Gemeente Amsterdam

Vastgesteld 25 september 2018

Taken en verantwoordelijkheden bij het verwerken van persoonsgegevens door de gemeente Amsterdam

Taken en verantwoordelijkheden

Het Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam maakt zowel bestuurlijk als ambtelijk duidelijk hoe de gemeente Amsterdam om gaat met de verwerking van persoonsgegevens.

Organisatorisch kader
Het organisatorisch kader voor de taken en verantwoordelijkheden maakt duidelijk wat de rol, taken en verantwoordelijkheden zijn van de betrokken bestuurlijke en ambtelijke actoren op het gebied van de verwerking van persoonsgegevens in de gemeente Amsterdam.

Het organisatorisch kader ziet er als volgt uit:

Bestuurlijk:

College B&W, Burgemeester,
Het College van Burgemeester en Wethouders, dan wel de Burgemeester, ieder vanuit hun eigen taak en bevoegdheid[1], verantwoordelijk voor de verwerkingen van persoonsgegevens die door of namens de gemeente worden uitgevoerd. Zij zijn dan ook de verantwoordelijke in de zin van de wet.

Portefeuillehouder ICT
De portefeuillehouder ICT heeft de stelselverantwoordelijkheid voor het verwerken van persoonsgegevens en is verantwoordelijk voor:
- het door het College laten vaststellen van generiek beleid voor het verwerken van persoonsgegevens;
- het initiëren van flankerende activiteiten om de bescherming van persoonsgegevens binnen de organisatie te bevorderen, zoals een communicatieplan, training en bewustwording van medewerkers, risicomanagement en de informatie aan Amsterdammers over de wijze waarop de gemeente Amsterdam omgaat met informatie en de wijze waarop deze gebruik kan maken van zijn/ haar rechten ingevolge de wet.

Burgemeester
De Burgemeester is verantwoordelijk voor:
- De rechtmatigheid[2] van de verwerking van persoonsgegevens, waarvoor de Burgemeester verwerkingsverantwoordelijke is.

Vakportefeuilles
Daar waar de Burgemeester portefeuillehouder is op een domein en het een verwerking van persoonsgegevens betreft waarvoor het college de verwerkingsverantwoordelijke is, is de burgemeester te beschouwen als een vakportefeuillehouder.

[1] De Raad is verantwoordelijk voor de verwerkingsactiviteiten in het kader van de uitoefening van taken van de Raad.
[2] Met rechtmatigheid wordt telkens bedoeld de compliance aan wet- en regelgeving op het gebied van de bescherming van persoonsgegevens en het Stedelijk kader verwerken persoonsgegevens door de gemeente Amsterdam.

De vakportefeuillehouders zijn -politiek- verantwoordelijk voor

- De rechtmatigheid van de verwerking van persoonsgegevens van de RVE's of van stadsdelen die binnen zijn/haar eigen vakportefeuille vallen, zoals Dienstverlening, Jeugd, Onderwijs, Zorg, Participatie, Handhaving, Basisinformatie, Onderzoek, Informatie en Statistiek;
- Het ter besluitvorming aan het college voorleggen van complexe en/of politiek gevoelige verwerkingen van persoonsgegevens.

Ambtelijk, stelselverantwoordelijkheid

Chief Information Officer (CIO)
De Chief Information Officer (CIO) is verantwoordelijk voor het laten vaststellen van beleid voor het verwerken van persoonsgegevens in relatie tot het technische informatiebeveiligingsbeleid van de gemeente. De Chief Information Security Officer (CISO) ziet toe op de naleving van het informatiebeveiligingsbeleid. De CIO, de CISO en de Functionaris Gegevensbescherming werken samen daar waar informatiebeveiliging en privacy in elkaar grijpen.

