Gemeente Amsterdam

Jaarverslag Functionaris Gegevensbescherming 2024

Hatice Dogan



Inhoud

Managementsamenvatting 3
Inleiding 9
Leeswijzer 10

1 Werkzaamheden 11
Instrumenten 11
Register van verwerkingen 11
Data Protection Impact Assessments (DPIA's) 11
Datalekken 13
Rechten van betrokkenen 13
Klachten, vragen en signalen 14

2 Deel A: Algemene Verordening Gegevensbescherming 16
Bevindingen en aanbevelingen 16
Beleid 16
Regie op risico's 17
Rollen en verantwoordelijkheden 18
Bewustzijn 19
Technologie en innovatie 19
Audit Privacyfunctie 20

Deel B: Wet politiegegevens 21
Bevindingen en aanbevelingen 21
Reikwijdte 21
Governance 21
Audits 21
Maatregelen / Knelpunten 22
FG Toezicht 22

Vooruitblik 24
Lijst van afkortingen 25

Managementsamenvatting

Positionering

Sinds 2018 heeft de gemeente Amsterdam een Functionaris Gegevensbescherming (FG). De FG is de interne onafhankelijke toezichthouder op de gegevensverwerkingen van de gemeente Amsterdam als uitvoerder van de wettelijk opgedragen taken maar ook als werkgever. Dit is een verplichting op grond van de Algemene Verordening Gegevensbescherming (AVG) die in mei 2018 van kracht werd. Bij de reorganisatie van het i-domein is gekozen om de functie onder te brengen bij de directie Digitalisering Strategie en Innovatie (DS&I). Om de FG bij de uitvoering van de taken te ondersteunen is in 2018 ook een assistent FG toegevoegd aan het FG-office. De toenmalige FG is in maart 2023 uit dienst getreden en de functie is tot januari 2024 waargenomen door een tijdelijke FG. In die periode is onderzocht of de positionering van de FG binnen de organisatie in voldoende mate onafhankelijk was geborgd. Om te waarborgen dat de FG onafhankelijk kan opereren is gekozen om de huidige FG per 1 januari 2024 onder te brengen bij de directie Juridische Zaken (JZ). Functioneel valt de FG nu onder de gemeentesecretaris (GS). De P-verantwoordelijkheid is belegd bij de directeur JZ.

De FG merkt op dat de huidige formele positionering voldoende garantie biedt om onafhankelijk toezicht te kunnen uitoefenen.

Verantwoordelijkheden/rollen

Taken van de FG zijn beschreven in de AVG en in 2018 verder uitgewerkt in een intern document. Voor de goede taakuitoefening van de FG is het van groot belang om de organisatie goed te kennen. De FG heeft in het eerste jaar zoveel mogelijk een rondje langs de velden gedaan om de organisatie te leren kennen en naar verbinding gezocht. Zo heeft de FG onder andere presentaties gehouden in het gemeentelijk managementteam (GMT) en een aantal directies om bekendheid te geven over intern toezicht, de taakopvatting van de FG, rolverdeling in de organisatie met betrekking tot gegevensbescherming, en vooral om op te halen wat er binnen de organisatie leeft en wat de verwachtingen zijn. De FG heeft niet alleen op directieniveau gezocht naar verbinding, maar ook de link gelegd met de verschillende organisatieonderdelen die een ondersteunende en adviserende rol hebben in gegevensbescherming richting de directies.

De FG merkt op dat er bereidwilligheid is om gegevensbeschermingsregels in acht te nemen, maar dat juiste kennis en bewustzijn bij de lijndirecties ontbreekt. Er is veel ruis en onduidelijkheid in de rol- en verantwoordelijkheidsverdeling in de lijndirecties en wat zij van de privacyorganisatie (mogen) verwachten. De verantwoordelijkheid voor de verwerking van persoonsgegevens ligt bij de lijndirecties. De privacyorganisatie die centraal wordt aangestuurd vanuit de Vakgroep Digitale Rechten, Ethiek en Privacy (DREP) adviseert de lijndirecties in de toepassing en naleving van de AVG en maakt beleid.

De FG beveelt aan om meer bewustzijn te creëren binnen de lijndirecties om de rollen en verantwoordelijkheden te verduidelijken om zo ook de vrijblijvendheid en aannames over wie waarvan is te voorkomen.

De FG zal ook voor het komende jaar de ingezette lijn vanuit het toezicht, in samenwerking met de privacyorganisatie, doorzetten om de lijndirecties bewuster te maken in rol- en verantwoordelijkheidsverdeling en verder de verbinding zoeken. Wanneer de verbinding tussen de lijndirecties en de privacyorganisatie is gerealiseerd en de rollen en verantwoordelijkheden duidelijk zijn in de toepassing en naleving van de AVG zal de FG zich meer toespitsen op proactief toezicht. Onder proactief toezicht verstaat de FG vooraf stimulerend en richtinggevend toezicht.

Instrumenten FG

De FG geeft (on)gevraagd advies en houdt toezicht op de toepassing en naleving van de AVG en de Wet politiegegevens (Wpg). De FG heeft een aantal instrumenten om haar advies- en toezichtstaak te kunnen uitoefenen. Deze zijn klachten, vragen en signalen van de betrokkenen (bewoners, bezoekers, ondernemers en de medewerkers). Klachten, vragen en signalen van betrokkenen geven inzicht hoe de verwerkingen binnen de organisatie plaatsvinden en geven aanleiding om ongevraagd te adviseren en richting te geven. Gerichte vragen voor advies komen voornamelijk vanuit de privacy organisatie daar waar de privacy organisatie om een standpunt vraagt van de FG. Voor klachten van betrokkenen over verwerking van hun persoonsgegevens is er een klachtenloket. Betrokkenen vinden de gang naar de FG of de Autoriteit Persoonsgegevens (AP) wanneer de klachten niet naar hun tevredenheid worden afgehandeld. De AP heeft met de FG de afspraak om de klachten die bij de AP binnenkomen via de FG in de organisatie uit te zetten. Door deze werkwijze krijgt de FG inzicht in hoe er binnen de organisatie om wordt gegaan met gegevensbeschermingsregels en over de wijze waarop de klachten aanvankelijk door de organisatie al dan niet zijn afgehandeld. De meeste klachten, die zowel direct bij de FG of bij de AP zijn ingediend, gaan over het niet naar tevredenheid van de betrokkene afhandelen van inzage- en correctierecht, onrechtmatige verstrekking van persoonsgegevens aan derden en opvragen en registreren van persoonsgegevens. Onrechtmatige verstrekkingen van gegevens aan derden kunnen worden aangemerkt als datalek die (on) bedoeld niet zijn gemeld aan de AP.

