

Publicatieblad van de Europese Unie

C 124 I



Uitgave
in de Nederlandse taal

Mededelingen en bekendmakingen

63e jaargang

17 april 2020

Inhoud

II *Mededelingen*

MEDEDELINGEN VAN DE INSTELLINGEN, ORGANEN EN INSTANTIES VAN DE EUROPESE UNIE

Europese Commissie

2020/C 124 I/01

Mededeling van de Commissie — Richtsnoeren in verband met gegevensbescherming voor apps ter ondersteuning van de bestrijding van de COVID-19-pandemie 1

NL

II

*(Mededelingen)*MEDEDELINGEN VAN DE INSTELLINGEN, ORGANEN EN INSTANTIES VAN
DE EUROPESE UNIE

EUROPESE COMMISSIE

MEDEDELING VAN DE COMMISSIE

**Richtsnoeren in verband met gegevensbescherming voor apps ter ondersteuning van de bestrijding
van de COVID-19-pandemie**

(2020/C 124 I/01)

1 ACHTERGROND

De COVID-19-pandemie betekent een ongekende uitdaging voor de Unie en de lidstaten, hun gezondheidszorgstelsels, hun levenswijze, hun economische stabiliteit en hun waarden. Digitale technologieën en gegevens spelen een waardevolle rol in de bestrijding van de COVID-19-crisis. Mobiele applicaties (apps) die doorgaans op smartphones worden geïnstalleerd, kunnen gezondheidsinstanties op nationaal en EU-niveau ondersteunen om de COVID-19-pandemie in het oog te houden en in te perken, met name in de fase waarin de inperkingsmaatregelen worden opgeheven. Zij kunnen dienen om de burgers rechtstreeks te begeleiden en de tracering van contacten te ondersteunen. In een aantal landen, zowel binnen de EU als daarbuiten, hebben nationale of regionale instanties of ontwikkelaars de lancering aangekondigd van apps met verschillende functionaliteiten ter ondersteuning van de bestrijding van het virus.

Op 8 april 2020 heeft de Commissie een aanbeveling aangenomen over een gemeenschappelijke toolbox voor het gebruik van technologie en gegevens om de COVID-19-crisis te bestrijden en te boven te komen, met name wat mobiele applicaties en het gebruik van geanonimiseerde mobiliteitsgegevens betreft (hierna “de aanbeveling” genoemd) ⁽¹⁾. Het doel van de aanbeveling is onder meer een gemeenschappelijke Europese en op EU-niveau gecoördineerde aanpak (“toolbox”) voor het gebruik van mobiele applicaties te ontwikkelen, om burgers in staat te stellen doeltreffende socialeonthoudingsmaatregelen te treffen, en om te waarschuwen, te voorkomen en contacten te traceren ter beperking van de verspreiding van de COVID-19-ziekte. De aanbeveling bevat de algemene beginselen voor de ontwikkeling van een dergelijke toolbox en geeft aan dat de Commissie nadere richtsnoeren zal publiceren, onder meer over gevolgen van het gebruik van applicaties op dit gebied voor de bescherming van persoonsgegevens en de privacy.

