Meerinzicht
Ermelo | Harderwijk | Zeewolde

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 420
19 april
2023

Officiële uitgave van de gemeenschappelijke regeling Meerinzicht

Privacy beleid

bij de gemeente Ermelo, Harderwijk en Zeewolde en bij Meerinzicht

Inleiding

Een privacy beleid is een uitwerking van artikel 24 van de Algemene Verordening Gegevensbescherming (AVG). In 2018 is er door de verschillende gemeenten een privacy beleid gepubliceerd in het Gemeenteblad. Dit privacy beleid vervangt deze publicaties (Ermelo: gmb-2018-118584, Harderwijk: gmb-2018-159416, Zeewolde: gmb-2018-191295). Dit privacy beleid is ook van toepassing voor Meerinzicht.

Dit privacy beleid vervangt het door de gemeenten opgestelde beleid van 2018 en heeft primair tot doel om het beleid te harmoniseren over de 4 organisaties. Daarnaast dient het beleid ook om een stap vooruit te maken in het volwassenheidsniveau van de organisatie op het gebied van privacy. De veranderende omstandigheden in de maatschappij (denk aan grotere dreiging van cybercriminaliteit, maar ook de wens tot datagedreven en hybride werken) vragen om beleid wat een kader schept hoe erop te reageren.

Dit beleid is van toepassing op de gehele organisatie (dus op gemeenten, colleges, raden en griffies en Meerinzicht) en is primair gericht aan alle medewerkers die in het kader van hun taak persoonsgegevens verwerken. Het betreft een overkoepelend kader waarin de maatregelen op abstract niveau zijn uitgewerkt. In werkplannen, procedures en werkinstructies is, wordt (of dient te worden) een verdere uitwerking gegeven aan de wijze waarop de bescherming van persoonsgegevens is geborgd.

Burgers, ondernemers, medewerkers en partners moeten er namelijk op kunnen vertrouwen dat gemeenten en de gemeenschappelijke regeling passende bescherming biedt bij de verwerking van persoonsgegevens. Dat is onder andere bepaald in de AVG, de bijbehorende Uitvoeringswet (UAVG) en sectorspecifieke wetgeving, zoals bijvoorbeeld de Gemeentewet, de archiefwet, de Wet maatschappelijke ondersteuning 2015 (Wmo 2015), de Jeugdwet, de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet suwi) en de Wet politiegegevens (Wpg).

We hebben in veel gevallen voor de uitvoering van onze (wettelijke) taken persoonsgegevens nodig. Zonder de verwerking van persoonsgegevens is het bijvoorbeeld onmogelijk om een uitkering aan een burger te verstrekken of een vergunning te verlenen. Maar de AVG schrijft ook voor dat we niet meer persoonsgegevens mogen verwerken dan noodzakelijk voor de taak en dat kan best een uitdaging zijn.

En wat te doen bij nieuwe beleidsontwikkelingen of IT waarin persoonsgegevens nodig zijn. Hoe vindt dan een zorgvuldige afweging plaats van de risico's op de bescherming van privacy. Hoe wordt dat getoetst en wie is daar verantwoordelijk voor? De verwerking van persoonsgegevens leiden tot een zeker risico. Door passende gegevensbescherming willen wij risico's beheersen. Daarom dit privacy beleid.

Ambitie en visie privacy

Binnen de gemeenten en de gemeenschappelijke regeling zijn persoonsgegevens en de verwerking daarvan een van de belangrijkste zaken. Dit is onlosmakelijk verbonden aan de wettelijke taken van een gemeente.

Voor de burger is het, mede gezien de mogelijke afhankelijkheidsrelatie met de overheid, van belang dat zij erop kunnen vertrouwen dat met hun persoonsgegevens zorgvuldig en verantwoord wordt omgegaan. Een zorgvuldige verwerking van de persoonsgegevens wordt juist bereikt met de naleving van de AVG en daagt ons uit om een stevige ambitie uit te spreken ten aanzien van het gegevensbescherming niveau. Deze bescherming vinden wij dan ook van groot belang, zonder dat dit de dienstverlening aan de burger in de weg staat. Daarbij kunnen wij verantwoorden hoe wij omgaan met de gegevens van onze inwoners en kunnen hen hier ook over informeren.

