Duidingsrapportage CoronaMelder

Informatiebeveiliging en privacybescherming

Stand van zaken, lanceringsadvies

Document beheer

Versie	1.00
Opsteller/onderzoeker	Brenno de Winter
Auteurs	Brenno de Winter Ed Lute Andrew Dasselaar Maria Frenken-Farag

Managementsamenvatting

Deze rapportage beschrijft de werking van CoronaMelder en duidt de status op het gebied van informatiebeveiliging en privacybescherming. Die twee onderwerpen bestaan uit het inzicht krijgen in risico's en ze terugbrengen tot een acceptabel niveau. Dit rapport is geen goedkeuringssysteem, maar een hulpmiddel om tot een inschatting te komen.

In Europa zijn (medio augustus 2020) tot dusver 191.920 dodelijke slachtoffers gevallen vanwege het COVID-19 virus. Het is aannemelijk dat het werkelijke dodenaantal hoger ligt. In het licht van de capaciteitsuitdaging bij de GGD-en, die veel van hun resources moeten inzetten voor het analoge bron- en contactonderzoek, is de bijdrage van digitale ondersteuning meer dan welkom. Het Outbreak Management Team (OMT) heeft geadviseerd om de mogelijkheden voor ondersteuning van bron- en contactopsporing met behulp van mobiele applicaties te onderzoeken.

Het doel van CoronaMelder is om – aanvullend op het bestaande, analoge bron- en contactonderzoek van de GGD-en – bij een geconstateerde COVID-19 infectie andere gebruikers van de app die in de nabijheid van de geïnfecteerde zijn geweest te informeren over hun verhoogde kans op besmetting. Het systeem is zo ingericht dat op ieder moment het herleiden naar gebruikers extreem moeilijk of zelfs onmogelijk is. Het gebruik van de app is vrijwillig en mag – geschraagd door nieuwe wetgeving – niet worden verplicht. De inzet van de app is tijdelijk en er is voorzien dat deze stopt wanneer de corona-pandemie is ingedamd. Bron- en contactopsporing sorteert het meeste effect wanneer zoveel mogelijk mensen die risicovol in de nabijheid van een geïnfecteerde persoon zijn geweest zo snel mogelijk kunnen worden gewaarschuwd. Hiertoe is het vereist dat mensen nog voordat er sprake is van enige besmetting bijhouden in wiens nabijheid zij zijn geweest.

De bouw van de app vindt plaats op transparante wijze in open source. Het gebruik van Coronamelder doorloopt qua chronologie de volgende vijf fasen:
1) Installatie
2) Uitwisseling
3) Validatie
4) Koppeling
5) Notificatie.

Langs meerdere wegen zijn er risico's rond informatiebeveiliging en privacybescherming in kaart gebracht. Er is een gegevensbeschermingseffectbeoordeling (DPIA, Data Protection Impact Assessment) opgesteld. Er is een dreigingsanalyse opgesteld voor nationale en digitale veiligheid. Tevens is een ethische analyse van de app opgesteld door een panel onder voorzitterschap van Prof.dr.ir. P.P.C.C. Verbeek, Universiteit Twente. Toezicht op de ontwikkeling van CoronaMelder wordt uitgevoerd door de Taskforce Digitale Ondersteuning Bestrijding COVID-19 en de Taskforce Gedragswetenschappen. Een Begeleidingscommissie adviseert de minister over het plan van aanpak en de waarde van de app vanuit een breder maatschappelijk perspectief (veiligheid, juridische, epidemiologische en gedragsaspecten).

Adequate privacy speelt een cruciale rol in de ontwikkeling van CoronaMelder. Daar is breed vorm aan gegeven. Daarnaast voldoet de app ook aan het privacyrecht, zoals in de AVG staat. Juist om een zo breed mogelijke acceptatie van de app in de maatschappij te bewerkstelligen, zijn keuzes gemaakt met privacy op de eerste plaats. Direct daarna komt security en

vervolgens toegankelijkheid. Pas nadat deze drie issues helemaal in orde zijn, volgen features. Want hoe breder het gebruik hoe effectiever de app kan bijdragen aan het daadwerkelijk uitvoeren van de exit-strategie. Dit rapport beschrijft de negentien genomen concrete maatregelen qua privacybescherming.

Het manifest 'Veilig tegen Corona' beschrijft de basale rechten en vrijheden van mensen met betrekking tot de app. Dit rapport toetst in hoeverre is voldaan aan de punten uit dit manifest. De conclusie is dat CoronaMelder voldoet aan alle punten van het manifest. Op geen enkel punt vindt er inbreuk plaats op de fundamentele rechten van de burger. Daarnaast worden de kritische zorgen van diverse organisaties – waaronder de Autoriteit Persoonsgegevens en het Rathenau Instituut – geadresseerd in dit rapport. Het is begrijpelijk dat er zorgen zijn, omdat nog nooit eerder bij een pandemie een dergelijk middel is ingezet en daarbij de toepassing ook nog per land verschilt. De laatste maanden hebben sommige landen mensen geweerd op locatie op basis van de app of vragen ze veel informatie. CoronaMelder stelt geen vragen, mag niet gebruikt worden om mensen te weren en is zeer conservatief: geen enkele inbreuk op rechten van burgers.

Een discussie over de noodzaak van CoronaMelder-app moet niet alleen gaan over (vermeende) privacy-bezwaren, maar zeker ook over de consequenties van het niet gebruiken van zo'n app. In onze zorgvuldigheid omtrent privacy en veiligheid mogen we niet vergeten dat we te maken hebben met een pandemie, die wij een halt willen toeroepen. Op de eerste plaats om de verschrikkelijke uitwerking van de ziekte op lange termijn. Daarnaast uit economisch oogpunt en – in verband daarmee – om redenen van levenskwaliteit. CoronaMelder is een hulpmiddel dat zorgvuldig en weloverwogen tot stand is gekomen.

Er is fors geïnvesteerd in het uitvoeren van onderzoeken om een beeld te krijgen of de app 'fit for purpose' is. Op het moment van schrijven worden de beveiligingsonderzoeken afgerond en vervolgonderzoeken opgestart om zo te blijven toetsen of beveiliging en privacybescherming maximale aandacht krijgen.

Uit de beveiligingsonderzoeken, testfases en onderzoeken naar de privacybescherming komen geen hoge risico's naar voren. Het is moeilijk te bedenken welke app vergelijkbare maatregelen kent om privacybescherming en informatiebeveiliging te borgen en ook geborgd te houden.

Eindoordeel

Op dit moment is er een situatie waarbij er geen hoge risico's blijken uit beveiligingsonderzoeken en onderzoeken naar de privacybescherming. Uit de testfase zijn deze risico's ook niet gebleken. Dat betekent dat er geen zogenaamde 'showstoppers' zijn. Mij is gebleken dat de minister goed doordrongen is van de risico's en daar acteert op een manier die zeer verantwoordelijk is. Het is moeilijk te bedenken welke app vergelijkbare maatregelen kent om privacybescherming en informatiebeveiliging te borgen en ook geborgd te houden.

Alles overziende neemt de minister geen onoverwogen beslissing door met deze app te gaan beginnen. De verwachting is niet dat de beveiligingsonderzoeken die nu lopen de komende dagen opeens een radicaal ander beeld gaan opleveren. Op basis van de huidige kennis van de situatie kan ik zeggen dat deze app voor wat betreft informatiebeveiliging en privacybescherming 'fit for purpose' is. Het dringende advies is wel om na lancering te

blijven doorgaan met het intensief bewaken van alle risico's en weer opnieuw risico's in kaart te brengen.

Conclusie
Alles overziende neemt de minister geen onoverwogen beslissing door met deze app te gaan beginnen. Uit de werkwijze, de resultaten van de onderzoeken komt een beeld naar voren dat deze app fit for purpose is. Het dringende advies is wel om na lancering te blijven doorgaan met het intensief bewaken van alle bestaande risico's en het in kaart brengen van potentiële nieuwe risico's.

Inhoudsopgave

Managementsamenvatting 1
Inhoudsopgave 4
Over deze rapportage 9
  Leeswijzer 9
De context: COVID-19 10
  Samenvatting COVID-19 10
  Acute gevolgen 11
  Verloop ziekte vaak langer dan gedacht 12
  Schade bij intensive care-patiënten 12
  Longproblemen 12
  Neurologische schade 13
  Extra gevaar voor kankerpatiënten 13
  Gevolgen voor kinderen 13
  Gevolgen op de lange termijn 14
  Stollingsafwijkingen 14
  Effecten per orgaan of ziekte op lange termijn 15
    Longen 15
    Zenuwstelsel 15
    Hart 16
    Maag en darmen 17
    Nieren 17
    Reproductieve organen 17
    Kanker 17
  Medicijnschade 17
  Ervaringen met andere coronavirussen (SARS-CoV-1, MERS) 18
  Economische effecten van de COVID-19-pandemie 18
    Consumenten 19
    Bedrijven 19
Over CoronaMelder 22
  Wat eraan voorafging 22
  Doel en scope van CoronaMelder 23
  Wetenschappelijke studies naar effectiviteit 23
    Oxford 23
    Isle of Wight 23
  Open source 24
  Vijf fasen 24

1. Installatiefase ... 25
2. Uitwisselingsfase ... 25
3. Validatiefase ... 27
4. Koppelingsfase ... 29
5. Notificatiefase ... 30
De vijf fasen in twee overzichten ... 31
De software ... 33
Persoonsgegevens ... 34
Bijzondere persoonsgegevens ... 35
Gegevensverwerkingen ... 36
Risico's in kaart brengen ... 37
Failure mode effect analyses (FMEA) ... 37
Dreigingsanalyse nationale en digitale veiligheid ... 44
Belangen ... 45
Scenario's en maatregelen ... 46
Advies van NCTV, NCSC en AIVD ... 47
Ethiek ... 48
Ethisch kader ... 48
Vrijwilligheid ... 49
Effectiviteit ... 50
Privacy ... 51
Rechtvaardigheid ... 52
Inclusiviteit ... 52
Procedurele rechtvaardigheid ... 53
Verantwoordelijkheid ... 54
Voorkomen van oneigenlijk gebruik ... 55
Borgen burgerlijke vrijheden voor de toekomst ... 55
Proportionaliteit en subsidiariteit ... 56
Noodzaak en evenredigheid ... 57
Doelstelling ... 57
Proportionaliteit ... 58
Subsidiariteit ... 58
Effectiviteit en evaluatie ... 58
Privacybescherming ... 60
Diverse maatregelen ... 60
1. Vraagt geen gegevens van de gebruiker ... 60
2. Werkt decentraal ... 60

3. Bewaart gegevens niet langer dan strikt noodzakelijk. ... 60
4. Uitgezonden codes niet aan persoon te koppelen ... 60
5. Regelmatige variatie van codes ... 61
6. Stuurt regelmatig nepsleutels uit ... 61
7. Gebruikt uitsluitend strikt noodzakelijke gegevens ... 61
8. Bevestiging van besmetting ... 62
9. Vrijgegeven sleutels niet zichtbaar voor GGD ... 62
10. Software schermt gegevens af ... 62
11. Geen ander doel ... 62
12. Geen statistieken ... 62
13. Geen cookies ... 62
14. Wetgeving tegen verplichting ... 62
15. Melding niet traceerbaar ... 63
16. Sleutels gesorteerd op alfabet ... 63
17. Verkeersgegevens worden gescheiden ... 63
18. De sleutels hebben een digitale handtekening ... 63
19. Geen back-up ... 63
Privacy-recht ... 64
Juridische termen ... 64
Persoonsgegevens ... 64
Bijzondere (categorieën van) persoonsgegevens ... 64
Verwerking ... 66
Verwerkingsverantwoordelijke ... 66
Verwerker ... 67
Betrokken partijen ... 67
Verwerkingsverantwoordelijken ... 67
Verwerkers ... 70
Doel van de verwerking ... 71
Grondslag van de verwerking ... 71
DPIA en advisering Autoriteit Persoonsgegevens ... 73
Informatiebeveiliging ... 76
Beveiligingsmaatregelen ... 76
Betrokken partijen ... 82
Onderzoeken ... 84
Bevindingen uit beveiligingsonderzoeken ... 85
Veilig tegen Corona ... 100
1ste uitgangspunt ... 100

Eén doel: het onder controle krijgen van het virus 100
De situatie bij lancering 100
2de uitgangspunt 102
Gebaseerd op wetenschappelijk inzicht en bewezen effectief 102
De situatie bij lancering 102
3de uitgangspunt 103
Bewezen betrouwbaar en vanuit expertise 103
De situatie bij lancering 104
4de uitgangspunt 105
De inzet van de applicatie is per definitie tijdelijk 105
De situatie bij lancering 106
5de uitgangspunt 106
Niet tot individuen herleidbaar 106
De situatie bij lancering 106
6de uitgangspunt 107
Zo min mogelijk gegevens worden gebruikt 107
De situatie bij lancering 107
7de uitgangspunt 107
Geen centraal opgeslagen persoonsgegevens 107
De situatie bij lancering 107
8ste uitgangspunt 108
Veilig en bestand tegen misbruik 108
De situatie bij lancering 108
9de uitgangspunt 108
Gebruikersvriendelijk en toegankelijk 108
De situatie bij lancering 108
10de uitgangspunt 109
Nooit onder dwang van overheden of derden 109
De situatie bij lancering 109
Aanvullende punten aan het einde van het manifest 110
De situatie bij lancering 110
Invloed op fundamentele rechten 111
Conclusie 111
Analyse kritische punten en zorgen maatschappelijke organisaties 113
Rathenau Instituut 113
Burgerrechten 113
Dé oplossing 113

Gefragmenteerde informatievoorziening 114
Rechtvaardiging en proportionaliteit 115
Google en Apple 118
Medische gegevens 119
Risico op profilering en stigmatisering 120
Klachten, bezwaren, wederhoor, schade en verhaalmogelijkheden 122
Eindoordeel 123
Appendix A. Uitleg FMEA 124
Risico's simpel maken met de foutmodus 124
Een analyse uitvoeren 126
Gevolg geven aan een Risk Priority Number 127

Over deze rapportage

Deze rapportage beschrijft de werking van CoronaMelder en duidt de status op het gebied van informatiebeveiliging en privacybescherming. Die twee onderwerpen bestaan uit het inzicht krijgen in risico's en ze terugbrengen tot een acceptabel niveau. Risico's verdwijnen nooit en kunnen – hoe klein ook – altijd optreden. Dit rapport is geen goedkeuringssysteem, maar een hulpmiddel om tot een inschatting te komen.

Daarnaast vergroot het rapport de transparantie door begrijpelijke context te geven bij de risico-inschattingen, de uitgevoerde onderzoeken en juridische documenten. Het is niet mogelijk alle onderzoeken openbaar te maken, zoals in het geval van interne bedrijfsdocumenten in een datacenter. Door deze toch te (laten) bestuderen door een onafhankelijke partij en op basis daarvan verslag te doen, ontstaat er toch inzicht. Voor de onderzoeken die door het Ministerie van Volksgezondheid, Welzijn en Sport zijn de rapportages waar mogelijk wel openbaar. Leveranciers die in aanmerkingen wilden komen om een opdracht te verwerven, hebben ingestemd met het openbaar maken van de rapportages. Daarbij geldt als randvoorwaarde dat de bevindingen zoveel mogelijk reproduceerbaar zijn.

Leeswijzer

In deze rapportage wordt gewerkt met verwijzingen naar documenten. Wanneer er sprake is van documenten die in het kader van het maken van CoronaMelder door het project of ingehuurde experts zijn gemaakt, worden deze als bijlage bijgevoegd om het beeld zo compleet maken. Voor de overige documentatie wordt verwezen naar online bronnen, waarbij de vindplaatsen in voetnoten worden verwerkt en duidelijk aangegeven wanneer deze door de auteurs zijn geverifieerd.

Citaten zijn herkenbaar omdat deze anders zijn opgenomen in de rapportage, zoals dit stuk tekst.

De context: COVID-19

Een discussie over de noodzaak van CoronaMelder-app moet niet alleen gaan over (vermeende) privacy-bezwaren, maar zeker ook over de consequenties van het niet gebruiken van zo'n app.

De verregaande veiligheid en privacybescherming van CoronaMelder – zoals uit het vervolg van dit rapport zal blijken – geeft afdoende antwoord op de vraag 'Is de app veilig voor gebruikers?' Toch is er nog een andere vraag, die minstens zo belangrijk is: 'Mogen we de burger een dergelijke app onthouden?'

Het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (het EVRM) bevat diverse artikelen die gezamenlijk de basis vormen voor 'het recht op bescherming van de gezondheid'. Ook het Internationaal Verdrag inzake economische, sociale en culturele rechten (IVESCR) schraagt dit recht. Artikel 12, tweede lid aanhef en onder c van de IVESCR verplicht de Staat der Nederlanden om uitbraken, zoals COVID-19 te bestrijden. Het herzien Europees Sociaal Handvest vermeld zelfs een plicht tot het nemen van maatregelen.[1]

Er is duidelijk een spanningsveld tussen het enerzijds beschermen van privacy en anderzijds het bieden van bescherming van de gezondheid. De toekomst, waarin we ervaring met notificatieapps als CoronaMelder zullen opdoen en waarin nieuw wetenschappelijk onderzoek zal volgen, zal hier ongetwijfeld licht op schijnen.

De inzet van CoronaMelder gaat niet alleen om geredde mensenlevens, maar ook om voortdurende ziektelast bij overlevenden. Zoals verderop in dit hoofdstuk duidelijk zal worden, is het redelijk om te veronderstellen dat een aanzienlijke groep COVID-19-patiënten nog lange tijd nodig zullen hebben om te herstellen. Misschien is volledig herstel zelfs helemaal niet haalbaar voor een groep. De schade daarvan in immateriële termen en qua geld valt op dit moment nog nauwelijks uit te drukken. Het laat zich aanzien dat deze in ieder geval aanzienlijk zal zijn.

Samenvatting COVID-19

De ziekte COVID-19 wordt veroorzaakt door het SARS-CoV-2-virus, een coronavirus dat waarschijnlijk in 2019 van dieren op mensen is overgesprongen. Hoewel in sommige media en zelfs door sommige staatshoofden laconiek wordt gedaan over de ernst van COVID-19, is daar weinig reden toe. In Europa zijn (medio augustus 2020) tot dusver 191.920 dodelijke slachtoffers gevallen.[2] Het is aannemelijk dat het werkelijke dodenaantal hoger ligt.[3] [4]

COVID-19 verloopt in veel gevallen relatief mild, maar verspreidt zich snel. Het veroorzaakt met name bij ouderen, chronisch zieken en kankerpatiënten veel sterfte. De sterfte door

[1] Artikel 11, aanhef en derde lid

[2] Data van https://coronavirus.jhu.edu/ verwerkt op https://covid19-projections.com/#europe-summary - geverifieerd op 17-08-2020

[3] https://www.rivm.nl/monitoring-sterftecijfers-nederland - geverifieerd op 17-08-2020

[4] https://www.nytimes.com/interactive/2020/04/21/world/coronavirus-missing-deaths.html - geverifieerd op 17-08-2020

COVID-19 ligt vermoedelijk 6 tot 10 keer hoger dan bij andere veel voorkomende infectieziekten zoals seizoensgriep.

Ook in zogenaamd 'milde' gevallen kan COVID-19 serieuze consequenties hebben voor de gezondheid van de patiënt. Zo lijkt het er sterk op dat COVID-19 – ook bij sommige milde gevallen – vaak een langer beloop heeft dan verwacht. Er zijn bovendien aanwijzingen dat er nadien bij een significante groep patiënten langdurige en mogelijk blijvende schade optreedt aan longen, hart, zenuwstelsel en andere organen en weefsels.

Veel van deze inzichten zijn gebaseerd op recent onderzoek, dat vaak in haast is uitgevoerd, en waarbij kanttekeningen zijn te stellen qua onderzoeksopzet. De gouden standaard voor medische studies is prospectief, dubbelblind en gerandomiseerd onderzoek. Een flink aantal COVID-19-studies zijn echter retrospectief. Deze blikken met andere woorden terug op ziektegevallen.

Dat deze recente wetenschappelijke inzichten overeind blijven, wordt waarschijnlijker door de opgedane kennis tijdens de SARS-epidemie van 2003. Het hiervoor verantwoordelijke SARS-CoV-1-virus lijkt sterk op het huidige SARS-CoV-2-virus en veroorzaakt eveneens een zogeheten ARDS (acute respiratory distress syndrome, of acuut respiratoir stress syndroom). Ook hier was bij een grote groep patiënten nog jaren na afloop sprake van problemen.

Hierbij moet wel worden aangetekend dat een ARDS bij COVID-19 andere karakteristieken heeft dan het traditionele SARS-ARDS. Deze verschillen dragen bij aan het onzekere beeld over de langetermijngevolgen van COVID-19. De eerste medische onderzoeken naar het COVID-19-ARDS zijn niet per se hoopgevend.

Acute gevolgen

In Europa zijn (medio augustus 2020) tot dusver 191.920 doden gevallen.[5] Het is aannemelijk dat het werkelijke dodental hoger ligt.[6] [7] De World Health Organization (WHO) schat de grove sterfteratio door COVID-19 op 3 tot 4 procent.[8] Dit is echter geen bruikbare maatstaf, aangezien hier het aantal sterfgevallen wordt gedeeld door het aantal bekende infecties. Echter, lang niet iedereen die geïnfecteerd wordt met SARS-CoV-2, wordt ook middels een test geïdentificeerd, al was het maar omdat er vermoedelijk veel infecties zijn die asymptomatisch of mild verlopen, mogelijk omdat er bij sommige mensen al sprake is van gedeeltelijke immuniteit op basis van eerdere infecties met andere coronavirussen.[9]

De Amerikaanse Centers for Disease Control and Prevention (CDC) houden rekening met een Infection Fatality Rate (IFR), oftewel sterfte op het totaal aantal infecties, van 0,65 procent in de Verenigde Staten.[10]

---

[5] Data van https://coronavirus.jhu.edu/ verwerkt op https://covid19-projections.com/#europe-summary - geverifieerd op 17-08-2020

[6] https://www.rivm.nl/monitoring-sterftecijfers-nederland - geverifieerd op 17-08-2020

[7] https://www.nytimes.com/interactive/2020/04/21/world/coronavirus-missing-deaths.html - geverifieerd op 17-08-2020

[8] https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-similarities-and-differences-covid-19-and-influenza - geverifieerd op 16-08-2020

[9] https://www.cell.com/cell/fulltext/S0092-8674(20)31008-4?rss=yes - geverifieerd op 16-08-2020

[10] https://www.cdc.gov/coronavirus/2019-ncov/hcp/planning-scenarios.html - geverifieerd op 16-08-2020

Ook dit cijfer is met een hoop onzekerheden omgeven, maar ligt aanmerkelijk hoger dan de geschatte IFR van de seizoensgriep, die zo rond de 0,1 procent ligt.[11] Het wetenschappelijke tijdschrift Nature meldde dat de geschatte IFR's van land tot land variëren tussen de 0,6 en 1 procent.[12] Hierbij moet worden aangetekend dat de kwaliteit van en toegang tot de gezondheidszorg een belangrijke factor is: hoe beter de (toegang tot de) zorg, hoe lager de IFR.

Verloop ziekte vaak langer dan gedacht

Het verloop van COVID-19 duurt veelal langer dan de twee weken die meestal wordt aangehouden voor gevallen waarbij ziekenhuisopname niet noodzakelijk is. De UK Covid-19 Symptom Study App verzamelde informatie van (in juni 2020) bijna 4 miljoen COVID-19-patiënten. Daarvan had één op de tien patiënten een ziekteverloop dat drie weken of langer duurde.[13] Ook Amerikaans onderzoek, zoals gepubliceerd door de CDC, laat een herstel zien dat in één op de drie gevallen langer dan twee of drie weken duurt.[14]

Schade bij intensive care-patiënten

Opname op een intensive care-afdeling leidt vaak tot langdurige gevolgen, zoals spierverlies. Delier, geheugenverlies en cognitieve problemen worden ook vaak gerapporteerd.[15] Iemand die een intensive care-opname heeft ondergaan, heeft vaak veel nazorg nodig.[16] Zo bestaat de kans op chronische pijn.[17] Ook zijn er psychiatrische symptomen, zoals in één op de vijf gevallen angst, depressie en post-traumatische stress-stoornis. Deze aandoeningen kunnen, zo blijkt uit onderzoek bij andere intensive care-opnames, tot vijf jaar na een opname aanhouden.[18]

Longproblemen

Bij ernstige gevallen van COVID-19 doet zich vaak een zogeheten acute respiratory distress syndrome of ARDS voor. Hierbij verkeren patiënten in acute ademnood en moeten ze veelal geïntubeerd en beademd worden. Aanvankelijk werd gedacht dat het ARDS dat optreedt bij COVID-19 identiek was aan het ARDS zoals dat zich voordoet bij SARS-CoV-1, het coronavirus dat in 2003 toesloeg en MERS, het coronavirus dat tussen 2012 en 2015 voor meerdere uitbraken zorgde. Inmiddels is duidelijk dat het COVID-19-ARDS andere kenmerken heeft en ook een andere behandeling vereist.[19] Hoewel COVID-19 voor individuele patiënten minder dodelijk is dan SARS en MERS, verspreidt het SARS-CoV-2-virus zich wel sneller.[20]

---

[11] https://www.cdc.gov/flu/about/burden/2017-2018.htm - geverifieerd op 15-08-2020
[12] https://www.nature.com/articles/d41586-020-01738-2 - geverifieerd op 16-08-2020
[13] https://covid.joinzoe.com/post/covid-long-term - geverifieerd op 15-08-2020
[14] https://www.cdc.gov/mmwr/volumes/69/wr/mm6930e1.htm - geverifieerd op 16-08-2020
[15] https://www.termedia.pl/COVID-19-What-do-we-need-to-know-about-ICU-delirium-during-the-SARS-CoV-2-pandemic-,118,40590,0,1.html - geverifieerd op 15-08-2020
[16] https://www.medicaljournals.se/jrm/content/abstract/10.2340/16501977-2677 - geverifieerd op 16-08-2020
[17] https://journals.lww.com/anesthesia-analgesia/FullText/2020/07000/COVID_19_Pandemic_Acute_Respiratory_Distress.19.aspx - geverifieerd op 16-08-2020
[18] https://www.nature.com/articles/s41572-020-0201-1 - geverifieerd op 15-08-2020
[19] https://www.thelancet.com/journals/lanres/article/PIIS2213-2600(20)30304-0/fulltext - geverifieerd op 15-08-2020
[20] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7176926/ - geverifieerd op 16-08-2020

Neurologische schade

Acute serieuze neurologische consequenties van COVID-19 zoals beroertes, infarcten of hersenontstekingen zijn relatief zeldzaam, maar komen toch dusdanig vaak voor dat ze gezien de omvang van de pandemie relevant zijn.[21] COVID-19 zorgt wel voor diverse andere neurologische klachten, zoals reuk- en smaakverlies, waarover meer in de sectie 'Gevolgen op de lange termijn'.

Extra gevaar voor kankerpatiënten

Er zijn aanwijzingen dat een kankerdiagnose de kans verlaagt om COVID-19 te overleven. Dit blijkt onder meer uit een studie bij patiënten die bestraling van de longen ondergingen. Bij hen was het sterfterisico aan COVID-19 zo'n 35 procent.[22] Kankerpatiënten die besmetting met SARS-CoV-2 vrezen, zouden ervoor kunnen kiezen om bestraling te vermijden, wat hun kans om aan kanker te bezwijken vergroot. Bij kankerpatiënten die besmet zijn, kunnen bestralingen veelal niet doorgaan, maar daardoor krijgt kanker de kans om zich verder te verspreiden.

In een andere studie onder 800 kankerpatiënten die COVID-19 kregen, overleed 28 procent van de patiënten. Van de 800 hadden 412 patiënten (52 procent) een mild verloop van COVID-19. Uit dit onderzoek bleek overigens niet dat het ondergaan van chemotherapie, immunotherapie, hormoontherapie, targeted therapy (doelgerichte therapie) of radiotherapie in de vier weken voorafgaand aan een SARS-CoV-2-infectie enig effect had op de overleving.[23]

In een kleine retrospectieve studie in Saoedi-Arabië was eerder gebleken dat bij een MERS-uitbraak liefst 84 procent van de onderzochte kankerpatiënten overleed.[24] Daar moet wel bij worden aangetekend dat het hier ging om een retrospectieve, dus terugblikkende, studie. Dit type studie wordt door wetenschappers niet als ideaal beschouwd. Ook is het MERS-virus weliswaar een coronavirus, maar aanmerkelijk dodelijker dan SARS-CoV-2.

Gevolgen voor kinderen

Hoewel COVID-19 met name gevaarlijk is voor ouderen, kan zich bij kinderen een gevaarlijke, grootschalige ontstekingsreactie voordoen die meerdere organen treft, het zogeheten multisystemisch inflammatoir syndroom, dat lijkt op de ziekte van Kawasaki.[25] Deze ziekte doet zich meestal twee tot vier weken na een SARS-CoV-2-infectie voor.[26] Bij dergelijke patiënten worden onder meer vaak hartproblemen geconstateerd, net als

[21] https://www.thelancet.com/journals/laneur/article/PIIS1474-4422(20)30221-0/fulltext#seccestitle70 - geverifieerd op 16-08-2020
[22] https://www.sciencedirect.com/science/article/pii/S2452109420301226 - geverifieerd op 17-08-2020
[23] https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)31173-9/fulltext - geverifieerd op 16-08-2020
[24] https://doi.org/10.1200/GO.20.00064 - geverifieerd op 16-08-2020
[25] https://www.nejm.org/doi/10.1056/NEJMoa2021756 - geverifieerd op 15-08-2020
[26] https://www.cdc.gov/mmwr/volumes/69/wr/mm6932e2.htm - geverifieerd op 16-08-2020

ontstekingen in het maag-darmkanaal.[27] [28] [29] Zowel Franse als Amerikaanse onderzoeken laten zien dat in veel gevallen opname op de intensive care noodzakelijk is.[30] [31]

Gevolgen op de lange termijn

De Nederlandse huisarts Jako Burgers publiceerde in augustus in wetenschappelijk vakblad BMJ een brief waarin hij het heeft over 10.000 tot 20.000 Nederlanders met 'long COVID', de term waarmee patiënten worden aangeduid die hersteld zijn van COVID-19, maar nog steeds last hebben van symptomen.[32] Ook wordt hiervoor de term post-acute COVID-19 gebruikt. Nederlandse patiënten met aanhoudende longproblemen kunnen zich inmiddels online registreren.[33] Ook in andere landen, zoals Groot-Brittannië, zijn er soortgelijke initiatieven.[34]

De aanwijzingen voor problemen op de lange termijn als gevolg van COVID-19 worden steeds sterker. Een artikel in vakblad BMJ schat dat 10 procent van alle COVID-19-patiënten langdurige klachten heeft.[35] Uit Italiaans onderzoek gepubliceerd in het goed aangeschreven medische vakblad JAMA blijkt dat zestig dagen na het eerste ziektesymptoom liefst 87,4 procent van herstelde COVID-19-patiënten meldde tenminste één klacht te hebben, voornamelijk vermoeidheid en kortademigheid.[36] Volgens de studie had 32 procent één of twee symptomen, en 55 procent drie of meer. Slechts 13 procent was na zestig dagen volledig klachtenvrij.

Stollingsafwijkingen

Bij COVID-19 doen zich regelmatig problemen voor met de bloedstolling.[37] Een Canadees wetenschappelijk artikel noemt percentages tussen de 20 en 55 procent bij COVID-19-patiënten die in het ziekenhuis worden opgenomen.[38] Dit kan onder meer leiden tot longembolieën of veneuze trombose, waarbij een bloedstolsel de circulatie naar weefsels beperkt of stopt.[39] Als hierdoor weefsel afsterft, vergroot dit de kans op langetermijnproblemen. Stollingsstoornissen bij COVID-19 lijken te verschillen van stollingsstoornissen bij bijvoorbeeld bacteriële bloedvergiftiging (sepsis).[40]

---

[27] https://jamanetwork.com/journals/jama/fullarticle/2767207 - geverifieerd op 15-08-2020
[28] https://ard.bmj.com/content/79/8/999 - geverifieerd op 16-08-2020
[29] https://www.bmj.com/content/369/bmj.m2094
[30] https://www.eurosurveillance.org/content/10.2807/1560-7917.ES.2020.25.22.2001010 - geverifieerd op 15-08-2020
[31] https://www.nejm.org/doi/10.1056/NEJMoa2021680 - geverifieerd op 15-08-2020
[32] https://www.bmj.com/content/370/bmj.m3202 - geverifieerd op 16-08-2020
[33] https://coronalongplein.nl/ - geverifieerd op 16-08-2020
[34] https://www.phosp.org/study-news/phosp-covid-launching-press-release/ - geverifieerd op 15-08-2020
[35] https://www.bmj.com/content/370/bmj.m3026 - geverifieerd op 16-08-2020
[36] https://jamanetwork.com/journals/jama/fullarticle/2768351 - geverifieerd op 16-08-2020
[37] https://www.thelancet.com/journals/lanhae/article/PIIS2352-3026(20)30151-4/fulltext - geverifieerd op 15-08-2020
[38] https://www.cmaj.ca/content/192/21/E583 - geverifieerd op 16-08-2020
[39] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7225095/ - geverifieerd op 16-08-2020
[40] https://ccforum.biomedcentral.com/articles/10.1186/s13054-020-03077-0 - geverifieerd op 15-08-2020

Effecten per orgaan of ziekte op lange termijn

Longen

In een Chinees onderzoek werden bij 39 van de 55 patiënten afwijkingen in de longen aangetroffen via CT-scans. Bij 14 patiënten in hetzelfde onderzoek was de longfunctie niet normaal.[41] In een ander Chinees onderzoek, dat niet 'peer reviewed' is, was bij 22 procent van de onderzochte herstelde patiënten na dertig dagen of langer nog longschade te zien op een CT-scan.[42]

Zenuwstelsel

Van coronavirussen is bekend dat ze effect kunnen hebben op het zenuwstelsel.[43] Reuk- en smaakverlies zijn relatief vaak voorkomende klachten bij COVID-19-patiënten. Bij onderzoek in Italië bleek dat na veertig dagen 83,4 procent van de patiënten het reukvermogen teruggekeerd was.[44] In een Zuid-Koreaans onderzoek hadden de meeste patiënten na drie weken hun smaak- en reukvermogen terug.[45] Maar een Chinese studie toonde ook gevallen aan waarbij het reukverlies na 95 dagen nog aanwezig was. Oudere en rokende patiënten hadden meer last van reukverlies.[46] Duitse onderzoekers meldden dat bij 50 procent van onderzochte patiënten het reukvermogen na zeven weken nog niet (volledig) was hersteld. Het ging hier om relatief jonge patiënten, met een gemiddelde leeftijd van 43,2 jaar.[47] Italiaanse wetenschappers stelden vast dat bij 9,5 procent van onderzochte patiënten na 32 dagen nog sprake was van smaakverlies.[48]

In China werden bij een onderzoek in 36,4 procent van de gevallen neurologische gevolgen geconstateerd.[49] COVID-19 blijkt ook maanden na een infectie nog te zorgen voor veranderingen in de hersenen. Een ander Chinees onderzoek, gepubliceerd in het vakblad EClinicalMedicine, vond zulke veranderingen in een groep van zestig patiënten drie maanden na een infectie met het SARS-CoV-20-virus.[50]

Experts vermoeden dat COVID-19 bij één op de drie patiënten voor langduriger neurologische effecten kan zorgen, aldus het goed aangeschreven vakblad STAT op basis van een rondgang.[51] Ook een overzicht van de wetenschappelijke literatuur levert aanwijzingen op voor schade aan het zenuwstelsel.[52] Wetenschappers maken zich bovendien zorgen over

---

[41] https://www.thelancet.com/journals/eclinm/article/PIIS2589-5370(20)30207-8/fulltext - geverifieerd op 16-08-2020
[42] https://www.medrxiv.org/content/10.1101/2020.05.19.20107409v1.full.pdf - geverifieerd op 15-08-2020
[43] https://www.sciencedirect.com/science/article/pii/S0889159120303573 - geverifieerd op 16-08-2020
[44] https://journals.sagepub.com/doi/10.1177/0194599820939538 - geverifieerd op 15-08-2020
[45] https://jkms.org/DOIx.php?id=10.3346/jkms.2020.35.e174 - geverifieerd op 16-08-2020
[46] https://onlinelibrary.wiley.com/doi/full/10.1002/mds.28172 - geverifieerd op 15-08-2020
[47] https://www.journalofinfection.com/article/S0163-4453(20)30435-7/fulltext - geverifieerd op 16-08-2020
[48] https://link.springer.com/article/10.1007/s00405-020-06102-8 - geverifieerd op 16-08-2020
[49] https://jamanetwork.com/journals/jamaneurology/fullarticle/2764549 - geverifieerd op 15-08-2020
[50] https://www.thelancet.com/journals/eclinm/article/PIIS2589-5370(20)30228-5/fulltext - geverifieerd op 16-08-2020
[51] https://www.statnews.com/2020/08/12/after-covid19-mental-neurological-effects-smolder/ - geverifieerd op 15-08-2020
[52] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7324652/ - geverifieerd op 16-08-2020

mogelijke neuropsychiatrische gevolgen, zoals angst, slapeloosheid, delier, depressie, psychose, manie en suïcidale ideatie.[53]

Ten tijde van de Spaanse griep werd ook een toename van neuropsychiatrische verschijnselen gezien, mogelijk het gevolg van ontstekingen in de hersenen. Weliswaar wordt COVID-19 veroorzaakt door een coronavirus en niet door een griepvirus, maar ook bij de SARS- (2013) en MERS-uitbraken (2012-2015) – allebei wél veroorzaakt door een coronavirus – werden neuropsychiatrische gevolgen vastgesteld bij patiënten.[54]
In een artikel in het wetenschappelijke tijdschrift Alzheimer's Research & Therapy betogen Duitse en Amerikaanse onderzoekers dat COVID-19 de kans op het ontwikkelen van de ziekte van Alzheimer vergroot.[55] Uiteraard is op dit moment nog niet te zeggen of deze vermoedens kloppen; dit zal onderzoek op de lange termijn moeten uitwijzen. Hetzelfde geldt voor een artikel in het vakblad Brain, Behavior, and Immunity, waarin onderzoekers het vermoeden uitspreken dat de zogeheten cytokinestorm (een overreactie van het immuunsysteem) waarmee ernstige presentaties van COVID-19 vaak gepaard gaan, op lange termijn kan leiden tot cognitieve schade, beroertes en infarcten.[56]

Hart

Ook het hart wordt aangevallen door het SARS-COV-2-virus. Net als bij long- en andere celtypen gebruikt het virus de ACE2-receptor in hartcellen, waaronder pericyten, om toegang te krijgen tot deze cellen en zich daarin te vermenigvuldigen.[57] [58] [59] Slaagt dit, dan sterft de cel.

Aangenomen wordt dat patiënten met hart- en vaatziekten een grotere kans hebben op overlijden door COVID-19. Medicatie gebruikt voor de behandeling van COVID-19 kan zorgen voor extra bijwerkingen in combinatie met veelgebruikte hartmedicatie.[60]

Er zijn echter ook aanwijzingen dat COVID-19 voor langduriger schade zorgt bij patiënten die een SARS-CoV-2-infectie overleven. Zo is er een casus van een 31-jarige man die drie weken na herstel van COVID-19 een hartspierontsteking (myocarditis) kreeg. De man had geen relevante medische voorgeschiedenis op dit gebied.[61] Dit kan natuurlijk toeval zijn, maar een studie in JAMA Cardiology toonde hartspierontsteking aan in 60 procent van reeds herstelde COVID-19-patiënten die een MRI-scan ondergingen. In totaal was bij 78 procent een effect van COVID-19 op het hart te zien.[62]

---

[53] https://www.thelancet.com/journals/lanpsy/article/PIIS2215-0366(20)30203-0/fulltext - geverifieerd op 16-08-2020
[54] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7152874/ - geverifieerd op 16-08-2020
[55] https://alzres.biomedcentral.com/articles/10.1186/s13195-020-00640-3 - geverifieerd op 16-08-2020
[56] https://www.sciencedirect.com/science/article/pii/S0889159120312095?via%3Dihub - geverifieerd op 15-08-2020
[57] https://academic.oup.com/cardiovascres/article/116/6/1097/5813131 - geverifieerd op 16-08-2020
[58] https://www.jcvaonline.com/article/S1053-0770(20)30497-3/fulltext - geverifieerd op 16-08-2020
[59] https://www.ahajournals.org/doi/10.1161/JAHA.120.016219 - geverifieerd op 15-08-2020
[60] https://www.sciencedirect.com/science/article/pii/S0735109720346374?via%3Dihub - geverifieerd op 16-08-2020
[61] https://academic.oup.com/ehjcimaging/advance-article/doi/10.1093/ehjci/jeaa166/5847971 - geverifieerd op 17-08-2020
[62] https://jamanetwork.com/journals/jamacardiology/fullarticle/2768916 - geverifieerd op 16-08-2020

In een ander onderzoek werd bij 39 overleden COVID-19-patiënten het hart onderzocht. Bij 24 van hen was het virus in de hartspier aanwezig (61,5 procent); bij 16 was deze hoeveelheid groot (41 procent).[63]

Maag en darmen

SARS-CoV-2 kan cellen in het maag- en darmkanaal infecteren, specifiek zogeheten enterocyten, die zich op de wand van de darmen bevinden.[64] [65] [66] COVID-19 gaat soms gepaard met diarree, braken, misselijkheid en abdominale klachten.[67]

Nieren

Het is onduidelijk of COVID-19 nierschade veroorzaakt. Onderzoeken hierover spreken elkaar tegen.[68] [69]

Reproductieve organen

Er zijn aanwijzingen dat infectie met SARS-CoV-2 een negatief effect heeft op zwangere vrouwen en hun kinderen. Het is onduidelijk of het virus een effect heeft op de vrouwelijke of mannelijke vruchtbaarheid.[70]

Kanker

Als gevolg van de corona-uitbraak in Nederland in februari 2020 werd de zorgcapaciteit beperkt en voelden mensen zich minder gemotiveerd om medische hulp te zoeken. Er werden tussen 24 februari en 12 april 2020 aanzienlijk minder kankerdiagnoses gesteld. Dit effect was het sterkst bij huidkanker.[71] Het is waarschijnlijk dat hierdoor sommige patiënten later gediagnosticeerd zullen worden, wat nog gedurende langere tijd voor gezondheidsconsequenties zal leiden, zoals een slechter behandelresultaat. Bij een nieuwe uitbraak laat het zich aanzien dat opnieuw veel mensen de gang naar de dokter niet zullen durven of kunnen wagen.

