Privacymaatregelen

Deze diverse maatregelen zijn genomen om de privacy van gebruikers van CoronaMelder om zo goed mogelijk te borgen.

CoronaMelder vraagt geen gegevens van de gebruiker.

- De app werkt zonder locatie, naam, mailadres, telefoonnummer of andere contactgegevens.
- De app wisselt willekeurige codes uit met andere telefoons. In deze codes staan geen persoonsgegevens of locatiegegevens. De app weet niet wie of waar iemand is.
- Ook als iemand het coronavirus krijgt en deze persoon dit via de app meldt, is dit niet aan de naam of contactgegevens van deze persoon te koppelen.

CoronaMelder werkt decentraal

De app berekent op de telefoon – en niet op een centrale server – wanneer een gebruiker van CoronaMelder gewaarschuwd moet worden. Dit gebeurt op basis van verschillende factoren, zoals signaalsterkte van de bluetooth, duur van de ontmoeting en wanneer de besmette persoon zich ziek voelde. Hiermee weet niemand anders dat de persoon een melding krijgt.

CoronaMelder bewaart gegevens niet langer dan strikt noodzakelijk.

De willekeurige eigen sleutels en de via bluetooth low energy ontvangen codes blijven maximaal 14 dagen bewaard. Dit is de incubatietijd die gehanteerd wordt: langer dan deze periode is het onwaarschijnlijk dat iemand nog besmet kan worden met corona.

Uitgezonden codes zijn niet aan een persoon te koppelen

De codes die gedeeld worden via bluetooth, zijn niet aan een persoon te koppelen. Bij ziekte worden sleutels opgestuurd die niet meer worden gebruikt om uitwisselingscodes te maken.

- Via bluetooth delen telefoons met CoronaMelder elke tien tot twintig minuten willekeurige codes met elkaar. Deze codes zijn afgeleid van een, eveneens willekeurige, sleutel die elke de app elke 24 uur maakt. Deze codes zijn niet tot een persoon te herleiden.
- Als iemand na een test corona blijkt te hebben, kan deze persoon zijn of haar sleutels op een server zetten. De laatste sleutel wordt pas na middernacht geüpload, zodat een besmet persoon ook niet te herleiden is op de dag dat hij of zij te horen krijgt dat hij corona heeft.

Op deze manier zijn mensen niet te herkennen.

De codes die de gebruikers van CoronaMelder met elkaar delen, variëren iedere tien tot twintig minuten.

Elke tien tot twintig minuten maakt de app een willekeurige code, die telefoons met CoronaMelder elkaar delen als ze bij elkaar in de buurt zijn. Deze codes zijn afgeleid van een, eveneens willekeurige, sleutel die elke de app elke 24 uur maakt. Dit maakt herleidbaarheid van personen lastiger.

Vanuit een sleutel zijn de bijbehorende codes te herleiden: hiermee wordt de code van een besmette persoon herleid tot zijn of haar sleutel. Maar andersom is het niet mogelijk om vanuit de codes de bijbehorende sleutel te herleiden. Met dit eenrichtingsverkeer zijn de sleutels vergrendeld.

CoronaMelder stuurt regelmatig nepsleutels uit

CoronaMelder stuurt regelmatig nepsleutels uit, zodat iemand die ongewenst internetverkeer bekijkt niet kan zien welke ziekmeldingen echt zijn, en welke niet. Omdat de GGD de sleutels niet vrij geeft (het zijn echte ziekmeldingen) komen ze nooit als download beschikbaar. Iemand die het netwerkverkeer bekijkt zie dat niet, omdat het netwerkverkeer ook nog eens versleuteld is. Het is dus niet te onderscheiden of iemand écht anderen waarschuwt, of dat het een nep-waarschuwing is. Zo wordt voorkomen dat het opsturen van sleutels leidt tot herkenbaarheid.

Voorbeeld
Carla maakt via het wifi-netwerk op kantoor in CoronaMelder de melding dat ze corona heeft, en Tess kijkt stiekem mee via het netwerk. Dan kan Tess niet zien of Carla echt een melding gemaakt heeft, of dat het een nep-melding was.

CoronaMelder gebruikt alleen het absoluut strikt noodzakelijke om te functioneren.

In de app worden de volgende gegevens verwerkt:

- Rolling proximity indicators (RPIs): de codes die de app elke 10 tot 20 minuten maakt
- Temporary Exposure Keys (TEKs): de sleutel die de app elke 24 uur maakt
- Diagnosis Keys (DKs): een TEK die een besmet persoon deelt
- pseudo MAC-adres (een uniek hardware nummer van de Bluetooth-transmitter dat elke 10 tot 20 minuten verandert)
- signaalsterkte en de contactduur
- autorisatiecode (de GGD-sleutel in de app die een besmet iemand doorgeeft aan de GGD als deze persoon anderen wil waarschuwen)
- Exposure Risk Value (high, mid, low): de berekening van wanneer een gebruiker een melding krijgt
- IP-adres

Dit zijn allemaal zaken die echt strikt noodzakelijk zijn om CoronaMelder te laten functioneren. Al het andere zou alleen maar privacyrisico's kunnen introduceren.

