Beleid Algemene verordening gegevensbescherming (AVG) gemeente Harlingen 2021-2023

Inhoudsopgave

1. Inleiding

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) van toepassing. Deze verordening is de opvolger van de Wet bescherming persoonsgegevens. De AVG zorgt samen met de Uitvoeringswet AVG (UAVG) onder andere voor:

1. versterking en uitbreiding van de privacyrechten van betrokkenen
2. meer verantwoordelijkheden voor organisaties die persoonsgegevens verwerken.

De AVG legt de verantwoordelijkheid bij een organisatie neer om aan te tonen dat aan de privacyregels wordt voldaan. Door te voldoen aan de verantwoordingsplicht (accountability) wordt een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy geleverd.

2. Uitgangspunten voor de gemeente Harlingen

De AVG is het centrale kader en biedt het belangrijkste houvast voor de wijze waarop de gemeente omgaat met persoonsgegevens. Rechtmatigheid, behoorlijkheid en transparantie zijn de centrale uitgangspunten van de AVG voor de gemeente en in dit beleidskader staat hoe de gemeente Harlingen deze gaat realiseren.

Digitalisering en de toepassing van nieuwe technologieën leiden tot veranderingen in de samenleving. Hierdoor verschuiven ook de verwachtingen die inwoners hebben van de gemeentelijke dienstverlening, het beheer van de openbare ruimte, het toezicht en de handhaving, en de wijze waarop het beleid vorm krijgt. Het gebruik van gegevens speelt een belangrijke rol bij het waarmaken van die verwachtingen. De gemeente hecht veel waarde aan een betrouwbare verwerking van informatie, zeker als het persoonsgegevens betreft. Er wordt gestreefd naar kwalitatief hoogwaardige dienstverlening met daarbij een zorgvuldige omgang met persoonsgegevens.

3. Belangenafweging

Het is relevant te beseffen dat bij de verwerking van persoonsgegevens verschillende belangen bij elkaar kunnen komen. Dat vraagt om een zorgvuldige afweging, per situatie, in de tijd en binnen en tussen domeinen. Naast het belang van de individuele inwoner, is er het publieke (algemeen) belang en zijn er belangen van burgers ten opzichte van elkaar.

- Belang van de inwoner: inwoners van de gemeente Harlingen willen dat persoonsgegevens veilig en betrouwbaar worden verwerkt en dat transparant is wat de gemeente met de informatie doet. De wensen kunnen wel van verschillend karakter zijn. Aan de ene kant heeft de burger er belang bij dat zo min mogelijk gegevens worden opgeslagen en niet langer worden bewaard dan noodzakelijk. Aan de andere kant verwacht de burger efficiënte dienstverlening.
- Publiek belang: de gemeente kan geen publieke taken uitoefenen zonder verwerking van persoonsgegevens. De gemeente behartigt publieke belangen als efficiënte en effectieve dienstverlening en handhaving van de openbare orde en veiligheid. Voorbeelden zijn het betalen van uitkeringen en armoedevoorzieningen, de handhaving op betaling van parkeergeld en de aanpak van overlast.

- Belangen van burgers ten opzichte van elkaar: de bescherming van de rechten van de ene burger kan ingrijpende gevolgen hebben voor de belangen en de rechten van de ander. Optreden in een geval van ernstige woonoverlast kan er bijvoorbeeld toe leiden dat de overlastgever zijn woning moet verlaten.

Wanneer persoonsgegevens worden verwerkt, dan vindt voorafgaand daaraan een toets plaats over de toelaatbaarheid die volgt uit de AVG en eventueel andere van toepassing zijnde wet- en regelgeving. De gemeente maakt een analyse, zodat de risico's van de verwerking vooraf inzichtelijk zijn. Door middel van een onderbouwde belangenafweging wordt besloten over de toelaatbaarheid van de gegevensverwerking en de wijze waarop de risico's beheerst worden. Als er aanleiding toe is wordt dit voorgelegd aan het politiek verantwoordelijke lid van het college, die het inbrengt in het college als er sprake is van een complexe en/of politiek gevoelige verwerking van persoonsgegevens. Bij deze analyse wegen de maatschappelijke belangen die gediend zijn met de betreffende verwerking binnen de wettelijke kaders af tegen het belang van de bescherming van persoonsgegevens. Als het voor de uitoefening van een taak of beleidskeuzes bijvoorbeeld wenselijk is te weten hoeveel personen in een pand wonen dan volstaat het aantal en is het niet nodig om de namen te vermelden. Wanneer het voor onderzoeksdoelen noodzakelijk is om persoonsgegevens te gebruiken worden de resultaten zo gepresenteerd dat deze niet meer herleidbaar zijn tot personen.

Het college is er verantwoordelijk voor dat de verwerking van de persoonsgegevens voldoet aan de AVG en het beleid inzake persoonsgegevens. Het Managementteam is namens het college verantwoordelijk voor de rechtmatige verwerking van persoonsgegevens en handelen op basis van een mandaat van het college.

