DORDRECHT
GEMEENTEBLAD
Officiële uitgave van de gemeente Dordrecht

Nr. 382421
3 september
2025

Privacybeleid Gemeente Dordrecht 2025

De GEMEENTERAAD DORDRECHT van de gemeente DORDRECHT en de BURGEMEESTER van de gemeente DORDRECHT, ieder voor zover het zijn bevoegdheid betreft;

gezien het voorstel van het college van Burgemeester en Wethouders van 6 mei 2025 inzake Vaststellen Privacybeleid gemeente Dordrecht 2025;

gelet op artikel 160, lid 1 onder c van de Gemeentewet;

gelet op de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg);

B E S L U I T E N :

1. het Privacybeleid gemeente Dordrecht 2025 vast te stellen;
2. het Privacybeleid Drechtsteden 2020 in te trekken.

Aldus besloten in de vergadering van dinsdag 27 mei 2025.
De griffier, De voorzitter

Bijlage Privacybeleid Gemeente Dordrecht 2025

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.
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Dordrecht 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 heeft ook te maken met verwerkingen van persoonsgegevens op grond van de Wpg. Dan spreekt men van politiegegevens. Hierbij kan men denken aan de verwerkingen die de buitengewone opsporingsambtenaren (boa's) verrichten bij hun onderzoek naar en opsporing van strafbare feiten. Met betrekking tot het verwerken van politiegegevens is het “Addendum Privacybeleid Wet politiegegevens (Wpg) 2025” vastgesteld als addendum bij dit privacybeleid.

Inwerkingtreding, geldigheidsduur en intrekking oud privacybeleid
Op de eerste pagina van dit privacy beleid is aangegeven op welke datum dit beleid is vastgesteld door het college van B&W, de burgemeester en de gemeenteraad als eindverantwoordelijke voor de gemeentelijke gegevensverwerkingen, elk voor zover het zijn of haar bevoegdheden betreft. Het beleid treedt inwerking op de dag na die van de bekendmaking. Het privacybeleid 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 risicoanalyses) kan het college besluiten tot een tussentijdse herziening.
Het privacybeleid zoals dat is vastgesteld door het college op 25 augustus 2020, door de burgemeester op 25 augustus 2020 en door de gemeenteraad op 22 september 2020 wordt met de vaststelling van het voorliggende privacybeleid ingetrokken.

2. Begripsbepalingen

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

3. 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 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.

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 van wie 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 - 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 het Strategisch Informatiebeveiligingsbeleid Drechtsteden 2024 – 2028 vastgesteld. Hierin zijn richtinggevende 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.

- ***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, kan de gemeente van deze informatieplicht afwijken.

- ***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 zal de gemeente het op die manier verwerken (subsidiariteits- en proportionaliteitsbeginsel).

- ***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 Strategisch Informatiebeveiligingsbeleid Drechtsteden 2024 – 2028. 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.

- ***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, zoals is bepaald in artikel 38 van de AVG.

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.

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.

Verwerkingsregister
De gemeente beschikt over een verwerkingsregister, waarin 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 Data Protection Impact Assessment (DPIA) uitvoeren. Hierbij volgt de gemeente de lijst verplichte DPIA van

de Autoriteit Persoonsgegevens (AP)[1] . Voor de risico's die uit de DPIA komen, moet de gemeente voldoende maatregelen nemen om deze 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.

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 in het datalekregister, 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.

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.

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 het 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 privacybewustwordingstrainingen en e-learnings gehouden voor (nieuwe) medewerkers.

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 zelfstandig). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens 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 o.a. meegenomen op welke wijze datalekken worden opgepakt en rechten van betrokkenen worden geborgd.
Een speciale samenwerking betreft die tussen de Servicegemeente Dordrecht, als onderdeel van de gemeente Dordrecht, en de andere gemeenten. Deze organisatie verricht in opdracht van de gemeenten diverse bedrijfsvoeringstaken, waarbij zij voor de gemeenten persoonsgegevens verwerkt in de rol van verwerker. In dat kader is tussen de gemeente Dordrecht en de andere gemeenten een verwerkersovereenkomst gesloten.

Geschillenbeslechting
Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze zijn persoonsgegevens heeft verwerkt, kan hij/zij contact opnemen met de privacy coördinator (privacy@dordrecht.nl). De betrokkene heeft ook het recht een klacht in te dienen via de hiervoor ingerichte klachtenprocedure van de gemeente Dordrecht, dan wel hierover contact op te nemen met de Functionaris Gegevensbescher-

1) https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia
2) https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging

ming (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. De betrokkene wordt op deze mogelijkheden gewezen in de privacyverklaring op de website van de gemeente Dordrecht.

