Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam
Commissie Persoonsgegevens

Afdeling OJZ
Tav mw. 5.1, 2, e en mw. 5.15.1, 2, e
Kopie: de heer 5.15.1, 2, e
mw. 5.15.1, 2, e de heer 5.1, 5.1, 2, e
Kopie: ClO, J. Flippo
Kopie: Stedelijk Directeur Sociaal, de heer E. Ten Hulsen

Datum	18 juni 2015
Ons kenmerk	U150071
Behandeld door	Mw. 5.1, 2, e ., 25.1, 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 28 mei jl. was namens de Afdeling Basisinformatie de heer 5.15.1, 2, e aanwezig. Bij het agendapunt "Regioportaal" heeft de CPA het navolgende besproken.

De CPA heeft kennis genomen van de brieven van het CBP d.d. 16 maart 2015 inzake beroepsgeheim en declaraties Jeugd GGZ en de brief d.d. 13 mei 2015 inzake doorbreking geheimhoudingsplicht Jeugdwet. De CPA neemt geen standpunt in over het meningsverschil tussen het CBP en het ministerie van VWS over de wettelijke basis in de Veegwet voor de doorbreking van de geheimhoudingplicht van zorgaanbieders in de jeugd GGZ en het verstrekken van persoonsgegevens van cliënten aan gemeenten ten behoeve van de financiële afwikkeling van zorg.

Het CBP is de landelijke toezichthouder en de CPA wijst er op dat de gemeente Amsterdam kan worden aangeschreven, wegens afwezigheid van een wettelijke grondslag voor (en daarmee: onrechtmatigheid van) de gegevensverwerking. Een alternatief is dat zorgaanbieders hun cliënten vragen om toestemming en hun daarbij helder en duidelijk van informatie voorzien.

Door de heer 5.1, 2, e is betoogd dat scenario's zijn besproken met de wethouder Jeugd, mw. Kukenheim. Gekozen lijkt te gaan worden voor een scenario dat ten doel heeft het voorkomen van onzekerheid, vertragingen en extra kosten en gericht is op continuïteit van

zorg. Dit zou tot gevolg hebben dat het voorgenomen gegevensverwerkingsproces ten behoeve van het betalen van zorgaanbieders ongewijzigd doorgang vindt. De gegevensverwerking heeft betrekking op het Regioportaal en ook op de huidige beschikkingenadministratie in WMO-Ned Jeugd. Van dit standpunt heeft de CPA kennisgenomen.

Op de volgende punten van zorg zal de CPA wel expliciet ingaan.

Van belang is dat het Regioportaal veilig kan worden benaderd en dat de uitkomst van de verplichte penetration- and hack-test dit uitwijst. Eventuele aandachtspunten worden in de eerstvolgende vergadering besproken.

Het Regioportaal kan niet worden beoordeeld op privacyrisico's zonder documentatie. De CPA vraagt naar de verplichte risicoanalyse van de beveiliging en een privacy impact assessment. Ook wordt gevraagd naar een afschrift van de bewerkersovereenkomst tussen de bewerker en de gemeente Amsterdam. Afgesproken is dat deze documentatie op de eerstvolgende vergadering wordt geagendeerd. In het 'Bestuurlijk Handboek Regioportaal' zouden daarnaast een kadernota en beheer- en gebruikersafspraken worden vastgelegd. De CPA verzoekt om de melding van het gegevensverwerkingsproces voor het Regioportaal te verduidelijken en daarin uitgebreider te beschrijven wat de doeleinden van de verwerking zijn en wat de dataset is. Alleen het noemen van de werkprocessen, zoals 'onder handen werk', zegt een buitenstaander (te) weinig.

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 28 mei 2015

7. Regioportaal (RVE OJZ)
De CPA zegt dat het Regioportaal in maart op de vergadering van de CPA was geagendeerd. Er is toen een schets van het nieuwe systeem gepresenteerd door de heer 5.1, 2, e De CPA heeft nog geen inhoudelijk advies uitgebracht. Daarom is het Regioportaal opnieuw geagendeerd.

