Second Opinion DPIA CoronaMelder App

19 augustus 2020

Definitief

Second Opinion DPIA CoronaMelder App

Auteur
mr. drs. Jeroen Terstegge CIPP/E, partner
Privacy Management Partners

Opdrachtgever
Ministerie van Volksgezondheid, Welzijn en Sport

19 augustus 2020

Inhoud

Management samenvatting

Het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) heeft Privacy Management Partners (PMP) gevraagd om een second opinion te geven op de concept-gegevensbeschermingseffect-beoordeling (DPIA) van de CoronaMelder app (versie 13 augustus 2020).

Meer in het bijzonder heeft VWS ons de volgende vragen gesteld:

1. Zijn de gegevens die door de app en de backend verwerken persoonsgegevens?
   Antwoord: Ja, maar als Aanbeveling nr. 2 wordt overgenomen niet meer.

2. Uitgangspunt van de DP3T referentiearchitectuur is dat er geen persoonsgegevens worden verwerkt. Waar zit het verschil in de Nederlandse implementatie en de referentiearchitectuur van DP3T?
   Antwoord: Het belangrijkste verschil is dat de Nederlandse implementatie – uit veiligheidsredenen – de IP-adressen van de apps die contact maken met de backend 7 dagen bewaart. Hoewel de gegevens (TEKs) in de backend niet direct herleidbaar zijn tot een gebruiker, zijn ze dat wel in combinatie met het IP-adres waar ze afkomstig van zijn. Het feit dat er een afspraak is/wordt gemaakt met het CIBG om de IP-adressen functioneel gescheiden op te slaan van de overige gegevens, maakt dat niet anders. Om dit te verzekeren is – gelet op de jurisprudentie van het Hof van Justitie van de Europese Unie – wetgeving nodig die herleidbaarheid verbiedt (zie hieronder Aanbeveling nr.2).

3. Kan toestemming in dit geval een grondslag zijn voor de app door de overheid?
   Antwoord: Ja, maar dit is niet de meest logische verwerkingsgrondslag (zie hieronder Aanbeveling nr. 1).

4. Op welk deel van de verwerking is de AVG van toepassing en welk deel niet?
   Antwoord: De AVG is alleen van toepassing op de gegevensverwerking in de backend (tenzij aanbeveling nr. 2 wordt overgenomen). De AVG is vanwege het persoonlijk gebruik niet van toepassing op de gegevensverwerking door de gebruikers.

5. Wie is verwerkingsverantwoordelijk voor welk onderdeel van de verwerking?
   Antwoord: De Minister van VWS is verwerkingsverantwoordelijke voor de gegevens die onder het beheer van het CBIG worden verwerkt (tenzij aanbeveling nr. 2 wordt overgenomen). De GGD is verwerkingsverantwoordelijke voor de uploadt van de gegevens uit het GGD Portaal naar de backend server. De gebruiker is verwerkingsverantwoordelijke voor de uitwisseling van de RPI's met andere gebruikers via Bluetooth (maar o.g.v. art. 2(2)(c) AVG valt dit deel van de gegevensverwerking buiten de scope van de AVG).

6. Zijn u verder zaken opgevallen aan de DPIA die belangrijk zijn te melden?
   Antwoord: Zie hieronder.

Risico's binnen de informatie-infrastructuur

Er is veel aan gedaan om de privacy van de gebruikers in het gegevensproces te waarborgen, zowel in de app zelf als in de backend. Gekozen is voor een decentraal model gebaseerd op de DP3T architectuur, waarbij een minimale, in de praktijk onherleidbare, gegevensset centraal wordt verwerkt en waarbij het grootste deel van de gegevensverwerking decentraal plaatsvindt in het apparaat van de gebruiker.

Specifieke maatregelen ter bescherming van de privacy van de gebruiker zijn:

- Het gebruik van *Rolling Proximity Indicators* (RPI's) met een korte levensduur (10 tot 20 minuten), zodat niet iedereen met wie men in contact komt dezelfde RPI's ontvangt van dezelfde gebruiker.
- Het gebruik van dagelijks wisselende *Temporary Exposure Keys (TEK's)*, die de RPI's en de DK's genereren.
- Het gebruik van pseudo-MAC adressen die elke 10-20 minuten veranderen.
- Versleuteling van de gegevens op de telefoon (standaard Apple/Google functionaliteit).
- Het beperken van de dataset (TEK's/RPI's) op de telefoon tot 14 dagen (wat gelijk loopt met het krijgen van Covid-19 verschijnselen).
- Het sturen van *dummy data* naar de server, zodat iemand die het verkeer onderschept de echte data niet van de dummy data kan onderscheiden.
- De gegevens op de back end server worden niet langer dan 24 uur bewaard (om technische redenen).
- De IP-adressen worden bij binnenkomst op de backend server gescheiden van de TEK's, waardoor herleidbaarheid in de praktijk zo goed als onmogelijk is.
- Het direct weer verwijderen van de *Diagnosis Keys* (DK's) op de telefoon na berekening van het besmettingsrisico.
- Het direct weer verwijderen van de melding die de app genereert, zodat deze niet door derden kan worden ingezien.
- Het onmogelijk maken van een screenshot van de melding die de app genereert, zodat deze niet door derden kan worden ingezien.
- Het verwijderen van de gegevens zodra de app wordt gedeïnstalleerd.
- Een groot aantal informatiebeveiligingsmaatregelen gericht op het voorkomen van ongeautoriseerde onderschepping, toegang tot, verlies van of bewaren van de gegevens.
- Er worden op geen enkel moment door de app locatiegegevens of direct identificerende gegevens zoals naam of telefoonnummer verwerkt.
- Het maken van afspraken met het CIBG en het sluiten van een verwerkersovereenkomst met KPN.
- Het optuigen van een apart GGD Portaal, waardoor de GGD geen rechtstreekse toegang tot de backend server nodig heeft en dus niet bij de geüploade gegevens kan komen.

In de app en in de backend is gestreefd naar maximale dataminimalisatie (*privacy by design*). Ook de overige algemene beginselen van gegevensbescherming zoals die bijvoorbeeld in artikel 5 AVG zijn vastgelegd (beveiliging, doelbinding, transparantie en accountability) worden in voldoende mate nageleefd.

Wij beoordelen de maatregelen die genomen zijn binnen de informatie-infrastructuur van de CoronaMelder app (app en backend) daarom als toereikend om te garanderen dat de rechten en vrijheden van de gebruikers jegens de direct betrokken instanties (GGD, VWS/CIGB/KPN), andere gebruikers en kwaadwillenden niet geschaad worden. Hoewel een aantal punten voor verbetering vatbaar zijn (zie met name Aanbeveling nr.2 hieronder), zien wij qua gegevensbescherming geen dringende redenen om de landelijke uitrol van de app uit te stellen.

Risico's buiten de informatie-infrastructuur

In de DPIA komen de risico's die buiten de informatie-infrastructuur liggen niet of nauwelijks aan bod. Dit wordt wellicht mede ingegeven door het feit dat het *Toetsmodel Gegevensbeschermingseffect-beoordeling Rijksdienst* daar niet voor geschikt is. Wij noemen hier de volgende risico's:

- **Extra belasting voor mensen die niet thuis kunnen werken.** Het gebruik van de app heeft mogelijk extra nadelige effecten op mensen die niet in de mogelijkheid zijn om thuis te werken en derhalve vaker langdurig in contact komen met andere mensen, zoals winkelpersoneel, zorgmedewerkers, horecapersoneel en treinconducteurs. Zij zullen dus ook vaker dan gemiddeld een melding krijgen. Dit kan allerlei negatieve effecten hebben, zoals het negeren van blootstellingssignalen wegens gewenning (gezondheidsrisico) en het verlies van arbeidsproductiviteit wegens het ondergaan van extra coronatesten en zelfisolatie tot de uitslag daarvan bekend is (inkomensrisico).