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 intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG 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 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 en dat er een planning is van de maatregelen die nog niet genomen zijn. In een Plan-Do-Check-Act-cyclus is de evaluatie van dit privacybeleid een onderdeel. Daarmee worden ook de bijbehorende beleidsstukken geëvalueerd.

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 Informatiebeveiliging.

Verantwoordelijk	
Feitelijk verantwoordelijk	• Het management, waaronder de Directie, opgavemanagers, clustermanagers en 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 informatiebeveiliging • 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 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.

Management
De gemeentesecretaris van de gemeentelijke organisatie is operationeel eindverantwoordelijk voor de naleving van de privacywetgeving binnen de organisatie, alsmede voor de uitvoering van het privacybeleid. Alle managementleden hebben 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 en het informeren van de betrokkenen over de gegevensverwerking, 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 de 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 het 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 aangeboden.

Privacy Coördinator/privacy adviseur
De Privacy Coördinator en de privacy adviseur zijn het eerste aanspreekpunt, zowel binnen de organisatie als naar buiten rondom privacygerelateerde vraagstukken, en hebben een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. Zij hebben de volgende rollen en verantwoordelijkheden:
- Zij adviseren en faciliteren de verwerkingsverantwoordelijken en proceseigenaren ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Stellen het privacybeleid en modellen, formats en standaard overeenkomsten op, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitoren en ondersteunen verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitoren en ondersteunen het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseren de verwerkingsverantwoordelijke bij het uitvoeren van een DPIA en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseren over de bepalingen in verwerkersovereenkomsten en faciliteren bij het opstellen, aanpassen en uitonderhandelen daarvan;

- Adviseren over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseren over de verwerkingsgrondslag;
- Ontwikkelen de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseren deze en voeren deze trainingen uit;
- Adviseren de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunen en faciliteren bij het opstellen en uitwerken daarvan;
- Ondersteunen en faciliteren verwerkingsverantwoordelijken bij het afhandelen van datalekken (volgens de meldprocedure).
- Behandelen verzoeken in het kader van de rechten van betrokkenen.

Andere rollen en verantwoordelijkheden

Rol	**Betrokkenheid**
Juridische Zaken	Ondersteunen van Privacy Coördinator en privacy adviseur ten aanzien van privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten.
CISO en adviseur informatiebeveiliging	Toepassing en 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 Ambassadeur is het eerste aanspreekpunt binnen de afdeling waar de Privacy Ambassadeur 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. Voorbeelden hiervan zijn:
- Interne werkoverleggen
- Privacy coördinatoren overleg (PCO)
- Periodiek overleg met adviseurs informatiebeveiliging
- Periodiek overleg met informatiemanagers
- Periodiek overleg met de Functionaris Gegevensbescherming (FG)
- Periodiek overleg in de privacy werkgroep van het Regionale Informatie- en Expertisecentra Rotterdam (RIEC Rotterdam)

ADDENDUM – verwijzing naar gerelateerde documenten
Dit addendum behoort tot dit privacybeleid. In het privacybeleid wordt gesproken over bepaalde thema's. Voor deze thema's dienen nog specifieke documenten te worden opgesteld, zoals beleidsstukken, procedures of werkinstructies. Op deze manier kan de lezer eenvoudig achterhalen waar meer gedetailleerde instructies te vinden zijn over een bepaald thema. Hieronder is per thema aangegeven waar nog specifieke documenten voor moeten worden vastgelegd en vastgesteld:

- **Proces omtrent het verwerkingsregister**
  Een proces rondom het verwerkingsregister gaat over het bijhouden en documenteren van alle verwerkingsactiviteiten door de gemeente. Het bijhouden van het verwerkingsregister dient integraal onderdeel te zijn van de werkprocessen van de verschillende afdelingen binnen de gemeente. Om te bewerkstelligen dat (nieuwe) verwerkingen standaard worden meegenomen in het verwerkingsregister, dient dit proces te worden vastgesteld met daarin de verantwoordelijkheden van

de verschillende medewerkers, zoals de privacy officer en/of privacy coördinator, teamleiders en andere sleutelpersonen zoals de contactpersoon voor de specifieke verwerking(en).

