

Jaarverslag 2025

Gegevensbescherming

Gemeente Meierijstad



Functionaris Gegevensbescherming
Gemeente Meierijstad
Datum: Februari-2026
fg@meierijstad.nl



Inhoud

Inhoud	1
Inleiding	2
Leeswijzer jaarverslag	2
1. Deel 1. AVG (terugblik op 2025)	3
Bevindingen en aanbevelingen	3
1.1. Beleid	3
1.2. Routekaart AVG	3
1.3. Regie op risico's	3
1.4. Rollen en verantwoordelijkheden	4
1.5. Bewustzijn	5
1.6. Technologie en innovatie (AI)	5
2. Deel 2. WPG	6
Bevindingen en aanbevelingen	6
2.1. Inleiding	6
2.2. Reikwijdte	6
2.3. Governance	6
2.4. Audits	6
2.5. Maatregelen/knelpunten	7
2.6. FG toezicht	7
3. Werkzaamheden FG	8
Instrumenten	8
3.1. Verwerkingsregister	8
3.2. Data Protection Impact Assessment (DPIA)	8
3.3. Datalekken	8
3.4. Rechten van betrokkenen	9
3.5. Klachten, vragen en signalen	9
3.6. Middelen Functionaris Gegevensbescherming	9
4. Vooruitblik	10
5. Bijlage 1. FG toezicht activiteiten 2026	11
Overige werkzaamheden/rapportages/voorstellen/adviezen	14

Inleiding

De gemeente Meierijstad vindt het belangrijk om in deze digitale tijd goed om te gaan met persoonsgegevens. Hierbij staan de privacy en het vertrouwen van onze inwoners voorop. Het beschermen van deze gegevens zien wij als een verantwoordelijkheid die logisch is, en niet alleen omdat de wet het verplicht stelt. Het recht op privacy is vastgelegd in de Grondwet en het Europees Verdrag voor de Rechten van de Mens (EVRM). De Algemene Verordening Gegevensbescherming (AVG) is de belangrijkste wet die gaat over de bescherming van persoonsgegevens.

De AVG bevat regels waaraan de gemeente zich moet houden bij het verwerken van persoonsgegevens. De gemeente Meierijstad verwerkt veel gegevens in haar rol als bestuursorgaan én als werkgever. Hierbij gaat het om gegevens van inwoners, ondernemers, samenwerkingspartners en medewerkers. Zij moeten erop kunnen vertrouwen dat de gemeente Meierijstad zorgvuldig omgaat met hun persoonsgegevens.

Het verwerken van persoonsgegevens vindt plaats onder de verantwoordelijkheid van zowel het college van B&W, de burgemeester als de gemeenteraad. In de AVG en de Wet Politiegegevens (Wpg) wordt het wettelijk kader beschreven voor het verwerken van (strafrechtelijke) persoonsgegevens.

Sinds de invoering van de AVG en de Wpg is de functionaris gegevensbescherming (FG) voor gemeenten de interne onafhankelijke toezichthouder voor verwerkingen van persoonsgegevens. De FG adviseert en controleert de gemeente en brengt jaarlijks een verslag uit.

Het doel van het jaarverslag is om, als onafhankelijk toezichthouder, de hoogst leidinggevende van de organisatie rechtstreeks te informeren over privacy (bescherming van persoonsgegevens) en gegevensbescherming binnen de gemeente Meierijstad. Dit volgt ook uit de AVG (artikel 38 lid 3) en de Wpg (artikel 34 lid 3).

De FG geeft in dit jaarverslag inzicht in de uitgevoerde werkzaamheden, de instrumenten voor toezicht en advisering, interne en externe ontwikkelingen op het gebied van de AVG en Wpg en de positionering van de FG. Daarnaast deelt de FG zijn bevindingen over het afgelopen jaar en doet, indien nodig, aanbevelingen voor het komende jaar.

Leeswijzer jaarverslag

Hoofdstuk 1 geeft de bevindingen en aanbevelingen met betrekking tot de AVG weer. Hoofdstuk 2 geeft de bevindingen en aanbevelingen met betrekking tot de Wpg weer. In hoofdstuk 3 worden de werkzaamheden van de FG beschreven, gevolgd door de instrumenten die de FG gebruikt om invulling aan de advies- en toezichtrol te kunnen geven. Het jaarverslag wordt afgesloten met een korte vooruitblik waarin ook een opzet voor een toezichtjaarplan voor het jaar 2026 van de FG wordt gepresenteerd.

1. Deel 1. AVG (terugblik op 2025)

Bevindingen en aanbevelingen

In dit deel van de rapportage kijkt de functionaris gegevensbescherming terug op wat de gemeente Meierijstad in 2025 heeft bereikt, welke werkzaamheden zijn uitgevoerd en bevindingen zijn gedaan door de functionaris gegevensbescherming.

