# Notificatieapp 'CoronaMelder' – Zienswijzen van Functionarissen Gegevensbescherming GGD'en en GGD GHOR NL

## Zienswijze Conceptovereenkomst Notificatieapp VWS

### Algemene opmerkingen/ vragen

a. Het doel en de scope van de overeenkomst komt niet eenduidig naar voren. Dient middels deze overeenkomst de samenwerking tussen de GGD'en en het VWS tot stand te komen en partijen als gezamenlijke verantwoordelijke kwalificeren of is dit een dienstverleningsovereenkomst, waarin partijen eerder afspraken maken over het gebruik van de applicatie door GGD'en? In het laatste geval zou het VWS richting de GGD'en eerder als verwerker kwalificeren.

b. Als partijen als gezamenlijke verwerkingsverantwoordelijke kwalificeren dan blijkt dit niet uit de desbetreffende overeenkomst. De verhouding van de gezamenlijke verwerkingsverantwoordelijkheid is tevens niet eenduidig verdeeld. De GGD'en zouden in het kader van de notificatieapp enkel verwerkingsverantwoordelijk zijn voor wat betreft de validatiefase. Dat de GGD'en verantwoordelijk zijn voor de verwerking van persoonsgegevens bij bron- en contactopsporing is evident, maar dat valt niet onder de reikwijdte van de overeenkomst, nu de reikwijdte voor de verwerkingsverantwoordelijkheid van de GGD'en zich enkel richt op de validatiefase in de notificatieapp.

c. Het toevoegen van een bijlage waarin duidelijk alle te verwerken persoonsgegevens worden opgesomd en waarbij duidelijk wordt gemaakt welke persoonsgegevens precies wie, wanneer en hoe worden verwerkt is te adviseren. Hierdoor wordt in één oogopslag helder wie waarvoor verantwoordelijk is (nog behoudens de verdere feitelijke invulling van die verantwoordelijkheid). Ook toevoeging bijlage ten aanzien van beveiliging verdient ook aanbeveling.

d. In de conceptovereenkomst worden afspraken gemaakt voor verwerkingen, datalekken, etc. die zich 'buiten de notificatieapp' bevinden. Wat hiermee wordt bedoeld is niet duidelijk. Wat betekent als er sprake is van verwerking 'binnen' de app en verwerking 'buiten' de app? Het is relevant om waakzaam te zijn dat er geen afspraken worden gemaakt die buiten de reikwijdte van de notificatieapp en de verantwoordelijkheden van de partijen, voornamelijk de GGD'en, vallen.

e. Veel artikelen in de overeenkomst hebben een eenzijdig en verplichtend karakter. Hierdoor lijkt het meer op een gebruiksovereenkomst dan een samenwerkingsovereenkomst. Bij andere onderdelen heeft het weer meer een karakter van een verwerkersovereenkomst. Doel en scope moet scherper.

f. De toon in de conceptovereenkomst zou mogen worden verzacht, zodat de gezamenlijke verwerkingsverantwoordelijkheid van partijen meer mag blijken. Nu oogt er een mate van 'hiërarchie' tussen partijen.

g. De BCO-taak van de GGD'en is niet de grondslag voor de conceptovereenkomst inzake de notificatieapp. Dit heeft de Autoriteit Persoonsgegevens op 4 juni 2020 (ten aanzien van het oude wetsvoorstel Tijdelijke bepalingen in verband met maatregelen ter bestrijding van de epidemie van covid-19 voor de langere termijn). De AP adviseert te voorzien in een nieuwe wettelijke taak naast het eigenlijke bron-en contactonderzoek. In het uiteindelijk bij de Tweede Kamer ingediende wetsvoorstel komt de notificatieapp niet meer voor. We moeten voorkomen via de overeenkomst deze verantwoordelijk, ten onrechte, bij de GGD'en worden neergelegd.

h. De verantwoordelijkheid van de GGD'en is te breed geformuleerd. Het lijkt niet dat de GGD'en deze verantwoordelijkheid ook feitelijk kunnen waarmaken.

