Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam
Commissie Persoonsgegevens

Aan: de directeur Onderzoek, Informatie & Statistiek, de heer B. Daan
Aan: manager IVE Dienstverlening & Informatie, de heer 5.1, 2, e
C.c. Stedelijk Directeur Dienstverlening & Informatie, de heer M. Crooijmans
C.c. CIO, de heer J. Flippo
C.c. Programmamanager Datapunt, de heer , Privacy Officer Datapunt, de heer 5.1, 2, e , Privacy Officer Sociaal & Datapunt, de heer 5.1, 2, e , Privacy Officer Dienstverlening & Informatie, de heer 5.1, 2, e , Informatiebeveiligingcoördinator Dienstverlening& Informatie, de heer 5.1, 2, e

Datum	21-02-2018
Ons kenmerk	
Behandeld door	Mw. 5.1, 2, e
Doorkiesnummer	
Faxnummer	nvt
E-mail	5.1, 2, e amsterdam.nl
Bijlage	1
Onderwerp	Datapunt

Geachte heer Daan, de heer Schans,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 25 januari 2018 waren namens de gemeente Amsterdam aanwezig: de heer 5.1, 2, e (Programmamanager Datapunt), de heer 5.1, 2, e (Privacy Officer Datapunt) en de heer (Privacy Officer Sociaal)

Bij het agendapunt "Datapunt" is het volgende besproken.

U heeft de CPA geïnformeerd over privacyaspecten bij het functioneren als Amsterdams schakelpunt tussen aanbieders en aanvragers van data uit de hele gemeentelijke organisatie.

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 de uitvoering van die publieke taak. Ook kunnen 'derden' belang bij gemeentelijke informatie hebben. Het systematisch actueel houden van informatie, het centraal beheren van autorisaties en classificatie van informatiebronnen hebben dan ook een grote meerwaarde in de informatievoorziening van de stad.

Voorafgaand
De CPA heeft reeds eerder in haar vergadering d.d. 6 juli 2017 gesproken over de inrichting, werkwijze en bevoegdheid van het programma Datapunt binnen de RVE Onderzoek, Informatie en Statistiek (OIS). Dit in navolging van een eerste samenspraak met de CPA op 28 juni 2016 over de vormgeving van het programma Datapunt. In beide vergaderingen kwamen de volgende herhaalde aandachtspunten van de CPA naar voren die uit de adviezen van 23 augustus 2016 en 25 juli 2017 volgen:

- Een duidelijke rol van OIS/ Datapunt inzake de verantwoordelijkheid van OIS/ Datapunt bij de verwerking van persoonsgegevens ten opzichte van de andere gemeentelijke organisatie- onderdelen.
- Een visie van OIS/ Datapunt op de eigen rol bij de bewaking van de rechtmatigheid, kwaliteit en kwantiteit van de gegevensverwerking.
- De inrichting van toetsingsmomenten bij een verwerking door OIS/ Datapunt. De CPA ziet tenminste drie toetsingsmomenten, namelijk: bij de input van persoonsgegevens, het moment van gegevensanalyse en bij de output.

De CPA heeft naast deze herhaalde aandachtspunten in de vergadering d.d. 25 juli 2017 nog drie andere punten van aandacht genoemd, namelijk:

- Het beschikbaar stellen van statistische informatie en open data via bijvoorbeeld City Data kan 'gevoelige' resultaten opleveren, terwijl de data op zich niet te herleiden hoeven te zijn tot personen. Met betrekking tot dit vraagstuk adviseert de CPA OIS/ Datapunt een 'ethische commissie' in te stellen die wordt geraadpleegd alvorens deze data worden gepubliceerd op bijvoorbeeld City Data.
- De inrichting van een goede informatievoorziening voor de burger over wat er met zijn/ haar gegevens gebeurt en de mogelijkheid van de burger om zijn/ haar rechten uit te oefenen.
- De mate van informatiebeveiliging in de samenwerking van OIS/ Datapunt met Cloud VPS, de getroffen maatregelen in samenhang met dataclassificatie en de wederzijdse rechten en plichten terzake in de bewerkersovereenkomst welke de gemeente met Cloud VPS heeft afgesloten.

Reactie Datapunt
Op de vergadering van 25 januari jl. heeft Datapunt documenten aangeleverd met betrekking tot de bovenstaande aandachtspunten.