1.1. Beleid

In 2025 is het bestaand beleid herzien en is er een nieuw strategisch beleid Informatieveiligheid, Privacy en AI op- en vastgesteld. Het beleid biedt de organisatie de strategische kaders en een kapstok om met aandacht voor naleving de onderwerpen informatiebeveiliging, privacy en AI verder vorm te geven.

De FG is actief betrokken geweest bij het nieuwe strategisch beleid en heeft vanuit zijn rol advies gegeven.

In het verlengde van het strategische beleid zullen in 2026 de tactische privacy beleidsstukken ook herzien en, indien nodig, geactualiseerd moeten worden.

1.2. Routekaart AVG

In het afgelopen jaar heeft de directie, in afstemming met het bestuur, de ambities van de organisatie op het gebied van privacy vastgesteld. Dit betekent dat de gemeente Meierijstad in de komende jaren aan de slag moet gaan om dit niveau te bereiken. Om het huidige volwassenheidsniveau in kaart te brengen is er een nulmeting uitgevoerd. Daaruit is naar boven gekomen dat het huidige volwassenheidsniveau op 2 zit. De inhoudelijke resultaten van de nulmeting worden met het directieteam gedeeld, samen met een routekaart en tijdspad om het ambitieniveau te bereiken.

De routekaart en tijdspad zijn eind 2025 nog niet door de FG ingezien. Een belangrijke kanttekening bij deze routekaart is dat de focus niet moet liggen op het voldoen aan (zetten van vinkjes) de wet- en regelgeving (AVG) en normenkaders (CIP-overheid), maar voornamelijk op het aanpakken van de kritische privacyrisico's die er zijn. Als kader en hulpmiddel kunnen de AVG en normenkaders worden gebruikt. De aanpak moet in lijn met de informatiebeveiligingsaanpak risicogebaseerd zijn. Zo werkt de gemeente stap voor stap toe naar meer grip op privacy en naar werken met een Privacy Management Systeem. Dit helpt de gemeente privacy goed te borgen in haar beleid en processen.

1.3. Regie op risico's

Regie op risico's (risicomanagement) is randvoorwaardelijk voor een goede gegevensbescherming binnen de gemeente. Het uitvoeren van de volwassenheidsmeting is hierbij een mooie eerste stap. Daarnaast zal er een PDCA-cyclus ingericht worden om structureel risico's in kaart te brengen, deze aan te pakken en te zorgen dat zaken continu verbeterd worden.

Het IV&P team wordt binnen de gemeente steeds beter gevonden en bij nieuwe plannen en ontwikkelingen aan de voorkant betrokken. De FG merkt wel op dat er op dit gebied nog steeds stappen gezet moeten worden. De toepassing en naleving van de gegevensbeschermingsregels op risicovolle processen gebeurt op

dit moment voor een groot gedeelte nog op basis van incidenten (reactief) en niet proactief en preventief. Uitzondering hierop is het stukje techniek (I&A en AI), daarbij is IV&P al aan de voorkant betrokken en wordt security en privacy by design meegenomen. Aan de hand van dataclassificatie en een analyse van incidenten van het afgelopen jaar, is het mogelijk om deze risicovolle processen in kaart te brengen en er proactief mee aan de slag te gaan.

Uit landelijke ontwikkelingen en voorbeelden blijkt dat veel incidenten direct of indirect impact hebben op persoonsgegevens. Denk aan phishing, datalekken en verstoringen van systemen waarin gevoelige gegevens worden verwerkt. Dit benadrukt dat privacy en informatiebeveiliging onlosmakelijk met elkaar verbonden zijn. Een belangrijke les hierbij is dat privacyrisico's zelden beperkt blijven tot alleen de partij waar het incident plaatsvindt. Voor Meierijstad is dit niet anders. De gemeente werkt in allerlei ketens met leveranciers, samenwerkingspartners en landelijke voorzieningen. Juist in die samenwerkingen ontstaan risico's rondom gegevensdeling, verantwoordelijkheden en toezicht. Samenwerking en het tijdig delen van signalen binnen deze ketens zijn essentieel om datalekken te voorkomen of de impact snel te beperken.

Globaal gezien heeft gemeente Meierijstad de volgende kritische processen en ketens:

- Uitvoeringsprocessen binnen het sociaal domein inclusief alle samenwerkingen met derde partijen (stichtingen, hulporganisaties, etc).*
- Uitvoeringsprocessen binnen zorg en veiligheid.*
- Uitvoeringsprocessen binnen het veiligheidsdomein, ondermijning en openbare orde en veiligheid.*
- Uitvoeringsprocessen met betrekking tot Burgerzaken (BRP).*

Daarnaast heeft de Autoriteit Persoonsgegevens recent onderzoek¹ gedaan naar misbruik van persoonsgegevens door eigen medewerkers. Dit blijft een actueel risico en gemeente Meierijstad heeft hier in het verleden ook mee te maken gehad. Gezien de omvang van de organisatie, de grote hoeveelheid (gevoelige) persoonsgegevens, de koppelingen met landelijke voorzieningen, de bewaartermijn van gegevens², de inrichting en autorisaties van systemen is dit iets wat blijvend aandacht nodig heeft. Dit vraagt om balans tussen de inrichting van systemen en applicaties enerzijds en controle op het gebruik hiervan anderzijds. Het verdient aanbeveling om hier komend jaar op bestuurlijk en directieniveau richtinggevende keuzes in te maken. Een positief voorbeeld hiervan binnen de gemeente is het project Gegevensverstrekking BRP. Binnen dit project wordt er actief gekeken naar de huidige autorisaties en het beperken daarvan, het verstrekken en bewaren van BRP gegevens en het toepassen van controle mechanismes zodat eventuele misbruik proactief gemonitord kan worden.