4. **Beleid Privacy**

4.1 Waarom beleid?

Dit privacybeleid geeft naast het wettelijk kader weer wat binnen de gemeente Harlingen van belang is als het gaat om de bescherming van persoonsgegevens en de privacy van burgers. Door een betrouwbare en veilige gemeente te zijn dragen we bij aan de democratische rechtsstaat en vertrouwen in de overheid. Dit beleid is bedoeld om deze waarden uit te dragen als het gaat om de bescherming van persoonsgegevens. Zo kunnen we actuele vraagstukken rondom gegevensbescherming adequaat aanpakken.

4.2 Voor wie is het beleid bedoeld?

Het beleid is van toepassing op de hele organisatie, op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente Harlingen. Het college stelt het beleid vast.

4.3 Welke wettelijke kaders zijn van toepassing?

Verwerkingen van persoonsgegevens zijn gebonden aan wet- en regelgeving. In deze wet- en regelgeving staan bepalingen die aangeven hoe met de bescherming van persoonsgegevens moet worden omgegaan. De belangrijkste wettelijke kaders staan in:

- Artikel 8 Europese Verdrag voor de Rechten van de Mens;
- Artikelen 10 t/m 13 Grondwet;
- De Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG;

Wetten gericht op de uitvoering in specifieke sectoren zoals:

- Wet Maatschappelijke Ondersteuning 2015;
- Participatiewet;
- Jeugdwet;
- Wet op de gemeentelijke schuldhulpverlening;
- Wet Inburgering (vanaf 2022)
- Wet Algemene bepalingen Omgevingswet (WABO);
- Wet openbaarheid van bestuur (Wob);
- Wet Basis Registratie Personen;
- Drank- en Horecawet
- Archiefwet
- Wetboek van Strafrecht
- Wet politiegegevens

Naast de wet- en regelgeving van buiten kent de gemeente ook eigen kaders die van invloed zijn op de verwerkingen van persoonsgegevens:

- ✓ Informatieveiligheidsbeleid;
- ✓ Autorisatiebeleid;
- ✓ Wachtwoordbeleid.

5. Uitgangspunten

Uitgangspunten

Iedereen die binnen de gemeente werkzaam is, gaat verantwoord om met de bescherming van persoonsgegevens. Hierbij hanteren wij de volgende centrale uitgangspunten:

A) Persoonsgegevens worden rechtmatig, behoorlijk en transparant verwerkt

Persoonsgegevens worden alleen verwerkt als dat noodzakelijk is voor het doel en er een geldige grondslag uit de AVG is aan te wijzen. Dat betekent dat de verwerking alleen plaatsvindt als dat in verhouding staat tot het doel en als het doel met een vergelijkbare inspanning bereikt kan worden met een lichter middel, voor dat lichtere middel wordt gekozen.

Daarbij wordt de betrokkene (waar het kan) vooraf geïnformeerd voor welke doelen persoonsgegevens worden verwerkt en hoe dat gebeurt.

B) Doelbinding

Persoonsgegevens worden alleen verwerkt als vooraf de doeleinden zijn bepaald en deze precies zijn omschreven. Wanneer de persoonsgegevens later voor een ander doel nodig zijn, dan worden deze alleen gebruikt als het nieuwe doel verenigbaar is met het oorspronkelijke doel.

C) Minimale gegevensverwerking

Alleen die persoonsgegevens worden verwerkt die minimaal noodzakelijk zijn voor het doel. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

D) Persoonsgegevens zijn juist

Alle redelijke maatregelen worden getroffen om te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn worden gewist of gecorrigeerd.

E) Persoonsgegevens worden niet langer bewaard dan nodig

Persoonsgegevens worden niet langer bewaard dan dat nodig is voor het doel waarvoor ze zijn verzameld. Wanneer de gegevens niet langer nodig zijn, worden ze vernietigd of gewist volgens de geldende regelgeving (onder andere Archiefwet 1995).

F) Integriteit en vertrouwelijkheid

Er wordt voor gezorgd dat:

- persoonsgegevens goed beveiligd worden opgeslagen om misbruik, verlies, onbevoegde toegangen bewerking te voorkomen;
- aandacht wordt besteed bij inrichting van processen en systemen aan privacy verhogende maatregelen (privacy by design);
- persoonsgegevens beveiligd zijn en hierbij de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd wordt;
- persoonsgegevens alleen toegankelijk zijn voor die functionarissen (ambtenaren, externen, leveranciers, convenantpartners) die dat nodig hebben voor de directe taakuitoefening;
- het gebruik van persoonsgegevens zoveel mogelijk wordt vastgelegd met uitgevoerde handelingen (logging);
- er wordt gewerkt met geheimhoudingsverklaringen en contractuele afspraken bij het inschakelen van externen en leveranciers.