Met betrekking tot een duidelijke rol van OIS/ Datapunt is er in de ontwikkeling van het werkproces naar voren gekomen dat OIS/ Datapunt drie rollen kan onderscheiden bij een gegevensdienst waarin persoonsgegevens worden verwerkt:

I. Afnemer: verantwoordelijk voor het onderbouwen van de rechtmatigheid van de gewenste gegevensdienst en voor de inrichting van werkprocessen en beveiligingsmaatregelen in de eigen organisatie, overeenkomstig wet- en regelgeving.
II. Bronhouder/verstrekker: heeft de verantwoordelijkheid om te toetsen of het gevraagde gebruik door de afnemer overeenstemt met de wettelijke kaders en om erop toe zien dat in de gegevensdienst passende maatregelen worden genomen ten aanzien van informatiebeveiliging.
III. Eigen verantwoordelijkheid, 'zijnde verwerker': gezien de binnengemeentelijke positie van OIS/ Datapunt kan zij formeel geen verwerker zijn. OIS/ Datapunt valt onder het College en/of de Bm als 'verwerkingsverantwoordelijke'. OIS/ Datapunt heeft wel een 'eigen' verantwoordelijkheid aangaande het inrichten en uitvoeren van de gegevensverwerking binnen haar organisatie, vandaar: 'zijnde verwerker'.

Eigen rol
OIS/ Datapunt faciliteert de uitvoering van het dataproces door het aanreiken van templates en het doen van voorstellen over de inrichting van de gegevensdienst gericht op privacy en informatiebeveiliging. OIS/ Datapunt meent echter geen verantwoordelijkheid in de juridische afwegingen, aangaande rechtmatigheid en de verplichtingen uit de AVG, te hebben. Bij duidelijke onrechtmatigheid heeft OIS/ Datapunt wel een signalerende rol naar de afnemer en zou OIS/ Datapunt een opdracht kunnen weigeren.

De visie van OIS/ Datapunt wordt deels beantwoord bij de uitleg van de rol van OIS/ Datapunt. Daarnaast moet er worden bijgevoegd dat OIS/ Datapunt het wettelijke uitgangspunt van transparantie bereikt door een actuele en openbare registratie van klanten en de door hen gevraagde gegevensdienst met de bijbehorende documentatie.

Werkproces privacy
Het Werkproces Privacy gerelateerde Dataleveringen kent vijf fasen: de intake, de voorbereiding, de realisatie, de exploitatie en de beëindiging. Deze zijn te vertalen naar drie toetsmomenten waarbij passende documentatie is ontwikkeld of nog ontwikkeld wordt. Het gaat om de input (intake en voorbereiding), de verwerking (realisatie en exploitatie) en de output (beëindiging). Uit de vergadering kwam naar voren dat bij de klantvragen waarschijnlijk bij 90 procent geen sprake zal zijn van persoonsgegevens. Mocht uit de Privacy QuickScan blijken dat er sprake is van persoonsgegevens dan wordt er in de voorbereidende fase een Privacy Impact Assessment uitgevoerd.

Met betrekking tot de beveiliging van data wordt er ook uitvoerig geïnventariseerd of er naast privacyoverwegingen andere argumenten zijn om bepaalde gegevens geheim te houden.

Als het gaat om governance dan treedt OIS/ Datapunt op als ware verwerker. Er worden gegevens verstrekt aan klanten als de bronhouder schriftelijk akkoord heeft gegeven. In het proces is privacy gewaarborgd middels het governancemodel waarin ieders verantwoordelijkheden zijn vastgelegd. OIS/ Datapunt heeft geen data in beheer, maar regelt de schakels en loggingprocedures. Datapunt heeft wel een opslagfunctie waar data uit verschillende bronnen gecombineerd worden. Datapunt fungeert als een ondersteuningsfunctie en vanuit die hoedanigheid kan Datapunt signaleren of er sprake is van tegenstrijdigheden, dubbelingen of overmaat aan data. Dit soort signalen worden doorgegeven aan de broneigenaar.

Ethische commissie
De CPA adviseerde een ethische commissie in te stellen wanneer er sprake is van 'gevoelige' resultaten. OIS/ Datapunt stelt zich op het standpunt zelf geen uitspraak te doen over de rechtmatigheid van een verwerking. Indien een verwerking leidt tot 'gevoelige gegevens' die geen persoonsgegevens zijn en ook niet herleidbaar zijn tot personen, is de AVG niet van toepassing. Indien dit het geval is zijn dan zijn de afnemer en bronhouder verantwoordelijk om deze ethische vraag aan het juiste gremium te stellen.

Informatievoorziening
Een ander aandachtspunt was de inrichting van een goede informatievoorziening aan burgers. OIS/ Datapunt sluit aan bij de stedelijke inrichting zoals besloten in een vergadering van het Gemeentelijke Management Team (GMT) over privacy en invoering van de AVG binnen de gemeente. Daar kwam het plan van aanpak voor de implementatie van de AVG naar voren. Een onderdeel van dat plan is de stedelijke informatievoorziening. Daar werden de actiepunten; richtsnoeren voor de klachtbehandelaars, een digitaal loket etc. besproken.

