdeel van. Daarom zijn zij verantwoordelijk voor het zorgvuldig beheer van alle gegevens in deze systemen, in het bijzonder voor de verwerking van persoonsgegevens, de deugdelijke classificatie van gegevens, de beveiliging ervan en voor het toekennen van rechten in deze systemen. Zij zijn verantwoordelijk voor het zodanig uitvoeren van het beleid dat privacyrisico's tot een minimum worden beperkt.

De dagelijkse verantwoordelijkheid voor de zorgvuldige omgang met persoonsgegevens ligt daarom bij de eenheidsmanagers. Dat betekent dat de lijn kan worden aangesproken op het nakomen van de eisen die uit het privacybeleid voortvloeien. Privacy staat immers niet op zichzelf. Het is onlosmakelijk verbonden met de gemeentelijke dienstverlening.

2.3. Privacy Officer (PO)

De Privacy Officer (hierna: PO) biedt ondersteuning op het gebied van advisering over het handelen conform het privacybeleid en de privacy-administratie. De PO begeleidt de lijnmanagers bij de uitvoering van hun taken op het gebied van het privacybeleid en privacywetgeving. De PO heeft verstand van en kennis over deze taken en is betrokken bij de eenheidsprocessen die worden gestart of reeds plaatsvinden.

Ook begeleidt de PO DPIA's voor zover dat noodzakelijk blijkt te zijn volgens de standaarden van de AP en de AVG. Tot slot is de PO samen met de Chief Information Security Officer (hierna: CISO) verantwoordelijk voor de *Privacy & Informatiebeveiliging bewustwordingscampagne* binnen de gemeente.

De PO werkt nauw samen met de FG en de CISO.

2.4. Functionaris Gegevensbescherming (FG)

De AVG stelt het aanstellen van een Functionaris Gegevensbescherming (hierna: FG) verplicht voor overheidsinstanties en publieke organisaties.[8] De FG ziet er op toe dat de organisatie voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Hij is een interne toezichthouder en houdt toezicht op onder andere de naleving van de wettelijke eisen, gemeentelijke richtlijnen op het gebied van privacy en diens vastgestelde privacybeleid.

De FG is een onafhankelijke functionaris die de verwerkingsverantwoordelijke, namelijk het college, de burgemeester en de gemeenteraad rechtstreeks kan adviseren. De FG werkt nauw samen met de CISO en de PO.

De FG is ook degene binnen de organisatie waarbij de betrokkene terecht kan wanneer zij een klacht hebben ten aanzien van de verwerking van diens persoonsgegevens. Tot slot is de FG aangemeld bij de AP, bij vragen van de AP is de FG benaderbaar en officieel degene die bij een datalek melding maakt bij de AP. Dit laatste kan (en wordt vaak) door de PO namens de FG gedaan.

2.5. Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) is verantwoordelijk voor de informatiebeveiliging binnen de gemeente. De CISO stelt kaders op voor informatiebeveiliging en adviseert het college, de burgemeester of de raad en het lijnmanagement hierover. De CISO houdt toezicht op de informatiebeveiligingsmaatregelen, waaronder de beveiliging van persoonsgegevens. De CISO werkt hierbij nauw samen met de FG en de PO.

[8] Zie artikel 37, 38 en 39 AVG.

3. Governance van de gemeente

Het college en de burgemeester zijn integraal verantwoordelijk voor de bescherming van persoonsgegevens en de uitvoering van de AVG en Wet politiegegevens (Wpg) binnen de werkprocessen van de gemeente. De specifieke rol van het college is het vaststellen van kaders en normen voor privacybescherming om te voldoen aan wet- en regelgeving (compliance) op dit gebied. Het college legt verantwoording af aan de raad over de uitvoering en handhaving van deze kaders en normen.

3.1. Overzicht en inzicht

De gemeente moet overzicht en inzicht hebben in hoeverre zij aansprakelijk is. Hoe groot is de "corporate familie" en verbonden partijen (verwerkers), alsmede de achterliggende partijen (sub-verwerkers). Voor gemeenten is het verkrijgen van het gewenste overzicht een lastige opgave omdat zij met veel organisaties samenwerkt en het niet altijd duidelijk is op basis van welke titel de samenwerking is ingericht.

En natuurlijk is het verkrijgen van overzicht over welke persoonsgegevens er binnen de gemeente zelf allemaal verwerkt worden essentieel. Het hebben van een betrouwbare inventarisatie en vervolgens deze actueel houden, is een belangrijke basis om verdere maatregelen te kunnen treffen.

3.2. Privacy-administratie

Het systematisch vastleggen van verwerkingen van persoonsgegevens, het bewijs van effectieve werking van de getroffen beheers- en beveiligingsmaatregelen, en incidenten en datalekken is daarom erg belangrijk. Dit wordt bereikt door het bijhouden van een actueel verwerkings-, een verwerkersovereenkomsten- en een datalekregister. Het vastleggen van deze informatie wordt in dit beleidsdocument de *privacy-administratie* genoemd. Het college gebruikt deze administratie voor het afleggen van verantwoording over gegevensbescherming aan het maatschappelijk verkeer. Deze privacy-administratie draagt bij aan de verantwoordingsplicht die op de gemeente als verwerkingsverantwoordelijke rust.

3.3. Invulling verantwoordingsplicht

De gemeente verantwoordt zich in het maatschappelijk verkeer op twee manieren:

1. De voortgang en de stand van zaken met betrekking tot de uitvoering van het privacybeleid en andere privacymaatregelen worden in het jaarverslag en de jaarrekening van de gemeente meegenomen;
2. De betrokkenen (inwoners en medewerkers) kunnen hun passieve en actieve rechten uitoefenen. Passieve rechten hebben voornamelijk betrekking op de plicht van de gemeente dat zij betrokkenen uit zichzelf informeert over de verwerking van persoonsgegevens. De gemeente verstrekt de juiste informatie en is daarmee transparant ten aanzien van de gegevensverwerkingen. De betrokkene kan zijn/haar actieve rechten uitoefenen door vragen te stellen aan de gemeente (zie hiervoor hoofdstuk 4). Voor de betrokkene is de FG met

assistentie van de PO het eerste aanspreekpunt. Wanneer dit niet leidt tot een bevredigende uitkomst, kan de betrokkene zich wenden tot de AP;

3.4. Organisatie governance en privacy

De gemeentelijke planning en control cyclus is in essentie zo opgebouwd dat in het jaar t-1 (het jaar voor het begrotingsjaar) de voornemens worden opgesteld en de daarbij behorende middelen worden bepaald in de vorm van een kadernota of perspectiefnota en vervolgens worden vastgesteld in de begroting. Met de vaststelling van de begroting wordt daarmee het ambitieniveau van een onderwerp voor het volgende jaar vastgelegd.

Na afloop van een jaar, in het voorjaar t+1, wordt vervolgens een jaarverslag en jaarrekening opgesteld, waarmee door het college verantwoording over het afgelopen jaar wordt afgelegd.

