PELS RIJCKEN

Openbare samenvatting privacyanalyses bron- en contactonderzoekapps

19 april 2020
Gerrit-Jan Zwenne en Marte van Graafeiland

1 INLEIDING

1.1 Op zaterdag 11 april 2020 heeft het ministerie van Volksgezondheid, Welzijn en Sport ('**VWS**') aan de markt een uitnodiging gedaan voor het indienen van voorstellen voor slimme digitale oplossingen voor – voor zover van belang – bron- en contactopsporing (hierna: de bron- en contactonderzoekapp of kort gezegd app).

1.2 Doel van de uitnodiging is om VWS mede op basis van de opgehaalde informatie in staat te stellen naar beste inzicht een stap te zetten in de besluitvorming over de mogelijke inzet van een bron- en contactonderzoekapp bij de bestrijding van COVID-19 en de volgende fase uit de intelligente lockdown.[1] In de uitnodiging zijn verschillende uitgangspunten genoemd waaraan de voorstellen moeten voldoen, waaronder:

- De gegevens die worden verwerkt zijn en blijven niet tot individuen herleidbaar (anonimiteit);
- Valse positieven moeten zoveel mogelijk beperkt worden door de oplossing (juistheid);
- Gegevens worden zo min en zo kort mogelijk opgeslagen (dataminimalisatie);
- Gegevens mogen uitsluitend uitgelezen of gedeeld worden als er sprake is van a) contact- of brononderzoek als bedoeld in art. 6 Wpg of b) toestemming van de gebruiker (grondslag);
- Het huidige proces van bron- en contactopsporing is uitgangspunt ter ondersteuning. Het gebruik moet gericht zijn op het vereenvoudigen van contactonderzoek (doelbinding);
- Er is voorzien in een informatieportal voor de gebruikers waarin fouten en kwetsbaarheden kunnen worden gemeld (transparantie);
- Gangbare beveiligingsstandaarden;
- Als de app niet meer effectief of noodzakelijk is, moet de uitrol kunnen worden teruggedraaid en data kunnen worden verwijderd (verwijdering).

Overkoepelend geldt dat (voor zover van toepassing) wordt voldaan aan de Algemene Verordening Gegevensbescherming ('**AVG**').

1.3 Tegen deze achtergrond heeft VWS ons gevraagd een privacyanalyse te verrichten op zeven van de ingediende voorstellen. Dit document betreft een samenvatting van onze bevindingen.

---

[1] Zie: 'Uitnodiging slimme digitale oplossingen Corona'.

2 OPMERKINGEN VOORAF

Bij onze analyse hebben wij ons zoveel mogelijk gebaseerd op de documentatie die aan ons ter beschikking is gesteld.[2] De hoeveelheid stukken, het detailniveau en de kwaliteit daarvan verschilde per inschrijver. Daarnaast is van belang dat wij, gelet op de beperkte tijd die beschikbaar was, de inschrijvers bij het uitvoeren van onze analyse niet op de gebruikelijke wijze hebben kunnen bevragen op (onder andere) de voorgestelde techniek, de precieze inrichting van de app en andere relevante aspecten. Het voorgaande maakt dat deze samenvatting is beperkt tot een overzicht van onze bevindingen op hoofdlijnen.

Wij hebben de voorstellen beoordeeld aan de hand van zes fasen: de installatiefase, uitwisselingsfase, validatiefase, waarschuwingsfase, koppelingsfase en notificatiefase. Per fase hebben wij op basis van de beschikbaar gestelde documentatie beoordeeld of aan de hiervoor genoemde uitgangspunten en AVG is voldaan.

3 BEVINDINGEN

Hoofdconclusie

Wij hebben op basis van de beoordeelde stukken bij geen van de voorstellen kunnen vaststellen dat ze volledig voldoen aan de zojuist geformuleerde uitgangspunten. Evenmin hebben wij op basis van de stukken kunnen vaststellen dat wordt voldaan aan alle eisen van de AVG. Daarmee is echter niet gezegd dat niet alsnog aan de AVG kan worden voldaan. Dat vergt enerzijds een doorontwikkeling en anderzijds een meer gedetailleerde uitwerking van de voorstellen.

Deelbevindingen

Wij hebben op basis van de beoordeelde stukken bij geen van de voorstellen kunnen vaststellen dat volledige anonimiteit gegarandeerd.

Op basis van de beoordeelde stukken kan bij geen van de voorstellen worden vastgesteld dat volledige anonimiteit is gegarandeerd.

