Cruquiusweg 5
Postbus 94652
1090 GR Amsterdam
Telefoon 5.1, 2, e
Fax 5.1, 2, e
www.amsterdam.nl

Gemeente Amsterdam

Commissie Persoonsgegevens

Retouradres: Postbus 94652, 1090 GR Amsterdam

Servicehuispersoneel/DICT
Tav de heer 5.15.1, 2, e en de heer 5.15.1, 2, e
Postbus 94652
1090 GR Amsterdam

Datum	13 mei 2014
Ons kenmerk	U140074
Behandeld door	Mw. 5.1, 25.1, 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 heren 5.1, 2, e en 5.1, 2, e ,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 17 april jl. was u aanwezig namens het Servicehuis Personeel.
Het onderwerp Identitymanagement was geagendeerd.

U meent dat het gebruik van het versleutelde BSN van externen zowel als van medewerkers in dienst noodzakelijk is om het zogenaamde proces van het 'ontdubbelen van identiteiten' te kunnen uitvoeren voor het toekennen van autorisaties. Het verwerken van naam en geboortedatum brengt volgens u ook een grote mate van zorgvuldigheid betreffende dit proces met zich, echter u kunt deze risico's (nog) niet overzien.
U bent voornemens om in het project te borgen dat alleen een versleuteld BSN in de Identitymanagent-module gebruikt wordt zodat er geen sprake is van het schenden van de privacy van betrokkenen.
Tot slot is aangevoerd dat er een kernregistratie externe medewerkers zal komen bij SHP.

Over het verwerken van het BSN voor doeleinden van Identitymanagement zijn duidelijke mededelingen gedaan door het CBP. Ik verwijs naar het rapport van definitieve bevindingen van mei 2010 van het CBP 'Onderzoek naar de verwerking van het burgerservicenummer en kopie identiteitsbewijs voor de Rijkspas door de minister van Verkeer en Waterstaat' (z2010-000050).

De CPA is naar analogie van dit rapport van mening dat het verwerken van het BSN voor Idm-doeleinden in strijd is met artikel 10 Wabb en geen wettelijke grondslag kent in de zin van artikel 8 Wbp. Het staat immers niet ten dienste van de publieke taak van de gemeente Amsterdam, maar dient ten behoeve van de bedrijfsvoering.

De CPA constateert op basis van door u na afloop van de vergadering ingediende informatie, dat het CBP een mededeling heeft gedaan dat het opvragen van het BSN van ingehuurde krachten in hoedanigheid van inlener of aannemer geoorloofd is in het kader van de matiging van keten- en inlenersaansprakelijkheid. Voor medewerkers in dienst van de gemeente Amsterdam geldt dat het BSN in de loonadministratie aanwezig mag zijn op grond van de Wet op de loonbelasting.

De CPA blijft van mening dat het verwerken van het BSN ten behoeve van het beoogde doel geen wettelijke grondslag kent. Dat op grond van de Wet op de loonbelasting het BSN van medewerkers in de loonadministratie binnen SHP wordt vastgelegd en dat er mogelijk op korte termijn een centrale registratie van externen komt, doet hier niet aan af.

De CPA brengt een zekere nuancering aan in dit standpunt -hoewel het standpunt over de afwezigheid van een verwerkingsgrondslag onverkort gehandhaafd blijft- onder de volgende strikte voorwaarden:
1. een kernregistratie van externen is centraal beheerd net als van interne medewerkers;
2. het proces van het matigen van de wettelijke ketenaansprakelijkheid voor ingehuurde krachten is structureel belegd;
3. met het oog op uitsluitend dit doel wordt het BSN van ingehuurde krachten opgevraagd;
4. en vervolgens wordt vóór ontvangst in de Identitymanagement-module het BSN uit de bronadministraties ten behoeve van het 'ontdubbelen' encrypt.

In het geval aan al deze voorwaarden wordt voldaan is van het gebruik van het versleutelde BSN geen extra privacyrisico te verwachten.

Bijgaand treft u een zakelijke samenvatting aan van hetgeen op de vergadering is besproken (concept-versie).Het definitief verslag zal op de vergadering van 22 mei a.s. worden vastgesteld.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Met vriendelijke groet,

5.1, 2, e

.1, 2, e (ambtelijk secretaris)

Commissie Persoonsgegevens Amsterdam
Uittreksel van het verslag van de openbare vergadering op donderdag 17 april 2014

Openbaar deel.

9 Identitymanagement (SHP/DICT)

Er is geen nadrukkelijke scheidslijn gemaakt tussen de identificatieslag en de autorisaties. De CPA hamert er sterk op dat de rol die iemand vervult samenhangt met toegekende bevoegdheden. Het zgn. "role-based acces".
De autorisaties worden toegekend aan de rol die iemand heeft. In het voorstel lijkt de bevoegdheid aan de identiteit van de medewerker te zijn gerelateerd.
Het voorstel lijkt in dit opzicht zwak. Personen worden in de salarisadministratie geregistreerd. Deze personen worden gekoppeld aan een Amsterdsams-id zodat het gebruik van het BSN verder niet nodig is om deze personen te identificeren. Personen die niet in loondienst zijn van de gemeente, maar wel een rol hebben in de gemeente (bijvoorbeeld de leden van de CPA) moeten ook worden geregistreerd. Dat gebeurt niet met het BSN maar met een Amsterdamse identiteit die wordt toegekend.

