Gemeente Amsterdam

Jaarverslag Functionaris Gegevensbescherming 2025

Hatice Dogan

Inhoud

Managementsamenvatting
Inleiding
Leeswijzer

1. Werkzaamheden
   - 1.1 Uitvoering toezicht
   - 1.2 cijfers
     - 1.2.1 Register van verwerkingen
     - 1.2.2 Gegevensbeschermingseffectbeoordelingen
     - 1.2.3 Datalekken
     - 1.2.4 Rechten van betrokkenen
     - 1.2.5 In contact met de FG
     - 1.2.6 Autoriteit Persoonsgegevens

2. Algemene Verordening Gegevensbescherming
   - 2.1 Beleid
   - 2.2 Bewustzijn
   - 2.3 Regie op risico's
   - 2.4 Technologie en innovatie

3. Wet politiegegevens
   - 3.1 Reikwijdte
   - 3.2 Governance
   - 3.3 Audits
   - 3.4 Verstrekkingen
   - 3.5 Bewustwording en training
   - 3.6 FG Toezicht

4. Wet gegevensverwerking door samenwerkingsverbanden
   - 4.1 Regionale Informatie- en Expertisecentra (RIEC's)
   - 4.2 Coördinerend Functionaris Gegevensbescherming
   - 4.3 FG-statuut
   - 4.4 Actieventrum Veiligheid en Zorg (AcVZ)

5. Extern onderzoek privacyorganisatie

6. Vooruitblik

Lijst van afkortingen

Managementsamenvatting

Sinds 2018 is Functionaris Gegevensbescherming (FG) de onafhankelijke interne toezichthouder op de verwerkingen van persoonsgegevens van burgers, ondernemers, bezoekers en medewerkers van gemeente Amsterdam. De Autoriteit Persoonsgegevens (AP) is de landelijke onafhankelijke toezichthouder en handhaver van privacywetgeving. De FG is het centrale aanspreekpunt van de AP voor de gemeente Amsterdam. De FG werkt samen met de AP, bijvoorbeeld als er vragen zijn over de verwerking van persoonsgegevens binnen de organisatie van de FG.
Het toezichtdomein van de FG bestrijkt niet alleen de verwerkingen op grond van de Algemene Verordening Gegevensbescherming (AVG), maar ook verwerkingen op grond van de Wet politiegegevens (Wpg). De FG van gemeente Amsterdam is sinds maart 2025 met de inwerkingtreding van de Wet gegevensverwerking samenwerkingsverbanden (Wgs) ook aangewezen als coördinerend FG (cFG) voor verwerkingen van de samenwerkingsverbanden Regionaal Interventie- en Experticecentrum (RIEC) Amsterdam-Amstelland en het Actiecentrum Veiligheid en Zorg (AcVZ).

Dit is het tweede jaarverslag van de FG die vanaf januari 2024 in dienst is bij gemeente Amsterdam. De FG geeft gevraagd en ongevraagd advies. Aanleiding voor advies en toezicht kunnen zijn: vragen, klachten en/of signalen van betrokkenen, berichten uit de media en datalekken.
De aanbevelingen in dit jaarversla[1]·
De FG heeft waargenomen dat er gevolg is gegeven aan een aantal aanbevelingen door de Directie Strategie en Informatie (DSenI) zoals bewustzijn creëren en beleid ontwikkelen en/of herijken. Zo is er vanuit DS&I verbinding gerealiseerd met de privacy contactpersonen en compliance officers bij de directies door compliance gilde op te richten aan kennisdeling en eenduidig werkwijze te realiseren. De FG merkt alleen dat de beschikbaar gestelde middelen voor het creëren van bewustzijn, waaronder het tegengaan van AVG-ongeletterdheid niet voldoende is om de hele organisatie te bereiken. Het ontwikkelen/herijken van beleid door DSenI en het volgen van het beleid door de organisatie vereist het zoeken naar verbinding tussen het I-domein en de directies die belast zijn met de uitvoering van wettelijke taken. Om beleid te implementeren en richtlijnen te laten opvolgen is het ontwikkelen van een goede communicatie- en implementatiestrategie van belang. De FG vraagt aandacht hiervoor.
Bovendien merkt de FG op dat een door de hele organisatie gedragen bewustzijn programma nodig is om de AVG-ongeletterdheid tegen te gaan, soortgelijke programma als voor AI-geletterdheid getrokken door de directie P&O
Hieronder volgen de aanbevelingen per onderwerp en aanleiding waarover de FG heeft geadviseerd en/of toezicht heeft uitgeoefend.

Aanbevelingen

Data Protection Impact Assessments (DPIA's)
-De FG adviseert om bij voorgenomen verwerkingen die maatschappelijk gezien zeer wenselijk zijn, maar waarbij de grondslag in toepasselijke wetgeving ontbreekt, te

[1] Jaarverslag Functionaris Gegevensbescherming 2024

onderzoeken naar mogelijkheden volgens de geldende maatstaven en te onderbouwen met een zorgvuldige belangenafweging.
-De FG beveelt directie DSenI aan om in samenwerking met de directies een proces in te richten waarbij het register een compleet overzicht van bestaande en gemitigeerde risico's biedt.
-De FG beveelt aan om vanuit het I-domein het stedelijk proces voor het uitvoeren van een DPIA en de route naar risico-acceptatie goed onder de aandacht te brengen bij de directies en te investeren in de verbinding met de directies en adviseurs vanuit het I-domein.
-De FG beveelt aan:

- om vanuit het I-domein het stedelijk proces voor het uitvoeren van een DPIA en de route naar risico-acceptatie goed onder de aandacht te brengen
- de directies te wijzen op hun verantwoordelijkheid en rol in het proces en
- te investeren in de verbinding tussen de directies en adviseurs vanuit het I-domein. De FG wijst erop dat de directies hun verantwoordelijkheid en rol in het proces aannemen en ook verbinding zoeken om het proces niet te vertragen.

Datalekken
-De FG beveelt de directies en I-domein aan gezamenlijk op te trekken om medewerkers meer kennis bij te brengen over datalekken en bewustzijn te creëren, om zo ook de meldingsbereidheid te vergroten. Richt hiervoor een continue e-learningprogramma in. Nalatigheid in het melden kan meer schade veroorzaken voor betrokkenen. Ook kan er reputatieschade ontstaan voor de gemeente. Door tijdig te melden kunnen onvolkomenheden eerder aan het licht komen en zodoende kunnen de juiste maatregelen worden getroffen. Dit zijn niet slechts corrigerende maatregelen, maar ook preventieve maatregelen. In dit geval geldt het adagium: voorkomen is beter dan genezen.
-De FG merkt op dat onvoldoende beheer en controle op autorisaties een groot risico is binnen de organisatie en beveelt het I-domein aan stedelijk beleid te maken voor autorisatietoekenning, autorisatiebeheer, logging en monitoring, dan wel dit goed in te richten en te beheren. Richt een sluitend systeem in voor logging en monitoring, waarbij niet alleen reactief, maar ook preventief kan worden geacteerd. Het faciliteren van preventieve monitoring is noodzakelijk om de rechten en vrijheden van betrokkenen beter te waarborgen.
-De FG beveelt directie Juridische Zaken en I-domen aan gezamenlijk beleid/richtlijnen op te stellen voor schadeloosstelling van betrokkenen bij datalekken.
-De FG beveelt de directies aan om binnen eigen directie met behulp van privacy- en/of compliance officer een inventarisatie te maken van interne gegevensuitwisselingen (tussen directies) en gegevensuitwisselingen met derde partijen. Neem een voorbeeld aan directie Belastingen die projectmatig een inventarisatie heeft gemaakt van gegevensuitwisselingen. Beoordeel de gegevensuitwisseling op doelbinding, grondslag, wijze van uitwisseling en/of de gemaakte afspraken nog actueel zijn. Kortom, maak een actueel overzicht van verstrekkingen en toets alle convenanten op juistheid en houd het overzicht structureel bij, zodat er altijd een actueel overzicht is.

