Memo

Van:	mr. drs. Jeroen Terstegge CIPP/E CIPP/US, partner
Aan:	De Vaste Commissie Volksgezondheid, Welzijn en Sport
Datum:	20-04-2020
Betreft:	Privacy en de Corona app

Geachte Commissieleden,

Dank voor de uitnodiging om deel te nemen aan het rondetafelgesprek over de corona-app. Afgelopen weekend was ik een van de privacyexperts die op uitnodiging van VWS deelnemen aan de appathon. Hoewel iedereen zonder meer zijn en haar best deed om er ondanks weinig voorbereiding, beperkte/ontbrekende documentatie en de zeer korte tijd per leverancier iets van te maken, werd mij al snel duidelijk dat **de app nog onvoldoende doordacht is om de privacyrisico's goed te kunnen inschatten**. Ik licht een en ander hieronder kort toe.

Valse tegenstelling
Laat ik voorop stellen dat het gebruik van een app geen tegenstelling is tussen gezondheid en privacy. Gezondheid is een *doel* (sociaal grondrecht), privacy is een *waarde* (klassiek grondrecht). Het is dus niet óf óf. Het is wél: bescherming van de volksgezondheid met inachtneming van de regels over inperking van privacy, zoals legitimiteit, noodzaak, proportionaliteit en transparantie. Als deze regels niet goed in acht worden genomen, bestaat het risico dat de app door de rechter ongeldig wordt verklaard, zoals onlangs gebeurde met SyRI.

Kaders onduidelijk
Ondertussen staat het grondrecht op databescherming (zoals uitgewerkt in de AVG) onverkort overeind, ook in deze crisis. De AVG gaat over meer dan privacy; ook non-discriminatie, non-stigmatisering, reputatiebescherming, autonomie, menselijke waardigheid en veiligheid van de betrokkene behoren tot de doeleinden van de AVG. De AVG vereist dat gegevensverwerking rechtmatig, behoorlijk en proportioneel is en een geldige juridische basis heeft. Betrokkenen hebben rechten zoals inzage, correctie, bezwaar en verwijdering. Er is een verwerkingsverantwoordelijke die accountable en aansprakelijk is en die maatregelen moet nemen zoals privacy by design en het uitvoeren van risicoanalyses om de gegevensverwerking in goede banen te leiden (privacymanagement).

Het is echter vooralsnog volstrekt onduidelijk onder wiens juridische verantwoordelijkheid de app straks wordt uitgerold. Door het ontbreken van die kaders kan nog geen serieus begin worden gemaakt met het inrichten van de juridische, technische en organisatorische waarborgen.

Een ander aandachtpunt is dat de AVG niet van toepassing is op alle gegevensverwerkingen. Zo is de AVG *niet* van toepassing op persoonlijke gebruik van de gebruiker van de app (art. 2 lid 2 AVG). Bij een volledig decentrale en dus privacyvriendelijke oplossing waarbij de gebruiker er zelf voor kiest om

zijn/haar gegevens door te geven aan de huisarts of de GGD, bestaat de kans dat de AVG niet van toepassing is op de gegevens in de telefoon en de communicatie tussen de telefoons (of dit inderdaad zo is, moet voor elk voorstel nader worden onderzocht). Dit zou grote gevolgen hebben voor de governance rondom de app. Zo zou de Autoriteit Persoonsgegevens bijvoorbeeld niet bevoegd zijn om toezicht te houden en kunnen de gebruikers zich niet beroepen op hun rechten in de AVG.

Duidelijkheid over het doel van de app nodig.
Elke gegevensverwerking vereist een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel (art. 5 AVG). Het doel van de app is vooralsnog gekoppeld aan het werk van de GGD. Het is echter de vraag of de gebruikers dit doel ook zo zullen ervaren. Als de app wordt ervaren als een middel om besmettingen te voorkomen, creëert de app schijnveiligheid. Het doel van de app moet dus glashelder binnen en buiten de app worden gecommuniceerd. Een zogeheten '*layered privacy notice*', waarin de informatie in gradaties van gedetailleerdheid wordt aangeboden, kan daarbij helpen.

Noodzaak nog niet aangetoond
Noodzakelijkheid valt juridisch (grondrechtelijk/AVG) uiteen in twee componenten:

1. De app draagt effectief bij aan een concreet doel (zie ook hieronder *datakwaliteit*).
2. Een minder vergaand, maar even effectief middel is niet voorhanden of realistisch (subsidiariteit).

De Minister zal de noodzaak van de app moeten aantonen. Een "verwachting van de GGD" (zie Kamerbrief van 16 april) is onvoldoende om de noodzaak te onderbouwen. Ook het enkele feit dat het normale contacttracingproces van de GGD het niet meer kan bijbenen als de lockdown wordt opgeheven, is onvoldoende om de noodzaak te rechtvaardigen als de app niet ook effectief bijdraagt aan de oplossing van het probleem van de GGD.

