Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam

Commissie Persoonsgegevens

Aan: Manager Dienstontwikkeling en Platformen, 5.5.1, 2, e

C.c: Eindverantwoordelijk directeur: A. Bozia

C.c: Lead Risk: 5.1, 2, e

C.c: Functionaris Gegevensbescherming: 5.1, 2, e

Datum september 2023

Behandeld door 5.1, 2, e

E-mail cpa@amsterdam.nl

Onderwerp Cloud Voorziening gemeente Amsterdam (Cloud Platform)

Disclaimer:
Onderstaand advies is gebaseerd op informatie die beschikbaar was tot en met mei 2023. Sinds 10 juli 2023 zijn er nieuwe afspraken, met name het adequaatheidsbesluit als onderdeel van het 'Data Privacy Framework', van kracht geworden met betrekking tot het doorgeven van persoonsgegevens vanuit de Europese Economische Ruimte naar de Verenigde Staten. Om de actuele status en naleving van deze afspraken te verifiëren, is het raadzaam om de website van het Data Privacy Framework te raadplegen. Deze website biedt informatie over welke organisaties zich aan deze nieuwe afspraken hebben gecommitteerd en welke software compatibel is met deze afspraken.

Advies van de Commissie Persoonsgegevens Amsterdam (CPA) over de Cloud Voorziening van de Gemeente Amsterdam.

Geachte heer 5.1, 2, e

Tijdens de vergaderingen van de Commissie Persoonsgegevens Amsterdam (CPA) van 3 maart 2022, 2 juni 2022 en 26 januari 2023 waren bij het agendapunt "Cloud Voorziening gemeente Amsterdam" namens u aanwezig: de eindverantwoordelijk directeur en de Lead Risk.

Bijgaand treft u aan het advies van de CPA.

A. Algemeen advies (samenvatting)

De commissie adviseert om maatregelen te nemen om in het geval van uitval van de service niet met lege handen te staan. Ook geeft de commissie enkele overwegingen mee ten aanzien van het regelen van het risicomanagement.

De CPA verzoekt verder om conform de DPIA het stuk waaruit acceptatie of het niet opvolgen van de mitigerende maatregelen te verstrekken aan de CPA.[1]

Tot slot verzoekt de commissie om de te plaatsen applicaties in het Cloud Platform voor te leggen aan de CPA ter advisering, in het bijzonder als sprake is van applicaties waar gevoelige en/of gegevens van medewerkers en/of inwoners in worden verwerkt en de uitbreiding van de scope noopt tot het uitvoeren van een (aanvullende) Data Transfer Impact Assessment (DTIA). De CPA geeft in overweging om hiertoe het format van het Privacy Control Framework (PCF) aan te passen en daarin een verwijzing naar de CPA in op te nemen.

B. Aanleiding en omschrijving

Traditioneel houdt een organisatie alle informatie, servers en computers binnenshuis. De organisatie is dan ook zelf volledig verantwoordelijk voor het beheer, op peil houden en onderhoud van alle apparatuur en software. Amsterdam is kwetsbaar gebleken, met name als het gaat om het tijdig alle apparatuur van de benodigde patches te voorzien om de software 'bij de tijd' te houden. En dat maakt de organisatie extra kwetsbaar voor cyberaanvallen, die zich in de praktijk vrijwel altijd met succes richten op organisaties met achterhaalde software.

De gemeente Amsterdam heeft daarom op basis van de opgestelde Cloudstrategie[2] het Cloud Platform[3] ontwikkeld als basis voor de nieuwe dienstverlening in de cloud van de directie Digitale Voorzieningen (voorheen directie ICT). Dit is de basis voor de nieuwe dienstverlening in de cloud, waarbij applicatiebouw en hosting in de Azure Cloud van Microsoft plaatsvindt. Door scripting en geautomatiseerd werken met generieke bouwstenen, kan de ICT-capaciteit van de organisatie veel efficiënter en zichtbaarder voor de business worden ingezet.

Voorwaarde voor het ontwikkelen van een (eigen) specifieke applicatie betreft dat eerst wordt verkend of andere directies wellicht een gelijkwaardige applicatie in huis hebben. Is dat niet het geval, dan wordt de markt verkend op beschikbare open-source of Software-as-a-Service (SAAS) applicaties. Pas als er aantoonbaar geen geschikte applicatie beschikbaar is, kan de ontwikkeling van een eigen applicatie worden onderzocht en ontwikkeld.

---

[1] Zoals vermeld in de DPIA van het 'Azure Cloud Competence Center' van 7 maart 2022, p. 13.
[2] Zie voor de Cloudstrategie van de gemeente Amsterdam: https://amsterdam.raadsinformatie.nl/document/11995205/1/A+-+23+ICT+en+Digitale+Stad+%2849%29+2_+Cloudstrategie+gemeente+Amsterdam+2022-2.
[3] Cloud Voorziening gemeente Amsterdam, voorheen Cloud Competence Centre, CCC.