5.1 Centrale uitgangspunten toegelicht

Rechtmatigheid, behoorlijkheid en transparantie zijn de centrale uitgangspunten vanuit de AVG voor de gemeente. Deze uitgangspunten lichten we hieronder toe.

Rechtmatigheid (artikel 6 AVG)

De gemeente gaat uit van de geldende wet- en regelgeving voor gegevensverwerking en hanteert de AVG als basis. Voor verwerking van persoonsgegevens moet altijd een wettelijke grondslag bestaan.

- Wettelijke grondslagen (limitatief):
  - ✓ Algemeen belang / openbaar gezag;
  - ✓ Wettelijke verplichting;
  - ✓ Vitaal belang;
  - ✓ Overeenkomst;
  - ✓ Gerechtvaardigd belang;
  - ✓ Toestemming (enkel inzetten als geen andere grondslag van toepassing is).[1]

[1] Toestemming is alleen rechtmatig als die in vrije wil is gegeven en er een gelijkwaardige relatie is ten opzichte van de gemeente. Vanwege de afhankelijkheidsrelatie die de betrokkene met de gemeentelijke organisatie heeft, is toestemming meestal niet geschikt. Van vrije toestemming zal over het algemeen geen sprake kunnen zijn, omdat burgers afhankelijk zijn van de gemeente voor hulp of ondersteuning.

- De gemeente legt alleen persoonsgegevens vast als dit noodzakelijk is voor het doel van de verwerking, bijvoorbeeld om te voldoen aan een wettelijke verplichting of om de belangen van betrokkene te beschermen.
- De gegevensverwerking binnen de gemeente voldoet aan de beginselen van proportionaliteit en subsidiariteit. Proportionaliteit houdt in dat alleen die persoonsgegevens worden vastgelegd die in redelijke verhouding staan tot het doel van de verwerking. En subsidiariteit houdt in dat als het doel kan worden bereikt met behulp van een lichter middel, de gemeente dan kiest voor dat laatste.

Behoorlijkheid

- De gemeente streeft naar minimale gegevensverwerking.
- De gemeente bewaart persoonsgegevens niet langer dan noodzakelijk. De noodzakelijkheid is voor de gemeente altijd gerelateerd aan het doeleinde waarmee de persoonsgegevens zijn verkregen.
- Alleen functionarissen (ambtenaren, externen, leveranciers, convenantpartners) waarvoor het voor de directe taakuitoefening noodzakelijk is, hebben inzage in persoonsgegevens. De gemeente gaat zorg dragen voor het 'loggen' (het vastleggen van met data uitgevoerde handelingen) daar waar dat noodzakelijk is. Er wordt gewerkt met geheimhoudingsverklaringen voor externen en leveranciers en met externe partners worden convenanten afgesproken.
- Persoonsgegevens worden goed beveiligd opgeslagen zodat ze adequaat zijn beschermd tegen misbruik, verlies, onbevoegde toegang en bewerking. Door gebruik te maken van 'privacy by design' besteedt de gemeente al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht aan privacy-verhogende maatregelen.

Transparantie

- De gemeente is open en transparant over hoe zij met persoonsgegevens omgaat. Door de waarborg dat afwijkingen van dit beleidskader beargumenteerd worden voorgelegd aan het college en / of de burgemeester wordt maximaal invulling gegeven aan transparantie richting inwoners en de gemeenteraad.
- Als iets mis gaat met persoonsgegevens zal het datalek worden gemeld bij de Autoriteit Persoonsgegevens. Ook over hoe vaak het mis gegaan is en wat er misgegaan is, is de gemeente open en transparant (artikel 33 en 34 AVG).
- Indien het datalek grote gevolgen kan hebben voor de betrokkene, bijvoorbeeld identiteitsfraude, informeert de verwerkingsverantwoordelijke de betrokkene in eenvoudige en heldere taal.
- Het melden van beveiligingsincidenten zal plaatsvinden volgens de procedure datalekken.
- Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem /haar heeft verzameld en waarvoor die worden gebruikt. Als burgers willen weten welke gegevens over hem/haar worden verzameld en waarvoor die worden gebruikt, verstrekt de gemeente de gevraagde informatie tenzij de in de wet genoemde belangen zich daartegen verzetten. Ook kunnen burgers om verbetering, aanvulling of verwijdering van persoonsgegevens verzoeken. Dit verzoek wordt gehonoreerd, tenzij ook hier weer de in de wet genoemde belangen zich daartegen verzetten (bijvoorbeeld opsporingsbelang).

- De gemeente is transparant over het type persoonsgegevens dat zij binnen een specifiek doel met derden deelt, tenzij er belangen zijn, genoemd in wet- of regelgeving, die zich daartegen verzetten.