1.4. Rollen en verantwoordelijkheden

Heldere rollen en duidelijk belegde verantwoordelijkheden zijn voorwaarden om goed samen te werken. Ook met betrekking tot rollen en verantwoordelijkheden heeft de FG in het verleden signalen afgegeven. Binnen de organisatie zijn de rollen en verantwoordelijkheden in het afgelopen jaar helder in het beleid vastgelegd. Op de wijze waarop aan deze verantwoordelijkheden invulling wordt gegeven, liggen voor de gemeente nog mogelijkheden om verder te ontwikkelen.

De FG heeft in het jaarverslag over 2024 al aangegeven dat naar aanleiding van het programma 'organisatieontwikkeling' het aantal leidinggevendenden binnen de gemeente Meierijstad de afgelopen twee jaar

¹ <https://www.autoriteitpersoonsgegevens.nl/actueel/ap-datalekken-door-misbruik-persoonsgegevens-bij-gemeenten-blijven-vaak-onder-de-radar>

² <https://nos.nl/artikel/2602804-odido-overschrijdt-eigen-termijn-bewaren-gegevens>

sterk is toegenomen. De leidinggevendenden vullen, als management, een cruciale rol in om gezamenlijk te werken aan een veilige en privacybewuste organisatie. Intern zijn hiervoor ook al stappen gezet. In samenspraak met het DT wordt gefaseerd het three-lines-model ingevoerd en dit is reeds concreet gemaakt bij de afhandeling van datalekken, rechten van betrokkenen verzoeken en bij het herzien van het verwerkingsregister.

1.5. Bewustzijn

Een andere belangrijke randvoorwaarde voor verantwoord omgaan met persoonsgegevens is het privacy- en informatiebeveiligingsbewustzijn binnen de organisatie. Medewerkers dienen zich bewust te zijn van de verantwoordelijkheid die zij dragen en voldoende kennis te hebben om de juiste keuzes te maken. Een bepaalde mate van kennis is vereist en afhankelijk van functie en taken en verantwoordelijkheden kan aanvullende kennis nodig zijn.

Binnen de gemeente werden in 2025 bewustwordingsacties georganiseerd en/of gegeven in de dagelijks praktijk aan de hand van actuele casussen, vragen, datalekken en overige meldingen. Bij indiensttreding volgen medewerkers een e-learning over privacy en informatiebeveiliging, op afronding wordt echter nog onvoldoende gestuurd, waardoor dit een (te) vrijblijvend karakter heeft. De AVG-geletterdheid blijft daarmee achter in vergelijking met de AI-geletterdheid zoals deze proactief en als randvoorwaarde is uitgerold bij de introductie van GAIMS binnen de organisatie. Naast bewustwordingscampagnes zal het kennisniveau ook op peil gehouden moeten worden door bijvoorbeeld aanvullende e-learning modules, specifieke privacytrainingen (sociaal domein, veiligheid, boa's, burgerzaken, etc) afgestemd op functie en verantwoordelijkheden. Het advies is om deze elementen concreet mee te nemen in het IV&P opleidingsplan dat in 2026 doorgevoerd gaat worden.

1.6. Technologie en innovatie (AI)

In een tijdperk waarin digitalisering en technologische ontwikkelingen steeds sneller gaan, staat onze gemeente voor de uitdaging om kunstmatige intelligentie (AI) op een verantwoorde en effectieve wijze in te zetten. AI biedt ongekennde mogelijkheden om onze dienstverlening te verbeteren, werkprocessen te optimaliseren en maatschappelijke uitdagingen aan te pakken. Van het efficiënter afhandelen van vergunningaanvragen tot het voorspellen van onderhoudsbehoefte in de openbare ruimte.

Bovenstaand stukje tekst komt uit de intro van het A.I. beleid gemeente Meierijstad dat in 2025 is vastgesteld door het college. Dit beleid verwoordt de visie van Meierijstad als het gaat om de inzet en toepassing van AI. En schetst de kaders waarbinnen we AI gebruiken en ontwikkelen. Dit beleid is van toepassing op alle gemeentelijke taken en processen, ook wanneer deze door externe partijen worden uitgevoerd.

