CoronaMelder

Categorie 3: overheidsdiensten

Aanvrager: 5.1.2e, CSPO, Programma Realisatie Digitale Ondersteuning, Ministerie van Volksgezondheid, Welzijn en Sport – 5.1.2e @coronamelder.nl telefoon: 06- 5.1.2e
Namens: Ministerie van Volksgezondheid, Welzijn en Sport
Oplossing: CoronaMelder

Aanleiding
Bij infectieziekten is bron- en contactonderzoek zeer belangrijk om de verspreiding van de ziekte in te dammen. Wanneer een besmet persoon gemiddeld minder dan één persoon besmet wordt de ziekte ingedamd en de uitbraak gestopt. Om dat te realiseren voert de regionale GGD bron- en contactonderzoek(BCO) uit. Het doel is de bron van de uitbraak te achterhalen en mensen te waarschuwen. Dit betekent dat een besmet persoon wordt gevraagd naar de afspraken en contactgegevens.

Al is BCO sinds jaar en dag geaccepteerd dat neemt niet weg dat er een zeer forse inbreuk op de persoonlijke levenssfeer wordt gemaakt. Daarnaast leunt dit onderzoek op het geheugen van de persoon. Er zijn veel situaties waar de gegevens van contacten niet bekend zijn (bijvoorbeeld in openbare gelegenheden), niet alles even goed herinnerd wordt en niet altijd bekend hoe lang een contact duurde en met wie dat was. Kortom er wordt veel gemist. Toch blijkt dat het BCO een heel belangrijk hulpmiddel is in de strijd tegen infectieziekten.

De uitbraak van het Coronavirus (COVID-19) is voor het eerst sinds jaren een situatie waar bij herhaling de grenzen van het BCO worden bereikt. Dat betekent dat mensen dan het advies krijgen zelf contacten te waarschuwen of dat het in het geheel niet meer uit te voeren is. Mensen met een verhoogd risico krijgen geen concreet handelingsperspectief. De uitbraak van de infectieziekte wordt niet geremd.

CoronaMelder
Een fundamenteel verschil met eerdere uitbraken van infectieziekten is de brede verspreiding van smartphones onder de burgers. Met behulp van bluetooth (low energy) is het mogelijk te meten of iemand langdurig heel dichtbij iemand is geweest of binnen een redelijke afstand is geweest (grofweg één tot vijf meter). Een dergelijke vaststelling helpt bij het bepalen of bij een besmetting er dan sprake is van een contactmoment dat bij regulier BCO rechtvaardiging voor een waarschuwing. Voor dergelijke toepassingen zijn er diverse apps op de markt verschenen.

Het is eenvoudig een dergelijke technologie in te voeren, omdat er veel oplossingen beschikbaar zijn. Afgezet tegen traditioneel BCO zal in de meeste gevallen het eenvoudig zijn te stellen dat de privacyinbreuk minder met een app. Maar minder eenvoudig is het om een oplossing te bieden waar echt alle mogelijkheden zijn aangegrepen om iedere inbreuk op de persoonlijke levenssfeer tot een absoluut minimum terug te brengen.

Uitleg per voorwaarde om deel te nemen

A Waardering privacy

Zoals hiervoor beschrijven zijn veel vergelijkbare apps gemaakt, waarbij de privacy niet op de eerste plaats staat. Zo vragen sommigen persoonsgegevens bij ziekmeldingen, worden soms testuitslagen via de app geleverd, is er een centraal systeem, is er herleidbaar bewust aangebracht of kunnen zieken zeer gedetailleerde informatie aanleveren. Hoe nuttig dat ook misschien kan zijn, is CoronaMelder precies wat de naam zegt: alleen een waarschuwing als iemand langere tijd in contact is geweest met een besmet persoon. Niks meer, niks minder.

De minister heeft vanaf het begin aangegeven dat de privacy voorop staat en daarmee was het devies: privacy first, security meteen daarna en maximale toegankelijkheid (daarmee is CoronaMelder zo inclusief mogelijk opgezet). Bij iedere keuze die te maken is, staat de uitgangspunten voorop. Voor het proces geldt dat er maximale openheid wordt betracht: de documenten zijn openbaar van design tot DPIA, van risicoinschatting tot beveiligingsonderzoek, van verworven privacyadviezen tot notarisverklaringen om te controleren dat de open-sourcecode ook echt op de mobiele telefoon komt.

B – Maatschappelijke impact

In het traject is uitgebreid stilgestaan bij de impact die een app heeft. Door geen enkele functionaliteit toe te laten, die een inperking van persoonlijke levenssfeer mag worden. Om dit voor elkaar te krijgen, hebben we een onderscheid gemaakt tussen privacy in de praktijk en het privacyrecht. Je kunt prima aan de AVG voldoen en toch mensen in hun persoonlijke levenssfeer treffen. Er zijn losse privacymaatregelen getroffen aangevuld met de juridisch-gedreven stappen. Hierdoor staat de burger echt centraal en wordt gedacht vanuit het privacybelang van de burger.

Daarnaast is veel energie gestoken in een ethische analyse, waarin is onderzocht welke andere aspecten zouden kunnen spelen om daar vervolgens maatregelen op te nemen. Daarnaast is veel onderzoek gedaan naar gebruikersvriendelijkheid, zodat we echt weten of mensen begrijpen wat de app doet.

C – Innovatief vermogen

Een oplossing als deze was voor Corona niet beschikbaar. Het gebruikte protocol DP3T is vernieuwend, omdat het contacten registreert op zo'n manier dat voor overheid en burger niet gekend is wie met wie in contact is geweest. De cryptografie houdt deze informatie weg bij alle partijen. Ondertussen is het toch mogelijk een waarschuwing te geven volgens dezelfde regels als bij regulier bron- en contactonderzoek met grotere nauwkeurigheid en minder foutmarge ondanks de beperkingen van de bluetooth technologie.