3.5. De voornemens

Het governance- en compliancemodel van privacy volgt dit stramien van de gemeentelijke *planning en control*. Het start met het opstellen en vaststellen van het privacybeleid, de voornemens worden in de begroting meegenomen en uiteindelijk is het dan onderdeel van het jaarverslag en de jaarrekening als onderdeel van de algehele maatschappelijke verantwoording. In de loop van het jaar en na afloop van het jaar vindt evaluatie van het beleid plaats, die zo nodig tot aanpassing van het beleid kan leiden. Het privacybeleid en de nieuwe voornemens zullen opgebouwd gaan worden aan de hand van een normenkader en worden ingedeeld in het volwassenheidsniveau. Door het hanteren van volwassenheidsniveaus kan het privacybeleid een groeimodel worden.

4. Rechten van de betrokkene

4.1. persoonlijke rechten

Op grond van afdeling 2 van de AVG hebben betrokkenen een aantal rechten ten aanzien van de persoonsgegevens die door de gemeente worden verwerkt. De gemeente faciliteert deze rechten. Op de website van de gemeente kan de betrokkene een *privacy-contactformulier* invullen die hiervoor bestemd is.[9] Voor de verwerking van deze verzoeken is een procedure opgesteld.

Hieronder worden alle rechten toegelicht waar de betrokkene gebruik van mag maken ten aanzien van de persoonsgegevens die de gemeente van hem/haar verwerkt.

Recht op inzage

Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt. Dit wordt uitgevoerd met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

[9] Ook in de privacyverklaring van de gemeente wordt uitdrukkelijk verwezen naar het privacy-contactformulier.

Recht op correctie

Als de gemeente persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de gemeente om dit aan te passen. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

Recht op vergetelheid

Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de gemeente niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld wanneer de betrokkene een eerder gegeven toestemming intrekt, de gegevens onrechtmatig verwerkt zijn of de gegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld. Ook dit wordt uitgevoerd met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

Recht op bezwaar

Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens door de gemeente. De gemeente moet hieraan voldoen, tenzij er dwingende gerechtvaardigde gronden zijn voor de verwerking. Wanneer de gemeente bijvoorbeeld op grond van een wettelijke verplichting, persoonsgegevens van de betrokkene verwerkt, kan zij hiervan niet zomaar afwijken.

Recht op beperking

Wanneer een betrokkene gebruik maakt van het recht op beperking van de verwerking van zijn/haar persoonsgegevens, dient de gemeente hier in principe gehoor aan te geven. De gemeente mag deze persoonsgegevens dan *tijdelijk* en onder voorwaarden niet verwerken of wijzigen. Dit recht kan bijvoorbeeld worden aangewend wanneer de betrokkene de juistheid van de gegevens ter discussie stelt.

Recht op overdraagbaarheid

De gemeente is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van het algemeen belang, de uitoefening van het openbaar gezag, wanneer deze zijn openbare taken uitoefent of aan een wettelijke verplichting moet voldoen. Desondanks zal de gemeente in voorkomende gevallen voorzieningen treffen in het kader van de overdracht.

Verbod op geautomatiseerde besluitvorming, waaronder profilering

Uitgangspunt in de AVG is dat er geen geautomatiseerde besluitvorming op basis van profilering mag plaatsvinden als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) zijn verbonden of het besluit hem in aanmerkelijke mate treft. Daarbij kan gedacht worden aan bijvoorbeeld de kredietwaardigheid van een persoon. Een ander voorbeeld is het verwerken van sollicitaties via internet zonder menselijke tussenkomst.

Dit recht wijkt af van de vorige rechten, omdat het niet een actief recht is waar de betrokkene gebruik van kan maken. Het is eerder een garantie dat zijn/haar persoonsgegevens niet verwerkt worden op de manier zoals in de vorige alinea is omschreven. Dit verbod is echter niet absoluut. Het artikel

noemt namelijk drie uitzonderingen die het verbod opheffen. De gemeente zal zich hieraan houden wanneer zij voornemens is dit verbod te doorbreken.

Recht op informatie

Het recht op informatie is eveneens geen actief recht voor de betrokkene. Het recht op informatie houdt in dat de gemeente bij een verwerking van persoonsgegevens de betrokkene hierover – voor zover hij/zij daar niet reeds van op de hoogte is, dit een onevenredige inspanning vergt van de gemeente of er een zwaarwegend belang voor de gemeente is om dit niet te doen - actief dient te informeren. De gemeente verstrekt dan aan betrokkenen informatie over de gegevensverwerking, zoals het doel daarvan, welke persoonsgegevens worden verwerkt en of de gegevens aan anderen worden verstrekt. Dit met inachtneming van de beperkingen zoals die neergelegd zijn in wet- en regelgeving.

Om hier grotendeels aan tegemoet te komen zal een relevant deel van het register van verwerkingen worden gepubliceerd op de website van de gemeente Wassenaar. Daarnaast heeft de gemeente een privacyverklaring op dezelfde plaats gepubliceerd waarin zij algemene informatie verschaft over de verwerking van persoonsgegevens door de gemeente.

4.2. Uitoefening van rechten

Om gebruik te maken van deze persoonlijke rechten kunnen de betrokkenen een verzoek indienen. Hiervoor is een *Privacy Contact Formulier* op de website van de gemeente aangemaakt. Dit verzoek kan zowel per brief/e-mail als via het contactformulier worden ingevuld en ingediend.

De gemeente behandelt het verzoek uiterlijk binnen een maand. In uitzonderlijke gevallen kan deze behandeltermijn worden verlengd met maximaal twee maanden. Het gaat dan om een verzoek dat te complex is om deze binnen een maand volledig af te handelen. De gemeente stelt de betrokkene hiervan vóór het aflopen van de reguliere behandeltermijn op de hoogte.

Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie elektronisch verstrekt, tenzij de betrokkene uitdrukkelijk anders verzoekt. Deze informatie wordt via een beveiligd bericht aan de betrokkene verstrekt.

Enkel wanneer de gemeente redenen heeft om te twijfelen aan de identiteit van de betrokkene, zal de gemeente aanvullende informatie vragen die nodig is om diens identiteit te bevestigen. De gemeente kan om een identiteitsbewijs verzoeken, tenzij een minder ingrijpende methode voldoende zekerheid biedt.

Zoals gezegd mag de betrokkene in principe al deze genoemde persoonlijke rechten uitoefenen. Het kan echter voorkomen dat hij/zij dit recht op een zodanige wijze uitoefent dat niet van de gemeente gevergd mag worden hieraan tegemoet te komen. Het kan dan gaan om de volgende situaties waarbij de betrokkene:

- zijn/haar verzoek zodanig summier toelicht dat van de gemeente niet gevraagd kan worden om aan het verzoek tegemoet te komen;
- het verzoek met een ander doel indient dan waarvoor deze is gegeven, hij/zij te kwader trouw is ofwel misbruik van het recht maakt;

- het verzoek van de betrokkene kennelijk ongegrond of buitensporig is, met name vanwege het repetitieve karakter.

Wanneer de betrokkene niet tevreden is met de inhoudelijke reactie van de gemeente kan hij/zij:

- in bezwaar gaan bij de bezwaarcommissie van de gemeente en daarna, indien nodig, in beroep bij de bestuursrechter;[10]
- een klacht indienen bij de AP over het functioneren van de gemeente, en/of;
- een klacht indienen bij de Nationale Ombudsman.