De FG onderstreept het belang en noodzaak van technologie en innovatie (AI) en het A.I. beleid geeft duidelijke kaders, uitgangspunten en richtlijnen om dit op een verantwoorde manier in te zetten. Tegelijkertijd zit de wereld om ons heen ook niet stil en wordt AI door eigen medewerkers, externe partijen en leveranciers in producten, diensten en applicaties gebruikt, als standaard ingebouwd en beschikbaar gesteld. Hoe houden wij als organisatie hier grip op? En hoe zorgen wij ervoor dat het bewustzijn (AI geletterdheid) blijvend op peil wordt gehouden? En hoe gaan wij als organisatie om met de ethische vraagstukken en risico's die indirect en direct ontstaan door het gebruik van AI? Blijven wij zelf nog wel nadenken of vertrouwen wij straks volledig op AI? Grip op leveranciers zou vanuit inkoop en leveranciersmanagement proactief opgepakt moeten worden. Voor de ethische vraagstukken zullen er middelen (tijd en capaciteit) beschikbaar gesteld moeten worden, zodat hier intern actief aandacht aan besteed kan worden en dit niet door medewerkers 'erbij' wordt gedaan.

Binnen de gemeente wordt dit tot nu toe proactief en risicogebaseerd opgepakt. Er is beleid, er worden AI-geletterdheidstrainingen gegeven en er is een gecoördineerd team waar IV&P onderdeel van uitmaakt. Waarbij sprake is van een open dialoog tussen dit team, de directie en het bestuur over de technologische ontwikkelingen. De gemeente heeft wat dat betreft een goed fundament staan, maar dit heeft blijvend aandacht nodig.

2. Deel 2. WPG

Bevindingen en aanbevelingen

2.1. Inleiding

De FG houdt toezicht op de naleving van de Wet politiegegevens (Wpg). Het college van B&W dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van politiegegevens. De FG rapporteert jaarlijks de bevindingen aan de hand van een jaarverslag. In dit jaarverslag staat beschreven welke acties en maatregelen in 2025 zijn genomen om de doelstellingen en beginselen uit de Wet politiegegevens (Wpg) te behalen en te waarborgen.

2.2. Reikwijdte

De Wpg is binnen de gemeente Meierijstad van toepassing op de Buitengewoon opsporingsambtenaren (Boa's) onderdeel van het team Vergunningen, Handhaving en Toezicht (VTH) die werkzaam zijn binnen domein 1 (Openbare ruimte). De sociale rechercheurs die als Boa's werkzaam zijn binnen domein 5 (Werk, Inkomen en Zorg) vallen niet direct onder de Wpg. Zij verwerken alleen politiegegevens (strafrechtelijke) als het gaat om zaken boven de 50.000 euro. In de afgelopen jaren heeft de gemeente Meierijstad dit soort zaken niet gehad en de verwachting is dat de gemeente dit soort zaken in de toekomst ook niet gaat krijgen.

2.3. Governance

Verwerkingsverantwoordelijke voor de Wpg is de werkgever, dat is de gemeente Meierijstad als publiekrechtelijk rechtspersoon, vertegenwoordigd door de secretaris als algemeen directeur en/of burgemeester. Als proceseigenaar is de leidinggevende van het team VTH verantwoordelijk voor de werkzaamheden van de Boa's.

2.4. Audits

In 2019 is door middel van het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpgboa) de Wpg van toepassing verklaard voor buitengewoon opsporingsambtenaren (boa's). Op grond van deze wet is gemeente Meierijstad als verwerkingsverantwoordelijke verplicht om periodiek privacy audits te laten uitvoeren. Dit betreft jaarlijks een interne audit en eens in de vier jaar een externe audit.

In 2025 heeft de externe audit over de jaren 2021 tot en met 2024 plaatsgevonden. Deze externe audit is recent (eind februari 2026) afgerond. Uit de externe audit blijkt dat de gemeente in de afgelopen jaren goede stappen vooruit zijn gezet, maar nog niet volledig voldoet aan de wettelijke eisen van de Wpg. Zoals ook al aangegeven in het vorige jaarverslag zijn in deze externe audit de resultaten uit 2025 nog niet zichtbaar. Deze zullen meegenomen worden in de hercontrole die binnen één jaar na afronding externe audit uitgevoerd moet

worden. Daarnaast dient er binnen 3 maanden een verbeterplan te worden opgesteld waarin de maatregelen worden beschreven en gepland om te gaan voldoen aan de geconstateerde tekortkomingen. De hercontrole op de effectiviteit van de verbetermaatregelen mag door de interne auditor van de gemeente worden uitgevoerd. De resultaten uit de externe audit zijn in lijn met de interne audits die jaarlijks worden uitgevoerd.