Vals positieven moeten zoveel mogelijk worden beperkt

Alle voorstellen werken met Bluetooth. Bepaalde risico’s zijn daaraan inherent. Zo bestaat bij het gebruik van Bluetooth het risico dat niet-risicovolle connecties ook worden geregistreerd, bijvoorbeeld wanneer een Bluetoothconnectie wordt gelegd met devices die zich op voldoende afstand bevinden, of bijv. achter een muur, raam, of plexiglas. Ook is denkbaar dat iemand in de buurt is geweest van een device op een moment dat deze zich niet in de nabijheid van de gebruiker bevond.

---

[2] Een groot aantal partijen heeft gedurende dit weekend van 18 en 19 april 2020 nog aanvullende stukken toegestuurd.

Sommige inschrijvers hebben (door middel van instellingen) getracht dit probleem te ondervangen. Daarmee is het risico op vals positieven kleiner, maar ten aanzien van geen enkel voorstel hebben wij op basis van de aan ons ter beschikking gestelde stukken kunnen vaststellen dat dit inherente risico volledig wordt ondervangen.

Bij sommige voorstellen wordt de besmetting van de gebruiker gevalideerd door een arts. Het aantal vals positieven kan hiermee verder worden teruggebracht.

Er worden zo min en zo kort mogelijk gegevens opgeslagen (dataminimalisatie)

Alle voorstellen kennen enige vorm van centrale opslag. In het gros van de voorstellen betreft dat alleen ID's en/of keys. In bepaalde gevallen worden ook contactgegevens centraal opgeslagen. Dat laatste is behulpzaam voor de bron- en contactopsporing door de GGD en in zoverre lijken de genoemde contactgegevens toereikend, ter zake dienend en niet bovenmatig te zijn voor het doel waarvoor de app zal worden gebruikt.

Een ander belangrijk aspect van dataminimalisatie is het moment waarop de risicoanalyse plaatsvindt en door wie. Bij een volledig gedecentraliseerde opzet vindt de risicoanalyse plaats in de app zelf. Dat doet het meeste recht aan het beginsel van dataminimalisatie.

Wij zijn ook apps tegengekomen waarbij de risicoanalyse centraal plaatsvindt. Bij een dergelijke centrale opzet krijgt de beheerder van de server gedetailleerde inzichten in de contactmomenten en de risico's die de mogelijk besmette gebruiker heeft gelopen. Ook de wijze waarop gebruikers worden gewaarschuwd dat zij in contact zijn geweest met een besmette gebruiker, is van invloed op de omvang en de aard van de (gepseudonimiseerde) persoonsgegevens die worden verwerkt. Kort en goed zijn wij bij de centrale opzet twee varianten tegengekomen. Bij de eerste variant worden meldingen gericht verzonden naar de mogelijk besmette gebruikers. Bij deze variant bestaat een risico dat de mogelijk besmette gebruiker kan worden geïdentificeerd. In de tweede variant wordt een melding op een centrale server opgeslagen, waarna deze ongericht wordt 'gebroadcast' naar gebruikers. Bij de tweede variant lijkt dat risico kleiner. Tot slot zien wij verschillen in wie toegang heeft tot de vastgelegde contacten.

Onderling kennen de oplossingen verschillen in de gegevens die door middel van Bluetooth worden verwerkt (o.a.: de (gepseudonimiseerde) ID van de tegengekomen gebruiker, datum en tijd(sbestek) van het contact, duur van het contact en signaalsterkte) en in welke fase ze worden gepseudonimiseerd. Ook verschilt of contacten alleen zichtbaar worden bij een match dan wel dat gebruikers real time inzage hebben in alle signalen die de app heeft geregistreerd.

Gegevens mogen uitsluitend worden uitgelezen of gedeeld als er sprake is van a) contact- of bronondersoek als bedoeld in art. 6 Wpg of b) toestemming van de gebruiker (grondslag)

In de installatie- en uitwisselingsfase van ieder van de voorstellen kan een grondslag worden gevonden in de toestemming van de gebruiker. Het merendeel van de verwerkingen in de validatiefase, waarschuwingsfase en koppelingsfase en notificatiefase binnen de voorstellen vindt plaats om de GGD te ondersteunen bij het bron- en contactonderzoek inzake de bestrijding van COVID-19. Een deel van het contactonderzoek wordt geautomatiseerd in de zin dat een gebruiker zelfstandig met zijn smartphone (via de server) gewaarschuwd kan worden dat hij mogelijk een risico op besmetting heeft gelopen. Voor zover een app in die fases (gepseudonimiseerde) persoonsgegevens verwerkt, bestaan goede argumenten dat de overheidsinstelling (de GGD) de verwerking kan baseren op artikel 9, tweede lid, aanhef en onder i, AVG jo. artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 6, eerste lid, aanhef en onder c, Wet publieke gezondheid (Wpg). Zekerheid op dit punt vergt nadere analyse en/of een nieuwe specifieke wettelijke grondslag.

