

Privacy beleidskader 2025

1. Het privacy beleidskader 2019 in te trekken;
2. Het privacy beleidskader 2025 vast te stellen

1. Inleiding

De gemeente Landsmeer 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 van. 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 Landsmeer 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: AVG), de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG), de Wet Politiegegevens (hierna: Wpg) en het Besluit politiegegevens buitengewoon opsporingsambtenaren (hierna: Bpg boa).

Er was een Privacy Beleidskader 2019 vastgesteld. Daarin was opgenomen dat deze twee jaarlijks zou worden geëvalueerd, geactualiseerd en herijkt. Na evaluatie van het beleid is het met dit aangepaste Privacy Beleidskader 2025 herijkt.

Geldigheidsduur

Dit beleid is vastgesteld op 1 april 2025 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. Begripsbepalingen

De definities van art. 4 AVG en art. 1 Wpg hebben in dit beleidsdocument dezelfde betekenis.

3. Visie en ambitie

De komende jaren zet de gemeente in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. De gemeente streeft om tot privacy volwassenheidsniveau 4 te komen. Dit houdt in dat de gemeente beheerst, met een Plan, Do, Check, Act-cyclus, de AVG en Wpg implementeert.

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 team is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de gemeente.

4. Doel

Met dit privacy beleid 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 privacy beleid 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 domein specifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

Naast dit door het college vastgestelde privacy beleid 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 privacy beleid 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 privacy beleid worden opgevolgd en actief worden uitgedragen.

PDCA-cyclus

De gemeente streeft naar een gemanaged niveau van kwaliteit in bescherming van de privacygegevens. Dat vereist dat de gemeente *in control* is en daarover op professionele wijze verantwoording aflegt. *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.

5. Reikwijdte

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

Dit privacy beleid 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.

De gemeente verwerkt politiegegevens van betrokkenen in Domein 1: Openbare Ruimte en Domein 3: Onderwijs.

- Domein 1: Openbare Ruimte
 - o De gemeente gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving in de openbare ruimte. Daarom zijn binnen dit taakveld boa's aangesteld en is de Wpg van toepassing.
- Domein 3: Onderwijs
 - o De gemeente gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving van de leerplichtwet, in het bijzonder art. 16 lid 5 en art. 26. Daarom zijn binnen dit taakveld boa's aangesteld en is de Wpg van toepassing.

De interne en externe audits die voor de Wpg verplicht zijn, worden gecoördineerd door de privacy officer. De gemeente Landsmeer is verplicht om jaarlijks een interne audit en iedere 4 jaar een externe audit te laten uitvoeren en de resultaten van de externe audit te delen met de AP. De betrokkenen worden geïnformeerd over de verwerking van politiegegevens via de website en bij de eerste brief die zij ontvangen over strafrechtelijke handhaving.

Dit privacy beleid is van toepassing op de verwerkingen van persoonsgegevens die vallen onder de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

6. Principes voor de verwerking van persoonsgegevens

De belangrijkste wettelijke kaders van het privacy beleid zijn:

- De Algemene verordening gegevensbescherming;
- De Uitvoeringswet Algemene verordening gegevensbescherming;
- De Wet Politiegegevens; en
- Het Besluit politiegegevens buitengewoon opsporingsambtenaren.

De AVG en Wpg zijn 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.

Het privacy beleid schept een algemeen kader voor de omgang met persoonsgegevens. Er zijn echter ook veel andere wetten die aanvullende eisen stellen aan de bescherming van persoonsgegevens, zoals de Wet Basisregistratie Personen (BRP), de Wet maatschappelijke ondersteuning 2015 (Wmo) en de

Jeugdwet, maar ook het Besluit politiegegevens of de Regeling periodieke audit politiegegevens. De gemeente dient zich ook aan de aanvullende privacyregels te houden.

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.

In het kader van de Wpg voert de gemeente alleen verwerkingen uit in het kader van artikel 8 van de Wpg in het kader van de dagelijkse politietaak.

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.

De gemeente verwerkt politiegegevens uitsluitend in het kader van artikel 8 Wpg: uitvoering van de dagelijkse politietaak.

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.

De politiegegevens worden niet voor andere doeleinden verwerkt.

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.

Bijzondere persoonsgegevens worden uitsluitend verwerkt als dit noodzakelijk is voor het uitvoeren van wettelijke taken. Voor de uitvoering van strafrechtelijke handhaving op de leerplicht is het mogelijk dat bijzondere persoonsgegevens worden verwerkt, indien dit noodzakelijk is om aan te tonen voor het opmaken van een proces verbaal.

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.

De Wpg kent zijn eigen bewaartermijnen. De gemeente verwerkt alleen gegevens op basis van art. 8 Wpg. Dit betekent dat politiegegevens in het kader van de dagelijkse politietaak 1 jaar lang breed gebruikt mogen worden. In de 4 jaren daarna alleen via gericht zoeken, bijvoorbeeld op naam of kenteken.

