Gemeente Amsterdam

Raadsinformatiebrief

Aan:	De leden van de gemeenteraad van Amsterdam
Datum	17 juni 2025
Portefeuille(s)	ICT en Digitale Stad
Portefeuillehouder(s):	Alexander Scholtes
Behandeld door	Digitale Strategie en Informatie / Stadsarchief (bestuurszaken.dii@amsterdam.nl)
Onderwerp	Jaarverslagen 2024 Gegevensbescherming, Informatiebeveiliging en Informatiebeheer

Geachte leden van de gemeenteraad,

Hierbij bied ik u de jaarverslagen over 2024 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.

Betrouwbare digitale stad

Het college wil een betrouwbare digitale stad zijn, zoals is opgenomen in de Agenda Digitale Stad.[1] In 2024 zijn er concrete stappen gezet om de informatiebeveiliging, privacy en informatiebeheer op een hoger volwassenheidsniveau te brengen. Stapsgewijs wordt via de Baseline Informatiebeveiliging Overheid (BIO), de meetlat informatiebeheer en Baseline Privacy Amsterdam toegewerkt naar een risicobeeld per directie. Dit maakt het mogelijk om gerichte verbeteringen door te voeren en risicogebaseerd te werken. Ook is ingezet op het vergroten van bewustzijn in de organisatie op het gebied van onder andere informatiebeveiliging en privacy.

Er is sprake van elkaar snel opvolgende ontwikkelingen, zoals de nieuwe Cyberbeveiligingswet en BIO-2, die vanaf eind 2025/ begin 2026 nieuwe eisen stellen, en de vorige jaar vastgestelde AI Verordening. Om deze kaders goed te implementeren worden de nodige voorbereidingen getroffen. Op het gebied van Algoritmes/AI hebben we een plan van aanpak gemaakt om het beheerskader algoritmes te verbeteren. Op 5 juni 2025 hebben we in de gemeenteraad de halfjaarlijkse rapportage Plan van Aanpak Algoritmes besproken. Voor de stand van zaken van de acties en de voortgang daarop verwijzen we daarnaar.

Ondanks de vooruitgang, deelt het college de zorg van de toezichthouders dat er méér moet gebeuren om de privacy en informatiebeveiliging van betrokkenen te borgen en blijvend onder de aandacht te brengen. Dat geldt te meer nu de geopolitieke (digitale autonomie), technologische

[1] https://amsterdam.raadsinformatie.nl/document/13554872/1#search=%22agenda%20digitale%20stad%20en%20overheid%22

(ontwikkelingen rondom (gen)AI), maatschappelijke (vertrouwen in de overheid) en juridische (AVG, AI-Act) aspecten permanent en continue in beweging zijn.

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 2024

Jaarverslag 2024 van de Functionaris Gegevensbescherming (privacy)

Het Jaarverslag geeft het college en de burgemeester inzicht in ontwikkelingen binnen de gemeente inzake datalekmeldingen, verzoeken en klachten van burgers en diverse activiteiten waarbij gegevensbescherming een rol speelt. De FG merkt op dat met name de rollen en verantwoordelijkheden niet duidelijk zijn en de verbinding tussen de organisatieonderdelen ontbreekt. De belangrijkste aanbevelingen zijn samengevat:

- Creëer meer bewustzijn op het gebied van de AVG, het melden van datalekken, rollen en verantwoordelijkheden t.a.v. de AVG/Wpg en AVG-geletterdheid.
- Actualiseer of maak nieuw beleid en kaders t.a.v. risicomanagement en het verwerken van persoonsgegevens.

Jaarverslag 2024 van de Chief Information Security Officer (informatiebeveiliging)

De rapportage beschrijft de activiteiten, ontwikkelingen, risico's, dreigingen en incidenten ten aanzien van informatieveiligheid bij de gemeente Amsterdam over het jaar 2024 en geeft ook een vooruitblik op 2025. Daarbij wordt ook aandacht besteed aan de verbonden partijen en het netwerk digitale weerbaarheid Amsterdam-Amstelland. In de rapportage zijn de uitkomsten opgenomen van de audit op de gemeentelijke DigiD-portalen en de zelfevaluatie om te voldoen aan de landelijk voorgeschreven normen voor informatiebeveiliging (BIO).

De CISO concludeert dat de gemeente stappen zet in het verbeteren van de informatieveiligheid. Voor 2025 ziet de CISO de volgende aandachtspunten:

- Stuur actief op de voortgang van de implementatie van de BIO en opvolgers zoals Cyberbeveiligingswet (CBW) en BIO2.
- Organiseer bewustwording in de organisatie.
- Zet in op herijking van bestaand beleid en kaders en definieer wat nodig is ten aanzien van nieuwe regelgeving rondom CBW.

Jaarverslag 2024 van de Gemeentearchivaris (informatiebeheer)

De gemeentearchivaris concludeert dat het moeilijk is om een betrouwbaar inzicht te krijgen in hoe de informatie in de gemeentelijke organisatie wordt beheerd. Dit gebrek aan inzicht belemmert een effectieve sturing en beheersing van risico's. Dit jaarverslag belicht de huidige stand van zaken, de uitdagingen en de noodzaak van een gestructureerde aanpak voor toekomstbestendig en effectief informatiebeheer bij de directies, stadsdelen en stadsgebied van de gemeente Amsterdam.