Met het gezamenlijke Europese stappenplan voor de opheffing van de inperkingsmaatregelen tegen COVID-19 heeft de Commissie, in samenwerking met de voorzitter van de Europese Raad, een aantal beginselen vastgelegd voor de uitfasering van de als gevolg van de COVID-19-uitbraak opgelegde inperkingsmaatregelen. Mobiele applicaties, inclusief contacttraceringfunctionaliteiten, kunnen in deze context een belangrijke rol spelen. Afhankelijk van de kenmerken van de apps en de mate waarin ze door de bevolking worden gebruikt, kunnen apps een significant effect hebben op de diagnose, de behandeling en de beheersing van COVID-19 in ziekenhuizen en daarbuiten. Zij zijn met name relevant wanneer inperkingsmaatregelen worden opgeheven en het besmettingsrisico toeneemt naarmate steeds meer mensen met elkaar in contact komen. Deze applicaties kunnen helpen besmettingsketens sneller en efficiënter te doorbreken dan algemene inperkingsmaatregelen, en zij kunnen het risico op verspreiding van het virus aanzienlijk verkleinen. Zij moeten dus een belangrijk onderdeel van de exitstrategie zijn en andere maatregelen zoals uitbreiding van de testcapaciteit aanvullen ⁽²⁾. Een belangrijke voorwaarde voor de ontwikkeling van dergelijke apps en de aanvaarding ervan door de mensen is vertrouwen. Mensen moeten de zekerheid hebben dat de naleving van de grondrechten wordt gewaarborgd en dat de apps alleen voor de specifiek omschreven doelstellingen zullen worden gebruikt, dat zij niet voor grootschalig toezicht zullen

⁽¹⁾ Aanbeveling C(2020) 2296 final van 8 april 2020 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

⁽²⁾ https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

worden gebruikt en dat mensen zeggenschap over hun gegevens houden. Dit is het fundament voor de nauwkeurigheid en doeltreffendheid van dergelijke apps bij het indammen van de verspreiding van het virus. Daarom is het essentieel om de oplossingen in kaart te brengen die het minst ingrijpend zijn en die volledig stroken met de vereisten van het EU-recht inzake de bescherming van persoonsgegevens en de privacy. Bovendien moeten de apps uiterlijk wanneer wordt verklaard dat de pandemie onder controle is, worden gedeactiveerd. Ook moeten de apps over de allernieuwste informatiebeveiliging beschikken.

In deze richtsnoeren wordt rekening gehouden met de bijdrage van het Europees Comité voor gegevensbescherming (EDPB) ⁽³⁾ en met discussies binnen het e-gezondheidsnetwerk. Het EDPB wil in de komende dagen richtsnoeren publiceren over geolocatie en andere traceringsinstrumenten in de context van de COVID-19-uitbraak.

Reikwijdte van de richtsnoeren

Om te zorgen voor een coherente aanpak in de hele EU en lidstaten en appontwikkelaars houvast te geven, bevat dit document de kenmerken en vereisten waaraan apps moeten voldoen met het oog op de naleving van de EU-wetgeving inzake de privacy en de bescherming van persoonsgegevens, met name de algemene verordening gegevensbescherming ⁽⁴⁾ en de e-privacyrichtlijn ⁽⁵⁾. Deze richtsnoeren gaan niet in op verdere voorwaarden, inclusief beperkingen, die de lidstaten kunnen hebben opgenomen in hun nationale wetgeving inzake de verwerking van gezondheidsgegevens.

De richtsnoeren zijn niet juridisch bindend. Zij laten de rol van het Hof van Justitie van de EU, de enige instelling die bindende uitlegging van het EU-recht kan geven, onverlet.

Deze richtsnoeren hebben uitsluitend betrekking op vrijwillige apps ter ondersteuning van de bestrijding van de COVID-19-pandemie (apps die vrijwillig door mensen worden gedownload, geïnstalleerd en gebruikt) met een of meer van de volgende functionaliteiten:

- het verstrekken van nauwkeurige informatie aan personen over de COVID-19-pandemie;
- het verstrekken van vragenlijsten voor zelfbeoordeling en begeleiding van personen (symptoomcontrolefunctionaliteit) ⁽⁶⁾;
- het waarschuwen van personen die gedurende een bepaalde tijd in de buurt van een besmette persoon zijn geweest, om informatie te verstrekken over de vraag of men in zelfquarantaine moet en waar men zich kan laten testen (contacttracers- en waarschuwingsfunctionaliteit);
- het bieden van een communicatieforum tussen patiënten en artsen in geval van zelfisolatie of wanneer verder advies over diagnose en behandeling wordt verstrekt (meer gebruik van telegeneeskunde).