Datakwaliteit is belangrijk
Het succes van de app staat of valt met de kwaliteit van de gegevens (zie ook art. 5 AVG). Los van het feit dat onvoldoende testen op zich al leidt tot een lage datakwaliteit, moet een besmette persoon zijn/haar positieve status ook daadwerkelijk (willen) registreren in de app. Dit vereist dat zowel de app als het ecosysteem waarin de app functioneert volledig moeten kunnen worden vertrouwd door een besmette persoon. Niet alleen moet de app veilig zijn en alleen doen wat het zegt te doen, de partij onder wiens verantwoordelijkheid de app wordt uitgerold moet ook volstrekt betrouwbaar zijn, onder meer door aantoonbare en kwalitatief hoogstaande beheersmaatregelen, zoals privacy-by-design en default in de app en de organisatie, een openbare en periodiek bijgewerkte gegevenseffectbeoordeling (DPIA), een auditcyclus, en een kwalitatief goede functionaris gegevensbescherming (FG) die toezicht houdt en adviseert.

Daarnaast moet de app ook betrouwbaar een mogelijk risicocontact kunnen vaststellen. Dit stelt hoge eisen aan de gebruikte techniek. Veel loos alarm is immers funest voor de betrouwbaarheid en de acceptatie van de app. De eerste keer zullen de meeste mensen de adviezen wel opvolgen, de tweede keer misschien ook nog wel, maar de derde, vierde, vijfde of tiende keer? Er zit waarschijnlijk een grens aan hoeveel loos alarm mensen bereid zijn om te accepteren.

De app vereist wetgeving
De app kan op basis van ingebouwde beslisregels komen tot een signaal en mogelijk ook een advies aan de gebruiker die in contact is geweest met een besmette persoon. Dat signaal/advies kan grote gevolgen hebben voor zo'n gebruiker, zowel praktisch (isolatie) als emotioneel. De AVG verbiedt daarom categorisch dergelijke functionaliteit (art. 22 lid 1). Hoewel de AVG toelaat dat de betrokkene uitdrukkelijk toestemming geeft voor dergelijke functionaliteit (art. 22 lid 2 sub c AVG), raad ik het vragen van toestemming met klem af omdat mensen die gevolgen op voorhand niet of nauwelijks

goed kunnen overzien bij de installatie van de app. Logischer is dus om op basis van art. 22 lid 2 sub b AVG specifieke wetgeving te maken waarin ook voorschriften en waarborgen zijn opgenomen met betrekking tot die functionaliteit ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de gebruiker.

NB. Als de app het ook mogelijk maakt om een zelfdiagnose te stellen, is naast de AVG mogelijk ook de Verordening betreffende medische hulpmiddelen (MDR) van toepassing.

Flankerend privacybeleid is nodig
In de Kamerbrief van 16 april staan de eisen aan de app zelf. Maar de inzet van de app vereist ook beschermingsmaatregelen rondom het gebruik van de app in de maatschappij, zoals een verbod om het gebruik van de app verplicht te stellen voor toegang tot gebouwen of het openbaar vervoer, regels over wat werkgevers wel of niet mogen vragen aan hun werknemers, en een *sunset clause* in de wet waarmee de app wordt ingevoerd om te voorkomen dat de app langer wordt gebruikt dan nodig.

Verbod op nevengebruik
Gelet op de risico's van stigmatisering en uitsluiting van besmette personen en personen waarvan de app aangeeft dat zij een risicocontact hebben gehad, moet het gebruik van gegevens voor andere doeleinden zonder uitdrukkelijke toestemming van de gebruiker of voorafgaande wettelijke verplichting verboden worden. Dat betekent bijvoorbeeld ook dat de app zo min mogelijk additionele functies mag bevatten anders dan voorlichting of communicatie met de (huis)arts.

Digitale enkelband?
Terwijl wij in Nederland nadenken over een contacttracing app, werken Google en Apple aan hun Google Apple Contact Tracing (GACT) standaard, die het mogelijk maakt om contact tracing tussen iOS en Android telefoons via bluetooth mogelijk te maken. Daar zitten, ongeacht de privacykeuzes die Nederland maakt rondom de corona app, enorme risico's aan. GACT werkt op het operation system niveau, niet op app-niveau. Dit betekent dat contact tracing altijd beschikbaar is voor alle applicaties op de telefoon (dus niet alleen voor de corona app). Zelfs als je geen corona app op je telefoon hebt geïnstalleerd, zal je telefoon -zolang bluetooth aanstaat- voortdurend communiceren met andere telefoons in de buurt. In essentie creëren Apple en Google een systeem voor massa-surveillance, waarmee betrouwbaar kan worden nagegaan wie met wie in contact is geweest (en mogelijk ook wanneer, hoelang en waar).

Onze telefoon dreigt dus een digitale enkelband te worden die misschien wel nooit meer afgaat.

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