App Coronalert scoort goed op privacy en gebruiksvriendelijkheid

29 september 2020 – Test Aankoop
Met wat vertraging is ze er eindelijk: de Belgische corona-app om de verspreiding van het virus mee te helpen indijken. Wij namen Coronalert onder de loep. De app is heel privacyvriendelijk en makkelijk in gebruik. Wat ons betreft dus weinig redenen om ze niet te installeren. We beantwoorden de voornaamste vragen.

Wat je moet weten over Coronalert

Het doel van de Belgische app Coronalert is de **verspreiding van het coronavirus tegen te gaan door het bron- en contactonderzoek te versnellen**. De app zorgt ervoor dat wie in nauw contact is geweest met een besmet persoon eerder gewaarschuwd kan worden, mits beide personen de app gebruiken.

Wat is de meerwaarde?

Coronalert kan bijhouden met wie je contact hebt gehad zonder dat je die persoon kent, bijvoorbeeld op de trein. Ook voor gevallen waarbij mensen schroom hebben om hun contacten aan een telefonist door te geven, biedt de app een oplossing, want de contacten worden volledig automatisch en anoniem in kaart gebracht. De app kan ook sneller werken dan telefonisch contactonderzoek.

Hoe werkt de app?

Ze maakt voortdurend **anonieme, willekeurige codes** aan. Deze codes worden uitgewisseld met andere smartphones die in de buurt zijn en de app gebruiken. De uitwisseling gebeurt via bluetooth. Naast het installeren van de app moeten gebruikers dus ook bluetooth in de instellingen van hun smartphone activeren.

Je smartphone bewaart alle codes die hij zelf heeft uitgestuurd én de codes van de personen met wie je in nauw contact kwam. De codes afkomstig van andere smartphones blijven maximaal 14 dagen op je toestel bewaard. De app registreert bij iedere code-uitwisseling ook de afstand op dat moment tussen twee Coronalert-gebruikers en de duur van het contact.

Twee scenario's zijn denkbaar:

- **Je test zelf positief op corona.** Dan kun je dit aangeven in de app. Je eigen codes worden dan verzonden naar een centrale server die in België wordt beheerd door Sciensano. De apps van andere smartphones kunnen die server aanspreken en zo de codes die ze hebben verzameld vergelijken met de codes op de server. Als er een match is en zij binnen twee meter én minstens 15 minuten bij jou in de buurt waren, dan krijgen zij een melding in de app met de vraag om een test af te leggen en in quarantaine te gaan.
- **Je ontvangt de melding "verhoogd risico".** Dat betekent dat jouw app op de centrale server codes heeft gevonden die ook op jouw toestel werden bewaard en dat je dus nauw contact hebt gehad met iemand die besmet is met het coronavirus. Minstens één keer per dag checkt de app of er een match is tussen de bewaarde codes en de naar de server geüploade codes. De melding laat alleen zien op welke dag het contact heeft plaatsgevonden, niet wie dit is en waar je die persoon bent tegengekomen.

Moet de app continu actief zijn?

Alles gebeurt automatisch. De app werkt volledig op de achtergrond, waardoor je je smartphone normaal kunt gebruiken. Zelfs al sluit je de app af, dan nog kan de app op de achtergrond werkzaam blijven (een speciale API - zorgt daar voor). Eens geïnstalleerd, hoef je er dus niet op te letten dat de app altijd actief is.

Wat moet er gebeuren opdat twee smartphones codes kunnen uitwisselen?

Uiteraard moeten **beide personen de app downloade**n in de Google Play of Apple App Store en installeren. Daarnaast moeten op beide toestellen bluetooth én de zogenaamde blootstellingsmeldingen geactiveerd zijn. Bij het openen van de app wordt je gevraagd om beide te activeren, dus proactief hoef je dat in principe niet te doen.

Is mijn privacy beschermd?

Ja. Privacy was erg belangrijk tijdens het bouwen van de corona-app. Het is ook één van de redenen waarom de uitrol zo lang op zich heeft laten wachten. Niemand wil dat bedrijven of hackers met gezondheidsgegevens aan de haal kunnen gaan. Of dat de app voor een ander doel wordt ingezet dan het coronavirus onder controle krijgen.