Medicijnschade

Tijdens de eerste golf zijn veel patiënten behandeld met experimentele methodes, waaronder het malariamiddel hydroxychloroquine, maar ook antivirale middelen die niet voor COVID-19 zijn ontwikkeld. Het is mogelijk, maar niet duidelijk, dat het gebruik van deze middelen meer schade heeft aangericht dan goed heeft gedaan.[72]

---

[63] https://jamanetwork.com/journals/jamacardiology/fullarticle/2768914 - geverifieerd op 16-08-2020
[64] https://science.sciencemag.org/content/369/6499/50 - geverifieerd op 16-08-2020
[65] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7417263/ - geverifieerd op 17-08-2020
[66] https://www.cebm.net/study/covid-19-tmprss2-and-tmprss4-promote-sars-cov-2-infection-of-human-small-intestinal-enterocytes/ - geverifieerd op 16-08-2020
[67] https://www.gastrojournal.org/article/S0016-5085(20)30281-X/pdf - geverifieerd op 15-08-2020
[68] https://www.jocmr.org/index.php/JOCMR/article/view/4200 - geverifieerd op 17-08-2020
[69] https://www.karger.com/Article/FullText/507471 - geverifieerd op 16-08-2020
[70] https://www.fertstert.org/article/S0015-0282(20)30385-X/fulltext
[71] https://doi.org/10.1016/S1470-2045(20)30265-5 - geverifieerd op 16-08-2020
[72] https://www.sciencedirect.com/science/article/pii/S0924857920301618?via%3Dihub - geverifieerd op 17-08-2020

Ervaringen met andere coronavirussen (SARS-CoV-1, MERS)

Er zijn ook indirecte aanwijzingen voor de langetermijnschadelijkheid van SARS-CoV-2. De 'voorganger' SARS-CoV-1, die in 2003 voor meerdere uitbraken zorgde, heeft eveneens langetermijneffecten. Zo was bij 25 patiënten het lipidenmetabolisme (de vetstofwisseling) tot 12 jaar na de ziekte verstoord.[73] Het SARS-CoV-1-virus lijkt genetisch veel op het SARS-CoV-2-virus.[74] [75]

Ook het MERS-virus is een coronavirus, dat net als SARS-CoV-1 en SARS-CoV-2 voor een ARDS (acute respiratory distress syndrome, of acuut respiratoir stress-syndroom) kan zorgen. Zo'n 30 procent van de overlevenden van een SARS-CoV-1- of MERS-infectie kreeg te maken met permanente lichamelijke problemen. Op longfoto's was veelal schade te zien die leek op longfibrose.[76] [77]

Bij een onderzoek onder Hongkongse gezondheidswerkers die een ARDS overleefden, bleek dat zo'n 30 procent van hen na twee jaar nog niet terug aan het werk was gegaan.[78] Een literatuuronderzoek laat zien dat nogal wat SARS- en MERS-overlevenden zes maanden na ontslag uit het ziekenhuis nog te kampen hadden met een posttraumatische stress-stoornis (39 procent), depressie (33 procent) en angst (30 procent). Ook waren ze tot zes maanden na ontslag minder goed in staat een fysieke inspanningstest snel af te leggen.[79]

Hoewel een SARS-CoV-1-infectie bij kinderen minder ernstig verloopt dan bij volwassenen, werden ook bij kinderen zes maanden na herstel nog afwijkingen gevonden op röntgenfoto's, en was hun uithoudingsvermogen minder goed.[80]

Zuid-Koreaanse overlevenden van MERS meldden 12 maanden na de uitbraak in dit land last te hebben van depressie (27,0 procent) en posttraumatische stress-stoornis (42,9 procent). Mensen die een familielid hadden verloren aan MERS, hadden een hogere kans op depressie.[81]

Economische effecten van de COVID-19-pandemie

Naast de medische gevolgen zijn er ernstige economische effecten merkbaar. Maatregelen die helpen bij het beter beheersen van de uitbraak oefenen een invloed uit op deze economische gevolgen. Omdat de eerste effecten nu al merkbaar zijn, is het voor een belangenafweging dit mee te wegen naast de puur medische kant van deze pandemie.

---

[73] https://www.nature.com/articles/s41598-017-09536-z - geverifieerd op 16-08-2020

[74] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7180649/ - geverifieerd op 16-08-2020

[75] https://www.nature.com/articles/s41591-020-0820-9 - geverifieerd op 16-08-2020

[76] https://www.england.nhs.uk/coronavirus/wp-content/uploads/sites/52/2020/06/C0705-aftercare-needs-of-inpatients-recovering-from-covid-19-aug-2020.pdf - geverifieerd op 16-08-2020

[77] https://www.bmj.com/content/370/bmj.m3001 - geverifieerd op 16-08-2020

[78] https://pubmed.ncbi.nlm.nih.gov/20337995/ - geverifieerd op 15-08-2020

[79] https://pubmed.ncbi.nlm.nih.gov/32449782/ - geverifieerd op 16-08-2020

[80] https://www.sciencedirect.com/science/article/abs/pii/S1526054204000818?via%3Dihub - geverifieerd op 17-08-2020

[81] https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-020-08726-1 - geverifieerd op 16-08-2020

Consumenten

Volgens het Centraal Bureau voor de Statistiek kromp de Nederlandse economie in het tweede kwartaal van 2020 met 8,5 procent.[82] Het aantal werklozen was in juli 2020 419.000, wat overeenkomt met 4,5 procent van de beroepsbevolking.[83] De consumptie van huishoudens was in juni 2020 7 procent lager dan in juli 2019. Vooral de uitgaven in diensten waren lager; 13,9 procent onder het niveau van het jaar daarvoor. Aan duurzame goederen werd juist 3,1 procent meer besteed.[84] Het consumentenvertrouwen is in augustus 2020 verslechterd (-31) ten opzichte van juli (-26) en juni (-27), en komt daarmee terug op hetzelfde niveau als mei (-31).[85]

Bedrijven

Het volume van de goederenexport was in juni 2020 2,9 procent lager dan het jaar daarvoor, maar die daling was jaar-op-jaar aanmerkelijk lager dan in april (12,6 procent) of mei (11,4 procent).

Het producentenvertrouwen daalde volgens het CBS in april tot -28,7, maar krabbelt sindsdien weer op, tot -5,4 in augustus.[86] Afzetprijzen van de Nederlandse industrie waren in juli 2020 gemiddeld 4,9 procent lager dan een jaar daarvoor.[87] De omzet van de motor- en autobranche was in het tweede kwartaal van 2020 ruim 25 procent lager dan het jaar daarvoor.[88] Het consumentenvertrouwen is verder verslechterd, en lag in augustus 2020 op -29, waar dat in juli nog -26 was.[89] De omzet van de bouw daalde in het tweede kwartaal van 2020 voor het eerst in meer dan vijf jaar, en wel met 1,6 procent.[90] In de luchtvaart was de daling 13,8 procent in het eerste kwartaal van dit jaar vergeleken met dezelfde periode vorig jaar.[91] Hotels en andere logiesaccommodaties zagen een daling van gemiddeld 17 procent in datzelfde kwartaal (hotels afzonderlijk -19 procent).[92]

31 procent van de bedrijven met tussen de 10 en 250 werknemers heeft tot en met 12 juni uitstel van betaling aangevraagd bij de Belastingdienst. Veel van deze bedrijven maken ook

---

[82] https://www.cbs.nl/en-gb/news/2020/33/economic-contraction-of-8-5-percent-in-q2-2020 Geverifieerd op 28 augustus 2020.
[83] https://www.cbs.nl/en-gb/news/2020/34/unemployment-still-rising-in-july Geverifieerd op 28 augustus 2020.
[84] https://www.cbs.nl/nl-nl/nieuws/2020/33/consumptie-huishoudens-krimpt-met-7-procent-in-juni Geverifieerd op 28 augustus 2020.
[85] https://www.cbs.nl/nl-nl/nieuws/2020/34/consument-pessimistischer-in-augustus Geverifieerd op 28 augustus 2020.
[86] https://www.cbs.nl/nl-nl/nieuws/2020/35/producentenvertrouwen-neemt-opnieuw-toe-in-augustus Geverifieerd op 28 augustus 2020.
[87] https://www.cbs.nl/nl-nl/nieuws/2020/35/afzetprijzen-industrie-bijna-5-procent-lager-in-juli Geverifieerd op 28 augustus 2020.
[88] https://www.cbs.nl/nl-nl/nieuws/2020/35/auto-en-motorbranche-zet-ruim-25-procent-minder-om-in-tweede-kwartaal Geverifieerd op 28 augustus 2020.
[89] https://www.cbs.nl/nl-nl/nieuws/2020/34/consument-pessimistischer-in-augustus Geverifieerd op 28 augustus 2020.
[90] https://www.cbs.nl/nl-nl/nieuws/2020/34/bouw-zet-voor-het-eerst-in-jaren-minder-om Geverifieerd op 28 augustus 2020.
[91] https://www.cbs.nl/nl-nl/nieuws/2020/24/omzet-luchtvaart-bijna-14-procent-lager-in-eerste-kwartaal Geverifieerd op 28 augustus 2020.
[92] https://www.cbs.nl/nl-nl/nieuws/2020/23/aantal-gasten-logiesaccommodaties-17-procent-afgenomen-in-eerste-kwartaal Geverifieerd op 28 augustus 2020.

gebruik van andere steunmaatregelen.[93] De helft van alle gesteunde bedrijven gebruikte meer dan één noodmaatregel.[94] Vooral horecabedrijven doen een beroep op een tegemoetkoming voor schade door COVID-19 volgens de TOGS-regeling.[95] Vooral in de horeca, sport, cultuur en recreatie maken bedrijven zich zorgen over hun voortbestaan.[96]

Voor zzp'ers is de situatie ook precair. Eén op de vijf zelfstandigen gaf in 2019 aan een buffer van maximaal drie maanden te hebben.[97]

Met de detailhandel gaat het wel goed. Daar steeg de omzet in juni met 9, 8 procent vergeleken met een jaar eerder. Bij non-foodwinkels was die stijging 8,5 procent, bij winkels in voedings- en genotmiddelen 6,5 procent, en de online omzet was 45,1 procent hoger dan een jaar eerder.[98] In de groothandel was de stijging 2,2 procent in het eerste kwartaal van 2020 vergeleken met dezelfde periode dat jaar daarvoor.[99] Bouwmarkten en supermarkten doen het uitstekend.[100]

Overheid
De schuld van de Rijksoverheid steeg in de eerste helft van het jaar met 48 miljard euro naar 385 miljard euro, de grootste stijging sinds de kredietcrisis van 2008.[101] Gerekend vanaf februari tot juni was de stijging zelfs 61 miljard euro.

Herstel
Het Centraal Planbureau (CPB) verwacht dat de economie eind volgend jaar weer op hetzelfde niveau kan zijn als voor de crisis. Dat lijkt goed nieuws, maar betekent dat de economie twee jaar groei is misgelopen.[102] Aangezien verloren tijd per definitie niet kan worden ingehaald, is dit permanente schade. Het CPB brengt in zijn rapport in herinnering dat er na vier op de vijf diepe recessies sinds 1900 geen herstel is geweest, waaronder het CPB de situatie verstaat waarin het bruto binnenlands product zich niet herstelt tot de trend die voor de recessie stond. Het CPB verwacht ook dat de coronacrisis de komende vijf jaar tot schade

---

[93] https://www.cbs.nl/nl-nl/nieuws/2020/27/31-procent-bedrijven-met-10-250-werkzame-personen-kreeg-uitstel-belasting Geverifieerd op 28 augustus 2020.
[94] https://www.cbs.nl/nl-nl/nieuws/2020/34/helft-gesteunde-mkb-bedrijven-gebruikt-meer-dan-een-noodregeling Geverifieerd op 28 augustus 2020.
[95] https://www.cbs.nl/nl-nl/nieuws/2020/22/vooral-horeca-doet-beroep-op-tegemoetkoming-schade-covid-19 Geverifieerd op 28 augustus 2020.
[96] https://www.cbs.nl/nl-nl/nieuws/2020/28/in-meeste-sectoren-minder-zorgen-over-voortbestaan Geverifieerd op 28 augustus 2020.
[97] https://www.cbs.nl/nl-nl/nieuws/2020/16/1-op-de-5-zelfstandigen-schatte-buffer-in-2019-op-hooguit-3-maanden Geverifieerd op 28 augustus 2020.
[98] https://www.cbs.nl/nl-nl/nieuws/2020/31/omzet-detailhandel-bijna-10-procent-hoger-in-juni Geverifieerd op 28 augustus 2020.
[99] https://www.cbs.nl/nl-nl/nieuws/2020/24/omzet-groothandel-ruim-2-procent-hoger-in-eerste-kwartaal-2020 Geverifieerd op 28 augustus 2020.
[100] https://www.cbs.nl/nl-nl/nieuws/2020/14/omzet-bouwmarkten-piekt-omzet-supermarkten-nog-steeds-hoog Geverifieerd op 28 augustus 2020.
[101] https://www.cbs.nl/nl-nl/nieuws/2020/31/schuld-rijksoverheid-steeg-in-de-eerste-helft-van-2020-met-48-miljard-euro Geverifieerd op 28 augustus 2020.
[102] https://www.cpb.nl/sites/default/files/omnidownload/CPB-Coronapublicatie-Blijvende-economische-schade-van-de-coronacrisis.pdf Geverifieerd op 28 augustus 2020.

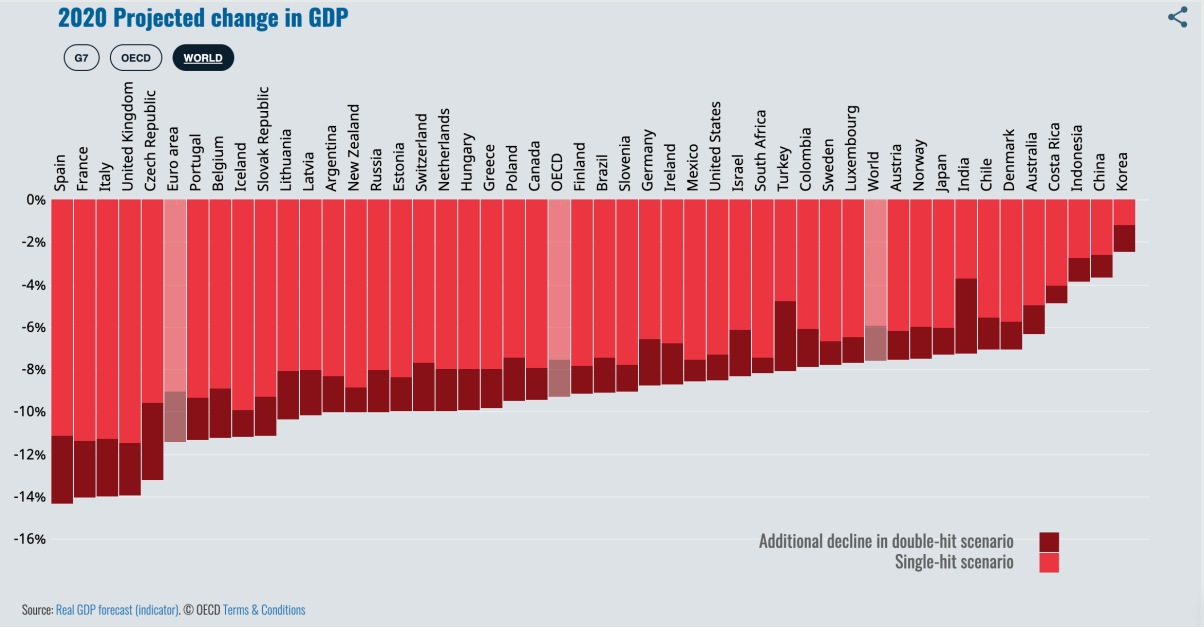
op de arbeidsmarkt kan leiden.[103] Het gaat dan ondermeer om zogeheten scarring-effecten; loonverlies dat optreedt door periodes van werkloosheid.

Verwachte wereldwijde effecten
De Wereldbank verwacht over heel 2020 een krimp van 7 procent in ontwikkelde economieën, en 5,2 procent wereldwijd. Als deze voorspelling uitkomt, wordt deze recessie de zwaarste in decennia.[104]

Volgens de Verenigde Naties zal de wereldwijde economische output de komende twee jaar met 8,5 biljoen (duizend miljard) krimpen.[105] Het wereldhandelsmomentum was in juni 2020 met 12,5 procent gedaald, aldus het Centraal Planbureau (CPB).[106]

De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) onderscheidt twee scenario's. In het scenario waarin een tweede golf wordt voorkomen, daalt de wereldwijde economische activiteit in 2020 met 6 procent en stijgt de werkloosheid in OESO-landen van 5,4 procent in 2019 tot 9,2 procent. In 2021 zal er sprake zijn van vijf jaar inkomensgroeiverlies. Dit is het optimistische scenario.

In het tweede, negatieve, scenario, waarin wel een tweede golf plaatsvindt, komen er nieuwe lockdowns en daalt de wereldwijde economische output met 7,6 procent in 2020 en zal deze in 2021 met 2,8 procent stijgen. De werkloosheid in de 37 OESO-landen zal in dit scenario verdubbelen tot 10 procent en in 2021 nauwelijks herstellen.[107]



Bron: https://www.oecd.org/economic-outlook/june-2020/

[103] https://www.cpb.nl/sites/default/files/omnidownload/CPB-Coronapublicatie-Langdurige-effecten-van-de-coronacrisis-voor-de-arbeidsmarkt.pdf Geverifieerd op 28 augustus 2020.
[104] https://www.worldbank.org/en/publication/global-economic-prospects Geverifieerd op 28 augustus 2020.
[105] https://www.un.org/development/desa/en/news/policy/wesp-mid-2020-report.html Geverifieerd op 28 augustus 2020.
[106] https://www.cpb.nl/sites/default/files/omnidownload/CPB-World-Trade-Monitor-June-2020.pdf Geverifieerd op 28 augustus 2020.
[107] https://www.oecd.org/economic-outlook/june-2020/ Geverifieerd op 28 augustus 2020.

Over CoronaMelder

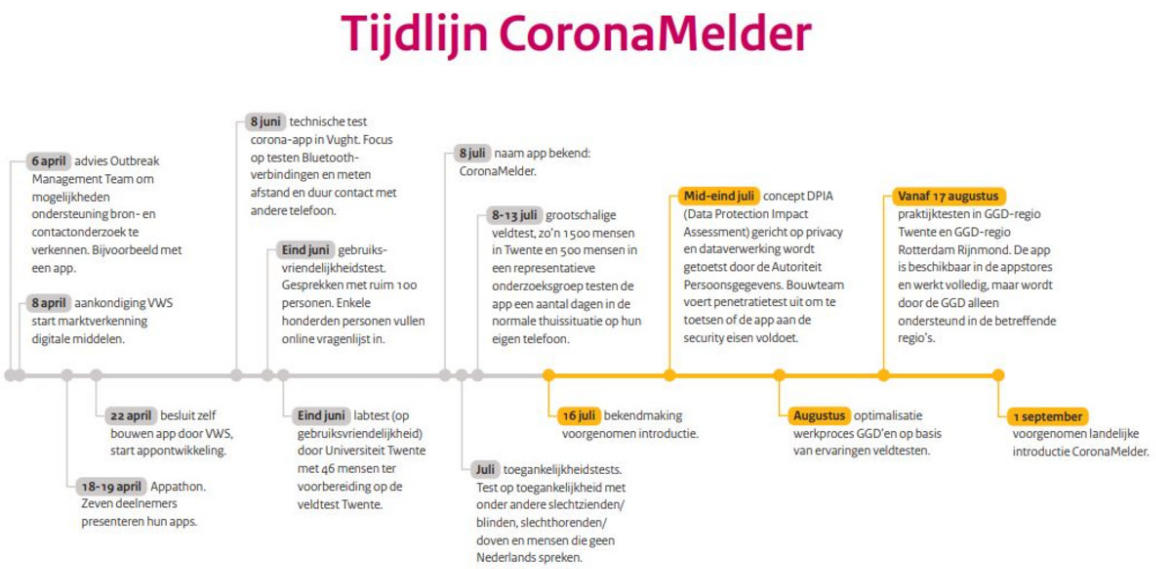
Wat eraan voorafging

Wat het verdere verloop van COVID-19 ook zal zijn, een digitale vorm van bron- en contactonderzoek onder de bevolking kan het zicht op en vroegtijdig waarschuwen van potentiële zieken aanmerkelijk versnellen. Zeker in het licht van de capaciteitsuitdaging bij de GGD-en, die veel van hun resources moeten inzetten voor het analoge bron- en contactonderzoek, is de bijdrage van digitale ondersteuning meer dan welkom.

Het Outbreak Management Team (OMT) heeft dan ook geadviseerd om de mogelijkheden voor ondersteuning van bron- en contactopsporing met behulp van mobiele applicaties te onderzoeken.[108] Ook de Tweede Kamer heeft in de breed aangenomen motie Jetten c.s. overwogen dat het gebruik van apps kan bijdragen aan het beheersen van het virus.[109]

Aanvankelijk werden nationale en internationale in de markt beschikbare apps verzameld. Via een openbare beproeving (Appathon op 18 en 19 april 2020) werden deze apps getoetst. De oplossingen voldeden in het geheel niet aan de eisen op het gebied van privacy, informatieveiligheid, nationale veiligheid, bruikbaarheid en toegankelijkheid. Vervolgens stelde minister Hugo de Jonge een team samen van experts dat in zijn opdracht een app heeft gebouwd.

Onderstaand schema toont de beoogde planning omtrent CoronaMelder.



[108] Bijlage 929506 bij Kamerstukken II 2019/20, 25 295, nr. 219.
[109] Kamerstukken II 2019/20, 25 295, nr. 223.

Doel en scope van CoronaMelder

Het doel van CoronaMelder is om – aanvullend op het bestaande, analoge bron- en contactonderzoek van de GGD-en – bij een geconstateerde COVID-19 infectie andere gebruikers van de app die in de nabijheid van de geïnfecteerde zijn geweest te informeren over hun verhoogde kans op besmetting. Deze mensen krijgen dan het advies om contact op te nemen met de GGD in hun regio.

Het systeem is zo ingericht dat op ieder moment het herleiden naar gebruikers extreem moeilijk of zelfs onmogelijk is. Het gebruik van de app is vrijwillig en mag niet worden verplicht. Er is wetgeving gemaakt om dwang voor gebruik strafbaar te stellen. De inzet van de app is tijdelijk en er is voorzien dat deze ook weer stopt, wanneer de corona-pandemie is ingedamd.

Wetenschappelijke studies naar effectiviteit

In deze fase van het bestrijden van de pandemie is meer onderzoek nodig om te bepalen hoef effectief notificatieapps zijn. Deze zullen zonder twijfel volgen, zodra de app in gebruik is genomen. Tot die tijd kunnen wij twee studies vermelden.

Oxford

Het onderzoek “Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown”[110] heeft simulaties gedaan. Deze bevestigen dat wanneer de helft van een populatie een adequate notificatieapp gebruikt, in samenwerking met de analoge interventies, dit in potentie de epidemie kan stoppen. Hierdoor hoeven landen niet langer drastische maatregelen te treffen zoals een lockdown. Deze onderzoeksresultaten worden bevestigd door diverse Europese projecten, waaronder het nationale programma van Groot Brittannië, geleid door NHSX.[111]

Analyse van de transmissiedynamiek van de vroege coronavirus-epidemie in China toont aan dat bijna de helft van alle transmissies plaatsvond voordat iemand symptomen vertoonde. Naar schatting maakt het uitstellen van contactopsporing met zelfs een dag vanaf het begin van de symptomen het verschil tussen epidemische controle en heropleving van het coronavirus.

Isle of Wight

In mei 2020 voerde Groot Brittannië een zogeheten ‘Test, Trace, Isolate’ onderzoek uit. De resultaten zijn weergegeven in het rapport ‘COVID-19 incidence and R decreased on the Isle of Wight after the launch of the Test, Trace, Isolate programme’.[112] Zoals de titel aangeeft, werd versie 1 van de NHS-app als aanvulling op het bron- en contactonderzoek voor het eerst uitgerold op het Isle of Wight. Onmiddellijk na de lancering van de app werden significante dalingen in R (het reproductiegetal) waargenomen. Volgens de onderzoekers werd de sub-epidemie op het Isle of Wight aanmerkelijk effectiever bestreden dan de sub-epidemieën van de meeste andere Upper Tier Local Authorities. Het is te vroeg om direct een oorzakelijk verband vast te stellen tussen de app en het afgenomen R. De bevindingen benadrukken de noodzaak tot verder onderzoek.

---

[110] https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

[111] Dit is een samengestelde unit bestaande uit teams van NHS England en de Department of Health & Social Care.

[112] https://www.medrxiv.org/content/10.1101/2020.07.12.20151753v1

Open source

De bouw van de app vindt plaats op transparante wijze in open source. Dat betekent dat tussentijdse versies van de app door het bouwteam doorlopend zijn gepubliceerd op GitHub. Op dit online softwareplatform worden anderen uitgenodigd om mee te kijken en mee te doen. Door deze open manier van werken, is door enthousiaste vrijwilligers in zogenaamde 'communities' al tijdens de bouw meegedacht en meegewerkt in het steeds verder verbeteren van tussentijdse versies van de app. Tevens is er uitgebreid getest op de aansluiting van de app bij de wensen van de GGD en de andere eisen.

Vanaf half juni zijn er ook tests in laboratoriumsetting en vervolgens in de praktijk (onder andere in de regio Twente) uitgevoerd. Ook is er met verschillende doelgroepen getest, zodat de app goed kan worden gebruikt door jongeren en ouderen van verschillende opleidingsniveaus en door mensen met een verstandelijke beperking. In augustus waren er onder meer stresstesten en een penetratietest.

Vijf fasen

Om het doel van Coronamelder te verwezenlijken gebruikt de app een implementatie van het DP-3T systeem.[113] Dit protocol werkt op smartphones met de besturingssystemen iOS (Apple) en Android (Google).

Termen om te onthouden

- BLE - Bluetooth Low Energy, het energiezuinige Bluetooth verbindingsprotocol.
- DP-3T-systeem – Het Decentralized Privacy-Preserving Proximity Tracing systeem is een veilig, gedecentraliseerd nabijheids-opsporingssysteem met behoud van de privacy. Ontwikkeld door een internationaal consortium van technologen, juridische experts, ingenieurs en epidemiologen.
- DKs - Diagnosis Keys. Hierin wordt de datum van de eerste ziektedag vergeleken met de datum van de TEKs. Op basis daarvan wordt het risico van overdracht (TransmissionRiskValue) bepaald (high, mid, low).
- Exposure Notification API – Een speciaal voor het traceren van digitale contacten ontwikkelde Application Programming Interface. Raamwerk en specificatie zijn gezamenlijk door Apple en Google ontwikkeld, op basis van het DP-3T-systeem.
- RPI - Rolling Proximity Indicator. Pseudonieme identificatiesleutel.
- TEK - Temporary Exposure Key. Pseudonieme identificatiesleutel. In de relevante Google en Apple documentatie worden TEKs aangeduid als Diagnosis Key op het moment dat iemand als geïnfecteerd is aangemerkt.

Het gebruik van Coronamelder doorloopt qua chronologie de volgende vijf fasen:

1. Installatie

[113] Ontwikkeld door een internationaal consortium van technologen, juridische experts, ingenieurs en epidemiologen. De afkorting DP-3T staat voor: Decentralized Privacy-Preserving Proximity Tracing. Het wordt omschreven als "een veilig, gedecentraliseerd nabijheids-opsporingssysteem met behoud van de privacy. Het doel is om het proces van identificatie van mensen die in contact zijn geweest met een geïnfecteerde persoon te vereenvoudigen en te versnellen, en zo een technologische basis te bieden om de verspreiding van het SARS-CoV-2-virus te vertragen. Het systeem heeft tot doel privacy- en beveiligingsrisico's voor individuen en gemeenschappen te minimaliseren en het hoogste niveau van gegevensbescherming te garanderen. Documentatie over DP-3T is openbaar en te vinden in het DP-3T Repository op https://github.com/DP-3T/documents.

2. Uitwisseling
3. Validatie
4. Koppeling
5. Notificatie

1. Installatiefase

De gebruiker downloadt en installeert CoronaMelder van de Play Store van Google (voor smartphones met Android als besturingssysteem) of de App Store (voor Apple smartphones met iOS als besturingssysteem).

2. Uitwisselingsfase

Twee pseudonieme identificatiesleutels[114] spelen de hoofdrol tijdens de uitwisseling tussen smartphones waarop de app actief is.

1. De app maakt voor elke telefoon een eigen code

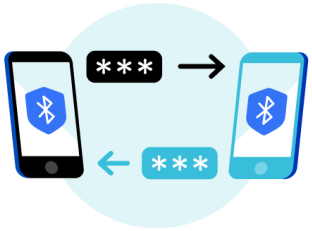
In deze code staat geen informatie over jou of je telefoon. De code is helemaal anoniem en verandert elk kwartier.

De eerste sleutel betreft de zogeheten Temporary Exposure Keys (TEKs). Deze tijdelijke sleutels blijven maximaal 24 uur geldig, waarna automatisch nieuwe TEKs worden gegenereerd.

De Rolling Proximity Indicators (RPIs) – de tweede sleutel – worden samengesteld op basis van de TEKs. Je kunt de RPIs zien als een serie deelverzamelingen van een TEK. Tijdens deze fase kunnen de RPIs niet wordt herleid naar de TEKs. Pas wanneer de sleutel op de telefoon komt als Diagnosis Key (DK), tijdens de validatiefase, wordt er een relatie gelegd met de RPIs.

De RPIs hebben een geldigheidsduur van tien tot twintig minuten. Daarna worden nieuwe RPIs gegenereerd.

[114] Zie voor een technische uiteenzetting: Exposure Notification. Cryptography Specification, v1.2 April 2020, te vinden via www.apple.com/covid19/contacttracing.



2. Telefoons delen hun codes als ze bij elkaar in de buurt zijn

Heeft de persoon die je tegenkomt ook de app? Dan delen jullie telefoons hun codes met elkaar via Bluetooth Low Energy. Zo weet de app welke telefoons in de buurt waren. De app weet niet van wie de telefoons zijn en ook niet waar jullie waren.

Tijdens de uitwisselingsfase wordt informatie meegestuurd die van belang is voor een eventuele toekomstige inschatting van een infectierisico.[115] Nabijheidsdetectie vindt plaats via Bluetooth Low Energy (BLE), een variant van het Bluetooth protocol. Deze detectie is erop gebaseerd dat het ontvangen BLE-signaal van een andere smartphone vergeleken wordt met de door diezelfde smartphone uitgezonden berichten die naast de RPIs ook de uitgezonden signaalsterkte bevatten. Het verschil tussen de sterkte van het uitgezonden en het ontvangen BLE-signaal wordt gebruikt als indicator voor de fysieke nabijheid. Gecombineerd met de duur van het contact kan hiermee achteraf een inschatting gegeven worden van het eventuele besmettingsrisico van COVID-19.

De ontvangen RPIs en eigen TEKs worden veertien dagen bewaard op de smartphone van gebruikers. Deze termijn hangt samen met de incubatietijd van het virus. Wie besmet raakt krijgt doorgaans na vijf tot zes dagen klachten. Soms gebeurt dat al na twee dagen, maar het komt ook voor dat dit zelfs na twaalf dagen gebeurt. In ieder geval weten we na veertien dagen zeker of er wel of geen besmetting heeft plaatsgevonden.

De gebruiker kan desgewenst de bewaartermijn verkorten, want hij/zij heeft te allen tijde de mogelijkheid om alle gegevens te verwijderen of de hele app te verwijderen waardoor ook alle opgeslagen gegevens op de telefoon worden verwijderd.

[115] Deze gegevens vallen geen van alle onder ‘persoonsgegevens’ zoals omschreven in de AVG.

3. Validatiefase

Zolang er geen sprake is van infecties blijft al het voorgaande technische verkeer – de uitwisseling van pseudonieme sleutels – ongebruikt. Pas wanneer iemand is geïnfecteerd en door de GGD positief is getest, kan deze persoon op vrijwillige basis de eigen TEKs sturen naar een speciaal daarvoor ingerichte backend server.[116]

De gebruiker maakt via de app zijn voornemen kenbaar dat hij zijn TEKs wil uploaden. Door dit signaal genereert de server een code die naar de gebruiker wordt verstuurd. Om deze code te valideren – zodat zeker is dat het om een bevestigde besmetting gaat – verzoekt de GGD de gebruiker deze code van zes posities voor te lezen. Deze code kan worden gevonden in een bepaald scherm van de app. Voor deze werkwijze is gekozen omdat verwacht kan worden dat mensen nerveus zijn en dan liever iets voorlezen in plaats van een code in te moeten tikken. Dit reduceert het foutrisico.

Nadat de code door de GGD is ingevoerd in het GGD-portaal, wordt deze op de server geverifieerd. Hierna kan de gebruiker daadwerkelijk actief uploaden naar de backend server. Deze upload omvat de TEKs en de gegenereerde code. Om loos alarm te voorkomen, accepteert de backend server alleen TEKs van mensen als daar een door de GGD gevalideerde autorisatiecode bij zit. Aan deze informatie voegt de GGD de datum van de eerste ziektedag[117] toe en plaatst het geheel in het GGD-portaal van de app.[118]

Vervolgens worden op de backend server de TEKs geconverteerd naar Diagnosis Keys (DKs). De TEKs met een gevalideerde code heten vanaf nu DKs. De DKs worden om een bepaalde tijd vrijgegeven voor

[116] Deze zou aanvankelijk door de Belastingdienst worden beheerd, maar deze taak is in tweede instantie overgegaan naar het CIBG, een uitvoeringsorganisatie van VWS.
[117] Uit wetenschappelijk onderzoek blijkt dat een persoon met COVID-19 de eerste paar dagen van de besmetting het meest besmettelijk is. Het verwerken van de eerste ziektedag is van belang, omdat dit een indicatie geeft van welke periode de gebruiker het meest besmettelijk was. Door deze toevoeging kunnen vals positieven worden vermeden.
[118] Het GGD-portaal is alleen toegankelijk voor GGD-medewerkers die beschikken over een GGD Identity Hub account. Dit account werkt met de veilige 2-factor authenticatie. Het portaal is er uitsluitend voor bedoeld om de autorisatiecode en de eerste ziektedag naar de backend server te kunnen uploaden. Deze twee gegevens worden niet in het GGD-portaal opgeslagen en er wordt ook geen koppeling gemaakt maken met het individu waarop die gegevens betrekking hebben. Van verdere verwerking van de gegevens die in het kader van de app door onder andere de GGD worden verwerkt, bijvoorbeeld door het college van B&W, is geen sprake. Er ontstaan derhalve geen met een verdere verwerking verband houdende additionele risico's.

download.[119] Dit gebeurt gesorteerd om herleidbaarheid te voorkomen. Hier voegt de GGD, bij het vrijgeven van de code, handmatig de datum van de eerste ziektedag aan toe.

Alleen de GGD-medewerker ziet uiteindelijk de naam van de besmette persoon. Dit gebeurt ook bij de analoge vorm van bron- en contactonderzoek. Deze medewerker ziet evenwel niet de pseudonieme sleutels, aangezien het CIBG (VWS) de server beheert. Deze scheiding van rollen is doelbewust doorgevoerd ter bescherming van de persoonsgegevens.

Op basis van de vergelijking van de TEK-datum en de eerste ziektedag wordt het risico van overdracht (TransmissionRiskValue) bepaald (high, mid, low). De backend server stelt de DKs vervolgens beschikbaar, zodat deze kunnen worden opgehaald door andere smartphones met een actieve app.

Wanneer de autorisatiecode niet door de GGD is geplaatst in het GGD-portaal, bijvoorbeeld vanwege verbindingsproblemen, wordt de code gedurende 24 uur op de backend server bewaard. Eenzelfde bewaartermijn wordt gehanteerd wanneer de GGD de autorisatiecode in de GGD-portaal heeft geplaatst, maar er geen corresponderende code door de gebruiker naar de backend server is gestuurd. De geüploade TEKs en DKs en de eerste ziektedag worden eveneens 24 uur op de backend server bewaard. Voor deze bewaartermijn van 24 uur is gekozen omdat het DP-3T protocol een nachtelijke nazending van TEKs van de laatste dag van de upload vereisen. Pas daarna kunnen dus alle relevante DKs voor download ter beschikking worden gesteld.

[119] Het voor downloaden beschikbaar maken van de DKs vindt plaats met standaard webtechnologie (content delivery network en storage), waarbij voor de flexibiliteit en de schaalbaarheid gebruik wordt gemaakt van het KPN platform.

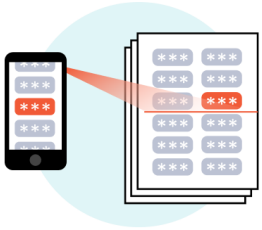
3. Als iemand corona heeft kan deze persoon zijn of haar codes op een lijst zetten

Deze lijst bevat alleen codes van besmette personen. Om de codes toe te voegen moet een besmet persoon eerst een GGD-sleutel doorgeven aan de GGD. Zo is altijd zeker dat de toegevoegde codes ook echt horen bij iemand die corona heeft. Alle codes ouder dan 14 dagen worden automatisch van de lijst verwijderd.

Tijdens de validatiefase worden voor beheers- en beveiligingsdoeleinden IP-adressen tijdelijk verwerkt. Dit is inherent aan het gebruik van internet en IP-technologie. Het IP-adres wordt na zeven dagen vernietigd.

Het gebeurt zodanig dat het onmogelijk is om te herleiden welke gebruiker welke gegevens heeft verstuurd. Zodra de data via internet aankomt bij het CIBG worden de TEKs/DKs doorgestuurd naar de server zonder dat daar een link met het IP-adres te maken is. De verkeersgegevens, waaronder IP-adressen, worden zonder de TEks/DKs geanalyseerd op mogelijk aanvallen. Als gevolg van de scheiding van verkeersgegevens en TEKs/DKs kunnen de onderscheiden gegevens niet aan elkaar worden gerelateerd, evenmin is op de server te achterhalen van welke gebruiker de TEKs/DKs afkomstig zijn.

4. Koppelingsfase



4. Elke telefoon controleert of het de codes op de lijst eerder is tegengekomen

De app kijkt een paar keer per dag naar de lijst met codes van besmette personen. Hij vergelijkt deze lijst met de codes die op jouw telefoon zijn bewaard. Zo ziet de app of je extra kans op besmetting hebt gelopen.

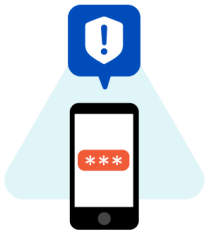
Nadat smartphones de beschikbaar gemaakte DKs hebben opgehaald, wordt de verbinding met de server verbroken. Het DP-3T protocol controleert op de smartphone zelf vervolgens of er voor elk van de bij deze DKs behorende RPIs een match is met de op de smartphone opgeslagen RPIs. Zoals gezegd, deze worden 14 dagen op de telefoon bewaard. Als er een match is, bepaalt de app op basis van bepaalde parameters en weegfactoren – signaalsterkte, contactduur en eerste ziektedag – of het contact risicovol is geweest. De parameters en weegfactoren worden vastgesteld door VWS, in overleg met RIVM, GGD-en en OMT, en kunnen op basis van nieuwe inzichten periodiek worden aangepast. Alleen wanneer een van de vastgestelde drempelwaardes wordt overschreden, geeft de app een signaal dat er sprake is geweest van risicovol contact.[120] De gebruiker ontvangt een notificatie met bijvoorbeeld een advies om scherper te letten op symptomen of om zich bij bepaalde symptomen te laten testen.

Direct nadat de opgehaalde DKs door de app zijn verwerkt voor het maken van de match en de weging, worden deze verwijderd van de telefoon. In de koppelingsfase controleert de app enkele keren per dag bij de backend server

[120] De Exposure Notification API berekent hier of er een melding moet volgen. Deze berekening vindt decentraal plaats. Zelfs de app weet niet welke RPI/TEK-combinatie het alarm geeft.

of er nieuwe DK's beschikbaar zijn. Is dat het geval dan herhaalt het bovenstaande proces zich.

5. Notificatiefase



5. Jij krijgt een melding als de codes van een besmet persoon op je telefoon staan

In deze melding lees je wanneer je in de buurt van de besmette persoon bent geweest. Niet wie het is en waar het was. Ook vertelt de app wat je nu zelf het beste kunt doen. Je eigen codes staan niet op de lijst met besmette codes, maar worden 14 dagen op je telefoon bewaard.

