datum: 23 juli 2020
uw kenm. z2020-11824
betreft: DPIA-Corona Melder App

Geachte mevrouw S, heer K en heer H,

In uw brief van 16 juli jl. met bovenvermeld kenmerk, zoals door u nader toegelicht in ons telefoongesprek van dezelfde datum, stelt u een aantal vragen over DPIA die wij u 7 juli j. hebben toegestuurd. U doet daarbij het verzoek binnen één week na dagtekening, dus uiterlijk op 23 juli 2020, deze vragen te beantwoorden.
In deze brief voldoen wij tijdig aan uw verzoek. U vindt hieronder, na een enkele verduidelijkende opmerking vooraf, de beantwoording van uw vragen.

Opmerking vooraf

In de DPIA heeft het ministerie beoordeeld wat de effecten zijn van de beoogde verwerkingsactiviteiten in het kader van de COVID-19 notificatie-app, inmiddels aangeduid als de CoronaMelder (hierna: "**de app**"). Uit deze DPIA blijkt dat deze verwerkingsactiviteiten, naar het oordeel van het ministerie, géén hoge risico's inhouden voor de rechten en vrijheden van de gebruikers van de app. Voor zover er sprake zou kunnen zijn van dergelijke risico's, zijn er passende technische, organisatorische en andersoortige maatregelen genomen om deze te beperken, met als resultaat een optimale waarborging van deze rechten en vrijheden. Dit wordt onderschreven door de FG's bij wie advies hierover is ingewonnen.

Er is derhalve geen aanleiding tot een verzoek om een voorafgaande raadpleging, in de zin van artikel 36, eerste lid, AVG. Niettemin wordt het, gelet op de mogelijke maatschappelijke impact van de app, wenselijk en nuttig gevonden dat ook de Autoriteit Persoonsgegevens (AP), in staat wordt gesteld haar oordeel daarover te geven. Ons verzoek om uw advies moet dan ook in die zin worden opgevat.[1] In ons telefoongesprek van 16 juli jl. bespraken wij een en ander al, het komt ons goed voor dit bij dezen te expliciteren.

[1] In zoverre lijkt de onderhavige adviesvraag dus goed vergelijkbaar met het verzoek dat vanuit de Ierse overheid is gedaan aan de bevoegde toezichthouder in Ierland, de Data Protection Commission. Zie https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/DPC%20review%20of%20CTI%20App%20DPIA%20June%202020.pdf ("COVID Tracker Ireland App. Data Protection Impact Assessment Review. June 2020), p. 2: "The review is provided to the Data Controllers on an informal consultation basis (…)".

Vraag 1: Verwerkingsverantwoordelijk voor de verwerking

a. Er is nu gekozen voor verwerkingsverantwoordelijkheid op 'twee niveaus' waarbij verwerkingsverantwoordelijkheid wordt gesplitst in beheer en inrichting (met de Minister van Volksgezondheid, Welzijn en Sport als verwerkingsverantwoordelijke) en de uitoefening van de rechten van betrokkenen (waarvoor betrokkene zich moet richten tot de eigen regionale GGD). Dit roept vragen op. Kunt u toelichten waarom hiervoor is gekozen en niet bijvoorbeeld enkel de minister van VWS aan te wijzen als verwerkingsverantwoordelijke? Dit staat immers het aanwijzen van een contactpersoon voor het uitoefenen van de rechten van betrokkenen niet in de weg (artikel 29 AVG).

Er is gekozen voor een opzet waarbij sprake is van verwerkingsverantwoordelijkheid op twee niveaus omdat dit het meest recht doet aan ieders rol bij de ontwikkeling en inzet van de app. Het louter als contactpersoon aanwijzen van de GGD zou in ieder geval niet passen bij het feit dat de app onderdeel uitmaakt van de wettelijk taak van het doen van bron- en contactopsporing door de GGD.

Enerzijds is de minister van VWS betrokken bij de ontwikkeling en toepassing van de app, en als zodanig verantwoordelijk voor de in dat verband verwerkte gegevens, 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). Anderzijds geldt dat de app onderdeel uitmaakt van de taak tot het doen van bron- en contactopsporing door de GGD op grond van artikel 6 Wpg. Dat maakt ook dat het programma van eisen van de GGD (in samenwerking met het RIVM) de basis voor de inrichting van de app vormt. Daarnaast is het ook de GGD en niet de minister van VWS die daadwerkelijk met de app gaat werken, bijvoorbeeld door de dag van ziekteverschijnselen en de van de besmette persoon ontvangen validatiecode naar de naar de server te sturen.

Het is, mede in het verlengde daarvan, onwenselijk dat de minister uitvoering geeft aan de rechten van betrokkenen. In dat geval zou hij juist extra persoonsgegevens moeten gaan verwerken die hij enkel verwerkt ter uitvoering van de rechten van betrokkenen, terwijl de GGD die betrokkenen in het kader van de bron- en contactopsporing heeft gesproken. Dat de minister, om te voldoen aan rechten van betrokkenen, die persoonsgegevens zou gaan verwerken, wordt, in ieder geval juridisch gezien, niet anders met de aanwijzing van een contactpersoon voor het uitoefenen van de rechten van betrokkenen.[2]

b. Het verzoek om voorafgaande raadpleging is ingediend door het ministerie van Volksgezondheid, Welzijn en Sport, welke aanvankelijk als

---

[2] Zie voor een vergelijkbare regeling overigens artikel 7.1.2.2 van de Jeugdwet.

verwerkingsverantwoordelijke is aangeduid. Uit de DPIA blijkt dat de verwerkingsverantwoordelijkheid bij zowel het ministerie als de verschillende regionale GGD'en komt te liggen. Dit zou betekenen dat het voorliggende verzoek om voorafgaande raadpleging niet ontvankelijk is wanneer het niet door alle verwerkingsverantwoordelijke partijen is opgesteld, ondertekend en ingediend. Hoe ziet u de verwerkingsverantwoordelijkheid in relatie tot het verzoek om voorafgaande raadpleging? Kunt u ons een overzicht geven van de verantwoordelijke organisaties inclusief contactgegevens, contactpersonen en FG's?

In onze opmerking vooraf hebben wij uiteengezet dat er, gelet op de uitkomsten van de DPIA, geen aanleiding is voor het doen van een verzoek om een voorlopige raadpleging, als bedoeld in artikel 36, eerste lid, AVG. In zoverre kan er om deze reden geen sprake zijn van niet ontvankelijkheid. Wij achten het niettemin wenselijk op te helderen dat de GGD betrokken is bij de totstandkoming van de DPIA. Als een van onze contactpersonen heeft de FG van de GGD-GHOR de DPIA uitvoerig bekeken, daar vragen over gesteld en input geleverd. De vragen zijn besproken en de input is verwerkt. Het adviesverzoek is gedaan in overleg met de GGD-GHOR. Tussen de Staat, de GGD-GHOR en de regionale GGD-en wordt een overeenkomst gesloten waarin onder meer afspraken worden gemaakt over het gebruik en het beheer van de app en over de wijze waarop uitvoering zal worden gegeven aan de verplichtingen op grond van de AVG. Ons contactpersoon namens de FG's van de GGD-en is de FG van de GGD-GHOR (fg@ggdghor.nl).

c. Waarom is de rol van de GGD-en als verwerkingsverantwoordelijken terwijl hun rol bij de app zeer beperkt t.a.v. de gegevensverwerking?