De ontwikkelingen in de samenleving en technologie maken dat privacy en informatiebeveiliging steeds belangrijker worden. Toenemende digitalisering en samenwerking met andere partijen in dienstverle-

ningsketens leidt tot meer en sneller uitwisselen van informatie. Onze inwoners willen snel en digitaal geholpen worden, maar willen dit doen zonder dat dit hun privacy onevenredig aantast.

Onze medewerkers willen en moeten steeds meer plaats en tijdonafhankelijk kunnen werken, maar dit mag niet leiden tot onrechtmatige toegang tot gegevens. De komende jaren moet er voortdurend blijven worden ingezet op het verbeteren of optimaliseren van gegevensbescherming, informatieveiligheid en de informatiebeveiliging. Er zal steeds moeten worden aangesloten op veranderende wetgeving op het gebied van gegevensbescherming, informatisering, digitalisering en informatiebeveiliging. De afdeling Informatisering & Automatisering faciliteert vrijwel alle werkprocessen van de gemeenten en de gemeenschappelijke regeling.

Onze ambitie beschreven in punten:
- Wij zorgen voor een juiste uitvoering van onze (wettelijke) taken en dienstverlening;
- Wij waarborgen de bescherming van persoonsgegevens, zoals de AVG dit voorschrijft;
- Wij leven ook overige wet- en regelgeving na op het gebied van gegevensbescherming;
- Wij handelen op dit vlak steeds transparant en controleerbaar;
- Wij leggen rekenschap af over beleid en maatregelen;
- Wij bieden personen eenvoudige mogelijkheden om de correctheid van hun verwerkte persoonsgegevens te controleren;
- Wij hebben de persoonsgegevens die wij verwerken beveiligd volgens de richtlijnen van de Baseline Informatiebeveiliging Overheid (BIO).

Verwerking van persoonsgegevens

Wettelijk kader

Voor de bescherming van persoonsgegevens gelden de volgende wettelijke kaders:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

Daarnaast is de verwerking van persoonsgegevens geregeld in diverse andere wet en regelgeving.

Uitgangspunten

Wij gaan op een veilige manier met persoonsgegevens om en respecteren de privacy van onze inwoners. Wij houden ons daarom aan de volgende uitgangspunten:

A) Persoonsgegevens worden rechtmatig, behoorlijk en transparant verwerkt
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Op ons rust echter een veelheid aan wettelijke verplichtingen op grond waarvan wij persoonsgegevens verwerken. Wij dienen ervoor te zorgen dat betrokkenen daar inzicht in hebben.

Dit kan onder andere gedaan worden door het verwerkingsregister online beschikbaar te maken. Op dit moment is het register nog niet online beschikbaar. We streven erna om dat in 2023 online beschikbaar te gaan maken. Op dit moment zijn de verwerkingsregisters alleen beschikbaar in Excel, wat publicatie lastig maakt; er zal eerst een pakket worden aangezocht waarin de verwerkingen en de publicatie ervan kan worden gerealiseerd. Het verwerkingsregister zal continu actueel en up-to-date worden gehouden door de proceseigenaren.

In 2022 wordt de Wet Open Overheid van kracht. Dit draagt bij aan transparantie, maar moet ook voldoen aan de eisen van de AVG. Alle documenten die actief openbaar moeten worden gemaakt mogen geen persoonsgegevens bevatten. Om dat te kunnen bereiken zal er ondersteunende software beschikbaar komen om te anonimiseren.

B) Doelbinding
Wij verwerken persoonsgegevens alleen als vooraf de doeleinden zijn bepaald en deze precies zijn omschreven. Veelal verwerken we persoonsgegevens vanuit een wettelijke verplichting. Wanneer de persoonsgegevens later voor een ander doel nodig zijn, dan gebruiken we dat alleen als het nieuwe doel verenigbaar is met het oorspronkelijke doel.

Zowel het stellen van doelen vooraf, als de beperking voor ander gebruik heeft bewustzijn nodig. We zullen dit bewustzijn continu blijven vergroten door opleiding, training en advisering. Ook is belangrijk dat we de beschikking hebben over een actueel en volledig verwerkingsregister.

