Richtsnoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19

Vastgesteld op 21 april 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Vastgesteld

Versiegeschiedenis

Versie 1.1	5 mei 2020	Kleine correcties
Versie 1.0	21 april 2020	Vaststelling van de richtsnoeren

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, onder e), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "AVG" genoemd),

Gezien de EER-overeenkomst en in het bijzonder bijlage XI en protocol 37 van die overeenkomst, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

Gezien de artikelen 12 en 22 van zijn reglement van orde,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD:

1 INLEIDING EN CONTEXT

1 Overheden en particuliere actoren overwegen in het kader van de respons op de COVID-19-pandemie datagestuurde oplossingen, hetgeen op privacygebied tot ernstige bezorgdheid leidt.

2 De EDPB onderstreept 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.

3 De EDPB is er vast van overtuigd dat, wanneer voor de beheersing van de COVID-19-pandemie persoonsgegevens moeten worden verwerkt, gegevensbescherming onontbeerlijk is om vertrouwen op te bouwen, de voorwaarden te scheppen voor de maatschappelijke aanvaardbaarheid van een oplossing, en zo te garanderen dat de maatregelen hun doel treffen. Omdat het virus geen grenzen kent, lijkt het wenselijk een gemeenschappelijke Europese aanpak voor de crisis te ontwikkelen, of in ieder geval een interoperabel kader op te zetten.

4 De EDPB is in het algemeen van mening dat data en technologie voor de bestrijding van COVID-19 moeten worden gebruikt om mensen een betere positie te geven, en niet om hen te controleren, te stigmatiseren of te onderdrukken. Data en technologie kunnen weliswaar belangrijke instrumenten zijn, maar ze hebben ook intrinsieke beperkingen en kunnen slechts de effectiviteit van andere volksgezondheidsmaatregelen versterken. De algemene beginselen van effectiviteit, noodzakelijkheid en evenredigheid moeten als leidraad dienen bij alle door lidstaten of EU-instellingen getroffen maatregelen ter bestrijding van COVID-19 die gepaard gaan met de verwerking van persoonsgegevens.

5 In deze richtsnoeren verduidelijkt de EDPB de voorwaarden en beginselen die gelden voor de evenredige inzet van locatiegegevens en instrumenten voor contacttracering met twee specifieke doelen:

- het gebruik van locatiegegevens om de respons op de pandemie te ondersteunen door een model van de verspreiding van het virus op te stellen, aan de hand waarvan de algehele effectiviteit van de afzonderingsmaatregelen kan worden beoordeeld;

1 Verwijzingen naar "lidstaten" in dit document moeten worden gelezen als verwijzingen naar lidstaten van de EER.

- het traceren van contacten, om mensen ervan op de hoogte te brengen dat zij in de onmiddellijke nabijheid zijn geweest van iemand die daarna als drager van het virus is bevestigd, teneinde de besmettingsketens zo snel mogelijk te doorbreken.

6 De mate waarin apps voor contacttracering kunnen bijdragen tot de beheersing van de pandemie hangt af van vele factoren (bijvoorbeeld het percentage van de bevolking dat de apps zou moeten installeren, en criteria in termen van de nabijheid en de duur van elk van de getraceerde contacten). Bovendien moeten dergelijke apps deel uitmaken van een brede volksgezondheidsstrategie ter bestrijding van de pandemie, die onder meer inhoudt dat mensen worden getest en dat handmatig contactonderzoek wordt uitgevoerd om twijfel weg te nemen. De inzet van apps moet vergezeld gaan van ondersteunende maatregelen die ervoor zorgen dat de informatie die aan gebruikers wordt verstrekt in de juiste context wordt geplaatst en dat de waarschuwingen die de app geeft nuttig zijn voor het volksgezondheidsstelsel. Is dat niet het geval, dan is het mogelijk dat dergelijke apps niet het gewenste effect sorteren.

7 De EDPB benadrukt dat zowel de AVG als Richtlijn 2002/58/EG (de e-privacyrichtlijn) specifieke regels bevat die toestaan dat gebruik wordt gemaakt van zowel anonieme gegevens als persoonsgegevens om overheidsinstanties en andere actoren op nationaal en EU-niveau te ondersteunen bij het bewaken en indammen van de verspreiding van SARS-CoV-2[2].

8 In dit verband heeft de EDPB al een standpunt ingenomen over het feit dat het gebruik van apps voor contacttracering vrijwillig moet zijn en niet gebaseerd mag zijn op het volgen van de verplaatsingen van een individuele persoon, maar op informatie over de nabijheid van gebruikers[3].

[2] Zie de eerdere verklaring van de EDPB over de COVID 19-uitbraak.
[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 GEBRUIK VAN LOCATIEGEGEVENS

2.1 Bronnen van locatiegegevens

9 De twee belangrijkste bronnen van locatiegegevens die beschikbaar zijn voor het modelleren van de verspreiding van het virus en de algehele effectiviteit van de afzonderingsmaatregelen zijn:

- de locatiegegevens die aanbieders van elektronische-communicatiediensten (zoals exploitanten van mobiele telecommunicatie) verzamelen bij het verlenen van hun diensten; en
- de locatiegegevens die aanbieders van diensten van de informatiemaatschappij verzamelen bij toepassingen waarvan de functionaliteit vereist dat dergelijke gegevens worden gebruikt (zoals navigatie- en vervoersdiensten).

10 De EDPB herinnert eraan dat de locatiegegevens[4] die door aanbieders van elektronische communicatie worden verzameld, uitsluitend mogen worden verwerkt voor de doeleinden genoemd in de artikelen 6 en 9 van de e-privacyrichtlijn. Dit houdt in dat deze gegevens alleen mogen worden doorgezonden naar autoriteiten of andere derden als zij door de aanbieder zijn geanonimiseerd of, wanneer het gaat om gegevens die de geografische positie van de eindapparatuur van een gebruiker aangeven (die geen verkeersgegevens zijn), als de gebruikers van tevoren toestemming hebben gegeven[5].

11 Wat betreft informatie, met inbegrip van locatiegegevens, die rechtstreeks vanuit de eindapparatuur wordt verzameld, is artikel 5, lid 3, van de e-privacyrichtlijn van toepassing. Derhalve is het slechts toegestaan informatie op het toestel van de gebruiker op te slaan of toegang tot reeds opgeslagen informatie te verkrijgen indien i) de gebruiker daarvoor toestemming[6] heeft gegeven of ii) de opslag en/of de toegang strikt noodzakelijk is voor de levering van een uitdrukkelijk door de gebruiker gevraagde dienst van de informatiemaatschappij.