Voorop staat dat de app ervoor is bedoeld om de GDD-en te ondersteunen in hun bron- en contactopsporingstaak. Voor zover er in de app persoonsgegevens worden verwerkt, is duidelijk dat de GGD daarbij een essentiële rol speelt. Dit omdat zij in de validatiefase, binnen 24 uur nadat is vastgesteld dat de gebruiker besmet is, de autorisatiecode van deze gebruiker met eerste ziektedag via het GGD-portaal naar de back-end server stuurt. Voor deze gegevensverwerkingen ligt de zeggenschap, en daarmee verwerkingsverantwoordelijkheid in de zin van art. 4, onderdeel 7, AVG, bij de GGD.

In zoverre lijkt de typering van de rol van de GGD-en als 'zeer beperkt' niet geheel adequaat. In de DPIA is uiteengezet dat, waar het gaat om de verwerking van gegevens in het kader van de app, de rol van de GGD-en beslissend is, omdat gegevens van een besmette gebruiker (TEKs, DKs) alleen op de server worden vastgelegd als er binnen 24 uur van de GGD een overeenstemmende autorisatiecode wordt ontvangen. Als zodanig is deze onder de verantwoordelijkheid van de GGD uitgevoerde gegevensverwerking dus onmisbaar om te kunnen komen tot notificaties aan andere gebruikers. Voor een nadere, meer gedetailleerde uiteenzetting van een en ander wordt verwezen naar de DPIA (par. A2 en A3).

De app, en meer specifiek ook de rol van de GGD-en daarbinnen, is bovendien ingepast in het reeds bij de GGD-en operationele proces van uitvoering van het bron- en contactopsporing. De app ondersteunt de aan de GGD-en opgedragen wettelijk taak van bron- en contactopsporing. Verwezen wordt naar de beantwoording van vraag 1a.

Overigens wijzen wij erop dat er binnen de app in algemene zin c.q. in zijn geheel weinig (zo niet: geen) persoonsgegevens worden verwerkt. Dit is inherent aan de gekozen decentrale opzet van de app.

d. Begrijpen we u goed dat u artikelen 3 en 7 van de Wpg voldoende specifiek vindt om als grondslag voor de verwerking van persoonsgegevens voor een notificatieapp te dienen en dat een soortgelijke zin zoals is opgenomen in het voorgestelde artikel 6d van de Wpg voor de GGD-en met betrekking tot de verwerking van bijzondere persoonsgegevens niet nodig is?

Zoals vermeld in het antwoord op vraag 1a bieden de bepalingen van artikel 3 en 7 de minister, en biedt artikel 6 Wpg de GGD-en, een grondslag voor de verwerking van persoonsgegevens in het kader van respectievelijk de bevordering van de kwaliteit en doelmatigheid van de publieke gezondheidszorg en het zorgdragen voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur (minister), respectievelijk de uitvoering van de algemene infectieziektebestrijding, waaronder in ieder geval behoort bron- en contactopsporing (GGD-en).

In de app is, zo blijkt ook uit de DPIA (o.a. par. 16 e.v.), een groot aantal maatregelen genomen waarmee het risico op identificatie van gebruikers effectief, in vergaande mate is beperkt. Voor zover er bij de app sprake is van de verwerking van persoonsgegevens waarvoor de minister verwerkingsverantwoordelijke is, kan deze zonder meer worden gekwalificeerd als bevordering van de kwaliteit en doelmatigheid van de publieke gezondheidszorg en het zorgdragen voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur.

Verder is van belang dat de in de Wpg voorgeschreven bron- en contactopsporing door de GGD een breed doel dient, namelijk het tegengaan van de verspreiding van infectieziekten zoals het virus, en dus ook breed moet worden uitgelegd.[3] De wijze waarop de bron- en contactopsporing wordt uitgevoerd laat de wet dan ook bewust vormvrij, juist omdat de GGD moet kunnen differentiëren naar wat afhankelijk van de omstandigheden van het geval de beste en meest effectieve aanpak is. Zo blijkt uit de wetsgeschiedenis dat de schaal van de bron- en contactopsporing afhankelijk is van de schaal van mogelijke besmetting en dat onder onderzoek door de GGD ook het waarschuwen van mogelijk geïnfecteerde personen moet worden begrepen.[4]

---

[3] *Kamerstukken II* 2007/08, 31 316, nr. 6, p. 7 en 8.
[4] Zie bijvoorbeeld *Kamerstukken II* 2002/03, 28 868, nr. 5, p. 3 en 4 en *Kamerstukken II* 2007/08, 31 316, nr. 3, p. 11.

Ook voor de bestrijding van de epidemie geldt dat het vanwege het grote besmettingsgevaar noodzakelijk is dat de bron- en contactopsporing breed wordt ingezet: zoveel mogelijk en zo vroeg mogelijk zicht krijgen op mensen die mogelijk besmet zijn met het virus. De notificatieapp draagt daaraan bij. Zo zorgt de notificatieapp voor ondersteuning van de bron- en contactopsporing doordat ook personen kunnen worden bereikt van wie de geïnfecteerde gebruiker geen contactgegevens heeft en die hij mogelijk zelfs niet eens kent. Dit aspect van de bron- en contactopsporing kan alleen worden uitgevoerd indien voorafgaand aan de constatering van een besmetting contactcodes van andere gebruikers zijn verzameld. De beide aspecten zijn onlosmakelijk met elkaar verbonden voor het goed kunnen uitvoeren van de bron- en contactopsporing en daarmee het bereiken van het daaraan ten grondslag liggende doel de verspreiding het virus tegen te gaan.

Een soortgelijke zin zoals is opgenomen in het voorgestelde artikel 6d Wpg voor de GGD-en met betrekking tot de verwerking van bijzondere persoonsgegevens, is niet nodig. Zoals hierboven reeds is toegelicht, moet de uitvoering van de bron- en contactopsporing breed worden opgevat. Ten behoeve daarvan mogen, in combinatie met het bepaalde in artikel 9, lid 2, aanhef en onder i, AVG, bijzondere persoonsgegevens worden verwerkt.

> Vgl. ook de EDPB, Richtsnoeren 04/2020 voor het gebruik van locatie-gegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19, vastgesteld op 21 april 2020, p. 4. De EDPB stelt over het verzamelen van gezondheidsgegevens het volgende:
>
> "Het gebruik van een app ter bestrijding van de COVID-19-pandemie kan er bovendien toe leiden dat gezondheidsgegevens worden verzameld (bijvoorbeeld over de toestand van een besmette persoon). De verwerking van dergelijke gegevens is toegestaan wanneer de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid en voldaan wordt aan de voorwaarden van artikel 9, lid 2, onder i), AVG, en wanneer de verwerking noodzakelijk is voor doeleinden op het gebied van gezondheidszorg, zoals beschreven in artikel 9, lid 2, onder h), AVG. Afhankelijk van de rechtsgrondslag kan de verwerking ook gebaseerd zijn op uitdrukkelijke toestemming (artikel 9, lid 2, onder a), AVG)."