Het is goed dat er een klachtenloket en een loket voor inzage- en correctierecht is. Bij de beantwoording van de klachten en inzage- en correctieverzoeken wordt de input door de lijndirecties geleverd. Wat opvalt bij de afhandeling van klachten en inzage- en correctieverzoeken is dat bij de lijndirecties inhoudelijke kennis en bewustzijn ontbreekt over gegevensbeschermingsregels.

De FG merkt op dat er in de toepassing en naleving van gegevensbeschermingsregels de gemeente een lange weg heeft te gaan en vraagt hiervoor bewustzijn en duidelijkheid te creëren in de lijndirecties. Bewustzijn dat persoonsgegevens, die worden verwerkt voor de uitvoering van de taken, voldoende en adequaat moeten worden beschermd. Het moet in het beenmerg van iedere medewerker zitten dat juist handelen bij verwerking van persoonsgegevens onontbeerlijk is. De FG beveelt aan om op reguliere basis voldoende aandacht te besteden voor bewustzijn om zo de "AVG-geletterdheid" te bevorderen.

De FG adviseert ook op de Data Protection Impact Assesments (DPIA). De uitvoering van een DPIA en de advisering daarop door de FG is verplicht voor hoog risicoverwerkingen. Om te bepalen of er hoog risicoverwerkingen zijn wordt de lijst gehanteerd die door de AP is opgesteld. De FG adviseert positief (mits) of negatief (mits) op de voorgenomen verwerking die in een DPIA is uitgewerkt. Het advies van de FG is zwaarwegend, dat wil zeggen dat de organisatie van het advies mag afwijken mits duidelijk en goed gemotiveerd.

In de DPIA worden de risico's in kaart gebracht waarvoor maatregelen moeten worden getroffen met een actiehouder en tijdpad voor de acties. De DPIA's geven inzicht in de verwerkingen en zijn opvraagbaar door de betrokkenen, de AP en in het kader van de Wet open overheid (Woo). In principe kunnen de DPIA's actief openbaar gemaakt worden om als organisatie transparantie te verschaffen in de wijze waarop de verwerking plaatsvindt. Het niet opvolgen van een negatief (mits) advies kan aanleiding geven tot klachten, signalen en vragen die vervolgens aanleiding kunnen geven tot een (handhavings-)onderzoek door de AP.

De FG merkt op dat, in het geval de FG negatief adviseert, niet duidelijk is of het advies wordt opgevolgd en hoe de vervolgprocedure verloopt. Hierdoor kan risico ontstaan voor de betrokkenen en de organisatie. Vaak is niet duidelijk op welke wijze de risico's worden geadresseerd, welke risico's er al dan niet worden geaccepteerd en wat de gevolgen kunnen zijn voor de organisatie en de betrokkenen wier gegevens worden verwerkt.

De FG heeft geadresseerd dat de kwalificatie van de risico's niet op een uniforme wijze geschiedt. De verschillende disciplines (privacyorganisatie, informatiebeveiliging, informatiebeheer, lijndirecties), die een bijdrage leveren aan de totstandkoming van een DPIA voor het adresseren van de risico's en de daartegenover staande maatregelen, staan niet in voldoende mate in verbinding met elkaar om de juiste input te leveren.

De FG adviseert om duidelijk/inzichtelijk te maken op welke wijze de risico's worden geadresseerd, hoe de risicoacceptatie plaatsvindt en de escalatieladder eruitziet. Hiervoor is verbinding tussen de verschillende disciplines (privacyorganisatie, informatiebeveiliging, informatiebeheer en lijndirecties) onontbeerlijk. Wel merkt de FG op dat de genoemde disciplines inmiddels initiatieven hebben genomen om dit inzichtelijk te maken.

Ontwikkelingen

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. Hieronder een opsomming van de veranderingen die van invloed zijn op de werkwijze, capaciteit en de taakopvatting van de FG:

- Sinds 2022 hoort toezicht op de toepassing en naleving van de Wpg ook tot het takenpakket van de FG. Advisering en toezicht op de toepassing en naleving van de Wpg is een aanzienlijke uitbreiding in de taken van de FG.
- Per 1 maart 2025 is de Wet gegevensverwerking samenwerkingsverbanden (WGS) in werking getreden. WGS maakt gegevensdeling tussen de deelnemers binnen samenwerkingsverbanden zoals het Actiecentrum Veiligheid en Zorg (“AcVZ”) en de Regionale Informatie- en Expertisecentra (RIEC’s) mogelijk. Eén van de vereisten van de WGS voor toezicht op de gegevensverwerkingen binnen de samenwerkingsverbanden, naast de taken die in de AVG zijn genoemd, is dat door de deelnemers een coördinerend FG wordt aangewezen. Wat de coördinerende rol inhoudt beschrijft de WGS niet. De FG van de gemeente Amsterdam is aangewezen als coördinerend FG onder de voorwaarde dat er extra capaciteit aan het FG-office wordt toegevoegd en er een reglement wordt opgesteld om de coördinerende rol te verduidelijken.
- De gemeente wil efficiënt en dienstverlenend zijn richting de burger. Ook wil de gemeente bij preventie en handhaving effectief zijn. De toenemende digitalisering en de technologische ontwikkelingen bieden hiervoor ruimte. Zodoende nemen de toepassing van algoritmes en AI gerelateerde technieken snel toe met als doel efficiëntie te bieden in de dienstverlening en effectief te zijn in de preventie en handhaving bij de uitvoering van de taken van de gemeente als dienstverlener, maar ook als werkgever. Dat betekent dat de FG veel aan kennisvergaring moet doen; ontwikkelingen op de voet volgen om de verwerking van persoonsgegevens die binnen de technologische toepassingen plaatsvinden op juistheid, rechtmatigheid en in ieder geval langs de beginselen van de AVG te kunnen toetsen.
- Ontwikkelingen in de organisatie hebben ook een grote invloed op de taken en verantwoordelijkheden van de FG. De privacy organisatie heeft sinds 2023 een grote vooruitgang geboekt. Echter, het aantal Privacy Officers (PO), ondergebracht in de vakgroep DREP bij DS&I met centrale aansturing, die een helpende hand kunnen bieden aan de directies bij de toepassing en de naleving van de AVG/Wpg is niet op het juiste capaciteitsniveau om te kunnen voorzien in de behoefte van de directies. PO’s fungeren als een link tussen de FG en de directies en zijn een informatiebron voor de FG.