12 Afwijking van de rechten en verplichtingen waarin de e-privacyrichtlijn voorziet, is evenwel mogelijk op grond van artikel 15, wanneer dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is voor het bereiken van bepaalde doelstellingen[7].

13 Voor het hergebruik van locatiegegevens die door een aanbieder van diensten van de informatiemaatschappij worden verzameld (bv. via het besturingssysteem of een eerder geïnstalleerde toepassing) ten behoeve van modellering, moet aan aanvullende voorwaarden worden voldaan. Wanneer gegevens zijn verzameld in overeenstemming met artikel 5, lid 3, van de e-privacyrichtlijn, mogen zij alleen verder worden verwerkt na aanvullende toestemming van de betrokkene of op grond van Unie- of lidstatelijk recht in het kader van een maatregel die in een democratische samenleving noodzakelijk en evenredig is om de in artikel 23, lid 1, AVG genoemde doelstellingen te waarborgen[8].

2.2 Voorkeur voor het gebruik van geanonimiseerde locatiegegevens

14 De EDPB benadrukt dat bij het gebruik van locatiegegevens altijd de voorkeur moet worden gegeven aan verwerking van geanonimiseerde gegevens boven de verwerking van persoonsgegevens.

---

[4] Zie artikel 2, punt c), van de e-privacyrichtlijn.
[5] Zie de artikelen 6 en 9 van de e-privacyrichtlijn.
[6] Toestemming behoudt in de e-privacyrichtlijn dezelfde betekenis als in de AVG en moet voldoen aan alle vereisten voor toestemming die zijn opgenomen in artikel 4, punt 11, en artikel 7 AVG.
[7] Zie voor de uitlegging van artikel 15 van de e-privacyrichtlijn ook het arrest van het HvJ-EU van 29 januari 2008 in zaak C-275/06 Productores de Música de España (Promusicae) / Telefónica de España SAU.
[8] Zie punt 1.5.3 van de richtsnoeren 1/2020 betreffende de verwerking van persoonsgegevens in het kader van verbonden voertuigen.

15 Met anonimisering wordt gedoeld op het gebruik van een reeks technieken die het onmogelijk maken om gegevens met een "redelijke" inspanning te koppelen aan een geïdentificeerde of identificeerbare natuurlijke persoon. Bij deze "redelijkheidstoets" moet rekening worden gehouden met zowel objectieve aspecten (vereiste tijd en technische middelen) als contextuele elementen die per geval kunnen verschillen (zoals zeldzaamheid van een verschijnsel, populatiedichtheid, aard en volume van de gegevens). Als de gegevens niet door deze toets komen, zijn ze niet geanonimiseerd en blijft de AVG er dus op van toepassing.

16 Of de anonimisering voldoende robuust is, wordt beoordeeld aan de hand van drie criteria: i) of het op basis van de gegevens mogelijk is een individu apart te nemen (te isoleren binnen een grotere groep); ii) of het mogelijk is twee records betreffende eenzelfde persoon te koppelen; en iii) of uit de gegevens met een significante waarschijnlijkheid nog onbekende informatie over een persoon kan worden afgeleid.

17 De term anonimisering kan verkeerd worden begrepen, en wordt vaak verward met pseudonimisering. Geanonimiseerde gegevens mogen zonder enige beperking worden gebruikt, maar op gepseudonimiseerde gegevens blijft de AVG van toepassing.

18 Er zijn veel mogelijkheden om gegevens doeltreffend te anonimiseren[9], maar er is wel een voorbehoud. Gegevens kunnen niet op zichzelf worden geanonimiseerd, wat wil zeggen dat alleen datasets in hun geheel al dan niet kunnen worden geanonimiseerd. Bewerkingen van één enkel gegevenspatroon (door middel van versleuteling of een andere mathematische bewerking) kunnen dus hooguit als pseudonimisering worden beschouwd.

19 Anonimiseringsprocessen en re-identificatiepogingen zijn terreinen waarop actief onderzoek plaatsvindt. Voor elke verwerkingsverantwoordelijke die van anonimiseringsoplossingen gebruikmaakt, is het cruciaal om de laatste ontwikkelingen op dit gebied bij te houden, met name wat betreft (van telecomexploitanten en/of diensten van de informatiemaatschappij afkomstige) locatiegegevens, waarvan algemeen bekend is dat zij moeilijk te anonimiseren zijn.

20 Uit veel onderzoeken is namelijk gebleken[10] dat *locatiegegevens die als anoniem worden beschouwd*, dat mogelijk in feite niet zijn. De sporen die personen over hun mobiliteit achterlaten, zijn inherent sterk gecorreleerd en uniek. Daardoor kunnen zij in bepaalde omstandigheden vatbaar zijn voor pogingen tot re-identificatie.

21 Een enkel gegevenspatroon waarmee de locatie van een persoon gedurende een significante periode wordt getraceerd, kan niet volledig worden geanonimiseerd. Dat kan nog steeds het geval zijn als de nauwkeurigheid van de geregistreerde geografische coördinaten niet voldoende wordt gereduceerd, of als gegevens uit het spoor worden verwijderd, en zelfs als alleen locaties waar de betrokkene lange tijd verblijft, worden bewaard. Dit geldt ook voor locatiegegevens die ondeugdelijk zijn geaggregeerd.

22 Om locatiegegevens te anonimiseren, moeten ze zorgvuldig zodanig worden verwerkt dat ze aan de redelijkheidstoets kunnen voldoen. De verwerking houdt in dit verband ook in dat locatiedatasets in hun geheel in overweging moeten worden genomen en dat gegevens van een voldoende groot aantal personen moeten worden bewerkt met de beschikbare robuuste anonimiseringstechnieken, waarbij geldt dat deze adequaat en doeltreffend moeten worden toegepast.

23 Gezien de complexiteit van anonimiseringsprocessen moet transparantie met betrekking tot de anonimiseringsmethode sterk worden aangemoedigd.

---

[9] (de Montjoye et al., 2018) "On the privacy-conscientious use of mobile phone data".
[10] (de Montjoye et al., 2013) "Unique in de Crowd: The privacy bounds of human mobility" en (Pyrgelis et al., 2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data".

3 APPS VOOR CONTACTTRACERING

3.1 Algemene juridische analyse

24 Het systematisch en grootschalig monitoren van de locatie van en/of de contacten tussen natuurlijke personen is een ernstige inbreuk op hun privacy. Die kan alleen worden gelegitimeerd als de betrokkenen de app vrijwillig gebruiken voor elk van de respectieve doeleinden. In het bijzonder houdt dat in dat personen die geen gebruik willen of kunnen maken van dergelijke apps, daarvan geen enkel nadeel mogen ondervinden.

