Gemeente Súdwest-Fryslân

GEMEENTEBLAD

Officiële uitgave van de gemeente Súdwest-Fryslân

Nr. 287376

17 juni

2026

Beleid Algemene verordening gegevensbescherming (AVG) en Wet politiegegevens (Wpg) gemeente Súdwest-Fryslân

Het college van burgemeester en wethouders van de gemeente Súdwest-Fryslân;

gelet op de Algemene verordening gegevensbescherming, de Wet politiegegevens en artikel 4:81 van de Algemene wet bestuursrecht;

besluit

vast te stellen het

Beleid Algemene verordening gegevensbescherming (AVG) en Wet politiegegevens (Wpg) gemeente Súdwest-Fryslân.

Inhoudsopgave

1. Inleiding

Algemene verordening gegevensbescherming
In heel Europa is de Algemene verordening gegevensbescherming (hierna: AVG) van toepassing. De AVG zorgt samen met de Uitvoeringswet AVG (hierna: UAVG) onder andere voor:

- versterking en uitbreiding van de privacyrechten van betrokkenen, en
- meer verantwoordelijkheden voor organisaties die persoonsgegevens verwerken.

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

Wet politiegegevens
Op grond van de Wet politiegegevens (hierna: Wpg) moet de gemeente als werkgever van buitengewone opsporingsambtenaren (hierna: BOA's) voldoen aan aanvullende wettelijke eisen wanneer BOA's politiegegevens verwerken. Een van die eisen is ook het afleggen van verantwoording. De Wpg en de AVG bestaan naast elkaar, maar kennen veel overeenkomsten als het gaat om de bescherming van persoonsgegevens.
Het beleid Algemene verordening gegevensbescherming (AVG) en Wet politiegegevens (Wpg) gemeente Súdwest-Fryslân werkt de beide wettelijke kaders uit voor de gemeente Súdwest-Fryslân.
Het eerste deel van dit document gaat over de AVG en het tweede deel betreft de Wpg.

2. Kader voor de gemeente Súdwest-Fryslân

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 Súdwest-Fryslân deze realiseert.
Digitalisering en de toepassing van nieuwe technologieën (waaronder Artificiële Intelligentie (AI)) 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.
In december 2022 heeft de Algemene Ledenvergadering van de VNG (Vereniging Nederlandse gemeentes) unaniem voor de Principes voor de Digitale Samenleving gestemd. Deze principes geven weer hoe gemeenten omgaan met digitalisering en innovatieve technologie in de openbaar toegankelijke ruimte. De principes bieden de gemeente Súdwest-Fryslân in aansluiting op de AVG ambities en een gezamenlijk kader voor het omgaan met dilemma's die digitalisering met zich meebrengt. Bijvoorbeeld bij het verzamelen en gebruiken van data voor beleid. Publieke waarden, zoals democratische besluitvorming, maatschappelijke waarde en transparantie staan daarbij centraal. https://vng.nl/sites/default/files/2022-12/Principes-voor-de-Digitale-Samenleving.pdf.

3. Belangenafweging

Het is belangrijk 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 inwoners ten opzichte van elkaar:

- Belang van de inwoner: inwoners van de gemeente Súdwest-Fryslân mogen verwachten dat persoonsgegevens veilig en betrouwbaar worden verwerkt en dat transparant is wat de gemeente met de informatie doet. De wensen kunnen wel verschillend van karakter zijn. Aan de ene kant heeft de inwoner er belang bij dat zo min mogelijk gegevens worden opgeslagen en niet langer worden bewaard dan noodzakelijk. Aan de andere kant verwacht de inwoner 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 inwoners ten opzichte van elkaar: de bescherming van de rechten van de ene inwoner kan ingrijpende gevolgen hebben voor de belangen en de rechten van de andere inwoner. 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, omdat er sprake is van een complexe en/of politiek gevoelige verwerking van persoonsgegevens wordt dit voorgelegd aan het college van burgemeester en wethouders (hierna: het college). Bij deze analyse worden de maatschappelijke belangen die gediend zijn met de betreffende verwerking binnen de wettelijke kaders afgewogen tegen het belang van de bescherming van persoonsgegevens. Een voorbeeld

