Gemeente Amsterdam

Raadsinformatiebrief

Aan:	De leden van de gemeenteraad van Amsterdam
Datum	22 september 2026
Portefeuille(s)	Digitale Zaken
Portefeuillehouder(s):	Melanie van der Horst
Behandeld door	Digitale Strategie en Informatie en Stadsarchief (bestuurszaken.dii@amsterdam.nl)
Onderwerp	Jaarverslagen 2025 over gegevensbescherming, informatiebeveiliging en informatiebeheer

Geachte leden van de gemeenteraad,

Hierbij bied ik u de jaarverslagen over 2025 aan van de interne toezichthouders op onze gegevensbescherming (privacy), informatiebeveiliging en informatiebeheer. In deze brief wordt een samenvatting gegeven van de belangrijkste punten uit de jaarverslagen en geeft het college aan hoe het omgaat met de aanbevelingen van de interne toezichthouders.

Voor de drie onderwerpen heeft de gemeente in 2025 stappen vooruit gezet. Er wordt door medewerkers eerder melding gemaakt van een inbreuk op de gegevensbescherming. De Functionaris Gegevensbescherming benadrukt dat we de rollen en verantwoordelijkheden beter in beeld moeten krijgen. We zijn verbeterd wat betreft informatieveiligheid. Er zijn minder datalekken gemeld. Daarnaast zijn de meldingen van kwetsbaarheden sneller opgelost. We lopen op dit moment niet meer risico dan in 2024. De Chief Information Security Officer vraag aandacht voor de verandering in werkwijze van kwaadwillenden. Voor het informatiebeheer van de gemeente zijn in 2025 met name in de organisatie en randvoorwaarden aanpassingen geweest. De gemeentearchivaris ziet nog wel dat informatiebeheer zelf nog verbeterd kan worden.

Digitale Zaken 2026-2030

Het college legt in het coalitieakkoord de nadruk op een gemeente die nabij, begrijpelijk, betrouwbaar en uitvoeringsgericht is. Digitalisering draagt hieraan bij met onder andere een betere dienstverlening. De dienstverlening moet echter wel veilig en verantwoord gebeuren. De gemeentelijke organisatie kent hiervoor verschillende regels. Vanuit de gemeentelijke organisatie wordt op gegevensbescherming, informatiebeveiliging en informatiebeheer toezicht gehouden. De interne toezichthouders houden de gemeentelijke organisatie scherp en bieden met hun jaarverslagen het college de mogelijkheid om hun ambities te sturen.

Voor digitalisering kent het college duidelijke ambities. Van minder afhankelijkheid van grote techbedrijven tot het versterken van de bescherming van gegevens en het vergroten van digitale gelijkheid. De gemeente werkt tegelijkertijd hard aan het implementeren van nieuwe wetten die gaan gelden voor digitalisering, zoals de Cyberbeveiligingswet, de AI Verordening en de Baseline

Informatiebeveiliging Overheid 2. De uitwerking van deze ambities vindt plaats naast het behouden van de huidige diensten en producten.

Het college deelt de zorg van de toezichthouders dat er meer moet gebeuren om de privacy, informatiebeveiliging en informatiebeheer te borgen en blijvend onder de aandacht te brengen. Ik dank de toezichthouders voor hun werk en ga met vertrouwen aan de slag met de adviezen. Het college neemt de aanbevelingen van de toezichthouders over.

Jaarverslagen 2025

Jaarverslag 2025 van de Functionaris Gegevensbescherming (privacy)

Het jaarverslag van de Functionaris Gegevensbescherming geeft het college inzicht in de ontwikkelingen binnen de gemeente met betrekking tot de bescherming van persoonsgegevens. De primaire verantwoordelijkheid voor de toepassing en naleving van gegevensbescherming ligt de directies van de gemeente. Vanuit de privacyorganisatie worden de directies geholpen bij de uitvoering van de wet. Er wordt ingegaan op datalekken, verzoeken en klachten van burgers over het gebruik en opslag van hun gegevens. Daarnaast wordt er ingegaan op activiteiten waarbij gegevensbescherming een rol speelt. De Functionaris Gegevensbescherming merkt op dat met name de rollen en verantwoordelijkheden, zowel bij de directies als bij het I-domein, nog onvoldoende helder zijn en dat de verbinding tussen organisatieonderdelen ontbreekt.

De belangrijkste aanbevelingen zijn samengevat:

- Versterk het proces voor Data Protection Impact Assessments (DPIA's) en risicobeheer. Zorg dat de directies hun verantwoordelijkheid nemen. Investeer hierbij in de verbinding tussen de directies en het I-domein.
- Zet in op bewustwording om datalekken te beperken en voorkomen. Zet in op het vergroten van het melden van datalekken door medewerkers. Gebruik continue e-learningsprogramma's en biedt deze samen met de directie P&O aan.
- Borg het proces van de rechten van betrokkenen.
- Er is onvoldoende beheer en controle op autorisaties. Dit is een groot risico 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.
- Inventariseer binnen de eigen directies met behulp van privacy- en/of compliance officer de interne gegevensuitwisselingen (tussen directies) en gegevensuitwisselingen met derde partijen.

