Jeroen van der Ham

[redacted]

College van burgemeester en
wethouders van Utrecht
Postbus 16200
3500 CE Utrecht

Uw kenmerk	Datum
14.039689	7 augustus 2014

Onderwerp: Bezwaarschrift beslissing WOB-verzoek inzake veiligheid DD-JGZ

Geachte college van burgemeester en wethouders Utrecht,

Op 12 maart 2014 heb ik u verzocht om documenten openbaar te maken met betrekking tot de veiligheid van de uitvoering van de (digitalisering van de) dossierplicht voor jeugdgezondheidszorg. Op 21 mei 2014 heeft u op mijn verzoek beslist en een aantal documenten openbaar gemaakt, ik dank u daarvoor hartelijk. Op 1 juli heb ik bezwaar aangetekend tegen uw besluit en toegezegd mijn bezwaar later te motiveren. Deze motivatie treft u hieronder.

U heeft besloten dat de veiligheid van de uitvoering van het DD JGZ aan te merken is als een bestuurlijke aangelegenheid. Daarom heeft u besloten een aantal documenten openbaar te maken, die voldoen aan de opsomming zoals ik die gaf in mijn verzoek van 12 maart. Daarbij heb ik echter de kanttekening gemaakt dat dit een ongelimiteerde opsomming was. In mijn originele verzoek omschreef ik de opsomming met ‘waaronder, maar niet gelimiteerd tot’.

U heeft mij uiteindelijk vijf documenten en gegevens opgeleverd die de veiligheid van de DD JGZ infrastructuur betreffen. Het acht mij zeer onwaarschijnlijk dat een zo belangrijke en omvangrijke taak slechts onderwerp is geweest van vijf verschillende documenten bij de gemeente en de GGD.

Allereerst heeft u naar mijn idee heeft u het begrip ‘beveiliging’ te beperkt opgevat. Het gaat mij om ‘informatiebeveiliging’ zoals die onder andere in de norm NEN 7510 is beschreven. Die norm (en een aantal gerelateerde normen) is ook genoemd in de offerteaanvraag zoals u mij die heeft toegezonden, en moet ook nog steeds van toepassing zijn op de DD JGZ infrastructuur. Volgens de NEN 7510 zouden er een groot aantal documenten moeten zijn die gaan over informatiebeveiliging, zoals de volgende (met een aantal verwijzingen naar desbetreffende secties in NEN 7510):

- Informatiebeveiligingsbeleid document (5.1)
- Beschrijving van het nformatiebeveiligingsproces (6.1.1/6.1.2)
- De resultaten van de uitvoering van een risicoanalyse, resulterend in beveiligingseisen (6.2.2)

- Een informatiebeveiligingsplan met vastgestelde prioriteiten (6)
- Beschrijving van het toegangsbeleid
- Geheimhoudingsovereenkomst afgesloten met werknemers (6.15)
- Business continuity planning (14.1)
- Beschrijving van het beleid voor bescherming van persoonsgegegevens (15.1.4)
- Verantwoordelijken voor de bedrijfsmiddelen (7.1.2)
- Acceptable use policy (7.1.3)
- Beschrijving van backup en restoreprocedures
- Overeenkomsten voor gegevensuitwisseling
- Een procedure voor het melden van beveiligingsincidenten

Bovendien vereist de NEN 7510 norm ook dat er zowel interne als externe audits uitgevoerd worden. In deze audit rapportages wordt de status van bovenstaande documenten beschreven, alsmede de status van de uitvoering daarvan.