kan zijn wanneer het voor de uitoefening van een taak of beleidskeuze wenselijk is te weten hoeveel personen in een pand wonen. Vaak volstaat dan het aantal personen en is het niet nodig om de namen van de bewoners te vermelden. Of wanneer er een klanttevredenheidsonderzoek wordt uitgevoerd om de gemeentelijke dienstverlening te blijven verbeteren, wordt een minimale set aan gegevens gebruikt en de resultaten worden zo gepresenteerd dat deze niet meer herleidbaar zijn tot personen.
Het college is uiteindelijk eindverantwoordelijk dat de verwerking van de persoonsgegevens voldoet aan de AVG en het beleid inzake persoonsgegevens.

4. Beleid Privacy en de AVG

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

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 Súdwest-Fryslân. 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 AVG en de Uitvoeringswet AVG.

Wetten gericht op de uitvoering in specifieke sectoren zoals:
- Wet maatschappelijke ondersteuning 2015;
- Participatiewet;
- Jeugdwet;
- Wet gemeentelijke schuldhulpverlening;
- Wet Inburgering 2021;
- Omgevingswet;
- Wet open overheid (Woo);
- Wet basisregistratie personen;
- Wet gegevensverwerking door samenwerkingsverbanden (Wgs);
- Wet gegevensverwerking persoonsgerichte aanpak radicalisering en terroristische activiteiten (Wet PARTA);
- Alcoholwet;
- Archiefwet 1995;
- Wetboek van Strafrecht;
- Wet politiegegevens;
- Artificial Intelligence Act (AI-Act).

Naast de wet- en regelgeving van buiten kent de gemeente ook eigen kaders die van invloed zijn op de verwerkingen van persoonsgegevens:
- Informatieveiligheidsbeleid;
- Camerabeleid;
- Integriteitsbeleid;
- Privacybeleid sociaal domein;
- AI-beleid.

5. Uitgangspunten AVG

5.1 Uitgangspunten AVG

Iedereen die binnen de gemeente werkzaam is, gaat verantwoord om met de bescherming van persoonsgegevens. Hierbij hanteren wij de volgende algemene 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. Wanneer het doel met een vergelijkbare inspanning bereikt kan worden met een lichter middel, wordt voor dat lichtere middel 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 (dataminimalisatie)

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 toegang en bewerking te voorkomen;

- Aandacht wordt besteed bij inrichting van processen en systemen aan privacy verhogende maatregelen (privacy by design en privacy by default) (https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht#privacy-by-design-en-default);
- Persoonsgegevens beveiligd zijn en hierbij de Baseline Informatiebeveiliging Overheid 2 (BIO2) 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 (in ieder geval voor de applicaties met de gevoeligste gegevens) wordt vastgelegd (logging);
- Er wordt gewerkt met geheimhoudingsverklaringen en contractuele afspraken bij het inschakelen van externen en leveranciers.

5.2 Rechtmatigheid, behoorlijkheid en transparantie

Rechtmatigheid, behoorlijkheid en transparantie is een belangrijk uitgangspunt van de AVG voor de gemeente. Dit uitgangspunt wordt hieronder toegelicht.