De Chief Information Officer (CIO) heeft de volgende taken:
- In opdracht van de Wethouder ICT formuleren en beheren van kaderstellende afspraken voor het gebruik van persoonsgegevens en voor informatieveiligheid bij het verwerken van privacygevoelige gegevens;
- Bewustwording van medewerkers op het gebied van informatiebeveiliging en bescherming persoonsgegevens;
- Het inrichten van het risicomanagement ten aanzien van de bescherming van persoonsgegevens.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) is de interne toezichthouder en brengt advies uit over de naleving van het stedelijk kader en verplichtingen ingevolge de wet.

De Functionaris Gegevensbescherming heeft de volgende taken:
1) De verantwoordelijke of de verwerker informeren en adviseren over hun verplichtingen uit hoofde van de AVG en andere gegevensbeschermingsbepalingen;
2) Toezien op het naleven van de AVG en andere gegevensbeschermingsbepalingen en van het beleid van de verantwoordelijke of de verwerker m.b.t. de bescherming van persoonsgegevens (i.c. het stedelijk kader), met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
3) Desgevraagd advies verstrekken m.b.t. de gegevensbeschermingseffectbeoordeling (data protection impact assessment) en toezien op de uitvoering daarvan;
4) Met de toezichthoudende autoriteit (Autoriteit Persoonsgegevens) samenwerken;
5) Optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden.
6) Het in stand houden van het register van verwerkingsactiviteiten;
7) Melding doen bij de Autoriteit Persoonsgegevens in het kader van de meldplicht datalekken en het bijhouden van het register van datalekken;
8) Behandeling van vragen en klachten van Amsterdammers en voorlichting;
9) Het adviseren en rapporteren aan de gemeentesecretaris;
10) Jaarlijkse rapportage aan het College en de Raad.

De Functionaris Gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

Ambtelijk, lijnverantwoordelijkheid:

Stedelijk directeur

- De stedelijk directeur ziet toe op de naleving van het stedelijk kader en op de samenhang daar waar domein-overstijgende uitwerking vereist is.

Rve-directeur/ dagelijks bestuur van het stadsdeel

De betrokken rve-directeur dan wel het dagelijks bestuur van het stadsdeel is verantwoordelijk voor:

- Het -indien aan de orde- opstellen en aan het via de vakwethouder aan het college ter besluitvorming aanbieden van uitwerkingen van het beleid m.b.t. verwerking van persoonsgegevens.
- De rechtmatigheid van de verwerking van persoonsgegevens binnen zijn/haar werkgebied. De beslissing over de gegevensverwerking wordt genomen met inachtneming van de vastgestelde kaders en het beleid.
- Het namens de verantwoordelijke uitvoeren van de taken verband houdende met de rechten van de betrokkene zoals omschreven in hoofdstuk III van de Algemene Verordening Gegevensbescherming (artikelen 12 tot en met 21 van de AVG).
- Het maken van transparante afspraken met andere, gezamenlijke, verantwoordelijken in de zin van artikel 26 AVG.
- Het sluiten van overeenkomsten met verwerkers als bedoeld in artikel 28 AVG.
- Het inschrijven van (wijzigingen van) verwerkingen van persoonsgegevens waarvoor een registratieplicht geldt in het register van de verwerkingsactiviteiten als bedoeld in artikel 30 AVG.
- Het nemen van beslissingen over het dichten van geconstateerde datalekken en de melding daarvan aan de betrokkenen;
- Het treffen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen;
- Het borgen van privacy by design en privacy by default;
- Voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande verwerkingen, met waarschijnlijk een hoog risico voor de rechten en vrijheden van personen, worden de privacy risico's in beeld gebracht en indien vereist toont de directeur/dagelijks bestuur door middel van een data protection impact assessment aan, dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd. De directeur/dagelijk bestuur zal advies over data protection impact assessments inwinnen bij de privacy-officer en in geval van complexe gegevensverwerking bij de Functionaris Gegevensbescherming.
- Het voorafgaand raadplegen van de Autoriteit Persoonsgegevens over risico's indien de AVG dit vereist.
- Het treffen van waarborgen in de zin van de AVG en zoals voorgeschreven door de Europese Commissie en/of de Autoriteit Persoonsgegevens, bij doorgifte aan derde landen of een internationale organisatie[3];
- Het sturen op bewustzijn en naleving van het beleid bij medewerkers van het organisatieonderdeel.
- Het rapporteren over de naleving van wet- en regelgeving en het stedelijk kader aan de CIO/FG.
- Indien er sprake is van een situatie van complexe gegevensverwerking en/of politiek gevoelige gegevensverwerking, zal de directeur/dagelijks bestuur voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande verwerkingen tevens advies inwinnen bij de Commissie Persoonsgegevens Amsterdam.