5. Aanverwante wet- en regelgeving

Naast de AVG en de UAVG is er een aantal andere wet- en regelgeving die voor de gemeente relevant is bij de verwerking van persoonsgegevens van betrokkenen. In dit hoofdstuk wordt specifiek aandacht besteed aan een aantal relevante regelingen.

5.1. Wet politiegegevens

Sinds begin 2019 is de Wpg in Nederland van kracht gegaan.[11] Deze wetgeving - dat oorspronkelijk in de EU is ontwikkeld - is in het leven geroepen om politiegegevens extra bescherming te geven. Een politiegegeven is volgens de Wpg elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak. De Wpg is dus een wet die van toepassing is op een speciaal soort persoonsgegeven.

5.1.1. Zes domeinen

Voor de gemeente betekent dit dat zij zich aan deze wetgeving dient te houden voor zover er sprake is van een verwerking van politiegegevens. Er zijn zes domeinen waarbinnen politiegegevens verwerkt kunnen worden:

I. Openbare ruimte;

II. Milieu welzijn en infrastructuur;

III. Onderwijs;

IV. Openbaar vervoer;

V. Werk, inkomen en zorg;

VI. Generieke opsporing.

[10] Wanneer een betrokkene van een van zijn/haar rechten gebruik wenst te maken, is de inhoudelijke reactie van de gemeente hierop een besluit in de zin van de Algemene wet bestuursrecht (hierna: Awb). Hierdoor is het hele wettelijke kader van overeenkomstige toepassing.

[11] Aan lagere wetgeving zoals het Besluit politiegegevens en het Besluit politiegegevens buitengewoon opsporingsambtenaren dient de gemeente zich ook aan te houden en is dus ook relevant.

5.1.2. Auditplicht

Volgens de Wpg moet de gemeente niet alleen voldoen aan deze normen, maar dient zij dit ook aantoonbaar te maken door elk jaar een interne audit en eens in de vier jaar een externe audit op de verwerking van politiegegevens uit te laten voeren. De uitkomsten van de externe audit worden ter controle aan de Autoriteit Persoonsgegevens (AP) toegestuurd.

De gemeente heeft zichzelf ten doel gesteld om aan de hand van een vierjarenplan volledig te voldoen aan de Wpg. Hierna blijft de gemeente zichzelf controleren en verbeteren door middel van de auditcyclus.

5.1.3. Privacy by design & default

De Wpg verplicht de gemeente bij de verwerking van politiegegevens het principe van *privacy by design & default* toe te passen. Dit houdt in dat met technische en organisatorische maatregelen de beginselen uit de AVG en de Wpg moeten worden nageleefd.

De (werk)processen dienen vooraf zodanig te zijn ingeregeld, dat tegemoet wordt gekomen aan het beginsel van minimale gegevensverwerking. Dit houdt in dat de gegevens niet langer worden bewaard dan strikt noodzakelijk, enkel worden gebruikt voor een gerechtvaardigd doel en het aantal werknemers dat toegang heeft tot deze gegevens wordt beperkt.

5.1.4. Overig

Er is geconstateerd dat de gemeente voor de verwerking van politiegegevens geen bijzondere persoonsgegevens verwerkt. De verplichtingen die uit de Wpg voortkomen worden hierdoor gedeeltelijk beperkt.

Speciaal voor de verwerking van politiegegevens is een verwerkingsregister opgesteld. Dit register geeft een actueel overzicht van de politiegegevens die binnen de gemeente worden verwerkt. Daarnaast is de verwerking van politiegegevens opgenomen in het algemene verwerkingsregister.

Bij de verwerking van politiegegevens doet de gemeente niet aan geautomatiseerd vergelijken en in combinatie zoeken. Hierdoor zijn de voorwaarden die de Wpg hieraan stelt niet op de gemeente van toepassing.[12]

Tot slot is vastgesteld dat de gemeente in de uitvoering van haar taken geen politiegegevens deelt met derde landen.

5.2. Wet basisregistratie personen

De gemeente houdt van al haar inwoners een basisregistratie personen bij (hierna: BRP). Wanneer een betrokkene zich inschrijft of uitschrijft bij de gemeente wordt dit in de BRP geregistreerd. Daarnaast worden ook andere gebeurtenissen geregistreerd, wanneer een betrokkene in de gemeente wordt geboren of juist overlijdt. Samenvattend gaat het om alle inwoners in de gemeente (ingezetenen) en alle inwoners die de gemeente (of zelfs Nederland) verlaten hebben (niet

[12] Voor de voorwaarden zie art. 11 Wpg.

ingezetenen). Bij de verwerking en gebruik van deze gegevens dient de gemeente zich te houden aan de Wet basisregistratie persoonsgegevens (hierna: Wet BRP). [13]

5.2.1. Gegevensverwerking in BRP

Er worden veel persoonsgegevens in de BRP geregistreerd. De volgende gegevens over de betrokkene staan in de basisregistratie:

- BSN;
- NAW-gegevens;
- Geslacht;
- Geboortedatum;
- Geboorteplaats;
- Geboorteland;
- Gegevens over de ouders;
- Nationaliteit;
- Huwelijk/geregistreerd partnerschap;
- Overlijden;
- Inschrijving in de BRP;
- Verblijfplaats;
- Kind;
- Verblijfstitel;
- Reisdocument.

5.2.2. Doel van gebruik BRP

Het eerste lid van artikel 1.3 Wet BRP zegt het volgende: *De basisregistratie heeft tot doel overheidsorganen te voorzien van de in de registratie opgenomen gegevens, voor zover deze gegevens noodzakelijk zijn voor de vervulling van hun taak.* Overheidsorganen - en dus ook de gemeente - hebben een algemene bevoegdheid om BRP-gegevens te gebruiken voor zover dat noodzakelijk is voor de uitvoering van hun wettelijk toebedeelde publieke taken.

De gemeente dient echter wel altijd rekening te houden met de zorgvuldigheidseisen uit de AVG. Het kan daarom voorkomen dat voor de uitvoering van een publieke taak geen gebruik wordt gemaakt van persoonsgegevens uit de BRP, omdat bijvoorbeeld het doel op een andere minder ingrijpende methode bereikt kan worden (subsidiariteit) of dat het gebruik ervan niet in verhouding staat tot het te bereiken doel (proportionaliteit). Bij een nieuw initiatief waarbij er gebruik gemaakt gaat worden van de BRP-gegevens, dient daarom altijd voorafgaand een privacy-toets (DPIA) uitgevoerd te worden.

5.2.3. Verstrekking aan derden

Op grond van de Verordening gegevensverstrekking basisregistratie personen Wassenaar 2014 (hierna: Verordening BRP Wassenaar) – dat door het college in het leven is geroepen – verstrekt het

[13] Aan lagere wetgeving, zoals het Besluit basisregistratie personen en de Regeling basisregistratie personen, dient de gemeente zich ook aan te houden.

college aan de eenheid Informatie & Datamanagement (hierna: I&D), het Klant Contact Centrum (hierna: KCC), Maatschappelijke Ontwikkeling en Ondersteuning (hierna: MOO), POI-COM (Koninklijke onderscheiding) en PU-VG gegevens uit de BRP.

De gemeente kan op verzoek van andere overheidsorganen gegevens uit de BRP aan hen verstrekken. Het vragende orgaan moet het verzoek onderbouwen met redenen waarom deze gegevens noodzakelijk zijn voor de uitvoering van diens publieke taken.