Omdat de beoogde applicatiebouw en hosting plaatsvinden in de Azure Cloud van Microsoft, zal ondanks het gebruik van zogenaamde Azure Regions[4], sprake zijn van internationale doorgifte van persoonsgegevens naar de Verenigde Staten (VS). Hoewel in beginsel gegevens van de gemeente in Nederland (regio West-Europa) worden opgeslagen, kunnen persoonsgegevens in bepaalde gevallen namelijk toch in de VS verwerkt worden. Dit komt omdat persoonsgegevens worden opgeslagen in een public cloud, waarvan de moedermaatschappij (Microsoft) is gevestigd in de VS, waar Amerikaanse inlichtingendiensten toegang kunnen hebben tot deze gegevens of na toestemming van de gemeente kunnen worden opgeslagen in de VS.

Vanwege het theoretische risico op toegang tot persoonsgegevens door Amerikaanse inlichtingendiensten, is het mede naar aanleiding van Schrems II noodzakelijk om een DTIA uit te voeren om daarmee de risico's van de voorgenomen internationale doorgifte in kaart te brengen en zo nodig maatregelen voor te stellen.[5] Een DTIA geeft een beeld van de informatieverwerking, de risico's en helpt bij het formuleren en nemen van mitigerende maatregelen. De DTIA is samen met de externe adviesbureaus Considerati en Dentons ontwikkeld en uitgevoerd.

Verwerking van persoonsgegevens
In het Azure Cloud Platform worden in eerste instantie alleen persoonsgegevens verwerkt van medewerkers, zowel intern als van externe medewerkers en van externe leveranciers van de betrokken diensten en afdelingen, die in het kader van ontwikkel- dan wel beheertaken werkzaamheden uitvoeren in de onder punt 2 beschreven systemen en omgevingen. De externe leveranciers hebben overeenkomsten gesloten met de gemeente Amsterdam.

Het doel van de verwerking van persoonsgegevens is tweeledig:

1. Een gebruikersaccount is noodzakelijk voor het verkrijgen van toegang tot de genoemde omgevingen. Dit betreft een persoonsgebonden gebruikersaccount, dat tevens wordt gebruikt voor de kantoorautomatiseringsomgeving (Amsterdamse Digitale Werkomgeving, 'ADW'); en
2. Voor de borging van de betrouwbaarheid van de systemen, dienen conform de richtlijnen van de interne controle en administratieve organisatie, acties te worden geregistreerd zodat de betrouwbaarheid kan worden geborgd. Betrouwbaarheid in deze houdt in: "Beschikbaarheid, Integriteit, Vertrouwelijk en Onweerlegbaarheid" volgens de Nederlandse Overheid Referentie Architectuur (NORA).

[4] Er is gekozen voor Regio West Europa (Amsterdam), https://azure.microsoft.com/en-us/explore/global-infrastructure/data-residency/#more-information
[5] Zie HvJEU 16 juli 2020 https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=NL (Schrems-II arrest) waarin het zogenaamde 'privacy shield' ongeldig is verklaard. Hoewel de Europese Commissie recentelijk een adequaatheidsbesluit heeft gepubliceerd voor de VS (https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-naar-de-vs, (art. 45 AVG) voor gegevensuitwisseling met de VS.

Het betreft verwerking van persoonsgegevens voor bovengenoemde doelen. De verwerking van persoonsgegevens in applicaties, ofwel zogenaamde Workloads, wordt bepaald door de betreffende applicatie-eigenaar dan wel opdrachtgever van een Workload. De scope van dit advies is daarom eveneens beperkt tot het Cloud Platform als zelfstandige entiteit en niet de (toekomstig) te plaatsen Workloads.

Elke applicatie- of proceseigenaar is verantwoordelijk voor het uitvoeren van gegevensbeschermingsanalyses, waaronder een (Quickscan) DPIA, voor de in de cloud te ontwikkelen en/of te plaatsen applicatie. Deze analyse betreft dan een aanvulling op de generieke (paraplu) DPIA die is uitgevoerd op Cloud Platform. Deze verplichting tot het uitvoeren van een DPIA vloeit voort uit de opgetuigde PCF en Security Control Framework (SCF). Deze frameworks zijn een concrete vertaling van de wettelijke verplichtingen uit de Baseline Informatiebeveiliging Overheid (BIO) en de AVG.