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).
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 draagt zorg 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' en 'privacy by default' 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 wordt de procedure datalekken gevolgd en indien noodzakelijk wordt het datalek gemeld bij de Autoriteit Persoonsgegevens (hierna: AP). 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 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 weten welke persoonsgegevens de gemeente over diegene heeft verzameld en waarvoor die worden gebruikt. Als burgers willen weten welke gegevens over diegene 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.
- Als er met (WiFi-)tracking of metingen signalen naar personen herleidbaar zijn zal de gemeente betrokkenen daarover proactief informeren dat er op dat moment gegevens worden verzameld en welke gegevens dit betreft.
- De inzet van cameratoezicht is geregeld in het Algemeen beleid cameratoezicht gemeente Súdwest-Fryslân. Dit beleid is te vinden op de gemeentelijke website en op: https://lokaleregelgeving.overheid.nl/CVDR676400/1

6. Basis

6.1 Register van verwerkingen (artikel 30 AVG)
De gemeente 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 AP daarom vraagt, wordt het verwerkingsregister ter beschikking gesteld. Daarnaast is de gemeente voornemens om een openbaar verwerkingsregister op de website te plaatsen.

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 door de functionaris gegevensbescherming (hierna: FG) gerapporteerd aan de directie, het college en de gemeenteraad.

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

Onder de AVG 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, bijvoorbeeld bij Smart City toepassingen, geldt er ook een DPIA-plicht.
De AP heeft de volgende lijst opgesteld waarbij de verplichting geldt tot het uitvoeren van een DPIA, 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).

Binnen de gemeente is een DPIA-team werkzaam. Het advies en de conclusie van het DPIA-team wordt voorgelegd aan de FG en Chief Information Security Officer (hierna: CISO). De FG en CISO vullen de DPIA aan vanuit hun expertise. De advisering vanuit de DPIA op mogelijke risico's en maatregelen dienen door de verantwoordelijke in de organisatie te worden geaccepteerd of te worden opgevolgd. Het afnemen van een DPIA vindt plaats volgens de vastgestelde procedure DPIA.

6.4 Verantwoordelijkheden uitvoering AVG

Het beleid wordt vastgesteld door het college en gecontroleerd door de gemeenteraad. Hieronder wordt omschreven wie wat doet.

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 zij het college op de uitvoering van deze kaders. Zij wordt hiertoe in staat gesteld door de verantwoordingsinformatie. Dit is onder meer het jaarlijkse verslag van de FG die het college aan de gemeenteraad beschikbaar stelt.

College

Het college is integraal verantwoordelijk voor de zorgvuldigheid van verwerking van persoonsgegevens. Zij is het 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 een portefeuillehouder aangewezen die namens het college de uitvoering van het beleid waarborgt. Daarnaast legt deze (politieke) verantwoording af over de privacy beleidsvoering aan de gemeenteraad.

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. De gemeentesecretaris vormt dus de schakel tussen het bestuur en ambtelijke organisatie en is in dit kader ambtelijk verantwoordelijk.

De gemeentesecretaris is samen met de directie verantwoordelijk voor een juiste uitvoering van het privacybeleid en stuurt op (concern) risico's. Daarnaast zorgt de gemeentesecretaris samen met de directie voor een passend niveau van informatieveiligheid en gegevensbescherming binnen de organisatie.

Uitvoering: teammanagers
De zorgvuldige omgang van verwerkingen valt onder de teammanagers (proceseigenaren) 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 en/of de FG. Daarnaast worden centraal bewustzijnscampagnes en op maat gemaakte trainingen 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 de 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 FG, CISO of Servicedesk worden gemeld;
- Het melden en uitwerken van nieuwe verwerkingen en gewijzigde verwerkingen in het verwerkingsregister;
- 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 teammanager of FG in. Alle medewerkers wordt een meerjarige e-learning aangeboden over de onderwerpen privacy en informatiebeveiliging. Daarnaast is er een verplichte fysieke training voor nieuwe medewerkers over deze onderwerpen.

6.5 Ondersteuning en advies uitvoering AVG
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 onder andere verantwoordelijk voor het bijhouden van het verwerkingsregister en handelt de verzoeken van burgers tot inzage, wijziging of verwijdering op grond van de AVG af. Daarnaast coördineert de PO de uitvoering van DPIA's. Gevraagd en ongevraagd adviseert de PO aan collega's, management en bestuur 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 de CISO een controlerende en toezichthoudende rol. Informatiebeveiliging maakt een wezenlijk onderdeel uit van de bescherming van persoonsgegevens. De CISO adviseert voornamelijk bij projecten, DPIA's en het beheersen van risico's.

