To: Covid19-app[(10)(2e)@minvws.nl]; (10)(2e)[(10)(2e)@minvws.nl]
From: (10)(2e) (10)(2e)
Sent: Fri 4/17/2020 2:18:46 AM
Subject: Stukken beoordeling Autoriteit Persoonsgegevens - DEUS - Uitnodigingslimme digitale oplossingen
Received: Fri 4/17/2020 2:19:01 AM

Geachte mevrouw, mijnheer,
Onder verwijzing naar de email van de heer (10)(2e) van 16 april j.l. en bijlage 3, stuur ik u onderstaand de gevraagde benodigde documentatie t.b.v. de autoriteit persoonsgegevens. Dit n.a.v. de uitnodiging slimme digitale oplossingen en de uitnodiging voor de publieke beproeving.

Informatie t.b.v. beoordeling Autoriteit Persoonsgegevens:

Het verwerkingenregister
Voor de voorgestelde app onder vraag 1 van het 'vraag en antwoordformulier' van de 'uitnodiging slimme digitale oplossingen Corona' is bijhouden van een verwerkingsregister niet noodzakelijk. Een verwerkingsregister bevat immers informatie over persoonsgegevens die worden verwerkt. Maar op basis van de door ons voorgestelde aanpak vindt er geen verwerking van persoonsgegevens plaats.

Om de privacy van de gebruiker te waarborgen, vindt er bij de app geen uitwisseling of opslag van persoonsgegevens en privacy gevoelige informatie plaats. Er is alleen sprake van uitwisseling van de anonieme sleutels en EphID's. De EphID's zijn op geen enkele manier herleidbaar naar het toestel, de locatie van de gebruiker of aan andere data-punten die de identiteit van de gebruiker zouden kunnen onthullen.

De DPIA

Er is geen DPIA opgesteld voor de app voorgesteld onder vraag 1 van het 'vraag en antwoordformulier' van de 'uitnodiging slimme digitale oplossingen Corona' omdat bij deze app geen uitwisseling of opslag van persoonsgegevens plaatsvindt.

Om de privacy van de gebruiker te waarborgen, vindt er bij de app geen uitwisseling of opslag van persoonsgegevens en privacy gevoelige informatie plaats. Bij de app is alleen sprake van uitwisseling van de anonieme sleutels en EphID's. De EphID's zijn op geen enkele manier herleidbaar naar het toestel, de locatie van de gebruiker of aan andere data-punten die de identiteit van de gebruiker zouden kunnen onthullen.

Technische documentatie over opzet en werking van de app, opslag van data en informatiebeveiliging.

De slimme digitale oplossing die wij kunnen bieden om bij te dragen aan bron- en contactopsporing, is een mobiele applicatie (app) op basis van het DP-3T protocol van de PEPP-PT standaard. De app voldoet aan de voorwaarden zoals voorgesteld door (10)(2e) van de Waag Society en is tijdelijk, transparant, volledig anoniem, vrijwillig, gebruiksvriendelijk, niet commercieel en kan onder de regie van onafhankelijke deskundigen worden geïmplementeerd. In verband met de gestelde privacy en informatieveiligheid zal de app als stand-alone functioneren. Er zal dus geen integratie zijn met andere apps.

Daarbij wordt gebruik gemaakt van bestaande en geteste systemen op basis van het DP-3T protocol van de PEPP-PT standaard. Een keuze voor dit protocol wordt onderschreven door het Koninklijk Instituut Van Ingenieurs. Ruim 40 universiteiten, hogescholen, bedrijven en individuele experts werken al samen aan een Nederlandse open source implementatie van het Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project. De app zal voort blijven bouwen op de kennis en ervaring van deze community. De broncode van de app wordt eigendom van de Nederlandse staat maar wij stellen voor deze ook ter beschikking te stellen aan andere overheden en ontwikkelaars. Zo kunnen we bijdragen aan de verdere ontwikkeling en verbeteringen van deze digitale oplossingen in alle (Europese) landen en ook snel innovaties uit andere landen implementeren. Ook de geplande samenwerking en verbetering in bluetooth compatibiliteit die Google en Apple voor mei hebben aangekondigd, zal op relatief eenvoudige wijze, d.m.v. een update van de applicatie beschikbaar kunnen worden gesteld.

Er vindt bij de voorgestelde aanpak geen uitwisseling of opslag van privacy gevoelige opslag plaats. Wij stellen voor de opslag van anonieme sleutels en EphID's zal plaatsvinden op de gecertificeerde server omgeving van de overheid.