6. Basis

6.1 Register van verwerkingen (artikel 30 AVG)

De gemeente Harlingen vindt het belangrijk dat er een integraal overzicht bestaat van de informatiehuishouding en de getroffen beheersmaatregelen. Hiermee komt zij de wettelijke eis van de registerplicht na. Tevens kan hiermee op ieder moment worden aangetoond hoe aan de verplichtingen van de AVG wordt voldaan. Hiervoor wordt een actueel elektronisch register van verwerkingsactiviteiten bijgehouden.

Wijzigingen en gestaakte verwerkingen worden met het oog op de bewijslast gearchiveerd. Wanneer de Autoriteit Persoonsgegevens daarom vraagt, stelt het college het register ter beschikking.

6.2 Accountability: rapportage en normenkader (artikel 5 lid 2 AVG)

Op de verwerkingsverantwoordelijke ligt de verplichting tot het afleggen van verantwoording over naleving van de AVG en andere wettelijke privacyregels. Jaarlijks wordt gerapporteerd.

6.3 Data Protection Impact Assessment (DPIA) (artikel 35 AVG)

Onder de Algemene verordening gegevensbescherming zijn organisaties verplicht Data Protection Impact Assessments (DPIA's) uit te voeren. Dat is een instrument om (liefst) vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Vervolgens kunnen daarna maatregelen worden ingesteld om de risico's te verkleinen. DPIA's zijn verplicht bij risicovolle verwerkingen en gewenst bij alle verwerkingen. Op grond van de vastgestelde risico's worden maatregelen genomen. Een DPIA moet altijd worden gedaan voor de start van een geautomatiseerde verwerking, bijvoorbeeld cameratoezicht. Bij een grootschalige verwerking of wanneer er een monitoring in de openbare ruimte wordt beoogd, geldt ook een DPIA, bijvoorbeeld bij Smart City toepassingen.

De Autoriteit persoonsgegevens heeft de volgende lijst opgesteld waarbij de verplichting tot uitvoering van een DPIA geldt ook als de verwerking reeds jaren plaatsvindt:

- ✓ Heimelijk onderzoek
- ✓ Zwarte lijsten
- ✓ Fraudebestrijding
- ✓ Creditscores
- ✓ Financiële situatie
- ✓ Genetische persoonsgegevens
- ✓ Gezondheidsgegevens
- ✓ Samenwerkingsverbanden
- ✓ (Flexibel) cameratoezicht
- ✓ Controle werknemers
- ✓ Locatiegegevens
- ✓ Communicatiegegevens
- ✓ Internet of Things
- ✓ Profilering en toepassen nieuwe technologieën (bijvoorbeeld algoritmes) .

De DPIA met advies en conclusie wordt aan de FG en aan het PIT (Privacy en Informatiebeveiligingsteam blz. 11) voorgelegd. Aangegeven advisering op mogelijke risico's en maatregelen dienen door de verantwoordelijke in de organisatie tijdens het PIT geaccepteerd te worden of te worden opgevolgd.

Het afnemen van een DPIA zal plaatsvinden volgens de procedure DPIA.

6.4. Verantwoordelijkheden

Het privacybeleid van de gemeentelijke organisatie wordt vastgesteld door het college van Burgemeester en Wethouders (hierna: het college) en gecontroleerd door de gemeenteraad. Hierna worden de verschillende rollen en bevoegdheden toegelicht. Als de organisatie werkt op de wijze die hier beschreven staat, dan is het framework aanwezig waardoor het beleid bestendig verder kan worden uitgerold en tevens kan worden gecontroleerd.

Gemeenteraad

De gemeenteraad ziet er op toe dat het college overkoepelend beleid ten aanzien van bescherming van persoonsgegevens voor de organisatie vaststelt. Door de gemeenteraad worden voor de uitvoering hiervan de benodigde middelen beschikbaar gesteld. Voorts controleert hij het college bij de uitvoering van deze kaders. Hij wordt hiertoe in staat gesteld door de verantwoordingsinformatie. Dit is onder meer het jaarlijkse verslag van de Functionaris Gegevensbescherming (FG), die het college verschaft.

College van B&W

Het college is integraal verantwoordelijk voor zorgvuldigheid van verwerking van persoonsgegevens. Zij is het meest aangewezen bestuursorgaan die de passende bescherming van persoonsgegevens waarborgt. Zo is zij verantwoordelijk voor een duidelijk te volgen privacybeleid, doet aan de gemeenteraad voorstellen over in te zetten middelen en stelt specifieke regelingen en procedures vast.

Het college heeft de burgemeester als portefeuillehouder aangewezen die namens het college de beleidsvoering waarborgt. Daarnaast legt deze (politieke) verantwoording af over de privacy beleidsvoering aan de Raad.

Gemeentesecretaris /directie

De uitvoeringsverantwoordelijkheid voor gegevensbescherming ligt bij de gemeentesecretaris. De gemeentesecretaris is de Algemeen directeur, de hoogste ambtenaar binnen de ambtelijke organisatie en de eerste adviseur aan het college. Hij of zij vormt dus de schakel tussen het bestuur en ambtelijke organisatie en is in dit kader ambtelijk verantwoordelijk.