i. De rol van GGD GHOR Nederland als partij van de overeenkomst is niet duidelijk en komt in de overeenkomst niet naar voren. Is het de bedoeling dat GGD GHOR een contractspartij is?

j. Hoe worden GGD'en betrokken en/of geïnformeerd over besluitvormingen ten aanzien van de notificatieapp vanuit het VWS?

k. Bewaartermijnen worden in de overeenkomst niet benoemd. Hoe lang worden de gegevens bewaard? Hoe lang worden de persoonsgegevens in het portaal bewaard? Wat als het gebruik van de notificatieapp wordt beëindigd? De bewaartermijn zouden moeten doorlopen zolang persoonsgegevens worden verwerkt

   Wordt de termijn ter zake de back-up hierbij gerekend? Hoe lang is de termijn van de back-up en wat voor procedures zijn ingesteld ter zake herstel in het geval het systeem van de notificatieapp zich begeeft?

l. Informatie over het portaal waar de GGD'en gebruik van zouden maken is beperkt. Waaruit bestaat het portaal, via welke server verloopt dit? Worden daarin ook persoonsgegevens bewaard of dient het portaal enkel als een communicatielijn met de back-end server? Hoe ver reikt de toegang van de GGD in het portaal?

m. De GGD is verwerkingsverantwoordelijke bij het verwerken van de gegevens ten behoeve van bron- en contactopsporing conform de Wpg, maar de GGD is niet verwerkingsverantwoordelijke voor het verwerken van de gegevens in de app, dit betreft immers geen direct BCO, maar een AANVULLING op het BCO. De GGD is wel een verplichte gebruiker en heeft een rol in de verificatie. Er dient dus idealiter wel een gebruiksovereenkomst met VWS te zijn waarin geduid wordt wat van de GGD wordt verwacht. Een SLA met VWS is dan ook niet nodig, een verwerkersovereenkomst ook niet. Indien de app een noodzakelijke ONDERSTEUNING zou zijn in BCO (en een noodzakelijk middel voor het uitvoeren van BCO) dan zou het wel gaan om een verantwoordelijkheid van de GGD (voor het uitvoeren van haar taken onder de Wpg) en levert VWS slechts het middel. Dan zou een (verwerkers)overeenkomst en SLA wel van toepassing zijn.

n. Is gezamenlijke verwerkingsverantwoordelijkheid wel het juiste uitgangspunt, omdat GGD nauwelijks een bijdrage leveren en het doel en de middelen niet hebben bepaald? Alleen het VWS heeft de notificatieapp ontwikkeld. De GGD heeft hierin verder geen rol gehad.

o. GGD is feitelijk niet in staat om aan de rechten van betrokkenen te voldoen. De gehele datastroom is dermate sterk versleuteld dat het niet meer te achterhalen is welk record bij welke betrokkene hoort; dit geldt mogelijk zelfs voor de validatiegegevens. Mocht dit het geval zijn dan dient de notificatieapp al bij installatie aan te geven dat er niet aan de rechten van betrokkenen kan worden voldaan. Dit voorkomt (massale) verzoeken voor inzage etc. bij GGD die hier dan standaard niet aan kan voldoen.

p. Word bij de inschakeling van een derde, zoals een verwerker rekening gehouden of de verwerker of diens subverwerker servers buiten de EER heeft? Denk hierbij aan de ongeldigheidsverklaring van het Privacy Shield.

q. Tot in hoeverre zijn de GGD'en verplicht om mee te werken aan de implementatie van de notificatieapp? Bestaat er de mogelijkheid om hiervan af te zien? Kan de GGD wettelijk worden verplicht om gebruik te maken van de notificatieapp?