- **Onomkeerbaarheid technologische ontwikkelingen.** Hoewel het de bedoeling is dat de app tijdelijk wordt ingezet en zodra het mogelijk is weer gedeactiveerd wordt (het Google/Apple Exposure Notification framework kan ook regionaal worden uitgezet), zijn langetermijneffecten niet uit te sluiten. In het verleden hebben we gezien dat tijdelijke privacyinbreuk makende maatregelen een permanent karakter krijgen.[1] Maar zelfs als de overheid de app deactiveert, is het niet ondenkbaar dat er een nieuwe toepassing wordt gevonden voor deze contact tracing functionaliteit. En met de toestemming van de Telecommunicatiewet in de hand staat er juridisch weinig in de weg aan dergelijke nieuwe toepassingen. M.a.w., de onbedoelde gevolgen van een contact tracing app op de maatschappij zijn nog niet of nauwelijks te overzien.

Aanbevelingen

1. **Maak een wettelijke regeling om een grondslag voor de gegevensverwerking te verkrijgen.** Omdat de app ondersteunend is aan de bron- en contactonderzoek, is – bij gebrek aan een wettelijke taak van de Minister – een wettelijke regeling nodig die de Minister/CIBG de mogelijkheid geeft om de gegevens van burgers te verwerken. Hoewel toestemming mijns inziens niet onmogelijk is (ook de European Data Protection Board (EDPB) sluit dat in haar opinie van 21 april 2020 niet uit), is het niet de meest sterke verwerkingsgrondslag voor een gegevensverwerking door de overheid. De overheid werkt in een democratische rechtsstaat immers op basis van democratisch toegewezen taken en bevoegdheden. Toestemming moet niet worden verward met vrijwilligheid. Bij toestemming is de verwerking volledig afhankelijk van de wil van de burger. Dit suggereert dat de overheid geen noodzakelijk en zwaarwegend belang heeft bij de gegevensverwerking, terwijl de huidige gezondheidscrisis juist een argument is om het algemeen belang te benadrukken. Een ander argument waarom toestemming niet voor de hand ligt, is dat VWS de privacybescherming zo ver in de CoronaMelder infrastructuur heeft doorgevoerd, dat intrekking van de toestemming feitelijk onmogelijk is omdat de gegevensverwerking van een besmette gebruiker die zijn/haar TEK's heeft geüpload niet kan worden gestopt in de backend (en dat zou bij intrekking van toestemming wel moeten). De gebruiker kan uiteraard de app deïnstalleren, maar dat raakt vooral de vrijwilligheid van de gegevensuitwisseling met andere gebruikers en het ophalen van de DK's uit de backend, niet de gegevensverwerking in de backend zelf.

2. Maak een wettelijk verbod op nevengebruik van de gegevens. Omdat het CIBG een uitvoeringsorganisatie is van het Ministerie van VWS, is het CIGB qua AVG niet gescheiden van de Minister. Interne afspraken tussen het kerndepartement en het CIBG zijn onvoldoende zelfstandige waarborg voor gebruik van de gegevens door de overheid voor andere doeleinden. Om de privacy van de geïnfecteerde gebruiker optimaal te beschermen, dient wettelijk geregeld te worden dat het de

[1] Zo werd 100 jaar geleden de paspoortplicht als noodmaatregel werd ingevoerd om paal en perk te stellen aan de instroom van immigranten in de VS na de Eerste Wereldoorlog. En na de aanslagen van 9/11 werd de beperkte identificatieplicht in Nederland razendsnel omgezet in een volledige identificatieplicht.

Minister van VWS verboden is om de IP-adressen te koppelen dan wel te laten koppelen aan de TEK's van de gebruiker dan wel een ander, zoals de GGD, daartoe in staat te stellen. Ook moet het wettelijk verboden worden om de gegevens te exporteren en/of selectietechnieken toe te passen op de TEK's en zo gebruikers uniek aan te wijzen in de database.

3. Creëer wettelijke waarborgen tegen drang om de app te installeren. Omdat het gebruik van de app vrijwillig is, is de Minister voornemens om in de wet op te nemen dat niemand kan worden gedwongen de app te installeren *(dwang*). Om te voorkomen dat mensen worden geweerd van hun werk, openbaar vervoer, kerk of andere gelegenheden, hoort daar een spiegelbeeldig verbod bij: een verbod om toegang tot gebouwen en evenementen afhankelijk te maken van het geïnstalleerd hebben van de app (*drang*).

4. Maak afspraken met Apple en Google over het einde van de app. Maak afspraken met Apple en Google om het Exposure Notification framework voor Nederlandse gebruikers op verzoek van de Minister uit te zetten als de Coronacrisis voorbij is (en eventueel weer aan te zetten als dat nodig mocht zijn). Verdergaande afspraken of wetgeving om meer grip te krijgen op het *Google Apple Exposure Notification framework*, zoals de Autoriteit Persoonsgegevens voorstaat[2], lijkt mij niet nodig. De publieke uitingen van Apple en Google zijn zodanig dat als zij daar van zouden afwijken, zij zich zowel in de Nederland als in de VS zouden blootstellen aan zowel bestuursrechtelijke handhaving (AP/FTC) als zware civielrechtelijke schadevergoedingsacties (WAMCA/class actions).[3]

5. Controleer het Google/Apple Exposure Notification framework op veranderingen. De app drijft op het Google/Apple Notification Framework. Apple en Google hebben aangekondigd hun framework verder te willen doorontwikkelen. Eventuele wijzigingen in het framework evenals updates van de besturingssystemen Android en iOS moeten worden geëvalueerd op de effecten op de gebruikers van de app en waar nodig moeten aanvullende maatregelen worden genomen. Ook dient de DPIA in dat geval te worden aangepast. In het uiterste geval moet de app in zo'n geval buiten werking worden gesteld.

6. Informeer de gebruikers hoe ze het verzamelen van telemetriegegevens door Google in Android kunnen uitzetten. De CoronaMelder app werkt in Android niet zonder Google Play Services, waardoor Google in staat is om telemetriegegevens te verzamelen over het gebruik van het *Exposure Notification framework* (NB. Google verzamelt geen besmettingsgegevens). Dit is overigens niet specifiek voor de CoronaMelder app. Wel kan de gebruiker in het Instellingenmenu van de Android telefoon (*Gebruik & Diagnostische gegevens)* het verzamelen van diagnostische gegevens over het gebruik van de app en het *Exposure Notification framework* uitzetten. Omdat deze functie nogal verstopt zit, is het mijns inziens logisch dat dit in de app onder het kopje Veelgestelde vragen wordt uitgelegd.

7. Informeer de gebruikers in de Veelgestelde vragen over het risico op herleidbaarheid door een andere gebruiker. Een verstandig adagium in het privacy- en gegevensbeschermingsrecht is het principe van *surprise minimization*. Al zal de gebruiker in de meeste gevallen volstrekt anoniem blijven, ook dan is het verstandig om mensen te waarschuwen dat anonimiteit tussen gebruikers niet in alle gevallen gegarandeerd kan worden. Daarbij moet worden uitgelegd onder welke omstandigheden andere gebruikers tot een identificatie kunnen komen.

---

[2] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-privacy-corona-app-gebruikers-nog-onvoldoende-gewaarborgd

[3] https://tweakers.net/nieuws/170932/stichting-dient-massaclaim-in-tegen-salesforce-en-oracle-wegens-overtreden-avg.html

Inleiding

Het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) heeft Privacy Management Partners (PMP) gevraagd om een second opinion te geven op de concept-gegevensbeschermingseffect-beoordeling (DPIA) van de CoronaMelder app (versie 13 augustus 2020).

PMP heeft deze second opinion uitgevoerd met de volgende scope:

- De begrijpelijkheid van de beschrijving van de gegevensverwerking.
- De volledigheid en aannemelijkheid van de conclusies over de risico's voor de gebruikers.
- De volledigheid en juistheid van de juridische conclusies.
- De redelijkheid van de getroffen maatregelen.