Het tweede lid van art. 1.3 Wet BRP zegt het volgende: *De basisregistratie heeft mede tot doel derden te voorzien van de in de registratie opgenomen gegevens, in bij of krachtens deze wet aangewezen gevallen.* De gemeente kan dus – wanneer de wet dit toelaat – gegevens uit de BRP ook aan derden verstrekken.

Om hier invulling aan te geven heeft het college in de Verordening BRP Wassenaar bepaald dat verstrekking aan derden mogelijk is wanneer betrokkenen voorafgaand toestemming hiervoor verlenen of wanneer aan derden wordt verstrekt die werkzaamheden uitvoeren met een gewichtig maatschappelijk belang. De derden die aan dit criterium voldoen zijn door het college middels een aanwijsbesluit aangewezen.[14]

De verstrekking van BRP-gegevens aan derden kan uitsluitend betrekking hebben op algemene gegevens over de naam, het geslacht, de geslachtsnaam van de echtgenoot dan wel geregistreerde partner, de eerdere echtgenoot of eerdere geregistreerde partner, het gebruik door de ingeschrevene van de geslachtsnaam van de echtgenoot dan wel geregistreerde partner, de eerdere echtgenoot of eerdere geregistreerde partner, het adres, de bijhoudingsgemeente, de geboortedatum en de datum van overlijden.[15]

Verstrekking aan derden blijft in principe volledig achterwege wanneer de betrokkene zich heeft aangemeld voor de voor beperking van verstrekking aan derden.[16] De betrokkene kan zich hiervoor aanmelden via de website van de gemeente.[17] De Wet BRP biedt een mogelijkheid om hiervan af te wijken, maar de gemeente neemt als uitgangspunt dat zij hier slechts in zeer uitzonderlijke gevallen gebruik van zal maken.

5.3. Wet algemene bepalingen BSN

Het BSN is een persoonsnummer dat het mogelijk maakt om personen te identificeren en om verschillende informatie over een individu te koppelen en te verbinden aan elkaar. Het BSN voorkomt daarmee verwisseling van personen en helpt bij de uitvoering van overheidstaken.

De Wet algemene bepalingen BSN (hierna: Wet BSN) stelt dat *overheidsorganen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik kunnen maken van het*

[14] Zie Aanwijzing werkzaamheden met een gewichtig maatschappelijk belang en categorieën van derden die in aanmerking komen voor verstrekking van gegevens uit de basisregistratie personen | Lokale wet- en regelgeving (overheid.nl).

[15] Zie artikel 3.9 Wet BRP.

[16] Zie artikel. 3.21 Wet BRP.

[17] Zie Geheimhouden persoonsgegevens | Wassenaar.

burgervicenummer, met inachtneming van hetgeen bij of krachtens dit hoofdstuk is bepaald.[18] De gemeente mag dus het BSN gebruiken voor zover dat nodig is voor een goede uitvoering van diens taken.

Echter, ook bij de verwerking van het BSN dient de gemeente rekening te houden met de zorgvuldigheidseisen uit de AVG. Het kan daarom voorkomen dat voor de uitvoering van een publieke taak geen gebruik wordt gemaakt van het BSN, omdat dit niet noodzakelijk is.

Soms stelt een wettelijke regeling dat de gemeente verplicht is om het BSN te verwerken,[19] maar wanneer dit niet expliciet wordt genoemd mag de gemeente nog steeds het BSN verwerken bij de uitvoering van diens publieke taken. Het verschil is dat in het eerste geval de wetgever de noodzakelijkheidstoets voor de gemeente reeds heeft uitgevoerd en in de tweede situatie dient de gemeente deze toets zelfstandig te maken.

Het BSN mag dus breed door de gemeente worden ingezet, ook wanneer zij in contact treedt met andere overheidsorganen. Dit ligt echter anders wanneer zij communiceert met derden, die geen overheidsorganen zijn. De gemeente mag namelijk alleen het BSN met een derde delen wanneer dit expliciet in een wettelijke regeling is opgenomen. Het BSN kan immers een fraudegevoelig gegeven zijn en daarom dient er buiten het publieke domein erg voorzichtig met dit persoonsnummer omgegaan te worden. De gemeente houdt zich vanzelfsprekend aan deze zorgvuldigheidsnormen en verstrekt enkel aan derden het BSN wanneer zij expliciet verplicht is om dat te doen.

5.4. Wet open overheid

De Wet open overheid (hierna: Woo) is een Nederlandse wet die het recht op toegang tot overheidsinformatie regelt. Deze wet vervangt de Wet openbaarheid van bestuur (hierna: Wob) sinds 1 mei 2022. De Woo heeft als doel de transparantie van de overheid te vergroten. Dit betekent dat overheidsorganisaties verplicht zijn om informatie actief openbaar te maken en beschikbaar te stellen wanneer iemand daarom vraagt. Dit helpt inwoners, journalisten en Kamerleden om de overheid te controleren en draagt bij aan een beter functionerende democratie.

De gemeente onderschrijft deze uitgangspunten. Onder deze wet is zij verplicht om veel informatie actief of passief openbaar te maken. Aangezien in deze informatie ook persoonsgegevens verwerkt kunnen worden, kan de AVG van toepassing zijn.

5.4.1. Verhouding tussen de AVG en de Woo

De AVG en de Woo moeten in balans worden gebracht om zowel transparantie als privacy te waarborgen. Hier zijn enkele belangrijke punten over hoe de AVG wordt toegepast op de verplichting tot openbaarheid volgens de Woo:

1. Bescherming van Persoonsgegevens: De gemeente moet ervoor zorgen dat bij het openbaar maken van informatie geen persoonsgegevens worden gedeeld zonder geldige reden. Dit betekent dat persoonsgegevens in de meeste gevallen geanonimiseerd of

[18] Zie artikel 10 Wet BSN.

[19] Denk bijvoorbeeld aan artikel 7.2.1 van de Jeugdwet.

gepseudonimiseerd moeten worden voordat de informatie openbaar wordt gemaakt[1] Bij de openbaarmaking van informatie maakt de gemeente daarom gebruik van een applicatie die in de te publiceren informatie alle persoonsgegevens identificeert en zwart lakt wanneer dat moet volgens de uitzonderingsgronden die in de volgende paragraaf worden genoemd.

2. Rechtmatigheid en Doelbinding: wanneer onder de Woo *wel* persoonsgegevens openbaar worden gemaakt, moet het voldoen aan de beginselen van de AVG, zoals rechtmatigheid, doelbinding en dataminimalisatie. Dit houdt o.m. in dat alleen die persoonsgegevens openbaar mogen worden gemaakt die noodzakelijk zijn voor het doel van de openbaarmaking.
3. Verantwoordingsplicht: Overheidsinstanties moeten kunnen aantonen dat zij voldoen aan de AVG bij het openbaar maken van informatie. Dit betekent dat zij moeten documenteren welke afwegingen zijn gemaakt bij de beslissing om bepaalde informatie wel of niet openbaar te maken

5.4.2. Uitzonderingsgronden Woo

De Woo houdt in artikel 5.1 en 5.2 rekening met de AVG door een aantal verwerkingen van persoonsgegevens uit te zonderen van de plicht tot openbaarmaking onder die wet. Daarbij wordt een onderscheid gemaakt tussen relatieve en absolute uitzonderingsgronden.