r. Worden gebruikers van de app ook geïnformeerd over eventueel ingeschakelde derden? Het is namelijk goed voorstellen dat er gebruikers zullen zijn die hun vraagtekens gaan plaatsen bij KPN als verwerker die gedeeltelijk het beheer van de app gaat voeren. Voor de slimmeriken die 1+1 gaan optellen zou het beeld kunnen ontstaan dat er door middel van het koppelen van locatiegegevens/verkeersgegevens van netwerkgebruikers met de codes die door bluetooth worden gegenereerd in de notificatieapplicatie, een tot personen herleidbare gegevensverwerking plaatsvindt. In de DPIA wordt dit op pagina 65 nog specifiek aangestipt als risico (door het analyseren van verkeersgegevens zou een netwerkbeheerder van bv. een telecomoperator kunnen achterhalen wie er TEKs uploaden waaruit de conclusie getrokken kan worden dat deze personen positief getest zijn op corona). Dit kan bij mensen argwaan wekken en reden zijn om de applicatie niet te gaan gebruiken. Hoe gaat men dit ondervangen?

s. De samenwerkingsovereenkomst waar Minister De Jonge op doelt in zijn brief van 24 juli jl., is dit de overeenkomst voor het gebruik van de notificatieapplicatie? Of gaat het hier om nog een geheel andere overeenkomst aangezien daarin e.e.a. geformaliseerd zou gaan worden met betrekking tot de juridische en medische verantwoordelijkheden van partijen en ook dit in de zo net besproken overeenkomst onduidelijk blijft?

## Zienswijze per artikel conceptovereenkomst VWS

**Overweging b**

- Misschien aangeven dat partijen voorafgaand afspraken maken over dataminimalisatie. En dat er in een ander document een opsomming wordt gegeven van de soort/ categorie persoonsgegevens.

- Is 'ondersteunen' bij BCO wel het juiste uitgangspunt?

  Ondersteunen klinkt hier alsof de app het bron- en contactonderzoek 'gemakkelijker' zal laten verlopen. In die zin ondersteunt de notificatieapp het bron- en contactonderzoek niet (het is niet een verlichting voor de bestaande taak), maar het draagt eerder bij aan de mogelijkheid om een groter groep mensen in beeld te krijgen die mogelijk in contact zijn geweest met een besmette persoon om zo de verspreiding van het virus zo goed mogelijk te reduceren.

  Het doel van de app lijkt eerder een 'aanvulling' op het huidige BCO.

**Overweging c**

- Moet voor het woord 'gebruik' geen definitie komen?

**Overweging d**

- De verwerkingsverantwoordelijkheid van de GGD is breed geformuleerd en volledig gestoeld op BCO. Zou dit niet genuanceerder moeten? Ten aanzien van de notificatieapp zijn de GGD'en alleen verwerkingsverantwoordelijk voor het verwerken van eventueele persoonsgegevens in de validatiefase.

**Artikel 1**

- De definitie van de notificatieapp is te breed. Er is onderscheid nodig tussen de CoronaMelder en de andere systemen (back-end server en de portal). Belangrijk voor leesbaarheid om daar onderscheid in te maken.

**Artikel 2**

- Heeft de GGD een mogelijkheid om de overeenkomst op te zeggen dan wel te ontbinden bij niet nakoming aan bijvoorbeeld de zijde van VWS ter zake het beheer van de Notificatieapp en uiteraard vice versa? Dit is momenteel niet geregeld in de overeenkomst. (2.1)

- Wat wordt verstaan onder 'definitief eindigen' van het gebruik van de notificatieapp? Wie bepaalt wanneer dit gebeurt? Alleen VWS of kan de GGD het gebruik van de notificatieapp ook definitief beëindigen? Worden hiervoor bepaalde voorwaarden gehanteerd of kan dit op ieder willekeurig moment?

**Artikel3**

- Aan de GGD niet alleen kopie van een ondertekend tekenblad verstrekken, maar ook de overeenkomst zelf.