Extra maatregelen naar aanleiding van de DTIA
Om het risico op inzageverzoeken van publieke autoriteiten van de VS te beperken zijn een aantal specifieke technische maatregelen voorgesteld, specifiek ter bescherming van bijzondere en strafrechtelijke persoonsgegevens:

- Het in eigen beheer houden van encryptiesleutels, deze worden dus niet door Microsoft of enig andere leverancier beheerd;[6]
- Met verwerkers worden extra maatregelen in contractuele bepalingen gesloten.

Cloudbrief Van Huffelen en reactie Cloud Voorziening
In 2022 heeft de Nederlandse staatssecretaris voor Koninkrijkrelaties en Digitalisering de zogenaamde 'Cloudbrief' gepubliceerd waarin een Rijksbreed kader is opgesteld met voorwaarden waar overheidsdiensten (zoals de gemeente Amsterdam) aan moeten voldoen om publieke clouddiensten te mogen gebruiken. Uit de reactie[7] vanuit de Cloud Voorziening Amsterdam volgt dat de gemeente het advies op alle elf de punten opvolgt en wordt voldaan aan de in de brief vastgelegde voorwaarden. Ten aanzien van basisregistraties (BRP, WOZ etc.) in de publieke cloud wordt opgemerkt dat dit enkel kan volgens een pas-toe-leg-uit constructie (waarbij de leg-uit is vervat in een risicoanalyse zoals een (pre)DPIA) en voorafgaand advies van de CIO Rijk.

Verzoek aan de CPA
Aan de CPA wordt verzocht kennis te nemen van en te adviseren over de uitgewerkte Data Protection Impact Assessment (DPIA), de DTIA en de overige aangeleverde stukken en eventuele vragen en opmerkingen over de werkwijze te delen vanuit de expertise van de CPA.

[6] Deze maatregel wordt van toepassing op BBN2+ en bijzondere en strafrechtelijke persoonsgegevens. Voor overige gegevens (BBN2) worden bestaande maatregelen voldoende geacht. Zie ook de notitie *Aanvullende maatregelen ter bescherming van bijzondere persoonsgegevens in de public cloud.*
[7] Reactie Cloud Voorziening Amsterdam Rijksbreed Cloudbeleid 2022 van 13 december 2022.

C. CPA-advies

De commissie dankt de aanwezigen voor hun toelichting en de aangeleverde stukken. Na de vergadering heeft de CPA een schriftelijke reactie ontvangen op de concept notulen die voor dit agendapunt zijn doorgezonden. Daarnaast is er een presentatie gehouden over de privacyaspecten behorend bij de aansluiting op het Cloud Platform.

Eigen verantwoordelijkheid Workloads en rol CPA

Uit de toelichting, ingediende stukken en presentatie over de privacyaspecten die zijn betrokken bij het aansluiten van applicaties op het Cloud Platform (dat fungeert als generieke voorziening, of 'container' voor te plaatsen applicaties) volgt dat er een hoge mate van verantwoordelijkheid is neergelegd bij de Workloads om te voldoen aan de security en privacy standaarden van de gemeente Amsterdam. Daartoe zijn een PCF en een SCF opgesteld om de Workload te toetsen. Het PCF bevat bijvoorbeeld de verplichting om bewijs te overleggen waaruit blijkt dat wordt voldaan aan de privacy maatregelen. Dit kan worden bewerkstelligd door een uitgevoerde DPIA te overhandigen aan het Risk Team van het Cloud Platform. Samen met de betrokken privacy officer van de Workloads wordt bekeken of aansluiting op het Cloud Platform mogelijk is. Om grip te houden op de applicaties die op het Cloud Platform landen, transparant te zijn over de (voorgenomen) aansluiting en verantwoorde omgang met persoonsgegevens te bevorderen, adviseert de commissie om in bepaalde gevallen de CPA te betrekken in dit proces. Onder het kopje 'ethische aspecten' wordt deze aanbeveling nader toegelicht en verdiept.

Getroffen (technische) maatregelen

De commissie is verheugd te constateren dat er verschillende aanvullende en mitigerende maatregelen zijn getroffen om een betrouwbare basis te creëren om persoonsgegevens op te laten landen. De commissie acht het in het bijzonder bewonderingswaardig dat men streeft naar technische oplossingen en standaarden[8] die hoger liggen dan normaliter worden aanbevolen, met name om een zo hoog mogelijk beschermingsniveau te handhaven voor bijzondere en strafrechtelijke persoonsgegevens. De commissie vertrouwt in het verlengde daarvan erop dat de jaarlijkse toetsingen en ISAE-verklaringen aandachtig worden bestudeerd en zo nodig acties worden ondernomen om het hoge (beschermings)niveau te behouden. Dit kan ook betekenen dat regelmatig wordt onderzocht of het wellicht benodigd is om extra technische en/of organisatorische maatregelen (zoals in de DTIA geïdentificeerd) te treffen om een 'in wezen gelijkwaardig beschermingsniveau' te behouden. Het behouden van een hoog beschermingsniveau van persoonsgegevens, zoals wordt verwacht van een gemeente als (lokale) overheid,[9] blijft een continu proces waarbij controle op de naleving van vastgesteld beleid en ontwikkelingen op het gebied van internationale doorgifte een noodzakelijk onderdeel is.