C) Minimale gegevensverwerking
Wij verwerken alleen de persoonsgegevens die maximaal noodzakelijk zijn voor het vooraf bepaalde doel. Dat doel wordt doorgaans vastgesteld door wettelijke regelingen die wij uitvoeren. Wij streven

naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt. Om dat te bereiken evalueren wij onze processen doorlopend en waken op die wijze voor overbodige verwerking van persoonsgegevens.

Medewerkers dienen op de hoogte te zijn van de persoonsgegevens die ze nodig hebben voor hun taak. Dit is vastgelegd in het verwerkingsregister. Daarnaast dienen ze door middel van autorisaties alleen toegang te hebben tot die persoonsgegevens die ze nodig hebben voor de uitvoering van hun taken. Dit onderdeel zal in de komende jaren verder moeten worden ingericht.

Geautomatiseerde besluitvorming kan onze dienstverlening verbeteren, maar de inbreuk die het kan doen op de privacy van mensen moet daarbij goed gemonitord blijven. Uitgangspunt in ons beleid is dat er geen geautomatiseerde besluitvorming zal worden ingezet, zonder menselijke tussenkomst, als de beslissing nadelige gevolgen kan hebben voor de persoon die onderworpen wordt aan geautomatiseerde besluitvorming.

Geautomatiseerde besluitvorming kan ook leiden tot profilering. Van profilering is sprake wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie.

De organisatie streeft geen profilering na. Indien dit in de toekomst aan de orde zal zijn zal het moeten voldoen aan alle eisen die de AVG hieraan stelt.

D) Persoonsgegevens zijn juist
Wij treffen alle redelijke maatregelen om te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn worden gewist of gecorrigeerd.

E) Persoonsgegevens worden niet langer bewaard dan nodig
Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen voeren, of om wettelijke verplichtingen te kunnen naleven. Gemeenten zijn daarbij gebonden aan het bepaalde in de Archiefwet, de daarop gebaseerde besluiten en andere wetten. Hoe lang het noodzakelijk is om persoonsgegevens te bewaren hangt daarom af van het bepaalde in de archiefwet of bijzondere wetten, zoals de Wet basisregistratie personen of fiscale wet- en regelgeving. De bewaartermijn varieert daardoor fors. In ons verwerkingsregister hebben wij daarom per gegevensverwerking de wettelijke bewaartermijn opgenomen.

Het is van belang dat onze applicaties de functies hebben om dit uitgangspunt en het uitgangspunt ‘persoonsgegevens zijn juist’ te ondersteunen. Niet in alle gevallen is dat nu op de juiste manier beschikbaar, hetgeen meer handmatig werk vraagt dan gewenst. Het is mogelijk dat dit alleen opgelost kan worden door een nieuwe applicatie aan te schaffen. Daarbij is dan een uitgangspunt van privacy by design belangrijk. We zullen in de komende jaren hier aandacht aan gaan schenken.

F) Integriteit en vertrouwelijkheid
Wij zorgen dat:

- persoonsgegevens goed beveiligd worden opgeslagen om misbruik, verlies, onbevoegde toegang en bewerking te voorkomen;
- aandacht wordt besteed bij inrichting van processen en systemen aan privacy verhogende maatregelen (privacy by design);
- zo nodig worden er Data Protection Impact Assessments (DPIA) uitgevoerd om de impact van een verwerking op voorhand goed in te kunnen schatten.
- persoonsgegevens beveiligd zijn en hierbij de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd wordt;
- persoonsgegevens alleen toegankelijk zijn voor die functionarissen (ambtenaren, externen, leveranciers, partners) die dat nodig hebben voor de directe taakuitoefening;
- het gebruik van persoonsgegevens wordt vastgelegd met uitgevoerde handelingen (logging);
- er wordt gewerkt met geheimhoudingsverklaringen en contractuele afspraken bij het inschakelen van externen en leveranciers.

