GEMEENTE Best

GEMEENTEBLAD

Officiële uitgave van de gemeente Best

Nr. 444368

15 oktober 2025

Privacybeleid gemeente Best 2025-2028

1. Inleiding

De gemeente Best werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Best is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

Geldigheidsduur
Dit beleid is vastgesteld op <datum> door het college van B&W als eindverantwoordelijke voor de gemeentelijke gegevensverwerking. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's) kan het college besluiten tot een tussentijdse herziening.

2. Wettelijk kader

Onder privacywetgeving verstaan we in het algemeen:

- Algemene Verordening Gegevensbescherming
- Uitvoeringswet Algemene Verordening Gegevensbescherming
- Grondwet
- Handvest van de grondrechten van de Europese Unie
- Europees Verdrag voor de Rechten van de Mens

Daarnaast is ook in specifieke regelgeving aandacht voor gegevensbescherming zoals[1]:

- Algemene wet inzake rijksbelastingen;
- Algemene wet Bestuursrecht;
- Archiefwet;
- Auteurswet;
- Burgerlijk Wetboek;
- Drank- en Horecawet;
- Gemeentewet;
- Handelregisterwet;
- Jeugdwet;
- Kadasterwet;
- Kieswet;
- Leerplichtwet;
- Omgevingswet;
- Participatiewet;
- Telecommunicatiewet;
- Wet algemene bepalingen Burgerservicenummer;
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg;
- Wet basisregistratie personen;
- Wet bijzondere maatregelen grootstedelijke problematiek;
- Wet maatschappelijke ondersteuning;
- Wet op de geneeskundige behandelingsovereenkomst;

1) Deze lijst is niet uitputtend en kan aangevuld worden.

- Wet Politiegegevens;
- Wet publieke gezondheid;
- Wet structuur uitvoeringsorganisatie werk en inkomen;
- Wet Verplichte GGZ;
- Wet WOZ.

3. Begripsbepalingen

De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis. Daarnaast worden de volgende begrippen in de AVG gebruikt en komen vaak terug in dit privacybeleid:

Algemene Verordening Gegevensbescherming (AVG): Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens).

Betrokkene(n): De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de persoonsgegevens worden verwerkt. Dit kan gaan om een inwoner, ondernemer, medewerker of contactpersoon van een (keten)partner.

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

Data Protection Impact Assessment (DPIA): In het Nederlands vertaald naar gegevensbeschermingseffectbeoordeling, maar de gangbare term is DPIA. Dit is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is een beoordeling over het effect van de (nieuwe of aangepaste) verwerking op de bescherming van de persoonsgegevens. Het uitvoeren van een DPIA is verplicht als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen. De beoordeling bevat tenminste een inschatting van de risico's van de verwerking en de vereiste beheersmaatregelen om tekortkomingen op te lossen.

Functionaris Gegevensbescherming (FG): Een onafhankelijke en deskundige interne toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG).

4. Visie

De komende jaren zet de gemeente in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. Een goede privacy boekhouding is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de gemeente.

5. Doel

Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is, of wordt - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook voor domein specifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

Naast dit door het college vastgestelde privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer
Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

6. Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:
1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Dit privacybeleid is bindend voor de gehele organisatie van de gemeente Best.

7. Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De gemeente onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag
Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

Welbepaalde doeleinden
De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

Verdere verwerking
De gemeente kan persoonsgegevens in bepaalde gevallen verwerken voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een verenigbaarheidstoets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking
Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden bereikt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

Juiste en actuele gegevens
De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Gegevens worden op tijd vernietigd
De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid
De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Default en Privacy by Design
De gemeente houdt bij gebruik van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt *Privacy by Design* (PbD) genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het programma van eisen. Daarbij neemt de gemeente *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk. Dit principe dient ook meegenomen te worden in het aanbestedingsproces

Toegang tot gegevens
Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens
Bij ongewenste en ongewilde toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de Autoriteit Persoonsgegevens (AP), de Nederlandse toezichthouder op de bescherming van persoonsgegevens en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Het vaststellen, melden en afhandelen van datalekken is opgenomen in de procesbeschrijving Datalekken 2019.

