Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam
Gemeente Amsterdam
Commissie Persoonsgegevens

Aan: Directeur Onderzoek, Informatie& Statistiek, de heer B. Daan,
C.c: Stedelijk directeur cluster Dienstverlening& Informatie, de heer M. Crooijmans
C.c: IV- manager cluster Dienstverlening& Informatie, de heer 5.1, 2, e
C.c: CIO AI, de heer 5.1, 2, e
C.c: Project- en relatiemanager Datapunt, de heer 5.1, 2, e, Privacy Officer Datapunt, de heer 5.1 5.1, 2, e en Privacy Officer D&I, de heer 5.1, 2, e

Datum	5 maart 2018
Behandeld door	T. 5.1, 2, e
E-mail	5.1, 2, e amsterdam.nl
Bijlage	1
Onderwerp	Datapunt

Geachte heer Daan,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 24 januari 2019 waren namens u aanwezig: de heer 5.1 5.1, 2, e (Privacy officer Datapunt), de heer 5.1, 2, e (Privacy officer Dienstverlening& Informatie) en de heer 5.1, 2, e (Project- en relatiemanager programma DataPunt).

Bij het agendapunt "Datapunt" is het volgende besproken:

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.

Tenslotte is tijdens de vergadering d.d. 25 januari 2018 het Werkproces Privacy gerelateerde Dataleveringen (WPD) besproken. 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).

Werkproces Privacy gerelateerde Dataleveringen (WPD)
Tijdens de vergadering gaf de heer 5.1, 2, e een presentatie over het WPD. Door middel van een OIS Privacy QuickScan wordt er gekeken of persoonsgegevens worden verwerkt. Indien dit het geval is wordt er, door middel van een Privacy Assessment, gekeken naar de rechtmatigheid en security. Vervolgens wordt er met behulp van een Template Vrijgave Gegevensdienst feitelijk getoetst of alle benodigde maatregelen zoals omschreven in de Privacy QuickScan en Assessment daadwerkelijk zijn genomen en of dit ook aantoonbaar is voor derden. Ten slotte wordt er van de Template Beëindiging Dienst gebruik gemaakt om de beëindiging van gegevensdiensten waarbij persoonsgegevens betrokken zijn, op een beheerste en aantoonbare manier uit te voeren zodanig dat er geen persoonsgegevens ergens in de keten ten onrechte opgeslagen blijven. Ook is er een data- incidentenprotocol opgesteld voor onverwachtse gevallen.
Ook werd tijdens de presentatie kenbaar gemaakt dat Datapunt slechts het technische vehikel is dat zorgt voor gegevenslevering uit een gemeentelijk bronbestand aan een andere gemeentelijke afdeling op een verantwoorde manier. Uiteindelijk is het aan de bronhouder om te beoordelen of zijn date geleverd mag worden voor het gevraagde doel.

Kanttekeningen en advies
De CPA vroeg zich tijdens de vergadering af of de **kwaliteit** van de aangeleverde bronbestanden gecontroleerd wordt. Datapunt gaf aan dat het niet zijn taak is om aangeleverde bestanden op juistheid te toetsen. Wel neemt men een signalerende en adviserende rol. Daarnaast heeft het GMT een governance programma opgesteld om verbetering van de kwaliteit van databestanden binnen de gemeente te realiseren.

De CPA merkte met betrekking tot de **verantwoordelijkheid** op dat de gemeente de juridische entiteit is. De gemeente draagt kortom de verantwoordelijkheid en kan daardoor aangesproken worden. De CPA geeft aan dat (interne) onderlinge afspraken over medeverantwoordelijkheid behulpzaam zijn voor het beschrijven van de functionele rollen. Echter, deze afspraken staan los van de rollen die in de AVG omschreven worden. De CPA adviseert ook om het begrip 'verwerker' voor Datapunt te laten vervallen als het gaat om verantwoordelijkheid. Door middel van een duidelijke Privacy Statement zou uitgelegd moeten

De CPA vroeg zich tijdens de vergadering ook af of er ervaringen zijn geweest met **datalekken**. Datapunt gaf aan dat er zich enkele incidenten hebben voorgedaan. Er is een data- incidentencoördinator aanwezig die na een melding contact opneemt met een Privacy Officer om te beslissen of er een formele melding gemaakt moet worden. Zo ja, dan wordt dat via de directie doorgegeven aan de Functionaris Gegevensbescherming die een formele melding indient bij de Autoriteit Persoonsgegevens mits daartoe een wettelijke plicht bestaat.