Met andere woorden: de artikelen 3, 7 en 6 van de Wpg worden (waar het eventuele bijzondere persoonsgegevens betreft: in combinatie met artikel 9, lid 2, aanhef en onder i, AVG) voldoende specifiek geacht om (in combinatie met artikel 6 lid 1 aanhef en onder e AVG) als grondslag voor de verwerking van (bijzondere) persoonsgegevens voor een notificatieapp te dienen.

<u>Vraag 2. De verwerking en risico's</u>

a. De in de DPIA opgenomen risico's lijken grotendeels gebaseerd te zijn op technische risico's in relatie tot de gebruikte infrastructuur. Hoewel deze infrastructuur verband houdt met de verwerkingen ziet de AP nog geen

uitgebreide afweging van de risico's voor de rechten en vrijheden van natuurlijke personen bij de voorgenomen verwerking. Kunt u toelichten hoe de identificatie van risico's heeft plaatsgevonden en welke rol de risico's voor de rechten en vrijheden van natuurlijke personen daarbij spelen?

Er is een uitgebreide risicoanalyse gedaan. Daaruit werd duidelijk dat er maar in zeer beperkte mate sprake is van risico's voor de rechten en vrijheden van gebruikers en/of andere natuurlijke personen. In drie uitvoerige sessies is het hele proces van de werking van app, de back-end en het proces bij de GGD indringend geanalyseerd. Voor iedere stap in het proces is geanalyseerd welke gegevens er in gebruik zijn, welke potentiële risico's er zijn en in hoeverre er sprake kan zijn persoonsgegevens en gezondheidsgegevens. Aan deze analyse hebben ook vertegenwoordigers van de GGD en het RIVM een bijdrage geleverd. Uiteraard is ook de FG van het ministerie van VWS hierbij betrokken en heeft zij de door haar geïdentificeerde potentiele risico's onder de aandacht gebracht. Vervolgens is deze input verwerkt om te komen tot een eerste, basale risicoanalyse. In dat verband is nadrukkelijk ook gekeken naar ervaringen in andere lidstaten die gebruik maken van een vergelijkbare notificatie-app, gebaseerd op een decentraal gegevensverwerkingsmodel. Op basis daarvan is vervolgens de DPIA opgesteld en zijn de realistische risico's benoemd.

Van belang is dat er in Nederland voor is gekozen om uit te gaan van veel minder gegevens dan in andere lidstaten die gebruik maken van op DP3T-gebaseerde notificatie-apps. Zo is er in Nederland voor gekozen om bij een melding van een besmetting te volstaan met een autorisatiecode om de op de server aanwezige diagnose keys ("DKs") vrij te geven en deze alleen te voorzien van een 'date of last exposure'. Dit in tegenstelling tot bijvoorbeeld Ierland, waar de grondslag voor de gegevensverwerkingen overwegend wordt gevonden in de toestemming van de gebruiker, en waar ook andere gegevens worden verwerkt, zoals: het telefoonnummer, geslacht, leeftijdsgroep, stad en COVID-19-symptomen. In het ontwerp (design) van de Nederlandse notificatie-app is de verwerking van dergelijke gegevens, en dus ook de koppeling daarvan aan de gebruiker, technisch uitgesloten.

Er is nadrukkelijk gekeken naar de DPIA die in Ierland is opgesteld voor de app die aldaar al geruime tijd in gebruik is en waarover de Ierse toezichthouder, de Data Protection Commission (DPC), heeft geadviseerd.[5] Dit omdat de Ierse notificatie-app eveneens gebruik maakt van de api software van Google en Apple.

Wij wijzen er nog op dat in de app geen statistieken worden verzameld om terug te sturen naar een centraal punt. Verder wordt bij het uploaden van TEKs het IP-adres direct verwijderd en bij het Security Operations Center dat monitort op aanvallen is geborgd dat op geen moment potentieel tot een persoon herleidbare informatie bij

---

[5] Zie https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%2026.06.2020.pdf (Data Protection Impact Assessment COVID Tracker App) en https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/DPC%20review%20of%20CTI%20App%20DPIA%20June%202020.pdf ("COVID Tracker Ireland App. Data Protection Impact Assessment Review. June 2020).

beheerders van het systeem kan komen. Waar er sprake was van een risico op herleidbaarheid tot de identiteit van de gebruiker zijn de maatregelen getroffen om dat te voorkomen. Op deze wijze zijn de rechten en vrijheden van gebruikers, gelet op de huidige stand van de techniek, optimaal gewaarborgd.

Zoals besproken in het telefonisch overleg van 16 juli jl. bespreken wij de verschillende criteria genoemd in overweging 75 uit de Preambule van de AVG:

1. Ernstige lichamelijke schade. De verwerking is uitsluitend gericht op het waarschuwen van gebruikers en aldus ondersteunen van bron- en contactonderzoek. Het is niet goed voorstelbaar dat de daarvoor te verrichten verwerkingen kunnen leiden tot ernstige lichamelijke schade. Integendeel. In voorkomende gevallen kan een tijdige melding ernstige lichamelijke schade voorkomen, zeker als de desbetreffende gebruiker (bijvoorbeeld: een verpleegkundige of iemand werkzaam in een verzorgingstehuis) nog niet te maken heeft met ziekteverschijnselen, maar wel contact heeft met kwetsbare personen.

2. Ernstige materiele schade. Van materiële schade zou mogelijk sprake kunnen zijn als een gebruiker ten onrechte een melding ontvangt van een contact met een andere besmette gebruiker (*false positives*). Voorstelbaar is dat een gebruiker als gevolg daarvan acties onderneemt waarvan hij nadeel heeft, bijvoorbeeld een vakantie annuleert of niet naar een sollicitatiegesprek gaat. Voor zover het gaat om de gegevensverwerkingen in het kader van de notificatie-app is dit risico in vergaande mate beperkt, zo niet uitgesloten, doordat de arts van de GGD, die de besmetting heeft vastgesteld, de naar de back-end verstuurde TEKs valideert. Ook is het in vergaande mate beperkt, zo niet uitgesloten, dat de er door manipulatie van de server onterechte meldingen worden gegenereerd.

3. Ernstige immateriële schade. Van immateriële schade zou mogelijk sprake kunnen zijn als een gebruiker ten onrechte een melding ontvangt van een contact met een andere besmette gebruiker (*false positives*). Voorstelbaar is dat een gebruiker daardoor te kampen krijgt met psychische problemen. Voor zover het gaat om de gegevensverwerkingen in het kader van de notificatie-app is ook dit risico in vergaande mate beperkt, zo niet uitgesloten, doordat de arts van de GGD, die de besmetting heeft vastgesteld, de naar de back-end verstuurde TEKs valideert. Ook is het in vergaande mate beperkt, zo niet uitgesloten, dat de er door manipulatie van de server onterechte meldingen worden gegenereerd.