1. Absolute uitzonderingsgronden

Artikel 5.1, eerste lid onder d van de Woo stelt dat het niet toegestaan is om *bijzondere persoonsgegevens* en *persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten* openbaar te maken. Dit is een harde regel, dus deze persoonsgegevens moeten in beginsel altijd zwartgelakt worden, tenzij de betrokkene uitdrukkelijk toestemming heeft verleend voor de openbaarmaking van zijn/haar persoonsgegevens. Het voorgaande betekent dat deze persoonsgegevens feitelijk vrijwel altijd geanonimiseerd moeten worden.

Artikel 5.1, eerste lid onder e van de Woo stelt dat nationale identificatienummers ook niet openbaar mogen worden gemaakt, tenzij verstrekking geen inbreuk maakt op de levenssfeer. Met deze 'tenzij' zal de gemeente voorzichtig zijn, aangezien er makkelijk met een BSN gefraudeerd kan worden. Uit jurisprudentie blijkt bovendien dat niet snel wordt aangenomen dat het publiceren van een BSN *geen* inbreuk maakt op iemands persoonlijke levenssfeer. Onder het begrip 'nationaal identificatienummer' valt het BSN, maar ook een Vreemdelingennummer of een ander nummer dat volgens een formele wet kan worden gebruikt ter identificatie van een persoon.[20]

2. Relatieve uitzonderingsgronden

Artikel 5.1, eerste lid onder e van de Woo legt uit dat informatie openbaar maken achterwege blijft als het niet opweegt tegen de *eerbiediging van de persoonlijke levenssfeer*. Hieronder valt voornamelijk de openbaarmaking van (normale) persoonsgegevens. Dit betekent dat de gemeente een afweging moet maken tussen het algemeen belang openbaarmaking ten opzichte van het recht op privacy van de individuele betrokkene. Dit klinkt erg cryptisch en doet vermoeden dat bij de

[20] Zie artikel 46 UAVG.

openbaarmaking van persoonsgegevens telkens opnieuw een afweging moet worden gemaakt tussen de genoemde belangen. Gelukkig valt dit erg mee. Uitgangspunt is dat normale inwoners die in het contact met de gemeente privacygevoelige gegevens verstrekken (of die uit andere hoofde bij de gemeente berusten) erop moeten kunnen vertrouwen dat dit niet zomaar openbaar wordt gemaakt. De gemeente zal daarom in beginsel bij de publicatie van informatie de persoonsgegevens anonimiseren, tenzij expliciet blijkt dat dit niet hoeft. Het beroepsmatig handelen van inwoners heeft in beginsel geen betrekking op de persoonlijke levenssfeer en een rechtspersoon kent in zijn geheel geen persoonlijke levenssfeer.

3. Uitzondering persoonlijke beleidsopvattingen

Volgens artikel 5.2 van de Woo wordt bij de openbaarmaking van documenten ten behoeve van intern beraad, geen informatie verstrekt over daarin opgenomen persoonlijke beleidsopvattingen. Hieronder wordt in ieder geval verstaan:

- Ambtelijke adviezen;
- Visies;
- Standpunten en overwegingen ten behoeve van intern beraad;

Onder persoonlijke beleidsopvattingen wordt in ieder geval niet verstaan:

- feiten;
- Prognoses;
- Beleidsalternatieven;
- De gevolgen van een bepaald beleidsalternatief;
- Andere onderdelen met een overwegend objectief karakter.

Daarentegen zegt het tweede lid van het artikel dat persoonlijke beleidsopvattingen met het oog op de democratische bestuursvorming alsnog openbaar gemaakt worden, maar dan in niet naar personen herleidbare vorm. Als degene toestemming geeft voor openbaarmaking hoeft de inhoud niet geanonimiseerd te worden.

De gedachte achter deze beperkingsgrond is om te waarborgen dat bij de voorbereiding van beleid en besluitvorming binnen het bestuur optimaal van gedachten kan worden gewisseld. Hierdoor is er een vertrouwelijke sfeer om ideeën te kunnen bedenken zonder dat er enige vrees hoeft te zijn. Daarnaast beoogd deze beperkingsgrond dat er geen recht bestaat voor verzoekers op de overheidsinformatie die onvolledig en onrijp is. Het verschaffen van deze informatie zou kunnen leiden tot onnodige onrust of onjuiste verwachtingen.

4. Uitzonderingen op de uitzonderingsgronden

Artikel 5.1, zevende lid van de Woo stelt dat de absolute en relatieve uitzonderingsgronden niet van toepassing zijn op milieu-informatie met betrekking tot emissie.

Tot slot stelt artikel 5.3 van de Woo stelt dat voor het gebruik van de genoemde uitzonderingsgronden een verzwaarde motiveringsplicht (zie artikel 5.1 derde lid van de Woo) geldt als het gaat om informatie ouder dan 5 jaar.

5.4.3. Anonimiseren & niet-openbaar maken

Wanneer er is besloten dat bepaalde persoonsgegevens in een document op een van de hiervoor genoemde gronden onder de Woo niet openbaar gemaakt mogen worden, doet de gemeente het volgende:

1. Het document wordt openbaar gemaakt, maar de betreffende persoonsgegevens worden zwartgelakt.
2. Het document wordt niet openbaar gemaakt, omdat door het zwartlakken van de persoonsgegevens niet kan worden voorkomen dat de identiteit van de betrokkene(n) geheim blijft. Dit kan het geval zijn wanneer uit de context van de inhoud van het document blijkt over welke betrokkene het gaat. Enkel het weglakken van de persoonsgegevens doet dan geen recht aan het recht op privacy.

De beoordeling van de toepasselijkheid van de uitzonderingsgronden uit de Woo en het zwart lakken van de persoonsgegevens vindt geautomatiseerd plaats door een speciaal hiervoor aangetrokken applicatie. Nadat de applicatie dit heeft uitgevoerd wordt het nog een laatste keer gecontroleerd door een werknemer van de gemeente alvorens de informatie openbaar wordt gemaakt. Door het (deels) geautomatiseerde proces is het voor de gemeente mogelijk om op grote schaal informatie openbaar te maken en te voldoen aan de Woo.

5.4.4. B&W besluitenlijsten

Tot slot dient er nog aandacht te worden besteed aan de publicatie van de besluitenlijst van het college en de verwerking van persoonsgegevens hierbij. Artikel 60, derde lid van de Gemeentewet bepaalt namelijk dat het college de besluitenlijst moet publiceren: *Het college maakt de besluitenlijst van zijn vergaderingen op de in de gemeente gebruikelijke wijze openbaar. Het college laat de openbaarmaking achterwege voor zover het aangelegenheden betreft ten aanzien waarvan op grond van artikel 55 geheimhouding is opgelegd of ten aanzien waarvan openbaarmaking in strijd is met het openbaar belang.*

Hieruit volgt dat besluitenlijsten openbaar gemaakt moeten worden, maar niet de achterliggende stukken. Daarnaast verplicht het niet tot openbaarmaking noch publicatie van persoonsgegevens. Het al dan niet openbaar maken en publiceren van namen of andere persoonsgegevens is dus afhankelijk van de noodzakelijkheid ervan. In de meeste gevallen is de gemeente van mening dat het niet noodzakelijk zal zijn om persoonsgegevens die hierin voorkomen te openbaren.