Naast het adviseren in de toepassing en naleving van de AVG/Wpg wordt het stedelijk beleid met betrekking tot AVG/Wpg gerelateerde onderwerpen ook vanuit de vakgroep DREP geïnitieerd, zoals beleid met betrekking tot rechten van betrokkenen (informatieplicht, inzage- en correctierecht), datalekken, schadevergoeding, klachten, uitvoeren van DPIA's. De FG merkt op dat er met betrekking tot een aantal onderwerpen vanwege capaciteitsgebrek geen beleid was/is dan wel niet is geactualiseerd. De FG heeft daar waar geen beleid was/is dan wel beleid moest worden opgesteld gesignaleerd en voor de totstandkoming van beleid de helpende hand geboden.

- De lijndirecties werken verschillend in de toepassing en naleving van de AVG/Wpg. De FG merkt op dat klachten, vragen en signalen van burgers en medewerkers verschillend worden afgehandeld door de organisatieonderdelen. Vooral de communicatie richting de burger maar intern ook richting de medewerker vereist eenduidigheid, zowel inhoudelijk als de wijze waarop. Gegevensbescherming is een generiek onderwerp en het is van belang dat binnen de organisatie eenduidigheid is in de toepassing en naleving van gegevensbeschermingsregels. De FG merkt op dat met name de rollen en verantwoordelijkheden niet duidelijk zijn en de verbinding tussen de organisatieonderdelen ontbreekt. De FG streeft samen met de privacy organisatie naar eenduidigheid in de toepassing en naleving van de AVG/Wpg, besteedt veel tijd en aandacht om de gewenste eenduidigheid te bereiken en heeft verbinding gezocht om bewustzijn te creëren met betrekking tot rollen en verantwoordelijkheden.

De FG heeft in een notitie de ontwikkelingen die gevolgen hebben en hebben gehad op de capaciteit van het FG-office beschreven. De FG heeft deze ontwikkelingen met verschillende stakeholders, GS en de verantwoordelijke bestuurder voor de privacy organisatie besproken. De beschreven ontwikkelingen leggen niet alleen capaciteitsdruk op het FG-office maar ook op de privacy organisatie. De besprekingen hebben geresulteerd in een opdrachtbrief voor extern onderzoek.

Taakopvatting FG / Vooruitblik

De FG dient als interne onafhankelijke toezichthouder een signalerende functie te hebben op de toepassing en naleving van de AVG/Wpg. Dus niet alleen achteraf toetsen of er voldaan wordt aan de eisen die de wet stelt, maar aan de voorkant adviseren, stimulerend toezicht uitoefenen. Primaire verantwoordelijkheid voor de toepassing en naleving ligt bij de organisatie. Vanuit de privacyorganisatie wordt een helpende hand geboden in de toepassing en naleving. De FG merkt op dat de verbinding binnen de organisatie in de implementatie van regelgeving niet voldoende is. In ieder geval streeft de FG ernaar een proactieve rol te vervullen om de organisatie te attenderen om verantwoordelijkheden die voortvloeien uit de wet- en regelgeving volgens de *bedoeling* te vervullen. Uiteindelijk gaat het om het waarborgen van de rechten en vrijheden van betrokkenen wier gegevens de gemeente verwerkt. Het is van groot belang

om zorg te dragen voor een goede gegevenshuishouding. Om de basis op orde te hebben is *goed huisvaderschap* onontbeerlijk. Dat betekent continu investeren in programma's voor bewustzijn en geletterdheid in de AVG/Wpg.

Om proactief te kunnen werken, stimulerend en vooraf toezicht te kunnen uitoefenen is goede organisatiekennis onontbeerlijk. De FG zal zich ook voor het komende jaar inzetten voor bewustwording binnen de organisatie en zorgen dat de verbinding tussen de disciplines en de rol- en verantwoordelijkheidsverdeling wordt gerealiseerd. De FG merkt op dat in de huidige omstandigheden, gegeven de capaciteit, proactief toezicht op zich laat wachten en voorlopig enkel vraaggestuurd adviseren en achteraf toezicht houden mogelijk is.

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. AVG is een dergelijke wet waarin bepaalde normen zijn opgenomen die in acht moeten worden genomen door de verwerkingsverantwoordelijke, zoals de gemeente, bij het verwerken van persoonsgegevens. Bij het uitoefenen van haar taken verwerkt de gemeente *als bestuursorgaan maar ook als werkgever* veel persoonsgegevens. Inwoners, 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, de burgemeester als de gemeenteraad.

In de AVG en de Wpg wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. De FG is de interne onafhankelijke toezichthouder voor verwerkingen van persoonsgegevens en brengt jaarlijks een verslag uit. In dit jaarverslag biedt de FG inzicht in de werkzaamheden, middelen voor toezicht en advisering, interne en externe ontwikkelingen en de taakopvatting van de FG. Daarnaast geeft FG haar bevindingen en focus voor het komende jaar weer en doet aanbevelingen.

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 de instrumenten die de FG ter beschikking heeft om invulling aan haar advies- en toezichtrol te kunnen geven. Hierin zijn de cijfers over 2024 opgenomen en toegelicht. Hoofdstuk 2 geeft de bevindingen en aanbevelingen met betrekking tot de AVG en de Wpg weer. Het jaarverslag wordt afgesloten met een vooruitblik waarin ook het jaarplan van de FG wordt gepresenteerd.

1 Werkzaamheden

De FG is onder andere belast met informeren, signaleren, (on) gevraagd adviseren en toezien op de naleving van gegevensbeschermingsregels. De taken van de FG zijn beschreven in de AVG en Wpg. Voor de uitoefening van haar taken heeft de FG een aantal instrumenten die helpen in de signalering, advisering en toezicht. Instrumenten die de FG helpen bij haar taakuitoefening zijn onder andere; het register van verwerkingen, DPIA's, datalekken, vragen, klachten, signalen en beleid. Ook verzoeken vanuit de AP die in 2024 zijn binnengekomen hebben een belangrijke bijdrage geleverd in het krijgen van inzicht over naleving van gegevensbeschermingsregels en hebben zodoende geleid tot het adresseren van nakomingsverplichtingen binnen de organisatie. Door deze instrumenten krijgt de FG een beeld van de onderwerpen die spelen binnen de organisatie, bij medewerkers en burgers.

Hieronder gaat de FG in op de instrumenten, geeft haar bevindingen, deelt de verkregen inzichten en adresseert de risico's.

Instrumenten

Register van verwerkingen

In een verwerkingsregister staat informatie over de persoonsgegevens die een organisatie verwerkt. Alle organisaties die persoonsgegevens verwerken zijn verplicht zo'n register op te stellen. Hiermee voldoet de organisatie onder andere aan haar informatieplicht. De gemeente kiest ervoor om het register te publiceren op de website. Tweemaal per jaar wordt een geactualiseerde versie gepubliceerd.

