Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam

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

**PER E-MAIL**
De heer R. Hoff, directeur Handhaving & Toezicht
De heer 5.1 5.1, 2, e , manager IVE
Dienstverlening & Informatie
Kopie: CIO, J. Flippo
Kopie: de heer 5.1, 2, e (IVE cluster D&I), mw. 5.1, 2, e 5.1, 2, e (IVE Stadsdelen)

| | |
|---|---|
| Datum | 3 oktober 2016 |
| Ons kenmerk | U16104 |
| 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 Hoff en heer 5.1, 2, e ,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 25 augustus 2016 was u vertegenwoordigd bij het agendapunt 'Privacy Impact Assessment Mobiele Handhaving'. Bijgaand treft u het deel van de zakelijke weergave aan van hetgeen op de vergadering over het betreffende agendapunt is besproken.

De CPA overweegt over de privacy impact assessment als volgt.

Er is sprake van een aanbesteding van een systeem voor mobiele handhaving waarbij gekozen is voor smartphones. Er worden om het risico dat daarmee gepaard gaat af te dekken, extra organisatorische en technische maatregelen getroffen, zoals dubbele authenticatie en de smartphones zijn persoonsgebonden.
De CPA acht het voor de informatieveiligheid en de bescherming van persoonsgegevens van belang dat er geen informatie op de smartphone kan worden opgeslagen, en uitsluitend gebruik gemaakt wordt van door de gemeente ter beschikking van de Buitengewoon opsporingsambtenaren (BOA) gestelde app's.

De CPA wijst er op dat de BOA de verantwoordelijke is in de zin van Wet bescherming persoonsgegevens voor de verwerking van persoonsgegevens in het kader van de hem bij akte toegekende bevoegdheden.
De Burgemeester is belast met de handhaving van de Openbare Orde en Veiligheid en de namens hem met Openbare en Orde en Veiligheid belaste ambtenaren verwerken ook

persoonsgegevens. Ook is de gemeente Amsterdam opdrachtgever voor het ontwikkelen van het ter beschikking van de BOA gestelde middel.
Om deze reden zijn er meerdere verantwoordelijken. Het is van belang de verantwoordelijkheden en de taken die daarbij horen goed te duiden en dat de BOA's goed worden opgeleid om met strafrechtelijke informatie om te gaan.

De CPA signaleert dat nieuwe middelen ook nieuwe technologische mogelijkheden hebben, en dat het daarom van belang is om van te voren te bepalen van welke mogelijkheden gebruik gemaakt wordt en zo niet, dat dit gebruik onmogelijk gemaakt wordt. Ook is van belang bij gebruikte toepassingen op welke wijze privacy in het design gebracht kan worden. Dit zal in de PIA expliciet naar voren moeten komen, zonder dat er nog zaken opengelaten worden.

Zo begrijpt de CPA bijvoorbeeld dat de camerafunctie niet gebruikt zal worden. Er zal wel gebruik gemaakt worden van een scanner om het burgerservicenummer van een identiteitskaart in te lezen. GPS- locaties zullen dienen voor het spreiden van de BOA's in verband met themagericht handhaven. De Ondernemingsraad zal dan ook betrokken worden bij het gebruik van de GPS-data ten behoeve van een personeelsvolgsysteem. Op deze wijze is de afbakening van het gebruik bij elke toepassing wenselijk.

De CPA constateert dat het systeem gebruikt zal worden voor de uitoefening van verschillende soorten bevoegdheden, zoals een waarschuwing, een waarneming, of het opleggen van een aankondiging van een politiestrafbeschikking of een bestuurlijke strafbeschikking. Het is van belang dat er strikte afspraken zijn over bewaar-en vernietigingstermijnen voor de te onderscheiden handhavingstaken, en dat na ommekomst van de bewaartermijn, de BOA niet meer beschikt over het actieve archief. De toetsing aan de bewaartermijnen in de Wet justitiële en strafvorderlijke gegevens en aan de richtlijnen van het Openbaar Ministerie voor het bewaren en vernietigen van informatie bij politiestrafbeschikkingen en bestuurlijke strafbeschikkingen is van belang als ook dat gemaakte afspraken systematisch worden nageleefd.