Meer in het bijzonder heeft VWS ons de volgende vragen gesteld:

1. Zijn de gegevens die door de app en de backend verwerken persoonsgegevens?
2. Uitgangspunt van de DP3T referentiearchitectuur is dat er geen persoonsgegevens worden verwerkt. Waar zit qua AVG het verschil in de Nederlandse implementatie en de referentiearchitectuur van DP3T?
3. Kan toestemming in dit geval een grondslag zijn voor de app door de overheid?
4. Op welk deel van de verwerking is de AVG van toepassing en welk deel niet?
5. Wie is verwerkingsverantwoordelijk voor welk onderdeel van de verwerking?
6. Zijn u verder zaken opgevallen aan de DPIA die belangrijk zijn te melden?

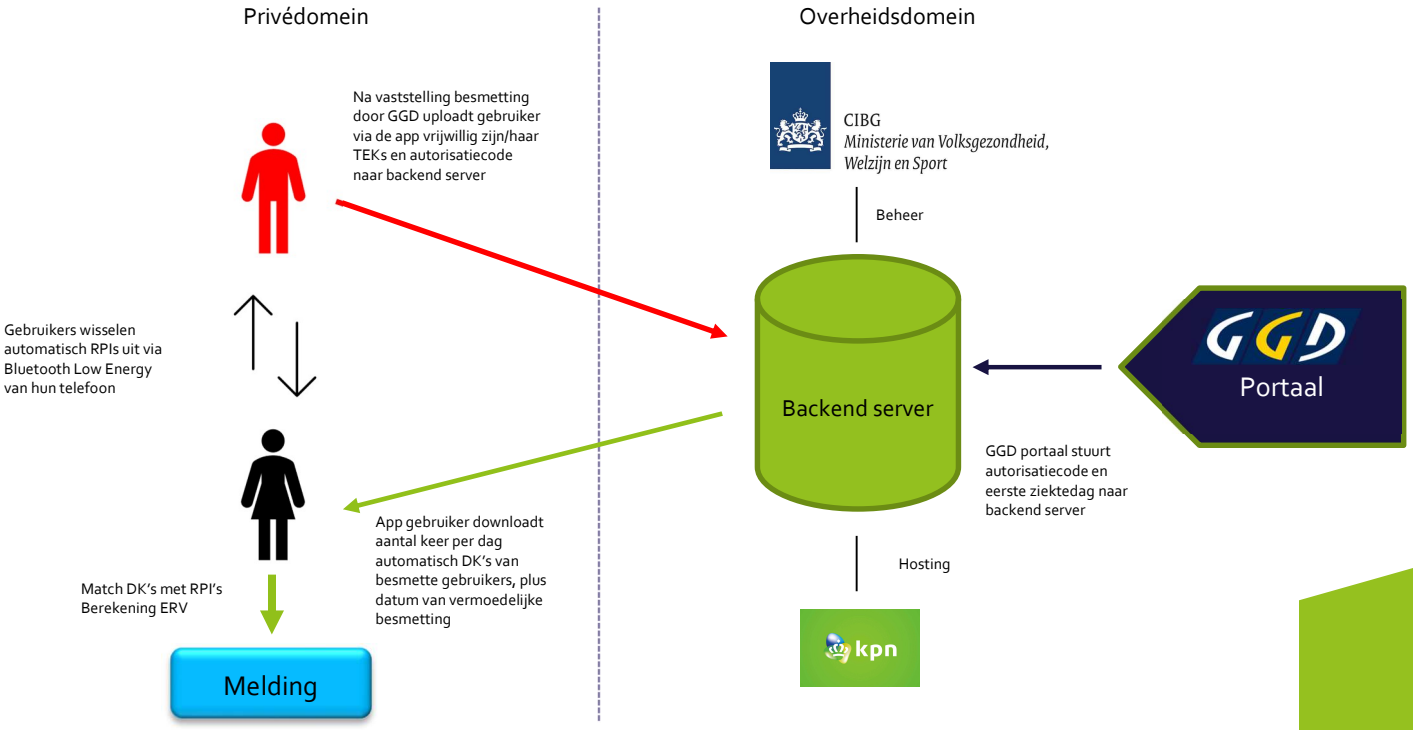
De antwoorden op deze vragen treft u in Hoofdstuk 2 van dit rapport aan.

1. Opzet van de gegevensverwerking

De gegevensverwerking bestaat uit de volgende elementen:

- De CoronaMelder app op de telefoon van de gebruiker;
- De backend server bij CBIG/KPN;
- Het Google Apple Exposure Notification Framework (GAEN), inclusief de API, dat werkt op het besturingssysteem van de telefoon van de gebruiker.

De samenhang van deze elementen is in het onderstaande plaatje grafisch weergegeven:



TEK *Temporary Exposure Key*, een gepseudonimiseerde identificatiesleutel van een gebruiker die elke dag opnieuw volledig willekeurig wordt gegenereerd. Wordt 14 dagen op de telefoon bewaard en na upload 24 uur op de backend server.

RPI *Rolling Proximity Indicator*, een gepseudonimiseerde identificatiesleutel van een gebruiker die iedere 10-20 minuten volledig willekeurig wordt gegenereerd. Wordt 14 dagen op de telefoon bewaard.

DK *Diagnosis Key*, een gepseudonimiseerde identificatiesleutel op basis van de TEKs van een geïnfecteerde gebruiker die door de backend server naar alle gebruikers wordt gestuurd. Wordt na de match en berekening ERV direct van de telefoon verwijderd.

ERV *Exposure Risk Value*, een op basis van de gedownloade DK's en verzamelde RPI's door het GAEN framework berekende waarde waarmee het risico van besmetting wordt uitgedrukt (hoog, midden, laag), waarbij tevens rekening wordt gehouden met de parameters die door VWS zijn vastgesteld.

- *Installatiefase*

De installatie van de CoronaMelder app vindt plaats via de App Store van Apple of de Play Store van Google. De app vraagt niet om persoonsgegevens zoals naam of telefoonnummer. In die fase worden geen gegevens uitgewisseld met de overheid.

Echter, de installatie vanuit de App Store cq Play Store betekent wél dat de gebruiker een aantal persoonsgegevens deelt met Apple en Google (net als bij de installatie van iedere andere app). De DPIA laat dit aspect buiten beschouwing, wellicht mede omdat het niet tot de scope van de hierboven geschetste gegevensverwerking behoort. Het is echter, gelet op het feit dat de overheid een app uitrolt die door de burger gebruikt wordt, nodig om te erkennen (en eventueel te accepteren) dat de burger daarmee als klant van de Apple en Google buiten de app en het GAEN framework om aanvullende gegevens prijs moet geven aan commerciële partijen. Dit risico is niet specifiek voor de CoronaMelder app, maar geldt voor alle apps die de Nederlandse overheid uitrolt. Hoewel het installeren van een app buiten de stores om technisch mogelijk is, is dit voor veel mensen waarschijnlijk te ingewikkeld en daarmee niet gebruikersvriendelijk. Daarmee is dit privacyrisico inherent aan de uitrol van de app op een telefoon van de gebruiker.

Onderzoekers van het Trinity College in Dublin wijzen er in een recente publicatie ook op dat tijdens het gebruik van de app door Google **telemetriegegevens** (niet te verwarren met de voornoemde blootstellingsgegevens) over het gebruik van het GAEN framework kunnen worden verzameld.[4]

> When the "Usage & diagnostics" option in Google Play Services is enabled (which it is by default), then telemetry data on GAEN operation is shared with Google. The data that Google Play Services sends to Google in these connections also includes, amongst other things, the phone IMEI, the handset hardware serial number, the SIM serial number, the handset phone number, the WiFi MAC address and the user email address.