Cloud
Het laatste aandachtspunt had betrekking op Cloud VPS. De CPA wil een inzage in de auditrapportage met CLOUD VPS. Deze zal naar verwachting eind Q1 gereed zijn.

Reactie CPA
De CPA merkte op dat documentatie over de rol van Datapunt als beheerder van data ontbrak. Ook was de CPA benieuwd of de logging actief of passief gemonitord wordt. Datapunt gaf in de vergadering aan dat de data wordt opgeslagen als flat file die niet voor iedereen leesbaar is. In de volgende fase streeft Datapunt naar dynamische monitoring van logging die op basis van uitzonderingen op loggingpatronen waarschuwingssignalen geeft.
Daarnaast merkte de CPA op dat door de stapeling van data bij Datapunt informatie samen komt die ook voor andere partijen interessant zou kunnen zijn. De CPA vraagt zich af hoe Datapunt hiermee omgaat, indien daar een markt voor blijkt te zijn. Datapunt gaf als antwoord primair een dienst van de Gemeente Amsterdam te zijn. Indien de marktvraag zich

zou aandienen dan zouden daarvoor alle fases vanaf de intake opnieuw beschreven moeten worden. Vooralsnog is het belangrijkste om dit proces binnen de gemeente zo goed mogelijk te regelen en de privacy te waarborgen. Datapunt meent medio 2018 met deze werkwijze aan de slag te gaan.

Advies
De CPA bedankt Datapunt voor de heldere toelichting. De CPA stelt voor om Datapunt uit te nodigen bij een CPA vergadering, wanneer Datapunt een half jaar praktijkervaring heeft opgedaan met de omschreven aanpak, om enkele praktijkvoorbeelden toe te lichten.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Hoogachtend,

5.1, 2, e

5.1, 2, e

De heer mr. dr. U van de Pol
Voorzitter Commissie Persoonsgegevens Amsterdam

Commissie Persoonsgegevens Amsterdam
Uittreksel van het concept-verslag van de openbare vergadering op donderdag 25 januari 2018

6. Datapunt

In vervolg op de bespreking van een half jaar geleden in de CPA heeft Datapunt een document aangeleverd met antwoorden op de adviezen. Verder vraagt Datapunt nu het advies van de CPA over het nu ook aangeleverde document Werkproces Privacy gerelateerde Dataleveringen (WPD) en de drie bijlagen. Er is hard gewerkt om te komen tot een standaardisatie van het functioneren als Amsterdams schakelpunt tussen aanbieders en aanvragers van data uit de hele gemeentelijke organisatie. Men wil komen tot transparantie over alle processen waarbij persoonsgegevens een rol spelen en daarom zoveel mogelijk structureel vooraf zaken regelen. Er hebben zich in de praktijk nog geen kwesties rond privacy voorgedaan. Men stelt voor het proces te doorlopen vanuit de optiek van een klant die een vraag stelt aan Datapunt.
In het proces onderscheidt men vijf fases: de intake, de voorbereiding, de realisatie, de exploitatie en de beëindiging. Bij de intake worden afspraken gemaakt rond privacy. Naar verwachting komen er per jaar enkele honderden klantvragen binnen, waarvan er bij 90% geen sprake zal zijn van persoonsgegevens. Een voorbeeld zou kunnen zijn de vraag van de uitrukkende brandweer naar het aantal personen dat in een pand staat ingeschreven waar een brand gemeld is. Daar kan Datapunt dan bijvoorbeeld een dashboard voor ontwikkelen waarmee de brandweer die gegevens kan opvragen uit het bronbestand op het moment dat men die nodig heeft. In de voorbereidende fase wordt scherp omschreven wat de vraag precies is, zodat men tot een afgewogen besluit kan komen of Datapunt kan ingaan op het verzoek. In de realisatiefase wordt het dashboard gebouwd zodat het in de exploitatiefase gebruikt kan worden. De beëindigingsfase doet zich vooral voor bij eenmalige, kleinere verzoeken met name voor onderzoeken. Als uit de privacy quickscan blijkt dat er sprake is van persoonsgegevens, wordt er in de voorbereidende fase een PIA uitgevoerd. Als het gaat om de beveiliging van data wordt ook uitvoerig geïnventariseerd of er naast privacyoverwegingen andere argumenten zijn om bepaalde gegevens geheim te houden. Bijvoorbeeld als het gaat om eigen kostenramingen van een dienst waar nog een aanbestedingsprocedure aan de orde is. In het programma wordt dat soort dingen automatisch langsgelopen.
Er wordt ook gevraagd naar het doel en de grondslag voor de vraag naar persoonsgegevens. Er wordt niet gekeken of die inhoudelijk kloppen, want dat blijft een verantwoordelijkheid van de bronhouder en de klant, maar er wordt wel gekeken of grondslag en doel aanvaardbaar zijn geformuleerd. In het proces is wel geborgd dat daar kritisch naar gekeken wordt. Als het gaat om governance treedt Datapunt op als bewerker. Datapunt levert pas gegevens aan een klant als de bronhouder daar schriftelijk mee akkoord gaat. Bij de intake zit de accountmanager van Datapunt erbij als de klant de formulieren invult, zodat hij meteen kritische vragen kan stellen en erop kan wijzen welke bronhouders voor het beantwoorden aan de vraag nodig zijn. De klant moet rechtstreeks met de bronhouder tot overeenkomst komen. In het proces is van begin tot eind de privacy geborgd middels het governancemodel waarin ieders verantwoordelijkheden scherp zijn vastgelegd. Datapunt heeft zelf geen data in beheer, maar regelt de schakels, loggingprocedures en dergelijke. Alles wordt gedocumenteerd en vastgelegd zodat achteraf alles ook goed te verantwoorden is.

