

Privacybeleid Gemeente Maashorst

¹ Privacybeleid op naam Maashorst overeenkomstig Informatiebeveiligingsdienst voor gemeenten (IBD), versie 1.1

Versiebeheer

Versie	Wijzigingen	Datum
0.9	Versie tbv stuurgroep	Juli 2021
1.0	Juridische afstemming, vigerend (Uden Landerd) blijft van kracht	Maart 2022
1.1	Besluit omzetten nieuwe standaard (Informatiebeveiligingsdienst)	September 2022
1.2	Nieuwe standaard verwerkt	Oktober 2022
1.3	Lokaal afgestemd JZ (concern)	Februari 2023
1.4	Besproken in security privacy overleg	Februari 2023
1.5	Besproken in Poho	Februari 2023
1.6	Korte juridische screening	Maart 2023
1.7	Bespreken HR	Maart 2023
1.8	Vooroverleg OR	Maart 2023

Inhoud

1. Inleiding	4
2. Begripsbepalingen	4
3. Visie	4
4. Doel	5
5. Reikwijdte	5
6. Principes voor de verwerking van persoonsgegevens	6
7. Rollen en Verantwoordelijken	11

1. Inleiding

De gemeente Maashorst 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 Maashorst persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente Maashorst 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 Maashorst 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 4 april 2023 door het college van B&W als eindverantwoordelijke voor de gegevensverwerking. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetwijzigingen, uitkomsten van privacy assessments) kan het college besluiten tot een tussentijdse herziening.

De rol van de raad is gelegen in haar controlerende functie, op basis van reguliere rapportages (Jaarrekening en indien noodzakelijk separate rapportage van de FG).

2. Begripsbepalingen

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

3. Visie

De komende jaren zet de gemeente Maashorst 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. De gemeente sluit hiermee ook aan bij het eigen Bestuursakkoord 2022-2026² en Uitvoeringsprogramma³

² [bestuursakkoord-gemeente-maashorst-2022-2026.pdf \(gemeentemaashorst.nl\)](#)

³ [21062022-uitvoeringsprogramma-maashorst-versie-14-definitief.pdf \(gemeentemaashorst.nl\)](#)

4. Doel

Met dit privacybeleid geeft de gemeente Maashorst 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 taken en bevoegdheden op het gebied van bescherming van persoonsgegevens zijn vastgelegd in de Organisatieregeling Maashorst⁴ en het hierop gebaseerde kwaliteitskader van de Werkwijze Algemeen Belang.⁵

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, logging, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning. Hiervan wordt een overzicht bijgehouden.

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. De vastgestelde beleidskaders zijn raadpleegbaar op [Beleid | Gemeente Maashorst](#)

Verantwoordelijkheid van iedere werknemer

Iedereen werkzaam binnen de gemeente Maashorst 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

5. Reikwijdte

De gemeente Maashorst 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;

⁴ <https://lokaleregelgeving.overheid.nl/CVDR677762/1>

⁵ [Microsoft Word - Bijlage 3 Kader Werkwijze Algemeen Belang versie met aanvulling IFR Rad vd Wet \(gemeentemaashorst.nl\)](#)

⁶ Terzake wordt verwezen naar de geactualiseerde privacyverklaring in het personeelshandboek [Documenten - Personeelshandboek - Weten en regelen - Gemeente Maashorst](#)

2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente Maashorst 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 Maashorst 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 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

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, dan kiest de gemeente bij voorkeur voor die mogelijkheid. 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 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 verzamelt 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 1995⁷ 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 vastgestelde 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* (PbD) 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

⁷ De archiefwet ondergaat momenteel een vernieuwing, en zal effect gaan krijgen op bewaartermijnen voorwaarden en – lokaties. Naar verwachting zal de nieuwe archiefwet in 2024 van kracht worden. De Autoriteit Persoonsgegevens heeft in een brief geadviseerd de nieuwe archiefwet meer in lijn te brengen met de AVG [. \(https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_modernisering_archiefwet.pdf\)](https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_modernisering_archiefwet.pdf).

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 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 beleidsregels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de rubriek “Weten en regelen” van het gemeentelijk Intranet.⁸

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.

Samenwerkingsverbanden⁹

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 individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat 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, 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. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

⁸ [Algemeen - Datalekken of het vermoeden daarvan - Weten en regelen - Gemeente Maashorst](#)

⁹ Het betreft hier niet alleen Samenwerkingsverbanden als bedoeld in het Wetsvoorstel samenwerkingsverbanden (Momenteel in EK), maar ook andere regionale en lokale samenwerkingsverbanden waarbij persoonsgegevens worden verwerkt.

