Gemeente Amsterdam

Raadsinformatiebrief

Aan:	De leden van de gemeenteraad van Amsterdam
Datum	7 juli 2021
Portefeuille(s)	ICT en Digitale Stad
Portefeuillehouder(s):	Touria Meliani
Behandeld door	CIO: Mark Crooijmans, [redacted] en [redacted] ([redacted]@amsterdam.nl)
Onderwerp	Rapportage 2020 Informatiebeveiliging en de Rapportage 2020 Functionaris gegevensbescherming

Geachte leden van de gemeenteraad,

Met deze brief informeert het college u over de stand van zaken ten aanzien van de informatie-beveiliging en de gegevensbescherming. Dit zijn actuele en urgente aandachtsgebieden voor het functioneren van de gemeentelijke organisatie en het zorgvuldig omgaan met gegevens van burgers, bedrijven en medewerkers. Het is daarom belangrijk om u als raad periodiek te informeren waar Amsterdam staat. In de bijgaande rapportages geven wij aan waar Amsterdam staat en welke verbeteracties lopen op deze gebieden. De rapportages laten zien dat Amsterdam op deze gebieden al veel heeft gerealiseerd, maar dat we nog niet zijn waar we willen zijn. Zowel de gemeenteaccountant als de Rekeningencommissie hebben in hun verslagen bij het Jaarverslag 2020 aandacht gevraagd voor het voldoen aan de wet- en regelgeving ten aanzien van informatiebeveiliging en gegevensbescherming. Die aandacht is zowel bij het college als in de ambtelijke organisatie aanwezig.

<u>De informatiebeveiligingsnorm BIO</u>
De gemeente verwerkt elke dag grote hoeveelheden informatie. De beveiliging van deze informatie is noodzakelijk voor het functioneren van de gemeente als betrouwbare overheid. Die beveiliging richten we in op basis van de Baseline Informatiebeveiliging Overheid (de BIO). Dit is een set aan beveiligingsnormen en voorgeschreven maatregelen die gelden voor de gehele overheid en is sinds 2020 de opvolger van eerdere normen die alleen voor gemeenten golden. Door de gehele overheid met één-BIO-normenkader werkt kan de overheid als geheel op een adequaat niveau van informatiebeveiliging worden gebracht en gehouden.

Informatiebeveiliging is er niet pas sinds de BIO. Zoals in de raad is besproken, was er ook vóór de BIO sprake van een beveiligingsnorm. Veel van de maatregelen die in de BIO worden benoemd zijn dan ook in Amsterdam al een tijd geleden geïmplementeerd. Enkele voorbeelden daarvan: alle informatiesystemen zijn voorzien van toegangsbeveiliging, voor toegang van buiten zijn tokens ingericht. Ook is Amsterdam voorloper bij het jaarlijks uitvoeren van veel pen- en hacktests op onze toepassingen. Aan het bewustzijn bij medewerkers wordt structureel aandacht besteed.

Op 15 december 2020 heeft het college (op basis van de BIO) een nieuw informatiebeveiligingsbeleid vastgesteld, het *Stedelijk kader informatiebeveiliging gemeente Amsterdam*. Daarin wordt aangegeven dat de wethouder ICT en Digitale Stad stelselverantwoordelijk is, maar ook is de rol van de andere bestuurders en de ambtelijke organisatie uitgewerkt. De raadscommissie Kunst, Diversiteit en Democratisering heeft hiervan op 27 januari 2021 kennisgenomen. Dit kader informatiebeveiliging geeft richting aan de wijze waarop informatie van de gemeente Amsterdam wordt beveiligd volgens de BIO. De BIO hanteert daarvoor drie basisbeveiligingsniveaus. Het middelste niveau (BBN2) is standaard van toepassing. Het eerste niveau is bedoeld voor openbare informatie en het derde niveau is alleen van toepassing voor zeer vertrouwelijke informatie die bijvoorbeeld gevoelig is voor spionage door statelijke (buitenlandse) actoren. De BIO kent een 130-tal beheersmaatregelen om een basisbeveiligingsniveau te kunnen doorvoeren.

Per proces en informatiesysteem moet worden bepaald welk niveau er van toepassing is. Dat gebeurt op basis van een risicoanalyse. Zo staat bijvoorbeeld een systeem dat wij gebruiken voor het regelen van het klimaat in een kantoorgebouw bloot aan andere risico's dan het systeem waarmee wij de Basisregistratie Personen bijhouden en het is niet efficiënt om het klimaatbeheersingssysteem (zonder persoonsgegevens) even zwaar te beveiligen als het systeem dat vertrouwelijke persoonsgegevens bevat.