Met betrekking tot het verder verzamelen van de gegevens act de CPA van belang dat er beoordeeld moet worden of er sprake is van **verenigbare doeleinden** zoals omschreven in artikel 5, eerste lid sub b juncto artikel 6, vierde lid van de AVG. In de DPIA van Datapunt ontbreekt deze verenigbaarheidstoets. Dit onderdeel zal bij elke levering getoetst moeten worden. De bronhouder bepaalt de grondslag in eerste instantie. Op het moment dat er sprake is van het verder verzamelen van gegevens moet dus gekeken worden of er sprake is van verenigbare doeleinden. Is dit niet het geval dan is er sprake van een nieuwe verwerking en is een nieuwe wettelijke grondslag nodig.

Samenhangend met de verenigbaarheidstoets is de **informatieplicht.** Als er sprake is van een nieuwe verwerking dan moeten de betrokkenen hierover ingelicht worden. De CPA adviseert dan ook om: of een algemene privacy verklaring of een algemene privacy verklaring of een privacy statement van datapunt op de website op te nemen die de betrokken gemeentelijke onderdelen wijst op het voldoen aan deze informatieplicht.

De CPA dankt Datapunt voor een heldere presentatie en voor de aangeleverde stukken die een overzichtelijk beeld geven van de structuur en procedure. De CPA is voornemens Datapunt uit te nodigen bij een CPA vergadering, wanneer Datapunt praktijkervaring heeft opgedaan met de omschreven aanpak omtrent WPD en hierbij enkele praktijkvoorbeelden toe te lichten.

Ten slotte biedt de CPA haar interne notitie aan over de relatie tussen de verschillende privacytoetsen voor stroomlijning van het WPD proces . De CPA blijft graag op de hoogte van de ontwikkelingen.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Hoogachtend

5.1, 2, e

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

Commissie Persoonsgegevens Amsterdam
Uittreksel van het verslag van het besloten agendapunt van de vergadering op donderdag 24 januari 2019

1. DataPunt (Cluster Dienstverlening & Informatie)
De heer 5.1, 2, e verzorgt een presentatie over het Werkproces Privacygerelateerde Dataleveringen (WPD) dat DataPunt hanteert. Een jaar geleden heeft DataPunt het WPD aan de CPA voorgelegd en daar is toen afgesproken na verloop van tijd hier enkele praktijkvoorbeelden te laten zien. De presentatie en de praktijkvoorbeelden zijn bij de vergaderstukken gevoegd.
De drie kernwoorden van het WPD zijn: Privacy, Security en Accountability. Die vormen de rode draad in de vier instrumenten van het WPD: de Privacy QuickScan, het Privacy Assessment, het Template van Vrijgave en het Template van Beëindiging. Voor het onverhoopte geval dat er iets misgaat, is er een data-incidentenprotocol opgesteld. Dit alles is ingebed in het standaard werkproces van OIS dat vijf stappen kent: intake, voorbereiding, realisatie, exploitatie en beëindiging. Bij de realisatiefase wordt gekeken of alle maatregelen die uit de QuickScan en de PIA naar voren kwamen en andere afspraken inderdaad gerealiseerd zijn en dat wordt in het template van vrijgave dan nagelopen zodat men kan overgaan tot de levering van de data. In het template van beëindiging wordt nagegaan of alle maatregelen getroffen zijn om de datalevering verantwoord te beëindigen zonder datalekken achter te laten. De klanten komen grotendeels uit afdelingen van de gemeente zelf. Open data zijn in beginsel voor iedereen toegankelijk, ook voor externe partijen. Maar verzoeken van externe klanten kunnen er ook komen en worden dan getoetst conform het WPD-proces. DataPunt is in beginsel alleen het technische vehikel dat ervoor zorgt dat de gegevens uit een gemeentelijk bronbestand aan een andere gemeentelijke afdeling of aan een externe partij geleverd worden op een verantwoorde manier. Alle documenten moeten door de desbetreffende partijen voor akkoord getekend worden.
De bronhouder kan als beste beoordelen of zijn data geleverd mogen worden voor het gevraagde doel. In het Stelselpedia – het stelsel van basisregistraties in Amsterdam – zijn de bronhouders van basisregistraties vastgelegd zodat geen misverstand meer over bestaat wie de bronhouder is. De klant is verantwoordelijk voor de goede/rechtmatige behandeling van de data volgens de geldende regelgeving. Een van de motieven om DataPunt op deze manier in te richten was nu juist dat OIS zelf niet alle kennis in huis heeft om te kunnen beoordelen of een bepaalde datalevering voor een bepaald doel binnen de regelgeving geoorloofd is. Het is een interessante vraag wie de naleving van de geldende afspraken zou moeten verifiëren. Uit de PIA komen maatregelen tevoorschijn en in de beide templates wordt gekeken of die maatregelen inderdaad getroffen zijn. Omdat alle partners die documenten ondertekenen, ontstaat er als het ware een auditrapport van begin tot einde van de gegevensdienst (privacy by design & accountability).
De SO en de PO van de clusters helpen de bronhouders en de overige stakeholders bij het invullen van de drie onderdelen van de PIA en het opsporen van maatregelen die nodig zijn voor de informatiebeveiliging. De PO en SO van het cluster worden door de accountmanagers van DataPunt bij het begin van de aanvraag met de klant gekoppeld. De PO en SO van DataPunt evalueren de ingevulden formulieren door de klant en controleren of de vragen zijn ingevuld, gemotiveerd, alle ondersteunende stukken zijn bijgevoegd (indien die er zijn), en hebben een signaalfunctie (dwz als zij van mening zijn dat er in strijd met de AVG wordt gehandeld zij dit signaal afgeven aan de klant, de PO en de SO van het cluster.Via dit proces worden de concrete (technische en organisatorische) maatregelen