De heer 5.1, 2, e heeft een concept-melding aan het CBP opgesteld. Deze melding is inmiddels aangevuld. Hij maakt namens mw. 5.1, 2, e het hoofd Jeugd, een compliment aan de CPA. Naar aanleiding van de adviezen van april 2015 is onlangs een versie van het privacyprotocol voor de Jeugdhulp door 20 Instellingen besproken en goedgekeurd. De sector is hier erg blij mee.

Ten aanzien van de stellingname van het CBP over de doorbreking van de geheimhoudingplicht door jeugdhulpaanbieders, merkt de heer 5.1, 2, e op dat het ministerie van VWS het niet eens is met de stelling van het CBP dat de Veegwet niet in een reparatie voorziet. Hij verwijst naar een recente brief van het CBP van 13 mei jl. met deze inhoud. Op dit moment is er een patstelling, waarvan de gemeente vreest dat dit de facturatie en betaling van de zorg en de continuïteit van de zorg ernstig bedreigt. De patstelling gooit roet in het eten en zou het primaire proces ernstig kunnen dwarsbomen. Zo zou de gemeente uitsluitend voorschotten kunnen betalen aan jeugdhulpaanbieders tot dat de leemte in de wetgeving is gerepareerd en definitieve vaststelling van de verschuldigde bedragen kan plaatsvinden.

De inhoud van de discussie is niet gericht op de vraag of de gemeenten de persoonsgegevens van de jeugdhulp cliënten zouden mogen verwerken, maar betreft een wetgevingsvraagstuk en een theoretische discussie. De dataset die het Regioportaal gebruikt betreft een beperkte set aan persoonsgegevens. De heer 5.1, 2, e verwijst naar de presentatie van 8 maart 2015 voor een opgaaf van de dataset. Overigens zijn de gevolgen breder dan alleen de verwerking van persoonsgegevens via het Regioportaal, maar treft ook de verwerking van facturen in WMO-ned Jeugd, de beschikkingenadministratie.

Overleg heeft plaatsgevonden met wethouder Kukenheim om de situatie te bespreken. Er zijn drie scenario's geschetst. Het eerste scenario is dat de gemeente afwacht en de facturatie en betaling wordt opgeschort. Het tweede scenario is dat de gemeente Amsterdam zonder de betreffende persoonsgegevens overgaat tot uitbetaling door middel van voorschotten en het derde scenario is dat de voorgenomen uitwisseling van persoonsgegevens ten behoeve van de facturatie doorgang vindt. De risico's die met de scenario's gepaard gaan zijn geschetst. Gekozen is voor het derde scenario waarbij de gemeente een pro forma handhaving door het CBP uitlokt. Het primair proces is immers niet gebaat met de kosten en vertragingen die de alternatieven met zich brengen.

De bedoeling van een pro forma handhaving door het CBP is om het ministerie te dwingen tot een stellingname en een eenduidig standpunt. De gemeente neemt hiermee een gecalculeerd risico en voorkomt een bedreiging van de continuïteit van de zorg. De gemeente Amsterdams zal de kwestie vooraf met het CBP afstemmen.

De CPA zegt dat zij het standpunt van het CBP afwacht. De CPA zal geen uitspraak doen hangende deze zaak. Er is wel begrip voor de keuze van de wethouder. In zijn algemeenheid adviseert de CPA altijd om het standpunt van de wetgever te volgen.

De CPA vraagt of het Regioportaal al werkend is en dus 'live' is. De heer 5.1, 2, e zegt dat het Regioportaal nog niet 'live' is. De voortgang van ingebruikname ligt stil in verband met de geschetste situatie. Er wordt wel getest.

De heer 5.1, 2, e zegt dat de applicatie vanaf het web benaderbaar is. Hij dringt namens de CIO aan op een Pen- and Hacktest voor ingebruikname. Dat is staand beleid van de gemeente Amsterdam. Gezien de werking van het Regioportaal worden zonder een dergelijke test onaanvaardbare risico's gelopen. De heer 5.1, 2, e verwijst naar OWASP-criteria en de BIG. Het moet gaan om een derde, onafhankelijk partij, los van de leverancier, die de verplichte test uitvoert.