Om het basisbeveiligingsniveau te realiseren maken we zoveel mogelijk gebruik van generieke beheersmaatregelen waarmee we de generieke risico's afdekken. Dat doen we bij voorzieningen die we centraal inrichten voor de gehele gemeentelijke organisatie, zoals bijvoorbeeld de ICT-werkplek, de telefoon, het netwerk of de internettoegang. Met deze generieke maatregelen kunnen we veel zaken in één keer regelen voor de gehele organisatie. Daarnaast kunnen er per systeem nog specifieke aanvullende maatregelen nodig zijn omdat er sprake is van specifieke risico's.

<u>Stand van zaken BIO</u>
De gemeente heeft een Chief Information Security Officer (CISO) aangesteld die toezicht houdt op de informatiebeveiliging van de organisatie. Jaarlijks wordt door hem beoordeeld (via de verplichte ENSIA-zelfevaluatie) in hoeverre de gemeente voldoet aan de BIO. Het beeld van eind 2020 laat zien dat alle aspecten van de BIO globaal op orde zijn, maar dat er nog verbeteringen nodig zijn in de beheersing van risico's en het voldoen aan de basisnormen van de BIO.

Amsterdam werkt sinds 2020 aan de implementatie van de vereiste maatregelen op basis van een implementatieplan. Dit plan heeft een tijdhorizon van 3-4 jaar. Deze planning is in lijn met andere grote / complexe overheidsorganisaties (ministeries en G4-gemeenten). Eind 2020 is besloten om voor 2021 en 2022 extra geld uit te trekken om de nodige stappen te kunnen zetten. Het volledig implementeren van de BIO raakt alle organisatieonderdelen, werkprocessen en informatiesystemen van Amsterdam en is geen geringe opgave. Daarom is ervoor gekozen om risicogericht te werk te gaan. Per directie wordt beoordeeld of de processen en informatiesystemen op het juiste niveau zijn beveiligd en of er specifieke aanvullende maatregelen nodig zijn.

In 2021 doen we dit als eerste bij:

- De directies Personeel & Organisatie, ICT, Dienstverlening, Communicatie en Facilitair Bureau. Deze organisatieonderdelen dekken een groot percentage (80%) van de beheersmaatregelen uit de BIO voor de gehele organisatie, bijvoorbeeld door veilige ICT-werkplekken aan te bieden, onze kantoren goed te beveiligen en het in- en uitstroomproces van medewerkers op orde te hebben.
- Directies die werken met gevoelige gegevens van heel veel Amsterdammers. Het gaat hierbij om Grond en Ontwikkeling, Verkeer en Openbare Ruimte, GGD, Werk, Participatie en Inkomen, Belastingen, Parkeren, OIS, Openbare Orde & Veiligheid, Financiën en Stadswerken.

Na bovengenoemde directies wordt een volgende tranche directies aangepakt, totdat alle organisatieonderdelen zijn afgerond. Verbeterpunten worden geprioriteerd naar ernst en urgentie. Daardoor is in eerdere stukken aangegeven dat de implementatie van de BIO 3 tot 4 jaar duurt.

Omdat de bedreigingen van onze informatieveiligheid zich blijven ontwikkelen, kunnen er nieuwe risico's ontstaan die we het hoofd moeten bieden om aan de BIO te blijven voldoen. In de rapportage over 2020 gaan we in op deze ontwikkelingen. Risicoanalyses worden daarom periodiek herhaald. Informatiebeveiliging is nooit af. Het zal continue aandacht, inzet en bijstelling blijven vragen.

<u>Rapportage 2020 Informatiebeveiliging</u>
Bij de vaststelling van het *Stedelijk kader informatiebeveiliging gemeente Amsterdam* door het college 15 december 2020 is bepaald dat er jaarlijks door het college aan de raad wordt gerapporteerd over de informatiebeveiliging.

Bijgevoegd treft u de Rapportage 2020 Informatiebeveiliging aan. De rapportage beschrijft de activiteiten, incidenten en ontwikkelingen ten aanzien van informatieveiligheid bij de gemeente Amsterdam over het jaar 2020 en geeft ook een vooruitblik op 2021. De rapportage is opgesteld vanuit de stelselverantwoordelijkheid van de wethouder ICT en Digitale Stad, maar raakt de informatiehuishouding van de gemeente als geheel en dus ook de portefeuilles van alle andere wethouders.