Volgens de e-privacyrichtlijn kan het gebruik van een app waarbij het recht op vertrouwelijkheid van communicatie als bedoeld in artikel 5 in het geding is, alleen worden opgelegd via een wet die noodzakelijk, passend en evenredig is om bepaalde specifieke doelstellingen te beschermen. Omdat een dergelijke aanpak zeer ingrijpend is en uitdagingen meebrengt, ook wat betreft de invoering van passende waarborgen, is naar de mening van de Commissie een zorgvuldige analyse vereist voordat deze optie kan worden gebruikt. Om deze redenen beveelt de Commissie het gebruik van vrijwillige apps aan.

Deze richtsnoeren hebben geen betrekking op apps die de handhaving van quarantainevoorschriften als doel hebben (waaronder verplichte apps).

2 BIJDRAGE VAN APPS AAN DE BESTRIJDING VAN COVID-19

De symptoomcontrolefunctionaliteit is een instrument voor de volksgezondheidsinstanties om de burgers te voorzien van advies over het testen op COVID-19 en informatie over zelfisolatie, de voorkoming van besmetting van anderen en de vraag wanneer men zich moet laten behandelen. Deze functionaliteit kan ook een aanvulling vormen op de eerstelijnszorg en inzicht geven in de besmettingspercentages met COVID-19 onder de bevolking.

⁽³⁾ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

⁽⁴⁾ 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 (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

⁽⁵⁾ Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

⁽⁶⁾ Als de apps informatie verstrekken met betrekking tot diagnose, preventie, monitoring, voorspelling of prognose, moet de mogelijke kwalificatie daarvan als medische hulpmiddelen worden beoordeeld overeenkomstig het regelgevingskader voor medische hulpmiddelen. Voor dit kader zie Richtlijn 93/42/EEG van de Raad van 14 juni 1993 betreffende medische hulpmiddelen (PB L 169 van 12.7.1993, blz. 1) en Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen (PB L 117 van 5.5.2017, blz. 1).

Contacttracings- en waarschuwingsfunctionaliteiten zijn instrumenten om de personen te achterhalen die in contact zijn geweest met een persoon met COVID-19 en om de betrokkene te informeren over passende volgende stappen, zoals zelfquarantaine, testen of advies over wat te doen bij symptomen. Deze functionaliteit is dus nuttig voor zowel personen als volksgezondheidsinstanties. Zij kan ook een belangrijke rol spelen bij het beheer van inperkingsmaatregelen tijdens het afbouwscenario. De impact ervan kan worden versterkt door een strategie om mensen met milde symptomen op grotere schaal te testen.

Beide functionaliteiten kunnen ook een relevante bron van gegevens voor de volksgezondheidsinstanties zijn en de doorgifte van deze gegevens aan de nationale epidemiologische instanties en het Europees Centrum voor ziektepreventie en -bestrijding (ECDC) vergemakkelijken. Dit zou inzicht geven in overdrachtspatronen en, indien gecombineerd met testresultaten, helpen de positieve prognostische waarde van respiratoire symptomen in een bepaalde gemeenschap te ramen en informatie te verstrekken over de mate van viruscirculatie.

De mate van betrouwbaarheid van de ramingen houdt rechtstreeks verband met het aantal doorgegeven gegevens en de betrouwbaarheid daarvan.