DPIA-team
Voor het uitvoeren van DPIA's is een zelfstandig DPIA-team ingesteld. In dit team zit op dit moment een juridisch adviseur, een financieel adviseur, de beleidsadviseur concerncontrol en de Privacy Officer. Dit DPIA-team bepaalt in overleg met de verantwoordelijke (de teammanager) en FG welke DPIA's worden uitgevoerd. De teammanager is verantwoordelijk voor het opvolgen van de adviezen en bevindingen uit de DPIA's.

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.

FG
De 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 AP.
De FG:

- informeert en adviseert de organisatie over de werking van de AVG, overige wetgeving en het beleid;
- houdt toezicht op de naleving 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;
- onderzoekt en beoordeelt datalekken en meldt deze indien nodig aan de AP;
- 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.

Ondernemingsraad
De ondernemingsraad (OR) komt op voor de belangen van het personeel. De OR kan door advisering of instemming invloed hebben op de bedrijfsvoering. De OR speelt een belangrijke rol bij privacy op het werk. Zo moet de OR om instemming worden gevraagd voor het gebruik van personeelsgegevens of het monitoren van werknemers (personeelsvolgsysteem). Ook kan de OR zich op eigen initiatief uitspreken over het gebruik van personeelsgegevens en adviseren over technologische voorzieningen. De OR heeft volgens artikel 27, lid 1, onder k van de Wet op de ondernemingsraden dan ook instemmingsrecht op elke regeling die te maken heeft met het verwerken en beschermen van persoonsgegevens van werknemers. Wanneer er sprake is van een dergelijke verwerking en de Privacy Officer en/of de FG hiervan in kennis zijn gesteld, verwijzen zij de betreffende medewerker of verantwoordelijke teammanager door naar de OR.

6.6 Ketensamenwerking (artikel 26 AVG)
Wanneer de verwerkingsverantwoordelijke samen met anderen het doel en de middelen bepaalt, bijvoorbeeld in een samenwerkingsverband, dan kan sprake zijn van gezamenlijke verwerkingsverantwoordelijkheid. 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 verwerkingsverantwoordelijkheid, 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.

6.7 AI-beleid
Artificiële intelligentie (AI), ook wel kunstmatige intelligentie genoemd is sterk in ontwikkeling. Daardoor worden geavanceerde algoritmische beslismodellen steeds krachtiger en ingewikkelder. Zowel bedrijven als de overheid gebruiken inmiddels op grote schaal algoritmes. Een algoritme is een formule om een bepaald doel te bereiken. Vaak om bepaalde beslissingen (deels) te automatiseren. Geavanceerde zelflerende algoritmes vallen onder AI. Het gebruik van geavanceerde algoritmes kan voordelen bieden, maar er zijn ook risico's. Algoritmes worden vaak gebruikt om geautomatiseerd besluiten te nemen.

