Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam
Commissie Persoonsgegevens

PER E-mail
Tav
Directeur OIS, de heer B. Daan
Kopie: de heer 5.1, 2, e , controller D&I en de heer 5.1, 2, e , Privacy- en Informatiebeveiliger D&I, de heer 5.15.1, 2, e , manager IVE D&I
Kopie: de heer 5.1, 2, e , Stedelijk directeur Dienstverlening & informatie
CIO, de heer J. Flippo

Datum	23 augustus 2016
Ons kenmerk	U160091
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 Daan,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 28 juni 2016 was u aanwezig namens de gemeente Amsterdam. Bij het agendapunt "Datalab en Datapunt" heeft de CPA het navolgende besproken.

De CPA onderschrijft het belang van een technische infrastructuur om informatie te ontsluiten die bij de verschillende onderdelen van de gemeente beschikbaar zijn. Datapunt bestaat uit een systeem van verbindingen om dat mogelijk te maken (platform). Het Datalab zal in feite de rol van gegevensmakelaar vervullen.

De CPA overweegt dat er een groot maatschappelijk belang gemoeid is met het juist en nauwkeurig houden van informatie die bij de gemeente berust en ook dat er een zwaarwegend belang bij is dat deze informatie beschikbaar is voor die publieke taak waarvoor deze is verzameld. Ook kunnen 'derden' belang bij gemeentelijke informatie hebben. Het systematisch actueel houden van informatie, het centraal beheren van autorisaties en classificatie van informatiebronnen heeft dan ook een grote meerwaarde in de informatievoorziening van de stad.

De CPA onderscheidt bij het stedelijk gegevensbeheer verschillende rollen en hecht aan het onderscheid hiertussen: de aanbieder van gegevens, de gegevensmakelaar en de afnemer van gegevens. De vraag die voorligt is welke spelregels op deze rollen van toepassing zijn, wie de betreffende rol (taak, verantwoordelijkheden en bevoegdheden) vervult en of die rol exclusief is.

Bij het leveren van persoonsgegevens is het zaak deze rollen helder te beschrijven en dat met aanbieders en leveranciers (dit kunnen in- of externe partijen zijn) eenduidige afspraken gemaakt zijn over de levering van persoonsgegevens. Dit gaat zowel over de toelaatbaarheid van de gegevensuitwisseling als over de kwaliteit van de levering. Toetsing aan de wettelijke kaders (Wet bescherming persoonsgegevens en in 2018: de Europese Algemene verordening gegevensbescherming) en met name de doelbinding dient permanent plaats te vinden. Open data moeten als regel geanonimiseerd worden aangeboden. Ook is het belangrijk dat de gemeente Amsterdam een standpunt in neemt over het gebruik van Big Data en het leveren van gegevens voor ongerichte statistische analyse.

De CPA wordt dan ook graag nader geïnformeerd over de wijze waarop het Datapunt wordt ingericht en op welke wijze de ontsluiting van aangesloten bronnen door het Datalab gaat plaatsvinden, waarbij deze vragen opvolging krijgen.
Ook adviseert de CPA graag in een vroeg stadium over de zogenoemde "Datakluis".

Onderstaand treft u een samenvatting aan van hetgeen over het agendapunt in de vergadering 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 dinsdag 28 juni 2016 januari 2016