Rechten betrokkenen
De FG adviseert directie Dienstverlening zorg te dragen voor voldoende capaciteit voor het Loket Persoonsgegevens om het aantal verzoeken tijdig te kunnen afhandelen. Weliswaar ligt

de inhoudelijke afdoening van de verzoeken bij de directies, maar het Loket fungeert als aanjager voor tijdigheid en inhoudelijke juistheid.

Autoriteit Persoonsgegevens (AP)
De FG adviseert I-domein om een proces in te richten waarin wordt beschreven welke stakeholders aan zet zijn bij aankondiging van een handhavingsonderzoek vanuit de AP en hoe de communicatie binnen de gemeente en richting de AP plaatsvindt.

Bewustzijn
-De FG ziet het ontbreken van privacybewustzijn als een groot risico en beveelt P&O als verantwoordelijke directie, in samenwerking met DSenI aan om organisatiebreed een programma voor privacybewustzijn/AVG-geletterdheid op te zetten.
-Bewustwordingstrainingen en -campagnes zijn niet structureel binnen de organisatie geborgd en de FG adviseert dan ook om continu e-learnings en trainingsprogramma's aan te bieden. Een e-learning module is een effectieve manier om veel medewerkers binnen een kort tijdsbestek te bereiken en zo bewustzijn te creëren en een basiskennis op te laten doen.
-De FG adviseert een structurele borging van de compliance rol bij de directies.

Inleiding

De bescherming van persoonsgegevens is een belangrijk onderdeel van het eerbiedigen van de persoonlijke levenssfeer. Het recht op het eerbiedigen van de persoonlijke levenssfeer is vastgelegd in de Grondwet en in het Europees Verdrag voor de Rechten van de Mens (EVRM). Inbreuk op de persoonlijke levenssfeer mag alleen als de verwerking van persoonsgegevens in de wet is geregeld. Binnen de EU/EER is de AVG een van de belangrijkste wetten waarin de bescherming van persoonsgegevens wordt geregeld. De AVG bevat (open) normen die in acht moeten worden genomen door organisaties die persoonsgegevens verwerken, zoals de gemeente. Bij het uitoefenen van haar taken verwerkt de gemeente als bestuursorgaan, maar ook als werkgever veel persoonsgegevens. Bewoners, ondernemers, bezoekers en ook medewerkers moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met persoonsgegevens omgaat. Verwerkingen vinden plaats onder de verantwoordelijkheid van zowel het college van B&W als de burgemeester. In de AVG en de Wpg wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens.

In dit jaarverslag biedt de FG inzicht in de werkzaamheden, de middelen voor toezicht en advisering en de taakopvatting van de FG. Daarnaast geeft de FG haar bevindingen weer en doet aanbevelingen. Ook is de focus voor het komende jaar opgenomen. Dit jaarverslag is bedoeld voor de gemeenteraad enerzijds als controlerend orgaan van het college van B&W, anderzijds als zelfstandig verwerkingsverantwoordelijke.

Leeswijzer

In hoofdstuk 1 worden de werkzaamheden van de FG beschreven, gevolgd door een weergave van aanleidingen voor werkzaamheden vanuit de advies- en toezichtrol van de FG. Hierin zijn de cijfers over 2025 opgenomen en toegelicht. In hoofdstuk 2 staan de bevindingen en aanbevelingen met betrekking tot de AVG en in hoofdstuk 3 met betrekking tot de Wpg. Hoofdstuk 4 gaat in op de Wgs en de coördinerende rol die de FG voor verschillende samenwerkingsverbanden heeft. Tot slot gaat de FG in op de resultaten van het externe onderzoek naar de privacyorganisatie en het FG-Office. Het jaarverslag wordt afgesloten met een vooruitblik waarin de FG ook de taakopvatting weergeeft.

1. Werkzaamheden

1.1 Uitvoering toezicht

In haar rol als toezichthouder probeert de FG verbinding te zoeken met de organisatie en handelingsperspectief te bieden bij het in acht nemen van de gegevensbeschermingsregels. De FG merkt dat het bieden van handelingsperspectief erg welkom is en uitkomst kan bieden op het moment dat zich een knelpunt voordoet op het gebied van gegevensverwerking. Echter, gezien de beperkte capaciteit, de toegenomen werkvoorraad door interne en externe ontwikkelingen, waaronder op juridisch, technologisch en maatschappelijk vlak heeft de FG vooral reactief opgetreden. De FG streeft ernaar om proactief te adviseren, handelingsperspectief te bieden en verbinding binnen de organisatie te realiseren door de focus op rollen en verantwoordelijkheden te leggen.

1.2 Aanleiding toezicht en cijfers

Klachten, vragen, signalen van betrokkenen (bewoners, bezoekers, ondernemers en medewerkers), verwerkingen die worden bijgehouden in het register van verwerkingen, gerichte adviesvragen, datalekken, en inzage- en correctieverzoeken kunnen de FG aanleiding geven voor het uitoefenen van toezicht en het geven van advies. Hieronder geeft de FG een kort overzicht in welke mate de gegevensbeschermingsregels al dan niet in acht worden genomen en waarop geacteerd moet worden.

1.2.1 Register van verwerkingen

In het register van verwerkingen staat informatie over de verschillende verwerkingen van persoonsgegevens door de gemeente. Het bijhouden van een actueel overzicht van verwerkingen is een verplichting uit de AVG. Door de verwerkingen in een register op te nemen en te publiceren wordt voldaan aan transparantieverplichtingen.
Evenals in voorgaande jaren is in 2025 door de gemeente Amsterdam tweemaal een geactualiseerde versie van het register van verwerkingen gepubliceerd.

1.2.2 Data Protection Impact Assessments (DPIA's)

Het uitvoeren van een DPIA evenals het inwinnen van het advies van de FG is verplicht bij verwerkingen die hoge risico's met zich meebrengen voor betrokkenen.
In 2025 zijn 70 DPIA's aan de FG voorgelegd. De FG heeft 45 DPIA's in behandeling genomen. Door de beperkte capaciteit binnen het FG-office zijn niet alle DPIA's van een advies voorzien. De FG merkt dat er een stijgende lijn is in de kwaliteit van de uitgevoerde DPIA's. Dit is onder andere toe te schrijven aan de investering in de verbinding tussen de verschillende disciplines, namelijk directies en ondersteuning vanuit de privacy organisatie. Het is noodzakelijk dat de verschillende disciplines elkaar weten te vinden om de juiste input te kunnen krijgen en ook de benodigde procedures te volgen (zoals het uitvoeren van een DPIA). De FG benadrukt het belang om meer te investeren in de verbinding tussen de verschillende disciplines en om rollen en verantwoordelijkheden helder te krijgen. Informatiebeveiliging- en beheer dient daar ook in te worden meegenomen.