De CPA wil daarnaast in overweging geven om te onderzoeken of er voldoende maatregelen zijn getroffen voor het geval dat het platform onverwacht niet beschikbaar is, zeker indien (kritieke) processen hierdoor stil komen te vallen. De

[8] Waaronder BBN2+.
[9] Zie de reactie van de Autoriteit Persoonsgegevens op het Rijksbreed cloudbeleid 2022, p. 2.

afhankelijkheidsrelatie die onlosmakelijk is verbonden aan het plaatsen van ICT-systemen in de cloud mag niet worden onderschat en het is belangrijk om hierop effectief risicomanagement op toe te passen. Het is raadzaam om een grondige analyse uit te voeren van de mogelijke impact en gevolgen van een uitval van het platform, evenals het implementeren van passende maatregelen om de continuïteit van kritieke processen te waarborgen. De CPA voegt hier nog aan toe dat in het geval Microsoft nu of in de toekomst keuzes maakt die in strijd zijn met de Tada-waarden die de gemeente hanteert, overwogen moet worden om over te stappen naar een andere cloudomgeving. Een onderzoek en analyse naar een goede exit-strategie is daarom des te belangrijker. Wanneer de gemeente pas bij een inventarisatie van alternatieven nadenkt over een exit-strategie wordt de overstap extra ingewikkeld. De exit-strategie moet er immers liggen voordat applicaties op het platform gaan draaien. Een eventuele overstap wordt namelijk met elke nieuwe applicatie ingewikkelder.

Daarnaast adviseert de CPA om een vinger aan de pols te houden voor wat betreft de telemetrische en diagnostische data die naar servicecentra in de VS gaan voor analyses. Hoewel het belang, de verbetering van de dienstverlening en beveiliging van de (wereldwijde) infrastructuur wordt onderkend, moet het risico dat hierbij gepseudonimiseerde gegevens alsnog worden herleid naar een natuurlijk persoon niet uit het oog worden verloren. Mocht daarom de benodigde expertise alsnog worden uitgerold binnen de Europese Economische Ruimte (EER) dan adviseert de commissie om daar uitsluitend gebruik van te maken en de doorgifte van gegevens buiten de EER te staken.

Ethische aspecten

De achterliggende bedoeling van de migratie naar de cloud hangt samen met het regelen van en voldoen aan technische en organisatorische (beveiligings)maatregelen die steeds lastiger zijn te realiseren in eigen beheer. Door in zee te gaan met een grote partij zoals Microsoft, met bijbehorende kennis en ervaring beoogt de gemeente een veilige keuze te maken en een hoog beschermingsniveau na te streven. Er kleven echter logischerwijs ethische bezwaren aan het gebruik van een publieke, commerciële clouddienst die is gevestigd buiten de EER op het gebied van privacy, cyberveiligheid en afhankelijkheid.

Hoewel zoals eerder vermeld de scope van dit advies is beperkt tot het uitgangspunt dat het Cloud Platform in eerste instantie enkel als spreekwoordelijke container fungeert voor applicaties die de Workloads op het Cloud Platform willen laten landen[10], is het onvermijdelijk om niet al voor te sorteren op de situatie dat in de toekomst ook gegevens van inwoners worden verwerkt via applicaties die op het Cloud Platform moeten landen. Dit brengt verschillende risico's met zich mee, waaronder dat ondanks de aanvullende maatregelen (onbedoeld) wordt bijgedragen aan het verzamelen van persoonsgegevens Microsoft voor doeleinden die niet zijn voorzien. [11] Daarnaast kan equivalente (rechts)bescherming, waaronder tegen inzageverzoeken door opsporings- of

[10] De verwerking van persoonsgegevens is beperkt tot medewerkersgegevens conform ADW, waarbij de verwerking is beperkt tot inlognaam (Amsterdam account), wachtwoord en IP-adres.
[11] Hier zijn overigens vooralsnog geen aanwijzingen voor en er zijn maatregelen genomen (onder meer contractuele afspraken in de verwerkersovereenkomst) om verwerking van persoonsgegevens voor andere doeleinden dan overeengekomen te voorkomen.

inlichtingendiensten in de Verenigde Staten vooralsnog niet voor de volle honderd procent worden bereikt. De Amsterdammer heeft voorts geen mogelijkheid om zich effectief te verzetten tegen deze keuze of zich hiervan uit te zonderen. Een zeker verlies aan controle en zeggenschap van individuen over hun gegevens is daarmee onvermijdelijk.