5. Datalab en Datapunt (Dienstverlening & Informatie)
De heer Daan, directeur OIS, verwelkomt de gelegenheid om met de CPA kennis te maken rond het onderwerp van bescherming van persoonsgegevens bij het vergaren en verwerken van data en informatie. Hij merkt op dat OIS veel samenwerkt met BI. Hij wil de commissie laten zien hoe OIS tegen databeheer bij de gemeente aankijkt en in het bijzonder tegen de omgang met persoonsgegevens. OIS vervult enerzijds een dienstverlenende functie waarbij gezorgd wordt dat de informatie betrouwbaar is en systematische garanties zijn ingebouwd dat medewerkers weten hoe ze om moeten gaan met vertrouwelijke gegevens. Daarnaast wil OIS een rol spelen bij het ontsluiten van data die bij de verschillende onderdelen van de gemeente beschikbaar zijn. Datapunt bestaat uit een systeem van verbindingen om dat mogelijk te maken. Op decentraal niveau zijn bij de gemeente in een grote variëteit van soorten bestanden veel data aanwezig die vaak verzameld zijn voor een specifiek doel. Waar het om gaat is te zorgen dat die informatie accuraat en betrouwbaar op een centraal niveau geaggregeerd kan worden. Dat vergt systematisch vastleggen hoe informatie actueel gehouden kan worden en op een geborgde, veilige manier kan worden doorgegeven naar een centraal niveau ten behoeve van analyses. Dat vraagt technische voorzieningen om informatie op te slaan, maar ook op centraal niveau vastgelegde procedures die mensen in staat stellen om die vertaalslag te maken.
Het gaat om een grote diversiteit aan databronnen binnen de verschillende domeinen. Die zijn niet zonder meer met elkaar te verbinden of re-ordenen en dat is ook niet wenselijk. Maar op centraal niveau of in de buitenwereld heeft men wel te maken met vragen en problemen die geholpen zijn met analyses van al die gegevens. OIS wil niet blijven werken met het ad hoc ophalen van informatie via maatwerkoplossingen. Datapunt is een systeem van verbindingen met de bronbestanden met daaraan gekoppeld een aantal functionaliteiten zoals catalogi en een centrale loggingfunctie die bijhoudt wat er allemaal wordt opgevraagd. Er zit ook een authenticatie- en identificatiemodule aan gekoppeld zodat alleen personen bij de informatie kunnen komen die daartoe gerechtigd zijn. Via de geheel herziene en opgewaardeerde interface ATLAS – die vroeger alleen voor de basisregistratie werkte - kan men aan de voorkant de gegevens bekijken. De controle op toegangsrechten vindt aan de achterkant plaats.
Zo ontstaat er een generiek systeem om steeds meer databronnen te ontsluiten. Per gebruikersgroep zijn modellen ontwikkeld met toegangsrechten. Aan elke databron wordt een risicocategorie toegekend. Bij combinaties van bronbestanden wordt het risiconiveau navenant verhoogd. Er wordt een zelflerend systeem ontwikkeld om verdachte opzoekpatronen en combinaties te signaleren. Dat is allemaal nog in ontwikkeling. Per vraag wordt nu bekeken welke onderdelen van datapunt nodig zijn om daarvoor een oplossing te realiseren.
Er zijn nu twee toepassingen waarbij men te maken krijgt met persoonsgegevens. Een ten behoeve van de brandweer die dan bij brandmeldingen meteen een overzicht krijgt van relevante gegevens die van het betreffende adres bekend zijn bij de gemeente. Dat systeem is al bij de CPA langs geweest, maar is nog niet in de lucht. Die informatie wordt alleen doorgegeven en niet opgeslagen. Een andere toepassing is Integraal Klantbeeld waarmee

Amsterdammers in de toekomst via Mijn Amsterdam inzage kunnen krijgen in hun eigen gegevens bij de gemeente. Dat vraagt natuurlijk wel een goed beschermde routering.

De CPA vraagt wie de regie gaat voeren over datapunt en hoe men brongegevens afgeschermd houdt.

De heer Daan zegt dat er bij OIS nagedacht wordt over het inrichten van een soort kluis die uitsluitend vanaf een beperkt aantal plekken toegankelijk is, waar informatie wordt opgeslagen en die niet naar buiten kan totdat die getoetst is op de aanwezigheid van privacygevoelige gegevens. Zodra daar een ontwerp voor is, wil men dat aan de CPA voorleggen. De toegang tot brongegevens heeft te maken met de autorisatie en identificatie. Als combinaties van bestanden tot verhoogde risico's zouden leiden moet systematisch voorkomen worden dat men zulke gecombineerde gegevens kan downloaden. Dat is echter niet generiek te doen en moet per bronbestand bepaald worden. Datapunt wil wel op centraal niveau kennis beschikbaar maken over het pseudo- en anonimiseren van bestanden, ook in technische zin, om directeuren in staat te stellen goede afwegingen te maken en niet afhankelijk te zijn van een individuele jurist of deskundige. De mooiste oplossing zou een organisatorische voorziening zijn die het gebruik van meervoudige systemen toetst, maar daar is men nog niet aan toe. Nu moet men per analysevraag onderzoeken wat legitiem is. Het hangt ook af van het gebruik dat men gaat maken van de gegevens. Aggregaties zijn op zich in orde, maar als men daar weer selecties in bestanden mee gaat maken kunnen zaken gevoeliger worden. Als men informatie voor individueel gebruik wil, is juist weer meer snelheid gewenst. Dus het valt niet eenduidig te bepalen wat wel en niet gedownload mag worden. In de datakluis kan men bijvoorbeeld wel correlaties maken, maar dan mogen alleen de uitkomsten eruit gehaald worden.