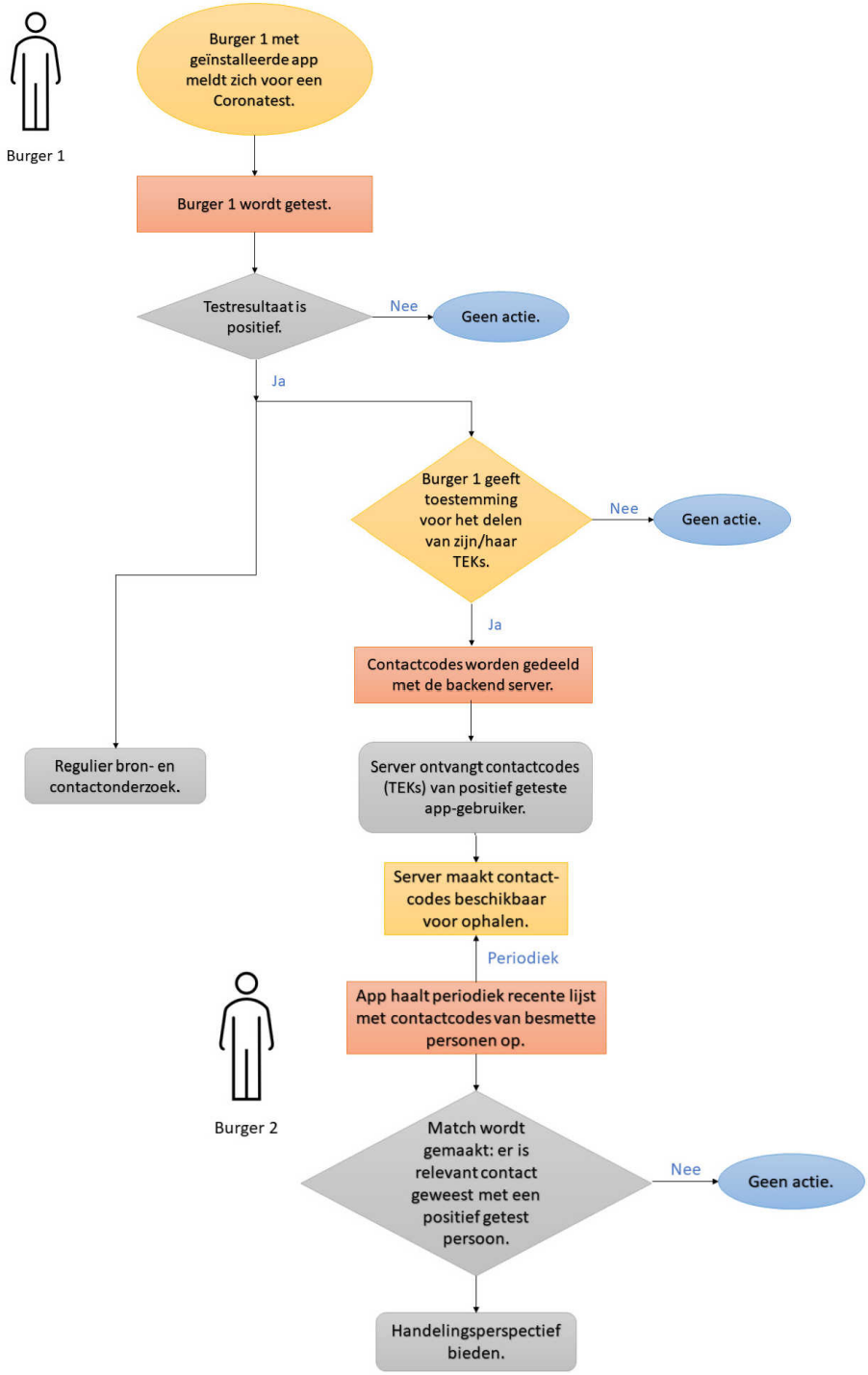
De app genereert een notificatie om de gebruiker te informeren over de verhoogde kans op een besmetting met COVID-19 en een advies om zich bij klachten te laten testen. De notificatie noemt ook de dag van de mogelijke besmetting. Als iemand zich heeft laten testen vóór de dag van de mogelijke besmetting, dan is het raadzaam dat deze persoon zich opnieuw laat testen. Helemaal wanneer er (opnieuw) klachten zijn. De GGD en het RIVM leveren input voor de tekst van de notificatie. Deze kan wijzigen afhankelijk van het overheidsbeleid dat toeziet op de te treffen maatregelen wanneer iemand besmet is. De notificatie blijft staan, totdat de gebruiker deze wegklikt. Na wegklikken blijven er van de notificatie geen sporen achter.

De vijf fasen in twee overzichten

In onderstaand overzicht staan de stappen in chronologische volgorde.

Installatiefase	Uitwisselingsfase	Validatiefase	Koppelingsfase	Notificatiefase
•Installeren van de app •Informatie over werking app •Geven van toestemming	•App werkt op de achtergrond •Wisselt codes uit met telefoons in de buurt	•Iemand is positief getest op Corona •GGD valideert met code de echtheid van de melding •Gebruiker geeft vrijwillig sleutels vrij	•Sleutels van zieke mensen worden gedownload •Er wordt gekeken naar match met contacten •Berekening of notificatie moet volgen	•Gebruiker krijgt een melding •Gebruiker krijg advies •Gebruiker klikt melding weg

Onderstaand stroomdiagram geeft de diverse stappen weer vanaf de validatiefase.



De software

De software waarmee de TEKs en RPIs worden gegenereerd is compatible met de Exposure Notification API (Application Programming Interface) die speciaal voor contact tracing is ontwikkeld door Apple en Google. Deze API is een voortzetting van het DP-3T-systeem. Binnen de API worden géén persoonsgegevens verwerkt. De Ierse DPC (en enkele andere Europese toezichthouders) beschikt over aanvullende van Apple en Google verkregen informatie over deze API. De Ierse toezichthouder op de Ierse DPIA op de COVID Tracker App heeft naar aanleiding van deze aanvullende informatie geen specifieke zorgen geïdentificeerd met betrekking tot de betrokkenheid van Apple of Google.[121]

Het consortium dat DP-3T heeft ontwikkeld, was kort na de release van de eerste versie van de Exposure Notification API van Apple en Google, van mening was dat er een beter design mogelijk was. Het nadeel van dit design was dat het veel bandbreedte zou gebruiken, wat belastend zou zijn geweest voor het netwerkverkeer. Om dit te voorkomen heeft DP-3T later een design versie 3 toegevoegd (het zogeheten 'hybrid design'). Hierover zegt DP-3T in hun white paper uit mei 2020:[122] "This design is very similar to the Google/Apple design." Inmiddels is DP-3T overgestapt op het GAEN protocol (Google Apple Exposure Notification (de Google-Apple API-software).

DP-3T heeft een set adviezen en best practices voorgesteld die richting geven aan hoe de app het beste kan worden gebouwd met gebruik van de API-software. Nederland onderschrijft die best practices en adviezen en heeft daar ook opvolging aan gegeven. Daarnaast werkt Nederland met andere landen actief samen in het Europese e-Health-netwerk. Een van de doelstellingen is het werken aan verdere verbetering van DP-3T. Dit doet Nederland samen met onder meer Duitsland, Ierland, Oostenrijk, Estland, Italië en Noorwegen. Google en Apple volgen deze ontwikkelingen nauwgezet. Wanneer de adviezen en best practices de API-software raken, overwegen Google en Apple om deze in die software op te nemen.[123] Inmiddels is er samenwerking tussen DP-3T, Google en Apple.

---

[121] "The DPIA refers to the choice of the data controllers to implement the Google/Apple Exposure Notification System (ENS) to facilitate processing of app data on-device. The DPC, in collaboration with EU data protection authorities, is engaged in ongoing dialogue with Google/Apple on the data protection implications of the ENS. At this time no matters giving rise to significant concern have been identified. However, it is incumbent upon the data controllers to implement the necessary organization and technical measures to ensure the technical specification of any APIs to ensure the security and confidentiality of personal data undergoing processing."
Vergelijk ook de Google COVID-19 Exposure Notications Service Additional Terms, waarin Google met zoveel woorden uitspreekt geen persoonsgegevens te willen ontvangen (artikel 3 aanhef en onder b sub vi):
"While end users of your App may provide personal data as part of their use of the App, you will not share this end-user personal data with Google. (...)"
[N.B.: Anders dan de Ierse COVID Tracker maakt de Nederlandse CoronaMelder géén gebruik van de optie van het verstrekken van persoonsgegevens als gevolg van het gebruik van de app.]
Het Exposure Notification APIs Addendum van Apple bevat een soortgelijk artikel (artikel 3.7):
"You will not share any user data with Apple that users of Your Contact Tracing App may provide in connection with their use of such App."

[122] https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

[123] Een voorbeeld ter illustratie: Nederland heeft ervoor gepleit om een TEK niet vast te houden tot middernacht en de hele dag geldig te laten zijn, maar deze te splitsen na upload. Vanaf versie 1.5 gaan Apple en Google deze lang gekoesterde wens honoreren. De aanpassing komt op het volgende neer: Tot aan GAEN-versie 1.4 zou bij iedere (handmatige) oproep om TEKs op dezelfde dag dezelfde set sleutels worden opgehaald. De onderliggende sleutels zouden daarbij dus niet wijzigen. Met GAEN 1.5 is onder meer veranderd dat wanneer een app de TEKs van het apparaat leest, er een nieuwe TEK voor het apparaat wordt gegenereerd. Deze nieuwe TEK is pas echt actief vanaf het moment van de reset, die nog steeds is ingesteld op middernacht. Toch betekent dit een verkorting van de interval, waardoor je niet uit een TEK kunt afleiden wat het echte moment was waarop het actief begon te worden.

Persoonsgegevens

Voorop staat dat de app ervoor is bedoeld om de GDD-en te ondersteunen in hun bron- en contactopsporingstaak. CoronaMelder is zodanig ontwikkeld dat het risico op identificatie van gebruikers via de app zo goed als uitgesloten is. Dit is inherent aan de gekozen decentrale opzet van de app. Op de smartphone van de gebruiker zelf worden geen persoonsgegevens verwerkt. Ook betrokken partijen zoals Apple en Google verwerken nergens in het hele proces persoonsgegevens.

Alleen de GGD verwerkt persoonsgegevens bij de vaststelling dat een gebruiker van de app besmet is. Dit doet de GGD al in het reguliere, analoge bron- en contactonderzoek. Tijdens het digitale onderzoek met behulp van de app stuurt de GGD tijdens de validatiefase, binnen 24 uur nadat is vastgesteld dat de gebruiker besmet is, de autorisatiecode van deze gebruiker met de eerste ziektedag via het GGD-portaal naar de backend server. Als zodanig is deze onder de verantwoordelijkheid van de GGD uitgevoerde gegevensverwerking dus onmisbaar om te kunnen komen tot notificaties aan andere gebruikers. Voor deze gegevensverwerkingen ligt de zeggenschap, en daarmee verwerkingsverantwoordelijkheid in de zin van art. 4, onderdeel 7, AVG, bij de GGD.

Bij de digitale verwerking van persoonsgegevens bij de GGD is voor niemand tijdens dat proces duidelijk welke geüploade TEKs/DKs bij welke (besmet gebleken) gebruiker horen. Ook op de backend server kan deze match niet worden gemaakt.
Identificatie van gebruikers via de app is dus zo goed als uitgesloten. Desondanks geven we per chronologische fase aan of er sprake is van persoonsgegevens, en zo ja of deze als gewoon, bijzonder, strafrechtelijk en wettelijk identificerend kunnen worden aangemerkt.

Installatiefase
Er worden geen persoonsgegevens verwerkt.

Uitwisselingsfase
Gewone persoonsgegevens:
- TEKs
- RPIs
- Signaalsterkte en de contactduur[124]

In deze fase worden uitsluitend RPIs uitgewisseld tussen gebruikers van de app. Wanneer zij in elkaars nabijheid zijn, worden de bij de RPIs behorende signaalsterkte (zowel uitgezonden als ontvangen), de duur van het bluetoothcontact en de eigen TEKs opgeslagen op de eigen smartphone. Deze uitwisseling gebeurt zonder tussenkomst van een server en worden nergens anders opgeslagen.
Gedurende de uitwisselingsfase zijn de uitgewisselde gegevens in beginsel aan te merken als ‘gewone’ persoonsgegevens. Het karakter van de TEKs en de daarvan afgeleide RPIs verandert naar ‘bijzondere’ persoonsgegevens wanneer sprake is van een positieve testuitslag. De betreffende gebruiker deelt dan zijn TEKs met de GGD.

Validatiefase
Bijzondere persoonsgegevens

[124] De signaalsterkte en de contactduur vormen op zichzelf geen persoonsgegeven, maar kunnen in combinatie met de andere gegevens wel iets zeggen over de duur en nabijheid van bepaalde contacten. Zekerheidshalve wordt er dan ook vanuit gegaan dat er sprake is van indirecte persoonsgegevens.

- TEKs en DKs
- Autorisatiecode
- Signaalsterkte en de contactduur[125]
- Eerste ziektedag
- Exposure Risk Value (high, mid, low)
- IP-adres

Koppelingsfase
Bijzondere persoonsgegevens
- TEKs en DKs
- RPIs
- Signaalsterkte en de contactduur
- Exposure Risk Value (high, mid, low)

Notificatiefase
Bijzondere persoonsgegevens
- De notificatie aan de gebruiker dat hij mogelijk besmet is met COVID-19
- De dag dat de gebruiker in contact is geweest met een besmet persoon (wordt vermeld in de notificatie)

Tijdens geen enkele fase worden locatiegegevens verwerkt.

Bijzondere persoonsgegevens

Voor de overgrote meerderheid van de gebruikers is er géén sprake van verwerking van bijzondere persoonsgegevens bij het gebruik van de app. Pas wanneer gegevens worden verstrekt aan de backend server naar aanleiding van een positieve testuitslag verandert het karakter van de door de gebruiker verstrekte gegevens. De verdere verwerking van de gegevens van de besmette persoon kunnen dan bijzondere persoonsgegevens betreffen. In dat geval kunnen de TEKs, de daarvan afgeleide RPIs/DKs, en de autorisatiecode worden aangemerkt als bijzondere persoonsgegevens, meer in het bijzonder gegevens betreffende de gezondheid.

De toestemming die door middel van de actieve handeling wordt verkregen voorafgaand aan het delen van gegevens met de backend server vormt een uitzonderingsgrond op het verwerkingsverbod.[126] Volgens de AVG[127] is het verwerkingsverbod niet van toepassing als de betrokkene (gebruiker) uitdrukkelijke toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

[125] De signaalsterkte en de contactduur vormen op zichzelf geen bijzondere persoonsgegeven, maar kunnen in combinatie met de andere gegevens wel iets zeggen over de duur en nabijheid van bepaalde contacten. Deze gegevens zijn van belang voor het inschatten van de medische kans op besmetting. Zekerheidshalve wordt er dan ook vanuit gegaan dat er sprake is van indirect bijzondere persoonsgegevens.
[126] ex. artikel 9 lid 1 AVG
[127] artikel 9 lid 2 onder a

Gegevensverwerkingen

Per fase bekijken we wat er aan gegevensverwerking plaatsvindt.

Tijdens de installatiefase vindt geen verwerking van persoonsgegevens plaats door VWS of de GGD-en.

Tijdens de uitwisselingsfase worden de eigen TEKs van de gebruiker bewaard, alsmede ontvangen RPIs. De daarbij behorende signaalsterkte – zowel uitgezonden als ontvangen – wordt bewaard en de duur van het bluetoothcontact.

In deze fase worden door de apps van de gebruikers weliswaar RPIs uitgewisseld, maar deze RPIs staan uitsluitend op de app van de gebruiker. Met andere woorden: volledig decentraal. Ander betrokken partijen – VWS, de GGD-en, het CIBG, Apple of Google – hebben geen toegang tot de door de app verzamelde RPIs.

Om het risico op identificatie van gebruikers zoveel mogelijk uit te sluiten, wordt bij de uitwisseling van TEKs het MAC-adres van de smartphone vervangen door een random gegenereerde code. Dit pseudo MAC-adres verandert elke 10 – 20 minuten, evenals de TEKs.

Tijdens de validatiefase worden TEKs na een autorisatieproces geüpload naar de backend werver. De geüploade TEKs van gebruikers die positief zijn getest op COVID-19 worden geconverteerd naar DKs en gevalideerd aan de hand van de autorisatiecode die de GGD in het GGD-portaal van de app heeft vastgelegd. Voor elke DK wordt de datum van de eerste ziektedag vergeleken met de datum van de TEKs. Op basis daarvan bepaalt de server een zogeheten Exposure Risk Value (high, mid, low).

Voor beheers- en beveiligingsdoeleinden worden ook IP-adressen verwerkt. Dit is inherent aan het gebruik van internet en IP-technologie. Het IP-adres wordt na zeven dagen vernietigd. Verkeersgegevens zoals IP-adressen worden zonder de TEks/DKs geanalyseerd op mogelijke aanvallen. Bij deze functionele scheiding wordt het IP-adres tijdelijk op een ander, afgescheiden gedeelte van de server opgeslagen dat wordt beheerd door KPN. Door de scheiding van verkeersgegevens en TEKs/DKs kunnen deze gegevens niet aan elkaar worden gerelateerd. Evenmin is op de server te achterhalen van welke gebruiker de TEKs/DKs afkomstig zijn. Het is dus niet mogelijk te herleiden wie welke informatie heeft verstuurd.

In de koppelingsfase worden DKs van gebruikers die positief zijn getest op COVID-19 beschikbaar gemaakt voor download vanaf de backend server. Vervolgens worden die DKs gedownload door de apps die in gebruik zijn, met het doel na te kunnen gaan of zij corresponderende RPIs hebben ontvangen in de afgelopen veertien dagen. Als er een match is, wordt op basis van de door VWS, in overleg met het RIVM, GGD-en en OMT, vastgestelde parameters en weegfactoren in de app afgewogen of er een risicovol contact is geweest, dat aanleiding kan zijn om de desbetreffende gebruikers een notificatie te sturen.

In de notificatiefase wordt aan de gebruiker gemeld dat hij mogelijk besmet is met COVID-19. Daarbij wordt vermeld op welke dag die gebruiker in contact is geweest met een besmet persoon.

Risico's in kaart brengen

Langs meerdere wegen zijn er risico's rond informatiebeveiliging en privacybescherming in kaart gebracht. We lopen de aanpak langs.

Failure mode effect analyses (FMEA)

Er is met behulp van de Failure Mode Effect Analyses een overzicht gemaakt van de risico's (foutmodi), de mogelijke ernst, hoe veelvuldig dit zal voorkomen en of bij het optreden van de fout dit te ontdekken is. We werken daarmee met een schaal van 1 (laag) tot 5 (hoog). Een uitleg over deze methodiek om tot risico's te komen, is bijgevoegd als appendix A. Deze risico's zijn allemaal teruggebracht tot een fors lager niveau. De duidingsrapportage beschrijft op hoofdlijnen de beschikbare beveiligingsmaatregelen, die genomen zijn om risico's te verminderen. Na livegang van CoronaMelder zal een nieuwe inschatting worden gemaakt op basis van de dan geldende status quo. Het doel is om tenminste eens per kwartaal een inschatting te maken, die geldt als drijfveer voor aanvullende maatregelen.

In de lijst wordt zowel de RPI (Risk Priority Number) berekend als de Critical Score. Deze vormen de basis voor het doorvoeren van beveiligingsmaatregelen.

De normering voor de analyse is als volgt samengesteld. Voor de ernst:

Effect	Score	Waardering
Kabinetscrisis/bewindspersoon treedt af	5	Catastrofaal
Surveillance tool	5	Catastrofaal
Verwerkingsverbod	5	Catastrofaal
App gaat ongewenst op zwart	5	Catastrofaal
Motie van wantrouwen in parlement	4	Zeer schadelijk
Integriteit telefoons aangetast	4	Zeer schadelijk
Integriteit app geschaad	4	Zeer schadelijk
Slechte pers die leidt tot fors lagere adoptie	4	Zeer schadelijk
Onwil in gebruik van de app	4	Zeer schadelijk
Niet voldoen aan wet- en regelgeving	4	Zeer schadelijk
Datalek van serieuze omvang > 100 betrokkenen	4	Zeer schadelijk
Instabiele dienstverlening	4	Zeer schadelijk
Onvoldoende dekking onder telefoontypes	4	Zeer schadelijk
Werking app (onbedoeld) veranderd	3	Ernstig
Pittig debat in parlement	3	Ernstig
Veel data versturen met mobiel > 1Gb	3	Ernstig
Onbetrouwbare melding uit app > 100K	3	Ernstig
Vertraagde melding	3	Ernstig
Langdurige onbeschikbaarheid backend	3	Ernstig
Hoge kosten	3	Ernstig
Mensen opgelicht door malafide apps	2	Schadelijk
Disproportioneel aantal vragen	2	Schadelijk
Herleidbaarheid naar max. 5 personen	2	Schadelijk
Beperkte discussie	2	Schadelijk
Kamervragen	1	Niet ernstig
Notificatie niet gezien/weggedrukt	1	Niet ernstig
Notificatie gezien door derde	1	Niet ernstig
Notificatie gehoord (tone) door derde	1	Niet ernstig
Enkele telefoons worden traag	1	Niet ernstig

Voorkomen:

5	Veel voorkomend	Incidenten komen dagelijks voor
4	Regelmatig	Incidenten komen wekelijks voor
3	Komt voor	Incidenten komen meerdere malen per jaar
2	Zelden	Incidenten komt minder dan eens per jaar voor (3-5)
1	Zeer zelden	Incident treedt (bijna) nooit op, bijna ondenkbaar

Detecteerbaarheid

5	Nagenoeg ondetecteerbaar	De detectie van de foutmodus is erg moeilijk of nagenoeg onmogelijk.
4	Slecht	Het detecteren van de foutmodus is moeilijk.
3	Detecteerbaar	De foutmodus is met inspanning detecteerbaar
2	Doorgaans detecteerbaar	De foutmodus is goed te detecteren.
1	Altijd detecteerbaar	Als de foutmodus gaat optreden dan is dat altijd snel te detecteren

Waardering FMEA-scores

Risicoklasse	**RPN**	**Kritiek (ernst*voorkomen)**
Kritiek	>60	>14
Hoog	40-60	>10
Ernstig	28-39	>6
Klein	9-27	>3
Verwaarloosbaar	1-8	>1

FMEA

Foutmodus	Ernst		Voor-komen	Detecteer-baarheid	RPI	CS
API van Google/Apple veroorzaakt veel stroomverbruik	4	Onwil in gebruik van de app	4	1	16	16
Gebruiker denkt matching verkeerd gaat	4	Slechte pers	4	1	16	16
In media artikel over privacy schending van de app	4	Slechte pers	4	1	16	16
Overslaan cruciaal onderdeel door tijdsdruk	3	Pittig debat	4	4	48	12
Sabotage meldingen	4	Slechte pers	3	4	48	12
Applicatiedata onbetrouwbaar door beheersfouten	4	Instabiele omgeving	3	4	48	12
Applicatiedata onbetrouwbaar door aanvaller	4	Instabiele omgeving	3	4	48	12
Door een lek in de applicatie wordt de telefoon kwetsbaar voor aanvallers	4	Integriteit telefoons geschaad	3	4	48	12
Beheerders onvoldoende getrained op security gebied waardoor de processen niet worden gevolgd en de omgeving langzaam minder veilig wordt	4	Instabiele omgeving	3	4	48	12
De omgeving functioneert niet meer doordat changes niet goed worden uitgevoerd	4	Instabiele omgeving	3	4	48	12
Eisen aan beheerpartijen bevatten onvoldoende security richtlijnen waardoor de dienstverlening niet in lijn is met de wens vanuit het ministerie	4	Instabiele omgeving	3	4	48	12
Verkeerde matching door GAEN	4	Slechte pers	3	3	36	12
Hoge kosten doordat er teveel data naar de telefoons worden gestuurd	4	Veel data > 1GB	3	3	36	12
Door een fout in de centrale omgeving wordt er teveel data naar de telefoons gestuurd; door een fout in de code op de telefoon (of in het GAEN raamwerk van de leverancier) wordt er te veel of te vaak data naar de centrale omgeving gestuurd	4	Te veel data, Hoge kosten, Veel data gebruik > 1Gb	3	3	36	12
Werking van de app onvoldoende duidelijk voor een bepaalde doelgroep	4	Onwil in gebruik van de app	3	3	36	12
Doel/intentie van de app onvoldoende duidelijk voor een bepaalde doelgroep	4	Onwil in gebruik van de app	3	3	36	12
De omgeving is niet goed gesized waardoor er performance problemen ontstaan en gebruikers hinder ondervinden	4	Onwil in gebruik van de app	3	3	36	12
Onderzoeker vindt kwetsbaarheid in de app, GAEN of centrale omgeving en maakt deze openbaar	4	Slechte pers	3	3	36	12
API van Google/Apple verandert waardoor app niet meer compatible is	4	Integriteit app geschaad	3	2	24	12

Google/Apple verandert (bewust of bij vergissing) GAEN berekeningen/calibratie factoren waardoor de app niet meer compatible is	4	Integriteit app geschaad	3	2	24	12
Google/Apple veranderen key parameters (bewust of bij vergissing) zoals de signing key/label waardoor de app niet meer werkt/compatible is met (oudere) data	4	Integriteit app geschaad	3	2	24	12
Applicatie instabiel door beheerdersfouten	4	Instabiele omgeving	3	2	24	12
Centrale omgeving kwetsbaar voor aanvallen	4	Instabiele omgeving	3	2	24	12
Helpdesk is onvoldoende bereikbaar voor vragen	4	Slechte pers	3	2	24	12
Datalek in framework	4	Integriteit app geschaad	3	1	12	12
Centrale omgeving niet beschikbaar door DDOS	4	Instabiele omgeving	3	1	12	12
Retentietijd wordt aangepast	5	Verwerkingsverbod	2	2	20	10
Door een update van het OS op het mobiel werkt de app niet meer	3	Onbedoelde werking	3	2	18	9
Door een update van het framework opn het mobiel werkt de app niet meer	3	Onbedoelde werking	3	2	18	9
Door een update van het play(google)/sideloading(apple) framework op het mobiel werkt de app niet meer	3	Onbedoelde werking	3	2	18	9
Sleutels op server worden verwijderd	4	Instabiele dienstverlening	2	4	32	8
Sleutels op server worden toegevoegd	4	Integriteit app geschaad	2	4	32	8
Datalek op server	4	Integriteit app geschaad	2	3	24	8
Cryptografische sleutel lek op de server(HSM)	4	Integriteit app geschaad	1	2	8	4
PKI Overheid tekent een rogue cryptographische sleutel	4	Integriteit app geschaad	1	2	8	4
Apple/Google accepteren een rogue unmanaged public key voor distributie `alsof' deze van NL komt	4	Integriteit app geschaad	1	2	8	4
Apple/Google accepteren revocation request voor een unmanaged public key voor distributie `alsof' deze van NL komt	4	Integriteit app geschaad	1	2	8	4
Kwaadwillende krijgt toegang tot infrastructuur	4	Instabiele dienstverlening, pittig debat, datalek van serieuze omvang	2	3	24	8
Malafide applicatie wordt gepubliceerd in de applicatiewinkels	2	Mensen opgelicht door malafide apps	4	3	24	8

Neppe app wordt gedownload	2	Mensen opgelicht door malafide apps	4	3	24	8
Applicatie crasht regelmatig op een bepaald type toestel/OS versie	4	Onvoldoende dekking onder telefoontypes	2	1	8	8
Centrale omgeving niet beschikbaar door grote hoeveelheid verstuurde sleutels	3	Langdurige onbeschikbaarheid backend	2	2	12	6
Onbevoegde functionaliteit	5	Verwerkingsverbod	1	3	15	5
Eenmalige notificatie is niet gezien door gebruiker	1	Notificatie niet gezien	4	5	20	4
Monitoring van RPIs op straat door derden	4	Slechte pers	1	5	20	4
Monitoring van RPIs door individuen	2	Herleidbaarheid naar max. 5 personen	2	5	20	4
Uit publicatiebestand zijn TEKs van een besmet persoon aan elkaar te relateren op basis van sortering in het bestand	2	Herleidbaarheid naar max. 5 personen	2	4	16	4
Decoy verkeer is te onderscheiden van authentiek verkeer	2	Herleidbaarheid naar max. 5 personen	2	4	16	4
Api omgeving kwetsbaar voor man-in-the middle aanvallen waardoor de data niet betrouwbaar is	4	Integriteit app geschaad	1	3	12	4
Encryptie/signing keys raken corrupt/kwijt	4	Instabiele dienstverlening	1	3	12	4
Oude sleutels worden op CDN gepubliceerd door boze beheerder/medewerker	4	Slechte pers	1	3	12	4
Datalek in applicatie	4	Integriteit app geschaad	1	2	8	4
Infrastructuur langdurig onbereikbaar door hoeveelheid verkeer	4	Instabiele dienstverlening	1	1	4	4
Batterij-besparende apps/OS functies sluiten de applicatie regelmatig af	3	Vertraagde melding	3	2	24	12
Telefoon van besmet persoon wordt tussen bekendmaking positieve test en uploaden veertiende dag aan een drager meegegeven in een druk gebied	1	False positive bij max. 10 personen	2	5	10	2
Vreemde mogendheid verschaft zich toegang tot backend om verkeer te bewaken	5	Surveillancetool	2	5	50	10
Onbevoegde verschaft zich fysiek toegang tot server (stelen schijven, usb-stick met malware, kapot maken server)	4	Instabiele dienstverlening, pittig debat, datalek van serieuze omvang	2	3	24	8
DNS wordt onbevoegd veranderd	4	Integriteit app geschaad, slechte pers	2	1	8	8
Temperatuur in datacenter loopt langdurige downtime	3	Werking app veranderd	2	1	6	6

Brand - automatisch gevolgd door blusschade	3	Werking app veranderd	1	1	3	3
Waterschade - langdurige downtime	3	Werking app veranderd	1	1	3	3
Een fout in de software wordt geintroduceerd en verspreid	3	Integriteit telefoons aangetast	4	2	24	12
Certificaten worden ongeldig verklaard	5	App gaat ongewenst op zwart	2	4	40	10
Certificaten verlopen	5	App gaat ongewenst op zwart	3	4	60	15
Niet authentieke software wordt verspreid onder naam CoronaMelder	5	Surveillancetool, integriteit app, malware	4	2	40	20

Dreigingsanalyse nationale en digitale veiligheid

Om de meest relevante en waarschijnlijke dreigingen, risico's en bijbehorende maatregelen in kaart te brengen, voerden de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Nationaal Cyber Security Centrum (NCSC) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) op verzoek van het Ministerie van VWS een dreigingsanalyse uit. Deze drie organisaties baseerden zich daarbij op de op dat moment beschikbare documentatie en informatie over CoronaMelder en het ontwerp van de app.

Deze stappen zijn onder coördinatie van het Ministerie van VWS doorlopen in een aantal expertsessies waaraan medewerkers van VWS (Programma Realisatie digitale ondersteuning), experts van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), van het Nationaal Cyber Security Centrum (NCSC) en van de Algemene Inlichtingen en Veiligheidsdienst (Nationaal Bureau voor Verbindingsbeveiliging, AIVD) aan deelnamen. Aan het doel en de bijbehorende opzet van de app kleven potentiële risico's op het gebied van nationale en digitale veiligheid. De app en bijbehorende systeemonderdelen en processen stellen de hoogste eisen aan privacy en beveiliging. Om de meest relevante en waarschijnlijke dreigingen, risico's en bijbehorende maatregelen in kaart te brengen leverden de NCTV, NCSC en AIVD leverden de input voor de dreigingsanalyse aangevuld met feedback op de docuenten. Deze drie organisaties baseerden zich daarbij op de op dat moment beschikbare documentatie en informatie over CoronaMelder en het ontwerp van de app.

Aangezien de dreigingsanalyse vertrouwelijke informatie, onder meer afkomstig van de intelligentiediensten, bevat over de meest waarschijnlijke dreigingen en scenario's en de genomen maatregelen, wordt deze analyse niet integraal beschikbaar gesteld. Wel kunnen we, zonder vertrouwelijke informatie openbaar te maken, laten zien op welke manier er bij de realisatie van CoronaMelder rekening gehouden is met risico's op het gebied nationale en digitale veiligheid. Ook kunnen we melden dat er maatregelen zijn genomen op basis van de analyse en de verstrekte informatie. Veel van deze maatregelen kunnen wij – vanwege dezelfde geheimhoudingsplicht – niet delen in dit rapport. Evenmin gaan wij nader in op de actoren van wie of vanwaar eventuele dreigingen kunnen komen.

De volgende documenten zijn gerelateerd aan deze dreigingsanalyse:

- Het Programma van Eisen[128] bevat de requirements voor CoronaMelder (inclusief niet-functionele eisen op het gebied van onder andere beveiliging).
- De Solution architecture[129] beschrijft de belangrijkste ontwerpkeuzes.
- Het Crypto raamwerk[130] beschrijft het cryptosysteem voor CoronaMelder.
- In de DPIA[131] zijn onder andere de risico's op het gebied van de bescherming van persoonsgegevens geanalyseerd.
- De analyse van het DP-3T project[132]. Hierin worden verschillende risico's van het door CoronaMelder gebruikte model van contact-tracering genoemd.

[128] https://github.com/minvws/nl-covid19-notification-app-coordination/blob/master/requirements/20200519%2BProgramma%2Bvan%2BEisen%2Bdef.pdf
[129] https://github.com/minvws/nl-covid19-notification-app-coordination/blob/master/architecture/Solution%20Architecture.md
[130] https://github.com/minvws/nl-covid19-notification-app-coordination/blob/master/architecture/Crypto%20Raamwerk.md
[131] https://github.com/minvws/nl-covid19-notification-app-coordination/blob/master/privacy/Gegevensbeschermingseffectbeoordeling_(DPIA).pdf
[132] https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf

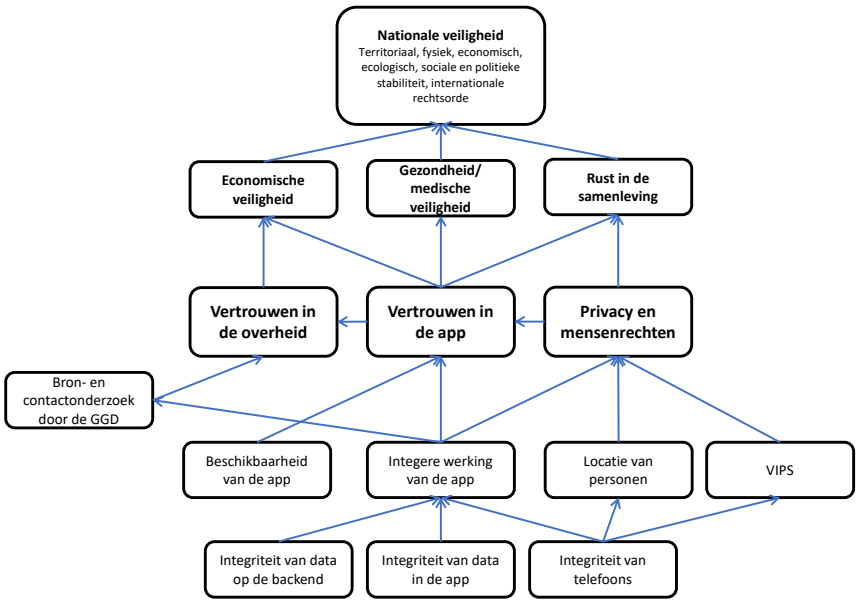
De dreigingsanalyse is uitgevoerd in vier stappen:

1. **Analyseren van de dreigingen** om inzicht te krijgen in de actoren, wat hun intentie is, welke middelen ze tot hun beschikking hebben en wat er bekend is over verschillende manieren van handelen.
2. **In kaart brengen van te beschermen belangen** rondom CoronaMelder. Het gaat daarbij om materiële en immateriële zaken waaraan schade kan ontstaan door een dreiging of door het falen van een beveiligingsmaatregel.
3. **Identificeren van scenario's** en meest voorstelbare risico's op basis van de dreigingen en te beschermen belangen.
4. **Bepalen van maatregelen** om de risico's zoveel mogelijk te mitigeren.

Deze stappen zijn doorlopen in een aantal expertsessies waaraan medewerkers van VWS (Programma Realisatie digitale ondersteuning), experts van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), van het Nationaal Cyber Security Centrum (NCSC) en van de Algemene Inlichtingen en Veiligheidsdienst (Nationaal Bureau voor Verbindingsbeveiliging, AIVD) aan deelnamen.

Belangen

Door het in kaart brengen van de te beschermen belangen verkrijgen we inzicht in de waarden, verworvenheden, materiële en immateriële zaken gerelateerd aan CoronaMelder. Een aanval of het (deels) falen van CoronaMelder kan schade toebrengen aan een van deze te beschermen belangen. Onderstaande figuur geeft de geïnventariseerde te beschermen belangen weer.



CoronaMelder is bedoeld om een bijdrage te leveren aan het te beschermen belang *gezondheid*. Wanneer de betrouwbaarheid van CoronaMelder in het geding komt, kan de gezondheid van personen schade oplopen. In het verlengde van de digitale aanvulling op het bestaande bron- en contactonderzoek kan CoronaMelder ook bijdragen aan het afbouwen of voorkomen van andere maatregelen voor de bestrijding van Covid-19, zoals de intelligente lockdown. Ook op deze manier draagt CoronaMelder bij aan de belangen *rust in de samenleving* en *economische veiligheid*. Deze drie belangen zijn samen de voornaamste bovenliggende te beschermen belangen.

Dichterbij de app zijn er twee centrale te beschermen belangen: de *privacy van gebruikers* en het *vertrouwen in de app*. Vanwege het doel van de app en potentieel gevoelige gegevens die verwerkt kunnen worden, is privacybescherming van gebruikers van groot belang. Hiermee hangt samen dat vertrouwen in de app het succes en de adoptie van CoronaMelder ten goede zal komen.

Deze twee te beschermen belangen worden beïnvloed door drie belangen die de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid volgen. De *integere werking van CoronaMelder* gaat onder meer om de integriteit van de data in de app, de backend en van de telefoons van gebruikers. De *beschikbaarheid van CoronaMelder* Betreft zowel de backend als de app zelf. De vertrouwelijkheid van *locatie en contacten van gebruikers* is sterk verbonden met de privacy van gebruikers.

Scenario's en maatregelen

Als onderdeel van de analyse is een aantal scenario's geïdentificeerd waarbij de te beschermen belangen geschaad kunnen worden. Hierbij is het ontwerp van CoronaMelder – specifiek het decentrale systeem DP-3T – als uitgangspunt genomen.[133] Deze ontwerpkeuze zonder centrale database sluit diverse aanvalsscenario's uit. De (inherente) risico's die het DP-3T systeem daarentegen met zich meebrengt op het gebied van privacy en beveiliging zijn bekend. Deze zijn onder meer gedocumenteerd in het reeds eerder genoemde analysedocument van het DP-3T-project.[134]

Twee algemene scenario's[135]:

- Kwaadwillenden gebruiken kwetsbaarheden in de app om bijvoorbeeld toegang te krijgen tot de telefoons van gebruikers. Om dit te voorkomen worden tests en beveiligingsonderzoeken uitgevoerd om kwetsbaarheden op te sporen. Het ontwikkelproces van de app is transparant en open en er wordt een meldingsproces voor kwetsbaarheden gehanteerd.[136]
- Criminelen zetten tijdens de lancering van de app malafide apps, domeinnamen of phishing aanvallen in om persoonsgegevens en/of geld van personen afhandig te maken. Risicobeperkende maatregelen omvatten onder meer goede en heldere voorlichting aan de gebruikers van de app en monitoring op (malafide) apps en domeinnamen.

Scenario gerelateerd aan de *beschikbaarheid* van de backend server:

- Uitval van de backend server – door een aanval of verstoring – kan de processen met betrekking tot de publicatie van sleutels van besmette personen verstoren. Er zijn technische maatregelen genomen om aanvallen tegen te houden en snel te herstellen na een verstoring. Er wordt uitgebreid getest op performance, stress en load.

Scenario's gerelateerd aan *integriteit* die onbetrouwbare notificaties kunnen veroorzaken:

---

[133] De keuze voor dit model heeft namelijk invloed op de relevante aanvalsscenario's.
[134] https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf
[135] In de DPIA zijn 33 concrete bedreigingsscenario's opgenomen, hun impact op verschillende niveaus en de maatregelen om deze risico's te mitigeren.
[136] CVD, Coordinated vulnerability disclosure bij NCSC. https://www.ncsc.nl/contact/kwetsbaarheid-melden

- Diverse aanvalsscenario's kunnen valse notificaties genereren of verstoren via het toestel van een gebruiker. Bijvoorbeeld door het opnieuw uitzenden van via Bluetooth ontvangen codes. Om dit tegen te gaan, worden de sleutels iedere vijftien minuten veranderd.
- Als een kwaadwillende toegang verkrijgt tot de backend server kan de data die daarop staat in theorie worden gemanipuleerd. Dit gaat om sleutels die door gebruikers zijn geüpload en die gepubliceerd worden na validatie door de GGD. Dit kan de integriteit van de centrale data schaden. Organisatorisch en technische maatregelen op het gebied van toegangsbeveiliging en logging helpen om dit risico te beperken. Ook hier worden veelvuldig tests en beveiligingsonderzoeken uitgevoerd om kwetsbaarheden op te sporen.

Scenario's gerelateerd aan de *vertrouwelijkheid* die erop gericht zijn gebruikers te identificeren:

- Er bestaan methoden om de door gebruikers uitgezonden sleutels tóch te herleiden naar een persoon. Dit beperkt zich tot één of enkele personen, of één locatie. Om dit risico te mitigeren vindt opvolging plaats op basis van het bestaande wettelijke kader.[137]
- Door netwerkverkeer intensief te monitoren kan iemand afleiden welke telefoon contact heeft met de backend server. Hieruit zou iemand kunnen opmaken dat de eigenaar van die telefoon besmet is met het virus. Een maatregelen tegen dit scenario is het versturen van afleidend verkeer naar de backend. Zodoende valt op basis van het verkeer niet af te leiden of de upload authentiek is of niet.
- Aan de kant van de backend kunnen gebruikers potentieel geïdentificeerd worden, bijvoorbeeld op basis van het ip-adres bij inkomend verkeer. Hiertoe worden technische maatregelen ingezet om herleidbaarheid te voorkomen en organisatorisch en technische maatregelen op het gebied van toegangsbeveiliging en logging. Tevens wordt er veel getest om kwetsbaarheden op te sporen.

Advies van NCTV, NCSC en AIVD

De NCTV, NCSC en AIVD brachten op basis van de dreigingsanalyse twee keer formeel advies en aanbevelingen uit aan VWS. Vanwege het vertrouwelijke karakter in verband met de nationale en digitale veiligheid van CoronaMelder kunnen we deze hier niet uiteenzetten. De conclusie van beide adviezen is dat, wanneer de gegeven adviezen worden geïmplementeerd, weerbaarheid georganiseerd is tegen potentiële risico's op het gebied van nationale veiligheid.

[137] Denk daarbij aan opvolging op basis van het verwerkingsverbod onder de AVG (een onbevoegde mag geen gezondheidsgegevens verwerken), of opvolging op basis van computervredebreuk en het toevoegen van gegevens aan een geautomatiseerd werk (138ab/350a Sr.)

Ethiek

Naast privacy, security en bescherming van persoonsgegevens is veel aandacht besteed aan de ethiek rondom CoronaMelder. Een ethische analyse van de app[138] is opgesteld door een panel onder voorzitterschap van Prof.dr.ir. P.P.C.C. Verbeek, Universiteit Twente.[139] (In bijlage G is het volledige rapport van dit panel opgenomen.) Het expertpanel richtte zich in zijn analyse op zowel het ontwerp van de app als de inbedding ervan in onze maatschappij.