25 Met het oog op verantwoording moet de verwerkingsverantwoordelijke van elke app voor contacttracering duidelijk worden aangegeven. De EDPB meent dat de nationale gezondheidsautoriteiten als verwerkingsverantwoordelijken zouden kunnen optreden[11], maar ook andere verwerkingsverantwoordelijken kunnen in aanmerking komen. Als bij de inzet van apps voor contacttracering verschillende actoren betrokken zijn, moeten in ieder geval hun taken en verantwoordelijkheden van meet af aan duidelijk worden vastgesteld en aan de gebruikers worden uitgelegd.

26 Gezien het beginsel van doelbinding moeten de doelstellingen bovendien voldoende specifiek zijn om uit te sluiten dat verdere verwerking plaatsvindt voor doeleinden die geen verband houden met de beheersing van de COVID-19-crisis (bijvoorbeeld commerciële of rechtshandhavingsdoeleinden). Zodra de doelstelling duidelijk is vastgesteld, moet ervoor worden gezorgd dat het gebruik van persoonsgegevens passend, noodzakelijk en evenredig is.

27 In het kader van een app voor contacttracering moet zorgvuldig rekening worden gehouden met de beginselen van minimale gegevensverwerking en gegevensbescherming door ontwerp en door standaardinstellingen:

- voor apps voor contacttracering hoeft de locatie van individuele gebruikers niet te worden getraceerd. In plaats daarvan moeten nabijheidsgegevens worden gebruikt;
- apps voor contacttracering kunnen werken zonder directe identificatie van personen, en derhalve moeten passende maatregelen worden genomen om re-identificatie te voorkomen;
- de verzamelde informatie moet worden opgeslagen op de eindapparatuur van de gebruiker en alleen relevante informatie moet worden verzameld, wanneer dat absoluut noodzakelijk is.

28 Wat de rechtmatigheid van de verwerking betreft, merkt de EDPB op dat er bij apps voor contacttracering sprake is van opslag van en/of toegang tot informatie die reeds is opgeslagen in de eindapparatuur, en dat bijgevolg artikel 5, lid 3, van de e-privacyrichtlijn van toepassing is. Indien deze bewerkingen strikt noodzakelijk zijn voor de verlening van een door de gebruiker uitdrukkelijk gevraagde dienst door de aanbieder van de app, is voor de verwerking de toestemming van de gebruiker niet vereist. Voor bewerkingen die niet strikt noodzakelijk zijn, moet de aanbieder de toestemming van de gebruiker vragen.

29 Voorts merkt de EDPB op dat het loutere feit dat apps voor contacttracering op vrijwillige basis worden gebruikt, niet betekent dat de verwerking van persoonsgegevens noodzakelijkerwijs op basis van toestemming zal plaatsvinden. Wanneer overheidsinstanties een dienst verlenen op basis van een mandaat dat is toegewezen door middel van en in overeenstemming met de wettelijke voorschriften, lijkt de noodzaak van de vervulling van een taak van algemeen belang (artikel 6, lid 1, onder e), AVG) de meest relevante rechtsgrondslag voor de verwerking.

30 In artikel 6, lid 3, AVG wordt verduidelijkt dat de rechtsgrond voor de in artikel 6, lid 1, onder e), bedoelde verwerking moet worden vastgesteld bij Unierecht of bij lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. Het doel van de verwerking moet in die

[11] Zie ook de "Richtsnoeren in verband met gegevensbescherming voor apps ter ondersteuning van de bestrijding van de COVID-19-pandemie", Europese Commissie, 16.4.2020, C(2020) 2523 final.

rechtsgrond worden vastgesteld of moet met betrekking tot de in lid 1, onder e), bedoelde verwerking noodzakelijk zijn voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend[12].

31 De rechtsgrondslag of de wettelijke maatregel die de wettige basis vormt voor het gebruik van apps voor contacttracering moet echter in zinvolle waarborgen voorzien, waaronder een verwijzing naar het vrijwillige karakter van het gebruik van de app. Er moeten een duidelijke omschrijving van het doel en uitdrukkelijke beperkingen op het verdere gebruik van persoonsgegevens in worden opgenomen en de verwerkingsverantwoordelijke(n) moet(en) duidelijk worden vermeld. Tevens moet worden vastgesteld welke categorieën persoonsgegevens aan welke entiteiten en voor welke doeleinden mogen worden bekendgemaakt. Afhankelijk van het interferentieniveau moet in aanvullende waarborgen worden voorzien, rekening houdend met de aard, het toepassingsgebied en de doeleinden van de verwerking. Tot slot beveelt de EDPB ook aan om, zo snel als praktisch mogelijk is, er de criteria in op te nemen aan de hand waarvan wordt bepaald wanneer de app buiten gebruik wordt gesteld, alsmede de entiteit die verantwoordelijk en aansprakelijk is voor het nemen van het besluit daartoe.

32 Indien de gegevensverwerking echter plaatsvindt op een andere rechtsgrondslag, zoals toestemming (artikel 6, lid 1, onder a))[13], moet de verwerkingsverantwoordelijke ervoor zorgen dat aan de strikte voorwaarden voor de toepassing van die rechtsgrondslag is voldaan.

33 Het gebruik van een app ter bestrijding van de COVID-19-pandemie kan er bovendien toe leiden dat gezondheidsgegevens worden verzameld (bijvoorbeeld over de toestand van een besmette persoon). De verwerking van dergelijke gegevens is toegestaan wanneer de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid en voldaan wordt aan de voorwaarden van artikel 9, lid 2, onder i), AVG[14], en wanneer de verwerking noodzakelijk is voor doeleinden op het gebied van gezondheidszorg, zoals beschreven in artikel 9, lid 2, onder h), AVG[15]. Afhankelijk van de rechtsgrondslag kan de verwerking ook gebaseerd zijn op uitdrukkelijke toestemming (artikel 9, lid 2, onder a), AVG).

34 In overeenstemming met het oorspronkelijke doel voorziet artikel 9, lid 2, onder j), AVG ook in de mogelijkheid om gezondheidsgegevens te verwerken wanneer dat nodig is voor wetenschappelijk onderzoek of voor statistische doeleinden.

35 De huidige gezondheidscrisis mag niet worden aangegrepen om onevenredige termijnen voor de bewaring van gegevens toe te staan. Wat de beperking van de opslag betreft, moeten de werkelijke behoeften en de medische relevantie in aanmerking worden genomen (hieronder vallen ook epidemiologisch relevante overwegingen inzake de incubatietijd e.d.). De persoonsgegevens mogen slechts worden bewaard voor de duur van de COVID-19-crisis; daarna geldt als algemene regel dat alle persoonsgegevens moeten worden gewist of geanonimiseerd.