In combinatie met passende teststrategieën kunnen de symptoomcontrole- en de contacttracingsfunctionaliteit dus informatie verstrekken over de mate van viruscirculatie en helpen de impact van afstandbewarings- en afzonderingsmaatregelen te beoordelen. Zoals in de aanbeveling is uiteengezet, moet worden gezorgd voor interoperabiliteit tussen de IT-oplossingen van de verschillende lidstaten om grensoverschrijdende samenwerking mogelijk te maken en ervoor te zorgen dat contacten tussen gebruikers van verschillende apps worden opgespoord (wat met name belangrijk is bij grensoverschrijdende verplaatsingen van burgers). Wanneer een besmette persoon in contact komt met een gebruiker van een app van een andere lidstaat, moet grensoverschrijdende doorgifte van de persoonsgegevens van die gebruiker aan de gezondheidsinstanties van zijn lidstaat mogelijk zijn, voor zover strikt noodzakelijk. De werkzaamheden met betrekking tot deze kwestie zullen plaatsvinden als onderdeel van de in de aanbeveling aangekondigde toolbox. De interoperabiliteit moet worden gewaarborgd door middel van technische voorschriften en door de communicatie en samenwerking tussen de nationale gezondheidsinstanties te verbeteren. Een model van bijzondere samenwerking ⁽⁷⁾ zou ook kunnen worden gebruikt als governance-model voor contacttracingsapps tijdens de COVID-19-pandemie.

3 ELEMENTEN VOOR EEN BETROUWBAAR EN VERANTWOORD GEBRUIK VAN APPS

De in de apps ingebouwde functionaliteiten kunnen verschillende gevolgen hebben voor een brede waaier in het Handvest van de grondrechten van de EU verankerde rechten, zoals de menselijke waardigheid, de eerbiediging van het privéleven en van het familie- en gezinsleven, de bescherming van persoonsgegevens, de vrijheid van verkeer, non-discriminatie, de vrijheid van ondernemerschap en de vrijheid van vergadering en vereniging. Aangezien sommige functionaliteiten gebaseerd zijn op een data-intensief model, moet wellicht vooral aandacht uitgaan naar inmenging in de privacy en het recht op bescherming van persoonsgegevens.

De hiernavolgende elementen bevatten richtsnoeren over de manier waarop de indringendheid van de appfunctionaliteiten kan worden beperkt met het oog op de naleving van de EU-wetgeving inzake de bescherming van persoonsgegevens en inzake de privacy.

3.1 Nationale gezondheidsinstanties (of entiteiten die taken van algemeen belang op gezondheidsgebied verrichten) als verwerkingsverantwoordelijken

Het is van cruciaal belang dat wordt bepaald wie beslist over de middelen en doelen van de gegevensverwerking (de verwerkingsverantwoordelijke) zodat kan worden vastgesteld wie verantwoordelijk is voor de naleving van de EU-regels inzake de bescherming van persoonsgegevens. Met name moet worden bepaald wie aan personen die de app downloaden informatie moet verstrekken over wat er zal gebeuren met hun persoonsgegevens (zowel bestaande als diegene die worden gegenereerd door het toestel waarop de app wordt geïnstalleerd, zoals een smartphone), wat hun rechten zijn, wie er verantwoordelijk is in het geval van inbreuken in verband met persoonsgegevens enzovoort.

Gezien de gevoeligheid van de betrokken persoonsgegevens en de hieronder beschreven doeleinden van de gegevensverwerking is de Commissie van oordeel dat de apps zo moeten worden ontworpen dat de nationale gezondheidsinstanties (of de entiteiten die taken van algemeen belang op gezondheidsgebied verrichten) de verwerkingsverantwoordelijken ⁽⁸⁾ zijn. De verwerkingsverantwoordelijken zijn verantwoordelijk voor de naleving van de algemene verordening gegevensbescherming (AVG) (verantwoordingsbeginsel). De reikwijdte van de toegang moet worden beperkt op basis van de in punt 3.5 hieronder beschreven beginselen.

⁽⁷⁾ Dergelijke samenwerking vindt al plaats met betrekking tot het project MyHealth@EU voor de uitwisseling van patiëntendossiers en elektronische recepten. Zie ook artikel 5, lid 5, en overweging 17 van Uitvoeringsbesluit 2019/1765 van de Commissie.

⁽⁸⁾ Zie overweging 45 van de AVG.