De CPA vraagt hoe het politiek bestuur staat tegenover datapunt.

De heer Daan zegt dat het behoort tot de portefeuille van de burgemeester, maar dat het iedere portefeuille raakt en dat het dus belangrijk is alle wethouders inzicht te geven in het belang van goede regelingen op dit terrein. Hij merkt daarbij op dat het vertrouwen van de burger in de overheid minder te maken heeft met de optimale bescherming van privacy als wel met de wetenschap dat die overheid beschikt over de juiste gegevens. Daarom is het Integraal Klantbeeld belangrijk, omdat de burger daarmee kan zien welke kennis de gemeente over hem in huis heeft.

De CPA vraagt hoe Datapunt omgaat met anonimiseren.

De heer Daan zegt dat het anonimiseren plaatsvindt voordat gegevens naar de kluis gaan of de kluis verlaten. De bescherming van privacy zit volgens hem in de genen van OIS en alle medewerkers. Datapunt wil dat technisch nog beter faciliteren.

De CPA is benieuwd of de gebruikersgroep door datapunt ook toeneemt.

De heer Daan bevestigt dat. Voor onderzoekers zal het gemakkelijker worden om alle mogelijke gegevens in de kluis te koppelen, waar ze nu nog naar afzonderlijke instellingen moeten. Dat betekent overigens ook dat de controle en het overzicht op het gebruik van gegevens groter wordt.

De CPA vraagt hoe de autorisatie werkt.

De heer Daan zegt dat net als nu de toegang tot privacygevoelige gegevens een zaak is van zorgvuldig beheer. De generieke toegang wordt geregeld op basis van groepen. Hij heeft zelf de indruk dat het belangrijker is mensen tijdens het werkproces signalen te sturen als ze privacygevoelige informatie aan het opvragen zijn die ze dus niet naar buiten mogen brengen of mogen combineren met andere informatie. Daarbij wordt dan ook vermeld dat alles gelogd wordt. Dat helpt volgens hem beter dan het instellen van een grote reeks beveiligingsniveaus met alle kwetsbaarheden van dien. Het doet ook een beroep op het verantwoordelijkheidsgevoel van medewerkers. De bronbestanden zelf krijgen een label met een beveiligingsniveau. De catalogus met een overzicht van alle bestanden en meta-informatie is wel breed beschikbaar, zodat iedereen wel kan zien welke databestanden erin zijn opgenomen. Dat is een belangrijk verschil met de huidige situatie.

De CPA vraagt of datapunt ook kan faciliteren bij externe onderzoekers die gemeenten vragen om BRP-gegevens of die reminders bij non-respons willen sturen. De CPA krijgt nu vaak vragen over specifieke enquêtes maar zou liever komen tot een model met spelregels in overleg met OIS.

De heer Daan denkt dat het wel goed zou zijn om daar centraal een overzicht van te hebben, maar dat hij niet meteen alles wil faciliteren. In technische zin is er op zich veel mogelijk.

De CPA is benieuwd of de gebruikers veel extra scholing nodig hebben.

De heer Daan zegt dat dit steeds minder het geval zal zijn, omdat het systeem mensen actief informeert op het moment dat ze die informatie nodig hebben. Dat wordt in de interfaces ingebouwd. Bij alles wat men bedenkt op dit gebied, blijft de mens immers de zwakke schakel.

De <u>voorzitter</u> bedankt de medewerkers van OIS voor deze toelichting op de ontwikkeling van Datapunt.

<u>Actiepunten</u>
OIS zal de CPA consulteren als een ontwerp voor de datakluis gereed is. De CPA overweegt OIS uit te nodigen om mee te denken over spelregels rond de toegang tot BRP-gegevens voor externe onderzoekers. De CPA overweegt OIS uit te nodigen voor een presentatie van Datalab en Datapunt bij de privacymiddag in januari.