Daar waar de verschillende betrokken partijen elkaar goed kunnen vinden en goed samenwerken, worden de beste resultaten behaald. Ook het tijdig informeren en/of betrekken van de FG draagt bij aan het resultaat.
In de beoordeling van de DPIA's ziet de FG de kans om de organisatie handelingsperspectief te bieden in situaties waarin de wetgeving daar op het eerste gezicht weinig ruimte voor lijkt te geven. In 2025 zijn er verschillende DPIA's voorbijgekomen, vooral binnen het sociaal domein, waarbij de voorgenomen verwerking maatschappelijk gezien zeer wenselijk was, terwijl de toepasselijke wetgeving geen duidelijke grondslag bood voor de gegevensuitwisseling. Een moreel conflict dat soms ook in de publieke opinie en/of landelijke politiek werd opgemerkt.,
Het gebrek aan een (duidelijke) grondslag betekent echter niet altijd dat een rechtmatige verwerking onmogelijk is. De AVG bevat weliswaar verbodsbepalingen, maar bestaat voor een groot deel uit open normen. Wanneer de aandacht zich vooral richt op die verbodsbepalingen, ontstaat er soms handelingsverlegenheid vanuit het idee dat er op basis van de AVG "toch niets mag". Dat is een veelvoorkomende misvatting. Juist de open normen bieden mogelijkheden, mits deze goed worden uitgelegd volgens de geldende maatstaven en onderbouwd zijn met een zorgvuldige belangenafweging. Een voorbeeld hiervan is het onderzoeksprogramma Gewoon geld geven, waarbij op basis van de verenigbaarheidstoets uit de AVG de verwerking toch rechtmatig kon plaatsvinden. De FG ziet het bieden van handelingsperspectief dan ook als een belangrijk onderdeel van haar adviesrol.
In 2025 heeft de FG eenmaal negatief geadviseerd. Dit betreft de DPIA die is uitgevoerd ten behoeve van de voorgenomen verwerkingen op het sociale media platform TikTok. Het college van B&W heeft besloten om de verwerking toch te starten, nadat een gedegen belangenafweging is gemaakt. De FG merkt op dat door de verschillende betrokken partijen goed is samengewerkt om de verwerkingen en de risico's in kaart te brengen, aan te passen, en mitigerende maatregelen te nemen om de risico's zoveel mogelijk te verkleinen. De FG heeft in dit geval ook geadviseerd om ook voor andere sociale media platformen, die voor verschillende doeleinden en door verschillende directies worden ingezet, de risico's in kaart te brengen.
De FG adviseert om bij voorgenomen verwerkingen die maatschappelijk gezien zeer wenselijk zijn, maar waarbij de grondslag in toepasselijke wetgeving ontbreekt, te onderzoeken naar mogelijkheden volgens de geldende maatstaven en te onderbouwen met een zorgvuldige belangenafweging.

DPIA-proces
Ten aanzien van het proces rondom de beoordeling van de DPIA constateert de FG dat de terugkoppeling van de beoordeling als positieve feedback wordt ontvangen. Het advies van de FG kan zijn: positief (met opmerkingen), negatief of geen advies. Wanneer de uit de DPIA voortvloeiende risico's niet voldoende gemitigeerd kunnen worden en de verwerking alsnog zal plaatsvinden, dan dienen de risico's formeel geaccepteerd worden door de betrokken (stedelijk) directeur.

Risicoregister en opvolging maatregelen
Directie DSenI registreert in DPIA's geïdentificeerde risico's en daartegenover gestelde maatregelen in de applicatie Fully in Control (FIC). Op deze wijze wordt een risicoregister

gecreëerd, waarop vervolgens risico gebaseerd gewerkt en gestuurd kan worden. De opvolging van maatregelen valt onder verantwoordelijkheid van de directies, maar er is geen sluitend werkproces om de risico's die worden geregistreerd te koppelen aan de verantwoordelijke directie(s), waardoor op dit moment geen actueel overzicht van risico's versus genomen maatregelen is.
De FG beveelt directie DSenI aan om in samenwerking met de directies een proces in te richten waarbij het register een compleet overzicht van bestaande en gemitigeerde risico's biedt.

Risico-acceptatie
De FG heeft aandacht gevraagd voor een risico-acceptatieproces. De FG merkt op dat er inmiddels een stedelijk proces is ingericht. Dit draagt bij aan de verantwoordingsplicht waarbij de organisatie in voldoende mate kan aantonen hoe de afweging wordt gemaakt bij het accepteren van risico's. Wanneer het stedelijk proces niet wordt gevolgd en de verbinding niet wordt gezocht loopt de voorgenomen verwerking vertraging op met frustratie bij betrokken partijen tot gevolg. Met betrekking tot het DPIA-proces benadrukt de FG het belang om helderheid te creëren inzake rollen en verantwoordelijkheden bij de uitvoering van een DPIA. De FG noemt het inzetten van Livecrowd tijdens grootschalige evenementen in de stad als een goed voorbeeld van een voorgenomen verwerking die vertraging heeft opgelopen doordat de directie in kwestie niet tijdig met de uitvoering van de DPIA is gestart en uiteindelijk het stedelijk proces voor de risico-acceptatie niet correct heeft gevolgd.
De FG beveelt aan:

- *om vanuit het I-domein het stedelijk proces voor het uitvoeren van een DPIA en de route naar risico-acceptatie goed onder de aandacht te brengen*
- *de directies te wijzen op hun verantwoordelijkheid en rol in het proces en*
- *te investeren in de verbinding tussen de directies en adviseurs vanuit het I-domein.*

1.2.3 Datalekken

In 2025 zijn 351 incidenten gemeld die zijn beoordeeld en geregistreerd als datalek. Van de 351 datalekken is ongeveer 13% beoordeeld als meldenswaardig bij de AP. In deze gevallen is de FG geïnformeerd dan wel om advies gevraagd over de afhandeling van het datalek.

Categorie	Aantal
Verlies/diefstal apparaat	165
E-mail aan foute ontvanger	46
Post aan foute ontvanger	23
Verkeerde autorisatie(s)	16
Persoonsgegevens gepubliceerd	15
Persoonsgegevens in verkeerd dossier	10
Hacking, malware, phishing	7
E-mail via CC i.p.v. BCC	6
Door storing geen persoonsgegevens	1
Persoonsgegevens bij oud papier gezet	1
Verkeerde persoonsgegevens klantportaal	1

Overig	60
Totaal	351

Het aantal datalekken is daarmee met 20% gestegen ten opzichte van 2024 (291 datalekken). Deze toename wordt hoofdzakelijk verklaard door toegenomen meldingen van verlies of diefstal van een apparaat, namelijk een toename van 54 meldingen ten opzichte van 2024.

De FG merkt op dat het aantal geregistreerde datalekken bijzonder laag is voor een organisatie ter grootte van gemeente Amsterdam en rekening houdend met de hoeveelheid taken die de gemeente uitvoert waarbij persoonsgegevens worden verwerkt. Een van de belangrijkste redenen hiervoor lijkt het ontbreken van kennis: wat is een datalek en wat moet ik doen bij een (vermoeden van) een datalek? Aandacht voor kennisdeling is er wel vanuit DS&I maar door beperkte capaciteit kan de grote groep niet bereikt worden.Daarnaast kan ook de meldingsbereidheid laag zijn. Het ontbreken van kennis en de meldingsbereidheid houden mogelijk verband met elkaar.
De FG beveelt aan om meer kennis bij te brengen, bewustzijn te creëren bij de medewerkers voor meldingsbereidheid. Richt continue e-learningprogramma's in. Nalatigheid in het melden kan meer schade veroorzaken voor betrokkenen en er kan reputatieschade ontstaan voor de gemeente. Door tijdige meldingen kunnen onvolkomenheden eerder aan het licht komen waardoor de juiste maatregelen getroffen kunnen worden. Dit zijn niet slechts corrigerende maatregelen, maar ook preventieve maatregelen. In dit geval geldt het adagium: voorkomen is beter dan genezen.

In 2024 is een aantal incidenten gemeld met hoge impact voor betrokkenen. Twee daarvan zijn ontstaan doordat logging en monitoring van applicaties onvoldoende waren ingericht. Hierdoor bleef onrechtmatige toegang tot persoonsgegevens onopgemerkt, met ernstige datalekken en schade voor betrokkenen tot gevolg. De FG merkt op dat het ontbreken van een stedelijk beleid en richtlijnen voor toekenning van autorisaties vermoedelijk een belangrijke oorzaak is van de incidenten.
Betrokkenen kunnen de gemeente aansprakelijk stellen voor schade die zij hebben geleden als gevolg van een datalek. Zij kunnen schadevergoeding eisen naargelang de ernst van de inbreuk op rechten en vrijheden Dit is wettelijk verankerd in de AVG.
Met regelmaat komt het voor dat betrokkenen schadevergoeding eisen. Van belang is dat er vanuit de gemeente richtlijnen komen over de schadeafhandeling naar de ernst van de inbreuk en de wijze van schadeloosstelling. Dit zal moeten worden opgepakt door directie Juridische Zaken en DSenI.
De FG merkt op dat onvoldoende beheer en controle op autorisaties een groot risico is binnen de organisatie en beveelt aan om een goed autorisatiebeheer, logging en monitoring in te richten dan wel dit goed te beheren om herhaling te voorkomen.
De FG beveelt ook aan om beleid/richtlijnen op te stellen voor schadeloosstelling van de betrokkenen bij datalekken.