**Artikel 4**

- Informatiebeveiliging is een aandachtspunt voor het toegang verlenen tot (achterliggende systemen) van de notificatieapp (4.1)

- Is er ook een SLA waar dit uit blijkt? En welke partij doet eigenlijk het onderhoud aan de Notificatieapp? (4.1 – beschikbaarheid van de app)

- Kunnen de GGD'en bij vragen op dit punt direct terecht bij VWS of moet dit via tussenkomst van GGD-GHOR? (4.1 – beschikbaarheid van de app)

- Misschien is een *matrix* wel handig om bij deze overeenkomst te voegen waaruit de verschillende contactmomenten volgen en tussen welke partijen. In de hiernavolgende artikelen is dit ook niet altijd even duidelijk opgeschreven naar mijn idee. (4.1 – beschikbaarheid van de app)

- Wordt hiervoor een additionele dienstverleningsovereenkomst of SLA opgesteld door VWS, zodat GGD'en kunnen verwachten dat de app aan een bepaalde standaard voldoet en met wie contact moet worden opgezocht op het moment dat de achterliggende systemen niet werken en daarmee geen gebruik kan worden gemaakt van de app? (4.1)

- Op welke wijze wordt het definitief staken en eindigen van de overeenkomst er dan gecommuniceerd richting betrokkene? Verloopt dit via de website? En uit naam van VWS? Het lijkt mij handig als Partijen dit vooraf afspreken en weten welke paden bewandeld worden. (4.2)

- Maakt VWS alleen besluit tot het beëindigen van de notificatieapp? Vooroverleg met de GGD'en is gewenst. Kan de GGD eenzijdig besluiten de notificatieapp niet meer te gebruiken? (4.2)

- Zit hier geen SLA achter? Dit wekt nu het idee van een dienstverleningsovereenkomst, maar waarbij de afspraken zeer summier zijn vastgelegd. Wat voor gevolgen heeft dit voor de GGD'en en wat betekent dit voor de 'ondersteuning' van het bron- en contactonderzoek voor de GGD'en? (4.2)

**Artikel 5**

- Waarom wordt ten aanzien van wijzigingen in overleg getreden met GGD GHOR Nederland? (5.2)

- Wat als de GGD'en het niet eens zijn met de aanpassingen/wijzigingen en/of partijen komen niet tot overeenstemming? Wat voor gevolgen heeft dit voor de GGD? Kan de GGD er voor kiezen om deze overeenkomst op te zeggen/ te beëindigen? Hoe? (5.2)

**Artikel 6**

- Wat houdt 'benodigde medewerking' van de GGD'en aan het VWS ter zake de implementatie van de app precies in? Wat wordt van de GGD'en precies verwacht? Dit moet namelijk wel haalbaar zijn per GGD rekening houdend met mankracht en kennis (6.1)

- VWS kan de implementatie uitstellen. Zijn hier bepaalde voorwaarden voor of kan dit op ieder moment? Zijn er richtlijnen hoe lang zoiets zou kunnen duren? Kunnen de GGD'en er dan voor kiezen om deze overeenkomst op te zeggen?

**Artikel 7**

- De overeenkomst stipuleert dat VWS namens de GGD'en een overeenkomst sluit met KPN als verwerker. Dit is zeer ongebruikelijk, omdat de GGD'en autonoom én zelf verantwoordelijk zijn. Uit artikel 7 blijkt ook nergens dat VWS hierbij met de GGD's overlegt. De GGD's 'machtigen' volgens deze bepaling VWS, maar op welke wijze dit dan is geschied is onduidelijk.

- Welke informatiebeveiligingsstandaarden hanteert KPN?

- Een deel van het beheer wordt bij de KPN belegd, welk deel VWS en welk deel KPN. Zijn hierover goede afspraken gemaakt?

- Beheer (KPN) en hosting (belastingdienst). Bij de laatste (belastingdienst) valt op dat niet genoemd wordt dat daar een verwerkersovereenkomst mee wordt afgesloten. Kan zijn dat dat klopt omdat de KPN het beheer doet en de hosting uitbesteed aan de belastingdienst, dan moet duidelijk zijn dat in die lijn een verwerkersovereenkomst geregeld is.

- Het gaat als het goed is alleen over back-end, niet over de applicatie. We kunnen geen verantwoordelijkheid nemen voor systemen waar we geen zeggenschap over hebben.