Ethisch kader

Uitgangspunt bij de ethische beoordeling van CoronaMelder was dat de voor bestrijding van de coronacrisis ingezette technologie dient te worden ingezet om individuen in staat te stellen hun verantwoordelijkheid te nemen, in plaats van hen te controleren, stigmatiseren of te beperken. Hoewel data en technologie belangrijke instrumenten zijn in de bestrijding van een pandemie, hebben deze intrinsieke beperkingen en kunnen deze uitsluitend dienen ter ondersteuning van de effectiviteit van een overkoepelend en omvattend bestrijdings-programma. Centraal hierbij staat het vinden van de juiste balans tussen het individu en het collectief. Aan de ene kant dienen de privacy en autonomie van individuele mensen te worden gewaarborgd, maar anderzijds vraagt een verantwoorde omgang met de situatie rondom het virus ook om onderlinge solidariteit.

Het expertpanel heeft de volgende tien kernwaarden geïdentificeerd die centraal dienen te staan in het beoordelen van CoronaMelder in combinatie met de backend server:

1. Vrijwilligheid: Het gebruik van de app dient geheel vrijwillig te zijn.
2. Effectiviteit: De app moet voldoende effectief zijn, op het niveau van het individu (betrouwbare meldingen), de GGD (behulpzaam bij bron- en contactonderzoek), en de overheid (effectief in het terugdringen van de verspreiding van het virus).
3. Privacy: De app dient de privacy van gebruikers te respecteren.
4. Rechtvaardigheid: Het gebruik en de inbedding van de app dienen bij te dragen aan een rechtvaardige verdeling van de lasten en de opbrengsten.
5. Inclusiviteit: De app moet zo breed mogelijk bruikbaar en toegankelijk zijn, ongeacht fysieke of mentale beperking, etnische achtergrond of digitale vaardigheden.
6. Procedurele rechtvaardigheid: Er is eerlijke toegang tot en deelname aan het ontwikkelproces van de app nodig.
7. Verantwoordelijkheid: Er dient een duidelijke en rechtvaardige verdeling van verantwoordelijkheden te zijn tussen overheid, GGD en burger.
8. Voorkomen van oneigenlijk gebruik: Er moet worden voorkomen dat de app voor andere doeleinden wordt gebruikt dan waarvoor deze is ontwikkeld.
9. Borgen burgerlijke vrijheden: De app dient tijdelijk te zijn en gewenning aan monitoring van burgers dient voor de toekomst voorkomen te worden.
10. Noodzakelijkheid en proportionaliteit: De inzet van de app is noodzakelijk en proportioneel voor bereiken van het doel.

Vanuit deze kernwaarden heeft het panel de ethische issues geïdentificeerd, onderzocht en beoordeeld. De aanbevelingen van het panel zijn - voor zover relevant en binnen de technische mogelijkheden - in het definitieve ontwerp van de app verwerkt.

---

[138] Ethische analyse van de COVID-19 notificatie-app ter aanvulling op bron en contactonderzoek GGD, 14 juli 2020.

[139] De andere panelleden waren: Prof.dr. Philip Brey, Universiteit Twente, Prof.dr. Rinie van Est, Rathenau Instituut en TU Eindhoven, Prof.dr. Lisette van Gemert, Universiteit Twente, Prof.mr. dr. Michiel Heldeweg, Universiteit Twente, Prof.dr.mr. Lokke Moerel, Tilburg University

Vrijwilligheid

In onze liberale rechtstaat is burgerlijke vrijheid het uitgangspunt. Een wettelijke regeling kan deze vrijheid en vrijwilligheid expliciet borgen.

Het gebruik van de app dient derhalve geheel vrijwillig te zijn. Er zijn geen drempels voor installeren (zoals kosten). Evenmin worden er incentives gegeven (voordelen bij installeren, of nadelen bij niet installeren) waardoor mensen zich gedwongen kunnen voelen de app te installeren. Aan weigering van de app zijn geen nadelen verbonden en burgers krijgen via de app geen hulp die ze zonder de app niet zouden krijgen.

Vrijwilligheid louter als afwezigheid van een verplichting (met bijbehorende sancties) impliceert niet vanzelf dat installatie en gebruik ook in de praktijk als vrijwillige keuze mogelijk zijn. Ook in dit opzicht zijn de aanwezigheid van een reële keuzemogelijkheid en de afwezigheid van plicht of dwang van belang. Zolang de prikkels die vrijwilligheid kunnen beïnvloeden uitsluitend zijn toegespitst op onderkenning van het belang van de app bij de bestrijding van COVID-19, zodat de potentiële gebruiker zich (meer) bewust wordt van het eigen en/of maatschappelijk belang bij het verminderen van de kans op verspreiding van het virus, wordt vrijwilligheid niet beperkt. Problematisch voor vrijwilligheid wordt het gebruik van prikkels waarbij voor- of nadelen worden ingezet voor andere belangen dan de bestrijding van COVID-19. Denk daarbij aan het koppelen van financiële toekenningen of de toegang tot niet aan COVID gerelateerde diensten aan de installatie en gebruik van de app. Of aan het verhogen van kosten van niet aan COVID gerelateerde dienstverlening, zoals hogere verzekeringspremies, beperkingen van toegang tot de werkplek, voetbalstadions of pretparken en beperkingen in de toegang tot COVID-testfaciliteiten.

Als volstrekte vrijwilligheid voorop staat, wordt tevens geaccepteerd dat sociaal verantwoordelijk gedrag, bij de keuze om de app te installeren en hoe deze te gebruiken, geheel een keuze van de autonome burger is.

Installeren en activeren van de app gebeurt vrijwillig als de gebruiker de app, op basis van goede en beschikbare voorinformatie, zelfstandig downloadt en activeert. Daarmee is in principe sprake van impliciete instemming (op basis van informed consent). Het is dan ook ethisch verantwoord om de app-toepassingen en het app-gebruik steeds afhankelijk te maken van (informed) consent. Daarmee beslist de gebruiker steeds zelf of een bepaalde functie wordt toegepast of niet. Denk aan de functionaliteit waarbij de app aan de geïnfecteerde gebruiker toestemming vraagt voor het delen van zijn/haar contactcodes (TEKs), opdat andere app-gebruikers een notificatie kunnen krijgen als ze met de geïnfecteerde persoon relevant contact hebben gehad.

Er dient onderscheid te worden gemaakt tussen deze instemming en toestemming voor het verwerken van persoonsgegevens. Toestemming heeft ook een specifieke juridische functie als een van de wettelijke grondslagen voor de verwerking van de persoonsgegevens onder de AVG. De grondslag voor de verwerking van de persoonsgegevens onder de AVG is dan de grondslag van de wet en niet de grondslag van toestemming. De privacy toezichthouders vereisen dat burgers specifiek worden geïnformeerd over de toepasselijke grondslag, omdat de rechten van het individu onder de AVG verschillen al naar gelang de grondslag voor de verwerking. Privacy-autoriteiten achten het bijvoorbeeld veelal misleidend om toestemming te vragen als een app in feite niet kan worden gebruikt zonder dat de betreffende data kan worden verwerkt. Bij het geven van de toestemming valt er dan namelijk niets te kiezen en is

de betreffende toestemming niet vrijwillig gegeven. Zo kan toestemming te allen tijde worden ingetrokken, terwijl bij een wettelijke grondslag dit niet mogelijk is.

Als vrijwilligheid voorop staat, impliceert dit ook de mogelijkheid om op elk gewenst moment eventuele notificaties te wissen, het gebruik te pauzeren (door de smartphone niet mee te nemen, of door bluetooth uit te zetten), of zelfs te beëindigen door de app te de-installeren.

Beoordeling van de app

Voor zover het expertpanel kan beoordelen worden er geen prikkels geboden waardoor mensen zich genoodzaakt voelen de app te downloaden en zijn er ook geen negatieve consequenties als mensen de app niet downloaden. Verder wordt (zelfs met voorgenomen wetgeving) voorkomen dat derde partijen de app feitelijk verplicht stellen. Denk aan werkgevers die de app verplichten voor werknemers. De app biedt gebruikers de mogelijkheid om een notificatie van potentiële besmetting te wissen. Hierdoor wordt voorkomen dat derden inzage vragen (of eisen) in notificaties van de app.

De app vraagt geen consent voor verwerking van de persoonsgegevens bij het installeren van de app. Dit is terecht aangezien de verwerking van de contactcodes een inherente feature van de app is waarvoor een wettelijke grondslag bestaat. Het vragen van toestemming voor de verwerking van de persoonsgegevens is hier niet nodig. Het zou de indruk wekken dat er wat te kiezen valt, hetgeen niet zo is.

De app vraagt wel specifiek toestemming van een geïnfecteerd persoon voor het delen van zijn/haar contactcodes (TEKs), opdat deze een notificatie kunnen krijgen indien ze met de geïnfecteerde persoon relevant contact hebben gehad. Ook hier is het vragen van consent niet vereist onder de AVG, omdat voor de dataverwerking via de app een wettelijke grondslag bestaat. In feite is het vragen van toestemming hier dus verwarrend, omdat die toestemming niet is vereist. Toch is het vanuit ethisch oogpunt wel belangrijk dat de gebruiker zich realiseert dat hij/zij de contactcodes gaat delen en de gevolgen hiervan goed begrijpt. Ook is belangrijk dat de gebruiker zelf het delen van de contactcodes initieert (user control), zodat deze wetenschap heeft van het moment waarop de contactcodes worden gedeeld. Misschien wil de gebruiker zelf bepaalde contacten informeren voordat deze de notificatie krijgen. Deze handeling is geen toestemmingsvereiste voor AVG-doeleinden.

Met een pauzeknop kan de werking van de app tijdelijk worden onderbroken. De app moet door de gebruiker zelf weer worden geactiveerd. Hiertoe krijgt hij/zij een herinnering wanneer de app niet binnen een bepaalde periode is gereactiveerd. De pauzeknop is een belangrijk mechanisme om de app daadwerkelijk op elk moment vrijwillig te laten zijn.
De app dient daadwerkelijk uitgeschakeld te kunnen worden. Als de enige mogelijkheid voor gebruikers is om de app geheel te de-installeren indien zij de app op enig moment niet aan willen hebben, is de app niet echt vrijwillig omdat deze optie te omslachtig is en daarmee geen reële optie.

Effectiviteit

Op individueel niveau moet de betrouwbaarheid van de meldingen worden afgewogen tegen de kans dat besmettingen worden opgespoord: er moet een juiste balans zijn tussen specificiteit (het voorkomen van vals positieven) en selectiviteit (het detecteren van reële besmettingsrisico's). Teveel vals positieve meldingen zorgt voor onnodige onrust en ondermijnt het vertrouwen in de app; te veel gemiste notificaties van potentiële besmetting

(vals negatieven) verkleint de effectiviteit van de app en ondermijnt daarmee eveneens het vertrouwen.

De effectief van de app alsmede de juiste balans tussen specificiteit en selectiviteit zal moeten blijken uit de pilotfase en de uiteindelijke praktijk. Het is in dat kader belangrijk om expliciet vast te stellen dat de app in technisch opzicht werkt, tijdig is met notificaties, door voldoende mensen wordt geadopteerd en leidt tot accurate data en inzichten.

Vals-positieven en vals-negatieven zijn onvermijdelijk, maar in die gevallen moeten er verzachtende of compenserende maatregelen worden getroffen. Het ethisch panel heeft hier twee bemerkingen.

1. De impact van de vals-positieve (overnotificatie) dient hier zwaarder te wegen dan de vals negatieve (ondernotificatie).
2. Het aantal vals-negatieven en vals-positieven dient zo laag mogelijk te zijn. Het percentage kan naar beneden worden gebracht door startdatum klachten te registreren en in de risicoanalyse voor notificaties mee te nemen. Het panel adviseert om te onderzoeken of dit op een privacy-vriendelijke manier kan gebeuren. Het panel is van mening dat hier het collectieve belang van het effectief afremmen van de verspreiding van het virus moet prevaleren boven het afschermen van de gegevens omtrent het begin van de klachten van patiënten met COVID-19.

Het is van belang om vast te stellen hoeveel werk de app met zich meebrengt voor de GGD. Gezien de huidige ondercapaciteit bij de GGD-en is de vraag gerechtvaardigd of het huidige systeem de workflow die deze digitale variant van het bron- en contactonderzoek met zich meebrengt aankan.

Om de effectiviteit te kunnen bepalen, moet het doel van de app duidelijk worden gecommuniceerd. Wat is de verwachte adoptie?

Privacy

De app moet voldoen aan vereisten van doelbinding, dataminimalisatie en opslagbeperking, securityvereisten en de beginselen van privacy-by-design. Via de app verstuurde notificaties dienen verder niet geheel geautomatiseerd te zijn: er dient menselijke tussenkomst te zijn waarbij een risico-inschatting wordt gemaakt door de gezondheidsautoriteiten voordat de notificaties worden verstuurd.

Het ethisch panel constateert dat de app aan belangrijke privacy-by-design, data minimalisatie en data retentie vereisten voldoet. De app is vrijwillig en werkt op basis van contact tracing en trackt niet de locatiegegevens van gebruikers. De door de app uitgezonden contactcodes zijn anoniem en wisselen periodiek waardoor ook bij onrechtmatig opvangen van codes door derden deze niet te herleiden zijn tot individuele personen. De ‘match’ van de contactcodes vindt plaats op de mobiele telefoon van de gebruiker zelf en niet in een centrale database. Op de server worden uitsluitend niet tot individuele burgers herleidbare gegevens verwerkt. Bij notificatie wordt geen informatie verstrekt over locatie of tijd, waaruit de identiteit van de geïnfecteerde persoon kan worden afgeleid.

Het ethisch panel is van oordeel dat registratie van de eerste ziektedag door de GGD (op de server en niet in de app) noodzakelijk en proportioneel is voor de contact tracing, mits dit op een privacy-vriendelijke manier kan geschieden. Er wordt voorkomen dat de notificaties voor andere doeleinden worden gebruikt dan waarvoor bedoeld, doordat de gebruiker de

mogelijkheid heeft de notificaties te wissen. Ook wordt voorkomen dat kwaadwillenden meldingen doen dat individuen besmet zijn, doordat deze melding de uitwisseling van een code tussen GGD en gebruiker van de app vereist indien de gebruiker positief is getest.

Rechtvaardigheid

Het ethisch panel onderkent in rechtvaardigheid drie aspecten:

1. erkenning – wiens belangen zijn beschermingswaardig?
2. procedure – hoe krijgt deze bescherming aandacht?
3. inhoud – welke mate van bescherming wordt geboden, met welke verdeling van voor- en nadelen?

Wat betreft de substantiële rechtvaardigheid moet het gebruik en de inbedding van de app bijdragen aan een rechtvaardige verdeling van de lasten en de opbrengsten. Eventuele ongelijk verdeelde negatieve sociale of economische effecten van quarantaine moeten worden gemitigeerd. Bij dergelijke ongelijkheid moet sociale hulp voorhanden zijn.

Inclusiviteit

De app moet zo breed mogelijk bruikbaar en toegankelijk zijn, ongeacht lichamelijke beperking, etnische achtergrond, of digitale vaardigheden. De app is ook bruikbaar voor burgers met een beperkte databundel of internetverbinding.

Gelijke beschikbaarheid houdt in dat iedereen in staat is om de app te downloaden voor gebruik op zijn of haar smartphone, zonder grote obstakels. Hierbij is bijzondere aandacht nodig voor de volgende gebruikers:

- Personen die niet in het bezit zijn van een smartphone.
- Personen met smartphones waarop de app niet is te installeren of niet goed werkt, bijvoorbeeld doordat een ander besturingssysteem wordt gebruikt dan Android of IOS, of doordat de smartphone verouderd is.

Gelijke toegankelijkheid houdt in dat iedereen voldoende in staat is om de functionaliteiten van de app te begrijpen en benutten. Dit wordt op een aantal dimensies gedekt.[140] Ook mensen met een laag opleidingsniveau en mensen met cognitieve beperkingen moeten in staat zijn om de werking van de app begrijpen en om de app effectief te gebruiken.

[140] Programma van Eisen: Q16 (beschikbaarheid in de voor de gebruikers belangrijkste talen), Q17 (voldoen aan toegankelijkheidsrichtlijnen voor mensen met een lichamelijke beperking), Q18 (bruikbaarheid door burgers met beperkte digitale vaardigheden en beperkte taalbeheersing) en Q37 (eenvoudige en laagdrempelige installatie).

Procedurele rechtvaardigheid

Er is eerlijke toegang tot en deelname aan het ontwikkelproces van de app nodig. Een rechtvaardige verdeling van baten en lasten vereist inclusieve participatie, eerlijk en transparant kennisbeheer en een open ontwerpwerpproces op basis van gedeelde waarden en normen. Hiertoe dient aan een aantal voorwaarden te worden voldaan:

a) Maatschappelijke betrokkenheid

Worden de perspectieven van alle relevante stakeholders gehoord en meegenomen in het ontwerpproces?

Binnen het huidige ontwikkelproces worden diverse relevante partijen bij de ontwikkeling van de app betrokken: diverse experts (wetenschappers en praktijkprofessionals van RIVM en GGD; universitaire wetenschappers), diverse gebruikers van de app (inclusief speciale doelgroepen, zoals slechtzienden/blinden, slechthorenden/doven, mensen met een motorische beperking, laaggeletterden en mensen die geen Nederlands spreken).

b) Transparantie

Transparantie betreft adequate en zo volledig mogelijke informatieverschaffing aan het publiek over de doelstelling van de app, de werking van de app, in zowel technische als functionele zin, de erbij betrokken organisaties en hun rol, de procedures en het beleid eromheen, en de mogelijke gevolgen die zijn verbonden aan het gebruik van de app voor zowel individu als maatschappij. Hiertoe zijn nodig: adequate voorlichting over wat de app maar ook wat de app niet kan, gebruik van open source.

c) Normatief afwegingskader

Er moet een duidelijk normatief afwegingskader zijn vastgesteld dat helderheid geeft over de publieke waarden die worden nagestreefd en de voorwaarden die de Nederlandse samenleving stelt aan een notificatieapp.

In het Programma van Eisen[141] worden zogenaamde functionele en niet-functionele eisen benoemd, evenals een aantal randvoorwaarden en uitgangspunten. Onder de niet-functionele eisen staat een aantal belangrijke maatschappelijke en juridische voorwaarden.

d) Aandacht voor sociale innovatie

Is er naast technische innovatie voldoende aandacht voor sociale innovatie? Het doel moet niet zijn een perfect functionerende app te realiseren, maar een verantwoorde bijdrage aan de samenleving te leveren, optimaal bij te dragen aan het afremmen van de verspreiding van het virus en burgers een instrument te geven om op vrijwillige basis hun verantwoordelijkheid te nemen voor hun eigen gezondheid en die van anderen.

Na een valse start (de Appathon) wordt de app nu tijdens het ontwikkelproces op diverse momenten en manieren getest op technische haalbaarheid, gebruikersvriendelijkheid, digitale veiligheid en privacy.

[141] Gepubliceerd op 19 mei 2020.

e) Maatschappelijke beoordeling

Om de app zorgvuldig te ontwikkelen dienen grondige analyses te worden uitgevoerd van de technische, veiligheids-, ethische en juridische kwesties die op het spel staan. Er is vooralsnog te weinig aandacht voor de invloed van de app op diverse sociale praktijken en voor de mate waarin de bestaande maatschappelijke en institutionele context waarin de app functioneert door burgers als voldoende vertrouwenwekkend wordt gezien.

Er moet een brede maatschappelijke beoordeling van de app worden uitgevoerd wanneer die eenmaal in werking is, die naast de huidige aandacht voor ethische aspecten ook gericht is op de sociale impact en juridische aspecten ervan.

f) Communicatie

Over de ontwikkeling van de app dient goed gecommuniceerd te worden door de overheid richting de burger. Deze communicatie moet doel- en doelgroepgericht zijn. De overheid moet alle informatie over het proces van de ontwikkeling van de app goed vindbaar en bereikbaar maken.

g) Toezicht

Adequaat toezicht is vereist op de ontwikkeling van CoronaMelder vanaf de ontwerpfase, de ontwikkeling en het gebruik tot de terugkeer naar 'normale' gezondheidsomstandigheden. Het RIVM heeft twee Taskforces en een Begeleidingscommissie ingesteld. Deze bewaken het proces van ontwikkeling van de app en voorzien het ministerie van VWS van onafhankelijk advies.

In de eerste Taskforce – Digitale Ondersteuning Bestrijding COVID-19 – kijken wetenschappers en praktijkprofessionals van het RIVM en vanuit de GGD-en en universiteiten naar de mogelijkheden van digitale ondersteuning bij de bestrijding van het coronavirus.

De tweede Taskforce – Gedragswetenschappen – adviseert vanuit gedragswetenschappelijke expertise over de bijdrage die digitale ondersteuning kan leveren aan het beheersen en opvolgen van besmettingen met het coronavirus. Het doel van de adviezen is dat de acceptatie van de digitale hulpmiddelen wordt vergroot, er minder ongewenste effecten zijn en gewenst gedrag wordt vergroot.

De Begeleidingscommissie adviseert aan de minister over het plan van aanpak en de waarde van de app vanuit een breder maatschappelijk perspectief (veiligheid, juridische, epidemiologische en gedragsaspecten).

Onder het hoofdstuk 'Veilig tegen Corona, 3de uitgangspunt, De situatie bij de lancering' wordt de samenstelling van deze Taskforces en Begeleidingscommissie vermeld.

Verantwoordelijkheid

Er moet een duidelijke en rechtvaardige verdeling van verantwoordelijkheden zijn tussen overheid, GGD en burger. Verantwoordelijkheden worden niet afgeschoven op de burger. De app ondersteunt burgers bij het zich verantwoordelijk gedragen en verantwoordelijkheid nemen voor het eigen gedrag en de gevolgen daarvan voor de ander.

Van burgers kan verwacht worden dat zij besmetting van zichzelf en anderen proberen te voorkomen en bij besmetting anderen informeren met wie zij in contact zijn gekomen. Van de

overheid kan verwacht worden dat zij de regie neemt op macroniveau en beleid uitvoert en handhaaft dat nodig is om de pandemie in te dammen. Met de app verschuift een deel van de verantwoordelijkheid van de overheid naar de burger.

Vermeden moet worden dat de app vooral wordt aangeprezen als middel om zichzelf te beschermen en solidariteit met anderen onderbelicht blijft. Hoewel het gebruik van de app door de overheid niet verplicht wordt gesteld, mag er in de communicatie wel een moreel appel worden gedaan op burgers in het kader van de collectieve verantwoordelijkheid.

Voorkomen van oneigenlijk gebruik

Er moet worden voorkomen dat de app voor andere doeleinden wordt gebruikt dan waarvoor deze is ontwikkeld. Geborgd moet worden dat de officiële app herkenbaar is, zodat fraude met fake apps wordt voorkomen. Analyse van de volgende zaken is belangrijk: mogelijke verstoringen door kwaadwillende partijen, mogelijke fouten door gebruikers of derden in het gebruik van de app of het hanteren van procedures daaromheen, mogelijk ongewenst gedrag dat kan optreden bij gebruik van de app, zoals het intimideren van contacten bij het verkrijgen van een melding of het stigmatiseren van gebruikers of niet-gebruikers.

Borgen burgerlijke vrijheden voor de toekomst

In de liberale rechtsstaat staan burgerlijke vrijheden voorop en is er expliciete democratische rechtvaardiging vereist voor overheidsbemoeienis, zeker als die vrijheidsbeperkend is. Om deze reden dient volstrekt helder te zijn welke publieke waarden en doelen worden nagestreefd en aan welke voorwaarden de introductie en het gebruik van de app is gebonden.

a. Algemeen vertrekpunt

Er moet een legitiem doel zijn voor het beperken van burgerlijke vrijheden. Het is voor de bescherming van burgerlijke vrijheden van groot belang dat burgers een laagdrempelige mogelijkheid hebben om over de door hen ervaren beperkingen en nadelen van de app met de bevoegde instanties in contact te treden, te kunnen klagen en rechtsbescherming in te kunnen inroepen.

Hiernaast is ook beperking van de tijdsduur van de (mogelijke) vrijheidsbeperking van belang, zowel ter bescherming van die vrijheden zelf als ter voorkoming van sluipende gewenning aan monitoring van burgers (‘glijbaan effect’) voor de toekomst. Wanneer de verspreiding van COVID-19 effectief is bedwongen, dient de app buiten werking te worden gebracht. Voorkomen moet worden dat de app een cultuurverandering inluidt waarin mensen minder huiverig worden voor surveillance.

b. Tijdelijkheid, experimenteren, beëindigingsproces

Vanaf het beschikbaar stellen van de app is er strikt genomen niet langer sprake van een experiment. De functionaliteit wordt verondersteld in en op orde te zijn, zowel wat betreft de app zelf alsook qua omringende infrastructuur (contact tracing, testen; informatievoorziening, klachtmogelijkheden; ondersteunende en randvoorwaardelijke wet- en regelgeving). Desondanks zal er, zeker in aanvang, sprake zijn van onzekerheden zoals het optreden van app/systeemfalen. Omdat hier grote publieke en private belangen op het spel staan (volksgezondheid; private gezondheid, veiligheid, privacy, en chilling-effects), acht het ethisch panel het belangrijk dat een ‘voorzorgsbenadering’ wordt toegepast. Dit behelst onder meer dat op voorhand wordt voorzien in tijdstippen en procedures voor tussentijdse evaluaties van de werking en het gebruik van de app. Ook moet op voorhand helder zijn wanneer het

reguliere gebruik van de app wordt beëindigd. Bijvoorbeeld wanneer er een probaat vaccin en/of medicijn tegen COVID-19 algemeen beschikbaar komt.

Het inbouwen van tijdelijkheid wordt niet alleen ingegeven door statisch te definiëren risico's, maar houdt ook verband met de dynamiek van risico-aanvaarding. Tijdens de piek van een pandemie worden andere risico's aanvaardbaar geacht dan wanneer de pandemie op z'n retour is.

Proportionaliteit en subsidiariteit

Het ethisch panel tracht de app qua ethisch-maatschappelijke aanvaardbaarheid via twee vragen te toetsen: 1. Is er sprake van een legitiem doel? 2. Is er sprake van een aanvaardbare (mogelijke) impact op bestaande belangen?

a. Noodzaak: legitiem doel

Het ethisch panel veronderstelt dat de app, met hoop op grootschalig gebruik, vanuit publiek belang bezien ten minste gewenst en misschien zelfs noodzakelijk is. Het ethisch panel veronderstelt tevens dat de uitvoering van de app zodanig wordt vormgegeven dat deze in strikte zin doelgebonden is. Het faciliteert uitsluitend het mogelijk maken van notificatie ter bestrijding van COVID-19.

b. Evenredigheid: proportionaliteit en subsidiariteit

Het ethisch panel beoordeelt de proportionaliteit en subsidiariteit van de effecten van de app vanuit drie elementen van proportionaliteit (het evenredigheidsbeginsel):

1. Doel-middel proportionaliteit. De specifieke publieke voordelen van introductie en gebruik van de app moeten groter zijn dan de nadelen in private en in andere publieke belangen. Zolang privacy, in elk geval in termen van desbetreffende juridische kaders, adequaat wordt beschermd, dan veronderstelt het ethisch panel dat deze proportionaliteit niet-problematisch hoeft te zijn – al blijft kritisch volgen gewenst. Het panel veronderstelt dat het risico van de onrust veroorzaakt door een besmettingsmelding vrijwillig wordt aanvaard. De nadelen van vals-positieven zijn problematischer dan die van vals-negatieve meldingen, aangezien positieve notificaties angst, onrust en mogelijk quarantaine meebrengen.
2. De kosten-proportionaliteit. De nadelen van het notificatiesysteem dienen zo klein mogelijk te zijn. Als hetzelfde doel met minder nadelen kan worden gerealiseerd, dan moet dat met die mindere nadelen worden gedaan. Een vergelijking met alternatieven zou, ook na introductie, moeten doorgaan
3. Private proportionaliteit voor publieke lasten en voordelen. Voor zover er sprake is van lasten en voordelen door overheidsbemoeienis dienen deze gelijkmatig over burgers te worden verdeeld. Het ethisch panel is van oordeel dat hieraan wordt voldaan wanneer het gebruik van de app daadwerkelijk vrijwillig en inclusief is.

Noodzaak en evenredigheid

Op het moment van schrijven[142] zijn we in de bestrijding van COVID-19 in een nieuwe fase belandt. Een tweede golf dreigt, maar blijft vooralsnog op enige afstand, zo lijkt het. Het aantal besmettingen neemt licht toe, met name in clusters van lokale besmettingshaarden[143], maar het aantal ziekenhuisopnames en opnames op IC's blijft redelijk stabiel. Nadat beperkende maatregelen werden versoepeld, worden deze nu mondjesmaat weer aangescherpt.

Ook het OMT uitte op 30 juli haar zorgen over het toentertijd recente verloop van het aantal bevestigde COVID-19-infecties. Bijzondere zorg is er voor besmettingen met onbekende bron. In ieder geval is duidelijk dat bestrijding van het virus nog nodig is.

Doelstelling

Beperkende maatregelen kunnen we alleen afbouwen als verdere infecties zoveel mogelijk worden voorkomen. Hier ligt een cruciale rol voor bron- en contactopsporing.[144] Het draagt ertoe bij dat keten van infecties wordt doorbroken en dat daarmee verdere infecties worden voorkomen. De GGD heeft de wettelijke taak tot het doen van bron- en contactopsporing. Dit is vormvrij en kan breed worden opgevat. De GGD moet immers kunnen differentiëren om afhankelijk van de omstandigheden de beste aanpak te kiezen.

Bron- en contactopsporing sorteert het meeste effect wanneer zoveel mogelijk mensen die risicovol in de nabijheid van een geïnfecteerde persoon zijn geweest zo snel mogelijk kunnen worden gewaarschuwd. Hiertoe is het vereist dat mensen nog voordat er sprake is van enige besmetting bijhouden in wiens nabijheid zij zijn geweest. Uiteraard moet dit zo privacy-vriendelijk mogelijk worden gerealiseerd. Om het bron- en contactonderzoek derhalve op zo groot mogelijke schaal in te kunnen zetten – opdat de effectiviteit optimaal is – ontwikkelen we digitale hulpmiddelen.

De app wordt ingezet als digitale aanvulling op de reguliere bron- en contactopsporing. Dit heeft een tweeledig doel:

1) Personen die in de nabijheid van geïnfecteerde personen zijn geweest worden sneller bereikt. De analoge methode van contactopsporing is een arbeidsintensieve bezigheid. Het vergt van de GGD (te)veel tijd en mankracht om de contactpersonen te bereiken, waardoor geïnfecteerde personen intussen opnieuw andere personen kunnen besmetten. Daarnaast is de doeltreffendheid, doelmatigheid en de te verwerken aantallen meldingen beperkt. In veel gevallen herinneren mensen zich niet altijd exact met wie zij contact hebben gehad over een bepaalde tijdsperiode, laat staan dat men van al die personen de contactgegevens zou hebben.
2) Het bereik van het contactonderzoek wordt in belangrijke mate vergroot. Het bron- en contactonderzoek wordt met de bijdrage van de app uitgebreid naar onbekenden. Iemand kan in de nabijheid zijn geweest van onbekende mensen. Denk hierbij aan een bezoek aan een speeltuin of park of een reis met het openbaar vervoer. Van deze nabije mensen is de identiteit onbekend en blijft ook na fysiek onderzoek niet te achterhalen.

[142] 22 augustus 2020
[143] Huishoudens, familie- en vriendenfeestjes.
[144] Dit sluit aan bij het uitgangspunt van de EDPB (Europees Comité voor gegevensbescherming) dat 'het rechtskader voor gegevensbescherming is ontworpen met flexibiliteit voor ogen en als zodanig een efficiënte respons mogelijk maakt die de pandemie indamt en de fundamentele mensenrechten en vrijheden beschermt'.

Proportionaliteit

De vraag is in hoeverre de voorgenomen (digitale) gegevensverwerkingen noodzakelijk zijn in de bestrijding van COVID-19. Daarbij kijken we naar proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden. Ook is er aandacht voor subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

De AVG bepaalt dat alle verwerkingen van persoonsgegevens moeten voldoen aan de vereisten van proportionaliteit en subsidiariteit. Kortom: doel, aard en omvang van de gegevens moeten met elkaar in verhouding. Daarnaast moet altijd worden gekozen voor de minst ingrijpende verwerking van persoonsgegevens.

De ernst en de gevolgen van het virus, zowel voor individuen persoonlijk als op landelijke schaal zijn aanzienlijk. Mensen kunnen ernstig ziek worden en zelfs overlijden. Mensen kunnen niet meer het leven leiden zoals zij gewend waren en kunnen daarvan ook psychische hinder van ondervinden. Daarnaast loopt de economie grote schade op. Tijd is een belangrijke factor: hoe eerder het virus opgespoord kan worden, hoe beter en effectiever het virus kan worden bestreden. Derhalve is dat het verwerken van een zeer beperkt aantal gegevens gedurende 14 dagen proportioneel. Helemaal wanneer deze gegevens zoveel mogelijk lokaal worden opgeslagen, op de smartphones van gebruikers.

De zorgwekkende trend (zie Inleiding) zet de capaciteit voor de GGD om het reguliere bron- en contactonderzoek uit te voeren onder druk. Eén bron- en contactonderzoek duurt volgens de GGD gemiddeld meer dan 12 uur. De GGD-en zien zich daardoor genoodzaakt om regelmatig hun capaciteit op te schalen. De GGD GHOR[145] spraak haar zorgen uit op 5 augustus, dat bij een doorlopende trend de maximale capaciteit (70.000 testen en 3000 onderzoeken per dag) geleidelijk in zicht komt. Enkele regio's kunnen niet meer zonder de hulp van andere regio's. De inzet van moderne digitale middelen zoals de app is daarom noodzakelijk en proportioneel.

Subsidiariteit

Naar verwachting zal de app een substantiële bijdrage leveren aan de bestrijding van de epidemie. De bestaande analoge bron- en contactopsporing is weliswaar minder ingrijpend, maar bereikt onvermijdelijk niet eenzelfde ruime groep mensen. Ook voorziet de bestaande werkwijze in minder snelle en gerichte actie. Zeker wat het waarschuwen van mensen die men niet kent betreft, is er geen goed alternatief voorhanden. Voor zover als sprake is van verwerking van persoonsgegevens, gaat het om een gepseudonimiseerde vorm.

Effectiviteit en evaluatie

De doeltreffendheid van CoronaMelder hangt nauw samen met het aantal personen dat de app gebruikt. Een fundamentele vereiste voor de inzet van de app is het vertrouwen van de burger. Hoe meer vertrouwen, hoe groter de vrijwillige deelname van burgers. Daarom is het gebruik van de app dan ook met de sterkste waarborgen omkaderd.

[145] De koepelorganisatie van 25 GGD-en.

Simulatiemodellen en eerste wetenschappelijke inzichten – onder meer van de Universiteit van Oxford[146] – suggereren dat een notificatieapp substantieel kan bijdragen aan de reductie van het aantal verdere besmettingen.[147] Ook helpt het om de tijd tussen besmetting en signalering van andere geïnfecteerde mensen te reduceren. Naar verwachting gebeurt dat zelfs wanneer de app beperkt in gebruik wordt genomen door de burgers.

Voordat CoronaMelder landelijk in gebruik wordt genomen, wordt deze uitvoerig getest op effectiviteit. Zowel technisch – stelt de app inderdaad risicovolle nabijheid vast? – als op gebruikersvriendelijkheid en toegankelijkheid. Deze tests worden vergeleken met testresultaten uit andere landen, zoals Duitsland en Zwitserland. Ook gedurende het gebruik van de notificatieapp wordt onderzoek gedaan naar de effectiviteit en worden buitenlandse ontwikkelingen op dit vlak nauwgezet gevolgd.

De werking van CoronaMelder zal verder worden gemonitord aan de hand van een vooraf vastgesteld evaluatieprotocol. Daarbij wordt periodiek bekeken of er daadwerkelijk sprake is van breder, sneller en efficiënter opsporen van besmette mensen. Deze monitoring leidt zo nodig – bijvoorbeeld wanneer niet beoogde neveneffecten zich openbaren – tot aanpassingen en bijstellingen van de notificatieapp. Denk aan het aanpassen van de parameters waarmee wordt berekend of er sprake was van een risicovol contact, zodat het aantal valse positieven zoveel mogelijk wordt beperkt. Mocht de notificatieapp onvoldoende effectief blijken dan wordt het gebruik ervan beëindigd.

Ook vindt er gedurende de inzet van de app zal doorlopend ethische toetsing plaats.

[146] https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown
[147] Zie ook: https://pubmed.ncbi.nlm.nih.gov/32234805/

Privacybescherming

Zoals blijkt uit dit rapport en de media-aandacht voor CoronaMelder, speelt adequate privacy van de notificatieapp een cruciale rol. Daarbij gaat het niet alleen om de richtlijnen van de AVG, maar ook om het verkrijgen van een zo breed mogelijke acceptatie van de app. Hoe breder die acceptatie hoe effectiever de app kan bijdragen aan het daadwerkelijk uitvoeren van de exit-strategie.

Diverse maatregelen

De volledige ontwikkelingsfase van de app werd volgens privacy-by-design gewerkt. Dit resulteert in diverse maatregelen om de privacy van gebruikers van CoronaMelder om zo goed mogelijk te borgen. Welke dat zijn zetten we hieronder uiteen.

1. 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. Binnen de app is het niet bekend wie iemand is noch waar iemand is geweest.
- Wanneer een gebruiker positief test op het COVID-19 virus en dit via de app meldt, is dit niet aan de naam of contactgegevens van deze persoon te koppelen.

2. Werkt decentraal

Tijdens de koppelingsfase controleert het DP-3T protocol op de smartphone of een gebruiker een notificatie moet ontvangen. Dit gebeurt dus lokaal en niet op een centrale server. De koppeling van de gebruiker met een andere door COVID-19 besmette gebruiker wordt gemaakt op basis van factoren als signaalsterkte, de duur van het contact en de dag waarop de besmette persoon zich ziek voelde. Op basis daarvan wordt middels parameters en weegfactoren bepaalt hoe risicovol een contact is geweest. Niemand anders dan de ontvanger van de notificatie is hiervan op de hoogte.

3. Bewaart gegevens niet langer dan strikt noodzakelijk.

De ontvangen RPIs en eigen TEKs worden veertien dagen bewaard op de smartphone van gebruikers. Deze termijn hangt samen met de incubatietijd van COVID-19. Wie besmet raakt krijgt doorgaans na vijf tot zes dagen klachten. Het is zeer onwaarschijnlijk dat er na veertien dagen nog een besmetting zal plaatsvinden. Na deze termijn worden de pseudonieme sleutels van de smartphone verwijderd.

4. Uitgezonden codes niet aan persoon te koppelen

De codes die gedeeld worden via Bluetooth Low Energy (RPIs) zijn niet aan een persoon te koppelen. Bij ziekte worden sleutels opgestuurd (DKs) die niet meer functioneren voor het aanmaken van uitwisselingscodes.

- Via Bluetooth Low Energy delen telefoons met de actieve CoronaMelder elke tien tot twintig minuten willekeurige codes met elkaar (RPIs). Deze codes zijn afgeleid van eveneens willekeurige sleutels (TEKs) die door de app elke 24 uur automatisch worden gegenereerd. Deze codes zijn niet tot een persoon te herleiden.
- Als iemand na een test COVID-19 blijkt te hebben, kan deze persoon toestemming geven om zijn/haar sleutels (TEKs) op de backend server te laten zetten. De laatste

sleutel wordt pas na middernacht geüpload, zodat een besmet persoon ook niet te herleiden is op de dag dat hij/zij te horen krijgt dat hij corona heeft.

Op deze manier zijn de codes niet aan personen te koppelen.

5. Regelmatige variatie van codes

De codes die de gebruikers van CoronaMelder met elkaar delen, variëren regelmatig. Elke tien tot twintig minuten maakt de app een nieuwe willekeurige code (RPI). Deze worden afgeleid van de TEKs. Dit zijn eveneens willekeurige sleutels die door de app iedere 24 uur worden vernieuwd. Hierdoor is herleidbaarheid naar personen erg lastig.

Hoe kan dan toch een notificatie bij de juiste persoon terechtkomen? Nadat een besmette gebruiker zijn/haar codes naar de backend server heeft geüpload, worden deze geconverteerd naar zogeheten Diagnosis Keys (DKs). In de DK zit de TEK-datum en de eerste ziektedag besloten. De backend server stelt de DKs beschikbaar, zodat deze kunnen worden opgehaald door andere smartphones met een actieve app. Op de smartphone zelf wordt gecontroleerd of er tussen de DKs een match is met de bijbehorende RPIs. Vervolgens genereert de een notificatie om de gebruiker te informeren over de verhoogde kans op een besmetting met COVID-19 en een advies om zich bij klachten te laten testen.

6. Stuurt regelmatig nepsleutels uit

Om eventuele ongewenste monitoring van internetverkeer te verstoren, stuurt de app regelmatig dummy uploads uit. Daardoor ziet een buitenstaander niet welke ziekmeldingen echt zijn en welke niet. Bovendien is het netwerkverkeer zelf ook nog eens versleuteld. Het is dus niet te onderscheiden of iemand écht anderen waarschuwt, of dat het een nep-waarschuwing betreft. Zo wordt voorkomen dat het opsturen van sleutels leidt tot herkenbaarheid.

7. Gebruikt uitsluitend strikt noodzakelijke gegevens

In de app worden de volgende gegevens verwerkt:

- Rolling proximity indicators (RPIs). Deze pseudonieme codes maakt de app elke 10 tot 20 minuten aan.
- Temporary Exposure Keys (TEKs). Deze pseudonieme sleutels wordt elke 24 uur door de app gemaakt.
- Diagnosis Keys (DKs). Een afgeleide sleutel van de TEK die een besmet persoon aan de backend server heeft geüpload.
- Pseudo MAC-adres. Om het risico op identificatie van gebruikers zoveel mogelijk uit te sluiten, wordt bij de uitwisseling van TEKs het MAC-adres van de smartphone vervangen door een random gegenereerde code. Dit pseudo MAC-adres verandert elke 10 – 20 minuten, evenals de TEKs.
- Signaalsterkte en de contactduur.
- Autorisatiecode. Dit is de GGD-sleutel in de app die een besmet persoon doorgeeft aan de GGD, als deze persoon heeft besloten anderen te willen waarschuwen.
- Exposure Risk Value (high, mid, low). Op basis van deze berekening wordt bepaald of een gebruiker wel of geen notificatie krijgt.
- IP-adres

Diverse notificatieapps uit andere landen gebruiken meer gegevens. CoronaMelder gebruikt uitsluitend bovenstaande gegevens die strikt noodzakelijk zijn om de app te laten functioneren. Al het andere zou meer privacy-risico's met zich meebrengen.