Het delen van persoonsgegevens binnen de organisatie (bijvoorbeeld tussen directies) of met derden vormt ook een risico op ernstige datalekken. In haar werkzaamheden signaleert de FG

dat gegevensdeling binnen de gemeente (tussen directies) en door de gemeente met externe partijen veel voorkomt zonder dat hiervoor de benodigde afspraken gemaakt zijn. Ook signaleert de FG dat gemaakte afspraken geactualiseerd dienen te worden. Dit is een terugkerend thema in klachten of signalen van betrokkenen, bij het beoordelen van DPIA's of terugkoppeling vanuit directies op vragen die door de FG gesteld worden.
De FG beveelt aan om per directie een inventarisatie te maken van interne (tussen de directies) en externe (met derde partijen) gegevensuitwisselingen. Neem een voorbeeld aan directie Belastingen die hiervoor projectmatig een inventarisatie heeft gemaakt van gegevensuitwisselingen en daarbij toetst op doelbinding, grondslag, wijze van uitwisseling en beoordeelt of de gemaakte afspraken nog actueel zijn.

1.2.4 Rechten van betrokkenen

Het Loket Persoonsgegevens coördineert verzoeken op grond van de rechten van betrokkenen uit de AVG. Het Loket fungeert als doorgeefluik tussen betrokkenen en de verantwoordelijke directie. Door de positie van het Loket vindt er geen eenduidige afhandeling op de verzoeken van betrokkenen plaats. De verantwoordelijkheid voor de inhoudelijke behandeling en het tijdig behandelen van verzoeken ligt bij de directies, omdat zij gemandateerd verwerkingsverantwoordelijke zijn. Het Loket is ondergebracht bij de directie Dienstverlening en staat op grote afstand van het I-domein waar de privacy officers zijn ondergebracht. In het onderzoek naar de privacy organisatie dat in 2025 door een extern bureau is uitgevoerd is ook gekeken naar de positie van het Loket. Het is van groot belang voor professionalisering van Loket dat medewerkers in goede verbinding staan met de privacy officers en worden meegenomen in kennisvergaring- en deling.
Tot 12 december 2025 zijn er in totaal 370 verzoeken ingediend, waarvan 313 door het Loket Persoonsgegevens zijn beoordeeld als AVG-verzoek. Dit is een stijging ten opzichte van 2024. Toen werden er 287 verzoeken ingediend, waarvan er 259 werden beoordeeld als AVG-verzoek. In 2025 werden 57 verzoeken geclassificeerd als overige vragen/verzoeken en 8 verzoeken zijn dubbel ingediend.

Type verzoek	Aantal
Inzageverzoek	249
Verwijderverzoek	41
Correctie-/rectificatieverzoek	15
Beperking van de verwerking	6
Bezwaar tegen de verwerking	2
Totaal	313

De wettelijke termijn voor de behandeling van AVG-verzoeken is één maand. Door te verdagen kan de wettelijke termijn worden verlengd met twee maanden. De verdaging dient gemotiveerd te zijn. In 2025 was gemiddelde doorlooptijd van verzoeken 52 dagen. 195 verzoeken hebben geleid tot een besluit. In 105 gevallen is de wettelijke termijn, ook na verdagen overschreden. Druk op de capaciteit bij het Loket Persoonsgegevens en vertraging doordat directies niet op tijd reageren, liggen ten grondslag aan het overschrijden van de wettelijke termijn. Hierdoor ontstaan onnodige bezwaarprocedures en klachten.

Er is een onderzoek gedaan naar de privacy organisatie, het Loket was hier onderdeel van. Eén van de adviezen uit het onderzoek is om het Loket onder te brengen bij het Stedelijke Openbaarheidsteam. Dit om deze genoemde risico's te beperken. In 2026 wordt gekeken naar de positionering van Loket Persoonsgegevens binnen de organisatie.
De FG adviseert om zorg te dragen voor voldoende capaciteit voor het Loket om het aantal verzoeken tijdig te kunnen behandelen. Weliswaar ligt de inhoudelijke afdoening van de verzoeken bij de directies, maar het Loket fungeert als aanjager voor tijdigheid en inhoudelijke juistheid. Ook adviseert de FG om goed te kijken naar de positionering van het Loket en te investeren in kennis.

1.2.5 In contact met de FG

De FG ontvangt dagelijks berichten van bewoners, ondernemers, bezoekers en ook van medewerkers met vragen, verzoeken en klachten, of berichten waarin iemand zijn zorgen uit. Veruit de meeste berichten komen binnen via het functionele e-mailadres van de FG.
Waar mogelijk beantwoordt de FG berichten zelf of worden uitgezet binnen de organisatie. Ook worden berichten als signaalfunctie gebruikt om met de organisatie in gesprek te gaan en de organisatie te helpen gegevensbescherming en privacy beter te borgen.
De Functionaris Gegevensbescherming is bereikbaar via:
functionaris.gegevensbescherming@amsterdam.nl.

1.2.6 Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) is de nationale toezichthouder en handhaver op de privacywetgeving. De FG is het centrale aanspreekpunt van de AP. De FG werkt samen met de AP, bijvoorbeeld als er vragen zijn over de verwerking van persoonsgegevens binnen de organisatie van de FG. De AP zet de vragen naar aanleiding van klachten/signalen van betrokkenen via de FG uit. Ook onderzoeken van de AP worden doorgaans via de FG kenbaar gemaakt. De FG vervult een centrale coördinerende rol in de beantwoording richting de AP. Beantwoording vindt door de directies plaats waarbij de privacy officers een adviserende rol hebben. De FG leest met de blik van de AP de antwoorden voordat de reactie naar de AP wordt verzonden. Op deze wijze adviseert de FG en bespreekt de FG tekortkomingen en te treffen maatregelen naar aanleiding van klachten en of onderzoeken. De AP kan ook een handhavingsonderzoek doen. In dat geval richt de AP zich tot de verwerkingsverantwoordelijke. Afhankelijk van het onderwerp kan dat het college van B&W of de burgemeester zijn. De FG wordt enkel in kennis gesteld. In het geval een onderzoek door de AP uitwijst dat sprake is van een overtreding, kan de AP handhavend optreden. De AP kan dan een last onder dwangsom of een bestuurlijke boete opleggen.
Het is nog niet voorgekomen dat de AP een handhavingsonderzoek bij de gemeente heeft aangekondigd. Wel is het van belang om hiervoor een proces in te richten, gezien de toenemende datalekken, klachten en signalen die voor de AP aanleiding tot het instellen van een handhavingsonderzoek kunnen zijn.
De FG adviseert om een proces in te richten waarin wordt beschreven welke stakeholders aan zet zijn bij aankondiging van een handhavingsonderzoek en hoe de communicatie plaatsvindt.