Hoewel deze gegevensdeling met Google door de gebruiker handmatig is uit te zetten via het Instellingen-menu van de Android telefoon, wijzen de onderzoekers erop dat deze functie *by default* aan staat. Het scherm om de gegevensdeling uit te zetten zit ook goed verstopt in het Instellingen-menu van Android telefoons (Instellingen --> Google --> [drie puntjes in de rechterbovenhoek]. **Met de onderzoekers ben ik daarom van mening dat VWS de gebruikers in de app en de privacyverklaring expliciet over deze mogelijke gegevensverzameling door Google moet informeren zodat ze de mogelijkheid hebben om Gebruik & Diagnostische Gegevens uit te zetten en het delen van de telemetriegegevens met Google te voorkomen c.q. te stoppen.**

Aanbeveling

Informeer de gebruikers hoe ze het verzamelen van telemetriegegevens door Google in Android kunnen uitzetten. Omdat de functie *Gebruik & Diagnostische gegevens* nogal verstopt zit, is het mijns inziens logisch dat dit in de app onder het kopje Veelgestelde vragen wordt uitgelegd.

Het verzamelen van telemetriegegevens over het gebruik van het GAEN framework is qua AVG overigens volledig de verantwoordelijkheid van Google, niet die van VWS.

[4] Leith & Farrell, *Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps* (Juli 2020), https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf

Hoewel de DPIA daar helaas geen melding van maakt, verzamelt de CoronaMelder app zelf overigens géén telemetriegegevens (zoals in sommige andere landen wel het geval is). Dit is een bewust keuze van VWS (privacy-by-design).

- *Uitwisselingsfase*

De uitwisseling van de RPI's tussen gebruikers is een functie van het GAEN framework. Door de app te installeren en de app toegang te geven tot Bluetooth (BLE) gaat de telefoon automatisch RPI's uitwisselen met andere gebruikers. Dit is een gegevensverwerking die geheel in het **privédomein van de gebruikers** plaatsvindt, d.w.z., de overheid (VWS, CIBG, GGD) is niet betrokken bij dit deel van de gegevensverwerking en deze kan daar – anders dan het uitrollen van de app – ook geen invloed op uitoefenen. Het is daarom vanuit het oogpunt van *verticale privacybescherming*[5] niet nodig om een rechtvaardiging te vinden als bedoeld in de Grondwet, het EVRM of het Europese Handvest voor inmenging in de persoonlijke levenssfeer van de gebruikers als de gebruikers tussen elkaar gegevens uitwisselen met een door de overheid gebouwde en uitgerolde app. VWS heeft hier slechts de rol van uitgever van software.[6]

De *horizontale privacy*[7] is in deze fase wél in het geding. Gebruikers verzamelen immers elkaars RPI's. Echter, omdat de uitwisseling geheel vrijwillig gebeurt (het gebruik van de app is immers vrijwillig), is de inbreuk die met het verzamelen van de RPI's gepaard gaat niet onrechtmatig. Als uitgever van de app ligt het voor de hand dat VWS de gebruiker over dit aspect dient te informeren, inclusief wat de gebruiker moet doen als hij/zij dat niet (meer) wil. Deze informatie is zowel in de app als in de privacyverklaring beschikbaar.

Omdat deze gegevensverwerking in de privésfeer plaatsvindt, betekent dit qua AVG dat de persoonsgegevens (want dat zijn de RFI's) die de gebruikers over elkaar verwerken onder de uitzondering voor persoonlijk gebruik (art. 2(2)(c) AVG) vallen. **De gebruiker hoeft zich dus niet aan de AVG te houden als hij/zij RFI's over andere gebruikers verzamelt.**

Dit onderscheid tussen verticale en horizontale privacy wordt in de DPIA onvoldoende onderkent[8]. Dit leidt vervolgens tot conclusies over de AVG en rol van de Minister die onjuist en onnodig zijn (daarover meer in Hoofdstuk 2).

In de Uitwisselingsfase worden uitsluitend RPI's verzameld. De app verzamelt geen locatiegegevens.

- *Validatiefase*

In de validatiefase verstuurt een gebruiker die positief getest is op het SARS-CoV-2 virus (*Coronavirus*) vrijwillig vanuit de app zijn/haar TEK's samen met zijn/haar autorisatiecode naar de backend server. Dit kan pas nadat de gebruiker zijn/haar autorisatiecode telefonisch aan de GGD heeft medegedeeld. Dit proces is nodig om te zorgen dat er geen valse meldingen worden gedaan, althans dat er geen DK's worden verstuurd op basis van valse meldingen. DK's kunnen dus pas worden aangemaakt als de

---

[5] Met 'verticale privacy' wordt gedoeld op de inmenging van de overheid in de persoonlijke levenssfeer van de burger. De bescherming van de burger tegen deze inmenging is vastgelegd in art. 10 Grondwet, art. 8 Europees Verdrag voor de Rechten van de Mensen en art. 7 Handvest van de Grondrechten van de Europese Unie.

[6] Uitgever van software is een civielrechtelijke rol, waar overigens wel verantwoordelijkheden op het gebied van het consumentenbeschermingsrecht bij kunnen komen kijken. Het gaat in het kader van deze second opinion te ver om hier verder op in te gaan.

[7] Met 'horizontale privacy' wordt bedoeld de privacy tussen burgers onderling. Dit wordt via de zogeheten *horizontale werking* van het grondrecht op bescherming van de persoonlijke levenssfeer gehandhaafd door de overheid (de rechter) in de vorm van het onrechtmatigedaadsrecht en het strafrecht.

[8] Dit wordt overigens mede veroorzaakt door het gebruikte DPIA-template, het *Toetsmodel Gegevensbeschermingseffectbeoordeling Rijksdienst*, dat door het Rijk verplicht moet worden gebruikt, maar dat volstrekt ongeschikt is voor een goede beoordeling van de onderhavige risico's.

server de autorisatiecode zowel vindt in de upload van de geïnfecteerde gebruiker als in het GGD portaal.

De backend server fungeert als een soort 'black box'. De GGD heeft geen toegang tot de gegevens die op de backend server worden verwerkt. CBIG heeft als beheerder van de infrastructuur wel (technische) toegang tot de gegevens, maar er zijn/worden met het CIBG afspraken gemaakt dat zij zich geen toegang verschaffen tot de TEK's. Dit risico en de daarbij behorende maatregelen staan beschreven in nr. 26 van de Bijlage 1 van de DPIA.

Het IP-adres waarmee telefoon van de geïnfecteerde gebruiker verbinding maakt met de backend server wordt door het CIBG functioneel gescheiden van de TEK's opgeslagen en zeven dagen bewaard. Het doel hiervan is dat dit het CIBG in staat stelt de infrastructuur te beveiligen tegen aanvallen van buitenaf.

Hoewel de DPIA tot de conclusie komt dat het risico van toegang door het CIBG laag is, is het belangrijk om te begrijpen dat **de geüploade TEK's bij de *HUIDIGE* maatregelen kwalificeren als persoonsgegevens in de zin van de AVG** (daarover meer in Hoofdstuk 2).

Aanbeveling

Om de privacy van de geïnfecteerde gebruiker optimaal te beschermen, dient wettelijk geregeld te worden dat het de Minister van VWS verboden is om de IP-adressen te koppelen dan wel te laten koppelen aan de TEK's van de gebruiker dan wel een ander, zoals de GGD, daartoe in staat te stellen. Ook moet het wettelijk verboden worden om de gegevens te exporteren en/of selectietechnieken toe te passen op de TEK's en zo gebruikers uniek aan te wijzen in de database.

Toelichting: Omdat het CIBG een uitvoeringsorganisatie is van het Ministerie van VWS, is het CIGB qua AVG niet gescheiden van de Minister. Dit betekent dat het CIGB, anders dan de DPIA suggereert géén verwerker is en dat de Minister formeel dus geen verwerkersafspraken kan maken met het CIGB (een verwerker is immers altijd een externe dienstverlener, zoals in casu KPN). Interne afspraken tussen het kerndepartement en het CIBG zijn onvoldoende zelfstandige waarborg voor gebruik van de gegevens door de overheid voor andere doeleinden. Daarom dient dit bij wet of een andere verbindende regeling te worden geregeld, zodat dit ook extern gehandhaafd kan worden.

