Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam
Commissie Persoonsgegevens

Afdeling OJZ, mw. 5.1, 2, e
Kopie: mw. 5.1, 2, e de heer mr. 5.1, 5.1, 2, e
de heer 5.1, 5.1, 2, e
Afdeling OOV, mw. 5.1, 2, e 5.1, 2, e
IVE Stadsdelen, de heer 5.1, 2, e mw. 5.1, 5.1, 2, e
GGD, de heer 5.1, 2, e
Kopie: CIO, J. Flippo
Kopie: Stedelijk Directeur Sociaal, de heer E. ten Hulsen

Datum	7 mei 2015
Ons kenmerk	U150051
Behandeld door	Mw. 5.1, 2, e ., 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, mevrouw,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 16 april jl. was aanwezig: namens Sociaal, mw. 5.1, 5.1, 2, e hoofd Afdeling Jeugd, de heer L. 5.1, 2, e projectleider RIS Wijkzorg, Afdeling OJZ, en de heer 5.1, 5.1, 2, e cluster informatiebeveiliger en privacy coördinator OJZ en namens Bestuur en Organisatie, mw. 5.1, 2, e 5.1, 2, e Treiteraanpak, OOV. Namens de Stadsdelen was aanwezig mw. 5.1, 5.1, 2, e informatiebeveiliging en privacy coördinator.
Bij het agendapunt "Rapport RIS" heeft de CPA het navolgende besproken.

Bij registraties van persoonsgegevens in RIS betreft het verwerkingen op grond van verscheidene afspraken in Convenanten en in verschillende modules. Er is daarom geen sprake van één verwerking in RIS. Het gaat om verschillende verwerkingen en om verschillende systemen.

Er is verscheidenheid in de afspraken met de bewerker Inforing. Onderzocht dient te worden of deze verscheidenheid een reden heeft die gelegen is in de betreffende aanpak of Convenantafspraken of dat verschillen onwenselijk zijn.
De CPA beveelt aan om ook de aanpak neergelegd in de onderliggende Convenanten opnieuw te beoordelen om te bezien of de verwerkingsgrondslagen en doeleinden juist zijn en of meer uniformiteit in afspraken kan worden bewerkstelligd.

De CPA neemt de vijf bevindingen van het rapport van de ACAM over. Dit betekent -kort samengevat- dat:
Ad 1. De vraag van belang is of diversiteit in afspraken ter zake van de inrichting en beveiliging van de modules wenselijk of juist onwenselijk zijn.
Ad 2. Er moet centrale aansturing zijn op de afspraken met Inforing ten aanzien van RIS.
Ad 3. Expliciet moet zijn of een koppeling van de modules onwenselijk is en in welke gevallen dit functioneel en noodzakelijk kan zijn en op basis van welke wettelijke grondslagen persoonsgegevens dan gedeeld mogen worden.
Ad 4. Het is wenselijk om altijd het proceseigenaarschap te bepalen.
Ad 5. Het zogenoemde ´hoofdcontract´ met RIS zou alle modules moeten betreffen c.q. expliciete bewerkersafspraken met Inforing zouden voor alle modules moeten gelden.

De CPA signaleert dat het voornaamste risico is gelegen in het gegeven dat de gemeente Amsterdam voor belangrijke verwerkingen van bijzondere persoonsgegevens in het Sociaal Domein, maar hiertoe niet beperkt, steunt op een relatief kleine leverancier. Het is wenselijk om bewerkersafspraken te maken waarbij maatregelen ter zake van continuïteit, zoals een calamiteitenplan, worden betrokken. Afspraken kunnen het risico matigen, echter nemen dit niet weg.

De CPA signaleert dat de leverancier vanuit ´role bases access´-modellen en beveiligingsstandaarden zoals de ISO-normering, geen toegang tot de persoonsgegevens en dus tot de inhoudelijke informatie in de modules zou mogen hebben. Ook dit is een significant risico dat gezien de omvang en de gevoeligheid van de gegevensverwerkingen in RIS, aanzienlijk is te noemen. `Privacy by design´ heeft de voorkeur boven het nemen van uitsluitend risico-beperkende afspraken zoals het tekenen van geheimhoudingsverklaringen.

De CPA adviseert om zo spoedig mogelijk te voorzien de in de gesignaleerde verbeterpunten. Toegezegd is dat de bewerkersovereenkomst voor alle te onderscheiden modules is getekend voor het derde kwartaal en dat ook ten aanzien van het proceseigenaarschap en de regie tegen deze termijn expliciet afspraken zijn gemaakt, zodat de regie op beheerafspraken in één hand is.