[3] Dit doet zich als er een verwerker wordt ingeschakeld die de gegevens opslaat op een server die zich bevindt in een land buiten de Europese Unie dat niet voorkomt op de lijst van landen waarvan de Europese Commissie heeft vastgesteld dat de bescherming van de privacy er adequaat geborgd is.

Directeur OOV
De directeur OOV is (namens de Burgemeester) verantwoordelijk voor:

- Het indien aan de orde opstellen en aan de Burgemeester ter besluitvorming aanbieden van een uitwerking van het beleid met betrekking tot persoonsgegevens.
- De rechtmatigheid van de verwerking van persoonsgegevens. De beslissing over de gegevensverwerking wordt genomen met inachtneming van de vastgestelde kaders en het beleid.
- Het namens de verantwoordelijke uitvoeren van de taken verband houdende met de rechten van betrokkene zoals omschreven in zoals omschreven in hoofdstuk III van de Algemene Verordening Gegevensbescherming (artikelen 12 tot en met 21 van de AVG).
- Het maken van transparante afspraken met andere, gezamenlijke, verantwoordelijken in de zin van artikel 26 AVG.
- Het sluiten van overeenkomsten met verwerkers als bedoeld in artikel 28 AVG.
- Het inschrijven van (wijzigingen van) verwerkingen van persoonsgegevens waarvoor een registratieplicht geldt in het register van de verwerkingsactiviteiten als bedoeld in artikel 30 AVG.
- Het nemen van beslissingen over het dichten van geconstateerde datalekken en de melding daarvan aan de betrokkenen.
- Het treffen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen;
- Het borgen van privacy by design en privacy by default;
- Voordat een beslissing wordt genomen over nieuwe of wijzingen van bestaande verwerkingen, met waarschijnlijk een hoog risico voor de rechten en vrijheden van personen, worden de privacy risico's in beeld gebracht en indien vereist toont de directeur door middel van een data protection impact assessment aan, dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd. De directeur zal advies over data protection impact assessments inwinnen bij de privacy-officer en in geval van complexe gegevensverwerking bij de Functionaris Gegevensbescherming.
- Het voorafgaand raadplegen van de Autoriteit Persoonsgegevens over risico's indien de AVG dit vereist.
- Het vaststellen van passende waarborgen bij doorgifte aan derde landen of een internationale organisatie.
- Het sturen op bewustzijn en naleving van het beleid bij medewerkers van het organisatie-onderdeel.
- Het rapporteren over de naleving van wet- en regelgeving en het stedelijk kader aan de CIO/FG.
- Indien er sprake is van een situatie van complexe gegevensverwerking en/of politiek gevoelige gegevensverwerking, zal de directeur voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande verwerkingen tevens advies inwinnen bij de Commissie Persoonsgegevens Amsterdam.

Privacy officer
De Privacy officers (gepositioneerd in de clusters) zijn belast met de coördinatie en uitvoering van het beleid inzake het verwerken van persoonsgegevens van de organisatieonderdelen die onder het cluster ressorteren.

Tot de taken van de Privacy officer behoren in ieder geval:

- Het adviseren over nieuwe of aangepaste verwerkingen in het licht van wettelijke verplichtingen en de naleving van het stedelijk kader.
- Het uitoefenen van het eerstelijns toezicht op de verwerking van persoonsgegevens.
- Het opstellen van en het houden van toezicht op het gebruik van privacy protocollen en verwerkersovereenkomsten.
- Advies over transparante afspraken met andere, gezamenlijke, verantwoordelijken in de zin van artikel 26 AVG.