36 De EDPB gaat ervan uit dat dergelijke apps slechts ondersteuning bieden, en niet in de plaats kunnen komen van handmatig contactonderzoek door gekwalificeerd personeel op het gebied van de volksgezondheid, dat kan nagaan of het waarschijnlijk is dat nauw contact al dan niet zal resulteren in overdracht van het virus (bv. bij interactie met een persoon die over adequate beschermingsmiddelen beschikt, zoals kassapersoneel). De EDPB benadrukt dat de procedures en processen, met inbegrip van de algoritmen die door de contacttraceringsapps worden toegepast, onder strikt toezicht van gekwalificeerd personeel moeten staan, zodat het

---

[12] Zie overweging 41.

[13] Verwerkingsverantwoordelijken (met name overheidsinstanties) moeten bijzondere aandacht schenken aan het feit dat toestemming niet kan worden geacht vrijelijk te zijn verleend als de betrokkene niet echt de keuze heeft om zijn toestemming zonder nadelige gevolgen te weigeren of in te trekken.

[14] De verwerking moet gebaseerd zijn op Unierecht of lidstatelijk recht dat voorziet in passende en specifieke maatregelen ter bescherming van de rechten en vrijheden van de betrokkene, met name het beroepsgeheim.

[15] Zie artikel 9, lid 2, onder h), AVG.

aantal fout-positieve en fout-negatieve resultaten wordt beperkt. Met name mag advies over de volgende stappen niet uitsluitend op geautomatiseerde verwerking worden gebaseerd.

37 Om te waarborgen dat algoritmen eerlijk functioneren en om voor verantwoording en, meer in het algemeen, naleving van de wetgeving te zorgen, moeten die algoritmen controleerbaar zijn en regelmatig door onafhankelijke deskundigen worden getoetst. De broncode van de app moet publiekelijk toegankelijk zijn, zodat zo veel mogelijk mensen die kunnen controleren.

38 Fout-positieve resultaten zullen altijd in zekere mate voorkomen. Het feit dat een infectierisico is vastgesteld, kan een grote impact hebben op iemand, bijvoorbeeld doordat die persoon mogelijk in afzondering zal moeten blijven totdat hij of zij negatief is getest. Daarom is het noodzakelijk dat gegevens en/of latere analyseresultaten kunnen worden gecorrigeerd. Dit moet uiteraard alleen gelden voor scenario's en implementaties waarbij gegevens worden verwerkt en/of opgeslagen op zo'n manier dat een dergelijke correctie technisch haalbaar is, en waarbij de genoemde schadelijke effecten met een zekere waarschijnlijkheid kunnen plaatsvinden.

39 Tot slot is de EDPB van mening dat, voordat zo'n app wordt ingevoerd, een gegevensbeschermingseffectbeoordeling noodzakelijk is, gezien het feit dat de verwerking waarschijnlijk met een hoog risico gepaard gaat (verwerking van gegevens inzake gezondheid, verwachte grootschalige toepassing, systematisch toezicht, gebruik van nieuwe technologische oplossingen)[16]. De EDPB beveelt ten zeerste aan om dergelijke gegevensbeschermingseffectbeoordelingen te publiceren.

3.2 Aanbevelingen en functionele vereisten

40 Volgens het beginsel van minimale gegevensverwerking (naast andere maatregelen inzake gegevensbescherming door ontwerp en door standaardinstellingen[17]) mag slechts het strikte minimum aan gegevens worden verwerkt. De app mag geen irrelevante of niet-noodzakelijke informatie verzamelen, zoals burgerlijke staat, communicatiekenmerken, inhoud van mappen op het apparaat, berichten, gespreksoverzichten, locatiegegevens, apparaatidentificatoren en dergelijke.

41 De gegevens die door de apps worden verzonden, mogen slechts een aantal voor de app specifieke en erdoor gegenereerde unieke en pseudonieme identificatoren bevatten. Die identificatoren moeten regelmatig worden vernieuwd, met een frequentie die verenigbaar is met het doel om de verspreiding van het virus te voorkomen, en moeten voldoende zijn om het risico van identificatie en fysieke tracering van personen te beperken.

42 Bij de implementatie voor contacttracering kan een gecentraliseerde of een gedecentraliseerde aanpak worden gevolgd[18]. Beide opties moeten als geschikt worden beschouwd, mits passende veiligheidsmaatregelen worden getroffen, en beide hebben een aantal voor- en nadelen. De conceptuele fase van de ontwikkeling van de app moet dus altijd een grondige overweging van beide concepten omvatten, waarbij de respectieve impact op gegevensbescherming/privacy en de potentiële gevolgen voor de rechten van personen zorgvuldig tegen elkaar worden afgewogen.

43 Op elke server die deel uitmaakt van het systeem voor contacttracering mogen slechts de contactgeschiedenis of de pseudonieme identificatoren worden verzameld van een gebruiker die als besmet is gediagnosticeerd, nadat de gezondheidsautoriteiten een gedegen beoordeling

---

[16] Zie de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679 (Groep artikel 29, bekrachtigd door de EDPB).

[17] Zie Richtsnoeren 4/2019 inzake artikel 25 – Gegevensbescherming door ontwerp en door standaardinstellingen (EDPB).

[18] De gedecentraliseerde oplossing is in het algemeen meer in overeenstemming met het beginsel van minimale gegevensverwerking.

hebben verricht, en alleen als de gebruiker vrijwillig actie heeft ondernomen. Als alternatief kan op de server een lijst worden bijgehouden van pseudonieme identificatoren van besmette gebruikers, of hun contactgeschiedenis, zolang als nodig is om mogelijk besmette gebruikers van hun blootstelling op de hoogte te brengen, maar er mag niet worden getracht mogelijk besmette gebruikers te identificeren.

44 Het invoeren van een globale methode voor contacttracering waarvan zowel apps als handmatig contactonderzoek deel uitmaken, kan in sommige gevallen vereisen dat aanvullende informatie wordt verwerkt. In deze context moet deze aanvullende informatie op de gebruikersterminal blijven en mag deze alleen worden verwerkt wanneer dat strikt noodzakelijk is, en met voorafgaande specifieke toestemming van de gebruiker.

45 Er moeten geavanceerde cryptografische technieken worden toegepast om zowel de op de servers en in de apps opgeslagen gegevens als de uitwisseling van gegevens tussen de apps en de server op afstand te beveiligen. Ook moet er wederzijdse authenticatie tussen de app en de server worden uitgevoerd.

