Gemeente Sliedrecht

GEMEENTEBLAD

Officiële uitgave van de gemeente Sliedrecht

Nr. 63769

12 februari 2026

Privacybeleid Sliedrecht

1. Inleiding

De gemeente 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 inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat. De burgemeester, het college en de raad zijn ieder verantwoordelijk voor het verwerken van persoonsgegevens. In het vervolg van dit beleid worden de burgemeester, het college en de raad gezamenlijk aangemerkt als de gemeente.
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Sliedrecht 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) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

Wet politiegegevens (Wpg)
De gemeente kan ook te maken krijgen met verwerkingen van persoonsgegevens op grond van de Wpg. Dan spreekt men van politiegegevens. Voor de gemeente Sliedrecht geldt dit alleen voor verwerkingen die buitengewone opsporingsambtenaren (BOA's) verrichten bij hun onderzoek naar en opsporing van strafbare feiten. Voor de inzet van BOA's heeft de gemeente Sliedrecht ervoor gekozen om een samenwerking met de gemeente Dordrecht aan te gaan.

Geldigheidsduur
Op de eerste pagina van dit beleid is aangegeven op welke datum het privacybeleid is vastgesteld door het college van B&W , de burgemeester en de gemeenteraad als eindverantwoordelijke voor de gemeentelijke gegevensverwerking, elk voor zover het zijn of haar bevoegdheden betreft. 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 bepaalde risico analyses) kan het college besluiten tot een tussentijdse herziening).

2. Begripsbepalingen

De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis.

3. Visie

De gemeente Sliedrecht is zich bewust van haar verantwoordelijkheid met betrekking tot het verwerken van (persoons) gegevens van haar inwoners, ondernemers, medewerkers en (keten)partners. Hierbij wil zij transparant te werk gaan. Vertrouwen en verbinding zijn hierbij belangrijke kernwoorden: het waarborgen van de privacy van haar inwoners, ondernemers, medewerkers en (keten) partners staat hierbij centraal.
De komende jaren zet de gemeente Sliedrecht in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. De gemeente beschikt over een privacy coördinator. Deze persoon is het dagelijkse aanspreekpunt voor collega’s als het gaat om privacyvraagstukken en levert daarom een actieve bijdrage aan het bewustwordingsprogramma en/of voorlichtingsbijeenkomsten.
Een goede privacy boekhouding is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van inwoners 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.
Alle medewerkers zijn verantwoordelijk voor het bijhouden van het register van verwerkingen. De privacy coördinator coördineert het proces rondom het bijhouden van register van verwerkingen. Processen waar privacy risico's in kaart moeten worden gebracht, worden in samenwerking met de privacy coördinator opgepakt.

4. 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).
De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.
Naast dit door het college vastgestelde privacybeleid is er een Strategisch Informatiebeveiligingsbeleid Drechtsteden. Hierin zijn richtgevende kaders opgenomen voor maatregelen 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.

5. Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, van medewerkers van bedrijven en instellingen 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.

6. 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 gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. 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 een specifiek doel te bereiken en ze mogen dan niet gebruikt worden om een ander doel te bereiken. Dit mag alleen in geval van een verdere rechtmatige verwerking.

Verdere verwerking
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt 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 toets 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, voert de gemeente het op die manier uit. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan verwerkt de gemeente dit op deze manier.

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 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 https://www.sliedrecht.nl/Bestuur_politiek/Beleid_en_regelgeving/Regionaal_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 de ontwikkeling 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 genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

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 toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de externe toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure meldplicht datalekken.

Samenwerking
De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. 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, waarin het zorgvuldig omgaan met persoonsgegevens wordt geborgd.
Samenwerkingsverbanden
Verder werkt de gemeente samen met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. Hierbij kan men bijvoorbeeld denken aan de samenwerking binnen de Gemeenschappelijke regeling Sociaal, waarbinnen de Sociale Dienst Drechtsteden valt, of aan de Gemeenschappelijke regeling Dienst Gezondheid & Jeugd, of aan de Gemeenschappelijke regeling Omgevingsdienst Zuid-Holland Zuid. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoons-

gegevens worden verwerkt en wie waarvoor verantwoordelijk is. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.
De gemeente legt de afspraken met de organisatie vast, passend bij de rol van de partijen. Hierbij kan men denken aan het sluiten van een dienstverleningsovereenkomst en/of een convenant en/of een verwerkersovereenkomst. Hierin wordt meegenomen op welke wijze datalekken worden opgepakt en rechten van betrokkenen worden geborgd.
Een speciale samenwerking betreft die met de Service gemeente Dordrecht, als onderdeel van de gemeente Dordrecht. Deze organisatie verricht in opdracht van de gemeente diverse bedrijfsvoeringstaken, waarbij zij voor de gemeente persoonsgegevens verwerkt. In dat kader is tussen deze organisatie en de gemeente een verwerkersovereenkomst gesloten.

Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

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. De gemeente heeft in dit kader een privacyverklaring op haar website opgenomen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

Rechten van betrokkenen
Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar/het heeft verzameld 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. Betrokkenen kunnen hun recht uitoefenen onder andere via een webformulier dat te vinden is op de website van de gemeente. Daar is ook nadere informatie over de rechten van betrokkenen opgenomen.

Geschillenbeslechting
Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij/zij contact opnemen met de privacy coördinator. De betrokkene heeft ook het recht een klacht in te dienen bij de Functionaris Gegevensbescherming (fg@drechtsteden.nl).. Indien de betrokkene dit wenst kan hij/zij daarna nog een klacht bij de Autoriteit Persoonsgegevens indienen, 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, de burgemeester, als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente, tezamen met andere gemeenten in de Drechtsteden en de Omgevingsdienst Zuid-Holland Zuid, 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, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

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 een verwerking van persoonsgegevens. De gemeente voert in dat geval een risico analyse (DPIA) uit. Als uit de DPIA blijkt dat er inderdaad 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 raadpleging1 genoemd.

