**Antwoorden VWS dd 10/8 op vragen Raad van State dd 29/7**

Beste (10)(2e) en (10)(2e)
Vanochtend heb ik telefonisch gesproken met (10)(2e) over het wetsvoorstel Coronamelder. Ik besprak met haar dat wij nav het voorstel een aantal vragen hebben. Ik heb toegezegd de vragen ook op de mail te zetten, zodat (10)(2e) deze na terugkomst kan beantwoorden. Ik zet mijn collega (10)(2e) ook in de cc. Zij werkt de zomer door aan het wetsvoorstel, ik ben vanaf volgende week drie weken met verlof.

Het gaat om het volgende:

1) **a. De regeling ten aanzien van de rechten van betrokkenen. In de PIA wordt verwezen naar de uitzonderingsmogelijkheid van artikel 11 in geval van gepseudonimiseerde gegevens. In het voorstel is ervoor gekozen om de GGD van de verblijfplaats van betrokkene aan te wijzen als verwerkingsverantwoordelijke voor de uitoefening van de rechten van betrokkene. Waarom is daarvoor gekozen?**
**b. Zou een mandaatconstructie/verwerkersovereenkomst nog een optie zijn geweest?**
**c. Past het ook bij de gegevensverwerkingen die in de verschillende fasen plaatsvinden (zie PIA)?**
**d. Daarnaast is de vraag hoe het feitelijk uitpakt. Kan de plaatselijke GGD feitelijk inderdaad bij de informatie over de gegevensverwerkingen van betrokkene?**
**e. Een deel van de gegevensverwerking vindt bij de plaatselijke GGD plaats (ihb bijzondere persoonsgegevens), maar een deel ook op via de (landelijke) back-end-server?**
**f. Ligt voor zover het gegevensverwerking via de back-end-server betreft niet een gezamenlijke verantwoordelijkheid van de GGD'en meer voor de hand?**

*Antwoord a en b en f*
*We hebben overwogen de verwerkingsverantwoordelijkheid bij één partij te houden, ofwel uitsluitend bij de minister, ofwel uitsluitend bij de gezamenlijke GGD'n. We kwamen erop uit dat een dergelijke constructie niet aansluit bij (1) de praktijk, namelijk bij de ontwikkeling (minister) en inzet van de app bij het bron- en contactonderzoek door de GGD'n én (2) zich niet goed verdraagt met privacyoverwegingen/gegevensbescherming/ dataminimalisatie.*

*De minister van VWS heeft de ontwikkeling (en het tzt het beheer) van de app op zich genomen vanwege zijn taken op grond van de artikelen 3 en 7 van de Wpg (het geven van leiding aan infectieziektebestrijding, de bevordering van de kwaliteit en doelmatigheid van de publieke gezondheidszorg en de instandhouding en verbetering van de landelijke ondersteuningsstructuur). Het PvE van de GGD (in samenwerking met het RIVM) vormt de basis voor de inrichting van de app.*
*De inzet van de notificatieapp maakt onderdeel uit van de bron- en contactopsporing door de GGD; het zijn dus de GGD'n die met de app gaan werken.*

*Een mandaat/verwerkersconstructie is dan ook naar onze mening niet passend in deze situatie. Een dergelijke constructie zou o.i. ook minder helder zijn. Minder helder omdat dan niet uit de wet zelf blijkt wat de bedoeling is, terwijl ons dat juist omdat het om de AVG-rechten gaat zo belangrijk lijkt, en ook omdat met mandaat de indruk gewekt zou kunnen worden dat de minister deze taken eventueel ook zelf zou willen doen. Daarom hebben we ervoor gekozen om in de wet zelf gewoon duidelijk uiteen te zetten wat de bedoeling is: onzes inziens is dat ook waar het hier in wezen om gaat: op grond van de AVG moet glashelder zijn waar een burger zijn rechten kan uitoefenen.*

*Gelet hierop, achten wij het passend dat de minister als verwerkingsverantwoordelijke voor de app is. Het zou echter zeer onwenselijk zijn de minister van VWS ook voor de uitoefening van de 'AVG-rechten' als verwerkingsverantwoordelijke aan te wijzen, aangezien hij dan juist persoonsgegevens ten behoeve van de notificatieapp zou gaan verwerken terwijl dat niet nodig en daarmee vanuit privacyrechtelijk perspectief zeer*

*onwenselijk is; er zouden dan immers gegevens van de GGD´n naar de minister moeten gaan om dat mogelijk te maken, m.a.w. er zou een extra gegevensstroom gegenereerd moeten worden. Eenzelfde constructie (dus met gedeelde verwerkingsverantwoordelijkheid) staat ook in artikel 7.1.2.2 van de Jeugdwet (verwijsindex risico´s jongeren).*