4. Discriminatie. Er worden in de notificatie-app maar in heel beperkte mate persoonsgegevens verwerkt en voor zover daarvan sprake is, gaat het, behoudens eventuele gezondheidsgegevens, niet om bijzondere categorieën van gegevens. Het is moeilijk voorstelbaar dat de gegevensverwerkingen in

het kader van de app – aan de hand waarvan identificatie zo goed als uitgesloten is – als gevolg heeft dat een gebruiker, of iemand anders, te maken krijgt met discriminatie. Wij wijzen er ook nog op dat in het voorgenomen wetsvoorstel Tijdelijke Wet notificatieapplicatie, zoals bekend, is voorzien in een antimisbuikbepaling (art. 6d, zesde lid), die het uitdrukkelijk verbiedt dat werkgevers, zorgverzekeraars, onderwijsinstellingen, winkels of wie dan ook, het gebruik van de notificatieapp of welk digitaal hulpmiddel bedoeld om met het virus besmette personen te identificeren dan ook, direct of indirect verplicht mag stellen. Daarmee is ook het risico geadresseerd van discriminatie van degenen die ervoor kiezen om géén gebruik te maken van de notificatieapp.

5. Identiteitsdiefstal. Er worden in de notificatieapp uitsluitend digitale sleutels verwerkt, die geen identificerende gegevens bevatten. Identiteitsfraude is daardoor niet realistisch. Als identiteitsfraude met behulp van de app al mogelijk kan worden geacht, vergt dat een aanzienlijke inspanning en zeer specialistische kennis, en levert dat voor de fraudeur (waarschijnlijk) een marginale *return on investment*.

6. Fraude. Er worden in de notificatieapp uitsluitend digitale sleutels verwerkt die geen identificerende gegevens bevatten. Het frauderisico is daardoor gering. Voorstelbaar is dat de informatie dat er Corona heerst en er maatregelen zijn genomen, een risico kan betekenen op fraudegericht handelen. Dit kan bijvoorbeeld door nep-websites op te tuigen die lijken op een site van de rijksoverheid. Dergelijke fraude is evenwel niet specifiek voor de notificatieapp en vallen als zodanig buiten het bereik van de DPIA.

7. Verwerking kan leiden tot financiële verliezen. De notificatieapp kan helpen deze te voorkomen. Vooral bij zelfstandigen zal eerder onderkennen van de ziekte onnodige uitval in voorkomende gevallen kunnen helpen voorkomen. Verwezen wordt naar de opmerkingen bij materiele en immateriële schade, respectievelijk nrs. 2 en 3.

8. Verwerking kan leiden tot verlies van vertrouwelijkheid van door beroepsgeheim beschermde persoonsgegevens. Dit risico is onderkend en in de risico inschattingen meegenomen en geadresseerd.

9. Ongeoorloofde ongedaanmaking van pseudonimisering. Ook dit risico is in de risicoinschattingen meegenomen en geadresseerd.

10. Aanzienlijk economisch en maatschappelijk nadeel. Verwezen wordt naar de opmerkingen bij nrs. 1 t/m 3 en 7 en, waar het maatschappelijk nadeel betreft, ook naar de overige nummers (4 t/m 6, 8, 9, en 11 t/m 17). Van belang daarbij is dat de app uitdrukkelijk beoogt om de nadelige economische een maatschappelijke gevolgen van de pandemie in te perken.

Verschillende studies hebben bevestigd dat, zelfs bij inachtneming van beperkt gebruik, de introductie van een notificatieapp kan bijdragen aan de reductie van het aantal verdere besmettingen en het reduceren van de tijd tussen besmetting en signalering van andere geïnfecteerden.[6] Wat dat betreft kan er in redelijkheid dus vanuit worden gegaan dat de app, en de gegevensverwerkingen in het kader daarvan, een betekenisvolle bijdrage kan leveren aan de vermindering van het economisch en maatschappelijk nadeel dat wordt veroorzaakt door de pandemie. Voor zover er, als gevolg van de gegevensverwerkingen in het kader van de app, al sprake zou kunnen zijn van economisch of maatschappelijk nadeel, moet dat nadeel bovendien worden afgezet tegen de met behulp van de app te realiseren vermindering van het nadeel dat het gevolg is van de pandemie. Verwezen wordt verder ook naar nr. 14 van de DPIA, waarin noodzaak en evenredigheid zijn beschreven.

11. Uitoefening rechten en vrijheden. Er is in voorzien dat, voor zover er in het kader van de app persoonsgegevens worden verwerkt, gebruikers hun rechten ten aanzien daarvan op grond van hoofdstuk III AVG onverkort kunnen uitoefenen (zie ook het antwoord op vraag 1a en 2g).

12. Verhindering uitoefening van controle over persoonsgegevens. In het ontwerp (design) van de notificatieapp is gewaarborgd dat de gebruiker altijd controle heeft over de verwerking van de op hem of haar betrekking hebbende persoonsgegevens. De gebruiker kiest ervoor om de app te downloaden en te installeren, en om deze aan te zetten. De gebruiker kan altijd de app uit (en desgewenst weer aan) zetten, hetzij in de app hetzij door Bluetooth uit (of aan) te zetten. Verder wordt verwezen naar het voornemen een antimisbruikbepaling in de Wpg op te nemen, zodat het een ieder verboden is om de app verplicht te stellen (opmerking nr. 4).

13. Verwerking van bijzondere gegevens, anders dan gezondheidsgegevens. Er is geen sprake van de verwerking van ras- of etniciteitsgegevens, van gegevens over politieke opvattingen of religie en levensbeschouwelijke overtuigingen, over vakbondslidmaatschap of over het seksuele leven of gedrag. Evenmin is sprake van de verwerking van genetische gegevens, of gegevens over strafrechtelijke veroordelingen of daarmee verband houdende veiligheidsmaatregelen.

14. Er kan wel sprake zijn van verwerking van gegevens over gezondheid, namelijk waar het gaat om het versturen van TEKs van een besmette gebruiker (door de gebruiker zelf) en de eerste ziektedag naar de back-end

---

[6] Zie bijv. 'Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown', University of Oxford 16 April 2020, te vinden via: https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown (laatst. geraadpl. 22 juni jl.); alsmede 'Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing', NIH 8 May 2020, te vinden via https://pubmed.ncbi.nlm.nih.gov/32234805/ (laatst. geraadpl. 22 juni jl.).

server (door de GGD) en het vervolgens waarschuwen van andere gebruikers. Overigens kan er pas sprake zijn van gezondheidsgegevens nadat op de back-end server binnen 24 uur de autorisatiecode is ontvangen van zowel de gebruiker als de GGD. In het ontwerp (design) van de app is rekening gehouden met de daarmee verband houdende risico's en deze zijn in de DPIA geadresseerd.

15. Profilering. Er is in het kader van de notificatieapp geen sprake van geautomatiseerde besluitvorming, waaronder profilering, omdat er altijd betekenisvolle menselijke tussenkomst is van de GGD. Voor zover er al zou worden aangenomen dat er sprake is van geautomatiseerde besluitvorming, waaronder profilering, zou dat uitsluitend betrekking kunnen hebben op het aan de hand van signaalsterkte en contactduur bepalen van het besmettingsrisico. De daarmee verband houdende risico's zijn in de DPIA geadresseerd.

16. Kwetsbare natuurlijke personen, met name van kinderen. Er kan uiteraard niet worden uitgesloten dat ook kwetsbare natuurlijke personen, waaronder kinderen, gebruik gaan maken van de app. Echter, in de app, en evenmin in de back-end server, kunnen dergelijke groepen worden onderscheiden. De daarmee verband houdende risico's (zoals: uitsluiting, stigmatisering) zijn daarom beperkt en zijn als zodanig geadresseerd in de DPIA.