De gemeentesecretaris is samen met de het management verantwoordelijk voor de uitvoering van het AVG-jaarplan, een juiste uitvoering van privacybeleid en stuurt op (concern) risico's. Daarnaast zorgen zij voor een passend niveau van informatieveiligheid en gegevensbescherming binnen de organisatie.

Uitvoering: teammanagers

De zorgvuldige omgang van verwerkingen valt onder de teammanagers (proceseigenaar) binnen de verschillende vak-afdelingen. Dat betekent dat zij zelf moeten zorgdragen voor het nakomen van de

naleving van het privacybeleid binnen hun organisatieonderdeel (bijvoorbeeld burgerzaken, sociaal domein, griffie, belastingen). Ook zijn zij verantwoordelijk voor voldoende bewustwording waarin zij worden ondersteund door de Privacy officer, CISO en/of de FG. Daarnaast worden centraal bewustzijnscampagnes georganiseerd.

De teammanager stuurt onder meer aan op:

- verzoeken tot uitvoering van een Data Protection Impact Assessments (DPIA's) bij het DPIA-team.
- naleving van principes van privacy by design & default;
- het hanteren van daartoe vastgestelde procesplannen en formats, zoals de DPIA en de (door de VNG/IBD vastgestelde) verwerkersovereenkomst;
- dat datalekken volgens de daartoe te volgen procedure zo snel mogelijk bij de Privacy Officer, CISO of Servicedesk worden gemeld;
- het melden en uitwerken van nieuwe verwerkingen en gewijzigde verwerkingen in het register van verwerkings-activiteiten;
- het informeren en het afhandelen van de rechten van de betrokkene;
- het maken van schriftelijke afspraken bij risicovolle verwerkingen en verwerkingen bij ketensamenwerking (verwerkingen in een samenwerkingsverband);
- het bekend maken van dit privacybeleid bij haar medewerkers.

Medewerkers

Alle medewerkers (inclusief inhuur/externen) zijn ervoor verantwoordelijk dat zorgvuldig wordt omgegaan met persoonsgegevens. Dat betekent dat iedereen, binnen de kaders van zijn taak, zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Indien er twijfel bestaat of aan deze beginselen uitvoering wordt gegeven, schakelt men de lijnmanager, FG of het PIT in.

<u>Ondersteuning en advies</u>

Om de organisatie te ondersteunen bij vraagstukken die leven omtrent de bescherming van persoonsgegevens en de directie te ondersteunen bij de uitvoering van het jaarplan AVG, zijn de volgende medewerkers belast:

Privacy Officer (PO)

De Privacy Officer (PO) is specialist voor de AVG en adviseert en ondersteunt bij vraagstukken omtrent de bescherming van persoonsgegevens. De PO is verantwoordelijk voor het verwerkingsregister en handelt de verzoeken van burgers tot inzage, wijziging of verwijdering af. Daarnaast coördineert de PO de uitvoering van DPIA's. Gevraagd en ongevraagd adviseert de PO over activiteiten ter bescherming van persoonsgegevens.

Daarnaast is de PO de verbindende schakel tussen de organisatie en de FG.

Chief Information Security Officer (CISO)

In het kader van de privacy heeft de CISO tevens een rol in ondersteuning en advies. Op het gebied van informatiebeveiliging heeft zij een controlerende en toezichthoudende rol. Informatiebeveiliging

maakt een wezenlijk onderdeel uit van de bescherming van persoonsgegevens. De CISO adviseert tevens bij projecten en het beheersen van risico's.

DPIA-werkgroep

Voor het uitvoeren van DPIA's is een zelfstandige DPIA-werkgroep ingesteld. In de werkgroep zit een juridisch adviseur, de CISO, een vertegenwoordiger van de ICT en de Privacy Officer. De interne werkgroep bepaalt in overleg met de verantwoordelijke (teammanager) en PO welke DPIA's worden uitgevoerd. De bevindingen uit de DPIA's worden meegenomen in de verdere uitwerking of als aandachtspunt gehouden voor de toekomst. Jaarlijks zullen deze punten geëvalueerd worden met de verantwoordelijken in het PIT.

Privacy en Informatiebeveiligingsteam (PIT)

De organisatie wordt waar nodig ondersteund door het Privacy en Informatiebeveiligingsteam (PIT). Dit team bestaat uit een vast kernteam van professionals, waaronder de hierboven beschreven functionarissen, aangevuld met de FG. Periodiek overlegt dit vaste team en op afroepbasis aangevuld met professionals uit cruciale domeinen. Deze professionals spelen een belangrijke rol in de ondersteuning en bewustwording van de uitvoering.

Juridische Zaken

Indien er sprake is van complexe privacyvraagstukken kan juridische ondersteuning noodzakelijk zijn. Bijvoorbeeld bij de afhandeling van complexe inzageverzoeken of bij datalekken waar schade is ontstaan en waar juridische vertegenwoordiging in rechterlijke procedures nodig is.