Bijgaand treft u het deel van de notulen van de vergadering aan over het betreffende agendapunt.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Hoogachtend,

5.1, 2, e

Drs. W.L. Posthumus
Voorzitter Commissie Persoonsgegevens Amsterdam

Commissie Persoonsgegevens Amsterdam
Uittreksel van het concept verslag van de openbare vergadering op donderdag 16 april 2015

6. Rapport RIS (ACAM , RVE OJZ, BDA, Stadsdelen)
Namens de gemeente Amsterdam zijn aanwezig: mw. 5.1, 2, e hoofd afdeling Jeugd, de heer 5.1, 2, e projectleider RIS Wijkzorg, Afdeling Onderwijs, Jeugd en Zorg en mw. 5.1, 2, e jurist bij Openbare Orde en Veiligheid voor de Treiteraanpak in verband met RIS TRAP.

De CPA zegt dat RIS vaak wordt genoemd in verscheidene contexten. Om deze reden heeft de CPA opdracht gegeven voor onafhankelijk onderzoek: wat is RIS, door wie wordt RIS gebruikt en waarvoor en met welk doel, hoe is RIS beveiligd en wie beheert het.
Een van de in het oog springende punten is dat niet over RIS als zodanig gesproken kan worden, het gaat om de te onderscheiden verwerkingen ín RIS. Het gaat daarnaast om gescheiden modules en dus verschillende systemen.
Achter de verschillende registraties ligt een andere Convenantaanpak ten grondslag. Het is goed om deze Convenanten afzonderlijk te beoordelen.

ACAM heeft in het rapport een vijftal bevindingen genoteerd.
Bevinding 1: diversiteit kan goed zijn, immers een verwerking kan gezien de wettelijke grondslagen en het doel verschillen van een andere verwerking. Het is zaak om naar de aard van de diversiteit te kijken om te beoordelen of dit passend is bij de afspraken of dat er geen goede reden voor is.

Een van de belangrijkste risico's van de verwerkingen in RIS is dat de gemeente afhankelijk is van de samenwerking met een kleine partij. Dit geeft risico's op het gebied van continuïteit. Voor zeer belangrijke verwerkingen wordt op een relatief kleine leverancier gesteund. Maatregelen kunnen het risico wel tot op zekere hoogte beperken. De vraag of de gegevensverwerking voor het Sociaal Domein niet meer beschikbaar is als de software van Inforing 'uit de lucht is', is een essentieel punt.
Het is van belang dat er een calamiteitenplan komt.

De heer 5.1, 2, e merkt op dat gewerkt wordt aan afspraken over een uitwijkregeling en een Escrow-regeling om de risico's te mitigeren. Het is de bedoeling om de verwerkingen in RIS voor het Sociaal Domein in deze hoofdovereenkomst te betrekken, maar niet uitgesloten is dat andere verwerkingen in RIS, zoals RIS TRAP (Treiteraanpak) ook worden betrokken in de afspraken. Er zijn echter meerdere proceseigenaren.

De heer 5.1, 2, e merkt op dat op korte termijn overleg plaats vindt met de CISO en de privacy- en informatiebeveiligers van de Clusters om te spreken over het proceseigenaarschap van de meldpunten Zorg en Samenleven en Zorg en Overlast. Voorgelegd zal worden om het proceseigenaarschap van een aantal modules nu ook bij het

cluster Sociaal onder te brengen zodat de regie op RIS in één hand is. De afspraken met Inforing zijn nu nog versnipperd. Het in een hand brengen van het proceseigenaarschap sluit aan bij het adagium 1-stad 1 opgave.

De CPA zegt dat met Inforing op het gebied van technische beveiliging afspraken zijn gemaakt. Het is van belang dat de regie op de afspraken in een hand komt. Echter ook als alles goed is afgedicht qua risico's blijft het risico van de bewerker als relatief kleine partij overeind staan.

Mw 5.1, 2, e zegt dat het van belang was om het stof van de decentralisaties te laten neerdalen. De gemeente en de aanbieders van zorg hebben hard gewerkt om het nieuwe stelsel vorm te geven. Nu is besluitvorming in voorbereiding over een vervangend systeem. Nu zijn er verschillende applicaties in werking.

De CPA vraagt onder wiens verantwoordelijkheid dit plaatsvindt.

Mw. 5.1, 2, e zegt dat de stedelijk directeur van Cluster Sociaal hiervoor verantwoordelijk is, de heer ten Hulsen. De Stadsdelen worden betrokken in het traject en in het vooronderzoek wordt breder onderzoek gedaan dan uitsluitend naar de drie decentralisaties. Maar het vooronderzoek gaat uit van de drie decentralisaties.

De CPA vraagt of de Afdeling ICT ook betrokken is.

Mw. 5.1, 2, e zegt dat de Afdeling ICT nauw betrokken is.

