Privacyverklaring CoronaMelder

Over CoronaMelder

CoronaMelder (app) is een technisch hulpmiddel dat helpt bij het beperken van de verspreiding van het COVID-19 virus. Als u CoronaMelder op uw smartphone heeft geïnstalleerd ontvangt u een bericht als u enige tijd in de buurt bent geweest van iemand die positief getest is op COVID-19, en deze persoon CoronaMelder ook geïnstalleerd heeft. Wanneer u mogelijk besmet bent door een andere gebruiker van CoronaMelder geeft de app het advies om u bij klachten te laten testen. Hieronder wordt in het kort uitgelegd hoe CoronaMelder werkt.

De app herkent via Bluetooth Low Energy andere smartphones waarop de app is geïnstalleerd. Het herkennen van de andere smartphones gebeurt aan de hand van willekeurige codes (getallenreeksen) die Rolling Proximity Indicators (RPIs) worden genoemd. Deze codes worden iedere 10 tot 20 minuten ververst, en zijn een afgeleide van zogenaamde Temporary Exposure Keys (TEKs). TEKs zijn ook willekeurige codes, maar deze codes worden per dag opnieuw gegenereerd, en 14 dagen op de telefoon van de gebruiker bewaard.

Als uw smartphone dichtbij een andere smartphone is waarop de app is geïnstalleerd, worden de verschillende RPIs uitgewisseld tussen die smartphones, en daarop lokaal opgeslagen. In het geval een gebruiker van de app positief getest is op COVID-19, kan de gebruiker er vrijwillig voor kiezen daarvan melding te maken in de app. Als daarvoor wordt gekozen stuurt de app de TEKs die de afgelopen 14 dagen zijn aangemaakt, en lokaal bewaard op de smartphone, naar een backend server. De backend server accepteert verzonden TEKs alleen als de gebruiker en de GGD de verzending hebben bevestigd met een validatiecode. Op de backend server worden de ontvangen TEKs omgezet in andere codes die Diagnosis Keys (DKs) worden genoemd.

De backend server stelt de DKs vervolgens beschikbaar, zodat deze automatisch kunnen worden opgehaald door de smartphones waarop de app is geïnstalleerd. Als uw smartphone de DKs heeft opgehaald van de server wordt de verbinding met de server verbroken. Dit geautomatiseerde proces herhaalt zich meerdere keren per dag om eventuele besmettingsrisico's up-to-date te houden. Vervolgens berekent uw smartphone aan de hand van de opgehaalde DKs of er een match is

met de verschillende RPIs van andere smartphones waarbij uw smartphone in de buurt is geweest. Direct daarna worden de DKs van uw smartphone verwijderd.

Als er een match is, wordt er op basis van een aantal weegfactoren bepaald of sprake is geweest van risicovol contact. Is dat het geval, met andere woorden bent u in de afgelopen tijd dichtbij een persoon geweest die besmet is met COVID-19, dan ontvangt u melding van uw verhoogde kans op besmetting. Ook geeft de app advies om u bij klachten te laten testen op besmetting met het virus.

1. Wie is verantwoordelijk voor de verwerking van de persoonsgegevens?

De Minister van Volksgezondheid, Welzijn en Sport is verwerkingsverantwoordelijk voor zover persoonsgegevens worden verwerkt bij de inrichting en het beheer van de CoronaMelder

Voor zover de Gemeentelijke Gezondheidsdienst (GGD) bij de bron- en contactopsporing gebruik maakt van persoonsgegevens die via de app worden verkregen is de GGD van uw regio verwerkingsverantwoordelijke.
Op www.GGD.nl kunt u vinden onder welke GGD u valt door de postcode van uw woonadres in te voeren. Indien u geen woonadres heeft in Nederland, kunt u de postcode van uw verblijfsplaats invoeren.

2. Met welk doel worden persoonsgegevens verwerkt?

Deze app is ontwikkeld als aanvulling op de bron- en contactopsporing van de GGD. Het doel ervan is om gebruikers met een verhoogde besmettingskans snel en op eenvoudige wijze te informeren, met een hoge mate van anonimiteit.

3. Grondslag voor het verwerken van persoonsgegevens

In de app kunnen persoonsgegevens worden verwerkt. De grondslag voor het verwerken van persoonsgegevens is de vervulling van, kort gezegd, een publieke taak. Voor de Minister van Volksgezondheid, Welzijn en Sport gaat het daarbij om de publieke taak om, kort gezegd, leiding te geven aan de bestrijding van COVID-19 en om zorg te dragen voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur.