Eventuele expertrapportages (deskundigen oordelen, contra-expertise rapportages, evaluaties, technische test rapporten, et cetera)

40 universiteiten, hogescholen, bedrijven en individuele experts hebben in de afgelopen weken samengewerkt aan een Nederlandse open source implementatie van het Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project. Onze app bouwt voort op dit werk. Er zijn geen officiële expert-rapportages beschikbaar maar de algemene consensus binnen de NL technologiesector is dat het DP-3T protocol van de PEPP-PT standaard momenteel de beste optie is om bron- en contactopsporing te faciliteren binnen de strenge privacy vereisten in Nederland.

De duidelijke handleiding en instructie

Basis functionaliteit

De gebruiker download de app vanuit de app stores. Na het, voor de eerste maal, starten van de app wordt de gebruiker gevraagd om toestemming te geven tot de Bluetooth functionaliteit.

Gegevens uitwisseling

Om te weten wie er in de buurt is zal er gegevensuitwisseling noodzakelijk zijn. Deze gegevensuitwisseling moet volledig anoniem zijn en niet terug te herleiden tot een persoon, mobiel nummer of locatie. Verder willen we de hoeveelheid data die periodiek door het toestel gedownload zal worden zoveel mogelijk beperken om het dataverbruik van de gebruiker zo klein mogelijk te houden. Om aan deze twee belangrijke voorwaarden te voldoen is er gekozen voor een 2-delige uitwisseling van gegevens:

Het 1e deel van informatie heet de Secret Key. Dit is een 32 bytes lang getal dat volledig willekeurig gekozen wordt door de telefoon tijdens installatie. Het getal is niet gebaseerd op persoonlijke informatie. Deze Secret Key zal gedeeld worden indien een besmetting geconstateerd wordt. Elke dag zal de app een nieuwe Secret Key genereren op basis van de Secret Key van de dag ervoor.

Het 2e deel van informatie heet de EphID, dit is een 16 bytes lang getal wat berekend wordt op basis van de Secret Key, en aangezien de Secret Key niet gebaseerd is op persoonlijke informatie, is de EphID dit ook niet. Deze EphID wordt elke paar minuten gedeeld met telefoons in de buurt.

Het aanmaken van nieuwe data (zowel de Secret Key voor de nieuwe dag als de EphID's gebeurt door middel van een 1-richting wiskundige formule/hash). Het resultaat is te berekenen aan de hand van de invoerwaarde, maar de invoerwaarde is niet te herleiden aan de hand van het resultaat. De app zal zijn eigen Secret Keys en de ontvangen EphID's bewaren voor een periode van 14 dagen. Ieder toestel met de app zal dus EphIDs genereren en uitzenden maar ook 'luisteren' naar andere EphIDs die worden uitgezonden door toestellen in de nabijheid. Op deze manier faciliteert de app bi-directionele communicatie, zonder daadwerkelijke uitwisseling van privacy gevoelige informatie.

Functionaliteit bij constatering infectie van de gebruiker

Zodra er bij de gebruiker een Covid-19 infectie is geconstateerd, zal de gebruiker door een medisch specialist gevraagd worden om zijn/haar gezondheidsstatus in de app aan te passen. Om misbruik te voorkomen raden wij aan dat het veranderen van gezondheidsstatus alleen gedaan kan worden via een eenmalig gegenereerde TAN-code, die via de medisch professional verstrekt zal worden. Het verstrekken van deze TAN codes kan d.m.v. een website waar medisch personeel op kan inloggen. Indien een kortere termijn oplossing noodzakelijk is, kan voor een low-tech methode worden gekozen met gebruik van TAN code lijsten die naar medisch personeel worden gedistribueerd. Direct na het updaten van de gezondheidsstatus zal de app de Secret Keys (van de afgelopen 14 dagen) uploaden naar een centraal back-end systeem van de overheid. Daarmee hebben we de beschikking over alle EphID's waar de geïnfecteerde persoon een 'proximity event' mee heeft gehad en kunnen de apps die met deze EphID's zijn geassocieerd, via alerts worden geïnformeerd over deze events.

Functionaliteit bij constatering infectie voor personen die met de geïnfecteerde in contact zijn geweest

De app haalt automatisch iedere 6 uur de anonieme data van geïnfecteerde gebruikers op. De data die opgehaald wordt bestaat opnieuw uit de geheime sleutel, waardoor de anonimiteit van de gerapporteerde gebruikers altijd gewaarborgd blijft. Op basis van deze data zal de app de EphIDs recreëren van de gebruikers die een infectie hebben gemeld voor de gegeven periode. Deze EphIDs zullen vervolgens vergeleken worden met de EphIDs waarmee het toestel in nabij contact is geweest. Als blijkt dat het toestel van gebruiker in contact is geweest met een geïnfecteerde gebruiker voor een bepaalde tijdsduur, dan ontvangt de gebruiker een notificatie. De exacte vervolgstappen na een dergelijke notificatie willen wij graag in samenwerking met de medische professionals opstellen. Denk hierbij aan het informeren van de gebruiker met betrekking tot de RIVM richtlijnen, contact opnemen met lokale GGD of huisarts etc.