In 2025 heeft de AP acht keer contact opgenomen via de FG met vragen over de aard en wijze van verwerkingen van persoonsgegevens binnen de gemeente Amsterdam en naar aanleiding van klachten en signalen van betrokkenen.
Zo heeft de AP een themastudie verricht over de inzet van algoritmes en AI bij directie Parkeren. De AP is als toezichthouder ook verantwoordelijk voor het toezicht op de toepassing van AI en algoritmes waarbij persoonsgegevens worden verwerkt. Uit de beantwoording door de directie blijkt dat aandacht en eisen voor privacy en informatiebeveiliging binnen de werkprocessen zijn toegenomen. Voorbeelden hiervan zijn het *blurren* van persoonsgegevens op foto's bij de bron, waardoor in het gehele proces alleen geblurde foto's beschikbaar zijn, en maatregelen met betrekking tot betekenisvolle menselijke tussenkomst bij het beoordelen van foto's. Daarnaast is er meer aandacht voor de menselijke maat. Dit is het gevolg van goed samenwerken en verbinding zoeken tussen de directie en privacy officers. De gemeente is zich ervan bewust dat mensen fouten kunnen maken. Bij parkeerhandhaving wordt hier op verschillende manieren rekening mee gehouden en in de bezwaarprocedure wordt altijd gekeken naar de omstandigheden per geval. Is er bijvoorbeeld sprake van overmacht of zijn er andere omstandigheden waardoor de kentekenhouder de fout niet is aan te rekenen?

Een ander voorbeeld waarover de AP vragen heeft gesteld is de inzet van Livecrowd bij evenementen, waaronder SAIL 2025, naar aanleiding van signalen van betrokkenen. De FG heeft na beantwoording van de vragen richting de AP de verantwoordelijke directie nadrukkelijk geadviseerd om een DPIA uit te voeren die kan worden gebruikt voor inzet van Livecrowd bij verschillende evenementen. De verantwoordelijke directie is tekortgeschoten in het tijdig uitvoeren van de DPIA waarna is gepoogd om buiten het stedelijk proces de risico's te laten accepteren. Het niet tijdig afronden van de DPIA, ondanks dat er meer dan voldoende tijd was voor afronding, is een tekortkoming van de verantwoordelijke directie. De FG heeft bij herhaling het belang van de DPIA bij de directie onder de aandacht gebracht en ook gepoogd om verbinding met de hiervoor noodzakelijke stakeholders te realiseren.

2. Algemene Verordening Gegevensbescherming

2.1 Beleid

Door ontwikkelingen op juridisch, maatschappelijk, technologisch en organisatorisch gebied is het stedelijk beleidskader privacy, opgesteld in 2018, achterhaald. Directie Digitale Strategie en Informatie (DS&I), verantwoordelijk voor beleid op het gebied van privacy en gegevensbescherming, is gestart met het herijken van onder meer het stedelijk beleidskader en ander beleid met betrekking tot privacy en gegevensbescherming, waaronder datalekken en met betrekking tot rechten van betrokkenen. De FG heeft meegelezen op het concept en geadviseerd op de inhoud.
De directie is voornemens om het geactualiseerde stedelijk beleidskader in 2026 vast te laten stellen door het college van B&W.
De FG is ook bezig met het opstellen van een statuut waarin wordt ingegaan op de rollen, taken en verantwoordelijkheden van verschillende disciplines in verhouding tot de FG en de werkwijze van de FG. Het FG-statuut zal tegelijk met het stedelijk beleidskader aan het college worden aangeboden

2.2 Bewustzijn

De FG heeft in het vorige jaarverslag aanbevolen om het privacybewustzijn/de *AVG-geletterdheid* bij de medewerkers te bevorderen. Door de organisatie is gekozen om de opgave bij DS&I te beleggen door een compliance awareness officer aan te stellen en hiervoor middelen beschikbaar te stellen. De FG merkt op dat het bewustzijn en de AVG-geletterdheid niet structureel zijn verbeterd en dat de beschikbaar gestelde middelen onvoldoende zijn om organisatiebreed bewustzijn te creëren.
De FG ziet het ontbreken van privacybewustzijn als een groot risico en beveelt aan om een organisatiebreed programma voor privacybewustzijn/AVG-geletterdheid op te zetten. Een e-learning module is een effectieve manier om veel medewerkers binnen een kort tijdsbestek te bereiken en zo bewustzijn te creëren en basiskennis op te laten doen. De FG adviseert om deze opgave te beleggen bij Personeel en Organisatie (P&O), hierbij samenwerking te zoeken met DS&I en op dezelfde wijze als AI-geletterdheid een project op te zetten.

2.3 Regie op risico's

Om regie te kunnen voeren op risico's moet eerst inzichtelijk zijn welke risico's er zijn. De FG ziet dat er in het afgelopen jaar stappen zijn gezet om risico's beter in de kaart te brengen, maar merkt ook op dat er nog een weg te gaan is om effectief en efficiënt regie te kunnen voeren op de risico's.

Baseline Privacy Amsterdam
In 2023 is gestart met de Baseline Privacy Amsterdam (BPA) vanuit de interne behoefte om te weten in hoeverre de gemeentelijke organisatie aan de AVG voldoet en vanuit de externe verantwoordingsplicht uit de AVG.
In 2025 zijn de resultaten van de eerste nulmeting beschikbaar gekomen. Deze nulmeting is het startpunt van een Plan-Do-Check-Act (PDCA) cyclus, waar verbeterplannen per directie een essentieel onderdeel van zullen vormen. Aan de risico's die als resultaat uit de BPA nulmeting zijn geïdentificeerd zijn inmiddels maatregelen gekoppeld.

In de BPA zijn verschillende thema's opgenomen, die weer zijn gekoppeld aan verschillende onderwerpen. Op elk van de onderwerpen volgt een score tussen 0 en 4, waarbij 4 inhoudt dat voldaan wordt aan de minimale vereisten uit de AVG.

De gemiddelde BPA-score op stedelijk niveau is 3,4 en is daarmee redelijk, maar nog niet goed genoeg. De meest significante en urgente verbeteringen zijn nodig op de onderwerpen:

- Privacybeleid, dit dient geactualiseerd te worden;
- Bewustwording, met name door middel van een programma om medewerkers doorlopend bewust te maken en te houden van de risico's en randvoorwaarden bij de omgang met persoonsgegevens.

De gemiddelde BPA-score van alle directies is 2,4 en is daarmee onvoldoende. De meest significante en urgente verbeteringen zijn nodig op de onderwerpen:

- Bewustwording, met name het kunnen aantonen dat medewerkers en contractanten een bewustwordingstraining hebben gevolgd en het toetsen of de trainingen effectief zijn geweest;
- Bewaar- en vernietigingsbeleid, met name het daadwerkelijk verwijderen en vernietigen van persoonsgegevens en het toezicht daarop;
- DPIA's, met name de controle op de uit te voeren maatregelen zoals die zijn vastgelegd in de DPIA en de effectiviteit van deze maatregelen.

Het voornemen is om de resultaten uit de BPA inzichtelijk te maken via de GRC-tool Fully In Control (FIC) en door middel van dashboards. Naar aanleiding van de resultaten uit de BPA worden samen met de directies verbeterplannen opgesteld voor de directies, met daarin geadviseerde en geprioriteerde maatregelen om privacy risico's te mitigeren.
De FG is periodiek geïnformeerd over de voortgang, zowel inhoudelijk als op procesmatig vlak. De resultaten zijn een instrument voor de organisatie dat inzicht biedt in het volwassenheidsniveau van de organisatie. Deze inzichten maken het mogelijk om gericht te sturen op risico's.
De FG merkt dat de BPA een waardevol instrument is waarmee inzichtelijk wordt gemaakt hoe de directies ervoor staan in de uitvoering van de AVG en adviseert om BPA te blijven inzetten om effectief en efficiënt regie te kunnen voeren op risico's.

Kwartaalrapportages
In 2025 is ook een start gemaakt met de kwartaalrapportage privacy. Hierin worden per cluster belangrijke bespreekpunten opgenomen, die vervolgens worden besproken in het gemeentelijk managementteam (GMT), waarna zij geadresseerd kunnen worden. De kwartaalrapportage zorgt ervoor dat er gedurende het jaar meer momenten zijn om te sturen op risico's. De FG wordt geconsulteerd bij het opstellen van de rapportage en kan op deze wijze bespreekpunten agenderen.
De FG kijkt uit naar de implementatie en verankering van deze wijze van rapporteren en adequate opvolging van bespreekpunten.