- **Bewaartermijnen beleid**
  Een bewaartermijnenbeleid is een beleid waarin wordt vastgelegd hoe lang bepaalde documenten, gegevens of informatie bewaard moeten worden en wanneer ze vernietigd moeten worden. Het doel is om te zorgen voor een efficiënte en wettelijke omgang met informatie, waarbij persoonlijke gegevens en andere gevoelige informatie niet langer dan nodig worden bewaard. Een centraal bewaartermijnenbeleid zorgt voor een meer uniforme toepassing binnen de organisatie en minder ad hoc. In dit beleid dienen in ieder geval de volgende onderwerpen te worden opgenomen:
  - Zowel wettelijke als zelf gedefinieerde bewaartermijnen;
  - Wie er verantwoordelijk is voor het verwijderen en anonimiseren;
  - Aanvullende informatie bij de zelf gedefinieerde bewaartermijnen, zoals wanneer deze termijnen ingaan.

- **DPIA beleid**
  Een DPIA (Data Protection Impact Assessment) beleid dient de procesafspraken rondom DPIA's te formaliseren. Hierin wordt ieders rol, taak en verantwoordelijkheid toegelicht en worden de structuur en de processen beschreven die gevolgd moeten worden bij het uitvoeren van een DPIA. Het beleid legt vast wie verantwoordelijk is voor elke stap in het proces en zorgt ervoor dat alle betrokken medewerkers hun specifieke verantwoordelijkheden kennen.

- **DPIA werkinstructie voor medewerkers**
  DPIA werkinstructie beschrijft het ingerichte werkproces voor het uitvoeren en registreren van DPIA's. Hierin dient onder andere te worden opgenomen:
  - Een praktische en begrijpelijke handleiding voor het uitvoeren van DPIA's met een duidelijke uitleg bij elke stap.
  - Een procedure voor het beoordelen van de noodzakelijkheid van een DPIA voor nieuwe verwerkingen.

- **Datalekken werkinstructie voor medewerkers**
  Een werkinstructie voor medewerkers binnen de gemeente over datalekken bevat richtlijnen en procedures die gevolgd moeten worden wanneer er een datalek plaatsvindt. De werkinstructie legt uit hoe medewerkers een datalek moeten herkennen, melden en welke stappen ze moeten ondernemen om het lek te beperken en te verhelpen. Hierbij dient de nadruk te worden gelegd op wat een datalek is, hoe zij deze kunnen herkennen en hoe/of zij deze in TopDesk moeten melden.

- **Datelekken beleid**
  Een datalekken beleid beschrijft de procedures en verantwoordelijkheden van medewerkers en afdelingen wanneer er een datalek wordt ontdekt. Het geeft aan wie verantwoordelijk is voor het melden van een datalek, hoe het incident moet worden behandeld, welke maatregelen moeten worden genomen om de schade te beperken en hoe het datalek moet worden gecommuniceerd naar de betrokkenen en toezichthouders. Het beleid definieert ook de taken en verantwoordelijkheden van specifieke rollen, zoals de functionaris voor gegevensbescherming (FG), IT, Informatiebeveiligingsteams en management.
  Het beleid dient onder andere de volgende informatie te bevatten:
  - De processen voor de wijze waarop datalekken moeten worden gemeld
  - De taken, bevoegdheden en verantwoordelijkheden
  - Vastgestelde uitzonderingen
  - Formeel vastgestelde richtlijnen over het voorkomen van datalekken
  - Hoe er wordt bepaald of er daadwerkelijk een datalek heeft plaatsgevonden en wat de gevolgen daarvan zijn

- **Rechten van betrokkenen procedure**
  Een rechten van betrokkenen procedure is een document dat beschrijft hoe de gemeente de rechten van betrokkenen in het kader van de AVG respecteert en uitvoert. Het beleid stelt vast hoe betrokkenen hun rechten kunnen uitoefenen en bevat daarnaast procedures voor medewerkers

en afdelingen waarin de rollen en verantwoordelijkheden worden beschreven. Hierbij dient in ieder geval te worden ingegaan op:

- Wie heeft welke taak bij het opvolgen van verzoeken van betrokkenen? Denk hierbij aan welke rol medewerkers in het algemeen hebben, maar ook de teamleiders, de privacy officer, de privacy coördinator en de FG.
- Zijn de taken voor elk AVG-verzoek hetzelfde? Mogelijk dat voor een verzoek tot gegevens-wissing intern een IT-medewerker of functioneel beheerder moet worden gecontacteerd om bijvoorbeeld een specifieke verwijdering door te voeren, of een correctie te maken.

- **Beleid omtrent privacy governance**
In het privacy governance beleid worden de taken en verantwoordelijkheden voor de eerste, tweede en derde lijn in kaart gebracht. Dit houdt in dat duidelijk wordt wie (functie medewerker) binnen een team of afdeling verantwoordelijk is voor het uitvoeren van bepaalde werkzaamheden (eerste lijn) en welke taken en verantwoordelijkheden zijn belegd in de tweede en derde lijn.