Met een gegevensbeschermingseffect beoordeling of Data Privacy Impact assessment (DPIA) worden de effecten en risico’s van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De organisatie voert deze in ieder geval uit wanneer er sprake is van een geautomatiseerde verwerking waarop een besluit wordt gebaseerd, een grootschalige verwerking, een verwerking van bijzondere persoonsgegevens plaats gaat vinden, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën

worden gebruikt. Er zijn in de afgelopen jaren beperkt DPIA's uitgevoerd. We maken inmiddels gebruik van de DPIA tool van de IBD (IRPA-tool). In deze tool kunnen we ook DPIA's die door andere gemeenten zijn uitgevoerd als basis gebruiken (ongoing proces).

Er zullen in de komende jaren regelmatig DPIA's moeten worden uitgevoerd. De procesverantwoordelijke zullen hierin geassisteerd moeten worden vanuit het privacy team.

Verwerkingsverantwoordelijke
In de AVG is sterk de nadruk gelegd op de verantwoordelijkheid van organisaties en instanties, aangeduid als verwerkingsverantwoordelijke. Binnen de gemeentelijke organisatie kan dat alleen een bestuursorgaan zijn. Dat zijn onder andere de Burgemeester, het college van B&W, de Gemeenteraad, of de commissie Bezwaar en Beroep. Een deel van de taken zijn gedelegeerd of gemandateerd door de gemeenten aan Meerinzicht. In het geval van delegatie wordt Meerinzicht verwerkersverantwoordelijke en in geval van mandaat zijn Meerinzicht en de gemeenten gezamenlijk verwerkersverantwoordelijke, of is Meerinzicht verwerker en de gemeenten verwerkersverantwoordelijke.

De verwerkingsverantwoordelijke moet kunnen waarborgen dat er sprake is van passende bescherming bij de verwerking van persoonsgegevens en dat ook kunnen aantonen. Tegelijk is het zo dat uiteindelijk alle medewerkers van de gehele organisatie medeverantwoordelijk zijn voor de zorgvuldige omgang met persoonsgegevens.

Doel privacy beleid?

Doel van dit privacy beleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacy rechten van personen waarvan de gemeente Ermelo, Harderwijk, Zeewolde en de gemeenschappelijke regeling Meerinzicht persoonsgegevens verwerkt. Het privacy beleid is ook een uitwerking van de Wet politiegegevens (Wpg). In het geval van de Wpg kunnen de rechten van betrokkenen beperkter zijn.

Dit beleid is van toepassing op de gehele gemeentelijke organisatie en daarmee alle bestuursorganen. Het is primair gericht aan alle medewerkers die in het kader van hun taak persoonsgegevens verwerken. Het beleid betreft een overkoepelend kader waarin de maatregelen tot bescherming van persoonsgegevens op algemene wijze zijn uitgewerkt. In werkplannen, procedures en werkinstructies wordt inhoudelijk uitgewerkt hoe uitvoering wordt gegeven aan de bescherming van persoonsgegevens. De invulling hiervan wordt in de jaarplannen van het Privacy Team beschreven.

Evaluatie privacy beleid
Dit privacy beleid geldt voor de duur van vier jaar (2022-2026) en wordt op doeltreffendheid tweejaarlijks geëvalueerd. Dat zal zijn eind 2024 en eind 2026.

Proceseigenaren doen periodiek verslag over de naleving van dit beleid, waaronder oplossingen en incidenten die zich hebben voorgedaan.

Het college van B&W legt over de privacy beleidsvoering (politieke) verantwoording af aan de raad en is transparant over de verwerkingen van persoonsgegevens naar betrokkenen. De directie van Meerinzicht legt verantwoording af aan het Bestuur van Meerinzicht voor gedelegeerde taken en is transparant over de verwerkingen van persoonsgegevens naar betrokkenen.

De gemeenten en Meerinzicht dragen zorg voor de documentatie van beleid en maatregelen, zodat het op ieder moment uitleg kan geven over de deugdelijkheid van de aanpak (aantoonbaarheid).

De Functionaris Gegevensbescherming (FG) brengt jaarlijks verslag uit aan de colleges en het bestuur van Meerinzicht en geeft aanbevelingen die strekken tot verdere optimalisering van de privacy beleidsvoering. De colleges en het bestuur besluiten over bijsturen van dit beleid met inachtneming van de aanbevelingen van de FG.