Een van de risico's hiervan is de kans op een oneerlijk, onjuist of bevooroordeeld besluit. Of zelfs op discriminatie.
Algoritmes en AI verwerken vaak persoonsgegevens. Dit betekent dat het gebruik van algoritmes moet voldoen aan de AVG, net als alle andere verwerkingen van persoonsgegevens.
Op 1 augustus 2024 is de Artificial Intelligence Act (hierna: AI-Act) in werking getreden. Deze Europese verordening treedt gefaseerd in werking en zal medio 2027 geheel van kracht zijn. De AI Act is er om ervoor te zorgen dat iedereen in Europa erop kan vertrouwen dat AI-systemen veilig werken en dat grondrechten beschermd worden. Ook al zijn er veel systemen met weinig risico's en zijn er allerlei voordelen aan AI, er is ook een hele andere kant. Bestaande wetten zoals de AVG en Wpg bieden al bescherming. Bijvoorbeeld als AI-systemen worden gebruikt om persoonsgegevens te verwerken. Maar dat is onvoldoende om alle risico's aan te pakken die bij AI komen kijken. Onverantwoord gebruik van AI kan bijvoorbeeld leiden tot discriminatie, beperkingen van onze vrijheden, hoog energieverbruik en misleiding en uitbuiting van mensen. De AI Act helpt ervoor te zorgen dat ontwikkelaars van AI-systemen risico's aanpakken en dat daar toezicht op is.
De AI-verordening treedt stapsgewijs in werking:
De gemeente heeft begin 2026 AI-beleid vastgesteld (https://lokaleregelgeving.overheid.nl/CVDR760013/1). In dat beleid staan de noodzakelijke randvoorwaarden en is uitgewerkt hoe deze technologie slim, veilig, verantwoord, gemotiveerd en ethisch kan worden geïmplementeerd. Dit stelt de gemeente in staat om de voordelen van AI te benutten, zoals efficiëntie en innovatie, zonder concessies te doen aan de integriteit en het vertrouwen van de burger.
De AI-verordening treedt stapsgewijs in werking:

6.8 Nieuwe relevante wetgeving

Wet gegevensverwerking door samenwerkingsverbanden (WGS)
De Wet gegevensverwerking door samenwerkingsverbanden (WGS) is per 1 januari 2025 van kracht geworden en heeft onder meer gevolgen voor de Zorg- en Veiligheidshuizen (ZVH-en). In het ZVH werkt de gemeente samen met andere partijen in het zorg- en veiligheidsdomein. Alle Friese gemeenten zijn bij het Zorg- en Veiligheidshuis Fryslân aangesloten. Met de WGS ontstaat een wettelijke grondslag voor het delen en verwerken van persoonsgegevens door de samenwerkende partijen. De wet regelt de gegevensverwerking van de persoonsgerichte aanpak bij complexe casuïstiek (PGA) en de 'Top X-lijsten' met geprioriteerde casussen.
Justitiële ketenpartners die als vaste deelnemer bijdragen aan de samenwerking in het Zorg- en Veiligheidshuis zijn:

- Openbaar Ministerie;
- Reclassering;
- Politie;
- Raad voor de Kinderbescherming;
- Dienst Justitiële Inrichtingen.

Daarnaast zijn vaste deelnemers in de netwerksamenwerking van het Zorg- en Veiligheidshuis:

- De sociale wijk- en gebiedsteams;
- Jeugdbescherming (Gecertificeerde Instellingen);
- Veilig Thuis;
- GGD;
- Instellingen voor de GGZ;
- Verslavingszorg.

Ook het bijbehorende Besluit gegevensverwerking door samenwerkingsverbanden (BGS) trad op 1 januari 2025 in werking. Het Algemeen Convenant en de Regelingen Gegevensverwerking van Zorg- en

Veiligheidshuis Fryslân zijn nog niet aangepast aan de nieuwe wetgeving. Toch werkt Zorg- en Veiligheidshuis Fryslân al wel volgens de WGS en het BGS.
Elk Zorg- en Veiligheidshuis heeft een coördinerend FG. Deze draagt zorg voor het uitvoeren van privacy audits en de taken uit artikel 39 AVG. Voor Friesland is de coördinerend FG de FG van de gemeente Leeuwarden. Daarnaast dient een samenwerkingsverband iedere twee jaar een audit te laten uitvoeren naar in hoeverre er wordt voldaan aan de geldende wet- en regelgeving waaronder de AVG.