Functionaris gegevensbescherming (FG)
De burgemeester, het college en de raad zijn overheidsinstanties die structureel en op grote schaal persoonsgegevens verwerken, waaronder bijzondere persoonsgegevens. Ieder van deze bestuursorganen is verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een advise-

rende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de burgemeester, college en gemeenteraad van zijn werkzaamheden, bevindingen en aanbevelingen. Dit verslag wordt ter kennisname aan de gemeentesecretaris / Algemeen Directeur aangeboden.

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 en bij bestuur 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. Daarnaast worden er privacybewustwordingssessies gehouden voor nieuwe medewerkers.

7. Rollen en Verantwoordelijken

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, burgemeester, gemeenteraad, het management en medewerkers, de Functionaris voor de Gegevensbescherming (FG), de Privacy coördinator (PC) , de Chief information security officer (CISO) en de adviseur Informatieveiligheid.

Verantwoordelijk	
Feitelijk verantwoordelijk	• Directie, griffier en proceseigenaren / teamleiders • De medewerkers (inclusief inhuur / externen) die persoonsgegevens verwerken
Eindverantwoordelijk	• Het college van B&W, burgemeester en raad, elk voor zover het de eigen bevoegdheden betreft
Adviserend	• Privacy coördinator (PC) • Adviseur informatieveiligheid en Chief information security officer (CISO) • Functionaris Gegevensbescherming (FG)
Geïnformeerd Toezicht	• Gemeenteraad (privacyrechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

College van B&W, Burgemeester en raad
Het College, de burgemeester en de raad, elk voor zover het zijn of haar eigen bevoegdheden betreft, is bestuurlijk eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. De bestuursorganen hebben de volgende rollen en verantwoordelijkheden:
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeentelijke organisatie (de gemeenteraad voor de griffie);
- Stelt afzonderlijk van elkaar 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 duurzame privacycultuur.

Het college van B&W
Het college van B&W is verantwoordelijk voor het verwerken van persoonsgegevens binnen de gestelde kaders. Het college van B&W stelt hiervoor de beleidskaders en specifieke regelingen en procedures

vast. Jaarlijks legt ze verantwoording af aan de raad over privacy en de toepassing van het privacybeleid via de paragraaf bedrijfsvoering in de jaarstukken en de FG-jaarrapportage.

De burgemeester

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

De raad

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

Management

De algemeen directeur van de gemeentelijke organisatie en de griffier van de raad zijn operationeel eindverantwoordelijk voor de naleving van de privacywetgeving, alsmede voor de uitvoering van het privacybeleid.

Binnen de gemeentelijke organisatie hebben de teamleiders de volgende rollen en verantwoordelijkheden:

- Verantwoordelijk voor de naleving van de privacywetgeving en privacybeleid binnen het eigen team;
- Verantwoordelijk als proceseigenaar voor het voldoen aan de AVG van de eigen processen, waaronder het doen uitvoeren van een DPIA, indien nodig;
- Informeert de Privacy coördinator (en op verzoek van de FG) de FG op welke manier het eigen team compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen het eigen team;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op het eigen team;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Bevordert duurzame privacycultuur;
- Betrekt Privacy coördinator en (via de PC) de 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 is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. 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 privacywetgeving 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 privacyklachten en verzoeken van
- betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy
- risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke gevraagd en ongevraagd, onder andere bij datalekken.
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Brengt jaarlijks een verslag uit aan de gemeenteraad en het college van B&W van zijn werkzaamheden, bevindingen en aanbevelingen. Dit verslag wordt ter kennisname aan de gemeentesecretaris / Algemeen Directeur aangeboden.

Privacy Coördinator

De Privacy Coördinator is het eerste aanspreekpunt, zowel binnen de organisatie als naar buiten rondom privacygerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Coördinator heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken en proceseigenaren ten aanzien van het naleven en de uitvoering van het privacybeleid;

- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij 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 een DPIA 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 privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseert over de verwerkingsgrondslag;
- Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert verwerkingsverantwoordelijken bij het afhandelen van datalekken (volgens de meldprocedure).
- Behandelt verzoeken in het kader van de rechten van betrokkenen.

Andere rollen en verantwoordelijkheden

Afdeling	Betrokkenheid
Juridische Zaken (eventueel bij Juridisch Kenniscentrum SGD)	Ondersteunen van Privacy Coördinator ten aanzien van privacyvraagstukken en adviseren over privacy- gerelateerde bepalingen in overeenkomsten.
CISO en adviseur informatieveiligheid	Adviseren over implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. Tijdig melden van Informatiebeveiligingsincidenten bij PC/FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident.
Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data op welke wijze / in welk systeem verwerkt kan / moet worden).
Privacy ambassadeurs /contactpersonen	De Privacy Contactpersoon is het eerste aanspreekpunt binnen de afdeling waar de Privacy Contactpersoon werkzaam is en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid.

Overlegstructuur
In diverse (regionale) overlegvormen komt het voldoen aan de AVG aan de orde. Genoemd kunnen worden het:
Interne werkoverleggen
Privacy coördinatoren overleg (PCO)
Periodiek overleg met adviseurs informatiebeveiliging Periodiek overleg met informatiemanagers
Periodiek overleg met het Juridisch Kenniscentrum (JKC) van de Service gemeente Dordrecht
Periodiek overleg met de Functionaris Gegevensbescherming (FG)