De FG constateert dat betrokkenen het register raadplegen en contact opnemen met de FG naar aanleiding van vragen of klachten met betrekking tot het register. Het is van belang om het register actueel en juist te houden en dat de lijndirecties daaraan meewerken.

Data Protection Impact Assessments (DPIA's)

In de AVG is de verplichting opgenomen voor organisaties om een DPIA uit te voeren bij bepaalde gegevensverwerkingen met een hoog risico en aan de FG voor te leggen voor advies. Het advies van de FG is zwaarwegend van aard. Bij afwijking van het advies moet de organisatie goed motiveren waarom het advies niet wordt opgevolgd. Het tijdig 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 juiste grondslag is en of er voldoende technische en organisatorische maatregelen worden genomen in geval van risico's, wie de actiehouders zijn en binnen welk tijdspad de realisatie plaatsvindt.

De FG constateert dat binnen verschillende lijndirecties vaak discussies plaatsvinden over verwerkingen waarvoor een DPIA uitgevoerd dient te worden. Die discussies zorgen voor vertraging terwijl het DPIA-proces goed is beschreven, er duidelijke richtlijnen zijn wanneer er wel of geen DPIA moet worden uitgevoerd en vanuit de privacyorganisatie hierin duidelijk wordt geadviseerd. In sommige gevallen ontbreekt de capaciteit om tijdig DPIA's uit te voeren, in andere gevallen ontbreekt het bewustzijn van de noodzaak hiertoe binnen de lijndirecties.

Het is van groot belang om tijdig een DPIA uit te voeren voor een voorgenomen verwerking en de juiste disciplines hierbij te betrekken.

DPIA's zijn opvraagbaar door middel van verzoeken op grond van de Wet Open Overheid (Woo) en door de betrokkenen. Het komt ook voor dat de AP in het kader van onderzoeken naast andere documentatie ook de DPIA's opvraagt. De AVG legt de verantwoordelijkheid *'accountability'* bij de organisatie neer.

De FG heeft geconstateerd dat in het DPIA-proces veel discussies ontstaan met betrekking tot advisering en verwachtingen. Vaak wordt het advies van de privacyorganisatie om een DPIA uit te voeren genegeerd dan wel in twijfel getrokken door de lijndirecties.

De FG wijst erop dat tijdig starten met een DPIA voor een voorgenomen verwerking van groot belang is. Het volgen van het DPIA-proces waarbij de verschillende disciplines vanuit hun rol hun bijdrage leveren is essentieel voor de kwaliteit. Een goed uitgevoerde DPIA biedt inzicht in de gegevenshuishouding van de organisatie en waar er eventuele verbeterpunten zijn. De FG heeft richtlijnen aangegeven waaraan een DPIA inhoudelijk en kwalitatief aan moet voldoen en dit besproken met besproken met de vakgroep DREP (Privacy) en Informatiebeveiliging.

In 2024 zijn 84 DPIA's aan de FG voorgelegd ter advies. Niet alle DPIA's konden van advies worden voorzien. Er zijn 59 DPIA's in behandeling genomen. Dit komt met name doordat in december een groot aantal DPIA's is binnengekomen (17). Een andere reden is de beperkte capaciteit binnen het FG-office. Ook de kwaliteit van de uitgevoerde DPIA's heeft in sommige gevallen voor vertraging in de advisering gezorgd. Als er onduidelijkheden blijven bestaan over de verwerking, neemt het advies meer tijd in beslag. Ook is het proces in deze gevallen arbeidsintensiever voor zowel de organisatie als de FG. Van de 59 DPIA's die in 2024 in behandeling zijn genomen zijn 26 DPIA's van advies voorzien. Voor 33 DPIA's is aanvullende informatie benodigd alvorens de FG kan adviseren.

De FG adviseert in de meeste gevallen positief, al dan niet na aanpassing of aanvullende maatregelen om risico's te mitigeren. In twee gevallen is *negatief* geadviseerd op een deel van de verwerkingen en in één geval op de gehele verwerking. In het geval de organisatie besluit om af te wijken van een negatief advies, dat wil zeggen, het risico accepteert, dan dient risicoacceptatie formeel te worden vastgelegd.

De FG merkt op dat een eenduidig beleid voor risicoformulering en risicoacceptatie ontbreekt en heeft dit geadresseerd. Er wordt nu gewerkt aan het ontwikkelen van beleid en een proces voor risicoacceptatie.

De directie waar de verwerking (hoofdzakelijk) plaatsvindt, is verantwoordelijk voor het implementeren van maatregelen en om eventuele risico's te mitigeren. Monitoring en een centraal risicoregister zijn noodzakelijk om goed regie te kunnen voeren op risico's en de opvolging van maatregelen. In 2024 zijn stap-

pen gezet om DPIA's en geïdentificeerde risico's in de applicatie Fully In Control (FIC) te registreren.

De FG merkt op dat het risicoregister dat op deze manier ontstaat en waarop gemonitord kan worden, nog niet volledig is. Er worden stappen gezet om een volledig overzicht in FIC te bewerkstelligen.

Datalekken

In 2024 zijn 291 incidenten gemeld die door de organisatie zijn aangemerkt als datalek. In 40 gevallen is geoordeeld dat het datalek meldenswaardig was en is een melding gemaakt bij de 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 signaal af te geven aan de organisatie, of om verder onderzoek te doen met het oog op het voorkomen van datalekken in de toekomst. In onderstaande tabel is het aantal in 2024 geregistreerde datalekken gecategoriseerd weergegeven.

De FG merkt op dat er heel weinig datalekken worden gemeld. Dit kan het gevolg zijn van onbekendheid en bewustzijn binnen de organisatie met betrekking tot wat wel en niet als datalek moet worden aangemerkt. De FG vraagt om hiervoor continu bewustzijn te creëren. Door datalekken te onderkennen kan inzicht ontstaan in de gegevenshuishouding van de organisatie. Met inzicht in de gegevenshuishouding kan de basis eerder op orde worden gebracht.