17. Grote hoeveelheid persoonsgegevens en gevolgen voor een groot aantal betrokkenen. Er is bij het ontwerp (design) van de app hiermee rekening gehouden en dit is in de DPIA geadresseerd.

b. Binnen de risicoanalyse lijkt terminologie door elkaar te lopen. Het bruto risico is het product van kans en impact voordat mitigerende maatregelen worden getroffen. Het netto risico is het restrisico. Deze begrippen worden niet consequent gebruikt. Zo wordt in 'risico' 16 van de bijlage al een mitigerende maatregel benoemd bij het bepalen van de impact. Daarnaast worden er kwaliteitscontroles genoemd waarbij niet duidelijk is of deze reeds zijn uitgevoerd of ze slechts gepland zijn. Kunt u toelichten of de nu gemaakte inschatting definitief is of dat er een nog een herziening is voorzien? Kunt u ook toelichten bij de risico's en mitigerende maatregelen waar het risico zich bevindt (bijvoorbeeld VWS, GGD-en, het framework van Google en Apple) en wie de mitigerende maatregel neemt?

Het doen van een gegevensbeschermingseffectbeoordeling is een continu proces.[7] In zoverre moet de u toegezonden DPIA worden opgevat als een eerste en gedetailleerde

---

[7] Zie bijv. 'Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown', University of Oxford 16 April 2020, te vinden via: https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown (laatst. geraadpl. 22 juni jl.); alsmede 'Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing', NIH 8 May 2020, te vinden via https://pubmed.ncbi.nlm.nih.gov/32234805/ (laatst. geraadpl. 22 juni jl.).

momentopname van diepgaande beoordeling van de risico's die de verwerkingsactiviteiten in het kader van de app kunnen inhouden voor de rechten en vrijheden van de gebruikers ervan. De genoemde kwaliteitscontroles vinden plaats op het moment dat dit op verantwoorde wijze kan gebeuren. Het heeft geen zin een beveiligingsonderzoek te starten van programmatuur, waarvan de ontwikkeling nog in volle gang is. Recentelijk is een tussenversie beschikbaar gekomen, waarbij testen wel zinvol zijn. Op deze software wordt momenteel een zogenaamde nulmeting in de vorm van een penetratietest uitgevoerd. Deze is begonnen op 3 juli jl. en is thans in de afrondende fase. De rapportage wordt eind deze week of volgende week verwacht. Op dit moment loopt een review van het cryptografisch raamwerk om op die manier helder te krijgen dat niet alleen cryptografie gebruikt wordt, maar deze ook effectief is.

De verwachting is dat omstreeks 24 juli a.s. er een codereview wordt gestart van de software op de back-end server. Dit betekent dat beveiligingsexperts de broncode gaan lezen en interpreteren op beveiligingsaspecten, op de vraag of geleverd is wat er moest worden geleverd, en niet meer dan dat (geen achterdeuren). In dezelfde periode start ook een onderzoek naar de broncode van de app. In Europees verband wordt onderzoek gedaan naar de software van Apple en Google, de zogenaamde API. Op reeds door Apple en Google gepubliceerde broncode wordt op korte termijn een review verricht (zie hierover ook het antwoord op vraag 3a). Bij het bouwen van de serveromgeving wordt door de leverancier ook een interne penetratietest uitgevoerd.

Op 10 augustus a.s. start een penetratietest op het hele stelsel van app en back-end server. Naast deze technische test wordt in augustus ook een onderzoek uitgevoerd naar de serveromgeving gericht op certificeringen, het juist hebben geïmplementeerd van de oplossingen en privacybeschermende maatregelen, de beheersomgeving en het security operations center. Over het geheel van onderzoeken en testen wordt een second opinion uitgevoerd. Over het geheel van privacyonderzoeken, het voldoen aan maatschappelijke wensen (veilig tegen corona) en beveiligingsonderzoeken wordt vervolgens een overkoepelend onderzoek uitgevoerd.

c. Bij de inschatting van de risico's, onderdeel impact, lijkt geen gewicht te zijn toegekend aan de gewenst brede adaptatie van de app en de mogelijkheid dat ongewenste verwerkingen de rechten en vrijheden van een groot aantal natuurlijke personen raakt. Daar speelt bijvoorbeeld mee de mogelijkheid dat een aanval eenvoudig kan worden opgeschaald. Kunt u toelichten hoe dit is meegewogen in de afweging?

Zoals in de DPIA is toegelicht zijn aan het gebruik van de app slechts minimale risico's voor de persoonlijke levenssfeer van de betrokkenen verbonden. Die risico's worden naar ons oordeel niet groter bij een eenvoudig op te schalen aanval: het risico per individu blijft klein omdat er per saldo maar weinig gegevens in de app worden verwerkt en een succesvolle aanval op een device, zo daarvan al sprake kan zijn, per

gebruiker niet meer kan opleveren dan de in de twee weken daaraan voorafgaand vastgelegde, versleutelde contactcodes.

Overigens kan een aanval op de back-end server er nooit toe leiden dat er ten onrechte een notificatie wordt gedaan. De notificatie wordt namelijk decentraal, op het device, gegenereerd nadat de DKs van de back-end server zijn gedownload en er op het device een vergelijking is gemaakt tussen die van de server gedownloade DKs enerzijds en de TEKs die de afgelopen 14 dagen op het device zijn verzameld naar aanleiding van contacten met andere gebruikers van de app anderzijds. De notificatie wordt dus niet verzonden vanuit de back-end server. Wel zou een succesvolle aanval op de back-end server ertoe kunnen leiden dat de DKs niet meer kunnen worden gedownload met *false negatives* tot gevolg (want zonder download van DKs kan er ook geen notificatie tot stand komen). In dat geval is aannemelijk dat zo een aanval vrijwel meteen wordt opgemerkt, zodat gebruikers via gebruikelijke kanalen kunnen worden geïnformeerd. Verder is de situatie na zo een aanval praktisch gelijk aan de situatie dat er in het geheel geen app is. De impact van een dergelijke aanval is om die reden beperkt.

Verwezen wordt verder naar de beantwoording van vraag 2d, hieronder.

d. Bij de inschatting van de risico's, onderdeel kans, lijkt de kans dat een gerichte aanval wordt uitgevoerd vaak relatief laag te worden ingeschat terwijl wordt beoogd de app binnen heel Nederland te gaan gebruiken. Dit laatste brengt met zich dat op veel fysieke plaatsen kan worden getracht aanvallen uit te voeren die, indien ze succesvol zijn, mogelijk leiden tot waardevolle informatie over bewegingspatronen van, en mogelijke ziekteverschijnselen bij mensen. Een bekend voorbeeld zijn winkelcentra met apparatuur om Bluetooth en WiFi signalen op te vangen. Dit soort informatie kan van invloed zijn op de kans dat er ergens een aanval wordt uitgevoerd. Kunt u toelichten hoe dit is meegewogen in de afweging?