46 Om gebruikers die als besmet met SARS-CoV-2 zijn aangemerkt, in de app te melden, moet passende autorisatie vereist zijn, bijvoorbeeld door middel van een code voor eenmalig gebruik die gekoppeld is aan een pseudonieme identiteit van de besmette persoon en aan een teststation of een professionele zorgverstrekker. Indien niet op veilige wijze bevestiging kan worden verkregen, mag geen verwerking van gegevens plaatsvinden waarbij van de geldigheid van de status van de gebruiker wordt uitgegaan.

47 De verwerkingsverantwoordelijke moet in samenwerking met de overheid duidelijke en expliciete informatie geven over de link waarmee de officiële nationale app voor contacttracering kan worden gedownload, om het risico te beperken dat gebruik wordt gemaakt van een app van een derde.

4 CONCLUSIE

48 Wij worden momenteel geconfronteerd met een ernstige volksgezondheidscrisis die een krachtige respons vereist. De gevolgen van deze respons zullen zich ook buiten deze noodsituatie doen voelen. Geautomatiseerde gegevensverwerking en digitale technologieën kunnen essentiële onderdelen zijn van de strijd tegen COVID-19. We moeten er echter voor oppassen dat we nu geen maatregelen nemen die later niet kunnen worden teruggedraaid. Het is onze taak ervoor te zorgen dat elke maatregel die in deze buitengewone omstandigheden wordt genomen, noodzakelijk is, in de tijd beperkt blijft en onderworpen wordt aan effectieve periodieke toetsing en aan wetenschappelijke beoordeling.

49 De EDPB benadrukt dat het niet zo mag zijn dat we moeten kiezen tussen enerzijds een efficiënte respons op de crisis en anderzijds de bescherming van onze grondrechten: beide doelen kunnen worden bereikt, en bovendien kunnen de beginselen van gegevensbescherming een zeer belangrijke rol spelen in de strijd tegen het virus. De Europese wetgeving inzake gegevensbescherming maakt verantwoord gebruik van persoonsgegevens ten behoeve van de gezondheidszorg mogelijk en zorgt er tevens voor dat individuele rechten en vrijheden daarbij niet worden aangetast.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)

BIJLAGE -- APPS VOOR CONTACTTRACERING LEIDRAAD VOOR ANALYSE

0. Afwijzing van aansprakelijkheid

De volgende leidraad is prescriptief noch uitputtend en heeft als enig doel algemene richtsnoeren te verstrekken voor het ontwerpen en implementeren van apps voor contacttracering. Andere dan de hier beschreven oplossingen zijn mogelijk en kunnen rechtmatig zijn mits ze in overeenstemming zijn met het toepasselijke rechtskader (de AVG en de e-privacyrichtlijn).

Deze leidraad is algemeen van aard. Dit betekent dat het kader van aanbevelingen en verplichtingen die in dit document zijn opgenomen, niet als uitputtend mag worden beschouwd. Elk geval moet afzonderlijk worden beoordeeld en het is mogelijk dat voor bepaalde apps aanvullende maatregelen nodig zijn die niet in deze leidraad zijn opgenomen.

1. Samenvatting

In veel lidstaten wordt overwogen om apps voor *contacttracering** in te zetten waarmee mensen kunnen nagaan of zij contact hebben gehad met een met SARS-CoV-2* besmette persoon.

Er is nog niet vastgesteld aan welke voorwaarden deze apps moeten voldoen om effectief bij te dragen aan het aanpakken van de pandemie. Deze voorwaarden moeten voorafgaand aan de implementatie van de apps worden vastgesteld. Om de bescherming van persoonsgegevens al vroeg in het ontwerpstadium te waarborgen, moeten de ontwikkelingsteams echter al vooraf over de nodige informatie kunnen beschikken. Hiervoor zijn richtsnoeren van belang.

Deze leidraad is algemeen van aard. Dit betekent dat het kader van aanbevelingen en verplichtingen die in dit document zijn opgenomen, niet als uitputtend mag worden beschouwd. Elk geval moet afzonderlijk worden beoordeeld en het is mogelijk dat voor bepaalde apps aanvullende maatregelen nodig zijn die niet in deze leidraad zijn opgenomen. Deze leidraad heeft als enig doel algemene richtsnoeren te verstrekken voor het ontwerpen en implementeren van apps voor contacttracering.

Het is mogelijk dat bepaalde criteria verder gaan dan de strikte vereisten die voortvloeien uit het gegevensbeschermingskader. In het belang van de maatschappelijke acceptatie van apps voor contacttracering moeten deze criteria het hoogste niveau van transparantie waarborgen.

Met het oog daarop moeten de aanbieders van de apps de volgende criteria in acht nemen.

- Het gebruik van de apps moet strikt vrijwillig zijn en mag geen voorwaarde zijn voor de toegang tot wettelijk gegarandeerde rechten. Personen moeten te allen tijde volledige controle over hun gegevens hebben en moeten vrij kunnen beslissen om zo'n app te gebruiken.
- Verwacht wordt dat apps voor contacttracering een hoog risico voor de rechten en vrijheden van natuurlijke personen inhouden en aan een gegevensbeschermingseffectbeoordeling moeten worden onderworpen alvorens te worden uitgerold.
- De apps kunnen informatie over de nabijheid tussen gebruikers verzamelen zonder hen te lokaliseren, en hebben dus geen locatiegegevens nodig.
- Wanneer is vastgesteld dat een gebruiker besmet is met SARS-CoV-2, moeten alleen de personen op de hoogte worden gebracht met wie de gebruiker nauw contact heeft gehad

binnen de bewaarperiode die epidemiologisch relevant is voor het traceren van contacten.

- Afhankelijk van de gekozen architectuur kan voor dit soort app een gecentraliseerde server nodig zijn. In dat geval moeten de door de gecentraliseerde server verwerkte gegevens – in overeenstemming met de beginselen van minimale gegevensverwerking en gegevensbescherming door ontwerp – tot het strikte minimum worden beperkt:
    - Gebruikers die als besmet zijn gediagnosticeerd, moeten toestemming geven voor het verzamelen van informatie over hun eerdere nauwe contacten of door hun app uitgezonden identificatoren. Er moet een verificatiemethode worden vastgesteld die, zonder de gebruiker te identificeren, kan bevestigen dat de persoon inderdaad besmet is. Dit is technisch gezien mogelijk, door contacten pas na de tussenkomst van een professionele zorgverstrekker op de hoogte te brengen, bijvoorbeeld door gebruik te maken van een speciale eenmalige code.
    - De op de centrale server opgeslagen informatie mag niet van dien aard zijn dat de verwerkingsverantwoordelijke gebruikers die als besmet zijn gediagnosticeerd of die contact met zulke gebruikers hebben gehad, kan identificeren, of dat er contactpatronen uit kunnen worden afgeleid die niet noodzakelijk zijn om de relevante contacten te bepalen.
- Voor de werking van dit type apps moeten gegevens worden uitgezonden die door apparaten van andere gebruikers worden gelezen en moeten de uitgezonden gegevens worden beluisterd:
    - Het is voldoende om pseudonieme identificatoren tussen de mobiele apparaten van de gebruikers (computers, tablets, geconnecteerde horloges, enz.) uit te wisselen, bijvoorbeeld door deze uit te zenden (bijvoorbeeld via Bluetooth Low Energy).
    - De identificatoren moeten worden gegenereerd door de meest geavanceerde cryptografische processen.
    - De identificatoren moeten regelmatig worden vernieuwd ter beperking van het risico van aanvallen op het gebied van fysieke tracering en linkage (pogingen tot re-identificatie van personen in een geanonimiseerde datareeks door die gegevens te combineren met een andere dataset).
- Om de veiligheid van de technische processen te waarborgen, moet dit soort apps worden beveiligd, met name met betrekking tot het volgende:
    - De app mag de gebruikers geen informatie verstrekken waaruit zij de identiteit of de diagnose van anderen kunnen afleiden. De centrale server mag geen gebruikers identificeren en geen informatie over hen afleiden.