De heer 5.1, 2, e zegt dat is afgesproken dat uitgenodigd zal worden tot 'Ethical Hacking'. Ook is het Regioportaal werkend in een NEN 7510 gecertificeerde omgeving.

De CPA vraagt de uitkomsten van de verplichte Pen-and Hacktest op. Eventuele aandachtspunten worden in de vergadering besproken. Gevraagd wordt naar de verplichte risicoanalyse van de beveiliging en een privacy impact assessment. Zijn deze analyses al gereed. Ook wordt gevraagd naar de bewerkersovereenkomst, is er één overeenkomst met de leverancier of zijn er 15 bewerkersovereenkomsten.

De heer 5.1, 2, e zegt dat namens de te onderscheiden 15 gemeenten één bewerkersovereenkomst wordt gesloten. Hij verwijst verder naar een zware autorisatieprocedure voor toegang tot de applicatie. Onlangs heeft hij opdracht verstrekt tot een Bestuurlijk Handboek voor het Regioportaal, met de verplichte documentatie, zoals een Kadernota, gebruikersovereenkomsten, beheerovereenkomsten ea. Hij licht toe dat de risicoanalyse op dit moment wordt uitgevoerd. Bij de bouw van het systeem heeft de leverancier het principe 'privacy by design' toegepast.

De CPA zegt dat er sprake is van een omgekeerde volgorde. Eerst behoort een risicoanalyse en PIA te worden verricht voor het bepalen van de functionele eisen, daarna wordt opdracht gegeven voor het leveren van een systeem, en wordt vervolgens getest of het aan de functionele eisen voldoet. Nu gebeurt deze exercitie achteraf, waardoor het kan zijn dat maatregelen achteraf moeten worden bijgesteld.

De heer 5.1, 2, e beschrijft het proces van de totstandkoming van het Regioportaal. Gaandeweg is duidelijk geworden dat door de regionale inkoop en samenhangende processen er sprake was van 'function creep' en is het beveiligingsniveau omhooggeschoten.

De offerte is vervolgens nader uitgewerkt en een 'strenge' leverancier is geselecteerd met het oog op privacybescherming.
Hij zal de set documentatie aanleveren bij de CPA.

De CPA toont begrip voor de tijdsdruk echter benadrukt dat het Regioportaal niet inhoudelijk kan worden beoordeeld op privacyrisico's zonder de benodigde documentatie. Deze wordt de volgende vergadering geagendeerd, zodat de CPA in de beoordeling dan pas de diepte in kan gaan.
Gevraagd wordt om de nut en noodzaak van het systeem aan te tonen en wat de verhouding is van het Regioportaal ten opzichte van de WMO-Ned Jeugd beschikkingenadministratie.

De heer 5.1, 2, e benadrukt dat het Regioportaal essentieel is omdat de inkoop regionaal is georganiseerd.

De heer 5.1, 2, e vraagt naar de afspraken over de verantwoordelijkheid voor de gegevensverwerkingen. In de CBP melding zijn geen afspraken terug te vinden. Waar is dit bepaald?

De heer 5.1, 2, e zegt dat -gezien het meldingsformulier- er sprake is van 15 te onderscheiden verantwoordelijken. Elke regiogemeente is de verantwoordelijke voor de gegevensverwerking van 'eigen' burgers. Er is geen sprake van gezamenlijke verantwoordelijkheid.

De CPA vraagt of het beheer van Regioportaal is belegd. De heer 5.1, 2, e zegt dat de beheerorganisatie wordt belegd en dat dit in het Bestuurlijk Handboek Regioportaal terugkomt in de beheerafspraken.

De CPA dringt aan op spoedige kennisname van de uitslag van de Pen- and Hack test. De melding bij het CBP is te summier. Niet duidelijk is welke persoonsgegevens worden verwerkt: wat wordt bedoeld met 'zorgcategorie'. Hetzelfde geldt voor de doelomschrijving. Alleen het noemen van de werkprocessen, zoals 'onder handen werk', zegt een buitenstaander (te) weinig.

De heer 5.1, 2, e zegt dat hij de opmerkingen in het concept zal verwerken.

De CPA agendeert het Bestuurlijk Handboek Regioportaal en de uitslag van de Pen- and Hack test op de volgende vergadering in juli.