Datalekken	
Categorie	**Aantal**
Verlies/diefstal device	109
E-mail aan foute ontvanger	43
Post aan foute ontvanger	31
Persoonsgegevens in verkeerd dossier	16
Verkeerde autorisatie(s)	15
Persoonsgegevens gepubliceerd	13
Verlies/diefstal papier	9
E-mail via CC i.p.v. BCC	9
Hacking, malware, phishing	8
Verkeerde persoonsgegevens klantportaal	3
Door storing geen persoonsgegevens	1
Post kwijtgeraakt	1
Overig	33

Rechten van betrokkenen

Het Loket Persoonsgegevens coördineert verzoeken over de verwerking van persoonsgegevens op grond van de AVG. In

2024 zijn in totaal 287 verzoeken gedaan, waarvan er 259 (90,2%) daadwerkelijke AVG-verzoeken waren. De overige 28 verzoeken zijn beoordeeld als niet zijnde AVG. Net als eerdere jaren vormen inzageverzoeken het grootste gedeelte van de AVG-verzoeken, gevolgd door verwijderverzoeken. De meeste AVG-verzoeken zijn voor meerdere directies bestemd.
De gemiddelde doorlooptijd van de afhandeling van een AVG-verzoek was in 2024 41 dagen. De wettelijke termijn is één maand. Door te verdagen kan de wettelijke termijn worden verlengd met nog eens twee maanden. De verdaging dient gemotiveerd te zijn.

De FG merkt op dat de coördinerende rol van het Loket persoonsgegevens enkel bestaat uit het doorgeleiden van de verzoeken naar de juiste directie en vervolgens de reactie vanuit de directie richting de betrokkene. De FG heeft geconstateerd dat de directies verschillend omgaan met de inhoudelijke afhandeling van de verzoeken en de wijze van communicatie richting de burger.

De FG adviseert om eenduidig te handelen in de afhandeling van de verzoeken en communicatie richting de burger. De FG heeft dit onder de aandacht gebracht. Inmiddels zijn er vanuit de vakgroep DREP in overleg met het Loket en de FG richtlijnen opgesteld.

Klachten, vragen en signalen
Contactgegevens van de FG zijn te vinden op de website van de gemeente. Dit is ook verplicht. Dit betekent dat eenieder contact kan opnemen met de FG voor vragen en opmerkingen. Er komen jaarlijks veel vragen, signalen maar ook klachten van betrokkenen met betrekking tot verwerking van persoonsgegevens binnen bij de FG. De FG beantwoordt vragen en klachten en zet deze waar nodig uit binnen de organisatie. Het schetst een beeld van de aard en de onderwerpen waar betrokkenen tegenaan lopen. De FG gebruikt deze informatie onder andere ook om een signaal af te geven aan de organisatie. In 2024 zijn 21 klachten bij de FG binnengekomen. De meeste klachten gaan over gegevensverstrekking aan derden, inzage- en correctieverzoeken en eventuele bovenmatige registratie van persoonsgegevens.

De FG merkt op dat er voor het indienen van klachten een stedelijk klachtenproces is en dat in dit proces een specifieke paragraaf voor klachten met betrekking tot verwerking van persoonsgegevens ontbreekt. De FG heeft hierover een signaal gegeven en is in gesprek gegaan met de organisatie. Het proces is inmiddels aangepast.

Betrokkenen dienen ook klachten in bij de AP in het geval zij 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 2024 heeft de

AP contact opgenomen met de FG over een aantal klachten met betrekking tot de verwerking van persoonsgegevens door de gemeente. Ook heeft de AP vragen gesteld aan de gemeente in het kader van een themaonderzoek met betrekking tot onrechtmatige inzage in persoonsgegevens door ambtenaren en middels een themastudie over het proces en risicobeheersing inzet AI-systemen voor parkeerhandhaving. De organisatie heeft de vragen van de AP beantwoord. De AP heeft de onderzoeksresultaten nog niet gecommuniceerd. Casusgerichte klachten zijn afgehandeld en teruggekoppeld aan de directie waar nodig om verder op te pakken.

De FG merkt op dat de binnengekomen klachten inzicht bieden in de gegevenshuishouding van de organisatie. Zo is te zien dat bewustzijn ontbreekt bij gegevensverstrekking aan derden en gegevensbeschermingsregels bij verstrekking van gegevens vaak niet voldoende in acht worden genomen. Dit brengt risico's met zich mee. De FG constateert onduidelijkheid over waar een verzoek tot gegevensverstrekking door een derde organisatie binnen moet komen. Er is geen proces aan welke eisen een verzoek van de derde organisatie moet voldoen, door welke disciplines binnen de gemeente het verzoek van de derde organisatie moet worden getoetst voor vertrekking van gegevens.

De FG adviseert het proces over gegevensverstrekking aan derde partijen duidelijk te maken en te communiceren in de organisatie.

2 Deel A: Algemene Verordening Gegevensbescherming

Bevindingen en aanbevelingen

Beleid

Stedelijk beleidskader

Het huidig stedelijk kader (*Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam*) is vastgesteld in 2018, kort nadat de AVG van kracht werd. Ontwikkelingen op onder andere maatschappelijk, juridisch en technologisch vlak vragen om een beleidskader dat aansluit bij de actualiteit. In 2024 is gestart met het actualiseren van het stedelijk beleidskader. Een stedelijk beleidskader met een heldere visie is richtinggevend voor beleid en kaders met betrekking tot verwerkingen van persoonsgegevens.

Aanbeveling: draag zorg voor vaststelling van geactualiseerd stedelijk beleidskader, met inbegrip van voornoemde elementen.

Beleidskaders privacy

In het afgelopen jaar is door de vakgroep DREP beleid ten aanzien van verschillende onderwerpen gericht op gegevensbescherming geactualiseerd of ontwikkeld. De FG heeft hierin een stimulerende en/of adviserende rol gespeeld.

Rechten van betrokkenen

Het Loket Persoonsgegevens coördineert verzoeken van personen die een beroep doen op de rechten en vrijheden uit de AVG. In veruit de meeste gevallen gaat het hierbij om inzageverzoeken. De procedure voor de coördinerende taken is geactualiseerd. De verantwoordelijkheid voor de inhoudelijke behandeling van verzoeken ligt bij de directies. De FG constateert inconsistentie in de wijze waarop directies verzoeken behandelen en dat deze inconsistentie leidt tot vragen en klachten van betrokkenen. Er bestaat, met name op het gebied van inzageverzoeken, veel jurisprudentie die richtinggevend kan zijn in het beleid dat de gemeente vaststelt voor de behandeling van inzageverzoeken. In 2024 zijn stappen gezet om het beleid voor de inhoudelijke behandeling te actualiseren en meer consistentie op stedelijk niveau te bewerkstelligen. Het aangescherpte beleid wordt in 2025 geëffectueerd.

Datalekken

In 2024 is de datalekkenprocedure geactualiseerd. De vakgroep DREP is eigenaar van het meldpunt datalekken. Dit meldpunt is de centrale plek waar datalekken worden gemeld. Na melding worden deze datalekken door een Privacy Officer behandeld. Het is essentieel om de werkwijze procedureel vast te leggen zodat de beoordeling en de afhandeling op correcte en consistente wijze gebeurt. De datalekkenprocedure en werkinstructies zijn herzien en worden vastgesteld.