8. Bevestiging van besmetting

Pas nadat de GGD een geüploade sleutel via een autorisatiecode heeft geverifieert met een besmette gebruiker, wordt een besmetting bevestigd. Deze code in de app en wordt door een besmet persoon voorgelezen aan de GGD-medewerker. Iedereen kan TEKs via de app uploaden. Om een wildgroei aan vals positieve meldingen te voorkomen – wat het vertrouwen in de app zou ondermijnen – is deze verificatie ingevoerd. Sleutels van niet besmette gebruikers komen dan weliswaar op de backend server, maar de DKs kunnen vanwege het ontbreken aan de verificatieslag niet worden gedownload door andere app-gebruikers.

9. Vrijgegeven sleutels niet zichtbaar voor GGD

Wanneer sleutels worden vrijgegeven, kan de GGD niet zien of de TEKs zijn geüpload. De GGD ook niet bij sleutels komen. Zo zijn deze gegevens ook voor de GGD afgeschermd. Een besmet persoon kan binnen 24 uur nadat hij positief op COVID-19 is getest, bepalen of hij zijn sleutels wil delen.

10. Software schermt gegevens af

CoronaMelder berekent wanneer een gebruiker een notificatie moet krijgen. Voor deze berekening gebruikt de app software van Google en Apple.[148] De notificatieapp kan niet bij de sleutels en de ontvangen codes, aangezien deze door de software van Apple en Google worden versleuteld en vergrendeld. Dit vormt extra bescherming tegen misbruik.

11. Geen ander doel

De voorwaarden van Apple en Google verbieden overheden gegevens voor een ander doel te gebruiken dan het bestrijden van COVID-19. Dit staat in hun licentievoorwaarden. Wanneer iemand toch probeert bij de sleutels te komen om die voor andere doeleinden te gebruiken, dan komt daarmee het bestaan van CoronaMelder in gevaar. Google en Apple kunnen om die reden de licentie namelijk intrekken. Ieder ander gebruik is onwenselijk en is dan ook verboden.

12. Geen statistieken

Anders dan bij sommige notificatieapps uit andere landen, worden er in CoronaMelder geen statistieken bijgehouden. Het bijhouden van statistieken is een gangbare toepassingen binnen veel apps, maar dit is bij CoronaMelder doelbewust vermeden. Er vloeit derhalve geen informatie terug naar centrale servers.

13. Geen cookies

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

14. Wetgeving tegen verplichting

Er komt wetgeving die het verplichten van CoronaMelder strafbaar stelt. 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 wordt opgenomen dat mensen die misbruik maken van CoronaMelder een half jaar gevangenisstraf of 8.000 euro boete kunnen krijgen.

[148] De Exposure Notification API

15. Melding niet traceerbaar

Niemand (behalve de gebruiker die zelf de notificatie ontvangt) 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 op het moment dat deze de notificatie ontvangt.

16. Sleutels gesorteerd op alfabet

Wanneer iemand die is besmet met COVID-19 anderen wil waarschuwen via CoronaMelder kiest deze persoon ervoor zijn of haar TEKs te delen. De sleutels van besmette personen worden op alfabetische volgorde geüpload, als extra stap om herleidbaarheid te voorkomen.

17. Verkeersgegevens worden gescheiden

Bij het versturen van de TEKs naar de server worden deze direct gescheiden van het IP-adres. Op de firewall van de backend server wordt het IP-adres ontkoppelt van de TEKs. Daardoor valt niet te herleiden van welke gebruiker de TEKs/DKs afkomstig zijn. Op deze manier is er geen herleidbaarheid.

18. De sleutels hebben een digitale handtekening

CoronaMelder downloadt DKs 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. Op deze manier wordt voorkomen dat mensen misbruik kunnen maken door valse sleutels beschikbaar te stellen.

19. Geen back-up

Apple en Google maken geen automatische noch handmatige back-up van de sleutels op telefoons. Alles is erop gericht om de identiteit van mensen te beschermen.

Privacy-recht

Een belangrijk onderdeel van CoronaMelder is het op orde hebben van het privacy-recht en in de meeste gevallen hebben we het dan over de Algemene Verordening Gegevensbescherming (kortweg: AVG). Die is van toepassing als er persoonsgegevens worden verwerkt.

Juridische termen

Er zijn veel verschillende begrippen in het privacy-recht, die vaak verwarring of discussie oproepen. We lopen de belangrijkste langs, waarbij zowel de definitie als een uitleg de revue passeert.

Persoonsgegevens

Definitie:

> *alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;*

Uitleg

Wat zijn persoonsgegevens? Persoonsgegevens zijn op de een of andere manier te herleiden naar een natuurlijke (dat is een nog levende) persoon. Of gegevens herleidbaar zijn, is soms ingewikkeld vast te stellen. Zaken als klantnummer, kenteken, internetadres of IP-adres, telefoonnummer, foto en huisadres zijn dat natuurlijk wel. Een internetadres, klantnummer of kenteken zijn geen persoonsgegevens als ze niet naar een persoon (of kleine groep van personen) te herleiden zijn. Soms zijn losse gegevens geen persoonsgegevens. In combinatie met andere gegevens kunnen ze wel herleidbaar zijn. Bij twijfel is het daarom slim om gegevens als persoonsgegevens te behandelen. Zolang het niet om persoonsgegevens gaat, is de AVG niet van toepassing.

Context bij CoronaMelder

- Een internetadres kan een persoonsgegeven zijn als iemand vanuit huis online is, maar op een groot kantoor is dat niet zo.
- De sleutel als Diagnosis Key (DK) is in theorie een persoonsgegeven. Want zolang de sleutel nog op de telefoon staat (dus niet na 14 dagen is verwijderd) is het denkbaar dat iemand met toegang tot de telefoon en de mogelijkheid van het kraken van de beveiligingslaag van Apple en Google bevestiging krijgt dat een DK bij iemand hoort. Is de sleutel op de telefoon verwijderd dan is er geen herleidbaarheid meer en is het geen persoonsgegeven.

Bijzondere (categorieën van) persoonsgegevens

Er is geen losse definitie van bijzondere persoonsgegevens opgenomen, maar ze worden benoemd in het eerste lid van artikel 9 AVG:

> *Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische*

gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Uitleg

In veel gevallen zijn persoonsgegevens 'gewoon', maar het kan voorkomen dat persoonsgegevens 'bijzonder' zijn. Deze zijn extra gevoelig en daarom gelden er bijzondere regels. Het gaat dan om:

1. gegevens waaruit ras of etnische achtergrond blijkt;
2. gegevens waaruit politieke opvattingen blijken;
3. gegevens waaruit religieuze of levensbeschouwelijke opvattingen blijken;
4. gegevens waaruit lidmaatschap van een vakbond, politieke partij, kerk of ander levensbeschouwelijke organisatie blijkt;
5. gegevens over gezondheid;
6. genetische gegevens;
7. gegevens over seksueel gedrag of gerichtheid;
8. biometrie op het moment dat deze gegevens gebruikt worden voor unieke identificatie. Een foto op sociale media is niet bedoeld om iemand te identificeren, maar op een legitimatiebewijs wel.

Er is een verbod op het verwerken van bijzondere persoonsgegevens. Dat is een strenge regel.

Uitzonderingen verwerkingsverbod

Er zijn uitzonderingen in de AVG opgenomen:

1. Als de betrokkene uitdrukkelijk toestemming heeft gegeven. Daarbij kunnen EU-landen ervoor kiezen om toestemming onmogelijk te maken voor bepaalde typen bijzondere persoonsgegevens. Het kan per land verschillen hoe dat vorm krijgt.
2. Om te voldoen aan verplichtingen op het gebied van arbeidsrecht en socialezekerheidsrecht.
3. Voor de vitale belangen van de betrokkene of andere natuurlijke personen. Denk daarbij aan het voorkomen van een epidemie of informatie die levensreddend kan zijn.
4. Een organisatie zonder winstoogmerk die zich richt op het gebied van politiek, levensbeschouwing, godsdienst of vakbond. Maar dan mogen deze bijzondere persoonsgegevens niet zonder toestemming buiten de instantie worden verstrekt.
5. Informatie die kennelijk door de betrokkene openbaar is gemaakt. Vooral het woordje 'kennelijk', zoals dat ook in de AVG staat, is verraderlijk. Dit lijkt uit te sluiten dat je zeker moet weten dat de betrokkene het openbaar heeft gemaakt. Dan kun je denken aan informatie die via sociale media naar buiten komt.
6. De gegevens zijn nodig voor een rechtsvordering.
7. De verwerking is noodzakelijk in verband met een zwaarwegend recht in de EU of in een lidstaat. Mocht daarvan sprake zijn, dan moeten er wel 'passende en specifieke' maatregelen zijn om de belangen van de betrokkene te beschermen.
8. De verwerking is nodig voor preventie of arbeidsgeneeskunde, het beoordelen van arbeidsgeschiktheid van de werknemer, medische diagnoses, het geven van gezondheidszorg, sociale diensten of behandelingen.
9. De verwerking is nodig voor een algemeen belang op het gebied van de volksgezondheid, grensoverschrijdende gevaren voor de gezondheid om hoge normen van de zorg te waarborgen. Opnieuw moeten er 'passende en specifieke' maatregelen worden genomen.

10. De verwerking is noodzakelijk voor de archivering in algemeen belang, de verwerking van gegevens voor wetenschappelijk of historisch onderzoek of statistische doeleinden. De randvoorwaarde is wel dat het recht op de bescherming van persoonsgegevens wordt geëerbiedigd en 'passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.'

Bijzondere persoonsgegevens mag je niet verwerken, tenzij je aan een van de uitzonderingen kunt voldoen. De AVG vraagt wel dat je goed nadenkt over hoe je dat zo verantwoordelijk mogelijk doet.

Context bij CoronaMelder

Bij CoronaMelder is al duidelijk dat een DK een persoonsgegeven is. Met iemands telefoon in de hand en goede hacker skills is de lijst van nog bewaarde sleutels te vinden en valt iemand ter herleiden. Het is daarom een persoonsgegeven. De DK is een sleutel die verraadt dat het gaat om iemand die positief heeft getest op het virus. Dat zegt derhalve iets over de gezondheid van een persoon. Daarmee spreken we over bijzondere gezondheidsgegevens, ook al is de kans dat bovenstaande scenario werkelijkheid wordt klein te noemen.

Verwerking

Definitie:

> *een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;*

Uitleg

Een 'verwerking' is eigenlijk alles waarin een persoonsgegeven een vorm van bewerking ondergaat, zodat jouw organisatie haar werk kan doen. Of dat nu een onderdeel van je administratie is, of een vastlegging in een CRM-systeem, mailinglijst enzovoort, het zijn allemaal 'verwerkingen'.

Context bij CoronaMelder

Er is sprake van verwerking bij CoronaMelder, omdat veel data te herleiden is tot een persoon. Die wordt in de verschillende fasen uitgewisseld en opgeslagen.

Verwerkingsverantwoordelijke

Definitie:

> *een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;*

Uitleg

Voor de verwerking is altijd tenminste een partij verantwoordelijk. Soms zijn het meerdere partijen. Volgens de wetgever ben je verantwoordelijk op het moment dat je het doel (het waarom je een verwerking doet) en de middelen (de manier waarop je de verwerking vormgeeft) bepaalt. Het kan ook zijn dat er bij een verwerking meer dan één verwerkingsverantwoordelijke is voor het geheel of een onderdeel van de verwerking.

Context bij CoronaMelder

Het doel van CoronaMelder is het digitaal ondersteunen van bron- en contactonderzoek van de GGD-en. Dat doel is bepaald door de Minister van VWS. Hij zet het hele systeem op. De GGD-en bepalen hoe het bron- en contactonderzoek verloopt. Beide zijn dan ook de verwerkingsverantwoordelijken. Het ministerie voor het geheel, terwijl de GGD-en verantwoordelijk zijn voor de verificatiefase.

Zoals verderop blijkt is er nog wel een onderdeel waarover discussie mogelijk is. Want wie is er nu verantwoordelijk voor de telefoon? Je zou kunnen stellen dat dat het ministerie is, maar zij beheren daar verder niets. Je kunt ook zeggen dat het de gebruiker van de telefoon is. Die bepaalt of hij/zij de app wil installeren en met welk doel (om verantwoordelijkheid naar anderen te nemen of zelf een waarschuwing te krijgen bij een verhoogd risico op besmetting met corona). Is de gebruiker de verwerkingsverantwoordelijke dan is het voor een zuiver huishoudelijk doel. In dat geval is op de telefoon de AVG niet van toepassing.

Verwerker

Definitie:

> *een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;*

Uitleg

Wanneer een verwerkingsverantwoordelijke gebruik maakt van de diensten van een andere partij om de verwerking te laten uitvoeren dan noemen we dat een verwerker. Het gaat daarbij dan om dat er gegevens worden verwerkt.

Context bij CoronaMelder

Het doel van CoronaMelder is het digitaal ondersteunen van bron- en contactonderzoek van de GGD-en. Dat doel is bepaald door de Minister van VWS. Hij zet het hele systeem op. De GGD-en bepalen hoe het bron- en contactonderzoek verloopt. Beide zijn dan ook de verwerkingsverantwoordelijken. Het ministerie voor het geheel, terwijl de GGD-en verantwoordelijk zijn voor de verificatiefase.

Betrokken partijen

Binnen het volledige proces van het digitale bron- en contactonderzoek zijn diverse partijen betrokken. Alle spelen zij een eigen rol in de gegevensverwerking, die varieert van verwerkingsverantwoordelijke tot verwerker en van verstrekker tot ontvanger.

Verwerkingsverantwoordelijken

De verwerkingsverantwoordelijkheid is op twee niveaus neergelegd.

1. Minister van VWS

De Minister van VWS is de verwerkingsverantwoordelijke voor gegevensverwerkingen qua de inrichting en het beheer van CoronaMelder. Ook de werking en de beveiliging van de app valt onder de primaire verwerkingsverantwoordelijkheid van de minister van VWS.
Het beheer omvat het mede inrichten, wijzigen en hosten van de app.

De minister laat zich adviseren door het Outbreak Management Team over het gebruik en de afstelling van de app. De minister van VWS verleent de GGD-en toegang tot het GGD-portaal. Tot slot valt ook de implementatie van de app onder de primaire verwerkingsverantwoordelijkheid van de minister.

Aangezien tijdens de ***installatiefase*** geen persoonsgegevens worden verwerkt, zijn noch de minister van VWS noch de GGD aan te merken als (gezamenlijke) verwerkingsverantwoordelijke. Tijdens deze fase wordt de gebruiker wel voor het eerst direct geïnformeerd over de werking van de app. De minister van VWS en de GGD-en zijn in gelijke mate gezamenlijk verantwoordelijk voor de inhoud van de informatie-disclaimers, de privacyverklaring en de toelichtende teksten in de app. Deze teksten worden in gezamenlijk overleg tussen de minister van VWS en de GGD-en vastgesteld. De minister draagt zorg voor de actualisatie van de privacyverklaring.

Tijdens de ***uitwisselingsfase*** hebben de minister van VWS en de GGD-en géén toegang tot de op de smartphone van een gebruiker vastgelegde gegevens (waaronder de RPIs, de TEKs, de signaalsterkte en de contactduur). Deze gegevens worden immers decentraal en zonder tussenkomst van enige server uitgewisseld. De minister van VWS en de GGD-en dragen in zoverre dus geen verwerkingsverantwoordelijkheid voor de gegevens die zich in de uitwisselingsfase in de app van de gebruiker bevinden.[149]

Tijdens de ***validatiefase*** vinden voor het eerst in het proces gegevensverwerkingen plaats die vallen onder de gezamenlijke verwerkingsverantwoordelijkheid van de minister van VWS en de GGD-en. Hiervan is alleen sprake wanneer een gebruiker positief wordt getest én deze ervoor kiest zijn TEKs te verzenden naar de backend server. De validatie van de besmetting en het versturen van de autorisatiecode valt onder de primaire verwerkingsverantwoordelijkheid van de GGD.

Vanaf dit moment verandert het karakter van de persoonsgegevens. Na de vaststelling van de positieve besmetting zijn de verstrekte persoonsgegevens – de TEKs/DKs, de autorisatiecode, de signaalsterkte en de contactduur, de registratie van de eerste ziektedag, de Exposure Risk Value en het IP-adres – aan te merken als bijzondere persoonsgegevens. Het betreft namelijk gegevens omtrent de gezondheid van de gebruiker en van zijn contacten.

2. De GGD

De GGD is zelfstandig verwerkingsverantwoordelijk voor de eventuele persoonsgegevens die buiten de app worden verwerkt. In deze fase kan de betrokkene desgewenst zijn AVG-rechten uitoefenen. Zodra de gebruiker door middel van de autorisatiecode toestemming heeft gegeven voor het uploaden van de TEKs/DKs is de uitoefening van de rechten van de betrokkene niet meer mogelijk. Het is namelijk na het uploaden van de TEKs/DKs niet meer

[149] Tijdens deze fase worden geen gezondheidsgegevens of andere bijzondere gegevens uitgewisseld als bedoeld in artikel 9 lid 1 AVG.

mogelijk om te achterhalen welke codes op de besmette gebruiker betrekking hebben (privacy-by-design).[150]

De beschikbaarstelling van de TEKs/DKs tijdens de ***koppelingsfase*** door middel van de backend server valt onder de gezamenlijke verwerkingsverantwoordelijkheid van VWS en de GGD-en. De verwerkingsverantwoordelijkheid voor het beheer en de beveiliging van de (bijzondere) persoonsgegevens ligt primair bij de minister van VWS. De GGD en VWS hebben gelijkwaardige verwerkingsverantwoordelijkheid voor het vaststellen van de parameters van de Exposure Risk Value.

VWS en de GGD-en zijn gezamenlijk verwerkingsverantwoordelijk voor de inhoud tijdens de ***notificatiefase***. In het uitzonderlijke geval dat een ontvanger van de notificatie het besmettingsrisico kan herleiden tot de besmette gebruiker – bijvoorbeeld wanneer de ontvanger die betreffende dag maar met één persoon contact heeft gehad – kan de notificatie een persoonsgegeven vormen over de besmette gebruiker.

3. De gebruiker

Een rapport van Privacy Management Partners is bijgevoegd als bijlage E. Zij hebben op basis van een aantal vragen gekeken naar verwerkingsverantwoordelijkheid. In hun analyse komen zij tot de conclusie dat de gebruiker voor de telefoon zelf de verwerkingsverantwoordelijke is. Vanuit deze zienswijze is de AVG niet van toepassing (met inbegrip van de API van Apple en Google). Privacy Management Partners schrijven daarover:

> *Artikel 4(2) definieert 'verwerking' als: Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.*
>
> *• CoronaMelder App*
>
> *Uit deze definitie blijkt dat – anders dan waar VWS in de DPIA van uitgaat – het uitgeven van software geen 'verwerking' is in de zin van de AVG. Hoewel de uitgever bepaalt welke gegevensverwerkingsfunctionaliteit in de software wordt ingebouwd en hoe deze eruit ziet, zoals in casu het feit dat gebruikers RPIs met elkaar kunnen uitwisselen via Bluetooth, is dit geen 'verwerking' in de zin van de AVG en is de AVG dus per definitie niet van toepassing op VWS voor zover gebruikers van de app gegevens met elkaar uitwisselen. De verwerking aan de kant van de overheid begint pas op het moment dat een gebruiker via de app de gegevens naar de backend heeft verstuurd.*
>
> *Dit ligt anders voor de gebruikers van de app. Zij verwerken elkaars RPIs en het is allerzins redelijk om aan te nemen dat de RPIs in veel gevallen ook persoonsgegevens zijn in de zin van de AVG. Echter, omdat de gebruikers de app in hun privédomein gebruiken, kunnen zij zich beroepen op de uitzondering voor persoonlijk gebruik (art. 2(2)(c) AVG), waardoor de*

[150] Uit artikel 11, tweede lid, AVG volgt dat vanaf dat moment dat de AVG-rechten van de betrokkene (artikelen 15 tot en met 20 AVG) niet meer van toepassing zijn.

AVG op de gegevensverwerking door die gebruikers niet van toepassing is. Idem voor de DKs die gebruikers downloaden om blootstellingsrisico's te berekenen.

De redenering is begrijpelijk, maar wordt door het ministerie niet gevolgd om twee redenen:

1. De minister heeft duidelijk aangegeven de privacy zo goed mogelijk te willen borgen. Het kiezen voor het volgen van deze lijn zou betekenen dat er verder niet sterk zou hoeven worden ingezet op het maken van afspraken met Apple en Google over hun API. Nadrukkelijk wordt ervoor gekozen dit wel binnen het verantwoordelijkheidsgebied houden van het hele stelsel. Dat reflecteert ook de wet.
2. Het zou kunnen leiden tot veel debat of er wel of geen verwerkingsverantwoordelijkheid is. De minister wil dit kortsluiten door de verantwoording te nemen en maximaal te sturen op informatiebeveiliging en privacybescherming.

Verwerkers

Het CIBG

Deze uitvoeringsorganisatie van het ministerie van VWS verzorgt de technische exploitatie van de backend server. VWS maakt (ook namens de GGD-en) verwerkersafspraken met CIBG. Voor het publiceren (het voor downloaden beschikbaar maken) van de DKs maakt de CIBG gebruik van het een daarvoor ingericht KPN platform. Dat bevindt zich binnen de Europese Economische Ruimte.

KPN

De minister van VWS en de GGD-en zullen een deel van het beheer van de app uitbesteden aan KPN. Voor zover het bedrijf al (bijzondere) persoonsgegevens verwerkt, zal KPN in dat verband optreden als verwerker van de minister van VWS en de GGD-en. VWS zorgt ervoor dat, mede namens de GGD-en, met KPN een verwerkersovereenkomst wordt gesloten die voldoet aan de vereisten van artikel 28 lid 3 AVG. VWS ziet er mede namens de GGD-en op toe dat KPN de verplichtingen uit de verwerkersovereenkomst naleeft.

Apple en Google

Hoewel ze in de lijst van verwerkers zijn opgenomen, maar verwerken Apple en Google zelf géén persoonsgegevens. Gezien de zorg omtrent de betrokkenheid van deze partijen, onder meer geuit door de Autoriteit Persoonsgegevens, besteden we er hier aandacht aan.

Deze bedrijven zijn betrokken als leveranciers van Exposure Notification API, dat de technische basis vormt voor de uitwisseling van nabijheidsgegevens via Bluetooth Low Energy. Google en Apple hebben technische voorwaarden gesteld aan het gebruik van de Exposure Notification API.

Google en Apple bepalen niet het doel. Zij bepalen of Nederland een app krijgt en houden als bedrijf niet de gegevens bij. Zij bouwen software dat bij CoronaMelder wordt ingezet als middel. De API vormt met de daarop rustende software een geheel dat op de telefoon draait. Bij de ontwikkeling van CoronaMelder is voor dit middel, maar bijvoorbeeld de Franse app laat zien dat het ook mogelijk is om zelf een dergelijke laag te maken.

In de app als geheel worden persoonsgegevens verwerkt. Maar de bedrijven Apple en Google als zodanig verwerken geen persoonsgegevens. De gegevens worden namelijk verwerkt op de

telefoons. Apple en Google zijn derhalve niet meer dan softwareleverancier. De situatie zou ander zijn wanneer Apple en Google op hun platformen gegevens zouden verwerken.

Bij het ontwerp van de Exposure Notification API is ervoor gezorgd dat Apple en Google geen toegang (kunnen) verkrijgen tot de gegevens in de app. In de gebruiksvoorwaarden van de API, opgesteld door Google, wordt het voorgaande bevestigd. Hierin zijn onder meer de volgende bepalingen opgenomen:

> *In providing the Service, Google has no role in determining the purposes for which, or manner in which, any personal data are processed by the App.*

En:

> *While end users of your App may provide personal data as part of their use of the App, you will not share this end-user personal data with Google. You may only share end-user personal data with third parties with user consent, and only as necessary for COVID-19 response efforts.*

Uiteraard is het van belang dat de minister van VWS en de GGD-en kritisch monitoren of en zo ja, in hoeverre eventuele toekomstige aanpassingen van de Exposure Notification API leidt tot veranderde risico's.

Doel van de verwerking

De verwerking van persoonsgegevens heeft zowel voor de minister van VWS als voor de GGD het volgende doel: burgers in digitale aanvulling op het analoge bron- en contactonderzoek van de GGD-en de mogelijkheid bieden om elkaar zo anoniem mogelijk te waarschuwen, in de bestrijding van COVID-19 besmettingen. VWS is met name stelselverantwoordelijk voor de inrichting en de werking van de app en het informeren van de gebruikers over de werking van de app. De GGD is in belangrijke mate verwerkingsverantwoordelijk voor de validatie van besmettingen.

Grondslag van de verwerking

Om gegevens te mogen verwerken moet er een grondslag zijn om van een rechtmatige verwerking te kunnen spreken. Omdat er veel discussie over dit punt is geweest, gaan we er hier nader op in.

De grondslag wordt besproken in het eerste lid van artikel 6 van de AVG:

> *De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:*
>
> *a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;*
>
> *b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;*
>
> *c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;*
>
> *d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;*

e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Voor overheden is er in de meeste gevallen sprake van "een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen". Ook voor CoronaMelder is dat het geval. De grondslag werd gezien in de Wet publieke gezondheid artikel 3 en 7. Er is geen losse wet nodig om de grondslag te creëren, maar hiertoe is wel besloten om daarmee nog explicieter te zijn en ook misbruik bij wet te verbieden.

In de fase van advisering stelde de Autoriteit Persoonsgegevens vragen bij dit onderwerp. Deze vragen met antwoorden zijn in bijlage F te vinden[151]. Op de vraag over dit onderwerp is uitgebreid geantwoord, waarbij de kern ligt in de interpretatie van de wetgeving:

Verder is van belang dat de in de Wpg voorgeschreven bron- en contactopsporing door de GGD een breed doel dient, namelijk het tegengaan van de verspreiding van infectieziekten zoals het virus, en dus ook breed moet worden uitgelegd[152].

De Autoriteit Persoonsgegevens is het daar in het advies (bijlage B) niet mee eens en schrijft[153]:

Vanwege de gezamenlijke verwerkingsverantwoordelijkheid moeten alle partijen zelfstandig beschikken over een rechtmatige verwerkingsgrondslag. De AP constateert dat de Minister afwijkt van het advies van de AP op het wetsvoorstel Tijdelijke wet maatregelen COVID-19. Met name is de Minister van mening dat de huidige publieke taak van hemzelf voldoende is opgenomen in de Wpg. Uit de artikelen 3 en 7 Wpg en de toelichting daarop blijkt dat hierin is geregeld dat de Minister de bevoegdheid heeft om de leiding te geven aan de bestrijding van infectieziekten zoals COVID-19. In dat kader kan de Minister de voorzitter van de veiligheidsregio opdragen hoe de bestrijding ter hand te nemen (Artikel 7, eerste lid, van de Wpg). Daarnaast heeft de Minister de taak om de kwaliteit en doelmatigheid van de publieke gezondheidszorg te bevorderen en draagt de Minister tevens zorg voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur (artikel 3, eerste lid, van de Wpg). Uit deze bepalingen kan worden afgeleid dat de Minister bevoegd is de burgemeesters aanwijzingen te geven over hoe zij gebruik moeten maken van hun eigen bevoegdheden, bijvoorbeeld die ze hebben uit hoofde van hoofdstuk V van de Wpg. De AP is van oordeel dat uit de bevoegdheid en

[151] Zie pagina 4 onder d van bijlage F.
[152] *Kamerstukken II* 2007/08, 31 316, nr. 6, p. 7 en 8.
[153] Pagina 10 bijlage B.

taak om leiding te geven aan de bestrijding echter geen zelfstandige grondslag voor de verwerking van (bijzondere) persoonsgegevens kan worden afgeleid. Deze dient nader te worden geëxpliceerd. De voorgestelde invoering van artikel 6d Wpg in het wetsvoorstel Tijdelijke wet notificatieapplicatie biedt de mogelijkheid om deze toevoeging alsnog in te voeren en dit probleem op te lossen.

Vanwege de omvang van verschil van inzicht en de bestaande twijfel over dit punt en andere punten is aan de landsadvocaat gevraagd om een juridische analyse uit te voeren (bijlage C). Zij komen tot de conclusie dat de grondslag wel aanwezig is:

Met andere woorden: de artikelen 3, 7 en 6 van de Wpg worden (waar het eventuele bijzondere persoonsgegevens betreft: in combinatie met artikel 9, lid 2, aanhef en onder i, AVG) voldoende specifiek geacht om (in combinatie met artikel 6 lid 1 aanhef en onder e AVG) als grondslag voor de verwerking van (bijzondere) persoonsgegevens voor een notificatieapp te dienen.

Na het advies blijkt ook in het wetgevingsadvies van de Raad van State (bijlage D) dat de grondslag aanwezig is en de wet daarmee niet strikt noodzakelijk is, maar wel wenselijk:

De Afdeling is met de regering van oordeel dat dit op zichzelf mogelijk is. Strikt genomen is een wettelijke basis voor vrijwillig gebruik van de app juridisch niet noodzakelijk.

Omdat het advies van de Autoriteit Persoonsgegevens zwaar wordt gewogen, heeft de minister besloten te wachten tot de tijdelijke wet voor de app door de Tweede en Eerste Kamer is goedgekeurd en van kracht is (na publicatie in de Staatscourant). Voor de lopende testperiode is gekozen voor de grondslag toestemming. Deze grondslag wordt bijvoorbeeld ook in Ierland, Italië, Duitsland, Oostenrijk en het Verenigd Koninkrijk gebruikt.

DPIA en advisering Autoriteit Persoonsgegevens

Omdat CoronaMelder door veel mensen gebruikt gaat worden, is er sprake van een grootschalige verwerking. In dat geval moet er een zogenaamde DPIA of gegevensbeschermingseffectbeoordeling worden uitgevoerd. Daarin doe je onderzoek naar de mogelijke risico's voor de betrokkenen (de mensen over wie de gegevens gaan). Uit de DPIA blijkt dat er geen hoge risico's zijn voorafgaand aan de verwerking.

Omdat de minister heeft toegezegd advies te vragen aan de Autoriteit Persoonsgegevens is dat na het opstellen van de DPIA ook gedaan. Dat komt overheen met de situatie in Ierland, waar eveneens zo'n advies is gevraagd voor de daar ontwikkelde notificatieapp. De Autoriteit Persoonsgegevens heeft echter aangegeven dat zij een dergelijk advies alleen kunnen gegeven als zij het verzoek om advies interpreteren als een voorafgaande raadpleging, zoals staat in artikel 36, eerste lid AGV:

Wanneer uit een gegevensbeschermingseffectbeoordeling krachtens artikel 35 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit.

Omdat hier geen sprake is van een hoog risico ontstond een bijzondere situatie, waarbij de Autoriteit zich geremd ziet regulier advies te geven en het ministerie bij een verschil van inzicht geen verwerkingsverbod wil opgelegd krijgen.

Dat verschil van inzicht kwam er uiteindelijk in de vorm van de hiervoor beschreven discussie over de grondslag van de verwerking. Daarnaast komt de Autoriteit Persoonsgegevens met twee andere zorgen:

1. De rol van Apple en Google. De AP spreekt de vrees uit voor de toekomst dat zij of alsnog gegevens gaan verwerken of een eigen app introduceren.
    a. Deze zorg wordt geadresseerd in de Tijdelijke wet notificatieapplicatie covid-19 op een aantal punten:
        i. De wet voegt artikel 6d toe aan de Wet publieke gezondheid waar onder 3a staat dat gegevens

worden niet langer bewaard dan noodzakelijk is om gebruikers in voorkomende gevallen te kunnen waarschuwen over een mogelijke infectie met het virus en worden vervolgens onmiddellijk vernietigd;

        ii. De wet voegt artikel 6d toe aan de Wet publieke gezondheid waar onder 3c staat dat gegevens

worden niet voor andere doeleinden gebruikt dan de bestrijding van de epidemie van covid-19, veroorzaakt door het virus SARS-CoV-2.

        iii. De wet voegt artikel 6d toe aan de Wet publieke gezondheid waar onder 3c staat:

Het is verboden een ander te verplichten tot het gebruik van de notificatieapplicatie dan wel enig ander vergelijkbaar digitaal middel.

        Dit laatste ontneemt Apple en Google de mogelijkheid om zelf functionaliteit in te bouwen, die voor alle gebruikers worden aangezet.
    b. Gegevens die met een bepaald doel worden verzameld mogen niet voor een ander doel worden ingezet. Dat verbiedt de AVG simpelweg. Ook als er een grondslag is dan kan dat niet. Daarvoor zal de betrokkene opnieuw moeten worden geïnformeerd en opnieuw een grondslag ontstaan. Omdat het hier deels bijzondere persoonsgegevens betreft, biedt de AVG extra waarborgen. De Autoriteit Persoonsgegevens is hiervoor de toezichthouder. Zij hebben bewezen scherp en kritisch te kijken naar de bijdragen van Apple en Google.
2. De wisseling van de Belastingdienst naar het CIBG met daaronder KPN als beheerder van de infrastructuur en KPN Security als bewaker van het netwerk. Daarbij is de belangrijkste aanpassing dat de rollen nadrukkelijker zijn verdeeld, waarbij functiescheiding een belangrijk onderdeel is. Omdat de Autoriteit Persoonsgegevens nadrukkelijk aangeeft dat voor de beveiliging minimaal hetzelfde niveau van beveiliging moet worden geboden en de minister informatiebeveiliging en privacybescherming maximaal wil borgen, volgt de minister de aanbeveling op. Er loopt momenteel een onderzoek naar mogelijke verschillen en het verbeteren van de beveiliging. Dat is nodig, omdat de verschillende organisaties aan verschillende normen voldoen. Als er verschillen zijn dan wordt gekozen om die stap te zetten die de beveiliging het beste dient (altijd het hoogst haalbare kiezen). Deze actie zal dan ook blijven lopen na lancering van CoronaMelder.

Er zijn diverse aanbevelingen gedaan door de Autoriteit Persoonsgegevens die zo goed mogelijk worden opgevolgd, zoals dat ook is gedaan bij alle andere adviezen.

Informatiebeveiliging

Er zijn veel verschillende stappen gezet om de informatiebeveiliging zo goed mogelijk in te regelen. Daarbij zijn er bij CoronaMelder een aantal uitgangspunten:

1. Na privacy is de beveiliging van gegevens het belangrijkste goed. Dat betekent dat waar er keuzes te maken zijn er maximaal wordt gekozen voor de veiligste optie als dat realistisch haalbaar is.
2. Waar het maar kan sluiten we aan bij standaarden. Hierdoor is het beter mogelijk te controleren wat er is gedaan en nog moet gebeuren. Het uitvoeren van testen gebeurt zoveel mogelijk conform standaarden.
3. Er wordt waar mogelijk gewerkt met gelaagde beveiliging. Dat betekent dat als een enkele maatregel niet blijkt te volstaan een tweede of derde maatregel alsnog bescherming kan bieden.
4. CoronaMelder is een open project, waarbij juist de toetsbaarheid in het publieke belang een belangrijke rol verdient. Daarbij hoort geen 'security through obscurity'[154], tenzij dit onvermijdelijk is.
5. Beveiliging is een continu proces van verbetering. We werken daarom volgens: plan, do, check, act[155]. Deze benadering is een hulpmiddel voor het verbeteren van kwaliteit, waarbij de vier activiteiten elkaar continu opvolgen. Dit cyclische karakter waarborgt continue verbetering.
6. Werk met foutmodus. Een transparant traject in combinatie met een plan, do, check, act-cyclus maakt dat fouten zullen optreden, worden bedacht voor ze optreden en daarmee kansen voor verbeteringen geven. Gelegenheden worden aangegrepen om verbeteringen door te voeren.

Beveiligingsmaatregelen

Om risico's te beheersen zijn er veel verschillende maatregelen genomen. Er zijn verschillende manieren hoe een beveiligingsmaatregel tot stand komt binnen het project:

1. Bij het ontwerp.
2. Bij het ontwikkelen van CoronaMelder.
3. Op basis van de adviezen van de begeleidingscommissie.
4. Bij het doen van risicoinschattingen.
5. Bij het beschikbaar komen van beveiligingsonderzoeken.
6. Na meldingen in het kader van bijvoorbeeld responsible disclosure.

Om risico's te bestrijden zijn er vier verschillende soorten maatregelen beschikbaar:

1. preventie ofwel zorgen dat de kans kleiner wordt dat een incident optreedt;
2. detectie om te zorgen dat een incident wordt ontdekt;
3. repressie om de gevolgen van een incident zo klein mogelijk te houden en daardoor het risico te verkleinen;

---

[154] Security through obscurity is een omstreden beginsel uit de beveiliging dat beoogt beveiligingsrisico's te beperken door beveiligingsmaatregelen en/of de werking van maatregelen geheim te houden. De gedachte is dat derden het mechanisme zonder kennis kunnen doorbreken. Al in 1883 heeft de Nederlandse cryptograaf Auguste kerckhoffs dit mechanisme bekriticeerd in La Cryptographie Militaire (https://petitcolas.net/kerckhoffs/index.html). Hij betoogt dat er geen probleem mag ontstaan als de werking van het systeem bekend is en dat de beveiliging daartegen robuust moet zijn. Meer op IT toegespitst zegt de gerenommeerde Amerikaanse cyptograaf Bruce Schneier dat bij herhaling, zoals in de 'The Insecurity of Secret IT systems' - https://www.schneier.com/blog/archives/2014/02/the_insecurity_2.html

[155] Plan – Het maken van een doel en aanpak voor verbeterringen, Do – Voer de verbeteringen gecontroleerd uit, Check – Controleer het resultaat, vergelijk met de uitgangspositie en de doelstellingen, Act – Stel bij wat uit de resultaten van de check blijkt

4. correctie om na een incident weer snel terug te kunnen naar een volledig normale situatie met verbeteringen waar mogelijk.

