Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam

**Gemeente Amsterdam**
**Commissie Persoonsgegevens**

PER E-mail
Gemeente Amsterdam
Mevrouw A. Bouchlas, directeur Personeel en Organisatieadvies
Mevrouw 5.1, 2, e , IV manager Bedrijfsvoering
De heer 5.1, 2, e , RVE PO, Cluster Bedrijfsvoering
Kopie: 5.1, 2, e , Privacy- en Informatiebeveiligingscoördinator, de heer J. Verhoeven (adviseur Privacy- en Informatiebeveiliging)
Kopie CIO, de heer J. Flippo

| | |
|---|---|
| Datum | 19 mei 2016 |
| Ons kenmerk | U160048 |
| Behandeld door | Mw. 5.1, 2, e |
| Doorkiesnummer | 5.1, 2, e |
| Faxnummer | nvt |
| E-mail | 5.1, 2, e @amsterdam.nl |
| Bijlage | 1 |
| Onderwerp | Advies Commissie Persoonsgegevens Amsterdam |

Geachte heer, mevrouw,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 14 april 2016 was namens u een vertegenwoordiging aanwezig van de gemeente Amsterdam. Bij het agendapunt "Protocol gegevensverwerking personen werkzaam voor gemeente Amsterdam" heeft de CPA het navolgende besproken.

De CPA adviseert positief over het protocol. Wel vraagt de CPA expliciet aandacht voor beveiligingsaspecten, waaronder controles van autorisaties en van logging. De CPA vraagt om het protocol en de invoering daarvan na een jaar te evalueren.

Bijgaand treft u een zakelijke samenvatting aan van hetgeen over het agendapunt is besproken. Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Hoogachtend,

5.1, 2, e

Mr. dr. U. van de Pol
Voorzitter Commissie Persoonsgegevens Amsterdam

**Commissie Persoonsgegevens Amsterdam**
**Uittreksel van het concept-verslag van de openbare vergadering op donderdag 14 april 2016**

**9.Protocol gegevensverwerking personen werkzaam voor gemeente Amsterdam (PO&A, Cluster Bedrijfsvoering)**
Het protocol heeft een lange voorgeschiedenis. Het dateert van 2007. Het moest worden aangepast. Na de reorganisatie van 1 januari 2015 is gewacht op het mandaatbesluit zodat daarbij kon worden aangesloten. De situatie met betrekking tot de gegevensverwerking is veranderd. Het protocol is van toepassing op persoonsgegevens van mensen die voor de gemeente Amsterdam werkzaamheden verrichten.

De CPA zegt dat het handig is om een standaard dataset te hebben van een ambtenaar. Gevraagd wordt welke persoonsgegevens er gemiddeld van een ambtenaar worden geregistreerd.

Personeel en Organisatieadvies (POA) zegt dat bijvoorbeeld betaalgegevens gedurende zeven jaar worden bewaard. Indien een medewerker in actieve dienst is worden naam, adres, woonplaats geregistreerd en geboortedatum, geslacht, eventuele partner en geboortedatum partner, burgerservicenummer, functie, inschaling, beoordelingen, functioneringsgesprekken, ziekteverzuim, orde- en disciplinemaatregelen in het kader van de rechtspositieregeling (NRGA), en bijvoorbeeld gegevens over etniciteit in geval van toestemming mits dit het inclusiebeleid dient.
Er kunnen verwerkingen van het bestand zijn door andere organisatieonderdelen. POA heeft bijvoorbeeld een mobiliteitscentrum (vrijwillige en verplichte mobiliteit), daar wordt een aparte administratie bijgehouden. Er is een rol voor de directeur van POA om daar voorwaarden aan te stellen als beheerder. Deze krijgt een exclusieve rol en moet akkoord geven voor het verwerken van persoonsgegevens uit het personeelsbestand. De bedrijfsarts heeft een apart systeem. Er mogen geen medische persoonsgegevens worden verwerkt door de gemeente. Er mogen ook geen medische gegevens in verslagen staan. Het protocol is een kader om afspraken over gegevensleveringen bij te sturen. Doordat de personeel- en organisatiefunctie nu zijn gecentraliseerd, is het ook mogelijk dat de directeur van POA exclusiviteit krijgt in de rol van beheerder.

De CPA vraagt of de kaders die in het protocol worden geschapen ook worden gecontroleerd. Wordt bijvoorbeeld gecontroleerd of mobiliteitsafspraken vertrouwelijk blijven en medische persoonsgegevens niet verwerkt worden in de bestanden.

Geantwoord wordt dat er een ziekteverzuimproject loopt waarbij een memoveld vormvrij was. Er worden nu instructies gemaakt wat er wel en niet met de formats gedaan mag worden.

De operationele processen worden nog geïmplementeerd. Bijvoorbeeld wordt vastgelegd waar die persoonsgegevens voor dienen, die niet centraal beheerd worden en hoe lang deze bewaard mogen worden.

De CPA vraag hoeveel ambtenaren de gemeente Amsterdam heeft.

Geantwoord wordt dat dit rond de 13.000 ambtenaren zijn.
Er is ook een ontwikkeling naar een kernregistratie voor medewerkers die niet in dienst zijn. Daar zou dan een subset voor komen. Er was nu nog te veel discussie wie daaronder zouden vallen.

De CPA vraagt aandacht voor het loggen, en controleren van autorisaties en het detecteren van datalekken.

Geantwoord wordt dat uitkeringsinformatie van het UWV komt. Het burgerservicenummer wordt verwijderd en veranderd in namen zodat de informatie op de juiste plaats kan worden opgeslagen. In het proces zitten dus checks and balances verweven. In het protocol is nu geborgd dat afspraken over informatieveiligheid door de beheerder met andere organisatieonderdelen gemaakt worden. De autorisaties zijn op meerdere plaatsen geregeld. In grote lijnen zijn bij POA rollen beschreven. Als de applicaties niet bij POA staan kan de beheerder voorwaarden stellen omdat persoonsgegevens uit het centrale systeem geleverd worden.
De CPA vraagt hoe de controle op het dagelijks gebruik van het systeem geregeld is.

Geantwoord wordt dat een controle op rol gedaan wordt en dat de autorisaties zijn verleend. Bij het pasjessysteem van Facilitair kan bijvoorbeeld bij het leveren van persoonsgegevens uit het centrale bestand een eis gesteld worden over logging.

De CPA vraagt opnieuw aandacht voor de achterkant van het proces.
Er zijn meerdere systemen van POA die gemonitord zouden moeten worden. Maar er zijn ook systemen buiten POA om waarin persoonsgegevens uit het personeelsbestand zitten. Daar zijn anderen eigenaar van.

Geantwoord wordt dat een opdracht aan de projectleider moet worden gegeven. Er moeten afspraken gemaakt worden welke applicatie-eigenaar voor de logging en monitoring moet zorgdragen.

De CPA vraagt naar het recht op inzage. Waarom staat vermeld dat de beheerder binnen vier weken een begrijpelijk overzicht van relevante persoonsgegevens verstrekt. Wie bepaalt wat relevant is.

Geantwoord wordt dat het woord 'relevant' wordt geschrapt.
Bepaalde systemen zoals MijnPersoneelsnet (MPN) maken het mogelijk dat de medewerker zijn eigen persoonsgegevens inziet.

Advies:
De CPA adviseert positief over het protocol. Expliciet wordt aandacht gevraagd voor beveiliging, waaronder een controle op autorisaties en logging. De CPA vraagt om een evaluatie na een jaar.