*Dus gelet op het bovenstaande zijn wij op deze constructie uit gekomen: gebruikers van de notificatieapp kunnen zich voor de uitoefening van hun rechten op grond van de artikelen 12 tot en met 23 en 33 AVG dus wenden tot hun GGD. Daarnaast voorziet artikel 6d, zevende lid, in de mogelijkheid om bij of krachtens amvb regels te stellen over de uitoefening van rechten van betrokkenen. Hierbij kan er ook aandacht zijn voor artikel 11 AVG.*

*Antwoord c*
*Deze gezamenlijke verwerkingsverantwoordelijkheid past ook bij de verschillende fasen van de gegevensverwerking. Het door middel van de notificatieapp uitwisselen en opslaan van contactcodes en TEK's is onlosmakelijk verbonden met elkaar en met de bron- en contactopsporing door de GGD. Hier geldt dus voor alle fasen voorgaande uitleg.*

*Antwoord d en e*
*Voor zover je onder d de tek's en server bedoelt. De GGD heeft geen toegang tot de gegevens op de server, maar heeft de interactie met de server door bijvoorbeeld de dag van ziekteverschijnselen naar de server te sturen en de validatiecode te verstrekken. Belangrijk is dat de gegevens die op die server staan niet terug te herleiden zijn naar individuen. Dit omdat het mogelijk identificerende gegeven (IP-adres) voor die tijd wordt gescheiden van de TEKs. Uiteraard beschikt de GGD wel over (bijzondere) persoonsgegevens van de cliënten waarover een besmetting gemeld is dan wel gegevens van betrokkenen bij bron –en contactonderzoek. Hier vindt echter geen wijziging in plaats door invoering van de app.*

**2) Hoe werkt de de-activering? Dit moet onafhankelijk van de gebruiker plaats vinden. Is dan verwijdering van de app voldoende? Hoe zit dat met de techniek achter de app, wordt dat allemaal gede-activeerd?**

**Zoals telefonisch door uw medewerker toegelicht spitst deze vraag zich toe op twee situatie. Ik geef hieronder per situatie een toelichting.**

**a. Wat gebeurt er met de gegevens (op de telefoon en in de backend server) op het moment dat je de app van je telefoon verwijdert.**

*Op het moment dat je de app van je telefoon verwijdert stopt de api met het uitzenden van RPI's. Conform de standaard werking van de api worden de TEKs en ontvangen RPI's na veertien dagen verwijderd. Vier dagen na verwijdering van de app staan er daarmee nog van tien dagen TEKs en ontvangen RPI's op de telefoon. Veertien dagen na deactiveren van de app zijn ook alle TEKs en RPI's verwijderd van de telefoons.*
*De gebruiker heeft te allen tijde de mogelijkheid om de TEKs en verzamelde RPI's te verwijderen in de systeeminstelling van de telefoon, dus ook nadat de app verwijderd is. De TEKs en ontvangen RPI's worden opgeslagen in de api, niet in de app. Op de backend server worden de geuploade TEKs tot veertien dagen na moment van uploaden bewaard. Er is geen link met de persoon die ze heeft geupload.*

**b. Wat gebeurt er met de gegevens als je na uitwerking van de wet, vergeet om de app van je telefoon te halen?**

*De app zal gedeactiveerd worden. Als dat van toepassing is gebeuren er drie dingen.*
1. *Burgers worden geïnformeerd via gangbare communicatiekanalen.*
2. *De app krijgt een deactivering file. Deze file gaat mee in de download van de Diagnose Keys (DKs) die meermaals per dag vanaf de server wordt opgehaald. (DK's: DKs zijn TEKs die zijn toegelaten op de centrale server; zie mvt). Dit leidt ertoe dat de app wordt uitgeschakeld. Dit houdt voor de api in dat deze geen TEKs meer aanmaakt en geen RPI's meer uitzend. Ook wordt in de app getoond dat de app is gedeactiveerd en worden alle achtergrondtaken gedeactiveerd. Conform de standaard werking van de api worden de TEKs en ontvangen RPI's na veertien dagen verwijderd. Vier dagen na deactiveren van de*

*app staan er daarmee nog van tien dagen TEKs en ontvangen RPI's op de telefoon. Veertien dagen na deactiveren van de app zijn ook alle TEKs en RPI's verwijderd van de telefoons.*

3. *De server waar TEKs worden geüpload wordt uitgeschakeld wat ervoor zorgt dat er technisch gezien geen TEKs meer op de server komen. In het geval DKs via de voorgenomen federated gateway uitgewisseld worden wordt ook deze uitwisseling technisch stopgezet. De download server blijft tot 30 dagen na het besluit tot deactivering actief om ervoor te zorgen dat de in punt 2 genoemde deactiveringsfile gedurende deze 30 dagen opgehaald kan worden door gebruikers die op uiteenlopende redenen deze file niet direct hebben ontvangen, bijvoorbeeld doordat zij geen internetverbinding hadden.*