Het is inderdaad de bedoeling dat veel gebruikers gebruik gaan maken van de notificatieapp. Ervan uitgaande dat er op grote schaal gebruik gaat worden gemaakt van de app impliceert dat er, zoals u het uitdrukt, op veel fysieke plaatsen kan worden getracht aanvallen uit te voeren. Er is in het ontwerp (design) van de app voorzien in verschillende maatregelen die beogen te voorkomen dergelijke aanvallen succesvol kunnen zijn. En, voor zover er al sprake zou kunnen zijn van een succesvolle aanval, zijn er ook maatregelen getroffen waarmee wordt beoogd te voorkomen dat een dergelijke succesvolle aanval eenvoudig kan worden gedupliceerd.

Voor het uitvoeren van een beschreven aanval is het nodig om nieuwe programmatuur te ontwikkelen. Omdat de app werkt met een cryptografisch stelsel dat zorgt dat een betrokkene iedere 10-20 minuten een andere code uitzendt, zal aanvullend software moeten worden ontwikkeld om na publicatie van een DK een link te berekenen met dan opgeslagen RPI's. Na het uitvoeren van die analyse is er geen sprake van

herleidbaarheid, omdat er geen andere link tussen een device en de sleutels bestaat dan de beveiligde lijst op het device zelf. Het opzetten van een beschreven aanval in een commerciële omgeving gericht op het verkrijgen van deze informatie op niet toegestane wijze schatten we derhalve als laag in.

Verder moet worden opgemerkt dat zeer specifieke en specialistische hardware moet worden gebruikt om op een juiste manier signalen op te vangen. Een beperking van het gebruikte Bluetooth Low Energy is dat op grotere afstanden het signaal minder consistent is, waardoor het moeilijker is om bruikbare signalen (in dit geval: RPIs) op te vangen. Tijdens de penetratietest is inmiddels waargenomen dat deze werking er inderdaad is. Dit is in lijn met andere onderzoeken in het algemeen naar Bluetooth Low Energy. Het technisch op grotere afstand niet kunnen gebruiken van de informatie is niet uitzonderlijk, omdat de technologie zoals hier ingezet al bekend is uit vergelijkbare protocollen als MQTT. Dat laatste protocol wordt door veel IOT-apparaten gebruikt en lost dit op door sterkere signalen uit te zenden. In de onderhavige toepassing (de app) is het doel echter juist om nabijheid vast te stellen en niet om grotere afstanden te overbruggen. Om deze redenen is het zeer onaannemelijk dat signalen op grote schaal succesvol worden afgevangen.

Het beschikbaar stellen van WiFi in winkelcentra voor het uploaden van gegevens, kan niet leiden tot inzicht in bewegingspatronen en ziekteverschijnselen. Het uploaden van sleutels naar de server zegt op zichzelf niets. Het netwerkverkeer is versleuteld wat een analyse in vergaande mate bemoeilijkt. Er zijn twee soorten uploads: 1) een gebruiker stuurt sleutels (TEKs) en 2) er worden automatisch dummy data (TEKS) verstuurd. In beide gevallen zegt een upload nog niets over een besmetting. In het eerste geval niet, omdat er ook een autorisatiecode van de GGD nodig is, dus als gebruikers zelf TEKs uploaden zonder dat ze ziek zijn zegt dat niets over een besmetting. In het tweede geval is geen verschil merkbaar in het netwerkverkeer tussen een upload door een gebruiker en een 'dummy-upload'. Wie data-analyse uitvoert kan op basis van dat netwerkverkeer daarom niets achterhalen. Reeds gelet hierop kan ook geen informatie over ziekteverschijnselen bij mensen in beeld worden gebracht.

Ook als niet volledig zou kunnen worden uitgesloten dat er met behulp van zo een succesvolle aanval waardevolle informatie over bewegingspatronen kan worden verkregen, dan nog is het niet bijzonder aannemelijk dat de notificatieapp daarvoor, vanuit het perspectief van de aanvaller, het meest geschikte doelwit is. Dit omdat er maar betrekkelijk weinig gegevens in het kader van de app worden verwerkt – zie par. 3 van de DPIA – en ook omdat het betrekkelijk veel moeite kost en specifieke expertise vereist om daaruit die bruikbare informatie te extraheren. Voor een aanvaller die belangstelling heeft voor bewegingspatronen zijn er andere, minder bewerkelijke mogelijkheden om daaraan te komen.

Opgemerkt kan nog worden dat de notificatieapp voor veel gebruikers waarschijnlijk niet de belangrijkste overweging is om Bluetooth aan te zetten. Bij de beantwoording van de volgende vraag, vraag 2e, wordt daarop verder ingegaan.

De mogelijkheid dat in winkelcentra WiFi-signalen worden opgevangen betekent voor de notificatieapp géén specifieke risico's, omdat de app geen gebruik maakt van WiFi. Daarbij moet worden opgemerkt dat WiFi voor tracking effectiever is dan Bluetooth om drie redenen. Ten eerste omdat het een grotere afstand overbrugt. Er zijn voorbeelden dat een WiFi-signaal onder juiste omstandigheden meerdere kilometers kan overbruggen. Ten tweede is de detecteerbaarheid groter dan bij Bluetooth. Tot slot biedt WiFi beter de mogelijkheid om een uniek profiel van de betrokkene op te bouwen op basis van de uitgezonden signalen, omdat het protocol de unieke bekende netwerken met identifier verstuurt. Dat is bij Bluetooth niet het geval.

e. Voor het gebruik van de app is het inschakelen van Bluetooth noodzakelijk. Bluetooth bevat echter enkele bekende kwetsbaarheden en daaraan gerelateerd aanvallen. Dit risico is niet geadresseerd. Daarbij geldt dat dit risico groter is als het gaat om verouderde Androidtoestellen. Kunt u toelichten waarom dit risico niet is onderkend en er geen differentiatie is toegepast naar besturingssystemen van mobiele telefoons?

In de vraagstelling wordt gesproken over Bluetooth. Dit is echter niet de technologie die voor de app wordt gebruikt. Voor deze app wordt gebruik gemaakt van een ander protocol, namelijk Bluetooth Low Energy (zie ook het antwoord op vraag 2d). Alleen modernere (dus niet verouderde) devices kunnen van dit protocol gebruik maken.

In de DPIA wordt ingegaan op de risico's die het gebruik van de app kan hebben voor de rechten en vrijheden van gebruikers ervan. Voor zover er aan het gebruik van Bluetooth Low Energy risico's zijn verbonden, ligt in de rede dat in de DPIA wordt ingegaan op die specifieke risico's die het gebruik van deze technologie voor de gebruiker van de app met zich brengt. In de u toegestuurde DPIA is dat gedaan in bijlage 1, onderdeel 7.

Het ligt minder voor de hand om in te gaan op de risico's die verband houden met het gebruik van Bluetooth Low Energy die niet specifiek zijn voor de app. Om deze reden wordt in de DPIA niet ingegaan op de risico's die het gevolg ervan zijn dat een gebruiker met behulp van Bluetooth beacons kan worden gevolgd, aangezien in verreweg de meeste gevallen de standaardconfiguratie van een device is dat Bluetooth aanstaat, en als dat al niet het geval zou zijn, de meeste gebruikers Bluetooth standaard om andere reden dan de app aanzetten, bijvoorbeeld om muziek te streamen naar een audiosysteem, of om handsfree te bellen, of om gebruik te maken van draadloze oortjes of speakers.[8] Wat dat betreft is het dus niet zonder meer zo dat

[8] Andere voorbeelden van Bluetooth gebruik zijn: toegang tot een woning, draadloze muizen of toetsenborden, koelkasten, acculaders, auto's, boten, televisies, spelcomputers, computers/laptops, smartwatches.

gebruikers, doordat zij gebruik gaan maken van de app, grote extra risico's lopen. En om deze reden ligt niet voor de hand dit risico te typeren als een risico van de app, dat in de DPIA moet worden beoordeeld.