5.5. Wet- en regelgeving binnen het Sociaal Domein

De gemeente verwerkt binnen alle domeinen allerlei soorten persoonsgegevens, maar het sociaal domein neemt een bijzondere positie in. Binnen het sociaal domein worden namelijk bovenmatig veel persoonsgegevens verwerkt die vaak ook nog eens bijzonder van aard zijn. Daar bovenop zijn de betrokkenen vaak minder mondig en vinden het moeilijker om voor hun eigen rechten op te komen.

Het is daarom zaak dat de gemeente extra zorgvuldig omgaat met de gegevensverwerking van deze doelgroep.

Ook de wetgever heeft bij het uitvaardigen van sociaal domeinwetgeving rekening gehouden met de precaire positie van deze doelgroepen in de samenleving. Zij heeft namelijk speciaal hoofdstukken geweid aan de wijze waarop omgegaan dient te worden met de persoonsgegevens van de betrokkenen. De gemeente dient en wil zich hier aan committeren. Specifiek gaat het om de Jeugdwet, de Wet maatschappelijke ondersteuning (hierna: Wmo), de Wet gemeentelijke schuldhulpverlening (hierna: Wgs) en de Participatiewet.[21]

De gemeente voert met betrekking tot de Jeugdwet en de Wmo haar toeleidingstaak uit. Hiervoor heeft zij consulenten in dienst die jongeren en volwassenen helpen bij het vinden van passende zorg- of hulpverlening. Na een onderzoek neemt de gemeente (in de meeste gevallen) een beschikking ten aanzien van de hulpvraag. Een verzoek voor een voorziening kan direct bij de gemeente worden ingediend of kan op advies van het Sociaal Team Wassenaar bij de consulenten terechtkomen.

5.5.1. Sociaal Team Wassenaar

Het Sociaal Team Wassenaar is een samenwerkingsverband tussen de gemeente en hulpverleningsorganisaties die laagdrempelige hulp verlenen. De gemeente regelt de toeleiding en verdeelt aanmeldingen van hulpvragen onder de organisaties die deelnemen aan het verband. Deze hulpverlening is geen uitvoering van een maatwerkvoorziening, maar een algemene voorziening in het *voorliggend veld*.

Bij de verwerking van dit samenwerkingsverband is grondig onderzoek gedaan naar een methode die tegemoetkomt aan een zorgvuldige verwerking van persoonsgegevens. De gemeente verwerkt hierin enkel persoonsgegevens in het kader van de uitvoering van haar publieke taken. Hierin wordt met name tegemoet gekomen aan de taakstelling zoals bepaald in de Jeugdwet en de Wmo.

5.5.2. Werk & inkomen

De gemeente Wassenaar, Voorschoten en Leidschendam-Voorburg (hierna: gemeente LV) zijn in 2012 een samenwerkingsverband aangegaan op het gebied van werk & inkomen. In de samenwerkingsovereenkomst is bepaald dat er een gezamenlijke uitvoeringsorganisatie in het leven wordt geroepen die opereert binnen de ambtelijke organisatie van de gemeente LV.

De uitvoeringsorganisatie neemt de uitvoering van alle voorkomende werkzaamheden en de dienstverlening op zich in het kader van de bijstandsverlening, de voorzieningen voor arbeidsongeschikte werkloze werknemers en (ex-)zelfstandigen, de re-integratie van werkzoekenden, inburgering, schuldhulpverlening, sociale recherche dan wel enige andere in de toekomst voor de desbetreffende wetten en regelingen in de plaats komende regelingen.

Aan de samenwerkingsovereenkomst is later een overeenkomst van gezamenlijke verwerkingsverantwoordelijkheid toegevoegd. De verwerking van persoonsgegevens binnen de

[21] Inclusief lagere wetgeving dat haar oorsprong vindt in de wet in formele zin.

uitvoeringsorganisatie is immers een bevoegdheid die plaatsvindt binnen de gezamenlijke verwerkingsverantwoordelijkheid van de drie gemeenten.

In deze overeenkomst zijn afspraken gemaakt over de verdeling van verantwoordelijkheden waar de uitvoeringsorganisatie aan moet voldoen op grond van de AVG. Zo houdt de uitvoeringsorganisatie het datalek- en verwerkingsregister bij, de FG van de gemeente LV meldt een datalek met een hoog risico voor betrokkenen bij de AP, en de betrokkenen kunnen hun privacyrechten bij de gemeente LV indienen. In de privacyverklaring op de website van de gemeente wordt hiernaar verwezen.

6. Bewaartermijnen

De termijn hoe lang persoonsgegevens bewaard worden, behoort tot een van de beginselen uit de AVG. Het betreft het beginsel van de opslagbeperking dat in paragraaf 1.1. als volgt wordt omschreven: *Persoonsgegevens mogen niet langer worden bewaard dan strikt genomen nodig is voor het doel dat door de verwerking bereikt dient te worden.*

De gemeente dient daarom voorafgaand aan de verwerking van persoonsgegevens zich altijd te vergewissen wanneer het doel van de verwerking is volbracht zodat de gegevens niet langer bewaard worden. Daarbij dienen alle omstandigheden van het te bereiken doel te worden meegewogen. Nadat deze bewaartermijn is bepaald, is het noodzakelijk dat ook naar de praktische invulling wordt gekeken zodat de gegevens daadwerkelijk op het juiste moment worden verwijderd. Het heeft hierbij altijd de voorkeur dat een dergelijke verwijdering geautomatiseerd plaatsvindt (*privacy by design and default).*

Het komt regelmatig voor dat in wet- en regelgeving is bepaald hoe lang de gemeente persoonsgegevens dient te bewaren. In dat geval maakt de gemeente dus niet zelf die afweging, want deze is al voor haar gemaakt. Een goed voorbeeld is de bewaartermijnen die in de Selectielijst gemeenten en intergemeentelijke organen 2020 (hierna: VNG Selectielijst) zijn opgenoemd. Deze lijst met bewaartermijnen bepaald alle bewaartermijnen voor de gemeente met betrekking tot archivering. Vanzelfsprekend committeert de gemeente zich hieraan.

7. Interne regelingen & afspraken

In dit hoofdstuk komen een aantal relevante regelingen en afspraken aan bod die een zorgvuldige omgang met persoonsgegevens ondersteunen en afdwingen.

7.1. Meldplicht datalekken

Indien zich een datalek voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt de gemeente in overeenstemming met de vastgestelde werkwijze in het Protocol Meldplicht en afhandeling van (vermoedelijke) datalekken. Dit protocol bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een datalek te beperken en de getroffen betrokkene(n) te beschermen.

Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden, waarbij beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat geen of onvoldoende beveiligingsmaatregelen zijn genomen. Ook gaat het om situaties waarbij persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn, en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

De plicht tot het melden aan de Autoriteit Persoonsgegevens van een (vermoeden van een) datalek geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene(n), dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het (mogelijk) lekken van persoonsgegevens uit gemeentelijke bestanden en/of gegevens waarvoor de gemeente verantwoordelijkheid draagt.