Het huidige proces van bron- en contactopsporing is uitgangspunt ter ondersteuning. Het gebruik moet gericht zijn op het vereenvoudigen van contactonderzoek (doelbinding)

Bijna alle apps zijn gericht op het ondersteunen van bron- en contactopsporing. Enkele voorstellen bieden een platform aan waarop een dergelijke applicatie zou kunnen aansluiten.

In alle voorstellen lijkt te worden uitgegaan van enige vorm van centrale opslag van gegevens. In het gros van de voorstellen betreft dat alleen ID’s en/of keys. In bepaalde gevallen worden ook contactgegevens centraal opgeslagen. Dat laatste is behulpzaam voor de bron- en contactopsporing door de GGD. In die zin lijken de genoemde contactgegevens toereikend, ter zake dienend en niet bovenmatig te zijn voor het doel waarvoor de app zal worden gebruikt.

Er is voorzien in een informatieportal voor de gebruikers waarin fouten en kwetsbaarheden kunnen worden gemeld (transparantie)

Wij concluderen dat alle voorstellen in potentie aan dit uitgangspunt voldoen.

Gangbare beveiligingsstandaarden (beveiliging)

De beveiligingsexperts van KPMG hebben op 19 april 2020 een eerste securitytest verricht op de deelnemende apps. KMPG heeft daarbij onder meer gekeken naar specifieke beveiligingseisen en risico’s (Randvoorwaarde 4, Uitnodigingseis 22 en 23). Voor de vraag of de voorstellen voldoen aan de geldende beveiligingseisen, verwijzen wij naar de door KPMG uitgevoerde securitytest.

Als de app niet meer effectief of noodzakelijk is, moet de uitrol kunnen worden teruggedraaid en data kunnen worden verwijderd (verwijdering)

Wij concluderen dat alle voorstellen in potentie aan dit uitgangspunt kunnen voldoen en dat kan worden aangesloten bij de guidelines van het European Centre for Disease Prevention and Control.

4 Disclaimer

Deze samenvatting en onderliggende privacy-analyses zijn in opdracht van het Ministerie van VWS opgesteld om inzicht te geven in de privacy aspecten van de 7 apps die publiekelijk zijn gepresenteerd tijdens de zogenaamde Appathon. De samenvatting en privacy-analyses zijn uitsluitend bestemd voor het Ministerie van VWS. Derden kunnen daaraan geen rechten ontlenen; reeds omdat zij geen kennis dragen van de onderliggende adviesrapporten en die ook niet voor hen zijn bestemd. De in deze samenvatting en privacy-analyses opgenomen informatie is met zorg samengesteld. Toch kan Pels Rijcken – gelet op de aard van de werkzaamheden en de tijdsdruk – niet instaan voor de juistheid en volledigheid van de informatie. Zo is veel informatie over de 7 apps niet tijdig aan ons beschikbaar gesteld. Er is – gelet op de tijdsdruk – ook beperkt navraag gedaan of de documentatie compleet was en alles tijdig was aangeleverd. Daarnaast zijn er mogelijk na het verkrijgen van de initiële documentatie aanpassingen gedaan. Deze aanpassingen zijn niet door ons in deze samenvatting en privacy-analyses betrokken. Ten behoeve van deze samenvatting en privacy-analyses is tevens gebruik gemaakt van informatie van het Ministerie van VWS, van derden en van links naar externe websites.

De bevindingen in deze samenvatting en privacy-analyses zijn – gelet op de tijdsdruk en gelet op de opdrachtverlening van het Ministerie van VWS – niet op voorhand met de leveranciers van de 7 apps besproken en/of aan de leveranciers van de 7 apps ter beschikking gesteld.

Aan de samenvatting en privacy-analyses kunnen geen rechten worden ontleend. Voor onjuistheden of onvolledigheden op deze samenvatting aanvaardt Pels Rijcken geen aansprakelijkheid. Op de samenvatting en privacy-analyses zijn de algemene voorwaarden van Pels Rijcken & Droogleever Fortuijn N.V. van toepassing, te raadplegen via https://www.pelsrijcken.nl/algemene-voorwaarden.