Daarnaast heb ik in de documenten die u mij toezond ook een aantal verwijzingen gevonden naar andere documenten die ook te maken zouden moeten hebben met de beveiliging van de DD JGZ infrastructuur. Ik loop hier in volgorde van de documenten zelf doorheen:

- Een belangrijke taak van jeugdgezondheidszorg is dat er data gedeeld wordt voor wetenschappelijke doeleinden. Dit is ook zo omschreven in de offerte. Het is zeer waarschijnlijk dat er ooit in de bestaansperiode van het DD-JGZ uitwisseling voor wetenschappelijk onderzoek is geweest. (Offerte (m)i-e-7)
- “Leverancier levert maandelijks schriftelijke documentatie over de werking ... en de beveiliging ervan in het bijzonder.” (Offerte kt-e-8)
- “Leverancier dient op verzoek aan te kunnen tonen hoe de beveiliging is geregeld.” (Offerte kt-e-10) Het is aannemelijk dat de gemeente gevraagd heeft om dit soort rapportages, dus dit soort documenten zouden er moeten zijn.
- “Alle datacommunicatie zal versleuteld plaatsvinden.” (Offerte kte-8) Het is aannemelijk dat de leverancier omschrijft hoe die data dan ook daadwerkelijk versleuteld (en ontsleuteld) wordt, zodat aan de offerte wordt voldaan. Het openbaar zijn van de werking hiervan zou de veiligheid van dit systeem niet moeten schaden, zie ook het principe van Kerckhoffs[1].
- “Het systeem moet een logboek bijhouden met informatie wie en wanneer toegang (inzage en mutaties) heeft gehad tot welk onderdeel (planning, dossier en (management)informatie) van het EKD-JGZ.” (Offerte ab-e-14) Dit was onderdeel van een van mijn vragen.
- “De leverancier stelt een overzicht van known bugs beschikbaar.” (Offerte l-e-20) Het is zeer onwaarschijnlijk dat de leverancier direct een systeem heeft opgeleverd zonder bugs, dus het is aannemelijk dat zo’n overzicht bestaat, danwel heeft bestaan.

1. http://nl.wikipedia.org/wiki/Principe_van_Kerckhoffs

- "Er dient een meldpunt zijn ingericht voor het melden van storingen." (Offerte sla-e-12) Het is aannemelijk dat er bij dit meldpunt een overzicht bestaat van meldingen. Het is ook zeer waarschijnlijk dat die meldingen op de een of andere manier een impact hebben gehad op de informatiebeveiliging. Verder is het aannemelijk dat er documentatie is over de inrichting van dit meldpunt.
- "Alle (fout)meldingen (bekende problemen) dienen te worden opgenomen in een log- bestand dat beschikbaar wordt gesteld aan het incidentbeheer." (Offerte sla-e-16) Dit logbestand bevat allerlei problemen die te maken hebben met beveiliging. Het is zeer aannemelijk dat er van dit soort (fout)meldingen zijn geweest.
- Het Privacyprotocol GG&GD Utrecht op pagina 13 verwijst naar 'Beveiligingsplan GG&GD Utrecht, managementsamenvatting, augustus 2002.'. Dit documenten (en mogelijke vernieuwde versies) heb ik niet van u ontvangen.
- U heeft mij een concept begrotingsvoorstel uit mei 2014 gestuurd. Het is aannemelijk dat er ook definitieve begrotingen zijn van eerdere jaren. Graag ontvang ik van u nog in ieder geval die van de periode 2011 - 2013.

Uit bovenstaande blijkt dat er helaas nog vele documenten moeten bestaan die te maken hebben met de beveiliging van de infrastructuur van het DD JGZ. Het is duidelijk dat de gemeente onzorgvuldig is geweest in de beantwoording van mijn verzoek tot dusver. Ik verzoek u dringend or een nieuwe inventarisatie te maken, op basis van bovenstaande gegevens, en met een niet-gelimiteerde uitleg van mijn opsomming zoals omschreven in mijn originele verzoek. Daarom verzoek ik u om de beoordeling te herzien en een nieuwe beslissing te nemen.

Ik zou graag zien dat u de betreffende documenten alsnog openbaar maakt, danwel de weigering hiervan te motiveren. Zoals ik al eerder aangaf ontvang ik die documenten liefst zoveel mogelijk digitaal. Tevens wil ik nogmaals benadrukken dat ik opensta voor toelichting en overleg over mijn verzoek, u kunt mij bereiken via email [redacted]) of via telefoon ([redacted]).

[redacted]

Jeroen van der Ham.

[redacted]