Dat zal er ook toe bijdragen dat de apps (en de onderliggende informatiesystemen over infectieketens) bij de bevolking op meer vertrouwen en dus aanvaarding kunnen rekenen en dat zij voldoen aan het beoogde doel, namelijk de volksgezondheid beschermen. De verantwoordelijke nationale gezondheidsinstanties moeten de onderliggende beleidskeuzen, verplichtingen en controles afstemmen en op een gecoördineerde wijze uitvoeren.

3.2 Ervoor zorgen dat de gebruikers zeggenschap behouden

Een bepalende factor om vertrouwen in de apps te wekken, bestaat erin de gebruikers duidelijk te maken dat zij zeggenschap over hun persoonsgegevens behouden. Om dat bereiken moet volgens de Commissie aan de volgende voorwaarden worden voldaan:

- de installatie van de app moet vrijwillig zijn en er mogen geen negatieve consequenties zijn voor wie beslist de app niet te downloaden/gebruiken;
- verschillende appfunctionaliteiten (bv. informatie, symptoomcontrole, contacttracering en waarschuwingen) mogen niet worden gebundeld, maar de gebruiker moet voor elke specifieke functionaliteit zijn/haar toestemming kunnen geven. Dat mag echter niet verhinderen dat verschillende appfunctionaliteiten worden gecombineerd als de aanbieder dat mogelijk heeft gemaakt;
- eventuele nabijheidsgegevens (gegevens die worden gegenereerd door een uitwisseling van signalen via Bluetooth Low Energy (BLE) tussen toestellen die zich gedurende een epidemiologisch relevante tijdsduur binnen een epidemiologisch relevante afstand van elkaar bevinden) moeten worden opgeslagen op het toestel van de gebruiker. Indien dergelijke gegevens met de gezondheidsinstanties moeten worden gedeeld, mag dat alleen gebeuren nadat is bevestigd dat de betrokken persoon is besmet met COVID-19 en op voorwaarde dat die persoon ervoor kiest die gegevens te delen;
- de betrokkene moet van de gezondheidsinstanties alle nodige informatie over de verwerking van zijn of haar persoonsgegevens krijgen (in overeenstemming met de artikelen 12 en 13 van de AVG en artikel 5 van de e-privacyrichtlijn);
- de betrokkene moet zijn of haar rechten uit hoofde van de AVG kunnen uitoefenen (met name het recht van toegang, rectificatie en uitwissing). Elke beperking van de rechten uit hoofde van de AVG en de e-privacyrichtlijn moet in overeenstemming zijn met die handelingen en moet noodzakelijk, evenredig en op wetgeving gebaseerd zijn;
- uiterlijk wanneer wordt verklaard dat de pandemie onder controle is, moeten de apps worden gedeactiveerd; de deactivering van de apps mag niet afhangen van de verwijdering ervan door de gebruiker.

3.3 Rechtsgrondslag voor gegevensverwerking

Installatie van de apps en opslag van informatie op het toestel van de gebruiker

Zoals hoger vermeld is het op grond van de e-privacyrichtlijn (artikel 5) 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 heeft gegeven of ii) de opslag en/of toegang strikt noodzakelijk is voor de levering van een uitdrukkelijk door de gebruiker gevraagde (d.w.z. geïnstalleerde en geactiveerde) dienst van de informatiemaatschappij (zoals de app).

Voor een goede werking van de apps is het in de regel noodzakelijk dat informatie wordt opgeslagen op het toestel van de gebruiker en dat toegang wordt verkregen tot informatie die reeds op het toestel is opgeslagen. Daarnaast vereist de contacttracerings- en waarschuwingsfunctionaliteit dat bepaalde andere informatie (zoals kortstondige, periodiek wijzigende alias-gebruikersnamen van gebruikers van deze functionaliteit die zich in de nabijheid bevinden) op het toestel van de gebruiker wordt opgeslagen. Het kan voor die functionaliteit ook nodig zijn dat nabijheidsgegevens van een (besmette of waarschijnlijk besmette) gebruiker worden geüpload. Voor de werking van de app als zodanig is dat echter niet noodzakelijk. Aan de voorwaarden van optie ii) in de vorige alinea is dan ook niet voldaan. Bijgevolg is toestemming (optie i) hierboven) het meest geschikt als grondslag voor de desbetreffende activiteiten. Het moet gaan om een "vrije", "specifieke", "uitdrukkelijke" en "op informatie berustende" toestemming in de zin van de AVG, die wordt uitgedrukt door middel van een ondubbelzinnige actieve handeling van de betrokkene. Het mag dus niet gaan om een stilzwijgende vorm van toestemming (bv. stilzwijgen of inactiviteit) ⁽⁹⁾.