De commissie adviseert daarom, mede om de transparantie tegenover de Amsterdammer te verhogen om, in het geval dat het laten landen van een applicatie op Cloud Platform het uitvoeren van een (aanvullende) DTIA noodzakelijk maakt, deze bij de CPA voor te leggen ter advisering indien de uitbreiding van de te verwerken persoonsgegevens een hoog risico voor de rechten en vrijheden van de betrokkenen betreft. Het uitvoeren van een aanvullende DTIA zou moeten volgen uit het PCF, de commissie geeft daarom in overweging om een verwijzing op te nemen naar de CPA in het PCF. De noodzaak voor het uitvoeren van een aanvullende DTIA hangt samen met de uitbreiding van de te verwerken persoonsgegevens die verdergaan dan onder de paraplu-DPIA in kaart zijn gebracht. Dit zou daarom een trigger kunnen zijn om de voorgenomen plaatsing van de applicatie in het Cloud Platform voor te leggen aan de CPA en zodoende bij te dragen aan een transparante gegevensverwerking en een verantwoorde omgang met persoonsgegevens te na te streven.

Laatstelijk merkt de CPA op dat met de keuze voor Microsoft de weg voor alternatieven die mogelijk duurzamer, open-source, privacy vriendelijker en/of democratischer zijn vooralsnog afgesloten, wat tot kritische geluiden vanuit de raad heeft geleid.[12] De CPA adviseert daarom de Amsterdamse Cloudstrategie bijtijds te herijken om te bezien of deze (nog) aansluit bij de publieke en maatschappelijke waarden en ambities van de gemeente. Mocht een bewezen alternatief binnen de EER beter aansluiten bij deze waarden en de mogelijkheid bieden om onafhankelijk te worden van grote (commerciële) partijen dan geeft de CPA in overweging om te onderzoeken of overstappen mogelijk is en/of bij te dragen aan de ontwikkeling daarvan. De CPA merkt echter op dat een exit-strategie niet pas relevant wordt als een alternatief beschikbaar is.

Tot slot
Verder verwijst de CPA u naar bijgevoegde notulen van de vergaderingen over het betreffende agendapunt.

Hoogachtend,

De heer F. van Rootselaar
Vice-Voorzitter Commissie Persoonsgegevens Amsterdam

[12] Zie het opiniestuk zoals verschenen in het Parool van 3 oktober 2022: Opinie: 'Amsterdam moet juist nu kiezen voor verantwoorde technologie gebaseerd op publieke waarden' (parool.nl).

Uittreksel van het verslag van het besloten agendapunt van de vergadering op donderdag 26 januari 2023

6. Cloud Platform

Voor deze derde keer dat het onderwerp hier aan de orde is, zijn de gevraagde stukken aangeleverd. De CPA had gevraagd nog een aantal zaken uit te zoeken en dat is gebeurd. Er is een DPIA en een DTIA uitgevoerd. Binnen de organisatie leeft het onderwerp en daarom is ook de reactie op het Rijksbreed Cloudbeleid toegevoegd. Er zijn zogeheten comfortmaatregelen getroffen om de beveiliging en privacy te beschermen door daar continue toetsen op uit te voeren en direct iets te doen met de bevindingen. Daartoe zijn het Privacy Control Framework (PCF) en het Security Control Framework (SCF) opgetuigd waarmee de engineers werken. Het PCF dwingt tot goed uitvoeren van de verschillende AVG-verplichtingen, waaronder het uitvoeren van een DPIA af. De frameworks vormen concretiseringen van de wettelijke verplichtingen, de BIO en AVG. Het SCF wordt binnenkort herzien en aangescherpt. Een aantal zaken uit het framework kunnen inmiddels worden geautomatiseerd. Het iteratieve karakter van deze werkwijze vormt een van de sterke punten. De relatie tussen ICT en de business is aanmerkelijk verbeterd. Er wordt toekomstgericht gewerkt, maar het systeem is nooit helemaal klaar en er zullen altijd aanvullingen mogelijk of nodig blijven. Daarnaast kunnen er diensten zijn of komen die onder een ander eisenpakket dan de BIO vallen, bijvoorbeeld sectorale wetten zoals Suwinet. Daarvoor moet dan gekeken worden of die in te passen zijn of op een andere plek moeten worden ondergebracht. Dat moet dan wel goed gepland en beschreven worden. Dankzij de organisatiestructuur is de leiding wel van meet af aan betrokken bij de invoering en de nodige beveiligingsmaatregelen rond applicaties.
De DPIA is hier al eerder aan de orde geweest. De scope is het platform en de Cloudstrategie. Er is een paraplu-DPIA gemaakt zodat bij elke applicatie die op het platform komt getoetst wordt op wat er in de cloud belandt. De DevOp-teams hebben een eigen verantwoordelijkheid voor dat deel dat ze willen laten aansluiten. Er worden standaard geen accounts aangemaakt. Wie een account wil, moet dat expliciet melden en dat blijft dan geldig voor maximaal drie maanden. Er zijn dus geen permanente accounts en ook geen algemeen admin-account. Er is gekozen voor een PAAS-constructie (Platform as a Service), waarbij het beheer van het platform bij de leverancier ligt en aan applicatiebouwers alleen bouwblokken geleverd worden. Er is gezocht naar de beste technische oplossingen en de standaarden liggen hoger dan bij de oplossingen die de VNG aanbeveelt. Er zijn veel contacten met de VNG om de kennis die hiermee de afgelopen vier tot zes maanden is opgebouwd ook beschikbaar te maken voor andere gemeenten. Het was een kostbare operatie, maar men heeft er alle vertrouwen in dat er nu een betrouwbare basis ligt om persoonsgegevens op te laten landen.
De DTIA (Data Transfer Impact Assessment) geeft inzicht in de datastromen. Bij de opstelling is Considerati ingeschakeld en Dentons heeft analyses gemaakt van de lokale rechtsbescherming van data in Amerika. Dat alles is van belang om de rechtsbescherming van data te waarborgen. Er wordt uitsluitend gewerkt met Nederlandse leveranciers die aan de Nederlandse wetgeving gebonden zijn. Ook de support komt uitsluitend uit Europese landen. Data worden nu op drie plaatsen in