Daarna moeten politiegegevens 5 jaar bewaard worden voor audit en klachten. Na de totale termijn van 10 jaar worden de politiegegevens vernietigd.

Beschikbaarheid, 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 iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

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. Aanvullend zijn er afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen. Deze bevoegdheden en afspraken worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden worden periodiek geëvalueerd. 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.

Politiegegevens worden alleen verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en Bpgb zijn opgenomen. Voor verstrekkingen wordt gebruik gemaakt van de verstrekkingenwijzer.

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 regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in het Protocol beveiligingsincidenten en 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 privacy beleid van de gemeente. De AVG en Wpg 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 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 privacy beleid.

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.

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.

Onder de Wpg zijn de rechten van betrokkenen anders dan die onder de AVG. Betrokkenen hebben de mogelijkheid om hun rechten uit paragraaf 4 van de Wpg uit te oefenen, te weten het recht van informatie, recht op inzage en recht op rectificatie en vernietiging van politiegegevens. 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 website [gemeente Landsmeer | Privacyverklaring](#). 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, 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 over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG en de Wpg 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. Artikel 30 AVG en artikel 31d Wpg noemen de gegevens die tenminste in het register moeten staan.

Proceseigenaren zijn verantwoordelijk voor het melden van nieuwe verwerkingen en relevante wijzigingen in bestaande verwerkingen, waarna deze in het register verwerkt worden. Voor het beheer van het verwerkingsregister hanteert de gemeente een interne procedure.

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 DPIA uit. 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 genoemd. Nadere regels ten aanzien van de DPIA's zijn opgenomen in de DPIA-procedure.

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

Om daadwerkelijk te kunnen waarborgen dat de bescherming van persoonsgegevens ingebed wordt in de gemeentelijke organisatie is het noodzakelijk dat alle medewerkers die persoonsgegevens gebruiken dit op een zorgvuldige wijze doen en het proces beheerst wordt vanuit een centrale visie.

Rollen en verantwoordelijkheden

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 privacywetgeving binnen de gemeente;
- Stelt het privacy beleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacy beleid op basis van de rapportage van de FG;
- Bevordert duurzame privacy cultuur.

Teammanagers

De teammanagers zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen het team, alsmede voor de uitvoering van het privacy beleid.

De teammanagers hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen het eigen team;
- Verantwoordelijk voor implementatie en uitvoering van het privacy beleid binnen het eigen team;
- Informeren gezamenlijk als MT 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 privacy cultuur;
- Maken van keuzen op het gebied van privacyrisico's, zoals het treffen van maatregelen en het accepteren van rest risico's, hierbij ondersteunt de privacy officer hen;
- Winnen advies in bij de PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

De teammanagers met daarin boa's hebben ook de volgende rollen en verantwoordelijkheden:

- Het nemen van autorisatiebesluiten voor toegang tot de applicaties met politiegegevens;
- Het vaststellen van de autorisatiematrix voor de applicaties waarin politiegegevens worden verwerkt;
- De periodieke controle van verwerkingen van politiegegevens;
- Het vaststellen van procesbeschrijvingen en gerelateerde documenten over de verwerking van politiegegevens.

Functionaris Gegevensbescherming (FG)

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 en Wpg;
- 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 privacy beleid 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 ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan het College van B&W.

De FG stelt jaarlijks een verslag op van zijn bevindingen over de naleving van de AVG en Wpg.

Privacy Officer

De Privacy Officer 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 privacy beleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacy beleid;
- Opstellen privacy beleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Het samenstellen van een jaarlijks Privacy uitvoeringsprogramma;

- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacy beleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Beheert het centrale verwerkingsregister;
- 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;
- Organiseert bewustmakingsprogramma's- en privacy trainingen voor medewerkers;
- 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).

In het kader van de Wpg is de rol van de Privacy Officer om jaarlijks te inventariseren of het bereik van de verwerkingen met politiegegevens is gewijzigd. De Privacy Officer heeft ook een coördinerende rol bij het implementeren van verbetermaatregelen voor de naleving op de wetgeving en is het eerste aanspreekpunt van de auditor.

Andere rollen en verantwoordelijkheden

Teams of Rollen	Betrokkenheid
Team Bestuur en Ondersteuning, onderdeel Informatiebeveiliging:	Toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens; Behandelen van datalekken bij afwezigheid van PO; Tijdig melden van informatiebeveiligingsincidenten bij PO/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 procedure beveiligingsincidenten en datalekken); Zichtbaar maken van de privacy informatievoorziening op de websites.
Team Bedrijfsvoering, onderdeel Informatiebeheer	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).
Team Fysiek, onderdeel toezicht en handhaving	Naleven van de Wet politiegegevens door domein 1 boa's
Team Inwoners, onderdeel leerplicht	Naleven van de Wet politiegegevens door domein 3 leerplichtambtenaar