Fully In Control
De door de gemeente aangekochte GRC-tool Fully In Control (FIC) is in 2025 doorontwikkeld en zal ook in 2026 verder doorontwikkeld worden. De resultaten van de BPA zijn vastgelegd in FIC. Ook

dient de tool te functioneren als risicoregister voor risico's op verschillende compliance vlakken, namelijk privacy en gegevensbescherming, informatiebeveiliging en informatiebeheer.
De FG merkt op dat er vorderingen worden gemaakt, maar dat het tempo laag is door de beperkte middelen en capaciteit voor de ontwikkeling en inrichting van de tool en beveelt aan voldoende middelen en capaciteit beschikbaar te stellen om het tempo waarmee de tool doorontwikkeld wordt te verhogen.

2.4 Technologie en innovatie

De gemeente wil efficiënt en dienstverlenend zijn richting de burger en effectief zijn wanneer het op preventie en handhaving aankomt. De toenemende digitalisering en technologische ontwikkelingen bieden hiervoor ruimte.

Algoritmen en kunstmatige intelligentie (AI)
Binnen de organisatie zien we steeds meer gebruik van toepassingen van (generatieve) kunstmatige intelligentie (AI). Bij inzet van AI waarbij er persoonsgegevens verwerkt worden, is de AVG ook van toepassing.
De FG merkt op dat de organisatie in 2025 stappen heeft gezet om verantwoord om te gaan met de inzet van AI. Een voorbeeld hiervan is de ontwikkelde *Amsterdamse AI Agenda* die is vastgesteld door het college van B&W, waarin ook aandacht is voor kaders en beleid.
Binnen het cluster Digitalisering, Innovatie en Informatie (DII) wordt gewerkt aan het in kaart brengen en beoordelen van algoritmen en AI-toepassingen en kaders en beleid daarop.
Binnen het *Quality Assurance Acceptatiecriteria*-proces is ook aandacht voor dergelijke toepassingen, zodat deze binnen de kaders van wet- en regelgeving en het beleid plaatsvinden.
Een toepassing die in het oog springt is *ChatAmsterdam*. ChatAmsterdam is een generatieve AI-toepassing die is ontwikkeld voor de medewerkers van de gemeente en voldoet aan het beleid rondom privacy, informatiebeveiliging en informatiebeheer.
De FG heeft ook een toezichttaak als het gaat om verwerking van persoonsgegevens in het kader van de AI-verordening. Het verantwoord gebruik van AI biedt veel kansen, terwijl onverantwoord gebruik juist grote risico’s met zich meebrengt.

3. Wet politiegegevens

3.1 Reikwijdte

De Wet politiegegevens (Wpg) is direct van toepassing op de directies Toezicht en Handhaving in de Openbare Ruimte (THOR), Onderwijs (leerplicht), Werk, Participatie en Inkomen (sociale recherche) en Sport en Bos (boswachterij) omdat deze directies Buitengewoon opsporingsambtenaren (Boa's) in dienst hebben. Een aantal directies werkt nauw samen met de politie en ook weer intern met de genoemde Boa directies: deze directies ontvangen gegevens uit het Wpg domein en moeten hier vanzelfsprekend verantwoord mee omgaan. Denk aan de uit de Wpg voortvloeiende beginselen van geheimhouding en doelbinding. De belangrijkste onder deze directies zijn Openbare Orde en Veiligheid (OOV), Veiligheid, Toezicht en Handhaving (VTH, onderdeel stadsdelen), Verkeer en Openbare Ruimte (V&OR) en Wonen.
Verspreid over de Boa directies heeft de gemeente Amsterdam Boa's in vijf Boa domeinen, I, II, III, IV en V. Daaronder zijn grote verschillen in kwantiteit. De directie THOR heeft ongeveer 450 Boa's in dienst, de directie Inkomen heeft een team van 3 – 6 sociaal rechercheurs. Ook het soort werk en de daaruit volgende gegevensverwerkingen kent grote onderlinge verschillen.

3.2 Governance

Verwerkingsverantwoordelijke voor de Wpg is de werkgever, in casu het college van B&W. Het college B&W heeft de verwerkingsverantwoordelijkheid per directie doorgelegd. Er is bij de vakgroep Digitale Rechten, Ethiek en Privacy DREP) van DS&I een stedelijke coördinator en privacy officer Wpg aangesteld. Elke directie waar Boa's werkzaam zijn moet uit hoofde van het stedelijk beleid een contactpersoon voor de coördinator Wpg aanstellen. Bij de directie THOR is in het laatste kwartaal van 2025 een compliance officer aangesteld op basis van externe inhuur. Ook bij Onderwijs wordt hieraan gedacht en is een kwartiermaker voor een compliance functie ingehuurd. Bij de directie WPI is voor ondersteuning van de sociale recherche tijdens de audit een privacy adviseur ingehuurd. WPI beschikt al over een compliance officer die zich (ook) met de Wpg bezighoudt. Bij Sport en Bos is momenteel op alleen de privacy contactpersoon aanspreekbaar voor de Wpg coördinator.
De in het jaarverslag van 2024 van de FG geconstateerde behoefte aan en noodzaak van een serieus ingevulde compliance functie bij een aantal directies wordt gevoeld en er zijn stappen gezet om hier invulling aan te geven. Echter is het van belang om de compliance rol structureel te borgen.
De FG adviseert een structurele borging van de compliance rol bij de directies.

3.3 Audits

In 2025 is door de ACAM een externe audit afgenomen op ‘opzet’ en ‘bestaan’ op basis van twee peildata. Voor de toezichtmaatregelen is de peildatum de gehele periode 2022-2024. De twee peildata zijn gekozen omdat, zoals in het FG jaarverslag over 2024 te lezen is, een groot aantal maatregelen en systeemwijzigingen in 2024 zijn doorgevoerd die in de zomer hun beslag kregen. Concreet leidt dit ertoe dat het resultaat van de audit in de ‘opzet’ periode een groot verschil vertoont met het resultaat in de ‘bestaan’ periode. Waar in juni door Onderwijs

en WPI grotendeels niet aan de Wpg-normen werd voldaan door het gebruik van oude applicaties voldoen dezelfde directies dat op 31 december grotendeels wel. De ACAM hanteert als systematiek dat de werking 'rood' kleurt ('onvoldoende') wanneer op enig moment in het jaar een norm als niet voldoende of deels voldoende is beoordeeld. De auditperiode voor 'werking' is daarmee het hele kalenderjaar. Hierdoor is in de 'werking' een groot aantal normen als 'onvoldoende' beoordeeld voor de auditperiode. Zodoende komt de ACAM tot een 'afkeurend oordeel'. Tegelijkertijd voegt de ACAM een aanbiedingsbrief bij waarin zij schrijven: "Hoewel wij in onze rapportage tot een afkeurend oordeel komen, signaleren wij wel dat er in de uitkomsten in onze rapportage gedurende het jaar 2024 een sterke verbetering zichtbaar is voor het voldoen aan de beheersmaatregelen tussen de beide peildata. Dit bevestigt het beeld dat gedurende het jaar 2024 bij de verschillende directies al verbeteringen zijn doorgevoerd." Het rapport is conform de verplichting opgestuurd naar de AP.
Op de onderdelen die als niet voldoende zijn beoordeeld en waarvoor de ACAM aanbevelingen heeft gedaan, zal in het eerste half jaar van 2026 een hercontrole worden uitgevoerd door interne auditdienst Directie, Middelen en Control (DMC).
De FG merkt dat er zowel op stedelijk als op directieniveau een aantal maatregelen zijn getroffen voor de Wpg-compliance. Specifiek vraagt de FG aandacht voor autorisatietoekenning en een sluitend systeem voor logging en monitoring, waarbij niet alleen reactief, maar ook preventief moet kunnen worden geacteerd.
In 2025 is de gemeente betrokken geweest bij een groot datalek als gevolg van het niet-integer handelen van een Boa die persoonsgegevens had verkocht aan derden. Als verwerkingsverantwoordelijke heeft de gemeente onder omstandigheden de plicht om de betrokkenen wiens gegevens zijn gelekt daarvan op de hoogte te stellen. In de onderhavige situatie beschikt niet de gemeente over deze gegevens, maar de Rijksrecherche, in verband met het strafrechtelijke onderzoek dat zij hebben uitgevoerd tegen de Boa. De Rijksrecherche ziet echter in de Wpg geen grondslag om deze gegevens met de gemeente te delen. De gemeente is met Rijksrecherche, Openbaar Ministerie en de AP in gesprek hoe met deze situatie omgegaan kan worden.
De FG beveelt aan specifiek aandacht te besteden voor autorisatietoekenning en een sluitend systeem voor logging en monitoring daarvan in te richten, waarbij niet alleen reactief, maar ook preventief kan worden geacteerd. Het faciliteren van preventieve monitoring is noodzakelijk om de rechten en vrijheden van betrokkenen beter te waarborgen, onder andere om betrokkenen beter te kunnen informeren.

