Nummer VN2020-029441
Directie

Gemeente Amsterdam

College van burgemeester en wethouders B&W

Voordracht voor de College vergadering van 15 december 2020

Portefeuille: ICT en Digitale Stad (42)

Agendapunt: B11

Tekst van openbare besluiten wordt gepubliceerd

**Onderwerp**

Instemmen met het Stedelijk kader informatiebeveiliging gemeente Amsterdam
OPENBAAR GEMAAKT OP 17-12-2020

**Het college van burgemeester en wethouders besluit**

1. **In te stemmen met het *Stedelijk kader informatiebeveiliging gemeente Amsterdam*. Dit beleidskader informatiebeveiliging geeft richting geven aan de wijze waarop informatie van de gemeente Amsterdam wordt beveiligd.**
2. **Kennis te nemen van de bijlage *Organisatie van de informatiebeveiliging bij de gemeente Amsterdam*, waarin de rollen en verantwoordelijkheden zijn beschreven.**
3. **Kennis te nemen van de Rapportage informatiebeveiliging 2018 – 2019.**
4. **Kennis te nemen van de Rapportage gegevensbescherming 2018 – 2019.**
5. **De verzending van bijgevoegde Raadsbrief inclusief de rapportages aan de raadscommissie Kunst, Democratisering en Diversiteit.**

**Kernboodschap**

Het college heeft ingestemd met het Stedelijk kader informatiebeveiliging gemeente Amsterdam. Dit geeft richting aan de wijze waarop we onze informatie beveiligen en bevat de belangrijkste beleidsuitgangspunten. Het informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Overheid, waarin de normen voor informatiebeveiliging voor de gehele overheid zijn opgenomen.

**Bestuurlijke achtergrond**

Op 12 juli 2016 heeft het college het Informatiebeveiligingsbeleid gemeente Amsterdam vastgesteld. Dit beleid is gebaseerd op de toen geldende Baseline Informatiebeveiliging Gemeenten (BIG). Het informatiebeveiligingsbeleid van de gemeente Amsterdam wordt (verplicht) periodiek geactualiseerd. Inmiddels is de BIG per 1 januari 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). Hierin zijn uniforme beveiligingsnormen openomen, die gelden voor alle bestuurslagen van de overheid. Het voorliggende Stedelijk kader informatiebeveiliging gemeente Amsterdam is gebaseerd op de BIO.

In het collegebesluit over de eindrapportages ICT Centraal en Applicatierationalisatie van 19 december 2017 (ZD2017-005362) is de opdracht verstrekt aan de gemeentesecretaris om jaarlijks bestuurlijk te rapporteren over informatiebeveiliging. De bijgevoegde rapportage informatiebeveiliging is een rapportage zoals bedoeld in de bovengenoemde opdracht. De rapportage van de functionaris gegevensbescherming komt voort uit haar wettelijke verplichting om verslag uit te brengen aan de hoogste leidinggevende van de verwerkingsverantwoordelijke (in dit geval het college en de raad).

**Bestuurlijke prioriteit**

Niet van toepassing

**Wettelijke grondslag**

- Art. 160, eerste lid onder a, Gemeentewet: het college is bevoegd om het dagelijks bestuur van de gemeente te voeren.

- Art. 169, eerste en tweede lid, Gemeentewet: het college van burgemeester en wethouders en elk van zijn leden afzonderlijk zijn aan de gemeenteraad verantwoording schuldig over het door het college gevoerde bestuur. Zij geven de raad alle inlichtingen die de raad voor de uitoefening van zijn taak nodig heeft.
- Art 38, derde lid, van de Algemene verordening gegevensbescherming (AVG) schrijft voor dat de Functionaris Gegevensbescherming rechtstreeks verslag uitbrengt aan de hoogste leidinggevende van de verwerkingsverantwoordelijke (in dit geval het college en de raad). De Functionaris Gegevensbescherming is de interne toezichthouder op de gemeentelijke omgang met persoonsgegevens.

**Onderbouwing besluit**

**Ad 1: instemmen met het Stedelijk kader informatiebeveiliging gemeente Amsterdam**

**Ad 2: kennisnemen van de bijlage *Organisatie van de informatiebeveiliging bij de gemeente Amsterdam***

Net als alle andere overheidsinstellingen is de gemeente Amsterdam gebonden aan de Baseline Informatiebeveiliging Overheid (BIO). Hierin zijn uniforme beveiligingsnormen openomen, die gelden voor alle bestuurslagen van de overheid. De BIO schrijft voor dat elke overheidsinstelling een strategisch informatiebeveiligingsbeleid opstelt. In ons geval is dat het Stedelijk kader informatiebeveiliging gemeente Amsterdam. Dit document is hoog-over: het bevat de belangrijkste beleidsuitgangspunten en geeft richting aan de wijze waarop we onze informatie beveiligen.