- Is er al een conceptovereenkomst met de verwerker KNP waar een blik op kan worden geworpen? Dit vanwege de check van het doorleggen van de juiste verplichtingen en eisen van de AVG. (7.2)

- Wordt door het VWS aan de GGD'en gerapporteerd ter zake of KPN voldoet uit de verplichtingen van de verwerkersovereenkomst, bijvoorbeeld middels een audit rapportage? Kan de GGD dit zelf opvragen bij VWS en bij wie moeten ze hiervoor precies zijn [contactpersoon?]. (7.3)

**Artikel 8**

- Hoe kunnen GGD'en aan verzoeken van hun betrokkenen voldoen?

**Artikel 9**

- Het is voor te stellen dat het goed is om voor betrokkene via de website te informeren over de rechten die er op basis van de AVG zijn. Dit kan bijv. in de vorm van een Q&A. En kan gedurende de looptijd van de overeenkomst worden aangevuld met de tot dan toe opgedane ervaring en kennis.

- Toevoeging: Iedere GGD is *zelf* verantwoordelijk. (9.1)

- Is hierin de nuancering niet ook belangrijk dat de GGD verzoeken in behandeling neemt van betrokkene ten aanzien van de persoonsgegevens die zij in het notificatieapp verwerkt (zoals de validatiefase)? En dus niet alle verzoeken van betrokkene (dit nog los van het gegeven dat feitelijk uitvoering kunnen geven aan het verzoek lastig zal zijn).

  Het VWS stelt namelijk ook verwerkingsverantwoordelijke te zijn. Voor welke persoonsgegevens is het VWS verantwoordelijk en is het dan wel aan de GGD om mogelijke verzoeken in behandeling te nemen buiten de verwerking van de GGD'en in de notificatieapp? Voor nu lijkt de formulering breed. (9.1)

- Het VWS verwijst inzake de rechten van betrokkene naar de GGD. Kan de GGD de betrokkene doorverwijzen naar het VWS? Wanneer wel en wanneer niet? (9.3)

**Artikel 10**

- Wellicht is het een goed idee om Q&A op de website te plaatsen. De GGD'en zouden op dit punt zeker moeten samenwerken en – eventueel via tussenkomst van GGD-GHOR – hun tot dan toe opgedane ervaring en kennis met elkaar te delen. Voor betrokkene ook wel fijn om eerst te website te kunnen raadplegen en niet van het kastje naar de muur te hoeven worden gestuurd. (10.2)

- De privacyverklaring zal gezamenlijk worden opgesteld, maar de wijziging worden slechts door het VWS doorgevoerd en GGD GHOR NL wordt hierover geïnformeerd.

  De GGD'en spelen dus geen rol meer bij de wijzigingen van de privacyverklaring? Wie is verantwoordelijk voor de privacyverklaring?

  Wat is de rol van GGD GHOR NL hierin precies? Waarom wordt GGD GHOR NL hierover geïnformeerd? Wellicht is het handig om dit hier specifiek te vermelden. (10.3)

**Artikel 11**

- Het lijkt erop dat het VWS als beheerder van de app verantwoordelijk is voor de opstelling van de cookieverklaring. Wat is de rol van de GGD'en hierin precies?

- Wordt er tussen Partijen nog vastgelegd om welke gegevens het precies gaat bij het plaatsen van cookies: zowel op de website als bij het gebruik van betrokkene (de burger) van de Notificatieapp? (11.1)

- De cookieverklaring zal gezamenlijk worden opgesteld, maar de wijziging worden slechts door het VWS doorgevoerd en GGD GHOR NL wordt hierover geïnformeerd.

  De GGD'en spelen dus geen rol meer bij de wijzigingen van de cookieverklaring? Wie is nu precies verantwoordelijk voor de cookies dan? Ik vermoed het VWS nu deze app ontwikkelen en in beheer hebben. Waarom stellen partijen de cookieverklaring dan samen op?