Afwijzing van aansprakelijkheid: de bovenstaande beginselen hebben uitsluitend betrekking op wat als doel van apps voor *contacttracering* wordt opgegeven, namelijk het automatisch informeren van mensen die mogelijk aan het virus zijn blootgesteld (zonder deze te identificeren).De exploitanten van de app en de betrokken infrastructuur kunnen door de bevoegde toezichthoudende autoriteit worden gecontroleerd. Het volledig of gedeeltelijk volgen van deze richtsnoeren volstaat niet om volledig aan de gegevensbeschermingsregels te voldoen.

2. Definities

Contact	In het kader van apps voor contacttracering wordt met “contact” een gebruiker bedoeld die betrokken was bij een interactie met een als drager van het virus gediagnosticeerde gebruiker, waarbij de interactie vanwege de duur en de afstand tussen de betrokkenen een risico op een significante blootstelling aan de virusinfectie inhield. De parameters voor de duur van de blootstelling en de afstand tussen de betrokken personen moeten worden bepaald door de gezondheidsautoriteiten en kunnen in de app worden opgenomen.
Locatiegegevens	Dit zijn alle gegevens die in een elektronischecommunicatienetwerk of door een elektronischecommunicatiedienst worden verwerkt, en die aangeven waar de eindapparatuur van een gebruiker van een voor het publiek beschikbare elektronischecommunicatiedienst (zoals gedefinieerd in de e-privacyrichtlijn) zich bevindt, alsook gegevens uit eventuele andere bronnen over: - de locatie van de eindapparatuur (lengtegraad, breedtegraad, hoogte); - de richting waarin de gebruiker zich beweegt, of - het tijdstip waarop de locatiegegevens geregistreerd zijn.
Interactie	In het kader van apps voor contacttracering wordt met “interactie” bedoeld de uitwisseling van informatie tussen twee apparaten die zich dicht bij elkaar bevinden (in tijd en ruimte), binnen het bereik van de gebruikte communicatietechnologie (bv. Bluetooth). De locatie van de twee bij de interactie betrokken gebruikers valt niet onder deze definitie.
Virusdrager	In dit document wordt met “virusdrager” bedoeld een gebruiker die positief is getest op het virus en een officiële diagnose heeft gekregen van een arts of een gezondheidscentrum.
Contacttracering	Personen die (volgens door epidemiologen vast te stellen criteria) nauw contact hebben gehad met een met het virus besmette persoon, lopen een significant risico zelf ook besmet te zijn en anderen op hun beurt te besmetten. Contacttracering is een ziektebestrijdingsmethode waarmee een lijst wordt opgemaakt van de personen die zich in de onmiddellijke nabijheid van een virusdrager hebben bevonden, om na te gaan of zij eventueel besmet zijn en om passende maatregelen voor hun behandeling te nemen.

3. Algemeen

GEN-1	De app moet een aanvulling zijn op traditionele technieken voor het traceren van contacten (met name gesprekken met besmette personen), d.w.z. deel uitmaken van een breder volksgezondheidsprogramma. De app mag uitsluitend worden gebruikt totdat de handmatige traceringstechnieken volstaan om het aantal nieuwe besmettingen te beheersen.

GEN-2	Ten laatste wanneer de bevoegde overheidsinstanties groen licht geven voor de hervatting van het normale leven, moet er een procedure worden ingesteld om de verzameling van identificatoren stop te zetten (volledige deactivering van de app, instructies om de app van het apparaat te verwijderen, automatisch verwijderen van de app, enz.) en om de schrapping van alle verzamelde gegevens uit alle databanken (mobiele apps en servers) te activeren.
GEN-3	De broncode van de app en de bijbehorende achtergrondtaken moet open zijn en de technische specificaties moeten openbaar worden gemaakt, zodat elke betrokken partij de code kan controleren en, waar dat relevant is, kan bijdragen aan de verbetering van de code, het corrigeren van eventuele bugs en het waarborgen van de transparantie bij de verwerking van persoonsgegevens.
GEN-4	In elk van de opeenvolgende stadia van de ontwikkeling moet kunnen worden gevalideerd hoe doeltreffend de app de volksgezondheid dient. Daartoe moet vooraf een evaluatieprotocol worden opgesteld met indicatoren voor het meten van de doeltreffendheid van de app.

4. Doel

PUR-1	De app heeft uitsluitend als doel contacten op te sporen zodat personen die mogelijk aan SARS-CoV-2 zijn blootgesteld, daarvan op de hoogte kunnen worden gesteld en kunnen worden behandeld. De app mag voor geen enkel ander doel worden gebruikt.
PUR-2	De app mag niet voor een ander dan het primaire doel worden gebruikt om te controleren of de quarantaine-/afzonderingsmaatregelen en/of de social distancing in acht worden genomen.
PUR-3	De app mag niet worden gebruikt om conclusies te trekken over de locatie van de gebruikers op basis van hun interactie en/of andere middelen.

5. Functionaliteit

FUNC-1	De app moet voorzien zijn van een functionaliteit om aan de gebruikers te melden dat zij mogelijk aan het virus zijn blootgesteld. Basis voor deze informatie is de nabijheid ten opzichte van een besmette gebruiker binnen een periode van X dagen vóór de positieve screeningtest (de X-waarde wordt door de gezondheidsautoriteiten bepaald).
FUNC-2	De app moet advies geven aan gebruikers bij wie is vastgesteld dat zij mogelijk aan het virus zijn blootgesteld. De app moet instructies weergeven inzake de maatregelen die deze gebruikers moeten volgen, en moet de gebruikers in staat stellen advies te vragen. In dergelijke gevallen zou menselijke tussenkomst verplicht zijn.