Informatiebeveiliging heeft ten doel dat Amsterdamse informatie beschikbaar, betrouwbaar en beschermd is. Informatiebeveiliging is de basis voor een goed functionerende organisatie met een weerbare informatievoorziening. Het is daarbij van belang dat informatie passend wordt beschermd. De organisatie treft daarvoor integraal en vóóraf - niet pas achteraf - passende beschermende maatregelen, op alle niveaus.

We hanteren daarbij de volgende uitgangspunten:

- De aanpak van informatiebeveiliging is risico-gebaseerd;
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement;
- Elk informatiesysteem heeft een eigenaar die onder andere verantwoordelijk is voor informatiebeveiliging;
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging;
- Toegang tot informatie wordt alleen verstrekt wanneer dit nodig is voor de functie/ rol of taak die iemand heeft, volgens het principe 'need to know';
- Elke medewerker, vast of tijdelijk en zowel intern als extern, is verplicht gegevens en informatiesystemen waar nodig te beschermen tegen onbevoegde toegang, gebruik,
- verandering, openbaring, vernietiging, verlies of overdracht;
- Elke medewerker meldt geconstateerde of vermoede inbreuken op de informatievoorziening direct aan het lijnmanagement en aan een daarvoor bestemde servicedesk en/of meldpunt;
- Er is een Chief Information Security Officer (CISO) aangesteld conform een vastgesteld functieprofiel.

Het *Stedelijk kader informatiebeveiliging gemeente Amsterdam* vervangt het Informatiebeveiligingsbeleid Gemeente Amsterdam uit 2016. Het nieuwe beleidskader is gebaseerd op de nieuwste internationale basisnormen voor Informatiebeveiliging, en toegespitst op het tegengaan van de meest recente bekende dreigingen op de

informatieveiligheid. Voor de invoering van het beleid is een meerjarenplan opgesteld, waarbij de aanpak gebaseerd is op het beheersen van risico's. Het is ook aangepast op de sinds 2016 de gewijzigde organisatie.

De taken, verantwoordelijkheden en bevoegdheden zijn uitgewerkt in de bijlage Organisatie van de informatiebeveiliging bij de gemeente Amsterdam. Het concrete 'hoe' wordt beschreven in onderliggende kaders en procedures op deelterreinen als toegangsbeveiliging, autorisatie of flexwerken, die ambtelijk worden vastgesteld.

**Ad 3: kennisnemen van de *Rapportage informatiebeveiliging 2018 – 2019***

De Rapportage informatiebeveiliging beschrijft de activiteiten, incidenten en ontwikkelingen ten aanzien van informatieveiligheid bij de gemeente Amsterdam over de jaren 2018 en 2019 en geeft ook een vooruitblik op 2020.

In 2018 zijn 20 incidenten met een hoge impact gemeld en in 2019 32. Daarvan was 75% (in 2018) respectievelijk 50% (in 2019) het gevolg van menselijke fouten. In aanvulling op de cijfers uit de bijgevoegde rapportage kan nog worden gemeld dat het aantal incidenten met een hoge impact in het eerste helft van 2020 33 bedroeg. De aantallen informatiebeveiligingsincidenten zijn vergelijkbaar met andere grote gemeenten.

Daarnaast neemt het aantal incidenten waarbij wordt gepoogd om van buitenaf toegang te krijgen tot gegevens of de gemeentelijke ICT-infrastructuur toe. Dit is in lijn met het landelijke beeld zoals het Nationaal Cyber Security Centrum (NCSC) dat schetst. Door toename van (cyber)dreigingen en risico's moet de gemeente continu inzetten op het verhogen van de weerbaarheid tegen steeds veranderende dreigingen. Dit gebeurt zowel door het nemen van organisatorische en technische maatregelen (ICT) als door het trainen en bewust maken van medewerkers. De Chief Information Security Officer (CISO) van de gemeente Amsterdam waarschuwt dat het van belang blijft continu de vinger aan de pols te houden: of de getroffen maatregelen voldoende zijn om beveiligingsrisico's af te dekken, of er door achterstallig onderhoud geen zogeheten achterdeurtjes zijn ontstaan in de informatievoorziening, of deze voldoende weerbaar is tegen cybercrime, en of de kennis en vaardigheden van het personeel op peil zijn.

Vanaf nu zal er jaarlijks een rapportage informatiebeveiliging worden opgesteld.

**Ad 4: kennisnemen van de Rapportage gegevensbescherming 2018 – 2019**

Op 25 mei 2018 werd de Algemene verordening gegevensbescherming (AVG) van kracht. De Rapportage gegevensbescherming beschrijft de acties en maatregelen die de gemeente Amsterdam in 2018 en 2019 heeft getroffen om de beginselen van de AVG te waarborgen en de doelstellingen te behalen. Zo is onder andere het Stedelijk kader verwerken persoonsgegevens door het college vastgesteld, is één digitaal loket voor burgers in gebruik genomen en is een verwerkingenregister ingericht waarin de activiteiten waarbij de gemeente persoonsgegevens verwerkt, worden geregistreerd.