De CPA wijst er op dat het van belang is om vooraf een proces vast te stellen voor verzoeken om gegevens uit het handhavingssysteem. Van belang is of deze verstrekkingen dienen voor het stellen van operationele doelen, en geen informatie op persoonsniveau is, of dat persoonsgegevens verstrekt worden. Dan is het van belang om te toetsen of er sprake is van verenigbaar gebruik, als ook of de gevraagde persoonsgegevens passend zijn voor het opgegeven doel. De CPA overweegt daarbij dat het gaat om strafrechtelijke persoonsgegevens zodat deze gevoelig van aard zijn en extra zorgvuldigheid is geboden. Van belang is dat een privacy coördinator adviseert over de verstrekking en daar voorwaarden aan stelt als ook dat de directeur van Handhaving & Toezicht of een functionaris op vergelijkbaar niveau beslist op het verzoek.

In dit verband merkt de CPA op dat het Informatie Gestuurd Handhaven graag apart plenair besproken wordt en niet binnen de scope van de advisering over het handhavingssysteem valt.

De CPA vraagt tot slot aandacht voor het feit dat een SAAS-leverancier wordt aangezocht, en dat aan deze leverancier strikte voorwaarden worden gesteld. Het is niet alleen van belang om deze eisen te stellen, maar ook dat er sprake is van een getekende bewerkersovereenkomst en dat er op wordt toegezien dat de afspraken door de gekozen leverancier worden nageleefd.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Hoogachtend,

5.1, 2, e

5.1, 2, e Mr. E.F. van Hasselt
Plv. Voorzitter Commissie Persoonsgegevens Amsterdam

**Commissie Persoonsgegevens Amsterdam**
**Uittreksel van het verslag van de openbare vergadering op donderdag 25 augustus 2016**

**10. Privacy Impact Assessment Mobiele Handhaving (Stadsdelen)**
De voorzitter geeft het woord aan de vice voorzitter en verschoont zich voor dit agendapunt. Het Privacy Impact Assessment Mobiele handhaving is ingediend. De secretaris is bij een vorig privacyreglement en de gebruikersovereenkomst betrokken geweest van het huidig systeem.

Handhaving & Toezicht licht toe dat het project primair de vervanging omvat van het huidige systeem met een nieuw systeem.
Sphynxx wordt niet langer ondersteund door de leverancier. Deze applicatie was aan de hand held device gekoppeld en deze werkt niet zonder deze software. Bestaande functionaliteiten worden nu door nieuwe functionaliteiten vervangen. Er wordt een standaard marktoplossing gezocht. Met het systeem wordt digitaal handhaven mogelijk gemaakt. Ook is er een faciliteit voor het leveren van bewijs in rechtszaken. Dat gaat nu ook digitaal. Komende weken wordt de definitieve gunning en opdracht bekend gemaakt. Dan volgt de tweede fase van het project.

De CPA vraagt naar de doorlooptijden.

Handhaving & Toezicht beoogt rond de jaarwisseling een werkende oplossing te hebben. Gekozen is voor smart phones. Er is daarom extra goed naar beveiligingsaspecten gekeken. Het apparaat wordt aan de Buitengewoon Opsporingsambtenaar gekoppeld en er vindt dubbele authenticatie plaats.

De CPA vraagt of er informatie op het device achterblijft. Ook wordt gevraagd of er foto's (kopie) van het identiteitsbewijs (ID) gemaakt worden en of er gebruik gemaakt wordt van een camerafunctie.

Handhaving & Toezicht antwoordt dat er geen gebruik gemaakt wordt van een camerafunctie. In de PIA staat dat af en toe een foto van het ID gemaakt wordt, inclusief pasfoto. Daar wordt nader naar gekeken. Uitgangspunt is dat er alleen gegevens van het ID worden overgenomen en geen foto gemaakt wordt. Daar komt voorlichting over als uitgelegd wordt hoe met de telefoon moet worden overgegaan.