Waar data uit verschillende bronnen gecombineerd worden, heeft Datapunt wel een opslagfunctie. Datapunt is een ondersteuningsfunctie en kan vanuit die hoedanigheid signaleren of er sprake is van dubbelingen, tegenstrijdigheden of een overmaat aan data. Zulke signalen worden doorgegeven aan de broneigenaar. Desgevraagd geeft men aan dat er nog geen lijsten zijn van bronhouders, maar dat er gaandeweg wel een overzicht zal komen van klanten en bronhouders. De signaleringsfunctie van bewerkers staat ook in de AVG vermeld. Door de stapeling van brongegevens binnen Datapunt kan men ook zicht krijgen op tegenstrijdigheden tussen verschillende bestanden of de overmaat aan herleidbare persoonsgegevens die door stapeling ontstaat. Dat geeft een speciale dimensie aan deze signaleringsfunctie. De verantwoordelijkheid voor de juistheid van gegevens blijft bij de broneigenaar. Bij de quickscan wordt overigens al gevraagd of het bij de persoonsgegevens gaat om input of output van de gecombineerde gegevens. Gaandeweg zal er ook meer zicht komen op het aantal signaleringen en eventuele patronen.

De CPA mist in het document de rol van Datapunt als beheerder van data. Verder is men benieuwd of de logging actief of passief gemonitord wordt.

Datapunt geeft aan dat er op dat gebied nog veel in ontwikkeling is. De data worden opgeslagen als een flat file die niet voor iedereen leesbaar is. In een volgende fase wil men komen tot dynamische monitoring van logging die op basis van uitzonderingen op loggingpatronen waarschuwingssignalen geeft. Daarbij moet wel de proportionaliteit goed bekeken worden.

De CPA merkt op dat er zeker door de stapeling van data bij Datapunt informatie samen kan komen die ook voor andere partijen – overheid of markt – interessant zou kunnen zijn. De vraag is hoe men dat denkt te gaan regelen als daar een markt voor blijkt te zijn. Hoeven dan alleen regelingen met bronhouders getroffen te worden?

Datapunt zegt primair een dienst te zijn voor de gemeentelijke organisatie. Partijen buiten de gemeente kunnen gebruikmaken van open data. Vooralsnog komt er meer dan genoeg vraag op de organisatie af vanuit de gemeente zelf. Maar als de marktvraag zich zou aandienen, zouden daarvoor alle fases vanaf de intake opnieuw beschreven moeten worden. In juridische zin is Datapunt het best vergelijkbaar met een verwerker van (persoons-)gegevens en is het college de eindverantwoordelijke instantie. Technisch gezien zou het wel mogelijk zijn. Maar het gaat er nu om dit proces binnen de gemeente zo goed mogelijk te regelen en de privacy van begin tot einde te waarborgen ten aanzien van bronhouder en klant. Voor een relatief kleine vraag zou het proces in twee tot drie weken kunnen worden doorlopen. Daarnaast spelen de technische en procedurele zaken zoals de afspraken met de bronhouders. Voordat een verklaring voor vrijgave tot exploitatie wordt afgegeven, vindt eerst nog een laatste controle plaats om zeker te weten dat alles conform de afspraken is geregeld en gedocumenteerd. De verwachting is dat Datapunt medio 2018 met deze werkwijze aan de slag kan gaan.

De voorzitter bedankt voor de toelichting en stelt voor Datapunt uit te nodigen om enkele praktijkvoorbeelden te laten zien als men een half jaar praktijkervaring heeft opgedaan met deze aanpak.