⁽⁹⁾ Zie de richtsnoeren van het Europees Comité voor gegevensbescherming inzake toestemming:
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Rechtsgrondslag voor de verwerking door nationale gezondheidsinstanties –Unierecht of nationaal recht

De nationale gezondheidsinstanties verwerken doorgaans persoonsgegevens wanneer een wettelijke verplichting in het EU-recht of het nationale recht in een dergelijke verwerking voorziet en in overeenstemming is met de voorwaarden van artikel 6, lid 1, onder c), en artikel 9, lid 2, onder i), van de AVG, of wanneer die verwerking noodzakelijk is voor de vervulling van een in het EU-recht of het nationale recht erkende taak van algemeen belang ⁽¹⁰⁾.

Elke nationale wetgeving moet voorzien in specifieke en passende maatregelen ter bescherming van de rechten en vrijheden van de betrokkenen. Als algemene regel geldt dat hoe sterker de impact is op de vrijheden van personen, hoe sterker de overeenkomstige waarborgen in de betrokken wetgeving moeten zijn.

De wetgeving van de EU en van de lidstaten die al bestond vóór de uitbraak van COVID-19 en de wetgeving die in de lidstaten specifiek wordt vastgesteld om de verspreiding van epidemieën in te dammen, kan in beginsel worden gebruikt als rechtsgrondslag voor de verwerking van persoonsgegevens indien daarin is voorzien in maatregelen die de monitoring van epidemieën mogelijk maken en indien die wetgeving voldoet aan de verdere vereisten van artikel 6, lid 3, van de AVG.

Gezien de aard van de betrokken persoonsgegevens (met name gezondheidsgegevens als een speciale categorie van persoonsgegevens) en de omstandigheden van de huidige COVID-19-pandemie, zou het gebruik van wetgeving als rechtsgrondslag bijdragen tot de rechtszekerheid, aangezien daarin i) gedetailleerde voorschriften zouden zijn opgenomen over de verwerking van specifieke gezondheidsgegevens, en de doeleinden van de verwerking duidelijk zouden worden gespecificeerd; ii) duidelijk zou zijn aangegeven wie de verwerkingsverantwoordelijke is, d.w.z. de entiteit die de gegevens verwerkt, en wie er buiten de verwerkingsverantwoordelijke toegang kan hebben tot de gegevens; iii) de mogelijkheid zou worden uitgesloten dat de gegevens voor andere dan de in de wetgeving vermelde doeleinden worden verwerkt; en iv) specifieke waarborgen zouden worden geboden. Om het openbare nut en de aanvaarding van de apps niet te ondermijnen, moet de nationale wetgever bijzondere aandacht besteden aan het kiezen van een oplossing die zo veel mogelijk burgers bereikt.

De verwerking door de gezondheidsinstanties op basis van de wetgeving doet geen afbreuk aan het feit dat eenieder zelf moet kunnen kiezen of hij de app al dan niet installeert en of hij zijn gegevens deelt met de gezondheidsinstanties. Het verwijderen van de app mag dan ook geen negatieve consequenties hebben.

Contacttracing- en waarschuwingsapps geven de gebruikers ervan waarschuwingen. Voor gevallen waarin een dergelijke waarschuwing rechtstreeks door de app wordt gegeven, vestigt de Commissie de aandacht op het verbod om personen te onderwerpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan rechtsgevolgen zijn verbonden of dat hem of haar anderszins in aanmerkelijke mate treft (artikel 22 AVG).