Quality Assurance Acceptatiecriteria

Door middel van voldoen aan de door de organisatie opgestelde Quality Assurance Acceptatiecriteria (QAA), zorgt de organisatie ervoor dat initiatieven voldoen aan Europese, landelijke en Amsterdamse wet- & regelgeving, bezien vanuit verschillende disciplines.

Privacy Quick Scan

De organisatie gebruikt verschillende producten om risico's te identificeren. De Privacy Quick Scan, bedoeld om in kaart te brengen of persoonsgegevens verwerkt worden en of er ten aanzien hiervan risico's bestaan. De Privacy Quick Scan wordt ingezet als onderdeel van de QAA, het beheerskader waarmee de gemeente compliance-risico's in kaart brengt. De Privacy Quick Scan is in 2024 doorontwikkeld.

Data Protection Impact Assessments
Het proces met betrekking tot het uitvoeren van DPIA's is tevens doorontwikkeld, waaronder het template voor de uitvoering ervan. De FG heeft de verwachtingen die zij heeft, de rollen en verantwoordelijkheden in de uitvoering van een DPIA en de procedure met betrekking tot voorleggen van een DPIA aan de FG verduidelijkt. Om geïdentificeerde risico's op juiste wijze en consistent te beoordelen dan wel classificeren, is samen met informatiebeveiliging en informatiebeheer ingezet op een standaardisering van risico-classificatie.

Regie op risico's
Baseline Privacy Amsterdam
De Baseline Privacy Amsterdam (BPA) is een initiatief van de vakgroep DREP om op stedelijk- en directieniveau inzichtelijk te maken in hoeverre de gemeente voldoet aan de eisen die de gegevensbeschermingsregels aan haar stelt. Het doel van de BPA is om de bescherming van persoonsgegevens van de betrokkenen beter te kunnen borgen. De BPA is een blijvend programma dat zal resulteren in verbeterplannen voor de directies als onderdeel van een Plan-Do-Check-Act (PDCA) cyclus.

De initiële BPA uitvraag is voor de meeste directies in gang gezet en door verschillende directies zijn deze uitvragen inmiddels gevalideerd. Het is de verwachting dat deze validatieronde medio 2025 zal zijn afgerond. Vanaf de tweede helft van 2025 zal per directie een PDCA-cyclus ingericht worden om de geïdentificeerde risico's te kunnen mitigeren.

De FG merkt op dat een goede uitvoering van de BPA inzicht zal bieden over de toepassing en naleving van gegevensbeschermingsregels.

Fully In Control
De resultaten uit de BPA worden opgenomen in Fully In Control (FIC), de governance, risk en compliance (GRC) software die door de gemeente is aangekocht. Door de resultaten op te nemen in FIC kan de organisatie op de resultaten (risico's)monitoren en hierop sturen.

Ook is in het afgelopen jaar ingezet op het opnemen van DPIA's in FIC. Door het registreren van risico's en daaraan gekoppelde mitigerende maatregelen ontstaat een risicoregister op stedelijk niveau waarop de organisatie kan monitoren en sturen.

De FG constateert uit gesprekken met gebruikers en de stand van zaken met betrekking tot implementatie van de software dat de ontwikkeling en inzet van de tool tot op heden achterblijven bij de ambitie en de mogelijkheden die de software kan bieden op het gebied van de bescherming van persoonsgegevens. Implementatie en doorontwikkeling van de software is

nodig om de gebruiksvriendelijkheid en de effectiviteit ervan te vergroten.

Risicoacceptatie
Risico's kunnen niet altijd voldoende gemitigeerd worden en in sommige gevallen kiest de organisatie ervoor om een voorgenomen verwerking toch door te laten gaan. In dat geval is het aan de organisatie om het risico te accepteren. De FG merkt op dat er geen stedelijk beleid is in het kader van risicoacceptatie. Het is belangrijk om in kaart te brengen welke risico's worden geaccepteerd, onder welke voorwaarden risico's geaccepteerd worden en wie verantwoordelijk is voor het accepteren van de risico's (wie dient te zijn geïnformeerd en wie tekent voor de risico's?).

De FG adviseert om consistentie aan te brengen door een proces op te stellen op stedelijk niveau. Hieraan wordt momenteel gewerkt.

Rollen en verantwoordelijkheden
Heldere rollen en duidelijk belegde verantwoordelijkheden zijn voorwaarden om goed samen te werken. Ook met betrekking tot rollen en verantwoordelijkheden geeft de FG een signaal af. Binnen de organisatie is onvoldoende helder waar wie welke rol heeft met betrekking tot de bescherming van persoonsgegevens, hoe verantwoordelijkheden belegd zijn en welke consequenties deze rollen en verantwoordelijkheden met zich meebrengen.

FG heeft zich in het afgelopen jaar met name ingezet om verbinding te realiseren tussen de verschillende disciplines en bewustzijn te creëren voor verantwoordelijkheids- en rolverdeling en zal de ingezette lijn het komende jaar doorzetten.

'Three Lines of Defense' model
Het is van belang dat de organisatie dusdanig is ingericht dat bescherming van persoonsgegevens adequaat is geborgd. De organisatie werkt volgens het 'three lines of defense' model. Privacy contactpersonen binnen de verschillende directies vormen de eerste lijn, daarmee zijn zij aanspreekpunt voor medewerkers binnen de directies. De privacy officers (PO's) vormen de tweede lijn, zij adviseren en helpen directies met privacyvraagstukken. De FG vormt de derde lijn. Om goed samen te werken is het van belang dat de verschillende disciplines elkaar weten te vinden om zodoende vanuit de eigen rol te acteren. Binnen de directies is vaak onduidelijk wie verantwoordelijkheid draagt voor een bepaalde gegevensverwerking. Het is van groot belang om het eigenaarschap voor gegevensverwerkingen binnen de directies duidelijk te beleggen.

De FG merkt op dat privacy, informatiebeveiliging, informatiebeheer als generieke onderwerpen in het verlengde van elkaar staan en dat verbinding en samenwerking onontbeerlijk is. De FG adviseert om eigenaarschap binnen de directies voor gegevensverwerkingen duidelijk te beleggen. Inmiddels zijn hiervoor concrete stappen gezet.

Bewustzijn
Een andere randvoorwaarde voor verantwoord omgaan met persoonsgegevens is het privacybewustzijn van 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 benodigd zijn.