- Het controleren, onderhouden en aanvullen van het register van verwerkingsactiviteiten, die binnen de rve's/stadsdelen die onder het cluster ressorteren, plaatsvinden.
- Alle handelingen aangaande de meldplicht datalekken die het organisatieonderdeel aangaan. Met uitzondering van het doen van de melding bij de Autoriteit Persoonsgegevens, die taak ligt bij de Functionaris Gegevensbescherming.
- Adviseren aangaande de verwerking van persoonsgegevens en data protection impact assessments.
- Advies over de verplichting om de Autoriteit Persoonsgegevens voorafgaand te raadplegen over risico's indien de AVG dit vereist.
- Een actieve bijdrage aan de ontwikkeling van bewustzijn en kennis van het beleid bij medewerkers.
- Het rapporteren over de naleving van wet- en regelgeving en het stedelijk kader aan de CIO/FG.

Contactpersoon voor de gegevensbescherming
Elk organisatieonderdeel heeft een contactpersoon die belast is met het signaleren van vraagstukken betreffende de uitvoering van verplichtingen in de AVG en het stedelijk kader verwerken persoonsgegevens in het betreffende organisatieonderdeel.

Commissie Persoonsgegevens Amsterdam (CPA)
Het College van Burgemeester en Wethouders heeft de Commissie Persoonsgegevens Amsterdam ingesteld. Deze commissie adviseert het College omtrent de gegevensverwerking in breedste zin. De werkwijze van de commissie en met name het houden van – in beginsel – openbare vergaderingen en uitbrengen van adviezen, draagt bij aan de transparantie rondom de verwerking van persoonsgegevens door de gemeente.
De Commissie Persoonsgegevens Amsterdam heeft in 2011 zowel een toezichthoudende als een adviserende rol gekregen. De interne toezichthoudende rol komt vanaf mei 2018 bij de Functionaris Gegevensbescherming te liggen.

De CPA heeft de volgende taak:
Gevraagd en ongevraagd adviseren van de verantwoordelijke over complexe en/of politiek gevoelige gegevensverwerking met inachtneming van de wet- en regelgeving, en de maatschappelijke en technologische ontwikkelingen. Indien de FG en de CPA conflicterende adviezen of verschillen van inzicht hebben, is het advies van de FG leidend. In dat geval wordt het besluit over de gegevensverwerking door de betrokken rve- directeur dan wel het dagelijks bestuur van het stadsdeel voorgelegd aan de verantwoordelijke.

Datalek
Iedere medewerker, verwerker of een ieder ander die een datalek constateert waarvoor het College of de Burgemeester of de Raad verantwoordelijk is, volgt het proces datalekken zoals vastgesteld in het GMT. De Functionaris Gegevensbescherming verricht, in afstemming met de Privacy officer van het cluster en de betrokken rve-directeur of het dagelijks bestuur van het stadsdeel, de melding van het datalek bij de Autoriteit Persoonsgegevens. De rve-directeur/dagelijks bestuur van het stadsdeel is verantwoordelijk voor het dichten van het datalek onder advisering van de Functionaris Gegevensbescherming en de Chief Information Security Officer (CISO). De rve-directeur dan wel het dagelijks bestuur van het stadsdeel doet - indien vereist- de melding van een inbreuk in verband met persoonsgegevens aan de betrokkene.

Organisatie van gegevensbescherming

Rapportage en escalatielijn is als volgt:
De rapportage en escalatielijn is als volgt: Privacy Officer -> FG -> Gemeentesecretaris / verantwoordelijke.
De FG rapporteert aan de gemeentesecretaris. Jaarlijks brengt de FG verslag uit aan het College en de Raad.

Landelijk overleg
De FG is -onder meer- vertegenwoordigd in het G4-privacy overleg, het privacy overleg van het landelijke CIO-platform.