  Wat is de rol van GGD GHOR NL hierin precies? Waarom wordt GGD GHOR NL hierover geïnformeerd? Wellicht is het handig om dit hier specifiek te vermelden. (11.3)

**Artikel 12**

- Artikel 12 is zeer algemeen geformuleerd. Kan er meer inzicht worden gegeven in welke beveiligingsmaatregelen er in elk geval toegepast worden en welke normen worden gehanteerd?

- GGD'en hebben geen toegang tot deze gegevens. Enige wat GGD doet is een autorisatiecode invoeren. Dit lid zou eruit kunnen (12.2)

**Artikel 13**

- Er mist een artikel inzake de mededelingsplicht van de verwerkingsverantwoordelijke richting de betrokkene.

- Is het wenselijk dat het VWS zelfstandig de inbreuken meldt? Is dit wenselijk? Het lijkt meer voor de hand te liggen dat de betrokken GGD'en hier meer over kunnen zeggen vanwege hun betrokkenheid en de gang van zaken vanuit hun eigen werkomgeving. (13.1)

- In plaats van GGD moet dit zijn 'betrokken' GGD. Het lijkt niet nodig dat een melding wordt gedaan door VWS namens alle GGD'en bij een specifieke inbreuk. (13.1)

- Waarom wordt GGD GHOR geïnformeerd over een ontdekte inbreuk? Wat is de rol van GGD GHOR? (13.2)

- Wat wordt bedoeld met 'persoonsgegevens die worden verwerkt buiten de notificatieapp'? Als het datalek zich buiten de app voordoet, dan valt dit toch buiten de werking van deze overeenkomst? Dit hoeft niet in de overeenkomst te worden opgenomen, nu het datalek buiten de notificatieapp plaatsvindt. Overigens is deze bepaling zo breed geformuleerd, dat hier ieder datalek binnen de GGD die buiten de notificatieapp valt (dus alle andere verwerkingen binnen de GGD) onder zou vallen. Ik stel voor om de bepaling te nuanceren – voor zover mogelijk – en anders te verwijderen. (13.4)

**Artikel 15**

- Uit artikel 15 blijkt dat VWS de DPIA uitvoert. Ook dit is opmerkelijk en onwenselijk vanuit het feit dat de GGD's verwerkingsverantwoordelijke zijn. Bovendien zijn het de GGD's die de meeste medische persoonsgegevens verwerken.

- De toon van dit artikel is eenzijdig en dwingend Het is duidelijk dat het VWS de DPIA uitvoert gezien hun rol als ontwikkelaar en beheerder van de notificatieapp, maar de toon ter zake de GGD zou wellicht verzacht kunnen worden, zoals 'partijen komen overeen dat de GGD waar nodig en gewenst een bijdrage levert aan de uitvoering van de DPIA'. (15.2)

- Wellicht aanvullen dat GGD'en niet alleen volledige medewerker, maar ook input leveren aan het uitvoeren van de DPIA.

**Artikel 16**

- Waarom wordt GGD GHOR geïnformeerd over een ontvangen verzoek van de autoriteit? Wat moet GGD GHOR dan? De GGD informeren? De rol van GGD GHOR is niet duidelijk. (16.1)

- Kan het verschil tussen binnen de app en buiten de app worden toegelicht?

- Eventueel iets opnemen over onderlinge overleg en afstemming in het kader van het informeren van de autoriteit. (16.1)

- GGD informeert niet direct VWS maar met tussenkomst GGD GHOR? Het lijkt in het algemeen gezien voor zich spreken dat GGD GHOR als overkoepelend orgaan en/of als spreekbuis van de individuele GGD'en functioneert. Wellicht kan dit op een andere plek in de concept ovk worden vermeld. (16.2)

**Artikel 17**

- Dit impliceert dat er in de bepaling iets wordt gezegd over verdere verwerking, bijv. voor wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig art. 89 lid 1 AVG. Is dit nu expliciet uitgesloten of staat dit open voor de individuele GGD'en?