De CPA zegt dat informatiebeveiligingsrisico's onderdeel zijn van privacyrisico's. De autorisatiesystematiek is essentieel. Wat in het oog springt is dat RIS op kleine schaal is gestart en dat vanuit dit vertrekpunt het systeem nu op veel grotere schaal wordt gebruikt. Bij een nieuw systeem moeten inrichtingsvraagstukken van begin af aan worden betrokken. Van belang is om niet alleen op het niveau van een specifieke applicatie functionele eisen te formuleren, maar dat ook de samenhang met andere applicaties en dat dus het systeem als geheel wordt beoordeeld.
Een van de zaken die op viel was dat Inforing altijd toegang heeft. Vanuit role based acces modellen zou Inforing niet bij inhoudelijke informatie moeten kunnen. De ISO-normering voorziet daarnaast in functiescheiding. De software installatie hoort gescheiden te zijn van de content. Ook de ontwikkel-,test- en productieomgeving dient te zijn gescheiden. Inforing is softwareleverancier en zou in de testomgeving moeten kunnen testen. Zeer belangrijk is bij dossiersystemen dat de leverancier niet bij de inhoud kan.

De heer 5.1, 2, e zegt dat een bewerkersovereenkomst wordt gesloten met Inforing en dat geheimhouding is opgelegd.

De CPA zegt dat het risico per applicatie misschien lijkt mee te vallen. Maar als de gegevensverzameling in het geheel wordt beschouwd, is het risico onaanvaardbaar groot. Een aanzienlijk deel van de populatie van Amsterdam komt in RIS voor. Maatregelen als een

geheimhoudingsplicht en bewerkersafspraken zijn goed en moeten ook, maar hiermee voorkom je niet dat iemand in de verleiding komt. Privacy by design is beter.

Mw. 5.1, 2, e zegt dat niet de gehele jeugdadministratie in RIS staat, maar in KIDOS. Niet elke Amsterdammer komt voor in het systeem. Dat maakt de verzameling iets minder groot.

De CPA zegt dat een beoordeling van de onderliggende Convenanten ook van groot belang is. Het is de vraag of de verschillen in de aanpak te motiveren zijn vanuit de grondslagen en doeleinden, of dat deze niet terecht zijn. Het is daarbij niet nodig om helemaal opnieuw te beginnen met een aanpak, er is een opzet aanwezig. Van belang is om een gelijke opbouw en opzet te volgen.

De CPA noemt de bevindingen van de ACAM op pagina 5 van het rapport.
Ad 1. diversiteit kan dus goed zijn, maar ook kan het onwenselijk zijn: dit moet worden beoordeeld.
Ad 2. van groot belang is dat er centrale aansturing komt op het geheel aan afspraken over RIS.
Ad 3. op zich is het goed dat de modules niet gekoppeld zijn uit een oogpunt van informatiebeveiliging en het in acht nemen van geheimhoudingsplichten. Soms kan het echter ook niet functioneel zijn. Het is goed om dit expliciet te beoordelen en nader te bekijken.
Ad 4. het proceseigenaarschap van het loket Zorg en Samenleven is niet bepaald.
ACAM licht toe dat voormalig Dienst Wonen Zorg en Samenleven 'eigenaar' was van het systeem. De afspraken stammen uit die tijd.
Ad 5. De CPA vraagt of het klopt dat het hoofdcontract met Inforing uitsluitend over de modules voor het Sociaal Domein gaat.

De heer 5.1, 2, e zegt dat een DAP is afgesloten voor de modules van het Sociaal Domein en dat deze nog niet van toepassing is op andere modules.

Mw. 5.1, 2, e zegt dat RIS TRAP zich bij de afspraken zal aansluiten.

Mw. 5.1, 2, e zegt dat het vanuit het leveranciersmanagement goed zou zijn om de regie op afspraken eenduidig te beleggen.

De CPA zegt dat er sprake zou moeten zijn van een centraal aanspreekpunt.
De CPA waarschuwt daarnaast dat de systemen operationeel zijn. Tijdens de implementatie van afspraken over het verbeteren van het beheer is ' de winkel open'.

De heer 5.1, 2, e zegt dat reeds goede maatregelen zijn getroffen en dat daartoe ook vorig jaar een risicoanalyse is gedaan die in juli 2014 is behandeld.

Mw. 5.1, 2, e zegt toe dat voor de zomer de modules zijn ondergebracht bij Cluster Sociaal en dat er dan sprake is van een getekende hoofdovereenkomst met bewerkersafspraken voor alle modules.

De CPA stelt deze toezegging op prijs. Het rapport is zeer verhelderend. De CPA wacht gezien deze toezegging af of er voor de zomer zichtbare resultaten zijn in het beheer, in getroffen maatregelen en het beheersen van de risico's. De CPA herhaalt dat Inforing te veel 'kan' en dat een calamiteitenvoorziening essentieel is. De CPA wordt graag geïnformeerd over de voortgang.

De ACAM bevestigt dat er aandacht is vanuit de verscheidene aanpakken voor het adagium ' gij zult niet combineren' .