Jaarverslag 2025 van de Chief Information Security Officer (informatiebeveiliging)

De rapportage beschrijft welke organisatorische en technische verbeteringen het afgelopen jaar zijn doorgevoerd en de noodzaak om hier blijvend op in te zetten. Weliswaar zijn het aantal gemelde kwetsbaarheden gedaald, maar dit betekent niet dat er geen nieuwe kwetsbaarheden ontstaan. Hierbij zijn risicomanagement, inzicht, kennis en vaardigheden, en voorbereiding op cyberincidenten van groeiend belang; de implementatie van nieuwe wetgeving en de ontwikkelingen met betrekking tot digitale autonomie vergen blijvend veel aandacht.

De aanbevelingen van de CISO zijn in lijn hiermee. Samengevat zijn dit de belangrijkste aanbevelingen:

- Zorg dat alle afdelingen de nieuwe regels voor cyberveiligheid volgen en beter samenwerken, vooral op het gebied van personeelszaken en beveiliging van gebouwen.
- De veiligheid van de belangrijkste systemen krijgt prioriteit en zorg dat alle systemen en websites up-to-date zijn en voldoen aan veiligheidseisen. Belangrijke onderwerpen hierbij zjin autorisatiebeheer, risicomanagement, leveranciersmanagement en operationele technologie.
- Werk het crisishandboek bij, plan regelmatig oefeningen en maak een duidelijk overzicht van risico's voor de afdeling Digitale Voorzieningen. Stel hiervoor een eenduidig risicobeeld op in samenwerking met de strategische leveranciers en security monitoring.
- Formaliseer het risicomanagement op het gebied van informatievoorziening (onderdeel van het integrale risicomanagement binnen de gemeente). Het GMT stelt dit vast en besteed daarbij met name aandacht aan de rol van de lijndirecties. Investeer in de relatie tussen i-domein en de lijndirecties.
- Leer van het toenemende aantal incidenten waarbij gebruik wordt gemaakt van AI door aanvallers. Onderzoek de mogelijkheden om AI in te zetten als verdedigingsmiddel.

Jaarverslag Gemeentearchivaris 2025-2026
De Gemeentearchivaris concludeert dat de randvoorwaarden voor degelijk informatiebeheer binnen de gemeentelijke organisatie zijn verbeterd. Zo zijn verantwoordelijkheden helderder belegd via de nieuwe rol van Information Steward naast de adviseurs Informatiebeheer. Informatiebeheer en openbaarheid zijn steviger verankerd in de bedrijfsvoering en de overgang naar een nieuwe digitale werkomgeving biedt een modernere basis voor geordende dossiervorming. Daarnaast is er opvolging gegeven aan de tussenevaluatie organisatieontwikkelplan i-domein (2024) wat heeft geleid tot het aanscherpen van de rollen en governance in het algemeen en investering in vakinhoudelijke ontwikkeling, zowel in de sturing op informatiebeheer als de operationele uitvoering.

Tegelijkertijd ziet de Gemeentearchivaris dat het informatiebeheer zelf nog niet is verbeterd. De Gemeentearchivaris concludeert dat de gemeente geen gestructureerde aanpak voor continue evaluatie en bijsturing op het gebied van informatiebeheer heeft, eigenaarschap van informatiebeheer op operationeel en tactisch niveau bij de organisatieonderdelen ontbreekt en dat de huidige Meetlat Informatiebeheer onvoldoende inzicht biedt in noodzakelijke verbeteracties, waardoor prioritering en aansturing van de opvolging van beheersmaatregelen tekortschieten.

De belangrijkste aanbevelingen zijn:

- Verbeter en ontwikkel de Meetlat Informatiebeheer (dan wel een ander instrument met gelijke doelen) en de kwartaalrapportages door.
- Specificeer in de organisatieonderdelen expliciet waar het eigenaarschap is belegd voor (onderdelen van) het informatiebeheer, wetende dat deze primair ligt bij de directeuren.
- Stel het meerjarenplan informatiebeheer op, waarin aandacht is voor een volledig en actueel, compleet, en logisch samenhangend overzicht van informatie.

Opvolging van de aanbevelingen van de interne toezichthouders door het college

Het college neemt de aanbevelingen van de Functionaris Gegevensbescherming, Chief Information Security Officer en gemeentearchivaris over en verzoekt de organisatie om de realisatie van de aanbevelingen ter hand te nemen. Daarbij is het, in het kader van het nieuwe collegeprogramma, ook van belang om een duidelijke taakverdeling tussen de vakgroepen van de directie Digitale Strategie & Informatie en de lijndirecties te hebben.