geformuleerd. Het is van wezenlijk belang dat de te nemen maatregelen bekend zijn voordat men daadwerkelijk iets gaat ontwikkelen om de gegevenslevering mogelijk te maken.
De privacy wordt op deze wijze gewaarborgd in een proces dat aansluit bij de scrum-werkwijze en voor elke fase dus met een soort thermometer werkt om de stand van zaken te monitoren. De stand van zaken wordt momenteel nog bijgehouden in een Excel-bestand, maar er is een dashboard in ontwikkeling.
Voor het geval er iets misgaat, is er bovendien het data-incidentenprotocol gemaakt met goed beschreven rollen en taken. Het is een nadere uitwerking van het stedelijk datalekprotocol. Iedere medewerker heeft er nu zicht op bij wie hij een lek of ander incident rond data moet melden. Dat schept een cultuur van bespreekbaarheid rond zulke incidenten.

De CPA is, indachtig de perikelen rond de bestanden van parkeerkaarten voor gehandicapten, benieuwd of DataPunt de kwaliteit van de aangeleverde bronbestanden controleert. Weigert DataPunt bijvoorbeeld gegevens verder door te geven als men constateert dat er iets aan schort?

DataPunt zegt daarin wel een signalerende en adviserende rol te nemen, maar als doorgeefluik niet proactief kwaliteitscontrole op bronbestanden uit te voeren. Het GMT heeft wel een governanceprogramma opgesteld ter verbetering van de kwaliteit van databestanden binnen de hele gemeente. DataPunt kan bronhouders bijvoorbeeld wel adviseren een bestand nog niet te publiceren of door te leveren. De bestanden voor het City Data Portaal worden wel goed gecontroleerd voordat ze gepubliceerd worden. Omgekeerd kunnen de combinaties van bestanden bij DataPunt inzichten opleveren waarmee de bronbestanden verrijkt of verbeterd kunnen worden. Het is een doorlopend proces om met elkaar te werken aan verbeteringen en het wegwerken van discrepanties. Als DataPunt iets signaleert, wordt er actie ondernomen naar de betreffende partij, waarbij men desnoods kan escaleren naar de FG of wethouder. Maar het is niet de taak van DataPunt om aangeleverde bestanden te toetsen op juistheid.

De CPA merkt op dat de gemeente uiteindelijk de juridische entiteit is die verantwoordelijkheid draagt en aangesproken kan worden. Interne onderlinge afspraken over medeverantwoordelijkheid voor de verwerking zijn goed om de functionele rollen te beschrijven, maar staan los van de rollen die de AVG benoemt. De CPA adviseert het begrip verwerker voor DataPunt los te laten als het gaat om verantwoordelijkheid en in een duidelijk voor buitenstaanders herkenbaar privacystatement aan te geven hoe het juridisch zit.

DataPunt geeft aan dat het sinds de hervorming van de gemeentelijke IV-structuur ook in technische zin meer onderdeel is van de gemeente, waar het voorheen toch vooral gezien werd als een extern element. Dat maakt het logisch de terminologie nu ook aan te passen aan de nieuwe omstandigheden. Het privacystatement is nu nog ondergebracht bij OIS. Men zal nagaan of dat meer herkenbaar als iets van DataPunt kan worden gemaakt.