2.5. Maatregelen/knelpunten

In 2025 is voortgebouwd op de eerder uitgevoerde interne audits en het opgesteld verbeterplan. Er zijn aantal verbeteracties uitgevoerd. Zo is er een handboek Wpg opgesteld, is de vakapplicatie conform Wpg verplichtingen ingericht, is het register van verwerkingen geactualiseerd, worden er iedere kwartaal controles uitgevoerd en wordt er ieder jaar de interne audit uitgevoerd. Daarnaast voert de FG jaarlijks toezicht uit op de uitvoering, controles en audits.

Tegelijkertijd moeten er ook nog een heel aantal verbeteracties worden opgepakt. Dit komt ook terug in de resultaten van de uitgevoerde interne en externe audits. De belangrijkste verbeterpunten, vanuit risico oogpunt bekeken, zitten in het aanscherpen van de controles op doelbinding, noodzakelijkheid en rechtmatigheid, uitvoeren van een risicoanalyse (DPIA) op het feitelijke werkproces, het opstellen van een autorisatiematrix en de controle op toegang en logging, de opslag van gegevens op andere locaties (e-mail, whatsapp, etc) dan de vakapplicatie en de documentatieplicht met betrekking tot doorgifte van politiegegevens.

De FG beveelt aan om deze verbeterpunten ook vanuit risicoperspectief op te pakken. In de externe audit worden ook organisatorische en technische verbetermaatregelen benoemd die niet direct zorgen voor een veiligere verwerking van politiegegevens. De gemeente kan hierin risico gebaseerde keuzes maken. Door bijvoorbeeld de her-audit binnen 6 maanden uit te voeren, hoeft alleen 'opzet' en 'bestaan' te worden getoetst. Voor het implementeren en aantonen van de 'werking' heeft de gemeente dan nog 3 jaar de tijd. Daarnaast vraagt de beperkte capaciteit binnen het Boa team aandacht. De FG adviseert dan ook blijvend te investeren in de kennis van medewerkers en in de standaardisatie van processen rondom de Wpg. Dit zorgt voor een stabiele basis en duurzaam beheer van politiegegevens.

2.6. FG toezicht

De NOREA, de vereniging van geregistreerde auditoren in Nederland, heeft in de handleiding voor de Wpg audits de FG opgenomen als een uitvoerende derde lijn in het "three-lines-model". Er zijn concrete taken als 'steekproefsgewijs controleren van de autorisaties' toebedeeld aan de FG. De FG is daardoor ook op tactisch niveau uitvoerend betrokken bij de Wpg. De vraag is echter of dit wenselijk is gezien de huidige toezichtsfunctie die de FG heeft. De Plan-Do-Check-Act cyclus dient in de organisatie zelf geborgd te zijn en daarop dient er intern FG-toezicht plaats te vinden.

De FG geeft bij voorkeur advies op strategisch en beleidsmatig niveau, om op die manier de organisatie als geheel te kunnen ondersteunen en informeren. Aangezien DPIA's worden voorgelegd aan de FG ligt daar de mogelijkheid om ook op het niveau van een specifieke verwerking te kunnen adviseren en toezicht te houden.

3. Werkzaamheden FG

Instrumenten

De FG is onder andere belast met informeren, signaleren, (on)gevraagd adviseren en toezien op de naleving van gegevensbescherming. De taken van de FG zijn wettelijk vastgelegd in de AVG en Wpg. Voor de uitoefening van deze taken heeft de FG een aantal instrumenten die helpen in de signalering, advisering en toezicht. Instrumenten die de FG helpen zijn onder andere; het register van verwerkingen, DPIA's, datalekken, vragen, klachten, signalen en beleid. Ook onderzoeken, adviesrapporten en artikelen vanuit de VNG, Informatiebeveiligingsdienst van de VNG, de Autoriteit Persoonsgegevens en/of landelijke en regionale media die in 2025 of de jaren daarvoor zijn gepubliceerd hebben een belangrijke bijdrage geleverd in het krijgen van inzicht over naleving van gegevensbescherming en hebben in sommige gevallen geleid tot het geven van advies of het signaleren van risico's. Door deze instrumenten krijgt de FG een beeld van de onderwerpen die spelen binnen de gemeente, bij burgers en medewerkers.

Hieronder gaat de FG in op de instrumenten, deelt zijn bevindingen en verkregen inzichten en benoemt de risico's.

3.1. Verwerkingsregister

In het verwerkingsregister staat informatie over de persoonsgegevens die de gemeente Meierijstad verwerkt. Alle overheidsorganisaties die persoonsgegevens verwerken zijn verplicht zo'n register op te stellen en bij te houden. Hiermee voldoet de gemeente onder andere aan haar informatieplicht. Het actief publiceren van het register is geen wettelijke plicht, maar de AP heeft het recht om het register op te vragen en in te zien.

Het huidige verwerkingsregister van de gemeente Meierijstad is jaren geleden opgesteld en sindsdien mondjesmaat geactualiseerd. De huidige versie van het register biedt te weinig inzicht in de bestaande processen en wordt met name vanuit het team IV&P incidenteel bijgehouden. De herziening van het verwerkingsregister staat op de planning voor 2026.