De FG geeft een signaal af met betrekking tot de 'AVG-geletterdheid' van de organisatie en adviseert een bewustwordingscampagne gericht op alle medewerkers en aanvullende specifieke kennis aan te bieden gericht op de functie die medewerkers hebben. Een adequaat kennisniveau bij alle medewerkers is onontbeerlijk. Kennisniveau op peil houden kan bijvoorbeeld door een e-learning module, specifieke privacy-training afgestemd op functie en verantwoordelijkheden. Onderzoek welke middelen hiervoor geschikt zijn en stel vast wie welke aanvullende kennis nodig heeft.

Technologie en innovatie
De gemeente wil efficiënt en dienstverlenend zijn richting de burger. Ook wil de gemeente bij preventie en handhaving effectief zijn. De toenemende digitalisering en de technologische ontwikkelingen bieden hiervoor ruimte. Zodoende nemen de toepassing van algoritmes en AI gerelateerde technieken snel toe met als doel efficiëntie te bieden in de dienstverlening en effectief te zijn in de preventie en handhaving bij de uitvoering van de taken van de gemeente als dienstverlener, maar ook als werkgever.

Algoritmen en Artificial Intelligence (AI)
Op 1 augustus 2024 is de AI-Verordening in werking getreden. De verschillende onderdelen in de verordening worden gefaseerd van toepassing. In 2024 is ook de Amsterdamse Visie op AI vastgesteld. De visie is in samenwerking met inwoners van de gemeente Amsterdam tot stand gekomen. De visie zet de mens centraal: *"We geloven dat technologie mensen moet helpen, niet andersom. We willen dat AI echte maatschappelijke waarde toevoegt en het leven beter maakt".* Daarnaast is het beleid van de gemeente omtrent AI volop in ontwikkeling en in 2025 volgt de AI-agenda. De gemeente werkt aan innovatie enerzijds en werkt anderzijds aan beleidskaders en waarborgen om nieuwe technieken verantwoord in te zetten. Binnen de vakgroep DREP zijn ook compliance kaders voor algoritmen en AI gerealiseerd. Zo zijn er Algoritmen en AI Compliance Officers en Digitale Rechten en Ethiek Officers die de organisatie helpen bij het voldoen aan de AI Act.

De FG onderstreept het belang en noodzaak van AI-geletterdheid binnen de organisatie.

Digitale autonomie
De gemeente is afnemer van diensten van (Amerikaanse) technologiebedrijven. Voorbeelden hiervan zijn applicaties voor de online werkomgeving van Microsoft en Azure, de clouddienst van Microsoft. Steeds regelmatiger zijn kritische geluiden te horen over de mate waarin de overheid, waaronder gemeenten, afhankelijk zijn van *'big tech'.* Zowel vanuit de politiek als in het maatschappelijk debat. Als gevolg hiervan legde de staatssecretaris

van Digitalisering de cloudmigratie van rijksoverheidsgegevens stil. Ook binnen de gemeente is de digitale autonomie onderwerp van gesprek.

Hoog vertrouwelijke landingszone van het dataplatform
De organisatie heeft in 2024 gewerkt aan migratie van applicaties en (persoons)gegevens naar de cloudomgeving. Ook hiervoor denkt de gemeente na over passende waarborgen. De gemeente werkt samen met Microsoft om als eerste organisatie in Nederland aan het beveiligen van gegevens op een wijze waardoor Microsoft geen toegang heeft tot gevoelige (persoons-) gegevens. Naast beveiliging van gegevens is beschikbaarheid van gegevens van groot belang.

De FG merkt op dat in het kader van digitale autonomie en continuïteit van belang is dat er een continuïteit strategie maar ook een exit strategie is.

Audit Privacyfunctie
In 2024 is directie Middelen en Control (DMC) gestart met een interne audit op de privacyfunctie. De doelstelling van deze audit is het bieden van inzicht in hoeverre de inrichting van de privacy functie binnen de gemeente Amsterdam op strategisch en tactisch niveau voldoende borging biedt voor naleving van de AVG en de voorschriften van de AP. Het uiteindelijke doel is daarbij vooral gericht op het identificeren van eventuele tekortkomingen of knelpunten die de effectiviteit van deze borging kunnen beïnvloeden, om zodoende aanbevelingen te doen voor verdere optimalisatie van de privacyfunctie. Tijdens de audit wordt nagegaan of voldoende beheersmaatregelen aanwezig zijn in verhouding tot de aanwezige risico's. Hierbij wordt niet alleen gekeken naar meetbare en tastbare maatregelen zoals procedures en werkinstructies (hard controls), maar ook naar het gedrag van medewerkers en de cultuur binnen het team (soft controls).

De centrale vraag in de audit luidt: "In welke mate biedt de inrichting van de privacy functie in de gemeente op strategisch en tactisch niveau voldoende borging voor naleving van de AVG en de voorschriften van de AP?" De resultaten van de audit worden in het tweede kwartaal van 2025 verwacht.

Deel B: Wet politiegegevens

Bevindingen en aanbevelingen

Reikwijdte

De 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, Koninklijke Marechaussee (externe partners) en ook weer intern met de genoemde Boa directies: deze directies ontvangen gegevens uit het Wpg domein en moeten verantwoord omgaan met de geheimhouding en doelbinding die voortvloeit uit de Wpg. De belangrijkste onder deze directies zijn Openbare Orde en Veiligheid (OOV), Veiligheid, Toezicht en Handhaving (VTH, onderdeel stadsdelen) en Verkeer en Openbare Ruimte (V&OR).

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 daaruit volgende gegevensverwerking kent grote onderlinge verschillen.

Governance

Verwerkingsverantwoordelijke voor de Wpg is de werkgever, in casu het college van B & W. Deze heeft de verwerkingsverantwoordelijkheid per directie gedelegeerd. Er is bij de vakgroep DREP een stedelijke coördinator en PO Wpg aangesteld sinds de zomer van 2023. Elke directie die Boa's heeft moet uit hoofde van het stedelijk beleid (zie ook "maatregelen") een contactpersoon voor de coördinator Wpg aanstellen.

Audits

In 2019 is door middel van het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpgboa) de Wet politiegegevens (Wpg) van overeenkomstige toepassing verklaard voor buitengewoon opsporingsambtenaren (boa's). Op grond van deze wet is gemeente Amsterdam 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 2024 zijn interne Wpg audits afgenomen bij de directies THOR, WPI en Sport en Bos. Onderwijs was al onderwerp van een interne audit in 2023. De interne audits zijn uitgevoerd door de directie Dienst, Middelen en Control (DMC). De interne audits dienden tevens als hercontrole en zijn ingestuurd naar de Autoriteit Persoonsgegevens (AP). In verband met een verkennend onderzoek onder verschillende gemeenten is naar aanleiding van deze hercontrole ook een gesprek met de AP gevoerd. De FG heeft aan dit gesprek deelgenomen. De hercontrole was een gevolg van de externe audit 2021-2022, waarin de gemeente voor de Wpg compliance een onvoldoende had gekregen. Uit de interne audits bleek dat de gemeente nog altijd niet voldeed aan de Wpg, maar ook dat er een duidelijke stijgende lijn was ingezet. Het implementeren van de Wpg is een complexe opdracht, waarin organisatorische, juridische en IT-systemische aspecten allemaal een rol spelen. Voor de mees-

te directies betekent de nieuwe manier van werken bovendien een grote cultuuromslag. De audits hebben het gevoel van urgentie bij de directies versterkt.