De CPA wijst er op dat het uitgangspunt is dat er geen kopie van het ID gemaakt en opgeslagen mag worden. Gevraagd wordt naar de autorisaties van Juridische Zaken.

Handhaving & Toezicht zegt dat alleen het burgerservicenummer hoeft te worden gescand. Dit kan met een scanner. Juridische Zaken heeft toegang vanwege het behandelen van bezwaar- en beroepszaken.

De CPA vraagt of het doel is om niet alleen de gegevens te gebruiken voor signaleringen en dergelijke maar ook voor bewijsvoering in rechtszaken.

Handhaving & Toezicht zegt dat in de rechtszaal sprake is van volledig digitale dossiers. Bonnen worden nu digitaal vastgesteld. Wijze van vastleggen, opslag en doorzenden aan partners moeten nu voldoen aan de eisen van het Openbaar Ministerie en daar wordt nu aan getoetst. Ook maken de stukken dan onderdeel uit in de rechtszaal van het digitaal dossier.

De CPA zegt dat in de toelichting wordt verwezen naar verschillende situaties waarbij het systeem wordt toegepast. Het gaat om:
waarschuwingen, waarnemingen, aankondigingen van beschikkingen.

Handhaving & Toezicht zegt dat er een commissie is voor waarnemingen. De instructies uit deze commissie (boomstructuur van het proces) worden gebruikt en met deze functionaliteit wordt het proces mogelijk gemaakt. Wat er in komt te staan wordt nog nader bepaald.

De CPA stelt vast dat waarschuwingen ook worden opgeslagen.
In de PIA staat dat soms gegevens over ras worden vastgelegd. Op pagina 9. Is dit standaard?

Handhaving & Toezicht zegt dat het ging om de relatie met de foto van het ID. Als het systeem kan scannen dan wordt alleen nog het burgerservicenummer gescand en niet de foto.
Gegevens over nationaliteit zijn nodig om te weten waar het CJIB de beschikking naar moet sturen.

De heer 5.1, 2, e zegt dat het niet om het Nederlanderschap gaat maar om het ingezetenschap.

Handhaving & Toezicht zegt dat er een samenwerking komt tussen landen om informatie uit te wisselen. Dit loopt via het CJIB.

De CPA vraagt naar de schets van het systeem, wie beheert het, waar staat de server.

Handhaving & Toezicht zegt dat de systemen in het rekencentrum van de leverancier staan die faciliteert de mobiele devices van de Buitengewoon Opsporingsambtenaar op straat. Het back office systeem logt in via een veilige verbinding. Er zijn eisen aan de leverancier gesteld. Die moet voldoen aan Europese wetgeving, de server moet in NL staan en een bewerkersovereenkomst wordt afgesloten. Er volgt een pentest voor ingebruikname en daarna wordt dit jaarlijks herhaald. De leverancier moet gecertificeerd zijn. Dit is opgenomen in het Programma van eisen.

De CPA vraagt naar de extracten die OOV ontvangt. Is dit voor beleidsdoeleinden. Wie geeft hier akkoord voor?
Is er een relatie bijvoorbeeld met de TOP 600 aanpak. Gaat het dan op individueel niveau?

Handhaving & Toezicht zegt dat het in principe gaat om operationele informatie. Waar is inzet nodig.

De CPA vraagt of beoordeeld wordt per verzoek of de levering wordt verstrekt. Informatie Gestuurd Handhaven (IGH) valt niet in de scope van de gepresenteerde PIA. Is daar een relatie mee?

Handhaving & Toezicht zegt dat BOA's toegang hebben tot Informatie gestuurd handhaven op operationeel niveau. Als het om beleid gaat dan kan OOV informatie opvragen.

De CPA vraagt of een privacy coördinator of de directeur van Handhaving & Toezicht deze verzoeken toetst.

Handhaving & Toezicht zegt dat daarover moet worden nagedacht en eventueel voor advies voorgelegd aan de CPA.
Voor IGH wordt veel informatie gevraagd. Het gaat om rapportagedoeleinden en gaat om geanonimiseerde data. Maar er zal meer kunnen worden gevraagd. Er zal moeten worden nagedacht over leveringen van gegevens ten behoeve van IGH of aan OIS voor onderzoeksdoeleinden.