FUNC-3	Het algoritme waarmee het besmettingsrisico aan de hand van de factoren afstand en tijd wordt gemeten en waarmee dus wordt bepaald wanneer een contact in de contacttraceringslijst moet worden geregistreerd, moet op een beveiligde manier kunnen worden aangepast aan de meest recente kennis op het gebied van de verspreiding van het virus.
FUNC-4	**Gebruikers die aan het virus zijn blootgesteld, moeten daarvan op de hoogte worden gebracht** of moeten regelmatig informatie krijgen over het feit of zij al dan niet aan het virus zijn blootgesteld, binnen de incubatieperiode van het virus.
FUNC-5	De app moet interoperabel zijn met andere apps die in de lidstaten worden ontwikkeld, zodat gebruikers die naar andere lidstaten reizen, efficiënt kunnen worden geïnformeerd.

6. Gegevens

DATA-1	Om het traceren van contacten mogelijk te maken, moet de app gegevens kunnen uitzenden en ontvangen via nabijheidscommunicatietechnologie zoals Bluetooth Low Energy.
DATA-2	De uitgezonden gegevens moeten cryptografisch sterke, pseudowillekeurige identificatoren bevatten die worden gegenereerd door en specifiek zijn voor de app.
DATA-3	Het risico op conflicterende pseudowillekeurige identificatoren moet laag genoeg zijn.
DATA-4	De pseudowillekeurige identificatoren moeten regelmatig en vaak genoeg worden vernieuwd om het risico van re-identificatie, fysieke tracering of linkage van personen door om het even wie – exploitanten van centrale servers, andere appgebruikers, kwaadwillige derden of anderen – te beperken. Deze identificatoren moeten worden gegenereerd door de app van de gebruiker, eventueel gebaseerd op een door de centrale server geleverde seed.
DATA-5	Volgens het beginsel van minimale gegevensverwerking mag de app geen andere gegevens verzamelen dan wat strikt noodzakelijk is voor het traceren van contacten.
DATA-6	De app mag geen locatiegegevens verzamelen voor het traceren van contacten. Locatiegegevens mogen uitsluitend worden verwerkt om de interactie met soortgelijke apps in andere landen mogelijk te maken, en de nauwkeurigheid ervan moet worden beperkt tot wat strikt noodzakelijk is voor dit doel.
DATA-7	De app mag geen andere gezondheidsgegevens verzamelen dan wat strikt noodzakelijk is voor de werking van de app, behalve op facultatieve basis en uitsluitend ter ondersteuning van het besluitvormingsproces voor het informeren van de gebruiker.

DATA-8	Aan de gebruikers moet worden meegedeeld welke persoonsgegevens zullen worden verzameld. Verzameling van deze gegevens is alleen toegestaan indien de gebruiker daarmee instemt.

7. Technische eigenschappen

TECH-1	De app moet gebruik maken van beschikbare technologie, zoals nabijheidscommunicatietechnologie (bv. Bluetooth Low Energy) om andere appgebruikers in de nabijheid op te sporen.
TECH-2	De app moet de geschiedenis van de contacten van de gebruiker in het apparaat bewaren gedurende een beperkte, vooraf vastgestelde periode.
TECH-3	Voor bepaalde functionaliteiten is het gebruik van een centrale server toegestaan.
TECH-4	De app moet gebaseerd zijn op een architectuur die zoveel mogelijk gebruik maakt van de apparaten van de gebruikers.
TECH-5	De contactgeschiedenis en de identificatoren van als besmet gesignaleerde gebruikers moeten aan de centrale server worden doorgegeven wanneer de gebruikers daartoe het initiatief nemen en hun status door een naar behoren gecertificeerde professionele zorgverstrekker is bevestigd.

8. Beveiliging

SEC-1	Een mechanisme moet de status van gebruikers die in de app als SARS-CoV-2-positief worden gesignaleerd, verifiëren, bijvoorbeeld aan de hand van een code voor eenmalig gebruik die gekoppeld is aan een testcentrum of een professionele zorgverstrekker. De gegevens mogen alleen worden verwerkt als de status op een beveiligde manier kan worden bevestigd.
SEC-2	Voor de doorgifte van de gegevens aan de centrale server moet een beveiligd kanaal worden gebruikt. Het gebruik van meldingsdiensten op platforms van aanbieders van besturingssystemen moet zorgvuldig worden beoordeeld en mag niet tot gevolg hebben dat gegevens aan derden worden bekendgemaakt.
SEC-3	Verzoeken moeten bestand zijn tegen manipulatie door kwaadwillige gebruikers.
SEC-4	Geavanceerde cryptografische technieken moeten zorgen voor de beveiligde uitwisseling tussen de app en de server en tussen de apps onderling, en voor de bescherming van de informatie die in de apps en op de server is opgeslagen. Hiervoor kunnen onder meer de volgende technieken worden gebruikt: symmetrische en asymmetrische encryptie, hashfuncties, PMT (private membership test), PSI (private set intersection), Bloom-filters, PIR (private information retrieval), homomorfe encryptie, enz.
SEC-5	De centrale server mag geen identificatoren van netwerkaansluitingen (bv. IP-adressen) van gebruikers bewaren, ook niet van gebruikers die positief zijn

	gediagnosticeerd en die hun contactgeschiedenis of hun eigen identificatoren hebben doorgegeven.
SEC-6	Om impersonatie of het aanmaken van nepgebruikers te vermijden, moet de server de app authenticeren.
SEC-7	De app moet de centrale server authenticeren.
SEC-8	De functionaliteiten van de server moeten worden beschermd tegen replay-aanvallen (pogingen om een netwerk aan te vallen door legale datapakketten te versturen, maar deze opzettelijk te vertragen of te herhalen).
SEC-9	De informatie die door de centrale server wordt doorgegeven, moet worden ondertekend om de oorsprong en integriteit ervan te authenticeren.
SEC-10	Enkel bevoegde personen mogen toegang hebben tot in de centrale server opgeslagen gegevens die niet openbaar toegankelijk zijn.
SEC-11	De permissiemanager van het apparaat op het niveau van het besturingssysteem moet alleen de toestemmingen vragen die vereist zijn voor de toegang tot en het gebruik van de communicatiemodules wanneer dat noodzakelijk is, voor de opslag van de gegevens in de terminal en voor de uitwisseling van informatie met de centrale server.

9. Bescherming van de gegevens en de privacy van natuurlijke personen

Opgelet: de volgende richtsnoeren hebben betrekking op apps die uitsluitend bedoeld zijn om contacten te traceren.