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar 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. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de <procedure rechten van betrokkenen>.

Geschillenbeslechting

- Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de gemeentelijke website. [Klacht indienen | Gemeente Maashorst](#)

De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, 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 Autoriteit Persoonsgegevens (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 taken en bevoegdheden van de FG staan omschreven in artikel 9 van de Organisatieregeling Maashorst.

Verwerkingsregister

De gemeente beschikt over een verwerkingsregister, waarin verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt. Dit register is gebaseerd op een standaard overzicht van de VNG en wordt stelselmatig geactualiseerd bij nieuwe verwerkingen.

Gegevenseffectbeoordeling .

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 privacy assessment (ook wel Data Protection Impact Assessment of DPIA genoemd) uit. Als hieruit 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](#)¹⁰ genoemd.

¹⁰ <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging>

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 het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen. In Maashorst maakt dit verslag deel uit van de gemeentelijke programmabegroting en het gemeentelijke jaarverslag. Dit verslag omvat zowel het werkingsgebied van de AVG als het werkingsgebied van de Wet Politie Gegevens, uitsluitend op het terrein van de werkzaamheden van de Bijzondere Opsporings Ambtenaren (Boa's).

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. Deze wordt regelmatig besproken met de directeur bedrijfsvoering.

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.

7. Rollen en Verantwoordelijken

De Organisatieregeling van de gemeente biedt een overkoepelende visie en strategie hoe de werkzaamheden waaronder de bescherming van persoonsgegevens effectief belegd worden binnen de organisatie (Integrale samenwerking en integrale dienstverlening) Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het College van B&W, het managementteam en medewerkers, de Functionaris voor de Gegevensbescherming (FG), en afgeleid daarvan de Privacy Officer en de CISO.

	Verantwoordelijk	
R	Responsible/ Feitelijk verantwoordelijk	• Teammanagers en Directeuren • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/ Eindverantwoordelijk	• Het college van B&W
C	Consulted/ Adviserend	• Privacy Officer • CISO • Functionaris Gegevensbescherming
I	Informerend/ Geinformeerd	• Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

Rollen en verantwoordelijkheden voor privacy gespecificeerd

College van B&W

Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het College heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de de privacywetgeving binnen de gemeente;
- 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 duurzame privacycultuur.

Teammanagers en directeuren

De teammanagers en directeuren zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de teams, alsmede voor de uitvoering van het privacybeleid.

De teammanagers en directeuren hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen het eigen team;

- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen het eigen team;
- Informeert 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;
- Aansturen van de privacy contactpersonen, voor zover benoemd binnen het eigen team;
- Bevordert duurzame privacycultuur;
- Betrekt PO 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 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 namens de Autoriteit Persoonsgegevens;
- 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 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 bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingenregister;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan het College van B&W.

Privacy Officer

De Privacy Officer is het eerste aanspreekpunt voor de gemeente rondom privacygerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken 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 geveenseffectbeoordeling (GEB) 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 (en adviseert, indien van toepassing, over de informed consent);
- 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 verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

Andere rollen en verantwoordelijkheden

Team	Betrokkenheid
Juridische Zaken/domein jurist	Primair binnen eigen team, daarna domein, cf organisatieverordening. Ondersteunen van Privacy Officer/FG ten aanzien van complexe privacyvraagstukken en adviseren over complexe privacy-gerelateerde bepalingen in overeenkomsten.
CISO	Toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. Adviseren van de organisatie bij datalekken (volgens de meldprocedure). Tijdig melden van Informatiebeveiligingsaspecten en - incidenten bij PO/FG

	als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het aspect en/of incident.
Communicatie zowel intern naar medewerkers als extern (woordvoering)	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)
Concern Control /controleer	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).
Privacy contactpersonen	De Privacy Contactpersoon is het eerste aanspreekpunt en vraagbaak binnen het team waar de Privacy Contactpersoon werkzaam is en heeft een ondersteunende functie rondom het uitvoeren van het privacybeleid. ¹¹

Overlegstructuur

Op regelmatige basis vindt overlegt plaats over informatieveiligheid en privacy, daarbij zijn de inhoudelijk betrokken functionarissen (CISO, FG, PO, teammanager I&G en IAS) betrokken alsmede de verantwoordelijk directeur (directeur dienstverlening) .

¹¹ Het betreft hier een beperkte deeltaak die binnen een bestaande functie wordt ondergebracht.