De privacy-technische aspecten van de app hebben we uitvoerig getest en uit onze analyse blijkt dat **de app geen steken laat vallen** op vlak van privacy. Aan de hand van de verzamelde en verstuurde gegevens is het niet mogelijk om je direct of indirect te identificeren. De app is **volledig anoniem**. Je wordt bovendien goed ingelicht over het privacybeleid.

Worden de gegevens ook veilig verstuurd?

Ja. Die worden zo goed mogelijk beschermd. De **uitwisselin**g van gegevens tussen de app en de servers **is versleuteld**. En dat geldt ook voor de gegevens die zich op je smartphone en op de servers bevinden. De servers zijn bestand tegen DDoS (Distributed Denial of Service)-aanvallen. Dat betekent dat IP-adressen die teveel verzoeken naar de server sturen, geblokkeerd worden. En de app is beschermd tegen "man-in-the-middle-aanvallen": hackers kunnen niet zomaar het internetverkeer tussen de app en de server onderscheppen.

Is installatie van de app verplicht?

Neen. De installatie is volledig vrijwillig. Ook het uploaden van de anonieme codes indien je positief test, is je eigen keuze.

Kan mijn kind de app installeren?

Er wordt vanuit gegaan dat een kind **vanaf 13 jaar** alleen kan instemmen met de installatie en het gebruik van de app. Onder deze leeftijd moet je als ouder in principe toestemming geven. De verantwoordelijkheid voor die toestemming ligt echter wel bij de ouders zelf. In de app is er geen aparte oplossing daarvoor voorzien.

Is mijn smartphonebatterij sneller leeg als ik de app gebruik?
De app gebruikt bluetooth en draait voortdurend op de achtergrond. Dat vergt altijd wat energie, maar volgens de makers van de app niet veel. De app gebruikt een bluetooth-techniek die minder stroom nodig heeft: Bluetooth Low Energy. Die techniek wordt onder andere ook gebruikt om de afstand en tijd tussen de gebruikers van de app in te schatten. Het stroomverbruik kan per smartphone wat verschillen, maar de **impact op je batterij zou heel beperkt moeten zijn**. Dit hebben we echter nog niet kunnen testen.

Werkt de app in andere landen?
Dat is wel de bedoeling. Er komt een overkoepelende "gateway" die gekoppeld is aan de nationale servers. Die gateway kan dan bijvoorbeeld gebruikt worden om Belgische anonieme codes te uploaden en codes van andere landen te downloaden. Coronalert zou hierbij aansluiten in oktober 2020.

Van wie is de app?
Coronalert werd gebouwd in opdracht van Sciensano, het Interfederaal Comité voor Testing & Tracing en de entiteiten verantwoordelijk voor de contactopsporing in Brussel, de Duitstalige Gemeenschap, Vlaanderen en Wallonië.

De app werd ontwikkeld door DevSide en Ixor. De veiligheidsaspecten werden gecontroleerd door NVISO.

Belangrijke onderdelen van de app zijn gebaseerd op de Duitse Warn-App, op de Europese open standaard DP3T (Decentralized Privacy-Preserving Proximity Tracing) en op de Exposure Notification-technologie van Apple en Google

Het privacyrapport

Uit onze test blijkt dat de app geen steken laat vallen op het vlak van privacy. Dit is wat we vaststelden:

- **Coronalert weet niet waar je bent:** gegevens tussen smartphones worden uitgewisseld via bluetooth. Locatiegegevens (gps) worden niet gebruikt en er wordt dus geen informatie verstuurd over de plaats waar je eventueel een "hoogrisicocontact" hebt gehad.
- **De app weet niet wie je bent of wie je ontmoet:** de enige gegevens die je met andere gebruikers uitwisselt, zijn anonieme codes. Geen namen, telefoonnummers of locaties. De uitgewisselde codes laten niet toe om iemand te identificeren.
- **Test je positief, dan weten andere gebruikers niet dat jij hen eventueel zou kunnen besmet hebben:** als je positief test en beslist om je codes naar de centrale server te uploaden, komen andere gebruikers met wie je een nauw contact hebt gehad enkel te weten dat ze een hoogrisicocontact hebben gehad, maar nooit met wie, waar of wanneer.
- **Op de centrale server passeren enkel de anonieme codes:** geen namen van patiënten of hun contacten.
- **De codes veranderen frequent:** ongeveer iedere 10 tot 20 minuten, zodat het niet mogelijk is om hiermee een smartphone te volgen.
- **De app vraagt niet om "verdachte" machtigingen:** de app vraagt bijvoorbeeld geen toegang tot je contacten, je locatie, je berichten of je telefoongesprekken.
- **Wanneer de app een server aanspreekt, gaat het internetverkeer via een proxyserver:** zo wordt je eigenlijke IP-adres verborgen.
- **Regelmatig doet de app een "dummy upload" naar de centrale server:** dit om uploads van "echte" codes naar de server (wanneer je positief zou testen) nog beter te maskeren.