Nederland opgeslagen. Als dat ook in Ierland zou gebeuren, zouden wellicht aanvullende maatregelen nodig zijn. China en India zijn niet aan de orde. Volgens Dentons is het hoogst onwaarschijnlijk dat Amerikaanse opsporingsdiensten ooit gegevens zullen komen opvragen. Er zouden hooguit wat organisatorische zaken geregeld dienen te worden, geen technische. Desondanks wil men zodra dat mogelijk is wel voor alle zekerheid extra technische maatregelen treffen, die niet in de DTIA als zodanig geadviseerd worden maar die we als comfortmaatregelen willen introduceren. Voorbeelden zijn het volledig in eigen beheer houden van de encryptie en encryptiesleutels, zodat niemand anders meer toegang kan krijgen tot de data, ook Microsoft zelf niet. De Azure-producten van Microsoft zijn bovendien aan een hele reeks interne regels gebonden en worden daar regelmatig op getoetst op onder andere verschillende ISO standaarden (certificeringen) er zijn jaarlijkse ISAE verklaringen beschikbaar. De lead krijgt daar de onderzoeksresultaten van, zodat hij de vinger aan de pols kan houden. De kans dat iemand dan toch nog toegang weet te krijgen tot de data is puur theoretisch. De datacentra zijn zo groot dat alles daar geautomatiseerd moet gebeuren en niemand precies kan weten waar bepaalde data te vinden zijn.

De CPA merkt op dat er volgens het document wel voor verschillende services gegevens – bijvoorbeeld telemetrische – naar Amerika zullen worden verstuurd. Daarbij valt het op dat daar wel het belang van Microsoft wordt vermeld, maar niet wat die dienst betekent voor Amsterdam.

Er zijn verschillende datatypen. De specifieke data van de organisatie worden locatiegebonden opgeslagen in de drie datacentra in Nederland. Daarnaast zijn er metadata ten behoeve van telemetrie en diagnostiek en daarvan kan inderdaad een deel gaan naar specialistische servicecentra in Amerika voor analyses. Het kan zijn omdat men die analysecapaciteit nog niet wereldwijd beschikbaar heeft en dat die expertise later alsnog naar Europa uitgerold wordt. Het kan bijvoorbeeld gaan om het opsporen van wereldwijde patronen van DDoS-aanvallen. Langs die weg kunnen anti-DDoS maatregelen tot stand komen waar ook Amsterdam baat bij heeft. Het gaat dus om verbetering van de dienstverlening en beveiliging van de infrastructuur. Per service is verder vastgelegd welke data eventueel buiten de EER mogen komen. Bijzondere gegevens zitten in een kluis waar Microsoft niet bij kan komen.
Bovendien heeft Microsoft recent laten weten de iets te gaan doen aan de databoundary in reactie op de kritische geluiden vanuit Europa. Verder heeft men een nieuwe bundel aan maatregelen aangekondigd rond security en privacy waar Amsterdam een voorlopersrol in zal krijgen.