De belangrijkste aanbevelingen zijn:

- Verduidelijk de verantwoordelijkheden rondom informatiebeheer.

- Zet een verbeteraanpak op ten behoeve van informatiebeheer bij de verschillende organisatieonderdelen.
- Verbeter het instrument Meetlat om de kwaliteit van het informatiebeheer te meten en help directies het instrument te gebruiken.

Opvolging van de aanbevelingen van de interne toezichthouders door het college

Kijkend naar de bevindingen van CISO, FG en Gemeentearchivaris kunnen we constateren dat veel bevindingen dezelfde onderwerpen raken in de respectievelijke vakgebieden. Daarbij gaat het vooral om het verduidelijken van rollen/eigenaarschap, het aanscherpen van (stelsel-) verantwoordelijkheid, het managen van risico's en om het vergroten van het bewustzijn binnen de organisatie. Daarvoor geldt:

- We brengen de feitelijke risico's in kaart door middel van gerichte risicorapportages voor de clusters en directies. We maken de geïdentificeerde risico's inzichtelijk via de applicatie Fully in Control.
- We gaan de rollen en verantwoordelijkheden van de drie vakgebieden binnen de organisatie verduidelijken met het 3-lines-of-defence model. We stellen een nieuw beleidskader op, waarin we de sturing en beheersing van de stelselverantwoordelijkheid in overleg met de drie toezichthouders duidelijk omschrijven. De eerste contouren zijn eind 2025 duidelijk.
- We bevorderen het bewustzijn en de kennis in de organisatie. Er zijn al diverse e-learnings op het gebied van privacy, informatiebeveiliging en AI beschikbaar en deze worden samengevat in een training 'de i is voor iedereen'.
- We evalueren (en zo nodig herijken) bestaand beleid en kaders.
- Op organisatorisch vlak zijn er ontwikkelingen om de (schaarse) beschikbare compliance capaciteit zo effectief mogelijk in te zetten. Zo vertalen we bevindingen uit een eerder onderzoek over het informatiebeveiligingshuis naar onder andere een integrale aanpak vanuit security om veiligheidsrisico's beter af te dekken en loopt er op dit moment een gelijksoortig onderzoek naar de privacyfunctie.

Privacy, informatiebeveiliging en informatiebeheer zijn nooit 'af', omdat het doorlopende processen betreft die zich steeds weer moeten aanpassen aan de veranderende omgeving. Dat betekent ook dat de inzet op verbetering doorlopend is. Daarom passen we een gestructureerde en cyclische verbeteraanpak toe. Hierbij wordt gekeken naar urgentie en de beschikbaarheid van middelen en capaciteit in de prioritering van de aanbevelingen. Ook wordt gekeken naar de onderlinge samenhang. Tot slot worden genomen maatregelen beoordeeld op effectiviteit (wederom in samenwerking met de toezichthouders) en zo nodig bijgestuurd.

Gerelateerde onderwerpen waarover het college u wil informeren

In het verlengde van de jaarverslagen over privacy 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 2024.

Eenduidige Normatiek Single Information Audit (ENSIA)

Als bijlage bij deze brief stuur ik u ook de twee ENSIA-audits mee over de informatiebeveiliging bij het gebruik van Suwinet en de kwaliteit van de basisregistraties. De ENSIA-methodiek heeft betrekking op wettelijk voorgeschreven zelfevaluaties.

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 uit het zorgen dat elke nieuwe medewerker binnen 3 maanden na indiensttreding een bewustwordingstraining heeft gevolgd, dat deze deelname wordt vastgelegd, en dat hierop door het management wordt gemonitord. Daarnaast wordt de toegang en toekenning van autorisaties verbeterd en bijgehouden, en wordt het verwerkingsregister AVG op de juiste wijze bijgewerkt.

Bij de basisregistraties is er gekeken naar de uitvoering van de basisregistraties Adressen en Gebouwen, Grootschalige Topografie, Ondergrond en Personen en van de registraties Reisdocumenten en Niet-ingezetenen. Aan alle gestelde normen wordt voldaan, behalve bij de terugkoppeling van geconstateerde fouten in BRP-gegevens aan de bron. Daarvoor zijn verbetermaatregelen opgesteld.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

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

Alexander Scholtes
Wethouder ICT en Digitale Stad

Bijlagen
1. Jaarverslag Functionaris Gegevensbescherming 2024
2. Bestuurlijke rapportage informatiebeveiliging 2024
3. Verslag van de gemeentearchivaris 2024
4. Collegeverklaring Suwinet 2024
5. Verantwoordingsrapportage Suwinet 2024
6. Compacte versie verbeterplan Suwinet ENSIA 2024
7. Verantwoordingsrapportage BAG, BGT en BRO 2024
8. Verantwoordingsrapportage BRP Kwaliteit 2024
9. Verantwoordingsrapportage BRP Volwassenheid 2024
10. Verantwoordingsrapportage Reisdocumenten 2024
11. Verantwoordingsrapportage RNI 2024