De externe audit vindt in 2025 plaats en wordt uitgevoerd door ACAM. Het auditrapport wordt in juli of augustus verwacht.

Maatregelen / Knelpunten
In 2024 is voortgebouwd op de Wpg-implementatie waarbij de aanbevelingen die voortkomen uit de audits als leidraad gelden. Er is een aantal maatregelen getroffen op stedelijk en op directieniveau. Zo is een privacy(beleids)kader Wpg, een richtlijn uitwisseling politiegegevens en een regeling rechten van betrokkenen Wpg vastgesteld. Ook is een aantal Wpg templates en producten toegevoegd aan de Quality Assurance en de documentatieplicht uit de Wpg is geborgd in het register van verwerkingen en het register van verstrekkingen datalekkenregister.

Voor de basisprocessen zijn bij de directies DPIA's uitgevoerd waaruit verdere maatregelen zijn afgeleid om de risico's te mitigeren. Een belangrijk aandachtspunt is het stedelijk Wpg beleid. Bij toepassing van de Wpg is het faciliteren van de Boa directies van groot belang, namelijk juiste kaders en richtlijnen om toe te kunnen passen in de praktijk.

De FG merkt op dat in de toepassing van de Wpg rollen en verantwoordelijkheden onduidelijk zijn en de samenwerking en afstemming tussen de eerste en tweede lijn niet goed verloopt. Het eigenaarschap voor gegevensverwerking wordt niet toegeeigend waardoor er vertraging ontstaat in procesgang en besluitvorming. Kennis en bewustzijn over de Avg én de Wpg, namelijk de reikwijdte van deze wetten ontbreekt. FG is actief geweest in het benaderen van de directies en het geven van presentaties en andere vormen van voorlichting. De FG constateert dat de te volgen processen binnen de directies niet bekend zijn. Dat is met name een probleem bij het delen van (ex-)politiegegevens met ketenpartners, maar ook met derde partijen. Het is inherent aan de grootte van de organisatie dat het aantal datastromen groot zijn. Van belang is om hier zorgvuldig mee om te gaan en tijdig de juiste deskundigheid hierbij te betrekken.

De FG beveelt aan om bewustzijn te creëren in rollen en verantwoordelijkheden en te investeren in kennis door cursussen en trainingen. Ook adviseert de FG datastromen in kaart te brengen en een proces voor gegevensuitwisselingen op te zetten en ook daarnaar te handelen.

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-of'defence-model". Er zijn concreet taken als "steekproefsgewijs controleren van de autorisaties" toebedeeld aan de FG. De FG is echter van mening dat ook de bedrijfsmatige controlefunctie onderdeel is van haar toezicht. Met andere woorden, de Plan-Do-Check-Act cyclus dient in de organisatie zelf geborgd te zijn en is ook onderwerp van het interne FG-toezicht.

Vanuit die visie is het niet aan de FG om op tactisch niveau uitvoerend betrokken te zijn. De FG geeft bij voorkeur advies op strategisch en beleidsmatig niveau, om op die manier de organisatie als geheel te kunnen ondersteunen en informeren. Omdat de DPIA's dienen te worden voorgelegd aan de FG ligt daar de mogelijkheid om daadwerkelijk op het niveau van een specifieke verwerking te kunnen adviseren en toezicht te houden.

De FG heeft regulier en terugkerend overleg met de coördinator Wpg en kan op die wijze signalen krijgen over wat goed gaat in de organisatie en wat niet. Vervolgens kan de FG over deze onderwerpen zelf onderzoek doen en/of in gesprek gaan met betrokkenen in de organisatie, zowel op uitvoerend als op leidinggevend en bestuurlijk niveau.

Vooruitblik

Toezicht kan niet oplossen wat in het primaire proces niet goed is geregeld. De toezichthouder kan wel signaleren wat niet goed is geregeld. Het is aan de organisatie om daar opvolging aan te geven. De gemeente opereert in het publieke domein, heeft voor de uitvoering van haar taken persoonsgegevens nodig. Op de juiste wijze, volgens *de bedoeling* van de wet- en regelgeving omgaan met persoonsgegevens is ook een taak van de gemeente die valt onder de zorgplicht.

De FG heeft in het afgelopen jaar, mede door onder de werkzaamheden beschreven instrumenten, een beeld gekregen wat er zoal noodzakelijk is om te streven naar een goede gegevenshouding. De FG constateert dat voor de realisatie van een goede gegevenshuishouding, in ieder geval om de basis op orde te hebben, een aantal elementen noodzakelijk zijn zoals het verduidelijken van rollen en verantwoordelijkheden en het eigenaarschap bij verwerking van persoonsgegevens bij directies en verbinding en samenwerking tussen de verschillende disciplines.

De FG hanteert het principe ‘toezicht op maat’. In ieder geval kijken hoever de organisatie is in de toepassing en naleving en de focus in toezicht bepalen aan de “behoefte”. De FG merkt op dat de gemeente nog een lange weg heeft te gaan 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.

De FG zal ook voor het komende jaar de ingezette lijn vanuit het toezicht om de organisatie bewuster te maken in rol- en verantwoordelijkheidsverdeling doorzetten en verder de verbinding zoeken. Wanneer de verbinding tussen de organisatieonderdelen is gerealiseerd en de rollen en verantwoordelijkheden duidelijk zijn in de toepassing en naleving van de AVG zal de FG zich meer toespitsen op proactief toezicht. Onder proactief toezicht verstaat de FG vooraf stimulerend en richtinggevend toezicht.

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
Bpgboa	Besluit politiegegevens buitengewoon opsporingsambtenaren
DMC	Directie Middelen en Control
DPIA	Data Protection Impact Assessment /
DREP	Digitale Rechten, Ethiek en Privacy
DS&I	Digitale Strategie en Informatie
FG	Functionaris Gegevensbescherming
FIC	Fully in Control
GMT	Gemeentelijk Managementteam
GS	Gemeentesecretaris
JZ	Juridische Zaken
NOREA	Nederlandse 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