De CPA vraagt of het beleid een voorkeur uitspreekt voor SAAS en hoe men dan omgaat met wensen uit de business voor specifieke applicaties die niet als SAAS beschikbaar zijn.

Het is inderdaad het beleid dat men allereerst de markt goed moet verkennen op geschikte SAAS-applicaties. Alleen als men overduidelijk kan aantonen dat er geen geschikte beschikbaar is, kan er gekeken worden naar de ontwikkeling van een eigen specifieke applicatie. Voorwaarde is dan wel dat men eerst ook bij andere directies

verkend of die ook met een vergelijkbare applicatie willen gaan werken. Men wil voorkomen dat directies ieder op zich vergelijkbare applicaties gaan ontwikkelen zoals voorheen vaak gebeurd is. Het is ook de bedoeling alle oude systemen, zoals het eigen datacentrum, te ontmantelen om te komen tot een coherent geheel.

De CPA is benieuwd welke gedachten er leven rond de exit-strategie.

In deze constructie kan men altijd bij alle data komen. Door de platformconstructie blijft het ook mogelijk alles over te hevelen naar een ander platform, bijvoorbeeld Amazon. Een dergelijke overstap levert wel veel hoofdpijn op, maar is in principe mogelijk. Hoewel het onmogelijk is om op voorhand te garanderen dat vendor lock-in 100% te vermijden is, lijkt het AWS en Azure aanbod op dit moment voldoende op elkaar om bij andere Cloud Service Parties een variant op de bestaande component / functionaliteit te vinden. Als een bepaalde applicatie niet uit de voeten kan met Azure, kan men daar een andere oplossing voor vinden. In de praktijk blijkt dat Microsoft veel applicaties opkoopt om die dan te voorzien van een eigen voor Azure geschikt sausje. Bovendien blijkt men ook veel met open-source elementen te werken.

De CPA bedankt voor alle toelichtingen. Voor het advies zullen de beschikbare documenten nog eens goed nagelopen worden door de leden met specialistische kennis en die houden zich aanbevolen voor eventuele aanvullende informatie.

Commissie Persoonsgegevens Amsterdam
Uittreksel van het verslag van het openbare agendapunt van de vergadering op donderdag 3 maart 2022

6. Cloud Voorziening gemeente Amsterdam (Directie stadsdelen en stadsbeheer)

In het traditionele model houdt een organisatie – in dit geval de gemeente – alle informatie, servers en computers binnenshuis. De organisatie is dan ook zelf volledig verantwoordelijk voor het beheer, op peil houden en onderhoud van alle apparatuur en software. Amsterdam is kwetsbaar gebleken, met name als het gaat om het tijdig voorzien van alle apparatuur van de nodige patches om software bij de tijd te houden. En dat maakt de organisatie extra kwetsbaar voor cyberaanvallen, die zich in de praktijk vrijwel altijd met succes richten op organisaties met achterhaalde software.
In de nieuwe situatie verandert er weinig in het opdrachtgeverschap voor applicaties. Dat blijft bij de afzonderlijke diensten die daar gebruik van gaan maken. Het grote verschil zit hem in de inzet van de ICT-diensten. Via scripting en dergelijke wordt er veel meer geautomatiseerd en verwerkt in generieke bouwstenen waarmee de DevOps-teams de afzonderlijke werkelijke applicaties configureren waar de gebruikers mee aan de slag kunnen. Daardoor kan de ICT-capaciteit van de organisatie veel efficiënter en zichtbaarder voor de business worden ingezet. Er is het Cloud Competence Centre geformeerd waar de nodige controles worden uitgevoerd voordat de gebruikers met de applicaties aan de slag mogen gaan. Op die manier worden de kaders voor privacy-by-design ook geborgd in het ontwikkelproces.
Voorheen moest een gebruiker eerst bij een server inloggen om bij een databestand te komen. In de nieuwe situatie zit alles op het Azure-portal waar de database direct beschikbaar is voor geautoriseerde medewerkers.
De DevOps-teams voeren de DPIA's en risicoanalyses uit die specifiek zijn voor de betreffende applicatie en business. Door de security tribe wordt gecontroleerd of de afgesproken privacy security frames inderdaad zijn toegepast en wat de resultaten zijn van de DPIA en andere risicoanalyses. Dat gebeurt als een applicatie aangemeld wordt voor toegang tot de Cloud. Voor de toegang tot de Cloud zelf worden afzonderlijke DPIA's en controles op de verwerking van persoonsgegevens (van medewerkers). CCC is daardoor op de hoogte van alle uitgevoerde DPIA's.
In Amsterdam is gekozen voor de PaaS-strategie. Dat staat voor ***Platform as a service***, een type aanbod dat applicatie infrastructuur (middleware) platformen als een service levert. Dat heeft als voordeel dat veel taken en verantwoordelijkheden komen te liggen bij de Cloud serviceprovider, in casu dus Microsoft. Het past naar men zegt het best bij een organisatie van deze omvang, terwijl de gemeente gevrijwaard wordt van alle tijdrovende beheertaken. Azure- Microsoft beheert de databestanden, maar de inrichting en invulling blijft aan de gemeente, net als de sleutels. IaaS geeft iets meer flexibiliteit, maar mist die kant van structuur en beheer.
Anders dan bij SaaS (software as a service) waarin de provider volledig eigenaar is van de software, kan de opdrachtgever in dit model zelf veel meer bepalen. CCC kan bij PaaS bijvoorbeeld gericht kijken welke maatregelen nodig zijn om gegevens te beschermen. CCC kan zelf zorgen voor versleuteling van data en de sleutel volledig in eigen beheer houden zodat de provider daar nooit toegang toe kan krijgen.