- *Koppelingsfase*

De app op de telefoon van de gebruikers maakt een aantal keren per dag contact met de backend server om DK's te downloaden. Omdat bij het huidige stelsel maatregelen de geüploade TEK's persoonsgegevens zijn, zijn de DK's dat ook. **Daarom geldt het advies om de Minister te verbieden om de TEK's tot personen te herleiden ook voor de DK's.**

Aan de kant van de gebruikers die de DK's ontvangen hebben de DK's een zeer korte levensduur. De DK's worden verwijderd zodra de *Exposure Risk Value* is berekend door het GAEN framework[9]. Het GAEN Framework berekent aan de hand van de parameters die door VWS in overleg met het RIVM, de GGD en het OMT zijn vastgesteld en in de app zijn ingebouwd het blootstellingsrisico van de

[9] De veelbesproken API (*application programming interface*) is onderdeel van het GAEN framework en zorgt ervoor dat de CoronaMelder app met het GAEN framework kan communiceren. De API communiceert niet met de servers van Apple en Google. Alleen apps van officiële instanties hebben toegang tot de API. Daardoor is in beginsel uitgesloten dat derden software ontwikkelen die ook gebruik maakt van de API en dat derden zich op die manier toegang verschaffen tot de blootstellingsgegevens.

bewaarde contacten. Alle functionaliteit voor het berekenen van blootstellingsrisico's is dus beschikbaar in de telefoon van de gebruiker. Er wordt bij het berekenen van de blootstelling geen verbinding gelegd met de servers van Apple of Google. Apple en Google hebben ook verklaard geen gegevens te willen ontvangen van de app.

> Apple Exposure Notification Addendum
> Art. 3.7 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 COVID-19 Exposure Notifications Service Additional Terms
> Art. 3.b.vi. While end users of your App may provide personal data as part of their use of the App, you will not share this end-user personal data with Google.

- Notificatiefase

Indien de berekende *Exposure Risk Value* de door VWS vastgestelde grenswaarde overschrijdt, genereert de app een melding op het scherm van de telefoon van de gebruiker. Daarin staat dat hij/zij mogelijk besmet is met het SARS-CoV-2 virus, de vermoedelijke besmettingsdatum (contactdatum) en een handelingsperspectief. Gelet op de criteria genoemd in overweging 35 AVG kan de notificatie aangemerkt worden als informatie betreffende de gezondheid (*gezondheidsrisico).* Dit betekent dat de notificatie als privacygevoelig moet worden aangemerkt. VWS heeft maatregelen genomen om deze privacygevoelige informatie te beschermen. De notificatie van de telefoon verdwijnt nadat hij is gelezen en van de notificatie kan geen schermafdruk worden gemaakt. Daarmee wordt voorkomen dat deze informatie toegankelijk is voor derden.

Omdat de melding de datum van de mogelijke besmetting geeft, heeft dit in sommige gevallen gevolgen voor de ***horizontale privacy*** van de besmette gebruikers. Het is immers niet uitgesloten dat de gebruiker die de melding ontvangt nog weet met wie hij/zij die dag in contact is geweest. Volledige anonimiteit tussen gebruikers onderling is dus niet te garanderen. Dit effect wordt versterkt als gebruikers zich netjes houden aan de maatregel van het kabinet om zoveel mogelijk thuis te werken en grote groepen (ook thuis) te vermijden. Minder sociale contacten per dag zal in de regel betekenen dat het risico van identificatie van de besmette gebruiker door gebruikers die een melding ontvangen toeneemt. Dit is een onvermijdelijk gevolg van het gebruik van de app.

Aanbeveling

Informeer de gebruikers in de Veelgestelde vragen over het risico op herleidbaarheid door een andere gebruiker. Een verstandig adagium in het privacy- en gegevensbeschermingsrecht is het principe van *surprise minimization*. Ook al zal de gebruiker in de meeste gevallen volstrekt anoniem blijven, ook dan is het verstandig om mensen te waarschuwen dat anonimiteit tussen gebruikers niet in alle gevallen gegarandeerd kan worden. Daarbij moet worden uitgelegd onder welke omstandigheden andere gebruikers tot een identificatie kunnen komen.

2. Vragen aan PMP

VWS heeft aan PMP de volgende vragen gesteld in het kader van deze *second opinion*:

1. Zijn de gegevens die door de app en de backend verwerken persoonsgegevens?
2. Uitgangspunt van de DP3T referentiearchitectuur is dat er geen persoonsgegevens worden verwerkt. Waar zit qua AVG het verschil in de Nederlandse implementatie en de referentiearchitectuur van DP3T?
3. Kan toestemming in dit geval een grondslag zijn voor de app door de overheid?
4. Op welk deel van de verwerking is de AVG van toepassing en welk deel niet?
5. Wie is verwerkingsverantwoordelijk voor welk onderdeel van de verwerking?
6. Zijn u verder zaken opgevallen aan de DPIA die belangrijk zijn te melden?

Wij zullen deze hieronder een voor een beantwoorden.

Persoonsgegevens

Vraag: Zijn de gegevens die door de app en de backend verwerken persoonsgegevens?

De definitie van persoonsgegevens luidt (art. 4(1) AVG):

> Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Deze definitie gaat uit van een **ruim identiteitsbegrip**.[10] Overweging 26 AVG werkt het begrip 'identificeerbaarheid' nader uit:

> De beginselen van gegevensbescherming moeten voor elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon gelden. Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over een identificeerbare natuurlijke persoon worden beschouwd. **Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.** Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen. De gegevensbeschermingsbeginselen dienen derhalve niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Deze verordening heeft derhalve geen betrekking op de verwerking van dergelijke anonieme gegevens, onder meer voor statistische of onderzoeksdoeleinden (*vet, JT)*.

[10] Zie ook Advies 4/2007 (WP136) van de voorloper van de EDPB, de Artikel 29 Werkgroep: "Deze definitie weerspiegelt de bedoeling van de Europese wetgever een brede definitie van persoonsgegevens te geven, waaraan tijdens het gehele wetgevingsproces is vastgehouden." Deze benadering is in de AVG voortgezet.

Het gaat bij het begrip 'identificeerbaarheid' dus niet om theoretische herleidbaarheid, maar om herleidbaarheid *in de context van de verwerking.* Het Hof van Justitie van de Europese Unie heeft in het *Breyer*-arrest[11] de criteria voor herleidbaarheid nader bepaald. In paragrafen 45 en 46 overweegt het Hof:

> Vastgesteld dient evenwel te worden of de mogelijkheid om een dynamisch IP-adres te combineren met de extra informatie waarvan die internetprovider in het bezit is, een middel vormt waarvan mag worden aangenomen dat het redelijkerwijs kan worden ingezet om de betrokken persoon te identificeren.
>
> Zoals de advocaat-generaal in punt 68 van zijn conclusie in wezen heeft opgemerkt, is dit niet het geval indien de identificatie van de betrokkene **bij de wet verboden wordt** of **in de praktijk ondoenlijk is**, bijvoorbeeld omdat zij – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt, zodat het gevaar voor identificatie in werkelijkheid onbeduidend lijkt.

Het karakter van persoonsgegevens kan volgens het Hof dus worden weggenomen door een **wettelijk verbod op herleidbaarheid**. De AVG gaat voor dit begrip immers uit van redelijke middelen (herleidbaarheid in de context van de verwerking), niet van onredelijke of illegale middelen (geen theoretische middelen). Dat laatste is wel van belang vanuit het oogpunt van informatiebeveiliging, omdat ook niet-persoonsgegevens beschermd moeten worden tegen misbruik.