Samenwerking
De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. We noemen deze derden verwerkers. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Samenwerkingsverbanden
Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of zelfstandig). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat tenminste gelijk is aan dat van de gemeente.

Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, vindt alleen plaats in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid. Het uitgangspunt binnen onze gemeente is dat persoonsgegevens zoveel mogelijk binnen de EER worden verwerkt. Als het noodzakelijk is om persoonsgegevens toch aan landen buiten de EER door te geven, dient dit te allen tijde te voldoen aan geldende wet- en regelgeving (Hoofdstuk V AVG).

Transparantie
De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze

waarop hij deze kan uitoefenen. Alleen wanneer als de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

Rechten van betrokkenen
Iedereen heeft het recht om te weten welke persoonsgegevens de gemeente over hem/haar verzamelt en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid.

Geschillenbeslechting
Als de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen door middel van de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. De betrokkene heeft ook het recht een klacht in te dienen bij de AP, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording
Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De AP houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingsregister
De gemeente beschikt over een verwerkingsregister. Daarin zijn alle verwerkingen van persoonsgegevens gedocumenteerd en inzichtelijk gemaakt. Iedere verwerking heeft een eigenaar die ervoor zorgt dat het verwerkingenregister actueel blijft.

Data Protection Impact Assessment (DPIA)
Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van de verwerking op de bescherming van persoonsgegevens. De gemeente voert in dat geval een Data Processing Impact Assessment (DPIA) uit (in het Nederlands Gegevensbeschermingseffectbeoordeling (GEB) genoemd). Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging[2] genoemd.

Functionaris gegevensbescherming (FG)
De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke interne toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG mag niet ontslagen of gestraft worden of voor of nadeel ondervinden bij het uitvoeren van zijn taken. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

PDCA Cyclus
De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen. *In control* betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

2) https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging

8. Rollen en Verantwoordelijkheden

Het governancemodel van de gemeente biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het College van B&W, het Strategisch Team, Teamleiders, medewerkers, de Functionaris voor de Gegevensbescherming (FG), de Privacy adviseur en de CISO.

Rollen en verantwoordelijkheden

College van B&W
Het College heeft de volgende rollen en verantwoordelijkheden:
- Bestuurlijk eindverantwoordelijk voor de aantoonbare naleving van de privacywetgeving binnen de gemeente (verantwoordingsplicht);
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert een duurzame privacycultuur.

Leidinggevende
De leidinggevenden hebben de volgende rollen en verantwoordelijkheden:
- Ambtelijk eindverantwoordelijk voor de naleving van de privacywetgeving binnen het eigen domein of team;
- Verantwoordelijk voor de implementatie en uitvoering van het privacybeleid binnen het eigen domein of team;
- Informeer de FG op welke manier het eigen domein of team compliant is aan de privacywetgeving;
- Verantwoordelijk voor het (laten) volgen van trainingen op het gebied van Informatiebeveiliging en Privacy door werknemers binnen het eigen domein of team;
- Verantwoordelijk voor het registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op het eigen domein of team;
- Verantwoordelijk voor het uitvoeren van DPIA's. De leidinggevende vraagt bij alle DPIA's een schriftelijk advies van de FG;
- Verantwoordelijk voor het treffen van maatregelen om privacyrisico's te mitigeren en het accepteren van eventuele restrisico's;
- Verantwoordelijk voor het aangaan van verwerkersovereenkomsten of andere overeenkomsten met betrekking tot het beschermen van persoonsgegevens;

- Verantwoordelijk voor de autorisatie en het intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Bevorderen een duurzame privacycultuur;
- Betrekken de privacy adviseur en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)
Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG heeft een onafhankelijke adviserende (gevraagd en ongevraagd) en toezichthoudende positie in de organisatie. De organisatie waarborgt die onafhankelijke positie. De FG kan in de uitoefening van zijn functie geen aanwijzingen of instructies ontvangen. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:
- Interne toezichthouder op de naleving van de AVG;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacy klachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken over verwerkersovereenkomsten en de risico's bij de doorgifte van persoonsgegevens naar landen buiten de EER;
- Adviseert verwerkingsverantwoordelijken over andere overeenkomsten met betrekking tot het beschermen van persoonsgegevens;
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, onder andere bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingenregister;
- Rapporteert aan het College van B&W, gemeentesecretaris en gemeenteraad over de naleving van de privacywetgeving en de gegevensbescherming in de organisatie.