De CPA zegt dat een dergelijke beslissing niet bij een BOA of de bonnenadministratie hoort.

Handhaving & Toezicht zegt dat iemand daartoe geautoriseerd moet zijn.

De CPA vraagt wat er met vernietigingstermijnen wordt gedaan. Hoe lang kan een waarschuwing bijvoorbeeld zichtbaar blijven.

Handhaving & Toezicht bewaart de gegevens voor bezwaar- en beroepszaken. Er wordt advies gevraagd aan Informatiebeheer over dit onderwerp. De Archiefwet en Wet bescherming persoonsgegevens hebben daarvoor een verschillende regeling. De eisen van het Openbaar Ministerie zijn ruim.

De CPA verneemt graag over het actieve en het passieve archief. Een BOA kan niet bij het passief archief.
De CPA stelt vast dat mobiel devices handig zijn maar er zijn privacy technische aspecten die nog beter bekeken moeten worden.

De CPA vraagt of andere toepassingen door de BOA op de device kunnen worden gebruikt.

Handhaving & Toezicht heeft gevraagd dat alleen apps gebruikt kunnen worden die de gemeente toestaat. De apparaten moeten clean blijven. Er komt een aparte container voor de gegevens en daar mag niets mee gecombineerd worden.

De CPA vraag of er een gps op de device zit. In de PIA staat dat niet bekend is of het een personeelsvolgsysteem is of niet.

Handhaving & Toezicht zegt dat het ook omwille van de veiligheid goed kan zijn waar de BOA is. Er wordt steeds meer gehandhaafd op thema's. BOA's moeten geïnstrueerd worden wat hij moet doen.

De CPA zegt dat het een element is dat hoort bij het werk.
In het verleden is de portofoon aangemerkt als personeelsvolgsysteem en heeft de OR naar de voorwaarden gekeken. Daarmee kon ook de spreiding in de stad worden bekeken en werd dit getoond op een scherm. Gesteld wordt dat de Burgemeester belast is met de handhaving van de openbare orde en veiligheid en de gemeente biedt het middel aan. De BOA heeft een eigen opsporingsbevoegdheid en is ook verantwoordelijk voor de invoering van de gegevens in de zin van de Wbp. Er zijn dus meerdere verantwoordelijken.

De CPA vraagt naar pagina 19 van de PIA 'voor zover mogelijk' wordt door medewerkers gebruik gemaakt van encryptie bij mailen. Deze beslissing moet niet bij medewerkers liggen. Het hoort veilig te zijn.

Handhaving & Toezicht zegt dat het om Outlook gaat waarbij een bewuste keuze gemaakt moet worden.

De CPA zegt dat de BOA dan zelf moet bepalen wat gevoelige informatie is. Dat hoort dan bij zijn rol als de verantwoordelijke in de zin van de Wbp.

De CPA zegt dat bewustwording een belangrijk onderwerp is. De PIA is nog vrij algemeen op bepaalde punten. Dan staat er bij dat de punten nog moeten worden uitgewerkt of aangepast. De persoonsgegevens uit het systeem worden gebruikt als training. Is dat nodig?

Handhaving & Toezicht zegt dat het dan om geanonimiseerde gegevens gaat. Dat moet met de leverancier worden afgesproken.

Handhaving & Toezicht heeft een termijn gesteld aan de leverancier waarin deze aangeeft op welke wijze zij voldoen aan de gestelde eisen op het gebied van informatiebeveiliging en privacy.

De CPA vraagt naar het privacyreglement. In de toelichting staat dat de leverancier onderhoud verricht aan de software. De leverancier doet nu ook de hosting. Dit moet worden aangepast. De inhoud moet aansluiten op de andere stukken.
Handhaving & Toezicht zegt dat de wettelijke grondslag worden vastgelegd en de onderlinge verhoudingen.

<u>Actiepunten</u>
Er volgt een brief met de aandachtpunten van de CPA.