De rapportage geeft aan dat er de afgelopen jaren al veel stappen zijn gezet, bijvoorbeeld op het gebied van de veilige ICT-infrastructuur, werkplekken, telefoons en het security operations center (24 uur per dag monitoring of er digitaal wordt ingebroken). Ook lopen wij voorop bij het structureel uitvoeren van pen- en hacktesten van de veiligheid van informatiesystemen en is er actieve informatie-uitwisseling met de Informatiebeveiligingsdienst van de VNG en het Nationaal Cyber Security Center over kwetsbaarheden en dreigingen.

De rapportage geeft aan dat binnen de gemeente Amsterdam met name de volgende risico's relevant zijn:

- De complexe Amsterdamse informatievoorziening maakt dat het zicht op de beveiliging van apparatuur en informatie nog niet op alle vlakken voldoende is;

- Het beheersen van toegang tot informatie en de beveiliging van Internet of Things – toepassingen (IoT) en mobiele apparatuur is een aandachtspunt;
- Het zicht op de informatiebeveiliging bij uitbestede werkzaamheden is nog onvoldoende;
- Voor het structureel testen van cybercrisissen is in 2020 in G4-verband een aanpak / handreiking ontwikkeld, vanaf 2021 gaan deze tests structureel plaatsvinden.

In de rapportage is de status van de informatiebeveiliging per eind 2020 weergegeven. Alle onderdelen zijn globaal op orde, maar er zijn verbeterpunten. De uitkomst hiervan is gebruikt bij het bepalen van de speerpunten voor 2021. De volgende speerpunten zijn inmiddels in gang gezet.

- Monitoring en response: doorontwikkelen van het gemeentelijk Security operations center;
- Standaardisatie en vernieuwing: toetsen websites en internetdomeinen, invoering nieuwe ICT-werkplek, realisatie van het kennis- en expertisecentrum voor de cloud;
- Toetsen ICT-infra en informatiesystemen, ook door het inhuren van specialisten die in onze opdracht –net als een hacker- proberen in te breken;
- Beveiliging van industriële automatiseringssystemen, te beginnen met het verhogen van de weerbaarheid in de watersector en de verkeerssector, in samenwerking met de rijksoverheid;
- Bevorderen bewustzijn en digitale vaardigheden medewerkers;
- Continuïteit en veerkracht: opzetten van Business Continuity Management en het oefenen met cyberincidenten;
- Agenda veilige stad: uitwerken ecosysteem rond de vitale infrastructuur van de stad met maatschappelijke partijen;
- Sturing op verbonden partijen (partijen die taken voor ons verrichten).

De rapportage biedt tot slot cijfermatig inzicht in het aantal incidenten met een hoge impact. Dit zijn (concernbrede) incidenten waarbij bijvoorbeeld de dienstverlening verstoord wordt of waarbij voorzieningen die iedere medewerker nodig heeft (Amsterdamse digitale werkplek, e-mail, internet) niet beschikbaar zijn. In 2020 waren er 30 incidenten met een hoge impact. Dit is lichte daling ten opzichte van de 32 incidenten in 2019. De meeste incidenten waren het gevolg van hardware- of software storingen. De informatieveiligheid was hierbij niet in het geding. De impact daarvan was hoog omdat meerdere organisatieonderdelen hierdoor werden geraakt. De directie ICT werkt inmiddels aan de implementatie van een nieuwe ICT-werkplek en het uitbesteden van de hosting van ICT-systemen, met als doel het versterken van de stabiliteit en bedrijfszekerheid van onze ICT-infrastructuur. Hierdoor moet het aantal incidenten gaan afnemen.

De rapportage bevat ook de uitkomsten van de (verplichte) jaarlijkse ENSIA-audit naar de staat van de informatiebeveiliging van onze DigiD-portalen, waarover aan de landelijke toezichthouder Logius gerapporteerd is. Via de landelijke DigiD-voorziening kunnen burgers toegang krijgen tot de digitale dienstverlening van de overheid. De gemeente Amsterdam beschikt over zeven verschillende DigiD-portalen. Uit deze audits blijkt dat deze portalen aan de eisen voldoen, met uitzondering van een aandachtspunt dat geen directe impact heeft op de informatieveiligheid. Dit punt wordt binnen de door Logius gestelde termijn opgelost.

De rapportage is primair gericht op de informatiebeveiliging van de gemeentelijke processen en informatiesystemen. In hoofdstuk 1.2 is de *Agenda digitale veiligheid* kort aangestipt, die in 2019 is opgesteld. Deze agenda richt zich vooral op de informatieveiligheid van burgers en ondernemers in de stad, wordt uitgevoerd onder verantwoordelijkheid van de burgemeester en kent een eigen rapportagelijn.