PRIV-1	Bij de uitwisseling van gegevens moet de privacy van de gebruikers (en met name het beginsel van minimale gegevensverwerking) in acht worden genomen.
PRIV-2	Directe identificatie van gebruikers bij gebruik van de app mag niet mogelijk zijn,
PRIV-3	net zo min als het traceren van de verplaatsingen van gebruikers.
PRIV-4	Gebruikers mogen via de app niets over andere gebruikers te weten komen (met name of ze al dan niet drager zijn van het virus).
PRIV-5	Het vertrouwen in de centrale server moet beperkt zijn. Bij het beheer van de centrale server moeten duidelijk omschreven governanceregels worden gevolgd en moeten alle maatregelen worden genomen die nodig zijn om de server te beveiligen. De centrale server moet staan op een locatie waar de bevoegde toezichthoudende autoriteit effectief toezicht kan houden.
PRIV-6	Er moet een gegevensbeschermingseffectbeoordeling worden uitgevoerd en deze moet openbaar worden gemaakt.
PRIV-7	De app mag de gebruiker alleen melden of hij aan het virus is blootgesteld en – zo mogelijk zonder informatie over andere gebruikers vrij te geven – hoe vaak en wanneer dat is gebeurd.

PRIV-8	De door de app verstrekte informatie mag gebruikers niet in staat stellen om gebruikers die drager van het virus zijn, te identificeren of de bewegingen van die gebruikers na te gaan.
PRIV-9	De door de app verstrekte informatie mag de gezondheidsautoriteiten niet in staat stellen om mogelijk blootgestelde gebruikers zonder hun toestemming te identificeren.
PRIV-10	Uit de verzoeken van de apps aan de centrale server mag niets op te maken zijn over de virusdrager.
PRIV-11	Uit de verzoeken van de apps aan de centrale server mag geen onnodige informatie over de gebruiker op te maken zijn, behalve eventueel, en alleen indien nodig, voor de pseudonieme identificatoren en de contactlijst.
PRIV-12	Linkage-aanvallen moeten uitgesloten zijn.
PRIV-13	De gebruikers moeten via de app hun rechten kunnen uitoefenen.
PRIV-14	Bij verwijdering van de app moeten automatisch ook alle lokaal verzamelde gegevens worden verwijderd.
PRIV-15	De app mag alleen gegevens verzamelen die zijn ingediend door verschillende instanties van de app of soortgelijke interoperabele apps. Er mogen geen gegevens met betrekking tot andere apps en/of nabijheidscommunicatieapparaten worden verzameld.
PRIV-16	Om re-identificatie door de centrale server te vermijden, moeten proxyservers worden geïnstalleerd. Het gebruik van deze *niet-colluderende servers* moet ervoor zorgen dat de identificatoren van verschillende gebruikers (zowel die van virusdragers als die welke door de verzoekers worden verstuurd) worden vermengd voordat ze met de centrale server worden gedeeld – dit om te voorkomen dat de identificatoren (zoals IP-adressen) van gebruikers bekend zijn in de centrale server.
PRIV-17	De app en de server moeten zorgvuldig worden ontwikkeld en geconfigureerd om te voorkomen dat onnodige gegevens worden verzameld (er mogen bv. geen identificatoren worden opgenomen in de logbestanden van de server) en dat SDK's van derden gegevens voor andere doeleinden verzamelen.

De meeste apps voor contacttracering die momenteel worden besproken, hanteren een van de twee volgende methoden wanneer een gebruiker besmet verklaard is: ze sturen de geschiedenis van de via scannen verkregen contacten die in hun nabijheid zijn geweest naar een server, of ze sturen de lijst van hun eigen uitgezonden identificatoren. Hieronder wordt een overzicht gegeven van de werkingsbeginselen van beide methoden. Het feit dat precies deze methoden hier worden behandeld, betekent niet dat er geen andere werkwijzen mogelijk of zelfs beter zijn, bv. wanneer daarbij gebruikt wordt gemaakt van end-to-end-encryptie of andere technologieën die de beveiliging verbeteren of de privacy beter beschermen.

9.1. Beginselen die alleen van toepassing zijn als de app een contactlijst naar de server stuurt:

CON-1	De centrale server moet de contactgeschiedenis verzamelen van gebruikers die als positief voor COVID-19 zijn gesignaleerd als gevolg van vrijwillige actie van hun kant.
CON-2	De centrale server mag geen lijst van de pseudonieme identificatoren van gebruikers die drager zijn van het virus, bijhouden of verspreiden.
CON-3	De op de centrale server opgeslagen contactgeschiedenis moet worden gewist zodra aan de gebruikers is gemeld dat zij zich in de nabijheid van een positief gediagnosticeerde persoon bevinden.
CON-4	Tenzij de gebruiker die als positief is gedetecteerd, zijn contactgeschiedenis met de centrale server deelt of tenzij de gebruiker bij de server een verzoek indient om zijn potentiële blootstelling aan het virus te achterhalen, mogen geen gegevens het apparaat van de gebruiker verlaten.
CON-5	Elke in de plaatselijke geschiedenis opgenomen identificator moet uiterlijk X dagen nadat deze is verzameld, worden gewist (de waarde van X wordt door de gezondheidsautoriteiten gedefinieerd).
CON-6	Door verschillende gebruikers ingediende contactgeschiedenissen mogen niet verder worden verwerkt, bv. door kruisverbanden te leggen om de nabijheid mondiaal in kaart te brengen.
CON-7	De gegevens in logbestanden van servers moeten tot een minimum worden beperkt en de vereisten inzake gegevensbescherming moeten hierbij in acht worden genomen.

9.2. Beginselen die alleen van toepassing zijn als de app een lijst van zijn eigen identificatoren naar de server stuurt:

ID-1	De centrale server moet de door de app uitgezonden identificatoren verzamelen van gebruikers die als positief voor COVID-19 zijn gesignaleerd als gevolg van vrijwillige actie van hun kant.
ID-2	De centrale server mag de contactgeschiedenis van gebruikers die drager zijn van het virus, niet bijhouden of verspreiden.
ID-3	De op de centrale server opgeslagen identificatoren moeten worden gewist zodra ze aan de andere apps zijn verstrekt.
ID-4	Tenzij de gebruiker die als positief is gedetecteerd, zijn identificatoren met de centrale server deelt of de gebruiker bij de server een verzoek indient om zijn potentiële blootstelling aan het virus te achterhalen, mogen geen gegevens het apparaat van de gebruiker verlaten.
ID-5	De gegevens in logbestanden van servers moeten tot een minimum worden beperkt en de vereisten inzake gegevensbescherming moeten hierbij in acht worden genomen.