De FG heeft de volgende bevoegdheden:
- Kan een onderzoek instellen naar de manier waarop, in een bepaald geval dan wel in het algemeen belang, de persoonlijke levenssfeer wordt beschermd;
- Kan, als hij dat nodig acht, voor zijn onderzoek gebruikmaken van de diensten van derden. Daarvoor vraagt hij voorafgaand aan de inzet toestemming aan de verwerkingsverantwoordelijke;
- Heeft toegang tot alle ruimten waar persoonsgegevens worden verwerkt;
- Is bevoegd apparatuur, programmatuur en gegevensbestanden te onderzoeken en indien noodzakelijk mee te nemen;
- Is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van de verwerkingsverantwoordelijke werkt of ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- Is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt;
- Is bevoegd van gegevens en bescheiden kopieën te maken. Als het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor maximaal één werkdag mee te nemen;
- Is bevoegd opdracht te geven tot de vernietiging van persoonsgegevens waarvan de bewaartermijn is overschreden of waarvan de verwerking onrechtmatig is;
- Is bevoegd zich te laten vergezellen en bijstaan door personen die daartoe door hem zijn aangewezen.

De FG maakt van bovengenoemde bevoegdheden alleen gebruik voor zover dit voor de uitoefening van de taak noodzakelijk is. De FG is verplicht tot geheimhouding van alles wat hem bekend is geworden, tenzij de betrokkene in bekendmaking toestemt.

Privacy adviseur
De Privacy adviseur is het eerste aanspreekpunt voor de gemeente rondom privacy gerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy adviseur heeft de volgende rollen en verantwoordelijkheden:
- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Stelt privacybeleid en modellen, formats en standaard-overeenkomsten op, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor de uitwisseling van persoonsgegevens;

- Monitort en ondersteunt verwerkingsverantwoordelijken bij de toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van DPIA's en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseert over de verwerkingsgrondslag;
- Ontwikkelt de bewustmakingsprogramma's- en privacy trainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij de ontwikkeling van nieuwe systemen in samenwerking met de IBF en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert de verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

Team Informatiebeveiliging en privacy
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;

Het team informatiebeveiliging en privacy bestaat uit de privacy adviseur, de CISO en de FG. Het team komt elke week tenminste één keer samen om actualiteiten op het gebied van privacy en informatiebeveiliging te delen en zo nodig acties uit te voeren. De uitvoerende en toezichthoudende rollen worden hierbij in acht genomen. Tenminste één keer per zes maanden worden actualiteiten en belangrijke bevindingen van de afgelopen zes maanden gedeeld met het college, de afdelingsmanagers en teamleiders middels een rapportage.

Andere rollen en verantwoordelijkheden

Afdeling	**Betrokkenheid**
Juridische Zaken	Ondersteunen de Privacy Adviseur ten aanzien van privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten.
IBF	Toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. Adviseert de organisatie bij datalekken (volgens de meldprocedure). Meldt Informatiebeveiligingsincidenten zo snel mogelijk bij de Privacy Adviseur en FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt, worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure)
Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Ondernemingsraad	Wordt door de organisatie actief geïnformeerd over privacy en gegevensbescherming voor wat betreft personeel. Wordt om instemming gevraagd als het gaat om een regeling die impact heeft op de bescherming van persoonsgegevens van medewerkers.
Gemeenteraad	Toezichthoudende en controlerende taak

9. Herzien van het beleid

Het beleid wordt periodiek, maar tenminste eenmaal per 36 maanden herzien.