Functionaris Gegevensbescherming

De Functionaris voor Gegevensbescherming (FG) is de onafhankelijke toezichthouder op de naleving van de AVG, gerelateerde wetgeving en het gemeentelijke beleid op het gebied van gegevensbescherming conform artikel 37-39 AVG. Het college informeert over de contactgegevens van de FG op de gemeentelijke website en communiceert zijn of haar contactgegevens aan de Autoriteit Persoonsgegevens (AP).

De Functionaris gegevensbescherming (FG):

- informeert en adviseert de organisatie over de werking van de AVG, overige wetgeving en het beleid;
- houdt toezicht op de nakoming van het privacybeleid en onderliggende wettelijke verplichtingen;
- helpt privacy-klachten en -issues tot een goed einde te brengen (ombudsfunctie);
- adviseert bij privacy-incidenten over ernst en omvang;
- helpt het privacybeleid uit te dragen en bewustzijn te creëren bij interne en externe medewerkers en doelgroepen;
- is het contactpunt voor landelijke toezichthouders – met name de AP.

De FG krijgt voldoende ruimte voor professionele uitvoering van taken. Dat betekent dat de FG:

i. naar behoren en tijdig wordt betrokken bij alle aangelegenheden die betrekking hebben op de verwerking van persoonsgegevens.

ii. volledig wordt geïnformeerd over aspecten van bedrijfsvoering waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.

Minimaal één keer per jaar brengt de FG verslag uit over de stand van zaken aan het college.

6.5 Ketensamenwerking (artikel 26 AVG)

Wanneer de verwerkingsverantwoordelijke samen met anderen doel en middelen bepaalt, bijvoorbeeld in een samenwerkingsverband, dan kan sprake zijn van gezamenlijke verantwoordelijkheid. Bij elk samenwerkingsverband dient op basis van de eigen doelen, de samenstelling van de partners en de taken op basis waarvan zij samenwerken te worden gekeken naar de wettelijke grondslag en het doel van het verstrekken en/of delen van informatie van en over personen.

In het geval van ketensamenwerking moeten de partijen onderling duidelijke afspraken maken over wie invulling geeft aan de diverse rechten en plichten uit de AVG. Het is in het bijzonder van belang dat de betrokkene weet waar hij terecht kan om zijn rechten uit te oefenen.

Indien sprake is van gezamenlijke verantwoordelijkheid, dan dienen afspraken conform artikel 26 AVG schriftelijk te worden vastgelegd en aan de betrokkene beschikbaar worden gesteld, bijvoorbeeld doormiddel van publicatie op de website van alle betrokken partijen.

Bij onduidelijkheden of complexe verhoudingen tussen de verwerkingsverantwoordelijke en de derde partij onder de AVG dient altijd contact gezocht te worden met de Privacy Officer, zodat bekeken kan worden welke afspraken eventueel gemaakt moeten worden.

Bijlage 1 Toelichting bepalingen AVG

Belangrijke begrippen:

- Betrokkene: een natuurlijk persoon op wie de persoonsgegevens betrekking hebben. Dit zal in de gemeentelijke context veelal de inwoner of een medewerker van de gemeente zijn. Maar ook een bezoeker uit een andere gemeente kan een betrokkene.
- PIT: Privacy en Informatiebeveiligingsteam.
- Data Protection Impact Assessment (DPIA): beoordeelt de effecten en risico's van een nieuwe of bestaande gegevensverwerking.
- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG. In sommige gevallen kan het zijn dat een enkel gegeven geen persoonsgegeven is, maar door deze te combineren met andere gegevens dat dan wel weer is. Bijvoorbeeld een postcode in combinatie met een huisnummer. Persoonsgegevens zijn bijvoorbeeld: naam, adres, woonplaats, geboortedatum, geslacht, emailadres, telefoonnummer, medische gegevens, biometrische gegevens, camerabeelden, BSN, stemopnames etc.
- Bijzondere persoonsgegevens: Bijzondere persoonsgegevens zijn door hun aard bijzonder gevoelig en worden door de AVG extra beschermd en zijn in principe verboden om te verwerken. Dit zijn persoonsgegevens die betrekking hebben op ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakvereniging, de gezondheid (fysiek en mentaal), iemands seksueel gedrag of seksuele gerichtheid, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon. Voor strafrechtelijke persoonsgegevens gelden onder de AVG specifieke eisen.
- Privacyverklaring: een verklaring die is bedoeld voor de betrokkenen en tot doel heeft de betrokkenen te informeren wat er met zijn gegevens gebeurt en waarom.
- Privacy by design: tijdens de ontwikkelingen van producten /diensten wordt aandacht besteed aan privacy verhogende maatregelen.
- Privacy by default: de gemeente treft technische en organisatorische maatregelen om alleen persoonsgegevens te verwerken die noodzakelijk zijn voor het specifieke doel.
- Proceseigenaar: teammanager/verantwoordelijke voor de uitvoering van de taken, processen en levering van producten binnen zijn afdeling /team.
- Verwerking: alles wat je met een persoonsgegeven kunt doen, zoals verzamelen, vastleggen, bewaren, vernietigen, verstrekken aan een ander, bij elkaar voegen, inzien, kopiëren etc.
- Verwerker: Een verwerker is een externe organisatie die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zoals de salarisadministratie of een clouddienst. Een ingehuurd schoonmaakbedrijf is dat bijvoorbeeld niet. De dienstverlening moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van de gemeente. De verwerker staat nooit onder het rechtstreekse gezag van één van de bestuursorganen, heeft nooit zeggenschap over de gegevens (hij mag bijvoorbeeld niet de bewaartermijnen bepalen) en mag alleen handelen onder de schriftelijke instructies van de gemeente Hilversum, bijvoorbeeld als dat in een verwerkersovereenkomst is bepaald.