Daarnaast is van belang dat gepseudonimiseerde gegevens in de AVG alleen als persoonsgegevens kwalificeren als zij in combinatie met aanvullende gegevens aan een specifieke persoon kunnen worden gekoppeld (art. 4(5) AVG). Voorwaarde om te spreken van 'gepseudonimiseerde gegevens' is dat die aanvullende gegevens apart bewaard worden en technische en organisatorische maatregelen zijn genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

De TEKs, RPIs en de DKs zijn **gepseudonimiseerde identificatoren**. Gelet op overweging 26 kwalificeren deze gegevens alle als persoonsgegevens vanwege de volgende omstandigheden:

- De unieke codes zijn steeds gekoppeld aan een datum;
- De TEKs worden samen met een bij de GGD op naam bekende autorisatiecode geüpload;
- De IP-adressen worden door het CIBG zeven dagen bewaard.

De TEKs, RPI's en DK's, die door de overheid worden verwerkt, zijn dus persoonsgegevens. Voor de RPI's geldt dat deze alleen in het privédomein worden verwerkt en daarom dus buiten de AVG vallen. De TEKs en DKs zijn naar hun aard anoniem, maar zijn in combinatie met de IP-adressen wel herleidbaar tot een gebruiker.

Aanbeveling (idem als hierboven)
Om de privacy van de geïnfecteerde gebruiker optimaal te beschermen, dient wettelijk geregeld te worden dat het de Minister van VWS verboden is om de IP-adressen te koppelen dan wel te laten koppelen aan de TEK's van de gebruiker dan wel een ander, zoals de GGD, daartoe in staat te stellen. Ook moet het wettelijk verboden worden om de gegevens te exporteren en/of selectietechnieken toe te passen op de TEK's en zo gebruikers uniek aan te wijzen in de database.

[11] http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=NL

De onmiddellijke consequentie daarvan is dat de TEKs en de DK's in de backend niet langer kwalificeren als persoonsgegevens en dat dus de AVG op die gegevens in de backend niet van toepassing is. Dit lost ook een tweetal problemen op:

1. Het feit dat het praktisch gezien onmogelijk is voor besmette gebruikers om hun toestemming in te trekken.
2. Het feit dat VWS zich bij de uitoefening van inzage, correctie of verwijderingsrechten van de betrokkene steeds moet beroepen op art. 11 AVG, waardoor de AVG-rechten van de betrokkenen in de praktijk betekenisloos zijn.

NB. De RPIs vallen via de uitzondering van persoonlijk gebruik al buiten de reikwijdte van de AVG.

DP3T referentiearchitectuur

Vraag: Uitgangspunt van de DP3T referentiearchitectuur is dat er geen persoonsgegevens worden verwerkt. Waar zit qua AVG het verschil in de Nederlandse implementatie en de referentiearchitectuur van DP3T?

Het *Decentralized Privacy-Preserving Proximity Tracing (DP3T)* consortium, waarin onder meer de Universiteit Delft, de KU Leuven, de Technische Universiteiten van Lausanne en Zürich, de Universiteit van Oxford, en het University College London deelnemen, heeft een referentie-implementatie ontwikkeld en een referentie-DPIA gepubliceerd.[12] Het *Exposure Notification* framework van Google en Apple (GAEN) is gebaseerd op de DP3T implementatie.

De documentatie van DP3T over privacy en security zegt over 'persoonsgegevens' (en dus de toepasselijkheid van de AVG):

> The decentralized approach notably minimises the amount of personal data collected by any one entity, and heavily reduces the possibility of accessibility of any information, providing the guarantee that the backend server learns nothing about identifiable individuals or their health status (...). The system is designed such that no entity beyond a user's device processes or stores any identifiable personal data about the user. As a whole, the system fulfils processing goals that would usually require personal data to be transmitted. We believe that under normal operation, none of the data used to achieve proximity tracing need be characterized as personal data, as no actors holding the data have the ability to re-identify it with means reasonably likely to be used (following the test outlined by the CJEU in *Breyer*).[13]

Net als VWS stelt in de DPIA, gaat ook DP3T er in principe van uit dat er geen persoonsgegevens worden verwerkt, maar ze kunnen het niet helemaal uitsluiten.

> The backend server that the data is transmitted to cannot link any of the infected EphIDs to natural persons. In normal functioning, therefore, we can even understand that the server will not be holding personal data, although, as mentioned, we err on the side of caution and consider it to be personal data with near-anonymous safeguards. No additional data needs to be stored beyond these identifiers.

Het 'voor-de-zekerheid' van toepassing verklaren van de AVG, zoals ook gebeurt in de DPIA, is onbevredigend, met name als het gaat om de uitoefening van de rechten van betrokkenen. Als er sprake is van persoonsgegevens, dan is de AVG van toepassing en dan hebben betrokkenen rechten zoals inzagerecht en verwijderingsrecht. Vanwege het '*near anonymous*'-karakter van de data in de

[12] https://github.com/DP-3T/

[13] https://github.com/DP-3T/documents/raw/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf (p.4)

backend, is de uitoefening van deze rechten in de praktijk een wassen neus omdat VWS dan, zoals VWS in de DPIA zelf stelt, onder verwijzing naar artikel 11 AVG een verzoek zal afwijzen.

Een andere reden dat dit onbevredigend is, is dat de toestemming, waarop VWS de gegevensverwerking thans baseert, niet zinvol kan worden ingetrokken. Het CIBG zal immers niet weten welke TEK's en/of DK's moeten worden verwijderd. Dat is in strijd met het uitgangspunt van de AVG dat de betrokkene bij toestemming als grondslag volledige controle heeft over de vraag of de gegevens wel of niet verwerkt worden. Dit probleem verdwijnt echter als in de wet een grondslag wordt gecreëerd.

In de Nederlandse implementatie is er sprake van de volgende omstandigheden:

- De unieke codes zijn steeds gekoppeld aan een datum;
- De TEKs worden samen met een bij de GGD op naam bekende autorisatiecode geüpload;
- De IP-adressen worden door het CIBG zeven dagen bewaard.

Het verschil tussen de Nederlandse implementatie en de DP3T referentie-implementatie zit voornamelijk is het bewaren van IP-adressen (7 dagen) voor informatiebeveiligingsdoeleinden. DP3T zegt hierover:

> When the backend receives the upload, it verifies the authorization code, and stores the seed. It does not store any other information related to the upload (such as IP addresses or time).[14]

Zolang de IP-adressen opgeslagen worden, is er sprake van "middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke … om de natuurlijke persoon direct of indirect te identificeren" (zie overweging 26 AVG) en zijn de TEKs en DKs op de backend server dus persoonsgegevens in de zin van de AVG. Om die herleidbaarheid *in redelijkheid* uit te sluiten, dient de herleidbaarheid wettelijk verboden te worden (zie Aanbeveling 2). Als Aanbeveling wordt overgenomen, dienen de gegevens uiteraard wel beveiligd te worden tegen herleidbaarheid met *onredelijke* c.q. *illegale* middelen.

Toestemming

Vraag: Kan toestemming in dit geval een grondslag zijn voor de app door de overheid?

De huidige versie van de app, zoals deze is uitgerold in Overijssel, Gelderland en Drenthe, baseert de verwerking van de gegevens op (uitdrukkelijke) toestemming van de gebruiker, zoals bedoeld in artikel 6(1)(a) voor 'gewone' persoonsgegevens en artikel 9(2)(a) AVG voor bijzondere persoonsgegevens.

Hoewel toestemming mijns inziens niet onmogelijk is en ook de European Data Protection Board (EDPB) dat in haar opinie van 21 april 2020 niet uitsluit[15], is het niet de meest sterke verwerkingsgrondslag voor een gegevensverwerking door de overheid. De overheid werkt in een democratische rechtsstaat immers op basis van democratisch toegewezen taken en bevoegdheden. Toestemming waarbij de verwerking volledig afhankelijk is van de wil van de burger, suggereert dat de overheid geen noodzakelijk en zwaarwegend belang heeft bij de gegevensverwerking, terwijl de huidige gezondheidscrisis juist een argument is om het algemeen belang te benadrukken.