  Wat er ook bedoeld wordt: het is goed om dit ook zo op te schrijven zodat er niet gegist hoeft te worden naar de bedoeling van Partijen op dit punt. Vanuit het perspectief van de GGD'en als onderdeel van een gemeente is het uit kunnen voeren van wetenschappelijk onderzoek op basis van verwerkte gegevens in de Notificatieapp natuurlijk een belangrijk aspect. Kortom: wat mag wel en niet?

**Artikel 18**

- Is onderzoek verricht door VWS dat KPN zelf of anders geen subverwerkers heeft die persoonsgegevens buiten de EER, waaronder US, verwerken/ opslaan (middels het gebruik van een servers buiten de EER)?

**Artikel 19**

- Toevoeging na 'Wijzigingen' met 'en eventuele aanvullingen op'.

## Zienswijze werking Notificatieapp VWS

1. De app kan werken zonder tussenkomst van de GGD. In Duitsland (ik gebruik de app al vanaf het begin, nu ongeveer een maand) krijg je als gebruiker die besmet is een brief met een QR-code. Met die code kun je zelf de gegevens uploaden, die versleutelt je telefoon verlaten. Pas wanneer dit niet lukt kan hulp van een dienstverlener worden ingeroepen via een telefoonnummer. Dit hoeft dus niet iemand van de GGD te zijn.

2. Google verwerkt locatiegegevens wanneer je de app gebruikt. Dit is bekend bij het ministerie (zie bijlagen). Waarom dit ontkend wordt in de DPIA is mij niet bekend. Op pagina 17 van de DPIA staat: "In keeping with our privacy guidelines, Apple and Google will not receive identifying information about the user, location data, or information about any other devices the user has been in proximity of."

   Hieruit zou kunnen worden gehaald dat Google geen locatiegegevens verwerkt, de app kan alleen geactiveerd worden wanneer je de locatiegegevens activeert.

3. Het gebruik van het IP-adres is voor de werking van de app niet noodzakelijk, dus waarom wel uploaden?

4. Onvoldoende benoemd risico:
   App wordt gebruikt als voorwaarde voor toegang (bijvoorbeeld bij een feestje). Alleen toegang met groen signaal. Er wordt van uitgegaan dat iedereen zich aan de wet houdt.

5. App werkt niet (meer) op de juiste wijze is een zeer reëel risico, zoals in Duitsland in de praktijk al is geconstateerd (waarom leren we niet van landen die dit al hebben ge-implementeert).
   (zie https://www.fr.de/wissen/corona-warn-app-download-covid-19-android-fehler-funktion-kosten-google-apple-berlin-zr-13799699.html), en
   https://www.giga.de/news/corona-warn-app-manche-android-handys-warnen-nicht-vor-covid-19/.

6. BNN-tracking (wordt nu in de praktijk al toegepast).
   Ik plaats 2 of meer telefoons binnen bluetooth afstand bij een BNN'er (bijvoorbeeld: vlak bij het hek waar iemand regelmatig wandelt, of met auto/fiets naar buiten gaat), en wacht op een signaal via bluetooth dat de BNN'er verdacht is van een besmetting.

7. Social Engineering (wordt nu ook op grote schaal toegepast).

8. Depseudonimisatie, staat nu op Laag-Laag. Het ligt er aan welke encryptie wordt gebruikt. Ik zag dat er een 256 bit encryptie wordt toegepast. Onder omstandigheden niet sterk waarom geen 512, of 1024, of bijvoorbeeld Diffie Hellman. Is het RSA of een andere methode?
   Hoewel RSA erg moeilijk is te kraken door de grote getallen die gebruikt worden, zijn er in de loop der tijd toch cryptografen, hobbyisten of zelfs criminelen die de afgelopen jaren oplossingen hebben gezocht om het 'onverwoestbare' RSA toch te kunnen kraken.