Vanaf mei 2018 tot 1 januari 2019 heeft het gemeentelijk meldpunt datalekken 74 datalekken geregistreerd waarvan er 42 bij de Autoriteit Persoonsgegevens zijn gemeld. Over de periode 1 januari 2019 tot 1 januari 2020 zijn 156 datalekken geregistreerd waarvan er 38 bij de Autoriteit Persoonsgegevens zijn gemeld (datalekken worden niet gemeld wanneer geen sprake is van nadelige gevolgen voor de burger of werknemer). In beide jaren is er in twee-derde van de datalekken sprake van het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. In aanvulling op de cijfers uit de rapportage kan nog worden gemeld dat er in de eerste helft van 2020 111 datalekken geregistreerd, waarvan er 27 gemeld zijn bij de landelijk toezichthouder (Autoriteit Persoonsgegevens).

De Autoriteit Persoonsgegevens heeft statistisch onderzoek uitgevoerd naar datalekregistraties bij overheidsorganisaties, waarbij onder andere het aantal gemelde datalekken is afgezet tegen de grootte van de organisatie. Hieruit kunnen we concluderen dat de gemeente Amsterdam in absolute aantallen ongeveer net zo vele datalekken meldt als kleinere organisaties. Het aantal datalekken dat binnen de gemeente wordt gemeld lijkt daarmee klein in verhouding tot de grootte van de gemeente. De oorzaak hiervan is niet bekend, maar de Functionaris Gegevensbescherming vermoedt dat nog niet alle datalekken binnen organisatie worden gemeld. De norm is dat alle datalekken gemeld worden bij de Functionaris Gegevensbescherming, waarna de Functionaris Gegevensbescherming beoordeelt of het lek bij de Autoriteit Persoonsgegevens wordt gemeld omdat er nadelige gevolgen voor burgers of werknemers zijn. De gemeentelijke organisatie wordt hiervan doorlopend bewustgemaakt.

De Functionaris Gegevensbescherming merkt in haar rapportage op dat gegevensbescherming als onderdeel van de organisatie en aantoonbaar voldoen aan de relevante wet- en regelgeving geen afvinklijst is, maar een continu proces. Het vraagt om structurele borging van dit onderwerp. Waar 2018 in het teken stond van de voorbereiding op de AVG en het treffen van de nodige maatregelen, stond 2019 in het teken van het borgen van de governance, het verder op orde brengen van de basis en de training en bewustwording van de organisatie. Dit wordt in 2020 gecontinueerd.

Vanaf nu zal er jaarlijks een rapportage gegevensbescherming worden opgesteld.

**Ad 5. De verzending van bijgevoegde Raadsbrief inclusief de rapportages aan de raadscommissie Kunst, Democratisering en Diversiteit.**

**Participatie**

Niet van toepassing

**Financiële onderbouwing**

**Conclusie**

De genoemde beslispunten in de voordracht hebben geen financiële consequenties.

**Communicatie**

Binnen de gemeente

Opnemen in de te publiceren besluitenlijst. De raadsbrief en rapportages worden via de dagmail verzonden.

Buiten de gemeente

Niet van toepassing

**Documenten**

| Registratienr. | Naam |
|---|---|
| AD2020-095693 | Advies (pdf) |
| AD2020-098919 | B - 11 Getekende brief VN2020-029441.pdf (pdf) |
| AD2020-095690 | BRIEF Raadsbrief informatiebeveiligingsbeleid.docx (msw12) |
| AD2020-095631 | Bijlage 1 Stedelijk kader informatiebeveiliging gemeente Amsterdam.pdf (pdf) |
| AD2020-095633 | Bijlage 2 Organisatie van informatiebeveiliging bij de gemeente Amsterdam.pdf (pdf) |
| AD2020-095634 | Bijlage 3 Rapportage informatiebeveiliging 2018-2019.pdf (pdf) |
| AD2020-095632 | Bijlage 4 Rapportage gegevensbescherming 2018-2019.pdf (pdf) |
| AD2020-095628 | College van B&W Voordracht (pdf) |

**Behandelend ambtenaar (naam, telefoonnummer en e-mailadres)**

CIO Office Chief Information Security Officer: [redacted] ([redacted]@amsterdam.nl of 06 – [redacted]) CIO Office Functionaris Gegevensbescherming: [redacted]@amsterdam.nl of 06 – [redacted])

**Besluit college van burgemeester en wethouders**

Conform besloten, voorts wordt de portefeuillehouder gemachtigd tot het bepalen van het moment van openbaarmaking