Volledigheidshalve wordt hier nog opgemerkt dat de app slechts werkt op iOS devices waarop de software update van 1 juni 2020 is geïnstalleerd en die maakt dat de API-software kan werken. Voor Android moet minimaal versie 6.0 worden gebruikt. Het veronderstelde beveiligingsrisico verband houdend met het gebruik van verouderde devices is daarom beperkt. Zeker omdat het hier niet regulier Bluetooth betreft, maar het Bluetooth Low Energy-protocol.

f. De DPIA noemt het GGD-portaal maar gaat verder niet in op de verwerkingen die daarin plaatsvinden. Wat is de relatie tussen (verwerkingen binnen) het GGD-portaal en de app? Welke additionele risico's ontstaan, bijvoorbeeld, door verdere verwerkingen van gegevens door het college van Burgemeester en Wethouders voor andere doelen dan infectieziektebestrijding, en hoe zijn deze geadresseerd?

Het GGD-portaal is er uitsluitend voor bedoeld om de autorisatiecode en de eerste ziektedag naar de back-end server te kunnen uploaden. De betreffende twee gegevens worden niet in het GGD-portaal opgeslagen en er wordt ook geen koppeling gemaakt maken met het individu waarop die gegevens betrekking hebben.

Van verdere verwerking van de gegevens die in het kader van de app door onder andere de GGD worden verwerkt, bijvoorbeeld door het college van B&W, is geen sprake. Reeds daarom ontstaan geen met een verdere verwerking verband houdende additionele risico's. Ook overigens is geen sprake van additionele risico's door het bestaan van het GGD-portaal.

g. In de DPIA komt het daadwerkelijke uitoefenen van de rechten van natuurlijke personen en de wijze van organisatie daarvan nauwelijks aan de orde. Aangezien in deze constructie vele organisaties verantwoordelijkheden dragen, kan het onduidelijk zijn bij wie deze rechten uitgeoefend kunnen worden en hoe dit georganiseerd is. Kunt u aangeven welke organisatorische maatregelen zijn getroffen om het uitoefenen van de rechten van natuurlijke personen te waarborgen? Zijn de FG's van de GGD'en ook betrokken geweest bij het opstellen van de DPIA, onderschrijven ze de resultaten, ook die van de FG van VWS?

In de app is, zo blijkt ook uit de DPIA (o.a. par. 16 e.v.), een groot aantal maatregelen genomen waarmee het risico op identificatie van gebruikers effectief, in vergaande mate is beperkt. Veelal zal dan ook sprake zijn van een situatie als bedoeld in artikel 11 lid 1 AVG. Dat laat onverlet dat voor betrokkenen duidelijk moet zijn hoe zij hun rechten op grond van Hoofdstuk III van de AVG kunnen uitoefenen en dat dat

probleemloos moet gaan. De Staat en de GGD-en (waaronder begrepen de GGD-GHOR) maken daar afspraken met elkaar over. Die afspraken zijn thans in de maak.

Uitgangspunt is vooralsnog dat een GGD verantwoordelijk is voor de afhandeling van verzoeken op grond van Hoofdstuk III van de AVG afkomstig van een betrokkene die woonachtig is in (een deel van) een gemeente die binnen het werkgebied van de betreffende GGD valt. Daarbij verleent VWS zo nodig haar medewerking aan het afhandelen van bedoelde verzoeken die verband houden met de app. Indien een betrokkene een verzoek op grond van Hoofdstuk III van de AVG met betrekking tot de app aan VWS richt, verwijst VWS de betreffende betrokkene door naar de GGD die verantwoordelijk is voor de afhandeling van dat verzoek. Betrokkenen zullen vanzelfsprekend worden geïnformeerd over de wijze waarop zij uitvoering kunnen gegeven aan hun rechten op grond van Hoofdstuk III van de AVG. Dat gebeurt in het privacystatement waarnaar in de app wordt verwezen en mogelijk wordt daar ook nog afzonderlijk de aandacht op gevestigd op de website van de app (www.coronamelder.nl). Daarbij zal ook worden verwezen naar de website van de GGD, die een postcode-checker bevat op basis waarvan de betrokkene kan bepalen tot welke GGD hij of zij zich met een AVG-verzoek moet wenden (zie www.ggd.nl/)

.

3. Techniek en framework

a. De door VWS uitgevoerde verwerkingen in en rondom de app leunen volledig op het framework dat is ontwikkeld door Google en Apple. Daarbij geeft VWS aan dat Google en Apple geen verwerker zijn. VWS betoogt dit middels een verwijzing naar een FAQ aangaande het framework van Google en Apple. Kunt u aangeven welke nadere informatie buiten deze FAQ bestaat die het standpunt van VWS in deze onderbouwt? Kunt u deze informatie aan de AP verschaffen?

Voorop staat dat de API die door Google en Apple is ontwikkeld slechts een stuk software betreft. Binnen die software worden geen persoonsgegevens verwerkt, zoals volgt uit de genoemde Exposure Notification, Frequently Asked Questions. Over overige informatie beschikken wij niet. De Ierse DPA (en andere Europese toezichthouders) beschikt wel over aanvullende van Apple en Google verkregen informatie en heeft geen specifieke zorgen geïdentificeerd. Zie de review van de Ierse toezichthouder op de Ierse DPIA op de COVID Tracker App[9]:

> "The DPIA refers to the choice of the data controllers to implement the Google/Apple Exposure Notification System (ENS) to facilate processing of app data on-device. The DPC, in collaboration with EU data protection authorities, is engaged in ongoing dialogue with Google/Apple on the data

[9] https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/DPC%20review%20of%20CTI%20App%20DPIA%20June%202020.pdf.

> protection implications of the ENS. At this time no matters giving rise to significant concern have been identified. However, it is incumbent upon the data controllers to implement the necessary organization and technical measures to ensure the technical specification of any APIs to ensure the security and confidentiality of personal data undergoing processing." (onderstreping toegevoegd)

Vgl. ook de Google COVID-19 Exposure Notications Service Additional Terms[10], waarin Google met zoveel woorden uitspreekt geen persoonsgegevens te willen ontvangen:

> "While end users of your App may provide personal data as part of their use of the App [N.B.: deze optie kent CoronaMelder niet, opm. VWS], you will not share this end-user personal data with Google. (...)" (artikel 3 aanhef en onder b sub vi)

Het Exposure Notification APIs Addendum van Apple bevat een soortgelijk artikel (artikel 3.7)[11]:

> "You will not share any user data with Apple that users of Your Contact Tracing App may provide in connection with their use of such App."