3.4 Verstrekkingen

De FG constateerde al in het vorige jaarverslag dat er nog het nodige te verbeteren valt wanneer het gaat om het documenteren en zorgvuldig afhandelen van verstrekkingen van politiegegevens naar (keten)partners buiten het opsporingsdomein. Het verbeteren hiervan is alleen mogelijk door een groot aantal procedurele onderwerpen tegelijk aan te pakken. Daarbij gaat het om documenteren (register van verstrekkingen op orde hebben), vastleggen van afspraken (bijvoorbeeld gegevensleveringsovereenkomsten) en bewustwording en training. Hiervoor is ook coördinatie nodig: een compliance officer in de eerste lijn die als ogen

en oren functioneert en weet met welke partijen politiegegevens worden gedeeld door de eigen lijndirectie.
Overzicht en inzicht – ten aanzien van het proces en de documentatie – is de stap op weg naar verbetering. Bij de ACAM audit is gebleken dat dit bij de Boa directies op peildatum 31 december 2024 nog altijd niet voldoende op orde was. De directies hebben in het verbeterplan naar aanleiding van deze audit als belangrijkste agendapunt voor het eerste half jaar van 2026 opgenomen om het register van verstrekkingen op orde te brengen. Tevens zullen daarbij alle convenanten waarbij op basis van artikel 20 Wpg gegevens worden uitgewisseld aan een kritische toets worden onderworpen om te beoordelen of deze convenanten nog actueel zijn of aanpassing behoeven.
De FG onderschrijft het belang van een actueel overzicht van verstrekkingen en adviseert om alle convenanten te toetsen op juistheid van verstrekkingen.

3.5 Bewustwording en training

De conclusie van de audit dat het beleid en de procedures voor de Wpg sinds december 2024 theoretisch grotendeels op orde zijn gebracht betekent in de praktijk niet automatisch dat elk individu deze volledig naleeft. Zo heeft elke Boa in de Wpg de bevoegdheid een verstrekking te doen. Dit betekent dat alle Boa's zich gedegen bewust moeten zijn van de spelregels op dit vlak.
De FG merkt dat bewustwording en training niet structureel is geborgd en beveelt aan continu e-learnings- en trainingsprogragmma's aan te bieden.

3.6 FG Toezicht

De FG geeft bij voorkeur advies op strategisch en beleidsmatig niveau, om op die manier de organisatie op integrale wijze te kunnen ondersteunen en informeren. Adviseren en toezicht houden op het niveau van een specifieke verwerking doet de FG door middel van DPIA's die aan de FG worden voorgelegd. Bovendien heeft de FG regulier en periodiek overleg met de coördinator Wpg en krijgt op die wijze signalen over wat goed gaat in de organisatie en wat beter kan. Daarbij heeft de FG aandacht voor onderwerpen als beleid, rechtmatigheid, noodzakelijkheid, doelbinding, juistheid en volledigheid, de verwerking van bijzondere persoonsgegevens, de toewijzing van autorisaties en het tijdig laten uitvoeren van audits.

4. Wet gegevensverwerking door samenwerkingsverbanden

4.1 Regionale Informatie- en Expertisecentra (RIEC's)

Het RIEC-samenwerkingsverband verwerkt persoonsgegevens in een complexe structuur met meerdere verwerkingsverantwoordelijken. Dit vraagt om zorgvuldig en goed afgestemd toezicht.

4.2 Coördinerend Functionaris Gegevensbescherming

Per 1 maart 2025 is de Wet gegevensverwerking door samenwerkingsverbanden (Wgs) in werking getreden. De Wgs bepaalt dat het samenwerkingsverband één van de FG's van de deelnemende overheidsinstanties aanwijst als coördinerend FG (cFG). Binnen de regio Amsterdam-Amstelland is ervoor gekozen om voor het RIEC-samenwerkingsverband de FG van gemeente Amsterdam aan te wijzen als cFG. Elke deelnemer van het RIEC-samenwerkingsbestand beschikt over een eigen FG. Taken van de FG zijn beschreven in de AVG.
De Wgs bevat echter geen nadere bepalingen over de inrichting van deze coördinerende rol. Ook de AVG voorziet niet in een wettelijk kader voor gezamenlijk FG-toezicht binnen een samenwerkingsverband en kent evenmin een cFG rol. De FG van gemeente Amsterdam heeft aangegeven de coördinerende rol op zich te nemen als er voldoende budget voor de uitvoering van de taken wordt toegekend en er een statuut wordt opgesteld waarin overeenstemming wordt bereikt over het uit te oefenen gezamenlijk toezicht.
Vanuit het bureau RIEC wordt jaarlijks voor 0,5 fte aan budget toegekend voor de cFG taken. Sinds de inwerkingtreding van de Wgs organiseert de cFG structureel overleggen met de FG's van de deelnemers. Het RIEC-bureau sluit aan bij deze overleggen om actuele ontwikkelingen en relevante informatie uit het samenwerkingsverband te delen met de (c)FG's. De deelname van het RIEC-bureau aan de FG overleggen ondersteunt het gezamenlijk toezicht en bevordert een goede afstemming tussen de FG's, de cFG en de deelnemers. Om duidelijkheid te creëren over de rolverdeling, samenwerking en verantwoordelijkheden is een gezamenlijk FG-statuut opgesteld. Het FG-statuut wordt ter informatie aan de Stuurgroep van het RIEC aangeboden.

4.3 FG-statuut

Het FG-statuut bevat basisafspraken voor het gezamenlijk toezicht binnen het samenwerkingsverband. Het statuut biedt daarmee een kader voor nadere werkafspraken.
In het statuut is onder andere geregeld hoe de FG's gezamenlijk invulling geven aan hun toezichthoudende rol, welke coördinerende taken bij de cFG zijn belegd, de voorwaarden voor het kunnen uitoefenen van de FG-taken binnen het samenwerkingsverband en de verantwoordelijkheden van de deelnemers. Het FG-statuut strekt tot doel om op een uniforme en zorgvuldige manier toezicht uit te kunnen oefenen en de deelnemers te attenderen op hun verantwoordelijkheden.
De deelnemers blijven individueel verantwoordelijk voor:

- verwerkingen van persoonsgegevens, waaronder rechtmatigheid, uitvoering van DPIA's en het nemen van passende technische en organisatorische maatregelen;
- het beschikbaar stellen van voldoende middelen en budget voor de uitoefening van de FG- en cFG- taken;
- het tijdig en naar behoren informeren van de eigen FG over alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

In 2026 wordt de samenwerking verder geprofessionaliseerd door werkafspraken op papier te zettten.