Wanneer er een dergelijk datalek heeft plaatsgevonden, wordt dit zonder onredelijke vertraging uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval wordt dit datalek – tenzij er zwaarwegende redenen zijn om dit niet te doen - ook aan de betrokkenen gemeld, in eenvoudige en duidelijke taal.

De gemelde datalekken worden door de PO bijgehouden in het datalekregister. De FG ziet erop toe dat deze wordt bijgehouden en up-to-date is.

7.2. Gegevensverwerkingsovereenkomsten

Wanneer de gemeente in samenwerking met andere partijen of organisaties persoonsgegevens verwerkt, dient de gemeente met hen een gegevensverwerkingsovereenkomst te sluiten. Een dergelijke overeenkomst kan nooit op zichzelf staan, maar is altijd verbonden aan een hoofdovereenkomst. Dit kan een samenwerkingsovereenkomst of een overeenkomst van opdracht zijn, maar er zijn meer vormen denkbaar. Het gaat erom dat er in de hoofdovereenkomsten afspraken en doelstellingen zijn gemaakt waarbij het voor de uitvoering hiervan noodzakelijk is om persoonsgegevens te verwerken.

Er zijn drie verschillende vormen van gegevensverwerkingsovereenkomsten denkbaar:

1. Verwerkersovereenkomst: wanneer de gemeente het doel en de middelen van de verwerking bepaalt, maar de uitvoering door een derde partij laat doen wordt een verwerkersovereenkomst gesloten. De gemeente maakt gebruik van het VNG model "Standaard verwerkersovereenkomsten gemeenten". Slechts in uitzonderlijke gevallen wordt hiervan afgeweken.[22]

[22] In de meeste gevallen is de gemeente de verwerkersverantwoordelijke die een verwerkersovereenkomst afsluit met een verwerker, maar in uitzonderlijke gevallen komt het voor dat de gemeente bij het sluiten van een verwerkersovereenkomst zelf optreedt als verwerker. In dat geval mag de wederpartij bepalen welke verwerkersovereenkomst er wordt gebruikt en kan dus voor een ander model worden gekozen dan het model van de VNG. De gemeente zal de inhoud altijd beoordelen en bepalen of zij hiermee akkoord kan gaan alvorens zij deze overeenkomst tekent.

2. Gegevensuitwisselingsovereenkomst: wanneer de gemeente persoonsgegevens met een derde partij uitwisselt, en deze partij vervolgens onder eigen verwerkingsverantwoordelijkheid deze persoonsgegevens gaat verwerken dient er een gegevensuitwisselingsovereenkomst te worden afgesloten. De VNG heeft hiervoor geen modelovereenkomst gepubliceerd. De gemeente probeert wel de inhoud van de gegevensuitwisselingsovereenkomst zo veel mogelijk te laten aansluiten bij de tekst van de verwerkersovereenkomst van de VNG.
3. Overeenkomst Gezamenlijke Verwerkingsverantwoordelijken: tot slot sluit de gemeente een overeenkomst van gezamenlijke verwerkingsverantwoordelijken af wanneer er in het kader van een samenwerkingsverband tussen twee of meerdere partijen gezamenlijk het doel en de middelen van de verwerking van persoonsgegevens wordt bepaald.

De eenheidsmanagers zijn ervoor verantwoordelijk dat, voorafgaande aan de start van de gegevensverwerking, met de wederpartij een daartoe geschikte gegevensverwerkingsovereenkomst wordt afgesloten. De PO dient altijd te worden betrokken om de eenheid hierin te adviseren en begeleiden. De PO houdt een register van de getekende verwerkingsovereenkomsten bij zodat het overzicht bewaart blijft. De FG ziet er op toe dat dit register wordt bijgehouden en up-to-date is.

Tot slot is het belangrijk dat *bijlage 1* van de gegevensuitwisselingsovereenkomst goed wordt ingevuld door zowel de gemeente als de wederpartij. Dit is een samenspel waarin wordt bepaald welke persoonsgegevens noodzakelijk zijn om te verwerken ter uitvoering van de hoofdovereenkomst. *Bijlage 2* van de gegevensuitwisselingsovereenkomst benoemt het beveiligingsniveau waar de verwerker aan dient te voldoen. De CISO controleert bijlage 2 alvorens deze ondertekend wordt. De eisen waaraan dient te worden voldaan worden genoemd in het Informatiebeveiligingsbeleid van de gemeente. Tot slot voegt de gemeente in beginsel altijd de GIBIT-voorwaarden als bijlage aan de verwerkersovereenkomst toe. Enkel in overleg met de gemeente kan hier (gedeeltelijk) van worden afgeweken.

7.3. Register van verwerkingsactiviteiten

De FG houdt er toezicht op dat er een register van verwerkingen van persoonsgegevens wordt bijgehouden. De PO draagt zorg voor de inschrijving van de verwerkingen van persoonsgegevens in dit register. Eenheidsmanagers dienen (nieuwe) verwerkingen of wijzigingen direct aan de PO te melden. Daarnaast gaat de PO één keer per jaar langs bij eenheidsmanagers om na te gaan of alles nog klopt.

Bij de inschrijving worden in ieder geval de volgende gegevens vermeld:

a) de naam van de verwerking;
b) wie de verantwoordelijke is voor de verwerking;
c) het doel van de verwerking;
d) de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
e) de categorie persoonsgegevens die bij de verwerking worden gebruikt;
f) de ontvangers van de gegevens;

g) de rechtmatige grondslag voor de verwerking van de persoonsgegevens;
h) eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;
i) de verwijderingstermijnen die in acht genomen worden;

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende documenten.

7.4. Data Protection Impact Assessment (DPIA)

Een DPIA is een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA wordt doorgaans uitgevoerd met ondersteuning van de PO. Dit gebeurt meestal voorafgaand aan de verwerking, maar ook bij bestaande verwerkingen wanneer dit noodzakelijk wordt bevonden.

De gemeente bepaalt aan de hand van een *quickscan* en/of een pre-DPIA of de verwerking een hoog risico voor de rechten en vrijheden van de betrokkenen met zich mee brengt. Bij een positief resultaat dient een DPIA te worden uitgevoerd.

Op grond van de AVG is in ieder geval sprake van een hoog privacy-risico indien de gemeente:

- Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profilering;
- Op grote schaal bijzondere persoonsgegevens verwerkt of op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied. Hierbij wordt gelet op het aantal betrokkenen, het volume van gegevens en/of het bereik van verschillende gegevens/items die worden verwerkt, de duur of het permanente karakter van de gegevensverwerkingsactiviteit en de geografische omvang van de verwerkingsactiviteit;
- Indien wordt voldaan aan twee of meer criteria van de in bijlage 1 opgenomen criteria van de werkgroep van Europese privacy-toezichthouders (WP29).

Bij de uitvoering van een DPIA gelden de volgende kaders:

1. Een DPIA vindt plaats vóórdat met de betreffende verwerking wordt gestart.
2. Een DPIA wordt herhaald bij wijzigingen waardoor de risico's van de verwerking toenemen.
3. Bij het uitvoeren van een DPIA wordt de FG altijd geïnformeerd.
4. Het afdelingshoofd ziet toe op het nemen van maatregelen die blijkens de DPIA nodig zijn om de risico's te verkleinen.
5. Het resultaat van de DPIA en de genomen maatregelen om het risico te beperken worden aan de FG voorgelegd ter toetsing en opneming in het verwerkingsregister.
6. DPIA's die binnen de gemeente worden uitgevoerd vinden plaats volgens een gemeentelijke standaard.