Wet gegevensverwerking persoonsgerichte aanpak radicalisering en terroristische activiteiten (de Wet PARTA)
Met ingang van 1 juli 2025 is de Wet gegevensverwerking persoonsgerichte aanpak radicalisering en terroristische activiteiten (de Wet PARTA) in werking getreden. De Wet PARTA biedt duidelijkheid over taken, verantwoordelijkheden en grondslagen voor gegevensverwerking tussen organisaties en waarborgen voor gegevensbescherming die aansluiten bij de AVG.
De wet PARTA legt de burgemeester de wettelijke taak op om casus overleggen te organiseren waarin de aanpak van radicaliserende of geradicaliseerde personen wordt besproken. Hiermee wordt de gegevensuitwisseling tussen organisaties die betrokken worden bij een casus van een rechtsgrondslag voorzien. Op basis van de wet PARTA worden het weegoverleg en het casusoverleg door de partijen gezamenlijk gedaan en geldt dat zij daarom gezamenlijk verwerkingsverantwoordelijk zijn voor de verwerking van persoonsgegevens in het casusoverleg. Voor het weegoverleg zijn de burgemeester, de politie en het OM gezamenlijk verantwoordelijk. Voor het casusoverleg zijn de deelnemers (behalve de incidentele deelnemers) de gezamenlijke verwerkingsverantwoordelijken. Dit staat los van de verwerking die de partijen zelf doen. Onder de wet PARTA mogen bijzondere en strafrechtelijke gegevens worden gedeeld, onder de WGS niet. De FG van de individuele organisaties moet toezicht houden op de toepassing van deze wet binnen de eigen organisatie.
De eerste audit moet uiterlijk twee jaar na de inwerkingtreding van de wet PARTA (1 juli 2027) plaatvinden. Daarna eenmaal in de vier jaar.

7. Beleid Wet politiegegevens

7.1 Introductie
De AVG geldt niet voor gegevens die worden verwerkt voor de opsporing of vervolging van strafbare feiten. Voor dat soort gegevens geldt de Europese Richtlijn gegevensverwerking opsporing en vervolging. Iedere lidstaat moest deze Richtlijn vertalen in eigen, nationale wetgeving. In Nederland is daarom de Wet politiegegevens (Wpg) herschreven. Zo kunnen politie en marechaussee aan deze Richtlijn voldoen. Een andere verandering is dat de Wpg nu ook voor de buitengewoon opsporingsambtenaar (BOA) geldt, zowel voor de BOA werkzaam in de publieke als private sector. Er gelden twee regimes voor de BOA: de AVG en Wpg. BOA's hebben vaak meerdere taken en verwerken verschillende soorten gegevens. Gegevens die een BOA verwerkt in zijn rol als toezichthouder of incidentbestrijder, vallen onder de AVG. De gegevens die de BOA als opsporingsambtenaar verwerkt, vallen onder de Wpg. Hij heeft dus een 'twee-petten-uitdaging'. Voor gegevens die hij onder de Wpg verwerkt (opsporing), gelden andere verwerkingstermijnen en andere regels voor het onderling delen van gegevens. Ook moet er soms een bevoegd functionaris worden aangewezen die als hoeder van de gegevens fungeert, en er geldt een plicht tot logging. De gegevenshuishouding, systemen en werkprocessen moeten dus anders worden ingericht dan bij de verwerkingen die in het kader van toezicht worden gedaan.

7.2 Algemene uitgangspunten
In het kader van de Wpg gelden de volgende uitgangspunten:
1. De organisatie hanteert als raamwerk voor beheersmaatregelen (Control Framework) het door Wpg-auditoren gehanteerde raamwerk, zoals dat is opgenomen in bijlage 3 en 4 van de NOREA handreiking privacy audit Wpg voor BOA's.
2. Wanneer gebruik gemaakt wordt van een informatiesysteem dat wordt beheerd door een leverancier (bijvoorbeeld SaaS), dan wordt met de leverancier een verwerkersovereenkomst afgesloten en dient deze een Third Party Memorandum (TPM) conform de NOREA handreiking privacy audit Wpg voor BOA's.
3. Bij gebruik van een informatiesysteem worden passende technische en organisatorische maatregelen ingeregeld om 'privacy by design' (gegevensbescherming door beveiliging en ontwerp) en 'privacy by default' (gegevensbescherming door standaard-instellingen) te bewerkstelligen.
4. De organisatie voert voor elke verwerking van politiegegevens een DPIA uit en deze wordt elke 3 jaar herzien. Daarin worden de volgende principes getoetst en geborgd:

a. gegevensbescherming door privacy by design, en
b. gegevensbescherming door privacy by default.