4.4 Actiecentrum Veiligheid en Zorg (AcVZ)

De FG van gemeente Amsterdam is ook cFG voor het AcVZ. De FG is in de rol van cFG voornemens om met de FG's van de deelnemers ook voor het AcVZ een (c)FG-statuut op te stellen.

5. Extern onderzoek privacyorganisatie

Sinds 2018 hebben er veel veranderingen plaatsgevonden op maatschappelijke, juridische, organisatorische en technologische gebieden die invloed hebben en hebben gehad op de gegevensbescherming en zodoende ook op de taakuitoefening en capaciteit van de FG. In een memo aan de gemeentesecretaris (GS) en in gesprek met de wethouder ICT/Digitale Stad heeft de FG in 2024 aangegeven dat de werkzaamheden en de door de organisatie aan het FG-office toebedeelde capaciteit en middelen niet in verhouding tot elkaar staan; er komt dusdanig veel werk op de FG af dat continue prioritering van werkzaamheden noodzakelijk is terwijl de werkvoorraad blijft groeien. Er moeten keuzes worden gemaakt over wat wel en niet kan worden opgepakt. De GS heeft opdracht gegeven tot het laten uitvoeren van een extern onderzoek, waarbij de governance en formatie van de gehele privacyorganisatie inclusief het FG-office en de verhouding FG en de Commissie Persoonsgegevens Amsterdam (CPA) zijn onderzocht. De CIO is aangewezen als gedelegeerd opdrachtgever. Het onderzoek heeft in 2025 plaatsgevonden en in november 2025 is het eindrapport opgeleverd. Begin 2026 is het aangeboden aan het college van B&W en de raad.
De conclusies uit het rapport over capaciteit en onduidelijkheden in rollen en verantwoordelijkheden komen overeen met de constateringen en het signaal dat de FG in de memo aan de GS en in het vorig jaarverslag heeft geadresseerd. De FG verzoekt om de aanbevelingen uit het rapport op te volgen.

6. Vooruitblik

De toenemende digitalisering, de technologische ontwikkelingen en de snelle opkomst van AI zorgen voor grote uitdagingen en veranderingen. Adequate naleving en toezicht op het gebied van gegevensbeschermingsrecht vereist een zorgvuldig ingericht en uitvoerbaar proces, waarin vooraf de relevante risico's in kaart worden gebracht en de noodzakelijke mitigerende maatregelen worden getroffen.
De FG kan verschillende toezichtactiviteiten uitvoeren zoals toezichtbezoeken, systeemgericht toezicht, thematisch onderzoek en de beoordeling van risicoanalyses. Ook kan de FG signaleren wat niet goed is geregeld. Het is aan de organisatie om daar opvolging aan te geven en verantwoording over af te leggen. De gemeente opereert in het publieke domein en verwerkt voor de uitvoering van haar taken persoonsgegevens. Dit brengt een zorgplicht voor de gemeente met zich mee op basis waarvan zij wordt geacht om op de juiste wijze, volgens *de bedoeling* van wet- en regelgeving met deze persoonsgegevens om te gaan.
De FG hanteert het principe 'toezicht op maat': De basis is de beoordeling hoever de organisatie is in de toepassing en naleving van de wet en de focus in toezicht bepalen aan de hand van "behoefte". De FG merkt dat een aantal aanbevelingen uit het vorige jaarverslag zijn opgevolgd, maar dat de gemeente nog steeds een lange weg te gaan heeft in de toepassing en naleving van de AVG/Wpg. Er is sprake van "AVG-ongeletterdheid". Voor de (privacy)organisatie ligt er een grote uitdaging om bewustzijn te creëren en kennis over gegevensbescherming bij te brengen onder de medewerkers van de gemeente.

De FG heeft in het afgelopen jaar, mede door de onder de werkzaamheden beschreven aanleidingen, een beeld gekregen wat er zoal noodzakelijk is om te streven naar een goede gegevenshuishouding. De gemeente werkt intensiever samen met publieke en private partijen. Er zijn samenwerkingsverbanden en informatieknooppunten waarbinnen gegevens worden uitgewisseld. Het is van groot belang dat de gegevensuitwisselingen worden ingericht binnen de kaders van de AVG, de Wpg en specifieke wetgeving zoals de Wgs.
De FG bevordert en bewaakt binnen de gemeente de rechtmatige verwerking van persoonsgegevens en levert daarmee een belangrijke bijdrage aan de bescherming van de persoonlijke levenssfeer van onder andere de burgers. De FG zal in 2026 extra aandacht geven aan deze vormen van gegevensuitwisselingen.
De FG constateert dat voor de realisatie van een goede gegevenshuishouding,op z'n minst om de basis op orde te hebben, een aantal elementen noodzakelijk zijn zoals het verduidelijken van rollen en verantwoordelijkheden, eigenaarschap bij de verwerking van persoonsgegevens bij directies en verbinding en samenwerking tussen de verschillende disciplines zoals ook in het vorige jaarverslag is benadrukt.
De FG zal voor het komende jaar de nadruk leggen op het bevorderen van het draagvlak voor bewustwording voor de regels voor het verwerken van persoonsgegevens en toezien op de naleving van relevante wet- en regelgeving met het oog op het versterken van de compliance.
De FG zal de contacten met de verschillende directies verder versterken om meer zichtbaarheid en bewustwording te creëren. De FG zal het komende jaar de ingezette lijn vanuit het toezicht om de organisatie bewuster te maken in rol- en verantwoordelijkheidsverdeling doorzetten en de verbinding tussen de verschillende disciplines bevorderen. Wanneer de verbinding tussen de organisatieonderdelen is gerealiseerd en de rollen en verantwoordelijkheden in de toepassing en naleving van de

AVG/Wpg duidelijk zijn zal de FG zich meer toespitsen op proactief toezicht. Onder proactief toezicht verstaat de FG vooraf stimulerend en richtinggevend toezicht.
Tekort aan capaciteit bij het FG-office door ontwikkelingen op juridisch, organisatorisch, technologisch en maatschappelijk vlak, uitbreiding van taken met de cFG rol (door het externe onderzoek ook vastgesteld) zorgt ervoor dat de FG veelal reactief handelt. Het streven om meer toe te spitsen op proactief toezicht, zoals de FG als taakopvatting voor ogen heeft kan alleen vorm krijgen als het capaciteitsprobleem is opgelost.

Lijst van afkortingen

AcVZ	Actiecentrum Veiligheid en Zorg
AI	Artifficial Intelligence (Kunstmatige Intelligentie)
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
B&W	(College van) burgemeester en wethouders
Boa	Buitengewoon opsporingsambtenaar
BPA	Baseline Privacy Amsterdam
BpgboaBesluit politiegegevens buitengewoon opsporingsambtenaren	
DMC	Directie Middelen en Control
DPIA	Data Protection Impact Assessment /
DREP	Digitale Rechten, Ethiek en Privacy
DSenI	Digitale Strategie en Informatie
FG	Functionaris Gegevensbescherming
FIC	Fully in Control
GMT	Gemeentelijk Managementteam
GS	Gemeentesecretaris
JZ	Juridische Zaken
NOREANederlandse Orde van Register EDP-Auditors	
OOV	Openbare Orde en Veiligheid
PO	Privacy Officer
QAA	Quality Assurance Acceptatiecriteria
RIEC	Regionaal Informatie- en Expertisecentrum
THOR	Toezicht en Handhaving Openbare Ruimte
VTH	Veiligheid, Toezicht en Handhaving
V&OR	Verkeer en Openbare Ruimte
WGS	Wet Gegevensverwerkingen door Samenwerkingsverbanden
WOO	Wet Open Overheid
WPI	Werk, Participatie en Inkomen
Wpg	Wet politiegegevens