Procedures en formats
In onderliggende beleidsnotities dan wel reglementen is de bescherming van persoonsgegevens uitgewerkt die betrekking hebben op verwerkingen van medewerkers, bestuur en Raad. Daarnaast geldt dit ook voor verwerkingen waar sprake is van bijzondere of gevoelige persoonsgegevens. Bijvoorbeeld voor cameratoezicht, of de Persoonsgerichte aanpak.

Samenhang privacy beleid met informatiebeveiligingsbeleid
Bescherming van persoonsgegevens kan niet zonder informatiebeveiliging. Gegevensbescherming gaat over behoorlijk bestuur in het digitale tijdperk en is met name gericht op de bescherming van personen.
Informatiebeveiliging is een onderdeel van gegevensbescherming en is specifiek gericht op de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de gemeentelijke informatievoorzieningen. In het informatiebeveiligingsbeleid is opgenomen hoe de omgang met de drie BIV-principes is.

Gemeentelijke organisatie

Het Privacy beleid van de gemeentelijke organisatie wordt opgesteld door het college van Burgemeesters en Wethouders (hierna: het college) en gecontroleerd door de gemeenteraad. Binnen Meerinzicht wordt het Privacy beleid opgesteld door de directieraad en gecontroleerd door het Bestuur.

Gemeenteraad/Bestuur
De gemeenteraad/bestuur ziet er op toe dat het college overkoepelend beleid ten aanzien van bescherming van persoonsgegevens voor de organisatie vaststelt. Door de gemeenteraad/bestuur worden voor de uitvoering hiervan de benodigde middelen beschikbaar gesteld. Voorts controleert zij de colleges bij de uitvoering van deze kaders. Zij wordt hiertoe in staat gesteld door de verantwoordingsinformatie. Dit is onder meer het jaarlijkse verslag van de Functionaris Gegevensbescherming (FG), die de colleges/directieraad verschaft.

Colleges van B&W/ directieraad
De colleges/directieraad is integraal verantwoordelijk voor zorgvuldigheid van verwerking van persoonsgegevens. Zij is het meest aangewezen bestuursorgaan die de passende bescherming van persoonsgegevens waarborgt. Zo is zij verantwoordelijk voor een duidelijk te volgen privacy beleid, doet aan de gemeenteraad/bestuur voorstellen over in te zetten middelen en stelt specifieke regelingen en procedures vast. Daarnaast controleert zij het management van de organisatieonderdelen op de maatregelen die verband houden met de bescherming van persoonsgegevens.

Het college heeft een portefeuillehouder aangewezen die namens het college de beleidsvoering waarborgt. Daarnaast legt deze (politieke) verantwoording af over de privacy beleidsvoering aan de Raad. De directieraad heeft eveneens een portefeuillehouder aangewezen die namens de directieraad de beleidsvoering waarborgt. En deze legt verantwoording af over de beleidsvoering aan het Bestuur.

Aansturing: Gemeentesecretaris/Directie
De uitvoeringsverantwoordelijkheid voor gegevensbescherming ligt bij de gemeentesecretaris. De gemeentesecretaris is de hoogste ambtenaar binnen de ambtelijke organisatie en de eerste adviseur van het college. Hij of zij vormt dus de schakel tussen het bestuur en ambtelijke organisatie en is in dit kader ambtelijk verantwoordelijk. Binnen Meerinzicht is de directeur Bedrijfsvoering de eerst verantwoordelijke voor de uitvoering van het privacy beleid. Hij is de schakel met de directieraad.

De Gemeentesecretaris en de directeur zijn samen met hun respectievelijke directeuren/managers verantwoordelijk voor de uitvoering van het meerjarenplan, een juiste uitvoering van privacy beleid en sturen op (concern) risico's. Daarnaast zorgen zij voor een passend niveau van informatieveiligheid en gegevensbescherming binnen de organisatie.