3.2. Data Protection Impact Assessment (DPIA)

In de AVG is de verplichting opgenomen voor organisaties om een privacy risicoanalyse (DPIA) uit te voeren bij bepaalde gegevensverwerkingen met een hoog risico en aan de FG voor te leggen voor advies. Het op tijd starten met een DPIA, een goed lopend DPIA-proces en een inhoudelijk goed uitgevoerde DPIA is belangrijk, omdat er inzichtelijk wordt gemaakt welk doel de verwerking dient, of er een juiste grondslag is en of er voldoende technische en organisatorische maatregelen worden genomen om de risico's te mitigeren, wie de verantwoordelijken zijn en binnen welke periode de verbetermaatregelen worden uitgevoerd.

In 2025 is er één DPIA afgerond en voorgelegd aan de FG ter advies. Daarnaast zijn er een aantal pré DPIA's uitgevoerd en zijn er nog een aantal DPIA's in uitvoering. Gezien de omvang van gemeente Meierijstad, het aantal kritische en risicovolle processen en de grote hoeveelheden gevoelige persoonsgegevens die verwerkt worden, zijn er in 2025 te weinig DPIA's uitgevoerd. Het instrument DPIA heeft daardoor beperkt bijgedragen aan de toezichtstaken van de FG.

3.3. Datalekken

In 2025 zijn er 43 incidenten gemeld die door de organisatie zijn aangemerkt als datalek. In 3 gevallen is geoordeeld dat het datalek meldenswaardig was en is een melding gemaakt bij de toezichthouder (AP). De

overige incidenten zijn als niet meldingswaardig aangemerkt en intern geregistreerd. Naar aanleiding van een datalek dienen passende maatregelen te worden getroffen. De FG wordt inhoudelijk geïnformeerd indien een datalek een grote impact heeft op de rechten en vrijheden van betrokkenen en er eventueel reputatieschade is voor de organisatie. In twijfelgevallen wordt advies gevraagd aan de FG.

Een datalek kan voor de FG aanleiding zijn om een onderzoek te doen of een signaal af te geven aan de organisatie, met het oog op het voorkomen van datalekken in de toekomst.

Er zijn in 2025 in verhouding tot de omvang van de organisatie weinig datalekken gemeld. Dit kan het gevolg zijn van onbekendheid en bewustzijn binnen de organisatie met betrekking tot wat wel en niet als datalek moet worden gemeld. Binnen gemeente Meierijstad moet hier continu bewustzijn voor worden gecreëerd. Het melden van een datalek/incident is geen fout, maar juist een leermoment voor de organisatie. Door datalekken te herkennen kan inzicht ontstaan in de risico's binnen de organisatie. Met dit inzicht kan de basis eerder op orde worden gebracht en kunnen incidenten en datalekken preventief voorkomen worden.

3.4. Rechten van betrokkenen

Het team IV&P coördineert verzoeken over de verwerking van persoonsgegevens op grond van de AVG en de Wpg. In 2025 zijn er in totaal 4 rechten van betrokkenen verzoeken ingediend. De 4 verzoeken zijn binnen de wettelijke termijn afgehandeld.

Het is voor betrokkenen nog niet mogelijk om via een DigiD e-formulier op de website verzoeken in te dienen. Betrokkenen kunnen schriftelijk (per mail of post) een verzoek indienen. Mogelijk zorgt dit voor een drempel bij het indienen van verzoeken. Een digitaal formulier is in concept beschikbaar en wordt begin 2026 op de website gepubliceerd.

3.5. Klachten, vragen en signalen

De contactgegevens van de FG zijn te vinden op de website van de gemeente Meierijstad. Dit is ook wettelijk verplicht. Dit betekent dat eenieder contact kan opnemen met de FG voor vragen en opmerkingen. In 2025 is er één klacht ingediend bij de FG die door het IV&P team is afgehandeld. Daarnaast zijn er een aantal vragen, meldingen en signalen bij de FG binnengekomen. Deze vragen zijn door de FG beantwoord en indien nodig doorgezet naar het IV&P team voor verdere afhandeling.

Betrokkenen kunnen ook klachten indienen bij de AP in het geval zij het niet eens zijn met de afhandeling van hun klachten door de organisatie. De AP behandelt klachten, maar doet ook op eigen initiatief onderzoek naar aanleiding van signalen. De AP hanteert de werkwijze om onderzoeken naar klachten en signalen via de FG binnen de organisatie uit te zetten. In 2025 heeft de FG hierover van de AP geen meldingen ontvangen.

Binnen de gemeente is er een algemene klachtenproces (beleidsregels intern klachtrecht college, burgemeester en organisatie gemeente Meierijstad 2020). In dat proces ontbreekt echter een specifieke paragraaf voor klachten met betrekking tot de verwerking van persoonsgegevens. Het advies is om de reikwijdte van het bestaande klachtenproces hierop aan te passen.