7.5. Gegevensverwerking door cameragebruik

De gemeente past op verschillende plekken binnen haar organisatie registratie van bewegende beelden toe. Voorbeelden hiervan zijn beelden van bewakingscamera's, burgerloketten, bodycams van boa's en wachtkamers. Voor elke registratie van camerabeelden bepaalt de gemeente of en

hoe lang deze worden bewaard. Er worden videotulen gemaakt van raads- en commissievergaderingen. Eventuele insprekers worden daarover ingelicht.

Er wordt een specifiek beleidsdocument opgesteld over de verschillende manieren van verwerking van persoonsgegevens bij cameragebruik door de gemeente. Hierin wordt specifiek aandacht besteed aan het juridisch kader en de informatiebeveiligingseisen die hierop van toepassing zijn.

7.6. Autorisatiebeleid

Medewerkers van de gemeente mogen alleen toegang hebben tot die persoonsgegevens die zij voor hun werk nodig hebben. Het is gewenst dit zorgvuldig vast te leggen en hier regelmatig een controle op te voeren. Hiertoe worden zo veel als mogelijk in de systemen harde toegangsgrenzen ingericht en alle systemen moeten van de mogelijkheid tot logging zijn voorzien en er dient op gezette tijd hierop controle te worden uitgevoerd.

Nadere uitwerking van deze materie kan worden teruggevonden in het beleidsdocument dat opgesteld zal gaan worden.

8. Deelnemingen

Vaak hebben gemeenten taken uitbesteed aan Gemeenschappelijke Regelingen (hierna: GR) (op basis van juridische titel) en samenwerkingsverbanden (zonder juridische titel). Meestal is er dan sprake van uitbesteding van een of meerdere verwerkingen. Ook de gemeente heeft verschillende soorten deelnemingen. Bij de meeste deelnemingen heeft de gemeente wel invloed, maar is zij samen met de andere deelnemers bepalend voor het uitzetten van de koers. Privacyrechtelijk reist hierdoor regelmatig de vraag wie in dit verband verwerker, verwerkingsverantwoordelijke of gezamenlijk verwerkingsverantwoordelijken zijn.

Voor de beantwoording van de vraag of de deelnemingen verwerkingsverantwoordelijke zijn, is het van belang om te onderzoeken:

1. wie het *doel en de middelen* van de verwerking van persoonsgegevens bepaalt;[23]
2. wie op grond van de wet bepaalde persoonsgegevens moet of mag verwerken, en;
3. of de deelnemingen op grond van mandaat of delegatie handelen.

In het register van verwerkingen (zie hiervoor paragraaf 7.3) worden de deelnemingen in samenwerkingsverbanden bij de specifieke verwerkingen van persoonsgegevens opgenomen, zodat zichtbaar is waar de verwerkingen plaatsvinden en wie er verantwoordelijk is voor de gegevensverwerking.

[23] Het gaat hier met name om de *essentiële* middelen.

Bijlage 1 Begrippenlijst

Autoriteit Persoonsgegevens (AP): de AP is de landelijke toezichthouder op het gebied van gegevensbescherming.

AVG (Algemene Verordening Gegevensbescherming): Europese privacywetgeving waarin de belangrijkste regels voor de omgang met persoonsgegevens in Nederland zijn geregeld. In sectorale wetgeving zoals de WMO of Participatiewet kunnen nadere regels voor de omgang met persoonsgegevens zijn opgenomen ter uitvoering van de betreffende wet.

Buitengewoon opsporingsambtenaar (boa): Een boa is in Nederland een beëdigd functionaris die is bevoegd tot de opsporing van bepaalde, meestal een beperkt aantal of een specifieke groep, strafbare feiten. De gemeente beschikt ook over een aantal boa's. Het college is hun werkgever.

Betrokkenen: degene wiens persoonsgegevens worden verwerkt. Dit kunnen bijv. inwoners of medewerkers zijn.

Datalek: bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens.

DPIA (Data Protection Impact Assessment): ook wel bekend als PIA of gegevenseffectbeoordeling. Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Functionaris voor de gegevensbescherming (FG): de FG is de onafhankelijk toezichthouder op de omgang met persoonsgegevens binnen de gemeente. De FG controleert en adviseert de gemeente op het gebied van gegevensbescherming.

Gemeente: is een verzamelbegrip voor de drie bestuursorganen dat de gemeente kent, te weten het college van burgemeester en wethouders, de burgemeester en de gemeenteraad.

Grondslag: de juridische basis voor de gegevensverwerking.

Persoonsgegevens: ieder gegeven dat is te herleiden tot een individuele persoon. Het gaat niet alleen om vertrouwelijke gegevens, maar om ieder gegeven dat te herleiden is tot een bepaalde persoon, zoals naam, adres, geboortedatum, maar ook kenteken en telefoonnummer.

Privacy Officer (PO): een privacy-adviseur die de gemeente adviseert op casusniveau bij gegevensbescherming binnen de organisatie.

Privacy by Design (Pbd): concept dat inhoudt dat privacy wordt meegenomen tijdens de ontwerpfase van een informatiesysteem of nieuw product.

Privacy by Default (Pbd): concept dat aangeeft dat instellingen van programma's, apps, websites, diensten of apparaten standaard zodanig zijn ingesteld dat maximale privacybescherming wordt nagestreefd.

UAVG (Uitvoeringswet algemene verordening gegevensverwerking): De UAVG is een Nederlandse wet die de AVG uitvoert.

Verwerken: alle handelingen die met persoonsgegevens kunnen worden verricht, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een derde en vernietigen.

Verwerker: een verwerker is een persoon of organisatie die persoonsgegevens verwerkt namens de gemeente Zwolle.

Verwerkingsverantwoordelijke: de eindverantwoordelijke voor de verwerking van persoonsgegevens. In de gemeente is het college van burgemeester en wethouders meestal verantwoordelijk voor het verwerken van persoonsgegevens. Dit betekent dat het college bepaalt wat er met de gegevens gebeurt. De burgemeester of gemeenteraad kunnen ook afzonderlijk verwerkingsverantwoordelijke zijn.

Verwerkingsregister: in het verwerkingsregister staat informatie opgesomd van alle processen binnen de gemeente waarbij persoonsgegevens worden verwerkt. Zoals de doeleinden, de soort persoonsgegevens en de bewaartermijnen.

Verwerkersovereenkomst: als een derde partij persoonsgegevens verwerkt voor de gemeente Zwolle dienen hiermee afspraken te worden gemaakt in de vorm van een verwerkersovereenkomst. Hierin staat onder andere opgenomen hoe de bescherming en verwerking van persoonsgegevens is geregeld.

Wetgever: de regering en beide kamers van de Staten-Generaal die gezamenlijk de bevoegdheid hebben om nationale wetten uit te vaardigen.

Wpg (Wet politiegegevens): De Wpg is een Nederlandse wet die de rechten en de plichten van de politie zelf, maar ook die van de inwoner regelt, voor wat betreft het verwerken van politiegegevens. Sinds 2019 is deze wetgeving ook van toepassing op boa's bij de opsporing van strafbare feiten.