De maatregelen zijn:

Onder-deel	Maatregel	Omschrijving	Pre-ven-tief	De-tec-tief	Re-pres sief	Cor-rec-tief
Ontwik-keling	Decentrale structuur	Door niet te werken met een centrale structuur is er niet een centrale database is er niet een centrale administratie van contactmomenten van personen. Hierdoor ontstaat niet het risico van een jackpot waar alle gegevens kunnen worden opgehaald.	X			
Ontwik-keling	Pseudo-nimisering	Doordat er gewerkt wordt met zeer sterk gepseudonimiseerde gegevens is bij ongeautoriseerde toegang nog geen inzicht in de betrokken personen	X		X	
Ontwik-keling	OTAP	Er wordt gebruikt gemaakt van verschillende systemen: ontwikkel, test, acceptatie en productie. Hierdoor doorloopt nieuwe software meerdere fases voordat de programmatuur publiek beschikbaar komt. Dit verkleint de kans dat ernstige fouten worden verspreid.	X	X		
Ontwik-keling	Dubbel gebouwde server	Omdat er risico's kleefden aan het bouwen van de server en de migratie van de Belastingdienst naar de huidige omgeving is er een los ontwikkeltraject gestart met een tweede serversoftware. Hierdoor zou er altijd een werkende oplossing zijn.	X			
Ontwik-keling	Dubbele infra/no-state	Het backend is dubbel uitgevoerd -en- de hoeveelheid 'state' tussen de twee backends is nagenoeg nihil. Beide backends kunnen geheel independent draaien; inherente avoidance van `split brain' risk in ontwerp.	X			
Ontwik-keling	Zero Trust Principle	Door te werken volgens het zero trust principle zijn er veel scheidingen aangebracht tussen de API en de App, tussen de backend server en de GGD'en, tussen beheerders.	X			
Ontwik-keling	Zero Trust Principle	Veel van deze scheidingen zijn op een 'need to know' basis; dus informatie die in de volgende laag niet nodig is (e.g. IP address) wordt niet doorgegeven.	X			
Ontwik-keling	Sonarcube	Inzet van een tool om fouten te vinden, onderliggende problemen inzichtelijk te krijgen en beveiligingszwakheden te vinden.	X	X		X
Ontwik-keling	Quality assurance team	Er is een quality assurance team dat handmatig testen uitvoert op de werking van software.	X	X		X
Ontwik-keling	Interne code reviews	Interne mensen reviewen de broncode van collega's	X	X		X
Ontwik-keling	Open-sourcesoft ware	De broncode is vrijgegeven als open-sourcesoftware. Dankzij de inzet van een community manager is er een gemeenschap van kritisch meekijkende experts, die aanvullende feedback geven.	X	X		X

Ontwik-keling	Coor-dinated Vulnera-bility Disclosure	Derden die los beveiligingsproblemen vinden kunnen die melden onder het coordinated vulnerability disclosure programma.		X		x
Ontwik-keling	Code reviews	Het uitvoeren van broncode reviews door een onafhankelijke partij. Daarbij wordt niet alleen naar risico's gekeken, maar ook gezocht naar achterdeuren in de software.		X		X
Ontwik-keling	Escrow/Pro venance	Er is een koppeling tussen de vrijgegeven broncode, de door onafhankelijke partijen gereviewde broncode en de broncode die gebruikt is om het productie systeem te bouwen c.q. naar de app-stores up te loaden. Deze koppeling wordt middels een escrow verificatie en een notaris verklaring geborgd.	X	X		
Ontwik-keling	Pentetratiet esten	Het uitvoeren van uitgebreide penetratietesten op de software van het hele stelsel door een onafhankelijke partij.		X		X
Ontwik-keling	Inkoopbelei d beveiliging sonderzoek en	Bij het inkopen van beveiligingsonderzoeken worden inkoopeisen gesteld: 1. Rapportages zijn reproduceerbaar - Dit maakt verificatie door derden mogelijk. 2. Rapportages worden geopenbaard - Dit geeft een druk om kwalitatief goede producten te leveren, omdat deze onderdeel wordt van het publieke debat. 3. Bij penetratietesten wordt niet alleen aangegeven welke bevindingen er zijn, maar ook welke testen zijn uitgevoerd. Hierdoor is duidelijk wat er getest iis 4. Vanaf livegang wordt bij bevindingen wordt een CVSS-score meegegeven en niet op basis van een waardeoordeel gewerkt 5. Penetratietesten vinden plaats op basis van standaarden, waardoor er consistentie is wat het minimale beschermingsniveau gaat zijn. Het is niet langer maar willekeurig testen.	X	X		
In-richting	Functiesch eiding	Door functies te scheiden is informatie niet voor iedereen beschikbaar en is het lastiger aan gegevens te komen of deze te misbruiken. Alleen de minimale gegevens komen beschikbaar. Deze scheiding zien we op verschillende punten: - Beheer van infrastructuur (KPN) is gescheiden van het beheer van de applicatie (CIBG) - Ontwikkeling (VWS) en beheer (CIBG/KPN) - Ontvangen sleutels (VWS) vrijgeven sleutels (GGD) - API-verkeer voor GGD'en en CDN-verkeer - Server voor aanleveren sleutels, server voor beschikbaar stellen van geverifieerde sleutels - Certificaten uit HSM worden beheerd door aparte partij (Justid) - Bewaking van systemen op verstoringen () is gescheiden van de bewaking (SOC) - Beveiligingsonderzoeken zijn gescheiden op: 1. Broncode van de app (Secura) 2. Broncode van de backend (Radically Open Security) 3. Penetratietest (hackerstest) 4. Procedurele onderzoeken	X			

		Forensisch onderzoek bij eventuele incidenten wordt onafhankelijk onderzoek gedaan				
In-richting	Hardening	Alle systemen die worden ingezet wordt gehardend op basis van best practices om de kans op een succesvolle aanval te verkleinen. Hieronder vallen ook het gebruik van veel verschillende standaarden.	X			
In-richting	DDOS-beschermin g	Door DDoS-beschermende technologie in te zetten, wordt tijdens een aanval downtime voorkomen of verminderd.			X	
In-richting	Redundanti e	Er worden dubbele servers gebruikt in verschillende datacentra, waardoor bij verstoring er kan worden overgeschakeld naar het andere datacenter. Bij grote drukte kan de verwerking over meerdere machines worden verdeeld	X		X	
In-richting	Ontkoppeli ng	Alle systeemlagen zijn ontkoppeld en kunnen onafhankelijk van elkaar reageren. Hierdoor vermindert het risico op een cascade fout.				
In-richting	Stateless	Alle gedupliceerde systemen zijn in hoge mate stateless/horziontal ontkoppeld. Zodat zij bij het valen van het partner systeem zonder ruggespraak kunnen fuctioneren.				
In-richting	Datacentra in EER	Door datacentra te plaatsen in de Europese Economische Ruimte (in dit geval Nederland) kunnen vreemde mogendheden op basis van wetgeving geen toegang krijgen.	X			
In-richting	Service Level Agreement s	Het maken van afspraken over beschikbaarheid om daarmee verstoringen tot een minimum terug te brengen.			X	
In-richting	Wetgeving met betrekking tot misbruik	Er is een verbod om gegevens voor een ander doel te gebruiken dan de kernfunctionaliteit van CoronaMelder (kort samengevat)	X		X	
In-richting	Licentieafs praken	Met Apple en Google zijn via de licentie afspraken gemaakt, waarin ander gebruik dan bestrijding COVID-19 is verboden	X		X	
In-richting	Dubbele handtekeni ngen	Om afhankelijkheid van externe partijen met de cryptografie tot een minimum te beperken zijn er eigen certificaten ingezet om downloadbare sleutels (DK's) te tekenen en ook handtekeningen bij de app toe te voegen. Dat geeft op twee punten een voordeel: het is mogelijk te werken met een CDN waar de cryptografie voor integriteit en authenticiteit niet meer relevant is (deze maatregel ondervangt dat immers). Daarnaast maakt dit het ministerie minder afhankelijk van de cryptografie van Apple en Google.	X	X	X	
In-richting	Hardware Security Modules	Voor het hebben van zowel de eigen certificaten als de 'unmanaged' naakte sleutels van apple/google wordt gebruik gemaakt van een hardware security module. Hierin worden certificaten geboren en verlaten de machine niet. Dit is omkleed met veel verschillende procedures om de integriteit te borgen. Daarnaast is het beheer van deze machine bij een andere partij belegd wat extra functiescheiding geeft.	X			

Operatie	Helpdesk voor gebruikers	Door een helpdesk in te richten, kunnen mensen advies krijgen over veilig gebruik en melding doen van misstanden (bijvoorbeeld druk om de app te installerren).		X	X	
Operatie	SOC	Het inrichten van een Security Operations Center. Hier worden de systemen van de servers bewaakt en het netwerkverkeer gemonitord op aanvallen. Wanneer een dreiging zich materialiseert vindt er detectie plaats en wordt er afhankelijk van de situatie ingegrepen.		X	X	
Operatie	Systeem monitoring	Er wordt detectie op systemen gedaan om verstoringen en problemen in een vroeg stadium te detecteren. Hierdoor wordt uitval voorkomen. Bij een storing of dreigende storing wordt actief ondernomen.		X	X	
Operatie	Incidentepr ocedure	Bovenop de losse procedure rond een datalek of beveiligingsincident wordt een overzicht bijgehouden, die binnen de security en privacy operations dient om lopende zaken te bewaken en te dienen als basis van evaluatie (actieve PDCA-cycle).			X	x
Operatie	CSPO	Chief Security en Privacy Operations – informatiebeveiliging en privacybescherming hebben veel raakvlakken, waarbij tijdens incidenten of bij het voorkomen ervan veel te combineren is. Door naast de security officer en de privacy officer een verbindende persoon te hebben, die juist voor lopende zaken een rol speelt worden beide wereld goed verbonden.	X	X	X	X
Beleid	IB&P First	Privacy en security staan in het beleid op de eerste plaats. Dat betekent dat er bij keuzes wordt gekozen voor primair een zo privacyvriendelijk mogelijke oplossing en daarna een zo veilig mogelijke oplossing.Bij strijdigheid volgen er privacybeschermende maatregelen als vanuit security echt iets noodzakelijk is.	X			
Operatie	Bewaking app stores	Door actief de verschillende appstores in de gaten te houden en te handhaven op verschijnen van CoronaMelder kunnen malafide applicaties worden verwijderd.		X	X	X
Operatie	Bewaking domeinnamen	Door actief domeinnamen lijkend op coronamelder(.nl) in de gaten te houden en te handhaven op het verschijnen van malafide domeinnamen kunnen deze worden verwijderd.		x	x	x
Operatie	Bewaking social media	Door social media in de gaten te houden kunnen signalen van gebruikers, bijvoorbeeld over malafide apps, sms-en of domeinnamen, worden gebruikt om waar nodig in te grijpen bij een phishing-actie.		x	x	x
Operatie	Logging	Handelingen van gebruikers en beheerders (aan de kant van de backend) worden in logbestanden geregistreerd, zodat deze periodiek (of in een geval van een melding/incident) kunnen worden geraadpleegd om vast te stellen dat de integriteit van de data niet gecompromitteerd is.		x		
Ontwikkeling	Decoy-verkeer	Door regelmatig decoy-verkeer te sturen tussen een telefoon en de backend is op basis van verkeer met de backend-server niet te achterhalen dat een gebruiker besmet is/sleutels upload.	x			

Ontwik-keling	IP-stripping	Binnenkomend verkeer (geuploade sleutels) wordt bij binnenkomst direct gescheiden door een proxy om te zorgen dat geuploade sleutels zo beperkt mogelijk te herleiden zijn tot een persoon (bijvoorbeeld via ipadres). Op het centrale systeem dat deze data verwerkt zijn deze IP addressen niet zichtbaar/beschikbaar. (Dus ook niet voor de systeem beheerders - dit is een ander team met ander lijn management).	x			
Ontwik-keling	Sorteren van sleutels	De op de CDN gepubliceerde lijst met sleutels wordt gesorteerd zodanig dat op basis van de volgorde niet is af te leiden welke sleutels bij dezelfde persoon horen.	x			
Inricht-ing	Toegangsb eveiliging KPN	Ter voorkoming van manipulatie aan de backend				
In-richting	Toegangsb eveiliging GGD	Ter voorkoming van manipulatie aan de backend/sleutelgeneratie. Identity-hub				
Ontwik-keling	PBKDF	Gebruiken van effectief een PBKDF om de 6 cijfer/letter code te verlengen via een HMAC				
Ontwik-keling	Naam-geving	In de naamgeving van de sleutels om te downloaden is dat versleutelde naam aanwezig om de kans op misbruik te verkleinen (in combinatie met ondertekening).	X	X	X	
In-richting	Aparte portal GGD'en	Om de kans op misbruik te verkleinen draait het portal dat de GGD'en gebruiken voor het goedkeuren van sleutels los van de andere systemen. De verbinding via een API is zeer restrictief in de mogelijkheden die de GGD'en hebben. Hierdoor kunnen er geen andere taken worden gedaan.	X			
In-richting	API systeem gescheiden van het distibutie-systeem	Er is een scheiding tussen de APi voor het backend systeem en het daadwerkelijke distributiesysteem. Hierdoor is bij een aanval op het distributiesysteem niet meteen de backend in direct gevaar .	X			
In-richting	Geen authenti-catie bij upload	Om herleidbaarheid te voorkomen is er geen authenticatie bij de upload.	X			
Ontwik-keling	Kerckhoff's principe	Strikt volgen van Kerckhoffs's principle - je kan een interoperable app bouwen zonder enig geheim/toestemming/controle van 'ons'.	X			
In-richting	Geen authenticati e bij download sleutels (CDN)	Geen enkele form van authenticatie op het CDN om herleidbaarheid naar gebruikers van CoronaMelder te voorkomen.	X			
In-richting	Pinning op PKI root	Er is certificate pinning op PKI root, waardoor bijvoorbeeld social engineering moeilijker wordt.	X	X		
In-richting	Verificatie issuer	Verificatie issuer laag genoeg in de tree om de scope van wat daarbinnen uitgegeven is dusdanig te beperken dat ook social engineering moeilijk wordt.		X		

In-richting	IP-stripping	IP stripping in het CDN, IP stripping in de firewall (API) buiten/door KPN team dat los staat van backend team.	X			
Ontwik-keling	Data minimalisatie	Er wordt met zo min mogelijk gegevens gewerkt. Het gevolg is dat bij een incident minder te halen is. Door de versleuteling en de moeizame herleidbaarheid tot de persoon is het minder aantrekkelijk als aanvalsplatform (je kunt er niet veel mee)	X		X	
Ontwik-keling	Korte retentieperiode	De data wordt zo kort mogelijk bewaard op de backend. Na upload moet bevestiging binnen 24 uur plaatsvinden en op het CDN is de data 14 dagen beschikbaar. Hierdoor is een mogelijke buit, zo die er al is, beperkt.	X		X	
Ontwik-keling	Native implementaties	Door specifiek te schrijven voor het platform, waarop de app moet functioneren, verklein je de attack surface.	X			
Ontwik-keling	Dummy download sleutels	Bij kleine volumes tests - 'stuffen' van de sleutels indien batches (erg) klein zijn met random sleutels (en daarna het sorteren TEKs om ze te ontkoppelen van de submission batches).	X			
Ontwik-keling	Geen root detectie	Bewust niet implementeren root-detectie en andere (account) validatie om zowel attacksurface te verminderen -en- fingerprint klein te houden.	X			
In-richting	Geen gebruik cookies	Er worrden geen cookies gebruikt op de website coronamelder.nl	X			

Betrokken partijen

Om een completer beeld te geven van de betrokken partijen bij het project vanuit de blik van informatiebeveiliging en privacybescherming:

Onderdeel	Betrokken partij	Rol
Software-ontwikkeling	Ministerie van VWS	Ontwikkelaar CoronaMelder.
	Apple	Maker API.
	Google	Maker API.
Beheer	Ministerie van VWS	Doorontwikkeling en regie.
	CIBG	Applicatiebeheer.
	KPN (via CIBG)	Beheer network.
		Leveren hosting.
	Justid	Beheer HSM (certificaten servers).
Beveiliging	eHealth network	Afstemming verbeteringen aan protocollen en API.
		Uitwisseling ervaringen.
	KPN Security via CIBG	Bewaking op aanvallen en eerste response.
	CIBG	Bewaking serversystemen op

		beschikbaarheid en performance.
	Logius	Bewaken van applicatie-winkels op internet op illegale of gemodificeerde CoronaMelder-apps.
	Apple/Google als app-winkel	Uitvoeren verificatieslagen[156] op privacy en security alvorens CoronaMelder toe te laten.
	Apple/Google als maker API-software	Het bieden van een beveiligingslaag tegen misbruik vanuit CoronaMelder.
Beveiligingsonderzoek	NFIR	Uitvoeren van een penetratietest (hackerstest) op de serveromgeving, de app en de combinatie.
	Europese Commissie	Onderzoek naar broncode Apple/Google API uitgevoerd door Radically Open Security.
	Noordbeek B.V.	Onderzoek onder leiding van professor Ronald Paans naar toepassen van afspraken voor backend, fysieke installaties
	Secura	Onderzoek naar de broncode van CoronaMelder app voor zowel iOS als Android.
	Radically Open Security	Onderzoek naar de broncode van de server-software van CoronaMelder.
	Ministerie van VWS	Het uitzetten van aanvullende en herhaalde verificatieslagen en beveiligingsonderzoeken.
Privacy(recht)	Autoriteit Persoonsgegevens	Geven van advies op de DPIA
	Pels Rijcken & Droogleever Fortuijn	Uitvoeren van een juridische analyse op het

[156] Voordat een app in de store wordt toegelaten, worden er verificatieslagen uitgevoerd door Apple en Google. Daarbij wordt gekeken naar de aanwezigheid van privacy-beleid, het beleggen van verantwoordelijkheden en het overeenkomen van de werking met rechten die worden geclaimd.

		advies van de landsadvocaat
	Raad van State	Advisering op het wetsvoorstel
	Privacy Management Partners	Advies op DPIA en advies AP

Onderzoeken

Er is door het ministerie breed ingezet op het waarborgen van de kwaliteit en het doen van intensief onderzoek en interne verificatieslagen. Intern wordt een aantal stappen gezet om de kwaliteit en beveiliging van de totale oplossing (app plus backend) te toetsen:

1. Uitgebreide pentest door pentesters in dienst van de overheid.
2. Uitgebreide codereview door overheidsreviewers.
3. Intensieve verificatie van configuratie en hardening

Daarnaast is ingezet op externe verificatie. Op weg naar de livegang wordt er een brede inventarisatie gedaan op het gebied van informatiebeveiliging en privacybescherming. De verslaglegging wordt – passend bij het project – zo maximaal mogelijk openbaar.

Hiervoor worden de volgende maatregelen genomen en onderzoeken gedaan:

1. Het opdelen van de verificatie in veel verschillende percelen, die ieder door een ander bedrijf worden afgetest:
    a. Hierdoor vindt er een druk tussen de bedrijven plaats, omdat er een dreiging is dat bevindingen over het hoofd worden gezien. Verschillende bedrijven hebben andere blikken, wat de kans op het maximaal vinden van aandachtspunten vergroot.
    b. Meerdere onafhankelijke partijen maken beïnvloeding lastiger, waardoor onafhankelijkheid maximaal is geborgd.
    c. Het voorkomt dat een partij ‘als vriend van xxx’ een rol krijgt en daarmee een vriendendienst regelt.
    d. Alles wat relatief goed af te testen is, wordt ook daadwerkelijk afgetest.
    e. Het selecteren van Europese bedrijven met een goede reputatie op het deelgebied waarvoor zij zijn gevraagd offerte uit te brengen.
    f. Het werken met verschillende percelen voor het uitvoeren van de beveiligingsonderzoeken:
        1. Uitgebreide penetratietest op de app plus de backend. Gericht op het vinden van fouten.
        2. Handmatige codereview van de app gericht op kwaliteit en het waarborgen dat er geen verborgen functionaliteit is of juist functionaliteit ontbreekt.
        3. Handmatige codereview op de backend gericht op kwaliteit en het waarborgen dat er geen ongedocumenteerde functionaliteit is of juist functionaliteit achterwege wordt gelaten.
        4. Review van de privacy-features van de app en de backend, beoordeling van de DPIA.
        5. Uitvoeren van een analyse op het voldoen aan de BIO door het CIBG.
        6. Vergaren van externe analyses en certificeringen m.b.t. het KPN platform.
        7. Verificatie van de instellingen in de backend conform de afspraken.

8. Het laten opstellen van een overall review over de onderzoeken om extra waarborgen te creëren dat de beveiliging en privacybescherming maximaal zijn geborgd.
9. Een procedurele toelichting over het doorlopen proces.
10. Het gebruik van de open-source community voor feedback.
11. Het starten van een bugbounty om doorlopend te blijven zoeken naar verbetermogelijkheden – deze wordt in de volgende fase na livegang gestart.
12. Het organiseren van een verified built, wat betekent dat een notaris toeziet dat de openbaar gemaakte broncode van de app daadwerkelijk wordt omgezet naar programmatuur en wordt gepubliceerd in de Apple en Google appstore. Van deze actie wordt een verslag gemaakt. U treft deze aan als bijlage L en M.

Bevindingen uit beveiligingsonderzoeken

Uit de beveiligingsonderzoeken komen bevindingen voort. Deze bevindingen zijn door beheerders, netwerkexperts en ontwikkelaars in de meeste gevallen verholpen. In een aantal gevallen is door de gekozen techniek een bevinding niet te verhelpen. Zoiets speelt bijvoorbeeld dat de werking van de app kan worden achterhaald. Juist omdat – mede op verzoek van de Tweede Kamer – open source is. Hierdoor is de werking al bekend en is juist de peerreview de beveiligingsmaatregelen. Daarmee wordt gehandeld conform het uitgangspunt: geen security through obscurity. In een aantal gevallen werd een beperking van technologie voorzien en is de bevinding vooraf reeds ondervangen door een of meerdere maatregelen. Dat maakt zo'n bevinding niet minder terecht, maar juist niet problematisch.

Een bevinding betreft bespreking en dat is de bevinding van Radically Open Security (NLC-019). Voor het aanmelden van medewerkers van de GGD maakt de GHOR gebruik van The Identity Hub als leveranciers om medewerkers te laten aanmelden. Voor de onderzoeker is uit de broncode van de software niet af te leiden welk afspraken kader met de leverancier gemaakt zijn. Omdat ze dat niet weten en toch willen waarschuwen ze hiervoor. Omdat het hacken van een toegangscontrole ernstige gevolgen zou kunnen hebben is dit gemarkeerd als 'hoog'. Het betreft geen technische tekortkoming. De onderzoekers schrijven zelf ook:

> *Using third party authentication components can be a valid choice, but from a code review perspective it adds another attack path, so we included it as a finding.*

Wat hier benoemd is, betreft een risico. Uit de FMEA-inschatting blijkt dat we vooralsnog dit als laag inschatten. Het beschreven alternatief (de GHOR zelf authenticatie laten regelen) leidt niet automatisch tot een lager risico. Dat neemt niet weg dat VWS dit onder de aandacht van de GHOR heeft gebracht. In het vervolgtraject zal hier nader naar worden gekeken.

Lijst met bevindingen

De lijst met bevindingen is bijgevoegd en leidt tot de slotsom dat er geen bevindingen zijn, die de lancering van CoronaMelder in de weg staan. Voor de omvang van het project zijn de bevindingen aan de lage kant.

ID	Organisatie	Titel	Omschrijving	CVSS-score	Status	Uitleg
RN1	Secura	Decoy messages not disabled when Exposure notification is disabled.	The decoy upload scheduler does not seem to take the disabled status of the application in to account. While this is not a security vulnerability, it might be not intuitive for users of the application.	3.7	wordt verholpen	
RN2	Secura	Outdated library used in iOS application: OpenSSL	CoronaMelder, Android and iOS application	0.0	Opgelost	
RN3	Secura	The subject name in the certificate used for TEK signing is not checked.	When validating the second signature (using the certificate based CMS/PKCS# format) on a TEK list received by the server, the root and issuing CA certificates within the chain are checked. The subject name in the leaf certificate is not validated.	1.9	wordt verholpen	Deze wordt verholpen, zodra de HSM's operationeel zijn
NLC-019	ROS	Identity Hub	The solution uses The Identity Hub (https:// theidentityhub.com) as its OAuth provider to allow users access to the healthcare API.	0.0	Gesloten	Was gemarkeerd 'hoog'. Het is geen bevinding, maar een beschreven risico. Volgens FMEA zou deze scoren: ernst: 4 (slechte pers, datalek van omvang) voorkomen: 1 (identity hub is geen onbekende partij) detecteerbaarheid: 3. RPN: 12 (klein), kritieke score: 4 (klein). Deze authenticatiemethode is aangschaft door de GGD/GHOR en is een professioneel bedrijf dat deze dienstverlening levert. De onderzoekers

						hebben louter gekeken naar de verwijzen. Er is niet gekeken naar het afsprakenkader, er is niet gekeken naar de implementatie of ander beveiligingsonderzoek gedaan. Er is contact geweest met de GHOR om deze bevinding onder de aandacht te brengen. De keuze van het uitbesteden van deze dienst wordt echter niet direct als beveiligingsrisico gezien gelet op afsprakenkader en de professionaliteit van de dienstverlener. Het in eigen beheer uitvoeren van authenticatie zou niet automatisch de kwaliteit verhogen ten opzicht van een bedrijf dat hierin is gespecialiseerd. Wel is de aanbeveling aanleiding hier in het beheersstadium samen met de GHOR nog wel onderzoek te naar laten doen.

NLC-013	ROS	API-feedback	HealthAuthorityEmployeesCanCheckIfKeysWere Uploaded		wordt verholpen in kader livegang	Deze functionaliteit was voor testen, maar wordt verwijderd voor definitieve versie.
NLC-002	ROS	Developer Options To Switch Off Security Features	DevelopmentOnlySettings.cs contains options to switch off security features such as the back-end's user authentication and use of HTTPS. The default is to have these security features switched on, which is good. As long as the option to switch off significant parts of the security features is present, however, these features might conceivably be turned off accidentally.		Opgelost	
NLC-004	ROS	RollingPeriod Not Limited To One Day	The RollingPeriod of uploaded keys is not properly checked. Uploaded keys can continue into the following days.		Opgelost	
NLC-005	ROS	It Is Possible to Update Diagnosis Keys With Future Dates	MobileAppApi does not check if an uploaded TEK is associated with a future date.		Opgelost	
NLC-007	ROS	Decoy Traffic Is Not Efficient	The decoy traffic analysis is not in line with the design and does not seem to be able to successfully mimic real traffic.		wordt verholpen	
NLC-014	ROS	Authorization Token Included in GET Parameter	The JWT for authentication against the health authority back-end is part of a GET parameter.		Opgelost	
NLC-017	ROS	Databases have Insufficient Privileges Separation	Even though the databases are accessed by different programs with different needs, there is limited privilege separation.		Opgelost	
NLC-018	ROS	Signing Components Imply Running as Local Administrator	Some components imply they need to run as local administrator. If they do, their compromise would occur in the context of the administrator role instead of in that of an isolated process.		Opgelost	
NLC-020	ROS	Health Worker Authentication Token Is Valid For Several Hours and Not Rate-Limited	The JWT used for authentication is valid for several hours. There is no rate limiting nor any way to revoke individual authentications.		Opgelost	
NLC-022	ROS	HSTS Header Not Set	A HTTP Strict-Transport-Security response header (HSTS) is		Onderva ngen	A discussion with the

			recommended for all APIs that only use SSL, in order to prevent adversaries from using SSL stripping attacks in a MitM scenario.		door maatregel	developers revealed that HTTPS is terminated at the load balancer. This could mean this finding is invalid; we cannot confirm this in a code-only review. We do not recommend terminating HTTPS here, to prevent information being available in plain text on the infrastructure network.
NLC-028	ROS	Timing Oracle in Signature Comparison	The signature validation used during diagnosis key upload contains a timing oracle.		Gesloten	Ofschoon dit in de database waar is, zou het aanpassen leiden tot het introduceren van nieuwe kwetsbaarheden. Zoals de ontdekker terecht aangeeft, is dit niet bewezen en een theoretische mogelijkheid met lage kans van slagen. Het introduceren van nieuwe problemen weegt niet op tegen het issue dat wordt verholpen
NLC-029	ROS	AuthorizationCode is weak	The authentication against the health authority back-end contains a weak single-use component.		wordt verholpen	
NLC-001	ROS	Deviation Between (API) Design and Implementation	The architecture and design deviates from the implementation. Inconsistent documentation can be a source of errors and confusion.		wordt verholpen	
NLC-003	ROS	Database Credentials in Components	Connection strings containing database credentials are included in the appsettings.json of		Opgelost	

		That Do Not Require Them	components/servers that do not require them.			
NLC-008	ROS	Database Stores Upload and Phone Call Times Etc.	The database stores time values relating to diagnosis keys. In combination with other information, this can aid de-anonymization efforts.		Opgelost	
NLC-009	ROS	Log Messages Store Sensitive Information	The log messages store information which, together with log timestamps, can aid de-anonymization efforts.		Opgelost	
NLC-010	ROS	API Exceptions Are Too Verbose	Developer exception page function is activated in production.		Opgelost	Deze bevinding betreft 'Security through Obscurity'
NLC-012	ROS	JWT Token Not Properly Validated	Any valid JWT token is accepted as valid regardless of its properties. As this token needs to match the one stored in the database, this does not currently result in an issue. It could however result in confusion or issues in future updates.		Opgelost	
NLC-015	ROS	Database Provision Default Setting Is To Generate Example Content	The default configuration is to add example keys to the database.		Opgelost	
NLC-016	ROS	Decoy Keys Can Largely Be Distinguished From Real Diagnosis Keys	The decoy keys added to increase anonymity can mostly be distinguished from real diagnosis keys by their properties.		Opgelost	
NLC-021	ROS	IccBackend API Allows CORS Requests From Any Source	The Cross-Origin Resource Sharing (CORS) policy facilitates Cross-Site Request Forgery (CSRF) attacks		Opgelost	
NLC-023	ROS	JWT Token Needlessly Contains Employee Information	JWT Token Needlessly Contains Employee Information		Opgelost	
NLC-025	ROS	Old Diagnosis Keys Are Not Deleted	Uploaded diagnosis keys are not deleted, only marked as published.		Opgelost	
NLC-026	ROS	Diagnosis Key Publishing Time Can Reveal the Time of the Phone Call	There is no intentional delay between the time of uploading and the time of publishing for diagnosis keys.		Gesloten	Deze bevinding is correct alleen betekent het maken van een aanpassing extra vertraging. Omdat niet bekend is of de

						zieke direct een upload doet, het ook niet bekend is in welke regio het gesprek heeft plaats gevonden en iemand toegang moet hebben tot het betreffende GGD-systeem is de waarschijnlijkheid uiterst klein. Wat vervolgens bekend zou kunnen worden is dat er sleutels zijn geupload niet welke sleutels dat betreft.
NLC-027	ROS	Database Can Retain Data after Deletion	The Microsoft SQL database used in the background can retain data for longer than strictly required.		Gesloten	De onderzoeker stelt vast dat het mogelijk zou zijn dat data te lang in de database kan staan. De technische review van de broncode onthult niet procedurele maatregelen en andere technische maatregelen. In de praktijk wordt de database geschoond en vindt er ook verificatie plaats.
NFIR 01	NFIR	HTTP Security Headers – Meerdere headers	Voor de hosts zijn geen of niet alle HTTP Security headers ingesteld. Door het instellen van deze headers kunnen webbrowsers diverse kwetsbaarheden voorkomen. De volgende headers zijn gecontroleerd: • HTTP Strict Transport Security (HSTS): Header die het gebruik van HTTPS forceert. • X-Frame-Options: Geeft een	7.5	Opgelost	

			melding aan de browser of de site in een frame geladen mag worden of niet. Met deze header kunnen clickjacking aanvallen voorkomen worden, aangezien de site niet in een frame geladen kan worden. Als een aanvaller de site wel in een frame zou kunnen laden, kan de aanvaller de gebruiker onbedoeld omleiden naar een malafide website. • X-Content-Type-Options: Voorkomt dat een MIME-sniffing-aanval kan worden uitgevoerd, waarmee een aanvaller een bestand kan verbergen als een ander bestandstype. Hierdoor kan een malafide bestand bijvoorbeeld worden geüpload met een jpg-extensie. Doordat het bestand de kenmerken heeft van een legitiem, uitvoerbaar bestand, wordt de applicatie in sommige gevallen opgeslagen en uitgevoerd. • Content-Security-Policy: Header die een site beschermt tegen Cross-site scripting (XSS) aanvallen. Door het definiëren van een lijst met toegestane content, kan je voorkomen dat de browser kwaadwillende code kan laden van een externe bron. Met de kwaadwillende code kunnen bijvoorbeeld cookies van gebruikers worden afgevangen en gebruikt om mee in te loggen, of om malware te injecteren in de website. • Referrer-Policy: Header die controleert welke informatie door een site opgehaald mag worden van een andere bron. • Feature-Policy: Header waarmee controle is over welke functies en API's gebruikt kunnen worden in de browser. Er is vastgesteld dat bij bovengenoemde hosts een of meerdere van deze zes security headers niet zijn ingesteld.			
NFIR 02	NFIR	TLS v1.0 en v1.1 protocol ondersteuning (WSTG-CRYP-01)	De host ondersteunt de onveilige TLS-versies 1.0 of 1.1. Deze protocollen zijn sinds maart 2020 end-of-life en worden daarom niet meer ondersteund door de meest gebruikte browsers. Het CDN-endpoint (https://productie.coronamelder-dist.nl/) wordt volgens de publieke	6.7	Ondervangen door maatregel	Bij het ontwerp werd al voorzien dat een content delivery network een dergelijk bevinding zou triggeren.

			documentatie1 door de CoronaMelder-applicatie voor iOS en Android gebruikt om publiek beschikbare informatie op te halen, waaronder bijvoorbeeld Diagnosis Keys (DKs), die apart voorzien zijn van een digitale handtekening.			Daarom worden DK's voorzien van een onderteke-ning met een PKI Overheids-cerrtificaat. De dreiging van integriteit en authenticiteit is daarmee ondervangen. Voor ver-trouwelijkheid speelt geen probleem, omdat de DK's naar hun aard Openbaar zijn. Juist het verdelen van deze sleutels is een kern-functionaliteit van de app.
NFIR 03	NFIR	JWT Token blijft tot 3 uur geldig na uitloggen	De JWT token van een gebruiker blijft geldig voor een periode van 3 uur, vanaf het moment dat er uitgelogd is van de applicatie via de uitlogfunctionaliteit. Hierdoor kan er gedurende deze 3 uur opnieuw van deze JWT-token gebruik worden gemaakt om toegang te verkrijgen tot de applicatie	6.6	Opgelost	
NFIR 04	NFIR	Denial of Service - Secure Client-Initiated Renegotiation	Secure Client-Initiated Renegotiation maakt het mogelijk om op een veilige manier te onderhandelen tussen de client en de host tijdens SSL-connecties. Een aanvaller kan honderden van deze onderhandelingen starten, en zo de host onbereikbaar maken door middel van een Denial of Service (DoS).	6.1	Opgelost	
NFIR 05	NFIR	Kwetsbare ciphers waargenomen	De host stelt kwetsbare ciphers beschikbaar, welke mogelijk kwetsbaar zijn voor een kwetsbaarheid genaamd BEAST – deze kwetsbaarheid draagt het CVE-nummer CVE-2011-3389.	5.2	Onderva ngen door maatrege l	Dit is al in de ontwerpfase als potentiële dreiging onderkend. Door aanvul-lende onder-tekening te bieden, wordt dit probleem ondervangen. Het inzetten

						van HSM's biedt hier de oplossing om dit probleem volledig te mitigeren en een hoger niveau van beveiliging te bieden dan een dienstverlener had geboden.
NFIR 06	NFIR	Niet-versleutelde HTTP-verbinding	De webserver ondersteunt HTTP. Hierdoor wordt data over een niet-versleutelde verbinding naar de webserver gestuurd.	4.8	Opgelost	
NFIR 07	NFIR	Testomgeving vindbaar via Google	De testomgeving van het meldportaal is beschikbaar via internet. Daarnaast is deze testomgeving geïndexeerd door Google.	4.8	Opgelost	
NFIR 08	NFIR	Informatie in foutmeldingen en headers	De webserver geeft veel informatie vrij bij foutmeldingen, waardoor het aanvalsoppervlak voor een potentiële aanvaller wordt vergroot.	4.4	Opgelost	
NFIR 09	NFIR	Sessie is niet gebonden aan IP-adres	De webapplicatie kijkt niet of voor een actieve sessie het publieke IP-adres gewijzigd is. De sessie blijft actief en er wordt niet gevraagd om extra validatie.	4.4	Open	"Dit probleem is onderkend, maar complex om op te lossen. Omdat het daad-werkelijk uitvoeren van een succes-volle aanvallen complexer is en daarna ver-volgens maar beperkte im-pact zal zijn in de executie. Zelfs als het lukt om in te loggen is de impact beperkt. Zelfs na het doorzetten van sleutels is het veel werk om daadwerkelijk een melding te activeren. Het probleem wordt echter wel Opgelost en is daarom

						aan de back log toegevoegd."
NFIR 10	NFIR	Angular Development modus ingeschakeld	De webapplicatie die gehost wordt op coronamelder-portal.nl is geconfigureerd om in de 'development modus' te worden uitgevoerd.	3.8	Opgelost	
NFIR 11	NFIR	Access-Control-Allow-Origin configuratie	Cross Origin Resource Sharing (CORS) is een HTML5-technologie die moderne webbrowsers de mogelijkheid geeft om beperkingen te versoepelen die standaard zijn geïmplementeerd door het Same Origin-beleid. De 'Access-Control-Allow-Origin'-header is onveilig geconfigureerd wanneer deze is ingesteld op '*' of null, omdat de header er dan voor zorgt dat elk domein het toestaat om cross-domein verzoeken uit te voeren en de reacties uit te lezen.	3.8	Opgelost	
NFIR 12	NFIR		De API controleert de invoer niet op tekens die een speciale betekenis hebben in HTML en JavaScript.	0.0	Opgelost	
NFIR 13	NFIR	Verouderde SSL-bibliotheek aanwezig	De COVID-19 Notificatie applicatie voor Apple iOS (buildnummer 1.0.0 – 644f133) maakt voor het verwerken van data vanaf internet gebruik van een verouderde externe software- bibliotheek (OpenSSL versie 1.1.1d). Deze software- bibliotheek is mogelijk kwetsbaar voor een Denial-of-Service (DoS) aanval. Deze kwetsbaarheid draagt het CVE-nummer: CVE-2020-1967.	6.9	Opgelost	
NFIR 14	NFIR	Cache aanwezig in app-container	De COVID-19 Notificatie applicatie voor Apple iOS (buildnummer 1.0.0 – 644f133) maakt voor het verwerken van data-sleutels gebruik van verschillende mappen binnen de applicatie- container. Na het verwerken van deze sleutels, blijven de cache-bestanden aanwezig binnen de applicatie-container.	5.6	Open	Dit probleem is aangemeld bij Apple.
NFIR 15	NFIR	Jailbreak detectie niet aanwezig	De COVID-19 Notificatie applicatie voor Apple iOS (buildnummer 1.0.0 – 644f133) detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, voorzien is van een zogenoemde "jailbreak".	3.7	Gesloten	Dit is een bewuste keuze. Door telefoons met jailbreak af te sluiten, sluiten we een doelgroep uit. Ook biedt het hebben van

						een jailbreak mensen de mogelijkheid te controleren dat de app niks anders is dan de Open-sourcebroncode laat zien.
NFIR 16	NFIR	Reverse Engineering Tools detectie	De COVID-19 Notificatie applicatie voor Apple iOS (buildnummer 1.0.0 – 644f133) detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, reverse engineering tools zoals Frida bevat.	2.7	Gesloten	Er is geen geheim op de werking van de app. Reverse engineering kan leiden tot de bevestiting dat de broncode die publiekelijk beschikbaar is overreenkomt met de geinstalleerde software. Het is daarom zelfs wenselijk dat reverse engineering niet onmogelijk wordt gemaakt. Er is bewust gekozen om niet te beveiligen. op basis van security through obscurity.
NFIR 17	NFIR		De COVID-19 Notificatie applicatie voor Apple iOS (GitHub versie - buildnummer 1.0.2) detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, een zogenoemde emulator betreft.	0.0	Gesloten	Inherent aan Open source code is dat de functionaliteit ook op andere devices werken met aangepaste functionaliteit. Zo draait het ook op niet-telefoonplatformen. Daarnaast is security through obscurity bewust iets wat niet wordt gedaan

NFIR 18	NFIR		iOS apparaten bevatten de mogelijkheid om een schermafdruk te maken terwijl de applicatie op de achtergrond actief is. Hiermee kan mogelijk gevoelige data worden opgeslagen in een schermafdruk.	0.0	Gesloten	Omdat sommige gebruikers moeite hebben om te communiceren, kan een schermafdruk ze helpen. Op verzoek GGD'en. De risico's worden beperkt door het inzetten van wetgeving om misbruik hiervan te voorkomen en te bestraffen.
NFIR 19	NFIR	Cache aanwezig in app-container	De CoronaMelder applicatie maakt voor het verwerken van de gepubliceerde TEK-sleutels gebruik van verschillende mappen binnen de applicatiecontainer. Na het verwerken van deze sleutels, blijven de cache-bestanden aanwezig binnen de applicatie-container.	5.6	Opgelost	
NFIR 20	NFIR	Root detectie niet aanwezig	De CoronaMelder applicatie voor Google Android detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, voorzien is van een zogenoemde “root-toegang”.	3.7	Gesloten	Dit is een bewuste keuze. Door telefoons met jailbreak af te sluiten, sluiten we een doelgroep uit. Ook biedt het hebben van een jailbreak mensen de mogelijkheid te controleren dat de app niks anders is dan de Open-sourcebroncode laat zien.
NFIR 21	NFIR	Reverse Engineering Tools detectie	De CoronaMelder applicatie voor Google Android detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, reverse engineering tools zoals Frida en Drozer bevat.	3.7	Gesloten	Er is geen geheim op de werking van de app. Reverse engineering kan leiden tot de bevestiting dat de broncode die publiekelijk beschikbaar is overreenkomt met de

						geinstalleerde software. Het is daarom zelfs wenselijk dat reverse engineering niet onmogelijk wordt gemaakt. Er is bewust gekozen om niet te beveiligen. op basis van security through obscurity.
NFIR 22	NFIR	Emulator detectie niet aanwezig	De CoronaMelder applicatie voor Google Android detecteert niet of het apparaat waarop de applicatie geïnstalleerd is, een zogenoemde emulator betreft.	0.0	Gesloten	Inherent aan Open source code is dat de functionaliteit ook op andere devices werken met aangepaste functionaliteit. Zo draait het ook op niet-telefoonplatformen. Daarnaast is security through obscurity bewust iets wat niet wordt gedaan
NFIR 23	NFIR	Voorspelbare willekeurigheid	De CoronaMelder applicatie voor Google Android maakt twee keer gebruik van de voorspelbare Random()-functie. Deze functie is minder willekeurig (en daarmee minder veilig)dan de SecureRandom()-functie.	0.0	Gesloten	De waarde wordt gebruikt om verplichte opvulling (padding) aan te leveren. Het dient geen doel om te anonimiseren of codes weer te geven. Veilige willekeurige getallen zijn geen doel. Een aanpassing levert daarom niets op.
NFIR 24	NFIR	WAKE_LOCK-permissie	De CoronaMelder applicatie voor Google Android maakt gebruik van de WAKE_LOCK- permissie. Deze permissie zorgt ervoor dat de processor actief blijft en het	0.0	Gesloten	Deze permissie is noodzakelijk voor het actief blijven van CoronaMelder.

			scherm niet gesluimerd kan worden. In de applicatie is geen functionaliteit aangetroffen waarvoor deze permissie noodzakelijk is.			Dit heeft internationaal de aandacht.
NFIR 25	NFIR	Apparaat beveiligingsbeleid opties	De applicatie controleert niet of één van de volgende beveiligingsinstellingen aanwezig zijn: - Pincode of wachtwoord om het apparaat te ontgrendelen - USB Debugging - Apparaat Encryptie Het risico dat een ongeautoriseerde gebruiker toegang kan verkrijgen tot het apparaat is hiermee verhoogd	0.0	Gesloten	Dit is een bewuste keuze, omdat anders gebruikers worden uitGesloten en veel complexiteit voor de gebruiker wordt toegevoegd. Het niet afsluiten van de telefoon is een taak van de gebruiker.

Veilig tegen Corona

Na de bekendmaking van het voornemen om tot een app te komen, is er door een groep mensen een manifest opgesteld om de basale rechten en vrijheden van mensen te borgen.[157] De opsteller van dit rapport is een van de ondertekenaars van dit manifest. In dit hoofdstuk toetsen we in hoeverre is voldaan aan alle punten en de in het naschrift van het manifest genoemde punten. Minister Hugo de Jonge heeft aangegeven te willen voldoen aan de uitgangspunten.

De introductie bij het manifest duidt de context:

> *De Nederlandse overheid onderzoekt het gebruik van een app waarmee jij inzicht zou moeten krijgen in of je in de buurt bent geweest van iemand die besmet is met het Covid-19-virus. Als de overheid al zo'n app inzet, dan moet deze voldoen aan de volgende uitgangspunten. Deze uitgangspunten zijn opgesteld door deskundigen op het gebied van informatietechnologie, computerbeveiliging, privacy en de bescherming van fundamentele grondrechten. Wij geloven dat deze uitgangspunten noodzakelijk zijn voor het beschermen van onze vrijheden en rechten, onze veiligheid en sociale cohesie. Als niet aan deze uitgangspunten wordt voldaan, hebben we geen vertrouwen in de app en zullen we ons tegen de implementatie ervan verzetten.*

1ste uitgangspunt

Eén doel: het onder controle krijgen van het virus

> *De app en de gegevens die ermee worden verzameld, mogen alleen worden gebruikt voor het onder controle krijgen van het virus. Het gebruik moet gericht zijn op het vereenvoudigen van contactonderzoek, dus op het informeren en beschermen van individuen. Ander gebruik moet verboden zijn en voorkomen worden. De applicatie mag bijvoorbeeld niet gebruikt worden voor de handhaving van beleid, voor het bepalen of iemand in aanmerking komt voor een vergoeding van of toegang tot zorg of voor commerciële doeleinden.*

De situatie bij lancering

Er is inderdaad sprake van een hulpmiddel dat is gebouwd om COVID-19 onder controle te krijgen. Dat blijkt uit de kamerbrief "Landelijke introductie 'CoronaMelder'" van minister Hugo de Jonge van 16 juli 2020 met kenmerk: 1722926-208233-DICIO[158]. Hierin schrijft hij:

> *Doel van CoronaMelder*
>
> *CoronaMelder is een aanvulling op de reguliere bron- en contactopsporing van de GGD om de verspreiding van het virus zoveel en zo snel mogelijk te helpen beteugelen. Met CoronaMelder kunnen meer contacten van een besmette persoon sneller bereikt worden en worden ook personen bereikt*

[157] https://www.veiligtegencorona.nl/
[158] Kamerstuk: 25295-460 - https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z14096&did=2020D29955 – geverifieerd 8 augustus 2020

die besmette personen zich niet herinneren of die ze niet kennen. Denk hierbij bijvoorbeeld aan personen die bij een besmet persoon in het openbaar vervoer in de buurt hebben gezeten of bezoekers op het werk. Mocht iemand achteraf positief getest worden op het Coronavirus, dan kan de betreffende besmette persoon via de app dergelijke contacten anoniem waarschuwen. Deze contacten krijgen dan via de app een notificatie als zij gedurende 15 minuten of langer in de nabijheid zijn geweest en dus mogelijk een risico lopen ook besmet te zijn. Bij de melding via de app krijgen zij direct een handelingsadvies over de te nemen maatregelen.