   *Trial division*
   Computers kunnen heel snel zeer grote getallen met elkaar vermenigvuldigen, maar een getal (in dit geval n) ontbinden gaat veel moeilijker. Het ontbinden van n wordt ook wel trial division genoemd. Met deze methode vindt men gegarandeerd een deler van n. Op supercomputers worden met grote processoren de sleutels geprobeerd te berekenen.
   Bovendien zijn er de afgelopen jaren nieuwe methodes toegevoegd aan de computers. Voor hele grote getallen, wat bij het RSA het geval is, is er echter zeer veel tijd voor nodig. Toch is het gelukt om de 512 bits RSA-modulus te kraken. Vandaar dat men is overgestapt naar 1024 bits RSA-modulus. Dit hebben zij gedaan, omdat het benodigde werk om zo n te ontbinden nu ook exponentieel toeneemt. Zo is het steeds mogelijk om de techniek van het ontbinden een stap voor te blijven. Trial division is bij 1024 dus praktisch onmogelijk en dan ook niet bruikbaar bij RSA.

   *Brute force hacking*
   De naam zegt al genoeg. Bij brute force hacking worden geen lastige berekeningen uitgevoerd, maar probeert men simpel 'met brute kracht' alle mogelijkheden uit. Bijvoorbeeld: Er is een willekeurige klare tekst. Men codeert m aan de hand van de publieke sleutels (c = me mod n). Vervolgens controleert men of de werkelijke tekst overeenkomt met het gevonden cijfer. Indien dit gelijk aan elkaar is, dan was het goed gegokt. Theoretische zal de code eens gevonden worden, maar net als trial division kan het zeer lang duren voordat dit gevonden zal worden.

   *Number Field Sieve (NFS)*
   De getallenlichamenzeeef, in het Engels Number Field Sieve (NFS), is een manier om samengestelde getallen te ontbinden in priemfactoren. Dit is een andere techniek dan trial division en de techniek van NFS is gebaseerd op 'verschil van twee kwadraten'. Deze methode is rond 1988 ontwikkeld door John Pollard, die het zevende fermatgetal factoriseerde. Het zevende fermatgetal staat gelijk aan $2256 + 1 = 59649589127497217 \cdot 5704689200685129054721$.
   Number Field Sieve werkt als volgt: Als men de uitdrukking $x 2 - y 2$ heeft, kan men die factoriseren in $(x - y)(x + y)$. Deze techniek past men ook toe bij het getal n. De factoren moeten dus voldoen aan de voorwaarde $x 2 \equiv y 2 \pmod{n}$, want er bestaat dan een getal k zo dat $x 2 - y 2 = kn$. Hieruit volgt dat GGD(x - y, n) en GGD(x + y, n) niet-triviale factoren van n zijn. En aangezien n, het product is van twee priemgetallen p en q, blijkt de kans 2/3 dat men één van die factoren vindt op deze manier.

   Natuurlijk geldt hier: Hoe sneller de computers, hoe sneller de bewerkingen uitgevoerd kunnen worden. Er zijn echter oneindig veel priemgetallen, dus is het altijd mogelijk om snelle computers moeilijk te maken. Hoe men precies de x's en y's vindt met de NFS is met een ingewikkeld en lang algoritme.

   *Gemeenschappelijke priemfactor*

Vaak wordt een van de twee priemfactoren herhaaldelijk gebruikt en verandert men alleen de tweede priemfactor. Iedereen kan zien dat dit fout zal gaan. Met de algoritme van Euclides is van het product n gemakkelijk de overige priemgetallen met p als gemeenschappelijke priemfactor te vinden, omdat die wordt gevonden door de grootste gemeenschappelijke deler te vinden. Het is dus belangrijk om steeds twee verschillende priemgetallen te nemen.
Echter zullen er altijd wel op de wereld toevallig twee dezelfde priemgetallen gebruikt worden. Er kan zelfs hetzelfde product van priemfactoren gemaakt worden. Op allerlei plaatsen in de wereld worden immers priemfactoren voor RSA gebruikt. Onlangs is er onderzoek gedaan naar ruim zes miljoen RSA sleutels. Daaruit blijkt dat 12.000 sleutels een dezelfde gemeenschappelijke factor hadden en meer dan 70.000 dezelfde product n. Deze sleutels en producten waren allen onafhankelijk van elkaar gemaakt. Toch is kan voor de gebruikers een groot risico zijn.