Voor de GGD-en gaat het om de taak om bron- en contactopsporing te doen bij meldingen van een besmetting met COVID-19.

Met het invoeren van CoronaMelder als ondersteunend middel voor bron- en contactopsporing wordt dus uitvoering gegeven aan hiervoor genoemde publieke taken van de Minister van Volksgezondheid, Welzijn en Sport en de GGD-en.

Gebruik van CoronaMelder is vrijwillig. CoronaMelder vraagt daarom uw toestemming voordat u de app kunt gebruiken. Als u de toestemming niet geeft, kunt u CoronaMelder niet gebruiken. Uw toestemming wordt ook gevraagd voordat u – bij een positieve test – uw gegevens met de GGD kunt delen.

4. Welke persoonsgegevens worden verwerkt?

In de app worden de volgende gegevens verwerkt:

- Rolling proximity indicators (RPIs)
- Temporary Exposure Keys (TEKs)
- Diagnosis Keys (DKs)
- Pseudo MAC-adres
- Signaalsterkte en de contactduur
- Eerste ziekte dag
- Validatiecode
- Exposure Risk Value (high, mid, low)
- IP-adres

Deze gegevens kunnen persoonsgegevens zijn.

Een TEK is een willekeurig cryptografisch gegenereerde getallenreeks die dient als tijdelijke referentie. Op de backend server worden de TEKs geconverteerd naar DKs. Daarnaast wordt elke 10 tot 20 minuten een RPI gegenereerd, dat wil zeggen een tijdelijke, eveneens cryptografisch gegenereerde getallenreeks. Deze getallenreeks is een afgeleide van een TEK, en wordt uitgewisseld met andere smartphones waarop de app is geïnstalleerd, en die gedurende een vastgestelde tijdspanne in de buurt zijn geweest van de betreffende smartphone. Het ontvangen en uitzenden van de RPIs gebeurt via Bluetooth Low energy. De RPI wordt dan ook gebruikt in combinatie met signaalsterkte zowel uitgezonden als ontvangen (om afstand tussen gebruikers te bepalen), en de duur van het (Bluetooth)contact. De ontvangen RPIs worden na 14 dagen van de smartphones verwijderd.

Zowel de TEKs, DKs, als de RPIs zijn gepseudonimiseerde identificatiesleutels.

Om het risico op identificatie van gebruikers zoveel mogelijk uit te sluiten wordt bij de uitwisseling van RPIs het MAC-adres (een uniek hardware nummer van de Bluetooth-transmitter) van de smartphone vervangen door een random gegenereerde code, een pseudo MAC-adres, die evenals de RPIs elke 10 tot 20 minuten verandert.

De validatiecode wordt gegenereerd met behulp van een in de app aangeboden functionaliteit en in de app getoond. De validatiecode wordt door de GGD gebruikt om de aan de GGD verstuurde TEKs te valideren. De GGD plaatst deze validatiecode, met de datum van de eerste ziektedag, in het GGD-portaal. Dit GGD-portaal is alleen toegankelijk voor GGD-medewerkers. De backend server accepteert alleen TEKs van gebruikers als daarbij een validatiecode wordt aangeboden die op deze wijze door de GGD is gevalideerd. Tijdens de validatiefase worden voor beheers- en beveiligingsdoeleinden IP-adressen verwerkt.

In aanvulling op de DKs, eerste ziektedag, en validatiecode wordt ook het IP-adres meegestuurd naar de backend server. Dit is inherent aan het gebruik van internet en IP-technologie. Het IP-adres wordt gescheiden opgeslagen van de andere gegevens, zodat er op de backend server geen IP-adressen worden opgeslagen. Hierdoor kan niet worden herleid wie welke informatie heeft verstuurd.

5. Statistische informatie

De met de app verzamelde gegevens worden uitsluitend gebruikt voor de in deze privacyverklaring genoemde doeleinden. Er wordt geen statistische informatie gegenereerd.

6. Aan wie worden persoonsgegevens verstrekt?

Het uitzenden en ontvangen van de RPIs gebeurt lokaal op de smartphones. Als een besmetting is vastgesteld kan de gebruiker ervoor kiezen zijn of haar TEKs, tezamen met een unieke validatiecode, naar de backend server te sturen. De backend server wordt beheerd door het CIBG met KPN als onderaannemer (verwerker).

De GGD verwerkt de validatiecode, met de datum van de eerste ziektedag, in het GGD-portaal van de app, welk portaal alleen toegankelijk is voor geautoriseerde GGD-medewerkers.

De smartphones van andere gebruikers halen periodiek, enkele keren per dag, de DKs op die op deze backend server staan.