Uitvoering: Proceseigenaren
De zorgvuldige omgang van verwerkingen vallen onder de proceseigenaar binnen de verschillende vak-afdelingen. Dat betekent dat zij zelf moeten zorgdragen over het nakomen van de naleving van het privacy beleid binnen hun organisatieonderdeel (bijvoorbeeld burgerzaken, belastingen). Ook zijn zij verantwoordelijk voor voldoende bewustwording. Regelmatig worden centraal bewustzijnscampagnes georganiseerd. Proceseigenaren worden in hun taken ondersteund door de Privacy Officers.

De proceseigenaar stuurt onder meer op:

- risico gestuurd werken. Hiervoor wordt gebruik gemaakt van de vastgestelde modellen van de DPIA-light en /of de 'schaal van erg' en/of Data Protection Impact Assessments (DPIA's).
- naleving van principes van privacy by design & default;
- het hanteren van daartoe vastgestelde procesplannen en formats, zoals de DPIA (IRPA-tool) en de (door de VNG vastgestelde) verwerkersovereenkomst;
- dat datalekken volgens de daartoe te volgen procedure zo snel mogelijk bij het Privacy team worden gemeld;

- het opnemen van nieuwe verwerkingen en gewijzigde verwerkingen in het register van verwerkingsactiviteiten (in afstemming met het Privacy team);
- het informeren en het afhandelen van de rechten van de betrokkene (uitvoering door het Privacy team);
- het maken van schriftelijke afspraken bij risicovolle verwerkingen en verwerkingen bij ketensamenwerking (verwerkingen in een samenwerkingsverband);
- het bijstaan van de uitvoering door professionals op het gebied van privacy en informatieveiligheid waar nodig;
- het bekend maken van dit beleid bij haar medewerkers.

Medewerkers
Alle medewerkers (inclusief inhuur/externen) zijn ervoor verantwoordelijk dat zorgvuldig wordt omgegaan met verwerking van persoonsgegevens. Dat betekent dat iedereen, binnen de kaders van zijn taak, zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Indien er twijfel bestaat of aan deze beginselen uitvoering wordt gegeven, schakelt men de lijnmanager en/of het Privacy team in.

Ondersteuning en advies

Om de uitvoering te helpen bij vraagstukken omtrent de bescherming van persoonsgegevens en de directie te ondersteunen bij de uitvoering van het privacy beleid, zijn de volgende professionals belast.

Privacy & Informatieveiligheid kernteam
De organisatie wordt waar nodig ondersteund door het Privacy & Informatieveiligheid kernteam. Dit team bestaat uit een vast team van professionals, waaronder business controllers en concern controllers, Privacy Officers, CISO en FG. Deze professionals spelen een belangrijke rol in de beleidsvorming en prioriteitstelling voor de uitvoering van het beleid.

Privacy Officer (PO)
De PO heeft, naast een strategische en tactische rol, ook een operationele rol als dagelijkse aanspreekpunt voor medewerkers wat betreft gegevensbescherming en privacy vraagstukken. De volgende taken worden uitgevoerd:

- De PO adviseert over de procedures en werkprocessen van afdelingen voor wat privacy vraagstukken betreft. De PO wordt daarom in een vroeg stadium van planvorming betrokken.
- In geval er derden worden ingeschakeld adviseert de PO over de noodzaak en de inhoud van verwerkersovereenkomsten en eventuele andere afspraken die met een derde gemaakt moeten worden in het kader van privacy.
- De PO beheert het verwerkingsregister. Voor de inhoud van verwerkingen zijn de afdelingsmanagers, of procesverantwoordelijke verantwoordelijk. De PO adviseert hierbij.
- De PO coördineert het proces rondom datalekken.
- De PO doet de afhandeling, waaronder besluitvorming, van verzoeken inzake rechten van betrokkenen. De organisatie levert hiervoor de benodigde informatie, zodat de PO tijdig een gefundeerde beslissing kan nemen met betrekking tot het verzoek.
- De PO adviseert en ondersteunt bij het in kaart brengen van privacy risico's in DPIA's, inclusief de eventuele voorafgaande raadpleging van de AP.
- De PO adviseert en ondersteunt in aspecten rondom data gedreven werken / digitale overheid voor zover hierin persoonsgegevens worden verwerkt.
- De PO draagt bij aan de bewustwording van de organisatie met betrekking tot de verantwoordelijkheden voortvloeiend uit de AVG. Dit kan door middel van presentaties, of informatie op Hi5, maar ook door het opstellen van protocollen, jaarplannen of beleidsstukken.