---

14 https://github.com/DP-3T/documents/raw/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf (p.9)

15 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

Een ander argument waarom toestemming niet voor de hand ligt, is dat VWS de privacybescherming zo ver in de CoronaMelder infrastructuur heeft doorgevoerd, dat intrekking van de toestemming feitelijk onmogelijk is omdat de gegevensverwerking van een besmette gebruiker die zijn/haar TEK's heeft geüpload niet kan worden gestopt in de backend (en dat zou bij intrekking van toestemming wel moeten). De gebruiker kan uiteraard de app deïnstalleren, maar dat raakt vooral de vrijwilligheid van de gegevensuitwisseling met andere gebruikers en het ophalen van de DK's uit de backend, niet de gegevensverwerking in de backend zelf.

NB. Toestemming moet niet verward worden met vrijwilligheid.[16] Artikel 6(1) AVG kent zes gronden voor gegevensverwerking:

a) Toestemming van de betrokkene.
b) De gegevensverwerking is noodzakelijk om een overeenkomst uit te voeren.
c) De gegevensverwerking is noodzakelijk voor de nakoming van een wettelijk verplicht.
d) De gegevensverwerking is noodzakelijk voor de bescherming van vitale belangen van de betrokkene.
e) De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of openbaar gezag.
f) De gegevensverwerking is noodzakelijk voor de behartiging van een gerechtvaardigde belang van de verwerkingsverantwoordelijke of een derde.

In de gronden a en b is per definitie sprake van vrijwilligheid. Bij de gronden e en f is er bij gebrek aan een verplichting of dwang sprake van een impliciete vrijwilligheid (waarbij de betrokkene bezwaar kan maken als hij/zij iets niet wil). Alleen bij de gronden c en d is er geen sprake van vrijwilligheid (juridisch c.q. feitelijk).

Kortom, de app kan prima op basis van vrijwilligheid worden ingevoerd, terwijl de grondslag voor de gegevensverwerking de e-grond is (taak van algemeen belang). Op grond van artikel 6(3) AVG dient die taak wel in de wet te zijn omschreven. Ik wijs er daarbij op dat het niet noodzakelijk is dat de publieke taak of de gegevensverwerking uitputtend is geregeld in een wet in formele zin; voldoende is dat de hoofdlijnen van de taak kenbaar zijn in de wet.[17]

Het creëren van een basis in de wet voor de gegevensverwerking is niet alleen noodzakelijk vanuit oogpunt van de AVG (als die al van toepassing is), maar ook vanuit het oogpunt van inbreuk op grondrechten door de overheid (*verticale privacy*). Alleen al om die reden is toestemming als grondslag niet logisch.

Aanbeveling

Maak een wettelijke regeling om een grondslag voor de gegevensverwerking te verkrijgen en een inbreuk op de persoonlijke levenssfeer van de gebruikers te mogen maken.

Toepasselijkheid AVG

Vraag: Op welk deel van de verwerking is de AVG van toepassing en welk deel niet?

[16] Zie https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, par. 29 en de Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe: https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7

[17] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2020:2917, 4.9

Voorop gesteld dat de gegevens die worden verwerkt persoonsgegevens zijn (dat hoeft niet per se), regelt artikel 2(1) AVG wanneer de AVG van toepassing is:

> Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Inherent aan deze bepaling is dat er door de verwerkingsverantwoordelijke (of door een verwerker namens hem) persoonsgegevens worden *verwerkt*.

Artikel 4(2) definieert 'verwerking' als:

> Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

- *CoronaMelder App*

Uit deze definitie blijkt dat – anders dan waar VWS in de DPIA van uitgaat – het *uitgeven van software* geen 'verwerking' is in de zin van de AVG. Hoewel de uitgever bepaalt welke gegevensverwerkingsfunctionaliteit in de software wordt ingebouwd en hoe deze eruit ziet, zoals in casu het feit dat gebruikers RPIs met elkaar kunnen uitwisselen via Bluetooth, is dit geen 'verwerking' in de zin van de AVG en is de AVG dus per definitie niet van toepassing op VWS voor zover gebruikers van de app gegevens met elkaar uitwisselen. De verwerking aan de kant van de overheid begint pas op het moment dat een gebruiker via de app de gegevens naar de backend heeft verstuurd.

Dit ligt anders voor de gebruikers van de app. Zij verwerken elkaars RPIs en het is allerzins redelijk om aan te nemen dat de RPIs in veel gevallen ook persoonsgegevens zijn in de zin van de AVG. Echter, omdat de gebruikers de app in hun privédomein gebruiken, kunnen zij zich beroepen op de uitzondering voor persoonlijk gebruik (art. 2(2)(c) AVG), waardoor de AVG op de gegevensverwerking door die gebruikers niet van toepassing is. Idem voor de DKs die gebruikers downloaden om blootstellingsrisico's te berekenen.

Hieruit volgt dat de AVG in het geheel niet van toepassing is op de gegevensverwerkingen die plaatsvinden in het privédomein (zie plaatje in Hoofdstuk 1).[18]

- *Backend*

Voor zover de TEKs en DKs in de backend kwalificeren als persoonsgegevens, is de AVG van toepassing op de backend. Er wordt immers voldaan aan de vereisten van art. 2(1) AVG. Zoals hierboven diverse keren aangehaald, is het echter niet nodig om de TEKs en DKs aan te merken als persoonsgegevens (ook niet voor-de-zekerheid). Om zeker te stellen dat de TEKs en DKs geen persoonsgegevens zijn, is het raadzaam om de herleidbaarheid bij wettelijke regeling te verbieden.

NB. Het feit dat de AVG bij zo'n wettelijk verbod formeel niet van toepassing is op de TEKs en DKs in de backend wil niet zeggen dat VWS de principes van zorgvuldige gegevensverwerking, zoals

[18] Dat wil overigens niet zeggen dat de gegevens in het privédomein niet beschermd zijn. Art. 138a Wetboek van Strafrecht maakt hacken strafbaar en het Burgerlijk Wetboek biedt ruimte voor civielrechtelijke claims jegens andere gebruikers. De AVG, de Wet Politiegegevens en het Wetboek van Strafvordering stellen regels over het verzamelen van die gegevens door overheidsinstanties en bedrijven.

dataminimalisatie, beveiliging, transparantie, datakwaliteit en accountability zoals het afspreken van waarborgen met het CIBG en KPN, niet kan toepassen.

Bij de HUIDIGE set maatregelen is de AVG dus van toepassing op de gegevens in de backend. Maar dat is vanuit het oogpunt van het niet effectief kunnen honoreren van de rechten van betrokkenen niet wenselijk en vanuit het oogpunt van bescherming van de gegevens niet nodig (zie Aanbeveling 2).

Verwerkingsverantwoordelijke

Vraag: Wie is verwerkingsverantwoordelijk voor welk onderdeel van de verwerking?

- *CoronaMelder App*

Uit het voorgaande blijkt dat in het privédomein de gebruikers de verwerkingsverantwoordelijken zijn, maar de AVG is op grond van art. 2(2)(c) niet op hen van toepassing.

- *Backend*

In de backend ligt het gecompliceerder. Omdat het CIBG een uitvoeringsorganisatie van het Ministerie van VWS is, kan het CIBG geen verwerkingsverantwoordelijke zijn voor de gegevensverwerking is de backend: dat is dus de Minister.

De GGD heeft geen toegang tot de backend, maar stuurt gegevens door naar de backend vanuit het GGD portaal.[19] Gelet op het feit dat de GGD een actieve rol speelt bij de autorisatie van de TEK upload, kan men stellen dat de GGD's gezamenlijk met de Minister verwerkingsverantwoordelijke zijn voor de verwerking van de TEKs en de DKs. De Minister heeft in dit geval een systeemverantwoordelijkheid (beheer) en de GGD heeft een gebruiksverantwoordelijkheid (autorisatie).

KPN heeft hier de rol van verwerker.

Bij de HUIDIGE set maatregelen is de Minister dus gezamenlijk met de GGD's verwerkingsverantwoordelijke voor de gegevensverwerking in de backend. Echter, dat is vanuit het oogpunt van het niet effectief kunnen honoreren van de rechten van betrokkenen niet wenselijk en vanuit het oogpunt van bescherming van de gegevens niet nodig (zie Aanbeveling 2).