Met CoronaMelder wordt beoogd een bijdrage te leveren aan het zo snel mogelijk informeren van burgers over hun risico op besmetting met het virus en daarmee aan het beheersen van de verspreiding van het virus. Elke vroegtijdig gevonden besmetting is winst omdat daarmee een mogelijke verspreidingsketen wordt verbroken. Ook bij een lage adoptiegraad is daarom al een effect te verwachten van het gebruik van de app. Dit neemt niet weg dat ik een zo hoog mogelijke adoptiegraad nastreef, want hoe meer mensen de app gebruiken hoe meer mogelijke ketens van besmetting verbroken kunnen worden.

Ook uit de technische werking van het systeem blijkt dit. Om mobiele waarschuwingen te laten genereren, moet een COVID19-slachtoffer actief de sleutels vrijgeven. Deze komen vervolgens pas beschikbaar nadat de GGD deze heeft vrijgegeven. Dit doet de GGD via het landelijke digitale registratiesysteem CoronIT dat speciaal is ontwikkeld voor het bestrijden van de COVID19-pandemie. De technologie en het hele stelsel waarin het is ingebed, zijn zo gemaakt dat het niet voor andere doeleinden kan worden ingezet, zonder forse aanpassingen.

Daarbij komt dat de wetgeving beperkingen oplegt, waardoor het doel ook niet mag veranderen. De verwerking valt onder de Algemene Verordening Gegevensbescherming[159] (kortweg: AVG). Dat staat in artikel 5, eerste lid aanhef en onder b[160]. Er is sprake van doelbinding en het maken van een aanpassing in de doelen is niet toegestaan. De verplichte[161] DPIA die is opgesteld, vermeldt dat het doel. Namelijk dat CoronaMelder alleen is bedoeld voor het bestrijden van de COVID-19 pandemie:

Doel van de voorgenomen gegevensverwerkingen is om in aanvulling op de bron- en contactopsporing van de GGD-en een app aan te bieden die gebruikers waarschuwt als zij risicovol contact hebben gehad met een op COVID-19 positief getest persoon. Hierdoor neemt de kans toe dat potentieel geïnfecteerde personen eerder in beeld komen en – daarmee – dat een exponentiële uitbraak van het virus sneller wordt afgeremd.

---

[159] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679 – geverifieerd op 9 augustus 2020.

[160] Aanhef: Persoonsgegevens moeten
b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding");

[161] Er is sprake van een grootschalige verwerking wanneer meer dan één miljoen mensen CoronaMelder gaan gebruiken. Dat verplicht tot een DPIA. Wat daarbij verwerkt wordt en wat je ermee zult kunnen, speelt daarbij geen rol.

Alle gegevens die worden verwerkt zijn strikt noodzakelijk om het bovenstaande doel op betrouwbare en veilige wijze te verwezenlijken.

CoronaMelder maakt gebruik van de API van Apple en Google. Om dat te mogen doen, moet de overheid zich houden aan licentievoorwaarden. Zowel in de licentie van Apple[162] als Google[163] wordt nadrukkelijk gesteld dat er alleen gebruik van de API mag worden gemaakt voor de bestrijding van COVID-19 en voor geen enkel ander doel (ook niet opsporing). Beide bedrijven geven duidelijk het doel van de API aan[164]:

Google en Apple voelen de verantwoordelijkheid overheden en de wereldbevolking te helpen COVID-19 te bestrijden. Daarom hebben we samen het systeem voor blootstellingsmeldingen ontwikkeld.

Zowel de wetgeving als de technische inrichting maken duidelijk dat de app slechts één doel kan dienen, namelijk het bestrijden van de COVID-19 pandemie. De kans op function creep is niet waarschijnlijk.

2de uitgangspunt

Gebaseerd op wetenschappelijk inzicht en bewezen effectief

De inzet van de app en de daarmee verzamelde gegevens moet gebaseerd zijn op wetenschappelijke kennis en aantoonbaar bijdragen aan het onder controle krijgen van het virus. Het moet vooraf helder zijn welke factoren van belang zijn voor de effectiviteit van de app, zoals bijvoorbeeld het percentage van de bevolking dat de app moet gebruiken. De app is vooraf getest op een beperkte groep gebruikers, op basis waarvan aantoonbaar is dat deze applicatie noodzakelijk, effectief en proportioneel is.

De situatie bij lancering

Internationaal wordt breed gebruikgemaakt van apps die melden wanneer er sprake is van een verhoogd risico op een besmetting. Bij vorige pandemieën werden deze hulpmiddelen nog niet ingezet. Het gevolg is dat er nog weinig wetenschappelijk onderzoek heeft plaatsgevonden naar de effectiviteit van dergelijke apps. Duidelijk is dat dergelijk onderzoek tijd kost. Dat betekent niet dat er geen wetenschappelijk onderzoek is gedaan.

---

[162] https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf - geverifieerd op 9 augustus 2020 – artikel 3.1: A Contact Tracing App, and any data collected through the Contact Tracing App or through the use of the Exposure Notification APIs, may be used only for the purpose of COVID-19 response efforts and not for any other purpose (such as law enforcement, including as enforced quarantine).

[163] https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf - geverifieerd op 9 augustus 2020 – artikel 1D: Is used exclusively for COVID-19 response efforts and not for any other purpose, such as law-enforcement or any punitive action (e.g., individual quarantine enforcement);

[164] https://www.google.com/covid19/exposurenotifications/ - geverifieerd op 9 augustus 2020

Het huidige wetenschappelijk inzicht is dat de inzet van dergelijke apps effectief is. Dat blijkt uit het onderzoek[165] 'COVID-19 incidence and R decreased on the Isle of Wight after the launch of the Test, Trace, Isolate programme' van Michelle Kendall, Luke Milsom, Lucie Abeler-Dörner, Chris Wymant, Luca Ferretti, Mark Briers, Chris Holmes, David Bonsall, Johannes Abeler en Christophe Fraser. Uit de paper[166] blijkt dat de Britse app op de Isle of Wright in een testfase door 38 procent van de bevolking is geïnstalleerd. Daarna komt het reproductiegetal R0 op de Isle of Wright substantieel lager te liggen dan in de rest van Verenigd Koninkrijk waar de app minder in gebruik. De onderzoekers kunnen niet uitsluiten dat er mogelijk ook andere factoren invloed hebben gehad en wijzen erop dat er meer onderzoek nodig is.

Daarnaast moet worden opgemerkt dat de Britse app gebruikmaakte van een centraal model en te boek staat als minder privacy-vriendelijk. Inmiddels is van deze app afgestapt en wordt gewerkt aan een app die vergelijkbaar is met het systeem zoals dat in Nederland is ontwikkeld.

De COVID-19 notificatieapp verschilt per land, waardoor de lijn niet zomaar kan worden doorgetrokken naar andere landen. De uiteindelijke effectiviteit van de app hangt immers niet alleen van de software af, maar ook van het gedrag van mensen. Wanneer zij geen verantwoording nemen, zal de uiteindelijke effectiviteit tegenvallen. Effectiviteit hangt verder af van het aantal besmettingen. Tijdens een besmettingsgolf zal de app meer effectiviteit sorteren dan tijdens periodes met nauwelijks nieuwe COVID-19-besmettingsgevallen.

Naast dit onderzoek is er aansluiting gezocht met wetenschappers op divers gebied, zoals uit het volgende punt blijkt.

3de uitgangspunt

Bewezen betrouwbaar en vanuit expertise

De app wordt ontwikkeld op basis van de expertise en onder de supervisie van onafhankelijke deskundigen, zoals dat nu ook al gebeurt voor wat betreft de medische aspecten van de bestrijding van het virus. Naast deskundigheid is ook publieke verantwoording en transparantie van de oplossing noodzakelijk. Daarmee worden de betrokken partijen scherp gehouden op zowel de effectiviteit als op het beschermen van mensenrechten en democratische beginselen. Op geen enkel moment in de ontwikkeling en inzet van de applicatie mogen we afhankelijk zijn van één enkele partij of systeem. De broncode van de applicatie en de overige infrastructuur is openbaar onder een vrije software licentie, zodat iedereen de werking van het systeem kan controleren. Ook moet aandacht besteed worden aan de controleerbaarheid van de daadwerkelijk gebruikte applicatie.

---

[165] Dit betreft de studie: COVID-19 incidence and R decreased on the Isle of Wight after the launch of the Test, Trace, Isolate programme. Michelle Kendall, Luke Milsom, Lucie Abeler-Dorner, Chris Wymant, Luca Ferretti, Mark Briers, Chris Holmes, David Bonsall, Johannes Abeler, Christophe Fraser - https://www.medrxiv.org/content/10.1101/2020.07.12.20151753v1 - link geverifieerd 8 augustus 2020.

[166] https://www.medrxiv.org/content/10.1101/2020.07.12.20151753v1.full.pdf - link geverifieerd 8 augustus 2020.

De situatie bij lancering

Op het moment van lancering is vast te stellen dat aan deze voorwaarde ruimschoots is voldaan.

1. Taskforce digitale ondersteuning bestrijding COVID-19, die vanuit wetenschap en praktijk adviseert. Deze taskforce bestaat uit;
    a. Dr. Sjaak de Gouw, Directeur Publieke Gezondheid Hollands Midden | GGD GHOR
    b. Dr. Mart Stein, Senior onderzoeker en coördinator onderzoek LCI, RIVM, CIb, LCI
    c. Prof. dr. Marc Bonten, Arts-microbioloog,UMC Utrecht
    d. Dr. Martin Bootsma, Wiskundige, universitair docent, UMC Utrecht, Universiteit Utrecht
    e. Dr. Nicole Dukers-Muijrers, Epidemioloog, universitair hoofddocent, GGD Zuid Limburg, Universiteit Maastricht
    f. Prof. dr. Lisette van Gemert-Pijnen, Professor of Persuasive Health Technology, Universiteit Twente
    g. Drs. Mariska Petrignani, Arts M&G, stafarts IZB en RAV, GGD Amsterdam
    h. Drs. Stijn Raven, Arts infectieziektebestrijding, GGD Regio Utrecht
    i. Dr. Jim van Steenbergen, Arts infectieziektebestrijding, epidemioloog
    j. Dr. Lex van Velsen, Clustermanager eHealth, Roessingh Research and Development
    k. Dr. Freke Zuure, programmaleider eHealth, NHG
    l. Dr. Albert Jan van Hoek, Senior onderzoeker modellering, RIVM, CIb, EPI
    m. Dr. Susan van den Hof, Hoofd Centrum voor Epidemiologie en Surveillance van Infectieziekten, RIVM, CIb, EPI
    n. Dr. Margreet ter Wierik, Arts M&G en senior onderzoeker, RIVM, CIb, LCI
    o. Dr. Ir. Albert Wong, Senior Statisticus en Coördinator Thema “Methoden voor Verzameling en Analyse van Data” binnen het Strategisch Programma RIVM, RIVM
2. Taskforce Gedragswetenschappen. Deze taskforce kijkt vanuit gedragswetenschappelijke expertise naar de bijdrage die digitale ondersteuning kan leveren aan het beheersen en opvolgen van besmettingen met het coronavirus. De Taskforce kijkt naar voorstellen van de ontwikkelaars, maar kan ook los daarvan adviezen uitbrengen. Het doel van de adviezen is dat de acceptatie van de digitale hulpmiddelen wordt vergroot, er minder ongewenste effecten zijn en gewenst gedrag wordt vergroot. Deze taskforce bestaat uit:
    a. Prof. dr. Catherine Bolman, Open Universiteit
    b. Prof. dr. Wolfgang Ebbers, Erasmus Universiteit Rotterdam
    c. Prof. dr. Lisette van Gemert-Pijnen, Universiteit Twente
    d. Dr. Sander Hermsen, OnePlanet Research Center
    e. Dr. ir. Nynke van der Laan, Tilburg University
    f. Prof. dr. ir. Peter-Paul Verbeek, Universiteit Twente
3. De Begeleidingscommissie heeft als opdracht om de minister van VWS te adviseren over digitale ondersteuning bij de bestrijding van COVID-19, onder andere op basis van voorstellen van de Taskforce digitale ondersteuning bestrijding COVID-19 en de Taskforce Gedragswetenschappen. Daarbij kijkt de Begeleidingscommissie naar de vraag in hoeverre een voorstel voor digitale ondersteuning bijdraagt aan de bestrijding van het COVID-19. En in hoeverre het voorstel voldoet aan de gestelde randvoorwaarden. Deze commissie bestaat uit:

a. Prof. Dr. Carl Moons, UMC Utrecht
b. Dr. Sjaak de Gouw, GGD Hollands Midden
c. Prof. Dr. Lisette van Gemert-Pijnen, Universiteit Twente
d. Prof. Dr. Peter Boncz, Centrum Wiskunde & Informatica (CWI) en Vrije Universiteit Amsterdam
e. Danny Mekić, NewTeam
f. Dr. Hester de Vries, Kennedy v/d Laan / Universiteit Utrecht
g. Prof. Dr. Maartje Schermer, Erasmus MC
h. Prof. Dr. Jan Kluytmans, Amphia Ziekenhuis / UMC Utrecht
i. Prof. Dr. Bart Jacobs, Radboud Universiteit
j. Anne-Miek Vroom, Stichting IKONE
k. Elisabeth van der Steenhoven, Public Matters
l. Bert Wijnen, voormalig Internet Engineering Task Force (IETF) participant
m. Patricia Heijdenrijk, Pharo
n. Prof. Dr. Janneke van de Wijgert, UMC Utrecht
o. Prof. Dr. Erik Buskens, UMC Groningen
p. Prof. Dr. Jochen Cals, Universiteit Maastricht

4. Bij de ontwikkeling van de software, de technische omgeving, het organiseren van de privacybescherming en informatiebeveiliging.
5. Advisering rond privacy. Naast de aangehaalde expertise is aan diverse externe partijen gevraagd om advies:
    a. Aan de Autoriteit Persoonsgegevens is gevraagd advies uit te brengen;
    b. Er is ondersteuning gevraagd aan de landsadvocaat, die onder meer door de Autoriteit Persoonsgegevens worden ingezet om hun ruime expertise.
    c. Er is een second opinion op de DPIA gevraagd aan Privacy Management Partners. Deze organisatie beschikt over expertise op het gebied van privacywetgeving en wordt eveneens door de Autoriteit Persoonsgegevens ingezet om hun expertise.
6. Onderzoeken en borging van de informatiebeveiliging. Om de informatiebeveiliging zo goed mogelijk te borgen, zijn de onderzoeken uitgevoerd door zeer vooraanstaande spelers op het gebied van informatiebeveiliging:
    a. Voor het toetsen van de broncode op de server voert Radically Open Security een onderzoek uit.
    b. Voor het toetsen van de server-setup voert KPN Security een interne toets en een penetratietest uit. De rapportages hiervan zijn intern voor KPN.
    c. Voor het toetsen van de broncode van de app voert Secura een onderzoek uit.
    d. Voor het toetsen van de vrijgegeven broncode door Apple en Google voert Radically Open Security een onderzoek uit.
    e. Beveiligingsbedrijf Noordbeek voert onder leiding van professor Paans een assessment uit naar de serveromgeving en de installatie van de servers voor beveiligingscertificaten.

4de uitgangspunt

De inzet van de applicatie is per definitie tijdelijk

De app mag alleen worden gebruikt voor het bovengenoemde doel en voor een vooraf bepaalde termijn. Enkel en alleen indien aantoonbaar noodzakelijk is dat de app langer wordt gebruikt, kan deze termijn worden

verlengd. Als de applicatie niet meer effectief of noodzakelijk is, wordt de uitrol teruggedraaid en wordt de data verwijderd. Dit kan ook indien er maatschappelijke onrust ontstaat, bijvoorbeeld omtrent veiligheid of mogelijk misbruik van de applicatie. Terugdraaien kan door de functionaliteit van de app ongedaan te maken en de geregistreerde gegevens te verwijderen.

De situatie bij lancering

De inzet van de app is tijdelijk. Dat vloeit voort uit het doel van het bestrijden van de COVID-19-pandemie. In dat antwoord is uitgebreid beschreven dat een ander doel niet is toegestaan op basis van de licentie van de API, de wetgeving (AVG) en voor zover de technische inrichting dat borgt.

De huidige inrichting maakt het mogelijk om de werking van de app tijdelijk (bijvoorbeeld bij weinig besmettingen) of definitief te stoppen. Zodra er geen sleutels beschikbaar komen, zullen er geen notificaties meer zijn.

5de uitgangspunt

Niet tot individuen herleidbaar

Het moet onmogelijk zijn om met de gegevens, die door de app worden verzameld, gebruikers te de-anonimiseren, ook niet als de gegevens worden gecombineerd met andere gegevens. Dit betekent dat het systeem niet gebouwd kan zijn op het gebruik van identificatienummers van hardware of andere identificerende gegevens, zoals het "Bluetooth Device Address".

De situatie bij lancering

CoronaMelder is zo opgezet dat alle inspanningen erop zijn gericht om herleidbaarheid tot personen te voorkomen. Dit is hiervoor in de rapportage al uitvoerig beschreven. De belangrijkste punten waar dat uit blijkt:

- Er wordt met dagelijks wisselende sleutels gewerkt, die door de API-laag wordt beheerd. De app kan daar slechts onder voorwaarden bij.
- Tijdens de uitwisseling van RPIs tussen telefoons wordt niet het Bluetooth Device Address gebruikt, maar een wisselend adres.
- Wanneer sleutels worden geüpload is zeker gesteld dat het IP-adres van de verzendende telefoon niet wordt bewaard.
- Notificaties worden op de telefoon zelf gegenereerd, waardoor niet herleidbaar is wie er een melding heeft gehad. Na het wegdrukken van een melding op de telefoon is niet te achterhalen dat er ooit een melding is geweest.
- Er worden geen gebruikersgegevens door de app bewaard of teruggestuurd. Er kan geen indirecte herleidbaarheid bestaan. Nederland is hierin strikter dan andere landen, waar nog wel aanvullende gegevens worden verwerkt of statistieken worden bijgehouden.
- Er is een strikte rollenscheiding tussen beheerders van de app en beveiligers. Hierdoor kan er geen data worden gecombineerd voor het geval er toch een theoretische herleidbaarheid zou zijn.

- Het hele DP-3T model[167] dat onder de app ligt, is opgesteld om iedere vorm herleidbaarheid te voorkomen.
- Als het netwerkverkeer wordt bewaakt dan zorgen dummy uploads ervoor dat niet is vast te stellen of verkeer een besmetting betekent of dat het gaat om dummyverkeer.

6de uitgangspunt

Zo min mogelijk gegevens worden gebruikt

De app slaat zo min en zo kort mogelijk gegevens op. Dat betekent bijvoorbeeld dat de app geen gegevens over iemands locatie vastlegt, maar slechts het identificerende nummer van andere gebruikers in de buurt. Ook is het niet nodig om het precieze tijdstip van zo'n ontmoeting te registreren. Om de gegevens op tijd te kunnen verwijderen is alleen een datum van registratie nodig, geen tijdstip.

De situatie bij lancering

Er is sprake van strikte dataminimalisatie. Locatie en tijdstip worden niet bijgehouden. Wel wordt de datum van registratie bijgehouden voor het tijdig verwijderen van de gegevens. Daarnaast is dat van belang voor het maken van een inschatting voor het al dan niet geven van een melding (ouderdom van het contact in relatie tot de duur en de afstand zeer dichtbij of iets verder weg). Waar het mogelijk is om binnen het DP-3T model te werken met meerdere risicoklassen, is uit oogpunt van privacy gekozen om hier slechts beperkt gebruik van te maken.

7de uitgangspunt

Geen centraal opgeslagen persoonsgegevens

Alle gegevens en processen worden in beginsel lokaal op iemands telefoon verwerkt. Dat betekent bijvoorbeeld dat het proces van de beoordeling of een gebruiker recent in contact is geweest met een besmet persoon, bij de gebruiker plaats moet vinden. Mocht het toch nodig zijn om gegevens te delen, bijvoorbeeld na het constateren van een besmetting, dan alleen na vrijwillige, expliciete en geïnformeerde toestemming van de gebruiker. De gegevens die wél de telefoon van de gebruiker verlaten, mogen op geen enkele wijze herleidbaar zijn tot die gebruiker.

De situatie bij lancering

Er worden geen persoonsgegevens centraal opgeslagen. Het model is decentraal opgezet. De gebruiker geeft toestemming voor het uploaden van sleutels naar de server toe. De sleutels op de server zijn voor de GGD niet inzichtelijk of toegankelijk. De code om de sleutels vrij te geven, stuurt de GGD naar de server. Als de code eenmaal is gebruikt dan wordt deze niet op de server bewaard. Het is niet mogelijk voor de GGD om vast te stellen of er daadwerkelijk een upload van sleutels is geweest. De gebruiker kan een code oplezen uit de app zonder ooit sleutels te uploaden.

[167] https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf – geverifieerd 9 augustus 2020.

8ste uitgangspunt

Veilig en bestand tegen misbruik

Het is belangrijk dat de vertrouwelijkheid en integriteit van gegevens beschermd worden. Dat kan door het gebruik van encryptie en andere beveiligingstechnologieën. Soms is meer nodig. Denk bijvoorbeeld aan een situatie waarin de app enkel bij de constatering van een besmetting een seintje geeft aan een andere gebruikers. Versleuteld of niet, uit de verzending van gegevens is al af te leiden dat de desbetreffende gebruiker mogelijk besmet is.

De situatie bij lancering

Zoals reeds uitgebreid in dit rapport beschreven wordt er niet alleen intensief gebruikgemaakt van cryptografie, maar is er tevens geïnvesteerd in het zo goed mogelijk borgen van de versleuteling. Er is sprake van dummyverkeer om herleidbaarheid op het netwerkverkeer te voorkomen. Er is kortom fors in vele maatregelen geïnvesteerd teneinde alle denkbare risico's te minimaliseren.

9de uitgangspunt

Gebruikersvriendelijk en toegankelijk

De applicatie is zo gebouwd dat deze voor iedereen in Nederland die het wil, te gebruiken is. Daarom moet nagedacht zijn over mensen die, bijvoorbeeld, niet beschikken over een smartphone, de Nederlandse taal niet machtig zijn of vanwege een beperking speciale aanpassingen behoeven.

De situatie bij lancering

Bij de ontwikkeling van CoronaMelder is gedacht aan mensen met allerhande beperkingen. Zo is de toegankelijkheid onderzocht voor mensen met een visuele beperking, 60+'ers, mensen met een licht verstandelijke beperking of een motorische beperking. Daarnaast is er veel onderzoek gedaan naar gebruikersvriendelijkheid.[168] Waar mogelijk zijn de aanbevelingen opgevolgd.

Voor hen die de Nederlandse taal niet machtig zijn, is er ondersteuning in negen andere talen. Dit kan in de toekomst desgewenst worden uitgebreiden.

Wie geen smartphone heeft, kan de app niet gebruiken. Deze beperking is in het kader van het ontwikkelen van een app ook niet op te lossen. Volgens recente cijfers van het CBS[169] gebruikt 92 procent van alle Nederlanders van 12 jaar en ouder een smartphone.

[168] Eindrapportage Ministerie VWS Gebruikerstesten Corona Notificatie app (Regio Twente). Te downloaden: https://www.rijksoverheid.nl/documenten/rapporten/2020/07/10/eindrapportage-ministerie-vws-gebruikerstesten-corona-notificatie-app-regio-twente

[169] https://www.cbs.nl/nl-nl/nieuws/2020/04/steeds-meer-ouderen-maken-gebruik-van-sociale-media

10de uitgangspunt

Nooit onder dwang van overheden of derden

> *Het gebruik van de applicatie mag op geen enkele manier worden afgedwongen. Als blijkt dat de app nodig is, dan is het belangrijk dat een groot deel van de bevolking deze app gebruikt. Dat kan alleen als de fundamentele grondrechten van de gebruiker worden gerespecteerd. Dus óók de keuze om de app niet te installeren. De overheid mag het gebruik ook niet met bijvoorbeeld een financieel lokkertje stimuleren. De applicatie moet daarnaast tijdelijk uit te schakelen en permanent te verwijderen zijn. Aan het weigeren van het gebruik mogen geen negatieve consequenties verbonden zijn. Dat betekent dat ook andere partijen, zoals een luchtvaartmaatschappij, zorgverzekeraar of een restaurant, geen voorwaarden mogen stellen aan het gebruik van de app. In het bijzonder moet het gebruik door werkgevers jegens werknemers en door opleidingsinstanties jegens scholieren/studenten strikt verboden worden.*

De situatie bij lancering

De eerder genoemde Taskforce gedragswetenschappen heeft tien kernwaarden opgesteld, waarvan vrijwilligheid bij het gebruik van de app de eerste is. Vrijwilligheid is iets wat in het beleid sterk wordt benadrukt. Dat blijkt bijvoorbeeld uit de kamerbrief "Landelijke introductie 'CoronaMelder'" van minister Hugo de Jonge van 16 juli 2020 met kenmerk: 1722926-208233-DICIO[170]. Hierin schrijft hij bijvoorbeeld op pagina 6 dat vrijwilligheid nadruk in de campagne krijgt:

> *In de communicatiecampagne zal ook sterk de nadruk gelegd worden op vrijwilligheid van het gebruik van de app.*

Verder schrijft hij rond de adoptie over vrijwilligheid:

> *Naast de massamediale publiekscampagne die ingezet gaat worden, wordt er gekeken welke organisaties kunnen helpen bij de adoptie van de app onder de Nederlandse bevolking. Op basis van bereik, bereidheid van vrijwillige adoptie en risico op virusverspreiding in de fysieke ruimtes van eventuele partnerorganisaties is een eerste selectie gemaakt van de te benaderen organisaties. Vanaf moment van introductie zal gestart worden met de partnerships. Hierbij blijft het benadrukken van vrijwilligheid uiteraard een voorwaarde waaraan ik niet zal tornen.*

Op pagina 13 van diezelfde brief schrijft hij het parlement:

> *Het gebruik van de app is vrijwillig en de app is gratis. CoronaMelder kan ook altijd weer van de telefoon verwijderd worden.*

Op pagina 14 benadrukt hij ook dat het doorgeven van de sleutels na het positief testen op Corona ook vrijwillig is:

---

[170] Kamerstuk: 25295-460 - https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z14096&did=2020D29955 – geverifieerd 8 augustus 2020

Als iemand positief getest is op het Coronavirus, zal deze persoon door de GGD gevraagd worden of de CoronaMelder is geïnstalleerd. Als dat het geval is, kan men dit vrijwillig en met hulp van de GGD medewerker melden in CoronaMelder.

Op pagina 17 van de brief benadrukt hij dat nogmaals:

Tot slot is van belang dat het gebruik van CoronaMelder, net als de deelname aan de analoge bron- en contactopsporing, uitsluitend plaatsvindt op basis van vrijwilligheid.

Op alle mogelijk manieren wordt duidelijk gemaakt dat er geen verplichting kan, mag en moet zijn. Op het moment van schrijven ligt er wetgeving voor die een verplichting tot gebruik van de app strafbaar stelt en waarbij ook over concrete handhaving is nagedacht. Mocht deze wetgeving worden goedgekeurd dan kan een overtreding van het verbod leiden tot een boete van 8.000 euro of tot zes maanden cel.

Aanvullende punten aan het einde van het manifest

Kortom, contact-apps moeten tijdelijk, transparant, volledig anoniem, vrijwillig en gebruiksvriendelijk zijn, zonder commerciële bijbedoelingen, en moeten onder regie staan van onafhankelijke deskundigen. De gelegenheidscoalitie roept de minister op om aan deze eisen gehoor te geven. De bestrijding van het coronavirus mag niet tot afkalving van onze privacy en fundamentele rechten leiden. Als het systeem dat nu ontwikkeld wordt niet aan deze eisen voldoet, zal deze coalitie zich met hand en tand tegen de implementatie ervan verzetten.

De situatie bij lancering

- De inzet van de app is tijdelijk. Er zijn voorzieningen getroffen om de werking te kunnen opschorten als de uitbraak is geremd of de werking van de app in zijn geheel te stoppen.
- Aan de transparantieverplichting wordt voldaan door waar mogelijk ontwerp, broncode, documentatie beschikbaar te maken en waar dit niet mogelijk is dit door basis van een audit inzichtelijk te maken.
- Zoals eerder uitgelegd in het rapport is het gebruik juridisch gezien pseudoniem, maar door alle maatregelen in de praktijk anoniem. De beperkingen worden opgelegd door de fysieke beperkingen van internettechnologieën. Het is moeilijk voorstelbaar om extra stappen te zetten die nog kunnen bijdragen aan verdergaande anonimiteit.
- Aan de verplichting tot vrijwilligheid wordt – zoals hiervoor uitgelegd – voldaan.
- Uit de onderzoeken met betrekking tot het gebruik blijkt dat CoronaMelder inderdaad gebruikersvriendelijk is.
- Er zijn geen commerciële bijbedoelingen. Doordat de Minister zelf de app vrijgeeft, zijn er geen andere doelen dan het bestrijden van de verspreiding van het COVID-19 virus.
- Zoals hiervoor duidelijk is geworden is breed ingezet op regie vanuit onafhankelijke experts. Zo zitten deze niet alleen in sleutelposities in het project, maar ook in de begeleidingscommissie en het College voor de Rechten van de Mens.

Invloed op fundamentele rechten

Onderliggend aan het manifest staan – zoals in het manifest sterk wordt benadrukt - de privacy en fundamentele rechten centraal (*De bestrijding van het coronavirus mag niet tot afkalving van onze privacy en fundamentele rechten leiden)*. Het uitgangspunt hiervoor is het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden[171] (kortweg: het EVRM). Uiteraard is de privacy (Recht op eerbiediging van privé-, familie- en gezinsleven – artikel 8) zelf een fundamenteel recht. Dat privacy vorm krijgt op zowel het punt van privacy-recht als daadwerkelijke privacy is in dit rapport al beschreven.

Daarnaast zijn er andere fundamentele rechten, die gezamenlijk een basis geven op een recht op bescherming van de gezondheid. Het College voor de Rechten van de Mens wijst hiervoor[172] naast diverse artikelen van het EVRM ook op het Internationaal Verdrag inzake economische, sociale en culturele rechten[173] (kortweg: IVESCR). Artikel 12, tweede lid aanhef en onder c[174] verplicht de Staat der Nederlanden om uitbraken, zoals COVID-19 te bestrijden. Overigens maakt het verdrag heel duidelijk dat IVESCR niet misbruikt mag worden om andere fundamentele rechten uit andere internationale verdragen in te beperken. Van een dergelijke inperking is geen sprake bij vrijwilligheid.

Nadrukkelijker vloeit een plicht om maatregelen te nemen voort uit artikel 11, aanhef en derde lid[175] van het herzien Europees Sociaal Handvest[176]. Of hieruit meteen ook voortvloeit dat het aanbieden van de app hiertoe behoort, zal waarschijnlijk pas na procederen zeker zijn. Maar dat er een druk is om mensen een kans te bieden een waarschuwing te krijgen bij een verhoogd risico op besmetting met COVID-19 mag duidelijk zijn. CoronaMelder zou dan gelden als een zogenaamde 'non pharmaceutical intervention'. Zeker als er meer wetenschappelijk bewijs komt dat er enige mate van effectiviteit blijkt te zijn. Hier is evident sprake van een spanning. Juist de vrijwillige benadering op een privacy-vriendelijke manier kleurt dit in ieder geval goed in.

Conclusie

Aan alle punten van het manifest wordt door CoronaMelder voldaan. Waar mogelijk is privacy het centrale uitgangspunt geweest. Op geen enkel punt is ingegrepen op de fundamentele rechten van de burger. Er is geen sprake van het zoeken van een balans tussen verschillende fundamentele rechten of het inperken van een fundamenteel recht. De Minister heeft waar mogelijk gekozen voor het borgen van de betrokken rechten met als uitgangspunt dat de privacy voorop moet staan. Het gevolg is dat CoronaMelder, vergeleken met andere landen die werken met een soortgelijk systeem, een hoger niveau van privacybescherming biedt. Het nadeel van die aanpak is dat het lastiger is statistieken van gebruik te verkrijgen, wat bijsturing moeilijker maakt.

---

[171] https://wetten.overheid.nl/BWBV0001000/2010-06-10 - geverifieerd 8 augustus 2020.
[172] https://mensenrechten.nl/en/node/707 - geverifieerd op 8 augustus 2020.
[173] https://wettten.overheid.nl/BWBV0001016/1979-03-11#Verdrag_2 – geverifieerd 8 augustus 2020.
[174] Artikel 12: De door de Staten die partij zijn bij dit Verdrag te nemen maatregelen ter volledige verwezenlijking van dit recht omvatten onder meer die welke nodig zijn om te komen tot:
c) Voorkoming, behandeling en bestrijding van epidemische én endemische ziekten, alsmede van beroepsziekten en andere ziekten;
[175] Aanhef: Teneinde de doeltreffende uitoefening van het recht op bescherming van de gezondheid te waarborgen, verbinden de Partijen zich, hetzij rechtstreeks, hetzij in samenwerking met openbare of particuliere instanties, passende maatregelen te nemen onder andere met het oogmerk:
Derde lid: epidemische, endemische en andere ziekten, alsmede ongevallen, zoveel mogelijk te voorkomen.
[176] https://wetten.overheid.nl/BWBV0001800/2006-07-01#Verdrag_2 – geverifieerd 8 augustus 2020.

Het enige punt waar niet optimaal aan kan worden voldaan is dat van wetenschappelijk bewijs van effectiviteit. De enige, op het moment van schrijven bekende wetenschappelijke studie[177] van 14 juli 2020, suggereert dat het gebruik van dit soort apps daadwerkelijk een invloed heeft op het verspreiden van COVID-19 en de veel besproken R0. Er blijft sprake van een kip-ei-probleem, omdat nog nooit eerder bij een pandemie dergelijke tools zijn ingezet. Zonder het inzetten van de tool zal de effectiviteit nooit meetbaar worden en het niet inzetten van een tool kan de fundamentele rechten van mensen schenden. Het is moeilijk voor te stellen hoe er beter aan de eisen van de gelegenheidscoalitie 'Veilig tegen Corona' had kunnen worden voldaan.

[177] Dit betreft de studie: COVID-19 incidence and R decreased on the Isle of Wight after the launch of the Test, Trace, Isolate programme. Michelle Kendall, Luke Milsom, Lucie Abeler-Dorner, Chris Wymant, Luca Ferretti, Mark Briers, Chris Holmes, David Bonsall, Johannes Abeler, Christophe Fraser - https://www.medrxiv.org/content/10.1101/2020.07.12.20151753v1 - link geverifieerd 8 augustus 2020.

Analyse kritische punten en zorgen maatschappelijke organisaties

Rathenau Instituut

Het Rathenau Instituut heeft vanaf het vroege begin van deze pandemie haar zorgen geuit over de mogelijke inzet van de app. Reeds in april stuurde het instituut vijf overwegingen als input voor de parlementaire discussie over de coronacrisis.[178] Toen al was er speciale aandacht voor de aangekondigde notificatieapp. Ook in andere uitingen laat het Rathenau Instituut zich kritisch uit over de inzet van zo'n app, zoals in "Overwegingen naar aanleiding van de Kamerbrief introductie "CoronaMelder" van 5 augustus 2020. [179] Dit is een aanvulling op de vijf overwegingen uit april.

Burgerrechten

Het document stelt:

> *De inbreuk op de rechten van burgers die gepaard gaat met de introductie van CoronaMelder is alleen gerechtvaardigd als die aantoonbaar noodzakelijk is en als de integratie in de publieke gezondheidsinfrastructuur effectief is.*

Er wordt niet geduid waar deze vermeende inbreuk op de rechten van burgers volgens hen uit bestaat. De opinie is volgens het Rathenau Instituut gevormd op basis van de informatie in de Kamerbrief.[180] Voor zover valt na te gaan zijn er geen vragen gesteld aan het ministerie. Het Rathenau Instituut heeft niet duidelijk gemaakt welke inbreuk op de rechten van de burgers zij zien.

Dé oplossing

Het Rathenau instituut waarschuwt de app niet te beschouwen als dé oplossing van de COVID-19 pandemie.[181]

> *Beoordeel de inzet van corona-apps in het kader van publieke gezondheid: niet als de kern van de oplossing, maar als één beleidsoptie.*

Nergens in de communicatie omtrent CoronaMelder wordt de app als zodanig gepresenteerd. Vanaf de samenstelling van het team dat na de Appathon in april zelf een app zou ontwikkelen, is het omschreven als een hulpmiddel om de bron- contactopsporing van de GGD-en aan te vullen.

De app waarschuwt gebruikers wanneer deze een risicovol contact hebben gehad met een op COVID-19 positief getest persoon. Hierdoor neemt de kans toe dat potentieel geïnfecteerde personen eerder in beeld komen en – daarmee – dat een exponentiële uitbraak van het virus sneller wordt afgeremd.

---

[178] https://www.rathenau.nl/sites/default/files/2020-04/BAP%20De%20Corona-crisis%20vraagt%20om%20zorgvuldig%20handelen%20en%20democratisch%20debat_1.pdf
[179] https://www.rathenau.nl/sites/default/files/2020-08/Overwegingen%20naar%20aanleiding%20van%20Kamerbrief%20introductie%20Coronamelder.pdf
[180] https://www.rijksoverheid.nl/documenten/kamerstukken/2020/07/16/kamerbrief-over-landelijke-introductie-coronamelder
[181] Tweede overweging van het Rathenau instituut uit april.

CoronaMelder wordt nergens gepresenteerd als een panacee tegen COVID-19. Wel wordt uit wetenschappelijk onderzoek, onder meer van de Universiteit van Oxford,[182] duidelijk dat notificatieapps wel degelijke een beperkende invloed kunnen hebben op de verspreiding van het virus.

Het systeem is zo ingericht dat op ieder moment het herleiden naar gebruikers extreem moeilijk of zelfs onmogelijk is. Het gebruik van de app is vrijwillig en mag niet worden verplicht. Er is wetgeving gemaakt om dwang voor gebruik strafbaar te stellen. De inzet van de app is tijdelijk en er is voorzien dat deze ook weer stopt, wanneer de Corona-pandemie is ingedamd.

Daarbij is het belangrijk om de context van de COVID-19 pandemie in oog te blijven houden. Het voorkomen van aanvullende besmettingen of het eerder behandelen kan een behoorlijk verschil maken in het verloop van de ziekte. Zo kunnen patiënten ernstige vormen van COPD ontwikkelen, hartproblemen oplopen of langdurig last houden van chronische vermoeidheid met een fors lagere productiviteit en verdiencapaciteit tot gevolg. Het kan en mag niet worden gezien als een griep.

Gefragmenteerde informatievoorziening

De informatievoorziening aan de Kamer is zeer gefragmenteerd. De brief van de minister en de vele adviezen zijn puzzelstukjes van een onvolledige puzzel. De Tweede Kamer kan het kabinet vragen om het politieke en maatschappelijke debat te helpen door te beginnen met een toelichting vanuit de bestaande wetgeving en de huidige bevoegdheden van de minister en de GGD en vervolgens aan te geven hoe CoronaMelder hieraan bijdraagt.

CoronaMelder is een lopend ICT-project. Kenmerkend bij een lopend project is dat er gaandeweg meer documenten beschikbaar komen. De nieuwe documentatie wordt met de eerstvolgende Kamerbrief ter beschikking van de Kamer gesteld, geheel in lijn met het open en transparante karakter van het project. Iedere betrokkene en geïnteresseerde wordt zo maximaal meegenomen in de ontwikkelingen terwijl het gebeurt, in plaats van hen te informeren als CoronaMelder af is. Dit biedt de mogelijkheid tot het stellen van inhoudelijke vragen, het organiseren van technische briefings of de inzet van andere stuurelementen. Zo is ook door de Tweede Kamer gevraagd in de motie Jetten.

Onvermijdelijk in deze aanpak is dat de informatie inderdaad op een fragmentarische manier beschikbaar komt. Gezien de urgente context van de pandemie is het belangrijk dat CoronaMelder zo spoedig mogelijk een rol gaat spelen tegen een pandemie. Dit betekent niet dat onzorgvuldigheid wordt toegestaan, maar wel dat er op zeer hoge snelheid gewerkt moet worden.

[182] https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown - geverifieerd 12 september 2020

Het punt van fragmentarische informatie met daarbij een heldere duiding is in een vroeg stadium onderkend. Daarom is in mei al besloten tot het maken van een eindrapportage, waarin de werking van CoronaMelder, de privacy, het privacyrecht, de informatiebeveiliging, de onderzoeken worden geduid. Hierdoor ontstaat een zeer gedetailleerd totaalbeeld.

Rechtvaardiging en proportionaliteit

> *Gezien de betrouwbaarheid van 70-75% van CoronaMelder in combinatie met de betrouwbaarheid van coronatests en het risico op onzorgvuldigheden in het meldingsproces is het de vraag of de introductie van de app voldoende effectief en daarmee proportioneel is. Vanwege het gebrek aan een duidelijke toelichting op de proportionaliteit is het nu tevens onduidelijk wanneer de inzet niet meer proportioneel is en wanneer het gebruik van de app wordt beëindigd.*[183]

CoronaMelder is niet bedoeld als panacee voor de COVID-19 crisis, maar Bluetooth is dat evenmin. De gebruikte Bluetooth Low Energy is namelijk niet geschikt om afstanden te meten. Dat was een van de leerpunten van de Appathon. Om de sterke en minder sterke kanten van Bluetooth te illustreren, gebruiken we het onderzoek dat het Rathenau Instituut opvoert om de mate van betrouwbaarheid van Bluetooth aan te tonen.[184] Dat onderzoek ging uit van de situatie dat er blind wordt vertrouwd op Bluetooth Low Energy als tool om afstanden te meten. Het is dan ook niet verwonderlijk dat dit leidt tot het beeld dat er sprake is van 'slechts' 70-75 procent betrouwbaarheid. Deze weergave komt echter niet overeen met wat er daadwerkelijk in CoronaMelder wordt gerealiseerd.