De CPA is benieuwd naar het ook toegezonden model van een mini-DPIA en naar een mogelijke relatie met het eerder deze vergadering aan de CPA gepresenteerd IRPA van de VNG. Ook wil de CPA een nadere duiding van het verschil tussen de eigen DPIA's van de CCC en die van de business.

Het blijkt te gaan om een eigen model dat is ontwikkeld als een *QuickScan* om in korte tijd zicht te krijgen op de meest voorkomende risico's. Men ziet wel enige snijvlakken met IRPA.
Er is de beheerkant van het platform waarin persoonsgegevens van voornamelijk medewerkers omgaan. Aan de andere kant bouwen de DevOps-teams applicaties voor het business-proces en de opdrachtgevers hebben de eigen verantwoordelijkheid om daar een DPIA op te laten uitvoeren. Die moet men in de toekomstige situatie ook gewoon blijven uitvoeren, net als een BIO-QuickScan. Daar wordt bij CCC ook uitdrukkelijk naar gevraagd bij de aanmelding van een applicatie. Daar moet men ook de te nemen maatregelen aangeven.
Een geval apart zijn standaardprogramma's als Office 365. Daarin zit standaard bijvoorbeeld een spellingcontrole. Men zal aparte maatregelen moeten treffen om te voorkomen dat via die weg persoonsgegevens kunnen uitlekken.

De CPA is benieuwd hoe het staat met dit soort ontwikkelingen in andere gemeenten.

Bij CCC is bekend dat Den Haag ook in deze richting beweegt.

De CPA is benieuwd of er bij dit soort contracten ook gekeken wordt naar aspecten van duurzaamheid, bijvoorbeeld als het gaat over het stroomgebruik van datacentra.

CCC wijst erop dat Microsoft is gecertificeerd als het gaat om het gebruik van Groene Stroom.

De CPA is benieuwd wat er geregeld is voor het geval er iets misgaat met Microsoft of als er een conflict ontstaat. Is er dan een exit-strategie afgesproken of wordt er ergens een externe back-up gemaakt die onafhankelijk van Microsoft te gebruiken is? Anders gezegd: maakt de gemeente zich niet te afhankelijk van een aanbieder.

Binnen Azure zelf heeft Microsoft voorzien in een systeem van replicatie zodat de klant er niets van merkt als onverhoopt een server of een heel datacentrum uit zou vallen. In het contract met Microsoft zouden ook exit-afspraken zijn opgenomen, maar die kan men ter plekke niet aanwijzen. Bij een echte ramp heeft Microsoft via Disaster Recovery de mogelijkheid uit te wijken naar een andere regio in Europa om daar de zaken op te pakken en te herstellen. De service level agreements (SLA's) van Microsoft zij dusdanig hoog dat men alleen bij contractuele of wettelijke obstakels het contract zou kunnen opzeggen en gebruik moet gaan maken van de exit-afspraken. Andere aanbieders hebben lagere standaarden en om een externe back-up te maken heeft ook veel haken en ogen. De kwestie van afhankelijkheid zou bij alle aanbieders spelen en men moet niet uit het oog verliezen dat de hele operatie juist bedoeld was om zaken te

centraliseren en verdere fragmentatie te voorkomen. Bij CCC zal men zich nader beraden en goed uitzoeken welke exit-afspraken er gemaakt zijn.

De voorzitter werpt het idee op te kiezen voor een centraal systeem, maar voor de back-up dan één externe partner in de arm te nemen, juist vanuit het oogpunt van risicobeheersing. Zij bedankt voor de toelichtingen en zegt dat de CPA het vertrouwelijke karakter van de bespreking zal respecteren en verder met belangstelling de ontwikkelingen zal volgen. Zij vraagt de commissie op de hoogte te houden.