**3) Wat is de stand van zaken mbt interoperabiliteit met andere landen?**

*Het antwoord op deze vraag kan gesplitst worden in 2 delen: de juridische en de praktische/feitelijke stand van zaken.*

*Juridische stand van zaken:*

*Op vrijdag 26 juni 2020 heeft de Commissie aan de Lidstaten medegedeeld dat het Uitvoeringsbesluit EU 2019/1765[1] van de Commissie voorschriften voor de oprichting, het beheer en de transparante werking van het e-gezondheidsnetwerk zal worden gewijzigd. Deze wijziging behelst de inzet van een technische oplossing genaamd "federated gateway". Middels deze technische oplossing wordt het mogelijk gemaakt om de gegenereerde TEKs* ***(hierna: codes)*** *in de notificatieapp binnen de Unie uit te wisselen zodat het COVID-19-virus kan worden bestreden. In dit verband is de minister medeverwerkingsverantwoordelijke voor het verwerken van de gegevens via federated gateway, wanner Nederland hierop aansluit en er ' Nederlandse codes' door de gateway gaan.*

*Op 16 juni 2020 heeft het Europees Comité voor gegevensbescherming het volgende verklaard:*

*"However, given the potential increased data protection risk arising from interoperability, […]. controllers should also explore other alternatives. […] The same legal bases as discussed in the Guidelines 04/2020 are still applicable. When relying on public interest, national law may need to be adjusted to provide for the sharing of the data with other services. In case of consent, an additional consent will need to be collected for the interoperability processing fulfilling all of its requirements. In particular, it needs to be specific and therefore sufficiently granular. When different legal bases are used by the different data controllers of the contact tracing applications, additional measures may be required to implement data subject rights related to the legal basis. Where it concerns health data art. 9 GDPR is applicable and the controllers will need to be able to rely on one of the exceptions mentioned there."[2]*

*In Nederland wordt de verwerking van gegevens in het kader van de notificatieapp gebaseerd op de taak van het bron- en contactonderzoek door GGD[3] én de algemene taak van de minister in artikel 3 en 7 Wet publieke gezondheid (Wpg). Hieruit volgt dat het uitgangspunt is dat de Nederlandse notificatieapp alleen kan worden ingezet ter ondersteuning van het bron –en contactonderzoek van de GGD. Deze grondslag voorziet dus niet in een uitwisseling van gegevens (de TEK codes van besmette personen) via federated gateway binnen de Unie. Bovendien kent Wpg een andere procedure voor internationale meldingen.[4] Internationale uitwisseling van appcodes kan onzes inziens niet op dit artikel worden gebaseerd.*

*Het huidige wetsvoorstel, zoals het nu bij u voor advies voor ligt voorziet niet in een dergelijke grondslag. In dit wetsvoorstel wordt immers alleen geëxpliciteerd wat nu al mogelijk is op basis van de wettelijke taak tot bron- en contactopsporing van de GGD en de algemene taak van de minister. Uitwisseling van gegevens via de federated gateway binnen de Unie zal daarom, op het moment dat dit daadwerkelijk plaats gaat vinden, vooralsnog alleen plaats vinden indien er sprake is van een expliciete en separate (los van*

[1] PbEU 2019, L 270/83, ELI: https://eur-lex.europa.eu/eli/dec_impl/2019/1765/oj.
[2] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en.pdf.
[3] Zie artikel 6 Wet publieke gezondheid.
[4] Deze procedure is dan dat het RIVM die meldt aan haar evenknie in het land van besmetting (artikel 12 Wpg). We kunnen dit niet relateren aan de huidige taken in de Wpg.

*de toestemming voor gegevensverwerking ihkv nationaal gebruik van de app) toestemming van de betrokkene.*

*Stand van zaken in de praktijk*
*De Europese Commissie heeft de opdracht op de federated gateway te bouwen belegd bij de bouwers van de Duitse app; SAP en Deutsche telecom. De verwachte oplevering is in september. Dit betekent dat de Federated Gateway niet beschikbaar zal zijn bij de voorgenomen Nederlandse livegang van 1 september. Om grensoverschrijdende interoperabiliteit te realiseren, moeten er ook nationaal nog een aantal zaken geregeld worden.*
*- Er moet aandacht zijn voor de juridische grondslag in uitdrukkelijke toestemming*
*- Verbinding maken tussen onze nationale back-end server met de Federated Gateway (technisch)*
*-Deelname aan de pilot met de Federated Gateway, waarvoor voorwaardelijk is dat de andere punten geregeld zijn.*