7. Bewaren van persoonsgegevens

De gegevens die lokaal zijn opgeslagen op jouw smartphone worden 14 dagen bewaard. Na deze 14 dagen worden deze gegevens automatisch en permanent verwijderd. U kunt ook zelf, op elk gewenst moment, de opgeslagen gegevens verwijderen.

Voor zover uw gegevens op de backend server zijn opgeslagen, worden de gegevens vanaf het moment van uploaden 14 dagen bewaard. Na deze 14 dagen worden de gegevens verwijderd.

IP-adressen die voor beheers- en beveiligingsdoeleinden worden verwerkt, worden na maximaal 7 dagen verwijderd.

8. Uw rechten ten aanzien van uw persoonsgegevens

U heeft een aantal rechten om controle te houden over uw persoonsgegevens. Deze kunt u hier vinden op de site van de Autoriteit Persoonsgegevens.

Omdat CoronaMelder is vormgegeven volgens de uitgangspunten van dataminimalisatie en privacy by design kunt u slechts beperkt een beroep doen op uw AVG-rechten. Er worden immers maar beperkt gegevens verwerkt. Gegevens zijn bovendien vrijwel niet herleidbaar en worden maar kort bewaard. Uit artikel 11 van de AVG volgt dat de rechten uit de artikelen 15 tot en met 20 van de AVG niet van toepassing zijn als de verwerkingsverantwoordelijke betrokkene niet (meer) kan identificeren.

In de eerste fase – vóórdat gebruikers TEKs naar de backend server uploaden – worden alleen gegevens verwerkt op de smartphones van gebruikers van CoronaMelder. Daar hebben de Minister van VWS en de GGD-en geen toegang toe. In deze fase kan dus bijvoorbeeld niet worden voldaan aan een verzoek tot wijziging of verwijdering van gegevens, waarbij uiteraard wel geldt dat deze

gegevens na maximaal veertien dagen automatisch van de smartphone worden verwijderd.

Door het privacy by design karakter van de app is het ook na het uploaden van de TEKs (later DKs) niet mogelijk om te achterhalen welke codes op de besmette gebruiker betrekking hebben. Het is voor VWS en de GGD-en technisch niet mogelijk om de codes die (tijdelijk) op de backend server zijn opgeslagen, te koppelen aan de gebruiker die zijn TEKs heeft geüpload. Vanwege de onmogelijkheid om de gebruiker te identificeren aan de hand van de codes zijn de rechten uit de artikelen 15 tot en met 20 van de AVG niet van toepassing.

De uitvoering van de AVG-rechten zal al met al dus maar beperkt nodig zijn, simpelweg omdat gegevens niet of maar zeer beperkt herleidbaar zijn tot personen dan wel omdat deze gegevens er niet meer zijn vanwege de korte bewaartermijnen. Hiermee wordt aangesloten bij artikel 11 van de AVG waaruit volgt dat de in de artikelen 15 tot en met 20 van de AVG opgenomen rechten niet van toepassing zijn als betrokkenen niet meer kunnen worden geïdentificeerd.

De mogelijkheid om een verzoek waarin u een beroep doet op een uw privacy rechten blijft echter bestaan. U kunt uw verzoek sturen naar de GGD die verantwoordelijk is in uw woonplaats. Op www.GGD.nl kunt u de postcode van uw woonadres invullen om te zien welke GGD verantwoordelijk is in uw woonplaats. Indien u geen woonadres heeft in Nederland, kunt u de postcode van uw verblijfsplaats invoeren.
U hebt altijd het recht een klacht over de verwerking van uw persoonsgegevens in te dienen bij de Autoriteit Persoonsgegevens of bij de rechter. Meer informatie daarover vindt u hier.

Contactgegevens van de Functionaris voor Gegevensbescherming van de GGD die verantwoordelijk is in uw woonplaats kunt u vinden via de website van die GGD.

Contactgegevens van de Functionaris voor Gegevensbescherming van het Ministerie van Volksgezondheid, Welzijn en Sport vindt u op de website van het dit ministerie.

9. Beveiliging van uw persoonsgegevens

De Minister van Volksgezondheid, Welzijn en Sport en de GGD-en nemen de bescherming van uw gegevens serieus en nemen passende maatregelen om

misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan.

10. Wijziging privacyverklaring

Deze privacyverklaring kan worden gewijzigd. In dat geval zullen wij de gewijzigde privacyverklaring op onze website publiceren, waarna deze privacyverklaring direct van kracht is. Laatste update: 10 september 2020