Je wordt bovendien goed ingelicht over het privacybeleid. Je krijgt voldoende informatie in de app en kan doorklikken op links voor meer uitleg. Voor zowat élke handeling – het inschakelen van bluetooth bijvoorbeeld – moet je expliciet je toestemming geven. De broncode van de app staat integraal online: dit toont dat men zo transparant mogelijk wil zijn.

Kan de app mijn locatie achterhalen?

Neen, er worden geen locatiegegevens bijgehouden of doorgestuurd.
Er is wel een vervelend probleem met de versie die draait op Android-telefoons: daar moet je locatiediensten sowieso activeren om bluetooth te kunnen laten werken, ook al gebruikt de app zelf geen locatie-informatie. De activatie van locatiediensten zit ingebakken in het systeem, en daar kan de app-ontwikkelaar weinig aan doen.

Welke gegevens deelt de app met wie?

Dat is heel miniem en in feite beperkt tot anonieme (pseudonieme) gegevens:

- **Centrale server:** je kan anonieme codes opladen naar de centrale server. Deze centrale server wordt gehost door Sciensano.
- **Andere Coronalert-gebruikers:** Indien je je anonieme codes naar de centrale server verstuurt, worden deze dagelijks naar alle apps verstuurd.
- **Andere Europese databanken:** Als je in de app aangeeft dat je een ander EU-land hebt bezocht, kunnen je anonieme codes rechtstreeks of via de EU-"gateway" naar de centrale servers van vergelijkbare contactopsporingsapps in die EU-landen worden gestuurd,
- **Apple en Google:** zij kunnen enkel zien wie Coronalert heeft geïnstalleerd. Zij zorgen er wel voor dat het systeem jouw identiteit niet met hen deelt.

Hoe installeer ik de app?

Op welke smartphones werkt de app?

Coronalert werkt op de meeste smartphones:

- **iPhone**-bezitters moeten **tenminste** besturingssysteem **iOS 13.5** hebben (vanaf iPhone 6s). Dat laatste is een beslissing van Apple om voor oudere toestellen geen ondersteuning te bieden, daar hebben de ontwikkelaars van de app geen invloed op.
- Bij **Android**-gebruikers werkt de app **vanaf Android 6** ("Marshmellow"). Recente smartphones van **Huawei** hebben momenteel geen toegang tot de app store waar Coronalert beschikbaar is. De app-ontwikkelaars zouden in contact zijn met Huawei om hiervoor een oplossing te vinden. Op Huawei-toestellen met Google Play zal Coronalert wel werken.

Hoe download en installeer ik Coronalert?

De app is te installeren via de **App Store** op iPhones en **Google Play Store** op Android-smartphones. Zoek op 'Coronalert'.

Als je de app opent, zal die vragen om bluetooth en blootstellingsmeldingen te activeren. Je hoeft dat dus niet proactief te doen.

Wil je dit toch zelf doen, dan kan dit via de instellingen van je toestel.

- **Bluetooth**
  iPhone: Swipe omhoog vanaf de onderkant van het scherm > tik op Bluetooth
  Android: Swipe omlaag vanaf de bovenkant van het scherm > tik op Bluetooth

- **Blootstellingsmeldingen**
  iPhone: Instellingen > Blootstellingsmeldingen > Schakel blootstellingsmeldingen in
  Android: Instellingen > Google > Blootstellingsmeldingen voor COVID-19 > Blootstellingsmeldingen gebruiken.