Chief Information Security Officer (CISO)
In het kader van de privacy heeft de CISO een rol in ondersteuning en advies. Op het gebied van informatiebeveiliging heeft hij een onafhankelijke, controlerende en toezichthoudende rol. Informatiebeveiliging maakt een wezenlijk onderdeel uit van de bescherming van persoonsgegevens. Hij adviseert voornamelijk bij projecten en het beheersen van risico's.

I-Adviseur
De I-Adviseur is de kenner op het gebied van de gemeentelijke producten, informatiestromen, processen en informatiesystemen. Hij adviseert op vraagstukken die betrekking hebben op de bescherming van persoonsgegevens en kan ondersteunen bij de opzet van autorisaties.

Applicatiebeheerder
De applicatiebeheerder is verantwoordelijk voor de inrichting en het onderhoud van applicaties. Deze rol kan op basis van vastgelegde functies, taken en verantwoordelijkheden van gebruikers van de applicatie de juiste autorisaties inregelen en controleren.

Toezicht en controle

Om het beleid binnen de gemeentelijke organisatie te borgen, is het van belang dat hier toezicht en controle op plaatsvindt. Dit is als volgt geregeld.

Functionaris Gegevensbescherming
De Functionaris voor Gegevensbescherming (FG) is de onafhankelijke toezichthouder op de naleving van de AVG, gerelateerde wetgeving en het gemeentelijke beleid op het gebied van gegevensbescherming conform artikel 37-39 AVG. De FG:

- informeert en adviseert onze organisatie over de werking van de AVG, overige wetgeving en ons beleid;
- houdt toezicht op de nakoming van het privacy beleid en achterliggende wettelijke verplichtingen;
- helpt privacy-klachten tot een goed einde te brengen (ombudsfunctie);
- adviseert bij privacy-incidenten over ernst en omvang;
- ziet toe op het beheer van het register van verwerkingen conform artikel 30 AVG;
- controleert de naleving van afspraken door onszelf en ketenpartners, eventueel ook in samenwerking met auditors;
- helpt het privacy beleid uit te dragen en bewustzijn te creëren bij interne en externe doelgroepen;
- is het contactpunt voor landelijke toezichthouders – met name de AP.

De FG krijgt ruimte voor professionele uitvoering van taken. Dat betekent dat de FG:
- naar behoren en tijdig wordt betrokken bij aangelegenheden die betrekking hebben op de verwerking van persoonsgegevens.
- volledig wordt geïnformeerd over aspecten van onze bedrijfsvoering waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.

Het college, directie en proceseigenaren ondersteunen de FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.

De FG wordt niet geïnstrueerd over invulling van taken, onder druk gezet, gestraft, ontslagen of beperkt in de middelen die hij nodig heeft voor de uitvoering van zijn taak. De zienswijze van de FG is zwaarwegend en geldt als de geëigende wijze voor naleving van de AVG.

Minimaal één keer per jaar brengt de FG verslag uit over de stand van zaken aan het college/directie.

Verhouding tot en verantwoording aan de Raad/Bestuur
De gemeenteraad/bestuur controleert vervolgens het college/directie door middel van de verantwoordingsrapportages. Jaarlijks legt het college/directie verantwoording af aan de gemeenteraad/bestuur over de realisatie en de toepassing van het privacy beleid en het informatieveiligheid beleid.

In de verantwoording in de jaarstukken komen in elk geval de volgende onderwerpen aan de orde:

- realisatie en uitvoering privacy beleid en integratie wettelijke eisen AVG in de werkprocessen;
- inventarisatie en implementatie per afdeling van de risico-inventarisatie (afgenomen DPIA's),
- stand van zaken met betrekking tot het verwerkingsregister, conform artikel 30 AVG;
- activiteiten die hebben plaatsgevonden op bewustwording en training;
- aard, omvang en afhandeling van eventuele klachten van de betrokkene;
- aard, omvang en afhandeling van (vermoedelijke) datalekken.