- Verwerkersovereenkomst: Een verwerker heeft een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens. Bij het inschakelen van een verwerker worden schriftelijke afspraken gemaakt over hoe om te gaan met de persoonsgegevens en informatieveiligheid. Dit is noodzakelijk omdat de eindverantwoordelijkheid bij de gemeente blijft liggen. In de praktijk wordt gesproken van een zogenoemde verwerkersovereenkomst. Door VNG/IBD is een standaard model verwerkersovereenkomst voor gemeenten opgesteld, die vanaf 2020 (verplicht)door alle gemeenten wordt gebruikt. Deze overeenkomst is afgestemd op de, eveneens door de VNG opgestelde, Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT).
- Verwerkingsverantwoordelijke: een persoon of instantie die alleen of samen met een ander het doelen en de middelen voor de verwerking van persoonsgegevens vaststelt. Dat is in de gemeentelijke organisatie een bestuursorgaan, zoals het College van B&W, de Burgemeester, de gemeenteraad of de bezwaarschriften Commissies.

Doeleinden verwerking (artikel 5, lid 1, onder b, AVG)

De gemeente voert het beleid dat persoonsgegevens alleen verzameld worden voor een doel dat vooraf is vastgesteld is. Dat doel mag dus niet gaandeweg de gegevensverzameling worden bepaald. Dat doel moet specifiek en rechtvaardig zijn. In sommige gevallen is dat vastgelegd per wet. Zo staan er doelen en bijbehorende verwerkingen van persoonsgegevens beschreven in onder andere de Jeugdwet of de Participatiewet.

Rechtmatige grondslag (artikel 6 AVG)

Bij het verwerken van persoonsgegevens dient dit altijd noodzakelijk te zijn en gebaseerd te worden op een rechtmatige grondslag. De verwerking kan gebaseerd worden op:

• Algemeen belang / openbaar gezag;

• Wettelijke verplichting;

• Vitaal belang;

• Overeenkomst;

• Ander gerechtvaardigd belang;

• Toestemming (enkel als geen andere grondslag van toepassing is).

De verwerking van bijzondere persoonsgegevens is in principe verboden, tenzij er een beroep kan worden gedaan op één van de uitzonderingsgronden die genoemd zijn in de Uitvoeringswet AVG, naast het hebben van één van bovengenoemde grondslagen.

Grondslagen gemeentelijke organisatie

Verwerkingen binnen de gemeentelijke organisatie kunnen gebaseerd zijn op één van onderstaande grondslagen zoals hierboven genoemd:

- Persoonsgegevens die noodzakelijk zijn om een **wettelijke verplichting** na te komen. Bijvoorbeeld bij de aanvraag om een bijstandsuitkering, dan bepaalt artikel 53a en 64 Participatiewet voor welk doel welke gegevens nodig zijn.

- Persoonsgegevens die noodzakelijk zijn om een **taak van algemeen belang** uit te voeren, ook wel de uitoefening van de publiekrechtelijke taak genoemd. Bijvoorbeeld de wet Schuldhulpverlening bepaalt dat de gemeente een taak heeft in de uitvoering van de schuldhulp. Dat betekent dat telkens uit de wet moet blijken dat de gemeente een taak heeft om een bepaald doel te realiseren. Bijvoorbeeld uit de Omgevingswet om een bouwvergunning te realiseren of de Wet waardering onroerende zaken (WOZ).

Indien de gemeente als werkgever optreedt dan kunnen de volgende grondslagen gelden:

- Persoonsgegevens die noodzakelijk zijn voor de **uitvoering van een overeenkomst**, bijvoorbeeld bij de inhuur van een externe medewerker.

- Persoonsgegevens die noodzakelijk zijn ten behoeve van het **gerechtvaardigd belang** dat de gemeente Hilversum als werkgever heeft, bijvoorbeeld het inzichtelijk maken van het rooster van de BHV-ers om bedrijfshulpverlening zo effectief mogelijk in te zetten.