3.6. Middelen Functionaris Gegevensbescherming

In 2025 had de FG beperkte middelen om zijn functie volledig uit te voeren. De beperkte middelen zitten met name in de beperkte tijd (gemiddeld 4 uur per week) die de FG beschikbaar heeft voor het uitvoeren van zijn taken. Dit is intern aangekaart en de gemeente Meierijstad is bezig om in samenwerking met gemeente

Maashorst een FG aan te stellen. Deze FG zal voor maximaal 0,5fte aan de slag gaan bij gemeente Meierijstad.

4. Vooruitblik

De gemeente Meierijstad heeft al veel stappen gezet om persoonsgegevens en politiegegevens zorgvuldig te verwerken. Wat goed geregeld is in het primaire proces, draagt bij aan duurzame verbeteringen. Tegelijkertijd blijft het nodig om door te gaan met verbeteren. De FG kan als toezichthouder signaleren waar verbeteringen nodig zijn, maar de organisatie zelf is verantwoordelijk voor het oppakken en doorvoeren van deze verbeterpunten.

De FG heeft in het afgelopen jaar, mede door onder de werkzaamheden beschreven instrumenten en de uitgevoerde nulmeting, een beeld gekregen wat er zoal noodzakelijk is om te streven naar het in control zijn op de gegevensbeschermingsrisico's en te groeien naar volwassenheidsniveau 4. De FG constateert dat voor de realisatie daarvan, in ieder geval om de basis op orde te hebben (niveau 3), een aantal elementen noodzakelijk zijn zoals een integrale risicomanagementaanpak en de invulling van rollen en verantwoordelijkheden bij verwerking van persoonsgegevens binnen de verschillende ateliers en teams. En het in kaart brengen van alle formele en informele samenwerkingen die de gemeente heeft met diverse andere organisaties, stichtingen, samenwerkingsverbanden en andere samenwerkingsvormen.

De FG hanteert met de huidige middelen en capaciteit het principe 'toezicht op maat'. Door te kijken hoever de organisatie is in de toepassing en naleving van de AVG en de focus in toezicht te bepalen aan de hand van de gemelde en geconstateerde gegevensbeschermingsrisico's. Het advies om de doorontwikkeling voor de middellange termijn te concentreren op het proactief toepassing van gegevensbescherming in alle lagen van de organisatie.. Door dit proactief vanuit alle lagen in de organisatie op te pakken, wordt de interne en externe dienstverlening verbeterd, het vertrouwen van de burger in de gemeente vergroot en kan de organisatie risicobewust aan de slag met alle nieuwe (digitale) mogelijkheden en ontwikkelingen.

De FG zet het komende jaar de ingezette lijn vanuit het toezicht om de organisatie bewuster te maken met betrekking tot gegevensbeschermingsrisico's door. Wanneer de verbinding tussen de organisatieonderdelen die verantwoordelijk zijn voor risicomanagement, kwaliteit en control is gerealiseerd, de FG instrumenten volledig worden benut en de FG capaciteit is uitgebreid, zal de FG zich meer toespitsen op proactief toezicht. Onder proactief toezicht verstaat de FG vooraf stimulerend en richtinggevend toezicht. Daarvoor kan door de FG een toezichtjaarplan worden opgesteld. Zie bijlage voor een overzicht met FG toezicht activiteiten voor het jaar 2026.

5. Bijlage 1. FG toezicht activiteiten 2026

Actie	Toelichting	Uitvoerder	Planning
A. Controle geregistreerde datalekken/incidenten en de afhandeling daarvan aan de hand van het datalekregister.	De FG ziet op een juiste en tijdige afhandeling van datalekken/incidenten en de genomen (beheers)maatregelen om het risico te mitigeren en/of te voorkomen.	FG en PO's	4x per jaar
B. Behandeling van privacy gerelateerde klachten en overige 'rechten van betrokkenen'	De FG ziet toe op een juiste en tijdige afhandeling van privacy gerelateerde klachten van medewerkers en inwoners en ingediende " rechten van betrokkenen".	FG en PO's	Doorlopend
C. Advies	De FG geeft zowel gevraagd als ongevraagd advies aan de verwerkingsverantwoordelijke en treedt in overleg met de directie, het management alsmede met het bestuur. Er wordt actief meegedacht over actuele vraagstukken (denk bijvoorbeeld aan AI, digitale soevereiniteit en ontwikkelingen sociaal domein) over het gebruik van persoonsgegevens met als doel een behoorlijke en rechtmatige dienstverlening door de overheid te bevorderen. De FG bevordert (samen met het team informatiebeveiliging en privacy) dat processen/projecten/taken binnen de Gemeente Meierijstad in lijn zijn met de geldende privacy wet- en regelgeving. De FG beoordeelt onder meer of de inbreuk op het recht op bescherming van persoonsgegevens gerechtvaardigd is	Strategisch adviseur Gegevensbescherming en FG	Doorlopend