Pas nadat de GGD een sleutel invoert, wordt een besmetting bevestigd.

Iedereen kan zijn sleutels via de app uploaden. Ook iemand die niet besmet is. De sleutels komen dan wel op de server, maar kunnen niet gedownload worden door andere app-gebruikers.

Sleutels kunnen pas gedownload worden als de GGD een GGD-sleutel (autorisatiecode) heeft gekregen. Deze staat in de app en leest een besmet persoon voor aan de GGD-medewerker die de besmette persoon telefonisch informeert over zijn of haar besmetting. De GGD-medewerker voert de GGD-sleutel in een portal in. Zo wordt de sleutel geverifieerd en wordt misbruik van de app voorkomen.

Als sleutels worden vrijgegeven dan kan de GGD niet zien of er is geüpload.

De GGD kan niet zien of iemand sleutels vervolgens daadwerkelijk uploadt en kan niet bij sleutels komen. Een besmet persoon kan binnen 24 uur bepalen of hij zijn sleutels wil delen nadat de GGD de GGD-sleutel in de portal heeft ingevoerd. Zo zijn deze gegevens ook voor de GGD afgeschermd.

De software van Apple en Google schermt gegevens af voor CoronaMelder.

CoronaMelder berekent wanneer een gebruiker waarschuwing moet krijgen. Voor deze berekening gebruikt de app software van Google en Apple. De app kan niet bij de sleutels en de ontvangen codes. Omdat deze versleuteld en vergrendeld zitten in de software van Apple en Google. Dit vormt extra bescherming tegen misbruik.

De voorwaarden van Apple en Google verbieden overheden gegevens voor een ander doel te gebruiken dan het bestrijden van COVID-19.

Apple en Google hebben hun software beschikbaar gesteld voor de bestrijding voor COVID-19. In hun licentievoorwaarden staat dat de app alleen hiervoor ingezet mag worden. Mocht iemand in de opsporing denken bij de sleutels te komen dan brengt daarmee CoronaMelder in gevaar. Want Google en Apple kunnen om die reden de licentie intrekken. Ieder ander gebruik is onwenselijk en is dan ook verboden.

Er worden in CoronaMelder geen statistieken bijgehouden.

Alhoewel het gebruikelijk is dat apps allerlei statistieken bijhouden, is dit bij CoronaMelder niet het geval. Er vloeit geen informatie terug naar centrale servers.

De website over CoronaMelder gebruikt geen cookies.

De website CoronaMelder.nl telt of registreert niets. Het bijhouden van gegevens zou tot personen kunnen herleiden, en wordt daarom vermeden. Er worden geen mensen gevolgd.

Er komt wetgeving die het verplichten van CoronaMelder strafbaar stelt.

Niemand mag iemand verplichten CoronaMelder te gebruiken. Werkgevers, verzekeraars, scholen of uitgaansgelegenheden mogen van niemand vragen de app te gebruiken.
Gebruik van de app moet geheel vrijwillig zijn en blijven. In het wetsvoorstel voor een noodwet voor de corona-app staat daarom bijvoorbeeld opgenomen dat mensen die misbruik maken van CoronaMelder een half jaar gevangenisstraf of 8.000 euro boete kunnen krijgen.

Niemand kan zien of iemand ooit een melding heeft gehad.

De app houdt geen gegevens bij. Er zijn geen statistieken of logboeken. Ook is nergens te zien of iemand een notificatie heeft gehad. Dit is alleen zichtbaar in de app voor de persoon zelf.

Sleutels gesorteerd op alfabet om herleidbaarheid te voorkomen.

Als iemand anderen wil waarschuwen via CoronaMelder, kiest deze persoon ervoor zijn of haar sleutels te delen. De sleutels van besmette personen worden op alfabetische volgorde geüpload, als extra stap om herleidbaarheid te voorkomen.

Bij het versturen van de sleutels naar de server worden deze direct gesplitst van het internetadres.

Als iemand anderen wil waarschuwen via CoronaMelder, kiest deze persoon ervoor zijn of haar sleutels te delen. Alleen de sleutel wordt dan geüpload naar de centrale server. Op de firewall wordt het internetadres ontkoppelt. Zo is niet te herleiden wie een sleutel heeft geleverd. Op deze manier is er geen herleidbaarheid.

De sleutels hebben een digitale handtekening.

CoronaMelder downloadt sleutels van mensen die besmet zijn met corona. Deze sleutels zijn altijd voorzien van een digitale handtekening. Zo herkent de app dat dit authentieke sleutels zijn. Zo wordt voorkomen dat mensen kunnen misbruik maken door valse sleutels beschikbaar te stellen.

Apple en Google maken geen back up van de sleutels op telefoons.

Of het nou een automatische of handmatige back up betreft, Apple noch Google maken back-ups van de sleutels op telefoons. Alles is erop gericht om de identiteit van mensen te beschermen.