Overige zaken

Vraag: Zijn u verder zaken opgevallen aan de DPIA die belangrijk zijn te melden?

Risico's buiten de informatie-infrastructuur

In de DPIA komen de risico's die buiten de informatie-infrastructuur liggen niet of nauwelijks aan bod. Dit wordt wellicht mede ingegeven door het feit dat het *Toetsmodel Gegevensbeschermingseffect-beoordeling Rijksdienst* daar niet voor geschikt is. Wij noemen hier de volgende risico's:

- **Extra belasting voor mensen die niet thuis kunnen werken.** Het gebruik van de app heeft mogelijk extra nadelige effecten op mensen die niet in de mogelijkheid zijn om thuis te werken en derhalve vaker langdurig in contact komen met andere mensen, zoals

[19] Zie Europees Hof van Justitie in de *Jehova Getuigen*-zaak (10 juli 2018), waarin het Hof oordeelde dat een verwerkersverantwoordelijke niet ook zelf toegang tot de gegevens hoeft te hebben. Voldoende is dat hij betrokken is bij het vaststellen van 'doel en middelen'. http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=NL&mode=lst&dir=&occ=first&part=1&cid=15342168

winkelpersoneel, zorgmedewerkers, horecapersoneel en treinconducteurs. Zij zullen dus ook vaker dan gemiddeld een melding krijgen. Dit kan allerlei negatieve effecten hebben, zoals het negeren van blootstellingssignalen wegens gewenning (gezondheidsrisico) en het verlies van arbeidsproductiviteit wegens het ondergaan van extra coronatesten en zelfisolatie tot de uitslag daarvan bekend is (inkomensrisico).

- **Onomkeerbaarheid technologische ontwikkelingen.** Hoewel het de bedoeling is dat de app tijdelijk wordt ingezet en zodra het mogelijk is weer gedeactiveerd wordt (het Google/Apple Exposure Notification framework kan ook regionaal worden uitgezet), zijn langetermijneffecten niet uit te sluiten. In het verleden hebben we gezien dat tijdelijke privacyinbreuk makende maatregelen een permanent karakter krijgen. Zo werd 100 jaar geleden de paspoortplicht als noodmaatregel werd ingevoerd om paal en perk te stellen aan de instroom van immigranten in de VS na de Eerste Wereldoorlog. En na de aanslagen van 9/11 werd de beperkte identificatieplicht in Nederland razendsnel omgezet in een permanente identificatieplicht. Maar zelfs als de overheid de app deactiveert, dan is het niet ondenkbaar dat er een nieuwe toepassing wordt gevonden voor deze contact tracing functionaliteit. En met de toestemming van de Telecommunicatiewet in de hand staat er juridisch weinig in de weg aan dergelijke nieuwe toepassingen. M.a.w., de onbedoelde gevolgen van een contact tracing app op de maatschappij zijn nog niet of nauwelijks te overzien.

Toetsingskader grondrechteninbreuk gegevensverwerking

In het Toetsmodel Gegevensbeschermingseffectbeoordeling Rijksdienst wordt marginaal aandacht besteedt aan de grondrechtelijke inbreuk die gepaard gaat met de verwerking van gegevens van burgers door de overheid. In de DPIA wordt kort ingegaan op artikel 8 EVRM (bescherming van de persoonlijke levenssfeer). Echter, artikel 52 EU Handvest en artikel 35 AVG spreken van 'rechten en vrijheden', wat een bredere term is dan het begrip 'persoonlijke levenssfeer' van artikel 8 EVRM.

Onder 'rechten en vrijheden' verstaan het Handvest en de AVG alle fundamentele rechten en beginselen die genoemd zijn in het Handvest, dus naast bescherming van de persoonlijke levenssfeer, ook recht op bescherming van persoonsgegevens, recht op non-discriminatie, vrijheid van godsdienst, vrijheid van meningsuiting, recht op gezondheidszorg, recht op arbeid, recht op onderwijs, recht op menselijke waardigheid, etc.

Een beoordeling van deze rechten en vrijheden ontbreekt in de DPIA. Daarom geven wij hier een voorzet:

- **Stap 1:** Wat is de basis in de wet voor de verwerking?
  De overheid heeft een basis in de wet nodig om een inbreuk te mogen maken op de rechten en vrijheden van de betrokkene. Deze leek te ontbreken, met name als het gaat om de rol van de Minister. Met genoegen constateer ik dat de Minister het advies van de AP opvolgt om middels een spoedwetprocedure deze basis te creëren.

- **Stap 2:** Welke fundamentele rechten en vrijheden van de betrokkene zijn in het geding?
  Behalve privacy en bescherming van persoonsgegevens kan het in casu ook gaan om recht op arbeid of onderwijs (zie voorbeelden hierboven bij mensen die niet thuis kunnen werken) en het recht op non-discriminatie (mensen die de app niet geïnstalleerd hebben in relatie tot toegang tot gebouwen en evenementen).

- **Stap 3:** Wordt de essentie van die rechten en vrijheden aangetast?
  Het gebruik van de app is vrijwillig zodat per definitie geen sprake kan zijn van een inbreuk die zodanig disproportioneel is dat de essentie van de rechten en vrijheden wordt aangetast.

- **Stap 4:** Welk maatschappelijk of eigen belang wordt gediend met de verwerking?
  De verspreiding van het Coronavirus indammen, de gezondheid van mensen te beschermen en de economie draaiende te houden.

- **Stap 5:** Wat is het specifieke doel van de verwerking?
  (Mogelijke) besmettingen sneller opsporen.

- **Stap 6:** Past dat doel binnen de doelstellingen van het EU-recht/Grondwet? Of is de verwerking nodig om de rechten en vrijheden van anderen te beschermen?
  Ja, bescherming van de volksgezondheid.

- **Stap 7:** Draagt de verwerking effectief bij aan dat doel?
  Daar hopen we op, maar dat moet nog bewezen worden.

- **Stap 8:** Is er een minder vergaand middel beschikbaar dat even effectief is?
  Nee.

- **Stap 9:** Wat is de omvang, duur, inhoud en indringendheid van de verwerking?
  De verwerking is grootschalig (= iedereen die een besmetting doorgeeft), per persoon kortdurend (maximaal 24 uur), de indringendheid is minimaal (backend).

- **Stap 10:** *Tussenconclusie:* Is de inbreuk op de rechten en vrijheden van de betrokkene die de verwerking maakt evenredig met het belang?
  Ja.

- **Stap 11:** Zo nee, welke passende waarborgen moeten worden ingebouwd om het evenwicht te herstellen?
  Zie de maatregelen in de DPIA en de aanbevelingen in dit document.

- **Stap 12:** *'Fair Balance' test:* Is de inbreuk op de rechten en vrijheden van de betrokkene die de verwerking maakt evenredig met het belang?
  Ja.

Bron: European Data Protection Supervisor / PMP

Verantwoording

De volgende documenten zijn door ons beoordeeld:

- Concept-gegevensbeschermingseffect-beoordeling (DPIA) van de CoronaMelder app (versie 13 augustus 2020).

Als achtergrondinformatie hebben wij o.a. gebruikt:

- De CoronaMelder app, test- en onderzoeksversie 1.0.0.
- De referentie DPIA van het DP3T Consortium, versie V01, 1 mei 2020.
- DP3T White Paper, versie 25 mei 2020.
- DP3T Privacy and Security, versie 3 april 2020.
- Apple Contact Tracing, FAQ's Exposure Notification.
- Google Informatie en bronnen over Covid 19.
- Trinity College Dublin, Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps

Privacy
Management
Partners
Coöperatie UA

adres
Vondellaan 58
3521 GH Utrecht

telefoon
+31 85 401 38 66

e-mail
info@pmpartners.nl

website
www.pmpartners.nl