Voor zover het een informatiesysteem betreft worden deze principes tevens afgedekt in de TPM.

5. De organisatie verwerkt politiegegevens op basis van artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en op basis van de artikelen over ter beschikking stellen en verstrekking van politiegegevens (artikel 15-21 en 23-24).
6. De organisatie verwerkte geen gegevens op basis van:
   a. artikel 9 Wpg (onderzoek in een bepaald geval). Wel verlenen BOA's medewerking aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten;
   b. artikel 11 Wpg (geautomatiseerd vergelijken en in combinatie zoeken voor een artikel 9 onderzoek;
   c. n het kader van artikel 13 Wpg (ondersteunende taken), voor zover die gegevens onder verantwoordelijkheid van instanties worden verwerkt;
   d. artikel 17a Wpg (Doorgifte aan derde landen, d.w.z. landen buiten de Europese Economische Ruimte), en;
   e. maakt geen gebruik van geautomatiseerde besluitvorming, waaronder profilering als bedoeld in artikel 7a Wpg.

7. Toegangsbeveiliging is zodanig ingericht dat alleen BOA's en geautoriseerden toegang hebben tot politiegegevens.
8. Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd.

7.3 Rollen, taken en bevoegdheden

Binnen de Wpg zijn er de volgende rollen, taken en bevoegdheden:

1. De Privacy Officer inventariseert jaarlijks of het bereik van de verwerkingen met politiegegevens is gewijzigd. Op basis daarvan worden het verwerkingenregister voor de Wpg indien nodig aangepast.
2. De Teammanager van het team met daarin BOA's is verantwoordelijk voor de implementatie en uitvoering van de Wpg en heeft in dat kader onder andere de volgende taken:
   a. het onder de aandacht brengen van de handreiking/gedragsregels voor BOA's bij de medewerkers en het toezien op deze gedragsregels;
   b. het bijhouden van een overzicht met geautoriseerden;
   c. het melden en uitwerken van nieuwe verwerkingen en gewijzigde verwerkingen in het verwerkingsregister Wpg;
   d. bijhouden van een lijst met veel voorkomende verstrekkingen met daarbij de onderbouwing van de grondslag voor de verstrekking;
   e. zorgen dat Artikel 8 Wpg gegevens:
      i. na 1 jaar alleen nog beschikbaar zijn voor gericht zoeken;
      ii. na 5 jaar worden verwijderd, dat wil zeggen alleen beschikbaar zijn voor audits en klachtenprocedures;
      iii. na 10 jaar worden vernietigd.

3. De Teammanager van het team met daarin BOA's heeft de volgende bevoegdheden:
   a. het nemen van autorisatiebesluiten in de zin van artikel 6 lid 3, 4, 5 Wpg met behulp van het formulier "Autorisatie verwerking politiegegevens";
   b. het besluiten over toegang tot informatiesystemen met politiegegevens, waaronder het vaststellen van de autorisatiematrix voor het informatiesysteem waarin politiegegevens worden verwerkt;
   c. het vaststellen van werkinstructies, procesbeschrijvingen en gerelateerde documenten.
   d. De applicatiebeheerder bewaakt beveiliging van de applicatie, onder andere door log-bestanden te analyseren.

4. De FG:
   a. adviseert en informeert over de Wpg, onder andere over DPIA's;
   b. houdt toezicht op de uitvoering van de Wpg;
   c. werkt samen met de AP en is contactpunt voor de AP;
   d. stelt jaarlijks een verslag op met bevindingen.