Beschreven aandacht voor vertrouwelijkheid en integriteit

Het DEUS team heeft meer dan een decennium hands-on ervaring met het design, de ontwikkeling, de (data)security en de 'run & maintain' van wereldwijde mobiele applicatie platforms. Het team was onder meer verantwoordelijk voor de wereldwijde mobiele app van bedrijven als Shell (live in 50+ landen, 20+talen, inclusief functionaliteiten als mobile payment, in-car payment en loyalty integratie), ABN AMRO, Aegon, De Nationale Politie, NUON, Van Lanschot Bankiers en voor pro-bono projecten als Smartify.org. Het team is het meest bekroonde app development team van Nederland met onder meer GSMA GloMo Awards (2x), Dutch Interactive Awards (3x), Edison Innovation Awards, FWA (4x), Webby Awards (3x), Smarties Awards (2x), SPIN Awards (2x), RedDot (best of the best) Awards.

Door onze ruime ervaring met payments, bancaire en apps met integratie van loyaliteitssystemen is vertrouwelijkheid en integriteit een vast onderdeel van onze project realisatie.

Beschrijving van controleerbaarheid van daadwerkelijk gebruikte oplossing

De ontwikkelde code en toekomstige nieuwe releases kunnen aan de hand van een code-review op kwaliteit en integriteit worden getest. D.m.v. ingebouwde crash-reporting software zal de app geautomatiseerd rapportages leveren m.b.t. betrouwbaarheid. De app, data-connecties en de servers zullen aan security en penetratie tests worden onderworpen. Zowel de code-review als security en pen-tests worden uitgevoerd door een gecertificeerde onafhankelijke derde partij.

Omschreven doel en doelgroep

Het doel van de app is om, de door het Outbreak Management Team (OMT) geadviseerde ondersteuning te bieden bij bron- en contactopsporing en daarmee de belasting van de GGD te reduceren. Daarbij moet de app de transitiestrategie faciliteren door mensen beter te informeren over mogelijk contact met geïnfecteerde personen. Daarbij moet de app gebruik maken van technieken die de privacy van eindgebruikers waarborgen conform de AVG-wetgeving en het publiek gerust kunnen stellen dat geen uitwisseling of opslag van privacy gevoelige informatie zal plaatsvinden.

Eventueel uitgevoerde audits
40 universiteiten, hogescholen, bedrijven en individuele experts hebben in de afgelopen weken samengewerkt aan een Nederlandse open source implementatie van het Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project. Onze app bouwt voort op dit werk. Er zijn geen audits uitgevoerd maar de algemene consensus binnen de NL technologiesector is dat het DP-3T protocol van de PEPP-PT standaard momenteel de beste optie is om bron- en contactopsporing te faciliteren binnen de strenge privacy vereisten in Nederland.

Documentatie waaruit volgt dat wordt voldaan aan de ISO normen

Er bestaan wereldwijd nog geen ISO gecertificeerde oplossingen voor de voorgestelde aanpak op basis van het DP-3T protocol van de PEPP-PT standaard.

Alle overige documentatie waarvan de ontwikkelaar / aanbieder denkt dat die relevant zijn in het kader van de vraag welke dataprotectierisico's gepaard gaan met het gebruik van de app.

Zoals eerder vermeld zal er geen uitwisseling of opslag van privacy gevoelige informatie plaatsvinden. Er is derhalve geen aanvullende informatie.

Contactgegevens voor aanvullende (technische en juridische dataprotectie gerelateerde) vragen.

(10)(2e) (10)(2e) - Managing Partner DEUS
Email: (10)(2e)@deus.ai
Mobiel: (10)(2e)

(10)(2e) (10)(2e) - Operations Lead
Email: (10)(2e)@deus.ai
Mobiel: 0647006160 (10)(2e)

(10)(2e) (10)(2e) - Technology Lead
Email: (10)(2e)@deus.ai
Mobiel: 062490239 (10)(2e)

Een overzicht per app van de bij die app aangeleverde documenten.
NVT

Ik hoor het graag als er naar aanleiding van deze informatie nog vragen zijn.

Met vriendelijke groet,

(10)(2e)

. . . . . .

(10)(2e) (10)(2e) - Managing Partner
Capite Procuratio

Keizersgracht 475, 1017 DL Amsterdam

(10)(2e)