De heer 5.1, 2, e zegt dat in de startarchitectuur een hoofdstuk is opgenomen over de principes die gehanteerd worden voor de Kernregistraties van medewerkers en het Identitymanagement. Een van die principes is het "role-based acces".
De ambitie is er wel degelijk om role based acces te implementeren. De praktische implementatie van role based acces is dat er een model van binnen de gemeente bestaande rollen moet zijn, op basis waarvan een rechtenstructuur kan worden geïmplementeerd. Vanuit SHP is echter alleen het organisatieonderdeel bekend. Deels kunnen toegangsrechten op dit gegeven worden gebaseerd (bijvoorbeeld toegang tot een gedeelde schijf of DMS). Tot dat er een goed model is gedefinieerd is het niet mogelijk role based acces volledig te implementeren. Voor zover mogelijk worden generieke rechtenstructuren nu gedefinieerd. Veel applicaties hebben echter hun eigen structuur. Het voorstel houdt daarom in dat voor een groot deel de functioneel beheerder rechten kan toekennen aan medewerkers in de juiste rol voor de applicaties die in beheer zijn. In het voorstel is dan ook sprake van op een lager, gedelegeerd niveau, role based acces.

De CPA zegt dat dit enigszins geruststelt.

De heer 5.1, 2, e zegt dat accesmanagement moet worden onderscheiden van identitymanagement. Identitymanagement heeft ten doel om rollen te kunnen toekennen.

De CPA zegt dat het op zich vreemd is dat in het voorstel het beheer van toegangsrechten op dezelfde plaats is ingedeeld als het identitymanagement (waaronder versleuteld BSN), terwijl er logischerwijs duidelijke scheiding tussen deze taken moet zijn. De vraag die aan de CPA is gesteld is: hoe moet met het BSN worden omgegaan. Voor de toegang is het BSN niet nodig. Dus dit hoeft niet in het Idm aanwezig te zijn. Een Amsterdams-id is voldoende. De vraag is waar het Amsterdams-id wordt gegenereerd. In de personeelsadministratie moet het Amsterdams-id bekend zijn en voldoende zijn voor het Identitymanagement. De vraag is of externen met het BSN herkend moeten worden.

De heer 5.1, 2, e zegt dat het afhangt of de representatiekosten belast worden op grond van de Wet op de loonbelasting.

De heer 5.1, 2, e zegt dat het niet gaat om het registreren van het BSN maar om het genereren van een unieke identiteit in de registratie van personen ten behoeve van het Idm. Daarvoor is een uniek identificatienummer vereist. Het maakt niet uit welk nummer het is. Het BSN is echter het meest geschikt als sleutel. Het wordt verder niet gebruikt.

De heer 5.1, 2, e zegt dat van personeel in dienst een BSN aanwezig is in de loonadministratie. Of dat gebruikt mag worden voor Idm- doeleinden is een tweede aspect. Het BSN van de externen is niet in het bezit van de gemeente, althans niet in de meeste gevallen. De grote consultancy bureaus sturen een factuur waarop het BSN van de ingehuurde kracht niet vermeld staat.

De heer 5.1, 2, e zegt dat het BSN niet vastgelegd wordt in de Idm-registratie. Het versleuteld BSN wordt gebruikt. De bedoeling is om dubbelingen in de bronadministraties te voorkomen.

De heer 5.1, 2, e zegt dat dit voor externen niet werkt omdat het BSN niet in het bezit is van de gemeente. Het kan dan ook niet versleuteld worden.
Alleen als een wettelijk voorschrift bepaalt dat de gemeente van externen het BSN moet gebruiken, mag het worden opgevraagd.

De heer 5.1, 2, e zegt dat het CBP heeft geadviseerd dat de gemeente van ingehuurde krachten het BSN mag uitvragen. Om deze reden is het voorstel om het encrypt BSN voor Idm-doeleinden te gebruiken.

De CPA vraagt naar het advies van het CBP. De vraag is of de externe ook verplicht is om het BSN te verstrekken.

De CPA vraagt waarom de ontdubbeling in de Idm plaatsvindt en niet in een ander systeem van SHP.

De heer 5.1, 2, e zegt dat SHP op dit moment nog niet in staat is om een volledige medewerkers-administratie te leveren. In het systeem staan interne medewerkers. De ambitie is er wel om externe medewerkers te registreren, maar dat is op dit moment nog niet mogelijk. Daarom wordt een tijdelijke externen administratie ingericht. De informatie komt dan uit twee bronnen, waardoor de ontdubbeling in de Idm noodzakelijk is. Het kan zijn dat in een latere fase ook andere bronnen worden aangesloten. Voor de toegangsrechten tot gebouwen moet ook een koppeling gemaakt worden.