Waar staan we ten aanzien van de gegevensbescherming (privacy) en hoe werken we daaraan?
Naast de hierboven beschreven maatregelen op het gebied van de beveiliging van gegevens, zijn op het gebied van gegevensbescherming eerder al de nodige vereiste generieke maatregelen getroffen. Dat doen we op basis van de wettelijke eisen in de Algemene verordening gegevensbescherming (AVG). Zo hebben we een interne toezichthouder (de Functionaris gegevensbescherming) aangesteld, is het *Stedelijk kader* verwerken persoonsgegevens door de gemeente Amsterdam vastgesteld, een verwerkingenregister en een datalekregister ingericht, het risicoanalyse-instrument Data Protection Impact Assessments (DPIA) ingevoerd, privacyverklaringen gepubliceerd en een Loket Persoonsgegevens ingericht.

De Functionaris gegevensbescherming gaat in haar rapportage in op welke maatregelen de gemeente Amsterdam in 2020 heeft getroffen om de beginselen van de AVG te waarborgen en waar nog actie is vereist. De rapportage van de Functionaris gegevensbescherming komt voort uit haar wettelijke verplichting om verslag uit te brengen aan de hoogste leidinggevende, verantwoordelijk voor de verwerking van persoonsgegevens (in dit geval het college en de raad).

De rapportage biedt inzicht in de activiteiten die in 2020 uitgevoerd zijn om de gegevensbescherming te borgen, zoals:

- In 2020 heeft de gemeente ingezet op het actualiseren van het verwerkingsregister en de termijnbewaking bij het Loket Persoonsgegevens. In het kader van de transparante overheid is een algoritmeregister gelanceerd, de ontwikkelingen op dit terrein worden door de FG met belangstelling gevolgd. De Functionaris gegevensbescherming heeft onderzoek laten doen naar de stand van zaken met betrekking tot de Data Protection Impact Assessments (DPIA's). Dit zijn wettelijk voorschreven risicoanalyses. Het eerste deel van het onderzoek is afgerond en daaruit blijkt dat de gemeente nog niet voor al haar risicovolle verwerkingen een DPIA heeft uitgevoerd. De organisatieonderdelen die dit betreft, gaan hiermee aan de slag. Hierbij wordt een prioritering aangebracht, waarbij de vanuit oogpunt van gegevensbescherming risicovolle gegevensverwerkingen die worden opgestart, met voorrang worden opgepakt;
- Wanneer de gemeente een dienstverlener inschakelt, zijn partijen verplicht om afspraken te maken over de manier waarop met persoonsgegevens wordt omgegaan. Met ingang van 2020 gebruikt de gemeente hiervoor het VNG-model verwerkersovereenkomst met daaraan toegevoegd een Amsterdams addendum met aanvullingen op de overeenkomst. De gemeente vindt deze aanvullingen noodzakelijk omdat daarmee de gegevens van burgers en anderen beter worden beschermd;
- De doorlopende bewustwordings-campagne 'Weet wat je deelt 2.0' draagt bij aan het interne bewustzijn over gegevensbescherming. Dit krijgt een extra stimulans door de e-learnings die zijn ontwikkeld een meer verplichtend karakter te geven.

De rapportage geeft daarnaast inzicht in de diverse aandachtspunten en activiteiten om te voldoen aan de AVG voor het jaar 2021:

- Aandachtspunt: inzicht in de actuele status van gegevensbescherming binnen de gemeente.
  Actie (lopend): inzicht verkrijgen in de actuele status van gegevensbescherming met de inrichting van operationeel risicomanagement via Versterking Operationeel Risico Management (VORM);
- Aandachtspunt: beschikbaarheid van voldoende aandacht en resources. In de periode 2018-2020 zijn belangrijke stappen gezet om de AVG te implementeren. Het is belangrijk dat er voldoende aandacht en resources beschikbaar zijn en blijven zodat de gemeente aan haar accountability verplichtingen kan voldoen. De FG adviseert om het register van verwerkingen en de benodigde basisdocumentatie actueel te houden, waaronder diverse overeenkomsten en Data Protection Impact Assessments (DPIA's) om te voldoen aan accountability verplichtingen.
  Acties (lopend): actualisatie van het verwerkingsregister, audit op DPIAs;
- Aandachtspunt: In juli 2020 heeft het Hof van Justitie een uitspraak gedaan in zaak Schrems II. Dit heeft tot gevolg gehad dat het verwerken van persoonsgegevens in de Verenigde Staten onder de bestaande afspraken, het EU-VS Privacy shield, niet rechtmatig plaatsvindt.
  Actie (lopend): De gemeente is in 2020 gestart met het inventariseren van de contracten die door deze uitspraak worden geraakt. Deze inventarisatie omvat mede de contracten die eventueel moeten worden herzien vanwege de Brexit. Deze inventarisatie wordt in 2021 afgerond;
- Aandachtspunt: invulling van het beginsel van privacy by design.
  Nog te starten actie: de mogelijkheden van een gemeentelijke standaardaanpak worden onderzocht;;
- Aandachtspunt: implementatie van bewaartermijnen. Voor elke verwerking van persoonsgegevens moet een bewaartermijn zijn bepaald en deze moet worden nageleefd. Gegevens moeten worden vernietigd als ze niet meer nodig zijn voor het doel waarvoor ze zijn ingewonnen. Dat is nu niet goed geregeld: bewaartermijnen zijn (te) vaak niet vastgesteld en er wordt te weinig informatie vernietigd. Dit hangt samen met de staat van het informatiebeheer binnen de gemeente.
  Actie (lopend): er wordt een stedelijk plan van aanpak opgesteld voor de bewaartermijnen, het programma 'Informatiehuishouding op orde'. De benodigde middelen hiervoor zijn opgenomen in de Voorjaarsnota;
- Aandachtspunt: voldoen aan Wet politiegegevens (Wpg).
  Actie (lopend): Sinds 2019 hebben BOA's bij de uitoefening van hun taken te maken met de Wet politiegegevens (Wpg). Deze wet verplicht de gemeente om jaarlijks een interne audit en in 2021 een externe audit uit te laten voeren op de gegevensverwerking onder de Wpg. De FG zal deze audit begeleiden;
- Aandachtspunt: bewustwording medewerkers op het gebied van privacy.
  Acties (lopend): De bewustwordingscampagne, 'Weet wat je deelt'2.0 wordt in 2021 voortgezet. Hierbij wordt onderzocht op welke wijze het volgen van e-learnings kan worden gestimuleerd stimuleren, bijvoorbeeld door deze een meer verplichtend karakter te geven en onderdeel uit te laten maken van het indiensttredingstraject van nieuwe

werknemers. Verder wordt er in 2021 specifiek aandacht besteed aan datalekken. Samen met de privacy officers organiseert de FG een Roadshow datalekken.

De Chief Information Officer (CIO) draagt namens het college en de burgemeester zorg voor de opvolging van de aandachtspunten en activiteiten. De organisatie is met verschillende projecten aan de slag waarbij de verbeterpunten worden geprioriteerd naar ernst en urgentie. De Functionaris gegevensbescherming voorziet hem van de benodigde informatie over de voortgang en knelpunten. In de volgende rapportage van de Functionaris gegevensbescherming (over 2021) wordt u over de voortgang geïnformeerd.

De rapportage biedt ook cijfermatig inzicht in klachten en verzoeken van burgers en in de gemelde datalekken:

- In 2020 heeft de Functionaris gegevensbescherming 27 klachten ontvangen tegen 38 in 2019;
- Via het digitale Loket Persoonsgegevens kan de Amsterdammer een verzoek indienen tot inzage, verwijdering of correctie van persoonsgegevens. In 2020 heeft het loket 120 AVG verzoeken in behandeling genomen. Dit betekent een kleine stijging (+7) ten opzichte van 2019;
- In 2020 zijn 180 datalekken geregistreerd waarvan er 53 bij de landelijke toezichthouder, (Autoriteit Persoonsgegevens) zijn gemeld. Datalekken moeten worden gemeld wanneer er een risico bestaat op nadelige gevolgen voor de burger of werknemer. In 2019 was er sprake van 156 geregistreerde datalekken, waarvan er toen 38 gemeld zijn bij de Autoriteit Persoonsgegevens. Het feit dat het aantal interne meldingen wederom is gestegen ten opzichte van het vorige jaar, wijst erop dat het bewustzijn rondom datalekken is toegenomen.

Tot slot

Naar aanleiding van het gesprek met de rekeningencommissie heeft de wethouder ICT en Digitale Stad toegezegd om een technische sessie te organiseren, zodat u (mede naar aanleiding van deze rapportages) detailvragen kunt stellen aan onze experts. U wordt hierover via de dagmail nog nader geïnformeerd.

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



Touria Meliani
Wethouder ICT en Digitale Stad

Bijlagen

1. Rapportage 2020 Informatiebeveiliging
2. Rapportage 2020 Functionaris gegevensbescherming