De CPA is benieuwd of er ervaringen zijn met datalekken.

Er zijn enkele incidenten geweest en toen heeft het protocol zijn nut bewezen. Er is een data-incidentencoördinator. Dit is de Architect bij DataPunt. Indien de Architect afwezig is

of anderzinds niet bereikbaar dan wordt er geschakeld met de Product Owner van Datapunt of anders met de directeur van OIS. De incidentcoordinator neemt na een melding van een medewerker contact op met de PO om te bepalen of een formele melding nodig is. Via de directie wordt dat dan doorgegeven aan de FG die de formele melding bij de AP doet indien daartoe een wettelijke plicht bestaat. Verder wordt de stedelijke procedure gevolgd. Het systeem blijkt dus in de praktijk te werken. Het enige wat nog moet gebeuren is het plaatsen van stickers met de contactpersoon op elk bureau zodat alle medewerkers in voorkomende gevallen meteen weten wie ze moeten waarschuwen.
De ervaringen met dit WPD-model zijn tot nu toe positief. Op dit moment worden negentig processen gemonitord, maar men signaleert een toenemende vraag. Er zijn in Amsterdam driehonderd datasets die via het Amsterdamportaal beschikbaar worden gesteld. Er is een ambitie om te groeien en daarom is het van belang dat dit proces er is en ook werkt. De belangstelling bij de Amsterdamse stakeholders neemt toe omdat zij er voordelen voor hun eigen organisatie in zien.
Wel signaleert men dat de klanten vaak komen met de vraag welke procedure zij moeten doorlopen. Daarom is mede op verzoek van de FG en de CISO van de gemeente Amsterdam een werkgroep opgericht om te bezien hoe de verschillende processen gestroomlijnd kunnen worden. Verder onderzoekt men de ethische kanten van de omgang met data als lokale overheid. Dit punt is onder meer ook aangekaart in het manifest TADA over de digitale stad (zie coalitieakkoord gemeente Asmterdam 2018). Daar gaat het om vragen als: wat mag je met data doen en wat betekent het werken voor een lokale overheid in relatie met de omgang met gevoelige gegevens. Ook wordt met de stadsarchivaris in het kader van de Archiefwet gekeken naar bewaartermijnen en andere kwesties, bijvoorbeeld rond dynamische en niet dynamische datasets. Er moet nog uitgezocht worden hoe dat allemaal concreet ingericht kan worden. Ook moet in het kader van de Wet overheid en markt nog uitgezocht worden hoe het zit met mededingingskwesties t.a.v. het publiceren van brondcode (open source). Er is Kortom, er is veel wet- en regelgeving rond de omgang met data en zaak is samen met de partners te zorgen dat daar rekening mee gehouden wordt. Het is zaak de procedures daar steeds beter op in te richten en wordt reeds ondervangen in het WPD proces (voor zover bekend).
DataPunt is benieuwd of met deze aanpak voldoende is tegemoetgekomen aan de punten die de CPA naar aanleiding van de bespreking in januari 2018 naar voren heeft gebracht. De CPA geeft aan dat hieraan is voldaan.

De CPA biedt aan de interne notitie van de CPA over de relatie tussen de verschillende privacytoetsen (VRA, PIA, DPIA en dergelijke) toe te sturen aan DataPunt ten behoeve van de werkgroep voor stroomlijning van het proces. Verder kan men bij concrete knelpunten en dilemma's altijd een advies vragen aan de CPA. De CPA blijft graag op de hoogte van ontwikkelingen. De aangeleverde stukken hebben de CPA een overzichtelijk beeld gegeven van de structuur en de procedure. De CPA is voorstander van het nog meer inzichtelijk maken van de procedures door de werkgroep en het in beeld brengen van de andere genoemde aspecten, vooral waar het gaat om samenwerking met commerciële partijen en innovatieve projecten. DataPunt zal nog meer vertakkingen krijgen en dat zal de zaken er niet eenvoudiger op maken.
De voorzitter bedankt voor de komst en nodigt DataPunt uit vooral weer langs te komen als zich spannende zaken aandienen. DataPunt nodigt de CPA uit om een keer langs te komen, zodat de CPA met eigen ogen kan zien hoe DataPunt werkt en de waarborgen die zij treffen om data op een geconroleerde, veilige en rechtmatige manier te ontsluiten.