Let op: het gerechtvaardigd belang is alleen van toepassing daar waar privaatrechtelijke wordt gehandeld. Bijvoorbeeld in het kader van de uitoefening van de gemeente als werkgever of wanneer dat noodzakelijk is voor de bedrijfsvoering, bijvoorbeeld bij een medewerkers onderzoek of de beveiliging van de gemeentelijke gebouwen door middel van cameratoezicht. Hiervoor geldt dat telkens een zorgvuldige belangenafweging moet worden gemaakt. Het belang van de gemeentelijke organisatie moet zwaarder wegen dan de rechten en vrijheden van de medewerker. In deze belangenafweging speelt de gevoeligheid van gegevens een rol. Als er sterkere beveiligingsmaatregelen zijn getroffen, kan de verwerking eerder gebaseerd worden op deze grondslag.

Toestemming

Vanwege de afhankelijkheidsrelatie die de betrokkene met de gemeentelijke organisatie heeft, is toestemming niet geschikt. Van vrije toestemming zal over het algemeen geen sprake kunnen zijn, omdat burgers afhankelijk zijn van de gemeente voor hulp of ondersteuning.

Bij het verstrekken van een nieuwsbrief is toestemming wel een aangewezen grondslag.

Bij toestemming moet er voldoende informatie gegeven worden: toegankelijk, in duidelijke en eenvoudige taal. De betrokkene moet immers snappen waar hij precies toestemming voor geeft. Toestemming kan te allen tijde worden ingetrokken en dit dient net zo gemakkelijk te zijn als het geven van de toestemming. Opt-out is dus niet toegestaan. Dat wil zeggen dat het vinkje om toestemming te geven niet van te voren al aangekruist mag zijn. Alleen een actieve handeling om de toestemming aan te vinken is toegestaan, opt-in genoemd.

De toestemming dient te zijn vastgelegd in het daartoe vastgestelde format van de gemeente Hilversum.

Vitaal belang

Het vitale belang kan alleen worden toegepast in geval van acute dringende hulp. Bijvoorbeeld in de situatie dat een hulpverlener persoonsgegevens moet verwerken om acuut dringende medische hulp aan de betrokkene te verlenen, bijvoorbeeld omdat iemand buiten bewustzijn is. Deze grondslag zal binnen de gemeentelijke organisatie dan ook niet snel van toepassing zijn.

Verdere verwerking (doelbinding, artikel 6, lid 4, AVG)

Persoonsgegevens mogen niet zomaar voor andere doeleinden verder worden verwerkt. Zo mogen de gegevens die door de ene afdeling zijn verzameld niet zonder meer aan een andere afdeling worden verstrekt. Het verdere gebruik van gegevens mag alleen als dat bij wet is bepaald. Indien dat niet het geval is zal in ieder geval moeten worden bepaald wat:

I. het verband tussen het bestaande doel en de voorgenomen verdere verwerking is;
II. de context is waarin de gegevens zijn verzameld en de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke;
III. de aard van de gegevens zijn; voornamelijk of sprake is van bijzondere of strafrechtrechtelijke gegevens.
IV. de mogelijke gevolgen voor de betrokkene zijn;
V. het bestaan van passende waarborgen zijn, zoals anonimiseren of pseudonimiseren.

Informeren (artikel 13 en 14 AVG)

De gemeente is open en transparant over hoe zij met persoonsgegevens omgaat. Dat stelt namelijk de betrokkene in staat om zijn rechten uit te kunnen oefenen.

Wanneer de gemeente persoonsgegevens verwerkt, heeft zij de plicht de betrokkenen hierover te informeren. De betrokkenen dienen in de meeste gevallen al voordat de verwerkingen begonnen zijn, op de hoogte te zijn van de manier waarop de gemeente met persoonsgegevens omgaat. Hiertoe dienen onder andere de algemene en specifieke privacy verklaringen. Deze worden gepubliceerd op de website. Ook in het eerste gesprek of contactmoment wordt toegelicht welke gegevens waarvoor nodig zijn en wie deze op basis van welke grondslag verwerkt.

Rechten betrokkene (artikel 12 en 15-22 AVG)

Om een eerlijke verwerking van persoonsgegevens te waarborgen heeft de betrokkene diverse rechten:

- ✓ Recht op inzage
- ✓ Recht op correctie als de gegevens niet kloppen
- ✓ Recht op verwijdering van de gegevens als de gegevens niet langer nodig zijn.
- ✓ Recht om 'vergeten te worden'. In het geval waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- ✓ Recht op beperking en recht op bezwaar
- ✓ Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming (verbod van profilering).
- ✓ Recht op contact met de Functionaris Gegevensbescherming.
- ✓ Recht om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens.

Het afhandelen van de rechten van de betrokkene zal plaatsvinden volgens de daartoe aangewezen procedure.