5. De FG of de PO voert de volgende controles uit:

a. steekproefsgewijze beoordeling van Processen Verbaal, ten minste jaarlijks, op de volgende criteria:
   i. werken conform de gedragsregels;
   ii. adequaat hanteren van doelbinding;
   iii. noodzakelijkheid, rechtmatigheid, juiste en volledige verwerking van politiegegevens;
   iv. vastlegging van de herkomst en wijze van verkrijging;
   v. alleen verwerken van bijzondere politiegegevens wanneer dit onvermijdelijk is;
   vi. onderscheid tussen feitelijke en subjectieve gegevens, c.q. feiten en persoonlijke oordelen;
   vii. onderscheid tussen verschillende categorieën van betrokkenen, zoals verdachten, slachtoffers, getuigen en veroordeelden;
   viii. vastlegging en rechtmatigheid van ter beschikkingstellingen en verstrekkingen.

b. toetsen van tijdige uitvoering en/of actualisering van DPIA;
c. toetsen van het testen en evalueren van de doeltreffendheid van de beheersmaatregelen, waaronder beveiligingsmaatregelen bijvoorbeeld n.a.v. de DPIA;
d. controle van Toewijzing van autorisaties en de controle daarvan door de systeemeigenaar;
e. controle van de verwerkersovereenkomst(en) op actualiteit en actuele bijbehorende certificaten en verklaringen;
f. controle van bewustmaking en opleiding van BOA's en andere geautoriseerden;
g. controle van de rechtmatigheid van verstrekkingen;
h. controle van correcte en tijdige uitvoering en documentatie, o.a. van de reden van afwijzing van verzoeken van betrokkenen, zoals vernietiging en rectificatie van politiegegevens;
i. toetsen van een adequate analyse van de logging;
j. controle van correcte en tijdige opvolging van datalekken, zoals documentatie, analyse en meldingen aan AP en betrokkenen;
k. controle van volledigheid en juistheid van het verwerkingenregister voor zover het Wpg verwerkingen betreft.

7. Interne en externe Wpg audits worden gecoördineerd door het team Concerncontrol.
8. Betrokkenen worden geïnformeerd over de verwerking van politiegegevens via de website en – indien van toepassing- bij de eerste brief die zij ontvangen over strafrechtelijke handhaving.

7.4 Specifiek beleid ten aanzien van de clusters

Cluster veiligheid (Domein I: Openbare ruimte)
De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving in de openbare ruimte. Daarom zijn binnen dit taakveld BOA's aangesteld en is de Wpg van toepassing.
Cluster Milieu (Domein II: Milieu, welzijn en infrastructuur)
De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving. Daarom zijn binnen dit taakveld BOA's aangesteld en is de Wpg van toepassing.
Uitvoering van de leerplichtwet (Domein III: Onderwijs)
De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving van de leerplichtwet, in het bijzonder artikel 16 lid 5 en artikel 26. Daarom zijn binnen dit taakveld BOA's aangesteld en is de Wpg van toepassing.

8. Slotbepalingen

1. Deze beleidsregels treden de dag na publicatie in het Gemeenteblad in werking.
2. Deze beleidsregels worden aangehaald als: Beleid Algemene verordening gegevensbescherming (AVG) en Wet politiegegevens (Wpg) gemeente Súdwest-Fryslân.

Aldus vastgesteld in de vergadering van het college van burgemeesters en wethouders van 2 juni 2026,
Mr. drs. J.A. de Vries, burgemeester
Drs. C. Smits, gemeentesecretaris

Bijlage 1 Toelichting bepalingen AVG en Wpg

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.
- 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 en Wpg. 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 en Wpg 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 Súdwest-Fryslân, 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 en artikel 2 en 3 Wpg)
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[1]).

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 AVG

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 Súdwest-Fryslân 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.

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 en artikel 3 lid 3 Wpg)

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;

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.

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 en artikel 24a Wpg)

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 en artikel 7a en 25-28 Wpg)

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 vindt plaats volgens de daartoe aangewezen procedure.