	en niet bovenmatig is gelet op het doel dat met de regelgeving wordt nagestreefd. De FG betreft daarbij de kennis en ervaring die hij opdoet in contact met het team IB&P, de strategisch adviseurs en andere FG's.		
D. FG als aanspreekpunt voor de AP	De FG functioneert als (eerste) aanspreekpunt voor de AP. Wanneer de AP contact heeft met een organisatie wordt de FG (direct of zo snel mogelijk erna) hiervan op de hoogte gesteld. De AP gaat ervan uit dat betrokkenen (burgers, klanten, medewerkers) die er met de organisatie niet uitkomen, zich eerst tot de FG wenden voordat zij zich bij de AP melden.	FG	Doorlopend
E. Controleren van de naleving	Om vast te stellen of aan de verantwoordingsplichten van de AVG is voldaan wordt aan de hand van geconstateerde risico's gericht onderzoek gedaan bij ateliers. Onderzoeken: – Controle op naleving aanbevelingen DPIA's. – Controle op opvolging aanbevelingen/voorgestelde beheers-maatregelen in de rapportage van een veiligheidsincident/datalek door de ateliers. Controle naleving beveiligingsbeleid Suwinet (norm 18.1.4). Er zal ieder kwartaal een toetsing plaatsvinden met betrekking tot de opvolging van de in het beveiligingsbeleid Suwinet genoemde punten. Om het lerend vermogen van organisaties ten aanzien van de naleving van de AVG te vergroten zullen de uitkomsten actief gedeeld worden in overleggen en zal er gecommuniceerd worden over de controles en bevindingen.	FG	Doorlopend
F. Toezicht Wpg (systeemtoezicht)	Toezicht gericht op de kwaliteit (opzet, bestaan en werking) van de Wpg-processen en van de (kwaliteits)systemen waarmee die processen bewaakt worden. Onderzoeken kunnen plaatsvinden op, onder andere: de procedure meldplicht datalekken, onderdelen van de verantwoordingsplicht en rechten betrokkenen. Hiervoor is een specifiek toezichtsplan opgesteld. De taken van de FG (artikel 36 Wpg) met betrekking tot de Wpg kunnen als volgt worden samengevat.	FG	4x per jaar na interne controle en Q3 (na afronding interne audit)

	De FG voert periodiek controles uit op het naleven van de wettelijke verplichtingen die voortkomen uit de Wpg, waaronder de controle op: 1. het hebben van een beleid aangaande de uitvoering van de Wpg; 2. de bewustwordingsverplichting; 3. het autorisatieproces met betrekking tot het vastleggen van politiegegevens; 4. de kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens; 5. het verwerken van politiegegevens; 6. de bewaartermijnen; 7. het ter beschikking stellen en verstrekken van politiegegevens; 8. de controle op de informatiebeveiliging en de controle op het uitvoeren van een risicoanalyse; 9. het register voor verwerkingen; 10. de verplichtingen ten aanzien van de audit.		
G. FG advies nieuwe DPIA's en controle op actualiteit bestaande DPIA's	De FG houdt toezicht op de uitvoering van de Data Protection Impact Assessments (DPIA's) full of light variant. Bij het opstellen van de DPIA wordt verplicht het advies ingewonnen van de FG, waarbij uiteindelijk ook een oordeel wordt gevormd over de kwaliteit van de DPIA en de acceptatie van eventuele restrisico's.	FG	Doorlopend

Overige werkzaamheden/rapportages/voorstellen/adviezen

A. Risicomanagement	Nader uit te werken in samenwerking met de concern controller en strategisch adviseur IV&P	FG	2026
B. Deelname regionaal FG overleg Noordoost-Brabant	Deelnemen aan het regionaal FG overleg Noordoost-Brabant. In dit overleg worden alle regionale zaken met betrekking tot privacy door de FG's besproken en wordt indien nodig gezamenlijk advies gegeven over gegevensverwerkingen die gemeente overstijgend of in regionaal verband plaatsvinden.	FG	Doorlopend (1x in de 6 weken)
C. Jaarverslag 2025	De FG stelt ieder jaar aan de hand van de uitgevoerde werkzaamheden een jaarverslag op over de naleving van de AVG en Wpg. Dit wordt opgepakt in samenwerking met de strategisch adviseur en het informatiebeveiliging en privacy team.	FG, Strat. Adviseur Gegevensbescherming en PO's	Q1 2026
D. Doorontwikkeling interne controles m.b.t. privacy (AVG/BIO/Wpg/Suwinet/etc?)	Binnen Meierijstad vinden diverse interne controles en audits plaats die te maken hebben met de AVG en/of aanverwante wetgeving. Centrale sturing en controle hierop vindt op dit moment nog niet plaats. Hiervoor zal er een Privacy Management Systeem verder moeten worden geïmplementeerd en uitgerold in de organisatie. De FG is vanuit zijn rol zijdelings als adviseur en belanghebbende m.b.t. toezicht betrokken.	Strat. Adviseur Gegevensbescherming en FG	Doorlopend