Bij de uitvoering van de aanbevelingen wordt aandacht gegeven aan:

- *Opvolging eerdere aanbevelingen*: Er wordt gewerkt aan risicomanagement, invoering van wet- en regelgeving, evaluatie van eerdere aanbevelingen en een plan van aanpak voor openstaande en nieuwe aanbevelingen.
- *Bewustwording en kennis:* Het bewustzijn en kennis over gegevensbescherming, informatiebeveiliging en informatiebeheer blijven aandacht vragen, met verplichte e-learnings en bewustwordingssessies op verzoek van directies.
- *Drie Lijnen Model (3LMO):* Dit is in 2025 en 2026 uitgewerkt en in 2026 formeel vastgesteld. Het model versterkt eigenaarschap van lijndirecties voor informatiebeheer, informatiebeveiliging en privacy en maakt het voor meerdere compliance onderwerpen toepasbaar (bijv. AI, openbaarheid).
- *Afweging belangen en mensenrechten:* Er komt in 2026-2027 een stedelijk afwegingskader voor ambtenaren. Risico's uit Data Protection Impact Assessments (DPIA's) worden opgenomen in een risicoregister. Er is nauwere samenwerking tussen directies en de privacyorganisatie via onder andere het Compliance Gilde. Directies worden gestimuleerd om gegevensuitwisselingen te inventariseren en actueel te houden.
- *Handhavingsonderzoeken:* In Q1 2027 wordt een proces ingericht voor duidelijke stakeholderbetrokkenheid en communicatie bij onderzoeken van de Autoriteit Persoonsgegevens (AP) voor gegevensbescherming.
- *Meetlat Informatiebeheer:* Wordt geactualiseerd en gekoppeld aan risicorapportages voor een integraal risicobeeld, in lijn met het Drie Lijnen Model voor de Overheids- en non-profit-sector (3LMO).
- *Meerjarenplan informatiebeheer:* De Directie Strategie en Informatie is voornemens om het meerjarenplan in het najaar van 2026 naar de raad te sturen. Om te zorgen dat de informatiehuishouding als adequaat wordt beoordeeld zetten we in 2026 stevigere sturing in door met dit vernieuwd meerjarenplan en een data- en informatiestrategie die gezamenlijk de directie Data en het Stadsarchief Amsterdam wordt opgesteld.

Gerelateerde onderwerpen waarover het college u wil informeren

In het verlengde van de jaarverslagen over gegevensbescherming en informatiebeveiliging wil ik, mede namens mijn collega's, u nog informeren over de uitkomsten van de zelfevaluaties over het gebruik van Suwinet en de kwaliteit van de basisregistraties in 2025.

Eenduidige Normatiek Single Information Audit (ENSIA)

Met deze brief stuur ik u ook de twee ENSIA-audits mee over informatiebeveiliging bij het gebruik van Suwinet. Suwinet is een landelijke voorziening waarmee overheidsinstellingen onder voorwaarden gegevens uitwisselen over werk, inkomen, uitkeringen en dergelijke Uit de zelfevaluatie blijkt dat we op bepaalde punten niet voldoen aan de norm. Daarom nemen we

verbetermaatregelen die bestaan het verbeteren van het bewustzijn over informatiebeveiliging en het vastleggen van rollen en verantwoordelijkheden.

Daarnaast zijn er vijf rapportages over de uitvoering van de regels omtrent kwaliteit en informatieveiligheid van de basisregistraties over Adressen en Gebouwen, Grootschalige Topografie, Ondergrond en Personen en van de registraties Reisdocumenten en Niet-ingezetenen. Aan alle gestelde normen wordt voldaan, behalve voor de kwaliteitseisen van de Basisregistratie Personen. Hiervoor zijn maatregelen genomen om in 2026 te voldoen aan de gestelde normen.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,
Namens het college van burgemeester en wethouders van de gemeente Amsterdam,

Melanie van der Horst
Wethouder Digitale Zaken

Bijlagen
1. Jaarverslag Functionaris Gegevensbescherming 2025
2. Bestuurlijke rapportage informatiebeveiliging 2025
3. Verslag van de gemeentearchivaris 2025
4. Collegeverklaring Suwinet 2025
5. Verantwoordingsrapportage Suwinet 2025
6. Compact verbeterplan bevindingen Suwinet 2025
7. Verantwoordingsrapportage BAG, BGT en BRO 2025
8. Verantwoordingsrapportage BRP Kwaliteit 2025
9. Verantwoordingsrapportage BRP Volwassenheid 2025
10. Verantwoordingsrapportage Reisdocumenten 2025
11. Verantwoordingsrapportage RNI 2025