De heer 5.1, 2, e zegt dat SHP zowel eigenaar is van de personeelsadministratie als het Idm.

De CPA zegt dat het proces van ontdubbelen niet in de personeelsadministratie plaatsvindt. Als dat zo zou zijn, dan zou aan dit vraagstuk over BSN gebruik in de Idm niet worden toegekomen.

De heer 5.1, 2, e zegt dat er een centrale registratie van externen komt.

De CPA vraagt of de geboortedatum en naam niet voldoende is voor het ontdubbelen.

De heer 5.1, 2, e zegt dat dit voor 99% dekkend zal zijn, maar niet sluitend. Het gaat wel om toegang tot systemen en gebouwen. Dat is een securityrisico.

De CPA vraagt of dat risico wel zo groot is.

De heer 5.1, 2, e zegt dat het om een mogelijkheid van vervuiling in het systeem gaat, waarvan niet zeker is wat de effecten zijn.

De heer 5.1, 2, e zegt dat het 'singel sign on' een zwaarder belang betekent voor een juiste toekenning van rechten. Met versleuteld BSN wordt 100% garantie mogelijk.
De heer 5.1, 2, e zegt dat encryptie voor het versturen naar Idm plaatsvindt.
Nieuwe registraties kunnen wel getoetst worden aan versleutelde BSN's.

De heer 5.1, 2, e zegt dat het BSN in één richting versleuteld wordt.

De CPA zegt uit de mededeling van het CBP zou moeten volgen dat het BSN van externen voor deze doeleinden gebruikt mag worden en of de gemeente een externe hiertoe kan verplichten. Het BSN moet legaal zijn verkregen. De CPA neemt graag kennis van deze mededeling. Een alternatief lijkt echter aangewezen.

DBI zegt dat deze kwestie vergelijkbaar is met een uitspraak van de rechter over toegangspasjes bij het Ministerie BZK en het gebruik van het BSN.

De heer 5.1, 2, e bevestigt dat wordt voorgesteld om encryptie toe te passen, maar dat dit niet wegneemt dat het BSN wel wordt verwerkt. Ook als het BSN van externen kan worden opgevraagd is nog de vraag of het verwerkt mag worden voor Idm-doeleinden.

De CPA zegt dat de vraag is of een encrypt BSN nog een persoonsgegeven is.

De heer 5.1, 2, e zegt dat de privacyrisico's dan beperkt zijn. Juridisch gezien zou er echter ook dan nog een formele belemmering kunnen zijn.

De CPA zegt tot een definitief advies te kunnen komen na kennis te hebben genomen van de mededeling van het CBP.
De CPA zegt tot slot dat ook de autorisatiesystematiek en het bespoedigen van de invoer van role based acces voorwaarden zijn voor een positief advies. Ook is van belang dat een Kernregistratie van medewerkers tot stand komt. De vraag is of alle gegevens van de medewerker die in het voorstel genoemd staan (achternaam, familienaam ea)

noodzakelijk zijn voor Idm. Opgemerkt wordt tot slot dat in de risico-analyse onvoldoende aandacht wordt besteed aan beveiliging van het systeem. Ook bij 'integriteit' komt de beveiliging van identiteitsfraude niet terug. Het risico wordt laag geschat.

De heer 5.1, 2, e zegt dat eerst wordt gestart met Idm en dat de kernregistratie de volgende stap is.

De heer 5.1, 2, e zegt dat de (verkorte) risico-inventarisatie verricht is om de eisen te bepalen op grond waarvan maatregelen worden vastgesteld. In de ontwerpfase wordt dit geïmplementeerd.

De heer 5.1, 2, e zegt dat Idm een gesloten systeem is dat dient ter beveiliging van de identiteit en toegangsrechten. De controle van de identiteit ligt in het bronsysteem. Er zijn geen gebruikers van het Idm-systeem. Vanuit privacy-oogpunt hebben in Idm opgeslagen gegevens weinig waarde. Het acces-systeem verleent autorisaties op basis van toegangsregels. Daarin zou dan ingebroken moeten worden.

De CPA zegt dat ook een gesloten systeem een beveiligingsrisico kent. Inbreuk kan leiden tot identiteitsfraude en/of het ongeoorloofd gebruik van overheidsmiddelen. Dit moet worden betrokken in de analyse. Het is een belangrijke module voor de gemeente Amsterdam. De rating is aan de lage kant. De beveiliging van een centraal systeem zou een belangrijk aspect moeten zijn. Het lifecycle-management zit in de Idm. Ook de samenhang met de bronsystemen is onderbelicht in de analyse. De rating is van belang voor de vraag of een PIA verricht moet worden. Als gesignaleerde risico's goed worden ondervangen is geen separaat PIA noodzakelijk.