Er zitten veel innovatieve onderdelen in CoronaMelder, zoals bijvoorbeeld:

- Innovatief voor de overheid is ook de 'mislukte appathon'. Deze marktconsultatie maakte duidelijk dat van de honderden oplossingen niets privacyvriendelijk genoeg was. De keus om dan maar zelf te beginnen is absoluut innovatief te noemen.

- Om herleidbaarheid van internetverkeer te voorkomen, wordt dummy verkeer gegenereerd.
- Bij weinig besmettingen worden er onbruikbare codes (dummies) neergezet. Hierdoor gaat bij laag volume de echte waarschuwing op in een pool van codes. Niemand kan zien of er nou 1 zieke is of er 150 zijn.
- Het model is zo opgezet dat de API-laag van Apple en Google die op de telefoon draait waarborgt dat CoronaMelder niet zomaar bij de uitgewisselde codes kan komen. Omgekeerd kan de API niet functioneren zonder een overheid goedgekeurde app. Iedereen vertrouwt elkaar minimaal, waardoor de beveiliging daarop is gericht. Dit dient de privacy direct.
- Er ligt een wet voor in de Eerste Kamer specifiek voor de app. Dat is nog niet eerder gedaan in Nederland. Hoogtepunten:
  - Het regelt de eindigheid van CoronaMelder.
  - Het stelt dwang en drang voor gebruik strafbaar.
  - Het verbiedt voor enig ander gebruik (dus ook opsporingsinstanties en inlichtigendiensten).
- Notarisverklaring (escrow) per release van de software, waardoor er zekerheid ontstaat dat de open-sourcecode op internet heeft geleid tot de app die naar de app stores in geüpload.
- Bij de bevestiging met een code is het invoeren bij de GGD neergelegd, zodat de gebruiker dat niet doet en kwaadwillenden niet kunnen afleiden dat een code is ingevoerd.

D – Zelfredzaamheid

Naar de aard van het product is het niet de bedoeling dat deze dienst blijvend wordt en kan blijven draaien.

E – Risicoanalyse

Er zijn meerdere risicoanalyses uitgevoerd. Uiteraard als eerste en vooral de gegevensbeschermingseffectbeoordeling (DPIA), daarnaast is er een dreigingsanalyse gemaakt, waarbij ondersteuning is verkregen van NCSC, NCTV & AIVD. Tot slot is er een uitgebreide Failure Mode Effect Analyses gemaakt. Alle resultaten zijn openbaar en zijn terug te vinden in de duidingsrapportage (zie de links aan het einde van het document voor nadere toelichting).

In de duidingsrapportage staan ook alle bevindingen uit onderzoeken. Tot slot staan alle genomen maatregelen op informatiebeveiliging en privacybescherming er uitgebreid in.

F - Privacyverantwoordelijke

Het Ministerie van Volksgezondheid, Welzijn en Sport beschikt over een Functionaris voor de Gegevensbescherming. Daarnaast is er een Chief Privacy Officer voor CoronaMelder en is er een Chief Security and Privacy Operations. Er is breed ingezet op het nemen van de privacyverantwoordlijkheid en wordt bewust de aansluiting gezocht met het onderdeel beveiliging. Uiteraard zijn er een Beveiligingsautoriteit, CISO en een project-CISO aanwezig.

G – Privacy policy

Er is een privacypolicy. Bij een complex thema als dit zoeken we nog naar de mogelijkheid om dit beeldender te krijgen (bijvoorbeeld in afbeeldingen) om het zo eenvoudiger te maken.

H – Privacy awareness

Privacy awareness is geborgd in dagelijkse communicatie binnen CoronaMelder en de centrale rol die juist privacy en security speelt. In alle processen heeft dat een centrale rol en in het team wordt veel toelichting en uitleg gegeven.

Maatregelen om privacy te beschermen

Er zijn 19 basale privacymaatregelen getroffen vanuit het ontwerp. De gedetailleerde beschrijving treft u in de duidingsrapportage aan, maar de punten zijn:

1. De app vraagt geen gegevens aan de gebruiker
2. De app werkt decentrale (geen herleidbare opslag)
3. Bewaart gegevens niet langer dan noodzakelijk
4. De uitgewisselde codes zijn niet te koppelen aan een persoon
5. De codes variëren regelmatig
6. Er worden regelmatig nepsleutels uitgezonden
7. Gebruikt alleen de strikt noodzakelijke gegevens
8. Besmetting worden door GGD'en gevalideerd. Anders worden contacten niet gedeeld.
9. GGD kan niet zien welke codes ze vrijgeeft
10. Software schermt gegevens voor app af
11. Er is en mag geen ander doel zijn dan COVID-bestrijding
12. Er worden geen statistieken in de app bijgehouden (om terug te zenden)
13. Geen cookies op de website, geen herleidbaarheid op website (logboeken voor VWS niet toegankelijk)
14. Specifieke wetgeving tegen verplicht gebruik, dwang of function creep
15. Melding niet traceerbaar
16. Sleutels wordt op alfabet gesorteerd beschikbaar gemaakt
17. Verkeersgegevens op internet worden meteen gescheiden van inhoudelijk verkeer
18. Sleutels zijn digitaal getekend
19. Geen backup mogelijk (dus geen rondslingerende informatie)

Er zijn ook ruim 60 beveiligingsmaatregelen getroffen, die in de duidingsrapportage staan. U treft deze hier aan: https://github.com/minvws/nl-covid19-notification-app-coordination/tree/master/privacy/Duidingsrapportage