Google heeft op 22 juli jl. aan VWS kenbaar gemaakt dat broncode openbaar gemaakt is[12] en Apple heeft op 23 juli jl. broncode openbaar gemaakt.[13] Er wordt op korte termijn geïnventariseerd of dit een deel van de broncode betreft of de gehele broncode. In beide gevallen wordt er een indringende review gedaan en in het eerste geval zal er ook een nieuwe (aanvullende) review worden verricht als er verdere broncode beschikbaar komt. Vanwege de urgentie van introductie van de app is er niet voor gekozen de (gedeeltelijke) reviews en de eventuele verdere openbaarmaking en de aanvullende reviews daarop van de broncode af te wachten.

b. Pagina 17 van de DPIA lijkt een aantal tegenstrijdigheden te bevatten hetgeen de transparantie niet ten goed komt. Een cruciaal voorbeeld daarvan is: "De implementatiesoftware van het DP3T protocol (de app van VWS) verwerkt de TEKs, DKs en RPIs/contactcodes, én kan een risicoscore bepalen aan de hand van een in de app opgenomen set parameters en weegfactoren." Volgens de door Google en Apple geleverde documentatie (en zoals ook te zien is in de broncode van de VWS app) is de app zelf enkel verantwoordelijk voor het opvragen en uploaden van de TEKs en de download van de DKs. Alle andere verwerkingen worden in het framework van Google en Apple gedaan, afgeschermd van de app. Kunt u dit toelichten?

---

10 https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf.
11 https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf.
12 Een en ander onder verwijzing naar https://github.com/google/exposure-notifications-internals.
13 https://developer.apple.com/exposure-notification/.

Het is juist dat de app zelf enkel verantwoordelijk is voor het opvragen en uploaden van de TEKs en de download van de DKs. Dit zal in de DPIA worden verduidelijkt door de passage "(de app van VWS)" te verwijderen.

c. De ontwikkelaars van DP-3T stellen: "We also strongly believe that Apple and Google should adopt our subsequent enhancements, detailed in our white paper, that increase user privacy. We also strongly encourage both companies to allow an external audit of their code to ensure its functionality corresponds to its specification."2 Kunt u toelichten in hoeverre de aanbevelingen van DP-3T door VWS worden onderschreven en deze in het framework van Google en Apple zijn opgenomen?

De opmerkingen waar u in de vraagstelling op doelt, komen uit een al wat ouder readme document van DP-3T van halverwege mei. Dit volgde op het vrijgeven van de eerste software van Google en Apple. Hierop is een discussie ontstaan, waarbij DP-3T toen van mening was dat er een beter design mogelijk was. Het nadeel van dit design was echter dat er substantieel meer bandbreedte zou worden gebruikt, met als gevolg meer netwerkverkeer. DP-3T heeft later het eigen standpunt herzien en een design versie 3 toegevoegd wat zij het 'hybrid design' is gaan noemen. In de laatste versie van de whitepaper zegt DP-3T daarover:

> "This design is very similar to the Google/Apple design."

Het hybride model, het design versie 3, is toegevoegd aan de whitepaper. Inmiddels is DP-3T in mei zélf overgestapt op het GAEN[14] protocol.[15] DP-3T heeft een set adviezen en best practices voorgesteld die richting geven aan hoe de app het beste kan worden gebouwd met gebruik van de API-software. Nederland onderschrijft die best practices en adviezen en heeft daar ook opvolging aan gegeven.

Nederland werkt met andere landen actief samen in het Europese e-Health-netwerk, onder meer met als doel om met de daarin participerende landen[16] te werken aan (ook verdere) verbeteringen van DP-3T. Google en Apple volgen deze ontwikkelingen nauwgezet. Voor zover het adviezen en best practices zijn die de API-software raken kunnen die door Google en Apple in die software worden opgenomen. Een voorbeeld ter illustratie: Nederland heeft ervoor gepleit om een TEK niet vast te houden tot middernacht en de hele dag geldig te laten zijn, maar deze te splitsen na upload. Hierdoor versnelt het proces van het waarschuwen van mensen die een verhoogd risico op besmetting hebben. Vanaf versie 1.5 gaan Apple en Google deze lang gekoesterde wens honoreren. Op onze GitHub[17] is te lezen wat de verschillen hierbij zijn. Google heeft bij ons aangegeven dat een van de redenen om dit te wijzigen, ons verzoek is geweest.

---

14 Google Apple Exposure Notification (de Google-Apple API-software).
15 Bijv. https://github.com/DP-3T/dp3t-sdk-android/commit/1362d81e26d41bffae4bae51ad8ad84372dfe768.
16 Waaronder Duitsland, Ierland, Oostenrijk, Estland, Italië en Noorwegen.
17 https://github.com/minvws/nl-covid19-notification-app-coordination/blob/master/architecture/Key%20Upload%20Process.md.

d. Zijn de genoemde rapportages aangaande pentesten, code reviews, code quality en code test coverage voorhanden? Is deze informatie voorhanden met betrekking tot zowel het framework van Google en Apple, de app, en de backend? Kunt u deze rapportages de AP verschaffen?

De rapportages zijn nog niet beschikbaar. Zodra dat wel het geval is worden deze openbaar gemaakt, zodat er publiekelijk gecontroleerd kan worden dat deze testen zijn doorlopen en aanbevelingen zijn opgevolgd. Voor de thans (wel) beschikbare documentatie wordt verwezen naar: www.rijksoverheid.nl/documenten/kamerstukken/2020/07/16/kamerbrief-over-landelijke-introductie-coronamelder.

e. Kunt u aangeven welke juridische entiteit, met vestigingsgegevens, er verantwoordelijk is voor wat genoemd wordt het framework van Google en Apple? Indien er sprake is van meerdere entiteiten, wat is dan de verhouding tussen deze entiteiten en wie is primair verantwoordelijk?

De API-software ofwel het framework is gezamenlijk ontworpen door Google LLC (1600 Amphitheatre Parkway, Mountain View, California 94043, United States) en Apple INC. (1 Apple Park Way in Cupertino, California, United States). Google heeft de software geschreven voor het Android platform, terwijl Apple de software heeft geschreven voor het iOS-platform.

Dit is nadrukkelijk met Google en Apple besproken en is ook af te leiden uit de bij vraag 3a genoemde COVID-19 Exposure Notications Service Additional Terms van Google (en meer in het bijzonder de daarboven hangende Google APIs Terms of Service[18]) en het Exposure Notification APIs Addendum van Apple (en meer in het bijzonder de daarboven hangende Apple Developer Overeenkomst[19])

Onder verwijzing naar par. 5 (p. 17) van de DPIA en het antwoord op vraag 3a hiervoor wordt benadrukt dat het hierbij níet gaat om *verwerkings*verantwoordelijkheid van Google en Apple, maar om de verantwoordelijkheid voor de door deze bedrijven geschreven software.

---

18 https://developers.google.com/terms.
19 https://developer.apple.com/terms/apple-developer-agreement/Apple-Developer-Agreement-Dutch.pdf.

Tot slot

Ik vertrouw erop u met deze antwoorden voldoende te hebben geïnformeerd. Heeft u vragen naar aanleiding van deze antwoorden? Dan kunt u hierover met contact opnemen met de Chief Privacy Officer, Jaap Hoorenman.

MCM Programmadirecteur Realisatie Digitale Ondersteuning