Als gevolg van dit onderzoek is duidelijk geworden dat Bluetooth signalen in drie groepen kunnen worden verdeeld:

1. Wanneer signalen sterk zijn, zijn telefoons in elkaars nabijheid. Deze signalen zijn betrouwbaar en bruikbaar. Deze worden gebruik voor de meting in CoronaMelder.
2. Wanneer signalen minder sterk zijn, zijn telefoons verder uit elkaar. De signalen zijn dan minder betrouwbaar. Deze signalen gebruiken we alleen als twee telefoons langer dan een kwartier onafgebroken in elkaars nabijheid zijn geweest. Dat geeft een hoge mate van zekerheid dat mensen daadwerkelijk bij elkaar in de buurt zijn geweest en dat een waarschuwing nuttig is.
3. Zwakke signalen blijken onbetrouwbaar en deze worden dan ook door CoronaMelder genegeerd.

Hieruit volgt dat Bluetooth als zodanig niet in staat is afstanden te meten. Uit de verzamelde informatie valt echter vrij eenvoudig te analyseren of signalen sterk, minder sterk of zwak zijn. Hieruit kan een doorslaggevende mate van nabijheid worden gededuceerd. Een en ander hangt samen met de gehanteerde perimeter van 1,5 meter. Wanneer bijvoorbeeld een grens van 3 meter zou worden gehanteerd, stijgt de sensitiviteit met aangepaste instellingen tot 90 procent. Dat betekent dat de meeste gevallen die bij de huidige instellingen een onterechte notificatie zouden ontvangen. De notificatie zou wel geldig zijn als we zouden uitgaan van een perimeter van 3 meter.

---

[183] Zie in relatie tot dit kritiekpunt ook het hoofdstuk 'Noodzaak en evenredigheid' elders in dit rapport.
[184] COVID-19 Notificatie APP, Veldtest Bluetooth Validatie, Ministerie van VWS, Defensie CBRN, Vught 8 juni 2020. Download: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/08/veldtest-bluetooth-validatie-covid-19-notificatie-app

Hoe groter de afstand tot elkaar, hoe kleiner de kans om geïnfecteerd te worden met COVID-19. De grenzen die in dit kader worden gehanteerd door diverse landen zijn arbitrair. Hier speelt een precair evenwicht tussen het verkleinen van risico's en het laten functioneren van de samenleving en economie.

Hoe dan ook neemt de schaal van besmetting logaritmisch af. Dat betekent dat iemand op meer dan anderhalve meter afstand of meer geen risico op besmetting meer loopt. Als er vanaf grotere afstand besmetting plaatsvindt, behoort dat tot de uitzonderingen. De keuze voor een perimeter van anderhalve meter kan het risico op besmetting zeer fors vergroten. Een melding van CoronaMelder boven de anderhalve meter is daarom in de juiste context nog altijd zinvol.

De metingen hebben geleid tot een verbetering van de betrouwbaarheid. Daarnaast zijn de bevindingen in internationaal verband besproken in het eHealth netwerk, zodat andere landen er hun voordeel mee kunnen doen. Ook hebben Apple en Google verbeteringen in de API doorgevoerd om tot betere resultaten te komen. Alles bij elkaar betekent dit dat de nulmeting vergelijkbaar is met de realiteit binnen CoronaMelder.

Er zijn altijd onnauwkeurigheden verbonden aan het gebruik van technologie. Desondanks kan CoronaMelder mensen waarschuwen voor een verhoogd risico’s op een infectie met COVID-19, zelfs wanneer iemand nog geen ziekteverschijnselen heeft ervaren. Dit maakt medisch ingrijpen mogelijk. Maar het kan met name een kettingreactie in besmettingen een vroegtijdig halt toeroepen. Dat is – zeker met de kennis van nu – een grote pre vergeleken met de situatie waarin mensen niet of nauwelijks de mogelijkheid krijgen te worden gewaarschuwd. Het analoge bron- en contactonderzoek is lovenswaardig, maar met de inzet van digitale hulp zal het zeer waarschijnlijk nog effectiever zijn.

Er is nog weinig wetenschappelijk bewijs over het gebruik van apps. Dat is niet vreemd, omdat er bij eerdere pandemieën dergelijke mogelijkheden niet of nauwelijks waren. Er is wel een studie, die suggereert dat een app effect kan sorteren. Dat blijkt uit het onderzoek[185] “COVID-19 incidence and R decreased on the Isle of Wight after the launch of the Test, Trace, Isolate programme”. De adoptie van de Britse app bleek op de Isle of Wright hoger dan in de rest van het Verenigd Koninkrijk, waarbij duidelijk werd dat er een invloed op de R0 bleek.

> *Uit het Europese Verdrag van de Rechten van de Mens (EVRM) volgt dat geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van rechten van burgers zoals hun privacy rechten, dan voor zover bij wet is voorzien. Daarnaast moet de inmenging in een democratische samenleving noodzakelijk zijn en in het belang van bijvoorbeeld de bescherming van de gezondheid of voor de bescherming van de rechten en vrijheden van anderen.*

Dit punt onderschrijven wij volledig. Juist daarom is er gekozen voor een benadering waarbij gebruik van CoronaMelder vrijwillig is en het kabinet iedere vorm van afdwingen van het gebruik van de app strafbaar wil stellen. Wie kiest voor het gebruik van de app moet erop kunnen vertrouwen dat er gedegen is nagedacht over privacy en dat de deugdelijk zonder

[185] Dit betreft de studie: COVID-19 incidence and R decreased on the Isle of Wight after the launch of the Test, Trace, Isolate programme. Michelle Kendall, Luke Milsom, Lucie Abeler-Dorner, Chris Wymant, Luca Ferretti, Mark Briers, Chris Holmes, David Bonsall, Johannes Abeler, Christophe Fraser - https://www.medrxiv.org/content/10.1101/2020.07.12.20151753v1 - link geverifieerd 28 augustus 2020.

meer is geborgd. Het hele stelsel van CoronaMelder leunt op DP-3T (Decentralised Privacy Preserving Proximity Tracing). Dit systeem werkt, zoals de naam al aangeeft, decentraal, wat een groot voordeel is qua privacy-bescherming. Dankzij dit systeem en de maatregelen die het ministerie heeft getroffen is het praktisch onmogelijk gebruikers van de app te volgen of te identificeren.

Los van het bovenstaande spelen er meer fundamentele rechten. Vergeet niet dat we te maken hebben met een pandemie die wij uit economische behoefte en – in verband daarmee – om redenen van levenskwaliteit zo snel mogelijk een halt willen toeroepen. Dit willen wij met behulp van CoronaMelder zorgvuldig en weloverwogen doen. De genoemde fundamentele rechten vloeien deels voort uit het EVRM, alsmede nadrukkelijk uit het Europees Sociaal Handvest[186]. In de laatste staat in artikel 11, aanhef en derde lid de volgende plicht:

> *Teneinde de doeltreffende uitoefening van het recht op bescherming van de gezondheid te waarborgen, verbinden de Partijen zich, hetzij rechtstreeks, hetzij in samenwerking met openbare of particuliere instanties, passende maatregelen te nemen onder andere met het oogmerk: 1. de oorzaken van een slechte gezondheid zoveel mogelijk weg te nemen; 2. ter bevordering van de volksgezondheid en de persoonlijke verantwoordelijkheid op het gebied van de gezondheid voorzieningen te treffen op het terrein van voorlichting en onderwijs; 3. epidemische, endemische en andere ziekten, alsmede ongevallen, zoveel mogelijk te voorkomen.*

Dit artikel laat er geen misverstand over bestaan dat er bij de verantwoordelijke partijen een plicht bestaat alle burger een gerede kans te bieden een waarschuwing te krijgen bij een verhoogd op een besmetting met COVID-19. Vanuit deze benadering zou CoronaMelder dan gelden als een zogenaamde ‘non pharmaceutical intervention’. Dit wordt des te waarschijnlijker wanneer er, zoals kan worden verwacht, meer wetenschappelijk bewijs komt dat notificatieapps effectief blijken te zijn. Hier is evident sprake van een spanning. Juist de vrijwillige benadering op een privacy-vriendelijke manier zou eventuele twijfel weg moeten nemen.

> *De Tweede Kamer kan het kabinet vragen hoe de aangekondigde wetgeving rondom de corona-app voldoet aan de kwaliteitseisen die (inter)nationale wetgeving, zoals het EVRM, daaraan stelt.*

Het EVRM, de AVG en andere internationale richtlijnen bieden ons algemene kaders. Het ontbreekt echter aan kwaliteitseisen. Wel zijn er verplichtingen zoals het maken van een DPIA. Uiteraard is die uitgevoerd net als andere risico-inschattingen. Het ministerie heeft dit in een vroeg stadium erkend en heeft aansluiting gezocht bij de regulier geldende normen. Een voorbeeld daarvan is het zoveel mogelijk werken volgens de Baseline Informatiebeveiliging Overheid of het toetsen tegen internationale standaarden tijdens de penetratietest.

[186] https://wetten.overheid.nl/BWBV0001800/2006-07-01#Verdrag_2 – geverifieerd 28 augustus 2020.

De Tweede Kamer kan het kabinet vragen de datum vast te leggen waarop het gebruik van de app wordt beëindigd, of de criteria kenbaar te maken die tot beëindiging zullen leiden.

De doorlopende evaluatie kan zo nodig leiden tot aanpassingen en bijstellingen van de app, het werkproces of de informatievoorziening over de app. De indicatoren zullen ook gebruikt worden als input bij het bepalen wanneer de app niet meer noodzakelijk is. De opsteller van dit rapport zal hiertoe te zijner tijd besluiten op advies van onder andere de begeleidingscommissie en de Taskforces. Vanzelfsprekend houdt de opsteller van dit rapport u op de hoogte van de uitkomsten van de doorlopende evaluatie.

Google en Apple

Met de eventuele introductie van CoronaMelder gaat de regering in haar publieke gezondheidsinfrastructuur een verregaande afhankelijkheidsrelatie aan met de private partijen Google en Apple. Zoals de begeleidingscommissie Digitale ondersteuning bestrijding Covid-19 reeds formuleerde (Advies 2: Gebruik Google en Apple API) zijn heldere en bindende afspraken met hen noodzakelijk.

Er zijn bindende afspraken met Apple en Google gemaakt. De software (de Exposure Notification API) is onderhevig aan een licentie waarin duidelijke afspraken zijn gemaakt. Uit de afspraken en de vragen blijkt duidelijk dat beide organisaties geen toegang krijgen tot de verwerkte gegevens. Bovendien is dit technisch uitgesloten. Zij zijn in deze louter een leverancier van software.

Google en Apple bieden nu bijvoorbeeld geen volledig inzicht in de broncode van de door hen aangeboden API en het is onzeker of de deels geopenbaarde broncode wel dezelfde is als de code die in werkelijkheid op de telefoons van gebruikers staat. Onafhankelijke controle op veiligheidsaspecten en controle op oneigenlijke verwerking van persoonsgegevens zijn daardoor onmogelijk.

Het is correct dat technisch niet is vast te stellen of de broncode die Apple en Google hebben overlegd, dezelfde is als de broncode die in gebruik is. Binnen het huidige stelsel van samenwerking is er echter geen aanleiding aan te nemen dat hier sprake zou zijn van een verschil. Het Nederlands recht zou het toevoegen van andere functionaliteit aan de API dan overlegd, door Google dan wel door Apple, vaststellen als een onrechtmatige daad. Wanneer er verwerking van gegevens zou plaatsvinden door verborgen functionaliteit, zou dat in strijd zijn met de richtlijn van de AVG. De informatie die Google of Apple zouden kunnen verkrijgen, staat niet in verhouding tot de omslachtige methode die ze in theorie daartoe zouden aanwenden. Als we het op die manier bekijken, weten we dat beide bedrijven langs legitieme weg toegang hebben tot gegevens die veel meer informatie opleveren.

Verder bepalen Google en Apple nu eenzijdig de voorwaarden voor gebruik en het staat hen vrij om in de toekomst die gebruiksvoorwaarden of het gedrag van de API te wijzigen. Nu zijn bijvoorbeeld voor het gebruik van CoronaMelder op Android-systemen de Play Store en het registreren van een Google-account voorwaardelijk gesteld, terwijl dit vanuit technisch oogpunt niet noodzakelijk is. Gebruikers met andere Android-systemen of

bijvoorbeeld diverse Huawei-telefoons waarop geen Play Store beschikbaar is, worden daardoor uitgesloten.

Dat is een correct vaststelling, waarvan het ministerie zich bewust is. De groep gebruikers die hier wordt aangegeven is dermate klein (iets boven de 5.000 gebruikers) dat omwille van de voortgang niet direct een oplossing kan worden geboden. Het aanbieden van een oplossing voor alle platformen is dermate arbeidsintensief dat dit een onverantwoorde vertraging zal opleveren. Er wordt gekeken of gebruikers van de nieuwste Huawei telefoons op een later moment alsnog bediend kunnen worden.

Kortom, Google en Apple worden door de keuze van het kabinet bevoordeeld in hun concurrentiepositie en het is niet vast te stellen of hun API een Trojaans paard betreft.

Het is niet duidelijk waarom het Rathenau Instituut veronderstelt dat de app als een trojaans paard zou worden ingezet. Beide bedrijven hebben reeds toegang hebben tot de mobiele telefoons. Wij achten het hoogst onwaarschijnlijk dat er omwille van vermeende data-acquisitie wordt meegelift op een app van een vreemde mogendheid. De app – die door een relatief klein deel van alle smartphonegebruikers wereldwijd wordt geïnstalleerd – heeft in vergelijking tot de besturingssystemen (iOS en Android) nauwelijks enig voordeel om eventuele verborgen functionaliteit in te zetten. De kans op ontdekking bij de API is vele malen groter, omdat die door beveiligingsbedrijven voortdurend wordt getest.

In Nederland wordt zeer zorgvuldig omgegaan met de introductie van het elektronisch patiëntendossier en de toepassing van AI in de zorg. Tot op heden wordt gewerkt aan de haken en ogen die dit met zich meebrengt. De Tweede Kamer moet ervoor waken dat deze private partijen via deze app toegang krijgen tot medische of andere gevoelige gegevens, zonder zorgvuldige garanties.

CoronaMelder heeft op geen enkele wijze toegang tot medische dossiers. Het wordt louter en alleen ingezet om mensen te waarschuwen voor een verhoogd risico op een besmetting met COVID-19 als gevolg van een contact met een positief getest persoon. De app heeft geen enkele andere functionaliteit.

Medische gegevens

In de Data & Privacy Impact Assessment (DPIA) wordt opgemerkt dat bij constatering door de GGD van een (mogelijke) infectie sprake is van een behandelrelatie tussen een geïnfecteerde burger en de GGD. Als die gegevens eenmaal onderdeel uitmaken van de behandelrelatie, dan worden ze beschermd door het medisch beroepsgeheim. De betreffende gegevens zijn dan onderdeel van het medisch dossier. Hierop is de huidige wet- en regelgeving van toepassing. Bijvoorbeeld in gevallen waarin de infectiegegevens worden gebruikt voor onderzoeken omwille van (inzichten in) de volksgezondheid.

Dat is correct, maar dit betreft niet direct de inzet van CoronaMelder.

Ook hebben app-gebruikers, in de hoedanigheid van patiënten, verschillende rechten met betrekking tot de gegevens in hun medisch dossier. Zo moet de patiënt in de regel toestemming geven voor verder

gegevensgebruik door anderen dan de behandelend GGD-hulpverlener. Het is nu onduidelijk hoe de app waarborgt dat het medisch beroepsgeheim wordt gerespecteerd en dat de gebruikers hierover worden geïnformeerd. In de tot nog toe verstrekte stukken is er nauwelijks aandacht uitgegaan naar deze aard van de gegevens en de daarbij geldende regels.

App-gebruikers zijn niet per definitie patiënten, maar burgers in algemene zin. In de app worden geen medische gegevens verwerkt. De sleutels die na actieve instemming worden gedeeld, wanneer de gebruiker positief heeft getest op COVID-19, worden gedeeld met andere gebruikers. Deze sleutels zijn niet tot de persoon te herleiden. De GGD heeft geen toegang tot de beschikbaar gestelde sleutels, waardoor zij geen link tussen de verificatiecode en de beschikbaar gestelde sleutels kunnen leggen. Aangezien er verder geen gegevens worden verwerkt, is het onmogelijk om nadere wettelijke kaders toe te passen. Er wordt niet behandeld op basis van CoronaMelder. Het is slechts een waarschuwingstool.

De Tweede Kamer kan het kabinet vragen of de app voldoet aan alle eisen die gesteld worden aan het verwerken van medische gegevens.

Zoals gezegd: de app verwerkt geen medische gegevens. Er is derhalve geen indicatie dat waar dan ook niet wordt voldaan aan de regels.

Risico op profilering en stigmatisering

In de DPIA wordt alleen aandacht besteed aan de AVG-aspecten van de app zelf en de data die daarin worden verwerkt. In een DPIA horen de risico's op profilering te worden beoordeeld, maar die zijn ditmaal buiten beschouwing gelaten.

Het is een onjuiste veronderstelling dat deze risico's buiten beschouwing zouden zijn gelaten. Ze zijn simpelweg niet aangetroffen. Het is inherent aan een DPIA dat wordt gekeken naar de privacy-aspecten voor de verwerking van gegevens waarvoor er verantwoordelijkheid is. Dat is geen miskenning van risico's maar een voortvloeisel van de werking van de AVG. Juist hierom wordt in de uiteindelijke duidingsrapportage niet alleen gekeken naar privacy-recht, maar ook naar privacy.

De app functioneert bijvoorbeeld binnen de besturingssystemen van Google en Apple. Het is voor hen mogelijk om de (telemetrische) gegevens van gebruikers te combineren met andere gegevens over gebruikers die reeds bij hen bekend zijn en zo profielen op te bouwen.

De afhankelijkheid van besturingssystemen waar het overgrote merendeel van de Nederlandse burgers mee werkt, is inderdaad de realiteit. Niet de app is hier de bottleneck, eerder de manier waarop de markt is vormgegeven. Anders dan de onderzoekers van het Rathenau Instituut stellen, worden er door de app geen telemetrische gegevens gebruikt die naar de persoon herleidbaar zijn. Zou dat wel het geval zijn dan wordt er alsnog een verwerking van persoonsgegevens gestart. Daarvan is nadrukkelijk geen sprake.

Gebruikers en niet-gebruikers van de app kunnen ook worden gestigmatiseerd. Mensen kunnen worden gevraagd of zij de app gebruiken en dit kan zonder hun medeweten worden bepaald door een scanner. Zo bestaat er in allerlei situaties het risico op stigmatisering, discriminatie en uitsluiting, waardoor gebruikers schade kunnen ondervinden, hun keuzes kunnen worden beïnvloed of hen bijvoorbeeld de toegang kan worden ontzegd tot belangrijke plaatsen, producten, diensten of behandelingen.

Er wordt actief beleid gevoerd op de vrijwilligheid. Een strafbepaling in voorgenomen wetgeving geldt voor iedereen die de app verplicht probeert te stellen. De straffen zijn fors: maximaal 8.000 euro boete of een half jaar cel per overtreding, waarbij er daadwerkelijk handhavend zal worden opgetreden.

De dreiging die uitgaat van profilering en stigmatisering kan langdurig van aard zijn. Profielen kunnen immers lang blijven bestaan, ook al zijn de app en de daarin gebruikte data tijdelijk.

Deze stelling is in het algemeen ontegenzeggelijk juist. Alleen wordt uit het onderzoek niet duidelijk aan welke stigma's in het kader van CoronaMelder moet worden gedacht. De risicoanalyse in de DPIA – waar stigmatisering in de voorbereiding nadrukkelijk is besproken – maakt duidelijk dat dit probleem praktisch nauwelijks voorstelbaar is.

Ook in de 'Ethische analyse van de COVID-19 notificatie-app ter aanvulling op bron- en contactonderzoek GGD' wordt aanbevolen om oneigenlijk gebruik te voorkomen, waaronder het stigmatiseren van gebruikers en niet-gebruikers. De ethische analyse heeft echter nog geen aandacht voor profilering.

Er wordt een breed beleid gevoerd op oneigenlijk gebruik, variërend van de eerder genoemde strafbepaling tot het bijstaan van mensen die het slachtoffer zijn van oneigenlijk gebruik. De AVG biedt mogelijkheden tot schadevergoeding bij misbruik. Hierop zal een actief beleid worden gevoerd, waarbij betrokkenen van oneigenlijk gebruik op hun rechten worden gewezen.

Het is onduidelijk of burgers wordt gevraagd om toestemming om gegevens geanonimiseerd te mogen gebruiken. Bij de bestaande Corona Check-app vraagt de app-bouwer (een private partij) bijvoorbeeld om data te mogen gebruiken, om zo bepaalde 'services' te verbeteren. Anonimiseren betekent echter niet dat er geen profilering mogelijk is. Ook als de data worden vernietigd of geanonimiseerd, kan persoonsgevoelige informatie blijven bestaan en kunnen (groepen) burgers hiervan nadeel of schade ondervinden. Op basis van de COVID Radar communiceert bijvoorbeeld het LUMC in welk postcodegebied meer risico bestaat op besmetting. Dit kan een bepaalde wijk stigmatiseren.

Anders dan de genoemde apps (Corona Check-app, COVID-radar) verwerkt CoronaMelder geen ziekteverschijnselen. CoronaMelder is uitsluitend gericht op het waarschuwen van gebruikers. Er worden geen locatiegegevens verwerkt. De functionaliteit verschilt fundamenteel van de genoemde apps. De functionaliteit van CoronaMelder valt op te maken uit de DPIA.

De Tweede Kamer kan het kabinet vragen of er naast de partijen die worden genoemd in de DPIA andere partijen toegang vragen tot gegevens, en zo ja, met welk doel.

In de DPIA en in dit rapport worden alle partijen genoemd die toegang hebben tot persoonsgegevens en waarom dat noodzakelijk is. Andere partijen toegang verlenen zou betekenen dat het Ministerie de AVG bewust zou gaan overtreden. Dit gebeurt niet.

De Tweede Kamer kan het kabinet vragen welke maatregelen het neemt om de dreiging die uitgaat van profilering en stigmatisering tegen te gaan, en daarbij niet alleen te kijken naar de app, maar de gehele brede context van het gebruik of niet-gebruik ervan.

De hiertoe genomen maatregelen zijn hiervoor benoemd.

Klachten, bezwaren, wederhoor, schade en verhaalmogelijkheden

De stukken die aan de Tweede Kamer zijn gestuurd gaan alleen in op de rechten van betrokkenen voor zover er sprake is van persoonsgegevens. Er zijn echter situaties denkbaar waarin er geen persoonsgegevens worden verwerkt, maar een burger toch een klacht of bezwaar wil indienen, wederhoor wil toepassen of schade heeft ondervonden. Deels valt dit binnen het domein van de GGD, in het kader van de behandelrelatie, maar in andere situaties is dat onduidelijk. Bijvoorbeeld met klachten over de app.

De Tweede Kamer kan het kabinet vragen hoe invulling wordt gegeven aan rechten die niet voortvloeien uit de AVG.

Het is niet duidelijk op welke rechten het Rathenau Instituut hier precies doelt. Voor de gevallen die hier worden verondersteld, is er een servicedesk. Deze staat mensen bij en geeft hen informatie. Wanneer de servicedesk het antwoord op een vraag niet direct weet, is er een mogelijkheid om de vraag door te geleiden.

Eindoordeel

Op dit moment is er een situatie waarbij er geen hoge risico's blijken uit beveiligings-onderzoeken en onderzoeken naar de privacybescherming. Uit de testfase zijn deze risico's ook niet gebleken. Dat betekent dat er geen zogenaamde 'showstoppers' zijn. Mij is gebleken dat de minister goed doordrongen is van de risico's en daar acteert op een manier die zeer verantwoordelijk is. Het is moeilijk te bedenken welke app vergelijkbare maatregelen kent om privacybescherming en informatiebeveiliging te borgen en ook geborgd te houden.

Alles overziende neemt de minister geen onoverwogen beslissing door met deze app te gaan beginnen. De verwachting is niet dat de beveiligingsonderzoeken die nu lopen de komende dagen opeens een radicaal ander beeld gaan opleveren. Op basis van de huidige kennis van de situatie kan ik zeggen dat deze app voor wat betreft informatiebeveiliging en privacybescherming 'fit for purpose' is. Het dringende advies is wel om na lancering te blijven doorgaan met het intensief bewaken van alle risico's en weer opnieuw risico's in kaart te brengen.

Brenno de Winter

Appendix A. Uitleg FMEA

Deze tekst is afkomstig uit 'De survivalgids voor de digtale jungle'.

Om risicomanagement goed te kunnen uitvoeren, zijn er verschillende methodes. Welke de beste is, is een kwestie van voorkeur. Iedere aanpak verschilt en in sommige gevallen zal de aanpak niet breed erkend worden. Daarom kies ik in dit boek een aanpak die wel geaccepteerd is: de Failure Mode Effect Analysis (FMEA). De reden dat ik die heb gekozen – na de nodige gesprekken met mijn sparringpartner Hans de Raad – is tweeledig. Het is de eenvoudigste methode om uit voeren. Daarnaast sluit de methodiek aan bij iets wat mensen goed kunnen, namelijk het verzinnen hoe zaken mis kunnen gaan. Daarmee vel ik geen oordeel over andere methodieken, maar kies ik dat wat laagdrempelig is.

De oorsprong van FMEA ligt bij het Amerikaanse leger. Inmiddels heeft de methodiek een plaats in het ICT-landschap. Het is niet ongebruikelijk de benadering te gebruiken voor het bepalen van risico's bij softwareontwikkeling en systeemontwerp in de zorg. Ook voor het bewaken van continuïteit in de ICT, zoals gebruikelijk in IT Service Continuity Management (ITSCM) en Business Continuity Management (BCM), sluit de methodiek goed aan. Het Europees Agentschap voor netwerk- en informatiebeveiliging, ENISA, accepteert en promoot de methodiek. Dat maakt deze manier van het inschatten van risico's voor zowel beveiliging als verplichtingen vanuit wetgeving (bijvoorbeeld de AVG) bruikbaar.

Risico's simpel maken met de foutmodus

Het proces van risicoanalyse komt voor veel mensen behoorlijk intimiderend over. Het is voor hen ingewikkeld om te bedenken welke gevaren er zijn. Het thema 'gevaar' is te groot of te ingewikkeld om effectief op te handelen. Net zoals 'het terrorisme' geen risico is om direct op te handelen. Het worden loze, nietszeggende termen, net als 'cyber'. Of zoals Hans de Raad zegt: "Het is zo omvangrijk dat we met risicobeheersing in complexe ICT-systemen het niveau van het primitieve reptielenbrein nog niet zijn ontstegen."

Het is niet erg dat deze benadering niet in onze natuur zit en dat het abstract denken risico-inschattingen lastig maakt. Mensen zijn namelijk wel goed in het zoeken naar fouten, manieren waarop beveiliging kan falen. Met andere woorden, we gaan op zoek naar de vraag: hoe zou dit mis kunnen gaan? Zo'n vraag is veel eenvoudiger te beantwoorden.

Dat ontdekte de National Aeronautics and Space Administration (NASA), de Amerikaanse overheidsorganisatie die verantwoordelijk is voor het ruimteprogramma, bij haar zoektocht om risico's goed boven tafel te krijgen. Bij het ontwikkelen van haar methodiek staan de mens en de gave om problemen te duiden centraal. De manier om dat te doen is de Failure Mode and Effects Analyses (FMEA) geworden. In deze methodiek kijken we naar de manieren waarop dingen fout kunnen gaan (de foutmodi of in het Engels de *failure modes*). Deze gaan we inschatten en van een waarde voorzien. We zijn bij die modes op zoek naar realistische problemen: zaken die fout kunnen gaan en makkelijker te verzinnen zijn dan het toch algemene begrip risico.

Na een incident maakt deze aanpak snel duidelijk of bepaalde problemen zijn onderkend of juist niet. In een recente zaak was het voorhanden hebben van deze analyse meteen een belangrijke indicator dat een bepaalde set aan problemen niet bij een organisatie op de radar was. Precies daar ging het natuurlijk wel verkeerd. Zo was eigenlijk binnen een uur de kern van het probleem helder waar dat anders veel meer zoeken was geweest.

Bij de ISO-14791-norm voor het omgaan met risico voor medische apparatuur is de FMEA-methodiek verplicht als risico-inschatting. In de ICT-industrie begint deze methodiek geaccepteerd te raken. Vooral de ENISA, de Europese organisatie voor netwerk- en informatiebeveiliging, heeft hiervan een goede uitwerking gemaakt, waarbij de Europese wet- en regelgeving is meegenomen. Voor het maken van inschattingen voor bijvoorbeeld de AVG kan deze methode heel bruikbaar zijn. Overigens kun je FMEA prima naast een andere methodiek gebruiken. Het is dan juist een aanvulling. Een nieuwe blik die meer risico's blootlegt. Alleen is het uitvoeren van een dubbele risicoanalyse naast elkaar veel extra werk en leidt dit tot twee soorten resultaten. Dat is niet erg, maar wel bewerkelijk.

Vanuit de bedachte realistische foutmodus voeren we vervolgens de risicoanalyse uit. In deze fase hangen we een waarde aan de foutmodus. Hoe hoger de waarde, des te urgenter het probleem. Wat je probeert is om de foutmodus te verhelpen, detecteerbaar te krijgen, de gevolgen te beperken of te zorgen dat het minder vaak optreedt. Zo krijg je een hanteerbare lijst met de grootste problemen bovenaan. Om zo'n inschatting te maken moet er een lijst ontstaan met iedere foutmodus die je kunt bedenken. Deze lijst kun je blijven bijwerken als je later nieuwe manieren van falen bedenkt, bijvoorbeeld op basis van een incident in het nieuws.

Met de lijst met manieren van falen in de hand, geef je een waarde aan iedere modus. We noemen het getal dat uit de analyse komt het Risk Priority Number (RPN). Het probleem is groter naarmate de waarde hoger wordt. Het RPN bestaat uit drie componenten. Alle componenten krijgen een waarde tussen bijvoorbeeld 1 en 5, waardoor er een RPN ontstaat met een waarde tussen de 1 en de 125. Maar een waarde tussen 1 en 10 zie je nog wel eens, waardoor het RPN tussen 1 en 1.000 kan variëren. Voor kleinere organisaties en simpelere processen volstaat een waarde tussen 1 en 5. Voor de overzichtelijkheid houd ik deze range aan. De methodiek is hetzelfde, maar het bespaart verder lange discussies waar iets moet worden ingeschaald.

De eerste van de drie onderdelen van het RPN is de '*severity*'. Met andere woorden, hoe ernstig is het als een foutmodus daadwerkelijk tot een incident leidt? Waarbij de waarde 1 staat voor 'totaal niet ernstig' en de waarde 5 'catastrofaal' betekent. Om het inschalen eenvoudiger te maken wordt eerst een beschrijving gemaakt die hoort bij iedere waarde. Het is verstandig hier eerst overeenstemming over te hebben en daarna pas de foutmodi te behandelen, zodat later sneller de juiste inschatting wordt gemaakt. Het maakt discussies eenvoudiger, omdat vooraf vastligt wanneer we iets ernstig vinden. Risico's worden nu aan de hand van normen en veel minder aan de hand van speculatie bepaald.

Een voorbeeld van het inkleuren van de ernst zou er zo uit kunnen zien:

Waarde	Omschrijving	Kenmerken (indien een van de criteria van toepassing is)
5	Catastrofaal	Er kunnen doden vallen. Grote delen van de administratie lekken uit. Er is schade die de continuïteit raakt (>€ 500.000). Herstel van de operatie is zeer lastig, zo niet onmogelijk (weken). Reputatieschade kan van zeer langdurige aard zijn, mogelijk zelfs permanent.
4	Zeer schadelijk	Er kunnen gewonden vallen. De persoonsgegevens van veel mensen (>100) lekken uit. Bijzondere persoonsgegevens van veel mensen lekken uit; Er is aanzienlijke schade > € 50.000 en < € 500.000. Er is brede media-aandacht, politieke aandacht. Zeer langdurige verstoring (dagen).

3	Ernstig	Er lekken bijzondere persoonsgegevens van een paar mensen (<5) uit. Er lekken grotere hoeveelheden persoonsgegevens uit (tot 100 mensen). Er is beperkt publieke aandacht. De schade is substantieel (> € 10.000 en < € 50.000); Er kunnen lichtgewonden vallen. Langdurige verstoring (>3 uur <24 uur).
2	Schadelijk	Verstoringen duren langer (tot 2-3 uur). Er lekken beperkt (minder dan 10) persoonsgegevens uit. Er is schade van > € 1.000 tot € 10.000.
1	Niet ernstig	Kleine verstoring van niet- kernprocessen (bijvoorbeeld minuten). Er lekken zeer beperkt gegevens uit. Schade is verwaarloosbare schaal (minder dan € 1.000).

Nogmaals: het ligt helemaal aan je eigen normen hoe je de kenmerken voor 'schadelijk' definieert. Waar een schade van een half miljoen voor een mkb-onderneming catastrofaal is, is dat voor een multinational niet zo. En waar bepaalde bedrijven een administratie op papier voor een paar weken niet erg vinden, legt dit een overheid of multinational plat. De normen zijn niet voor iedere organisatie hetzelfde.

De volgende factor voor de FMEA is de *'occurrence'* (voorkomen) ofwel de vraag: hoe vaak komt een incident reëel gesproken voor? Hoe vaker iets verkeerd gaat, des te meer last je ervan hebt. De schaal loopt op naarmate iets vaker voorkomt. Zo neemt het risico iets toe. Opnieuw gaan we uit van vijf categorieën.

Dat kan er bijvoorbeeld als volgt uitzien:

Waarde	Omschrijving	Criterium
5	Veelvoorkomend	Een incident komt een of meerdere malen per dag voor.
4	Regelmatig	Incidenten komen wekelijks voor.
3	Komt voor	Incidenten komen eens of meerdere malen per jaar voor.
2	Zelden	Een incident komt af en toe voor. Bijvoorbeeld eens per drie of vijf jaar.
1	Zeer zelden	Een incident treedt bijna nooit op. Het is eigenlijk onwaarschijnlijk.

De normen verschillen weer per organisatie. Waar voor een klein bedrijf een aanrijding met een auto een incident is dat zelden voorkomt, zal de politie van een grote stad zo'n incident als veelvoorkomend beschouwen.

De derde factor is de detecteerbaarheid van een falen. De gedachte daarbij is dat als je een fout eenvoudiger kunt detecteren je het sneller kunt verhelpen of de gevolgen kleiner kunt maken. Naarmate de detecteerbaarheid slechter wordt, neemt het getal toe.
Een invulling kan er zo uitzien:

Waarde	Omschrijving	Kenmerken (indien van toepassing)
5	Nagenoeg niet te detecteren	De detectie van de foutmodus is erg moeilijk of nagenoeg onmogelijk.
4	Slecht detecteerbaar	Het detecteren van de foutmodus is moeilijk.
3	Detecteerbaar	De foutmodus is met inspanning detecteerbaar
2	Doorgaans detecteerbaar	De foutmodus is goed te detecteren.
1	Altijd detecteerbaar	Als de foutmodus gaat optreden dan is dat altijd snel te detecteren

Een analyse uitvoeren

De manier waarop de risico-inschatting wordt uitgevoerd, is niet ingewikkeld. Maar hoe kun je dit goed uitvoeren? Hiervoor zijn er simpele stappen om te nemen en zelf aan de slag te gaan. De stappen maken het proces eenvoudig en geven houvast voor alles wat hierna in het boek wordt beschreven. Door dit proces te volgen is het mogelijk om de inschatting in stukken te knippen en bijvoorbeeld afdelingen, eigenaren van een systeem of processen na een deugdelijke instructie zelf een inschatting te laten maken.

Natuurlijk werkt FMEA alleen als je naar het geheel kijkt. Anders beveilig je een klein deel van een groter geheel en klopt de som van de delen niet. Het opknippen kan helpen meer onderdelen te beslaan en de juiste experts op het juiste onderdeel te zetten. Uiteindelijk moet natuurlijk alles van een systeem of proces tegen het licht worden gehouden. Zorg ervoor dat je de inschatting op het juiste moment uitvoert. Het heeft minder zin om naar risico's te kijken als je net klaar bent met het opstellen van eisen voor een systeem of net klaar bent met de introductie van het systeem. Dan is het immers lastiger om maatregelen te nemen. Had je de inschatting eerder gedaan, dan zou je de plannen nog kunnen bijstellen of maatregelen kunnen meenemen.

Via een goede FMEA kom je met deze vijf stappen tot goede beveiligingsmaatregelen:

1. Bepaal het onderwerp en de reikwijdte. Bepaal waarvoor de analyse wordt gedaan. We gaan op zoek naar de foutmodi binnen het onderwerp en de reikwijdte.
2. Zorg – als het nog niet bestaat – voor het bepalen van de norm/grens voor ernst, voorkomen en detecteerbaarheid, zodat iedereen volgens dezelfde regels de indeling maakt.
3. Stel het team van deskundigen samen. Kies mensen met verstand van het proces, het systeem en informatiebeveiliging. Vooral mensen met ervaring zijn cruciaal, omdat zij al veel verkeerd hebben zien gaan. Het is niet de bedoeling om het team vooral samen te stellen met verantwoordelijken voor risico-inschattingen of kwaliteit. Natuurlijk kan zo iemand voor begeleiding van het proces deel uitmaken van het team. De analyse moet echter worden gedaan door mensen die 'met de poten in de modder staan'.
4. Teken het proces of systeem uit. Als het proces al is uitgetekend, dan moet het team verifiëren of het proces/systeem nog altijd klopt. Is het er niet, dan moet het proces/systeem worden uitgetekend, zodat alle onderdelen inzichtelijk zijn.
5. Identificeer iedere te bedenken (realistische) foutmodus en classificeer ze volgens de normering. Dit zorgt voor de uiteindelijke lijst met foutmodi en de bijbehorende RPN's.

Na het vaststellen van de foutmodi willen we natuurlijk de RPN-waardes laten dalen. Daarvoor komen we met beveiligingsmaatregelen. Dat betekent: risico's identificeren en maatregelen kiezen. Nu de foutmodi bekend zijn, is het mogelijk om maatregelen te kiezen die een invloed hebben op de foutmodi door de detecteerbaarheid te vergroten (en een incident in de kiem te smoren), de ernst te beperken of te beperken hoe vaak een incident voorkomt. Hoe maatregelen worden gekozen, beschrijf ik later in het boek. Als we maatregelen hebben ingevoerd, nemen de risico's (foutmodi) af (maar ze verdwijnen niet!).

Gevolg geven aan een Risk Priority Number

Het Risk Priority Number (RPN) zorgt voor een handige rangschikking welke foutmodus het eerste aandacht verdient. Want hoe hoger het RPN, hoe ernstiger het risico. Wanneer de ernst hoger is, een probleem vaker voorkomt en de detecteerbaarheid laag is, dan komt er een moment waarop je zegt dat eerst de risico's kleiner moeten worden voor je verder kunt. Het is handig om daarvoor gebruik te maken van risicoklassen. Hoe hoger de klasse, des te sneller er maatregelen moeten volgen.

Zo'n tabel kan er zo uitzien:

Risico-klasse	RPN	Risico	Prioriteit/actie	Maximale duur

1	1-8	Verwaar-loosbaar	Alleen als dit relatief simpel te organiseren is.	Geen – mag geaccepteerd risico zijn
2	9-27	Mogelijk	Vraagt om aandacht	12 maanden
3	28-39	Belangrijk	Maatregelen vereist	6 maanden
4	40-60	Hoog	Directe actie noodzakelijk	1 maand
5	60+	Zeer hoog	Verwerking/systeem stoppen en eerst in actie komen	Onacceptabel / stoppen

In het voorbeeld zijn er vijf risicoklassen, waarbij de grens is getrokken bij de gemiddelde score van de drie onderdelen (ernst, voorkomen en detecteerbaarheid). Zo is voor risicoklasse 1 de grens gelegd op 2*2*2. In dit geval zeggen we voor de eerste risicoklasse dat je niet hoeft te handelen op basis van deze foutmodus. Het risico mag onbeperkt blijven bestaan. Daarmee geef je invulling aan het vinden van een balans tussen investeren in maatregelen en de bereidheid om risico te lopen. Bij de hoogste categorie (risicoklasse 5) stop je verwerking tot het risico is teruggebracht tot een acceptabel niveau.

Het werken met deze risicoklassen heeft nog wel iets onwenselijks in het systeem zitten. Stel, een foutmodus heeft catastrofale gevolgen, maar is heel zeldzaam en goed te detecteren. Dan zouden we dit als verwaarloosbaar afschrijven. Of neem de situatie van een goed detecteerbare foutmodus, die veelvoorkomend is en nog catastrofaal. Dat zouden we een RPN van 25 geven. Dat is risicoklasse 2 (mogelijk), terwijl we een risico hebben dat schreeuwt om aandacht. Catastrofale risico's zijn zo belangrijk dat je daar iets mee wilt. Daarom bepalen we vaak een critical risk of kritiek risico. In die indeling halen we de detecteerbaarheid uit het schema, want al detecteer je bijna perfect, je wilt geen 'bijna catastrofale incidenten'. Hoe weinig een incident ook voorkomt, uiteindelijk wil je geen catastrofaal incident, of continu optredende kleine incidenten. We delen de risico's daarom in met de kritieke factor: Laag, Midden, Hoog of Kritiek. Waarbij meteen duidelijk is waar risico's onacceptabel worden.

Kritieke risico matrix

	Zeer zelden	**Zelden**	**Komt voor**	**Regel-matig**	**Veelvoor-komend**
Cata-strofaal	Midden	Hoog	Hoog	Kritiek	Kritiek
Zeer schadelijk	Laag	Midden	Hoog	Hoog	Kritiek
Ernstig	Accep-tabel	Laag	Midden	Hoog	Hoog
Schadelijk	Accep-tabel	Accep-tabel	Laag	Midden	Hoog
Niet ernstig	Accep-tabel	Accep-tabel	Accep-tabel	Laag	Midden