3.4 Gegevensminimalisatie

De gegevens die via toestellen worden geproduceerd en reeds vooraf op deze toestellen zijn opgeslagen, worden als volgt beschermd:

- als “persoonsgegevens”, d.w.z. alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4, lid 1, van de AVG), worden zij beschermd overeenkomstig de AVG. Gegevens over gezondheid krijgen een bijkomende bescherming (artikel 9 van de AVG).
- als “locatiegegevens”, d.w.z. gegevens die in een elektronische-communicatienetwerk of door een elektronische-communicatiedienst worden verwerkt, waarbij de geografische positie van de eindapparatuur van de gebruiker wordt aangegeven, worden deze gegevens beschermd krachtens de e-privacyrichtlijn (artikel 5, lid 1, artikelen 6 en 9) ⁽¹¹⁾.
- Alle informatie die is opgeslagen in en toegankelijk is voor de eindapparatuur van de gebruiker, wordt beschermd overeenkomstig artikel 5, lid 3, van de e-privacyrichtlijn.

Niet-persoonsgebonden gegevens (zoals onomkeerbaar geanonimiseerde gegevens) worden niet beschermd in het kader van de AVG.

De Commissie brengt in herinnering dat overeenkomstig het beginsel van gegevensminimalisatie alleen persoonsgegevens die geschikt, relevant en met betrekking tot het doel tot het noodzakelijke beperkt zijn ⁽¹²⁾, mogen worden verwerkt. De noodzaak om de persoonsgegevens te verwerken en de relevantie van deze persoonsgegevens moeten worden beoordeeld in het licht van de nagestreefde doelstelling(en).

De Commissie merkt bijvoorbeeld op dat indien de functionaliteit symptoomcontrole of telegeneeskunde tot doel heeft, voor deze doeleinden geen toegang tot de contactlijst van de eigenaar van het toestel vereist is.

⁽¹⁰⁾ Artikel 6, lid 1, onder e), AVG.

⁽¹¹⁾ Het wetboek voor elektronische communicatie bepaalt dat ook diensten die functioneel gelijkwaardig zijn aan elektronische-communicatiediensten, binnen het toepassingsgebied vallen.

⁽¹²⁾ Beginsel van gegevensminimalisatie.

Het genereren en verwerken van minder gegevens beperkt de veiligheidsrisico's. Als de maatregelen voor gegevensminimalisatie worden nageleefd, wordt ook gezorgd voor veiligheidswaarborgen.

— Functionaliteit inzake informatie:

Een app die alleen deze functionaliteit biedt, brengt geen behoefte aan verwerking van gezondheidsgegevens van personen teweeg. Deze zal alleen maar informatie aan personen bieden. Om dit doeleinde te vervullen, mag geen andere op eindapparatuur opgeslagen of voor die eindapparatuur toegankelijke informatie worden verwerkt dan die welke noodzakelijk is om de informatie te verstrekken.

— Functionaliteiten inzake symptoomcontrole en telegeneeskunde:

Indien de app een of twee van deze functionaliteiten bevat, zal sprake zijn van verwerking van persoonlijke gezondheidsgegevens. Daarom moet in de onderliggende wetgeving die van toepassing is op de gezondheidsinstanties, een lijst worden bepaald van gegevens die mogen worden verwerkt.

Daarnaast kunnen de gezondheidsinstanties de telefoonnummers nodig hebben van de personen die van de symptoomcontrole gebruik hebben gemaakt en de resultaten hebben geüpload. Op eindapparatuur opgeslagen of voor die eindapparatuur toegankelijke informatie mag alleen worden verwerkt voor zover dit noodzakelijk is om de app in staat te stellen haar doel te vervullen en om deze te laten functioneren.

— Functionaliteiten inzake contacttracering en waarschuwing:

De meeste COVID-19-infecties doen zich voor via druppeltjes die slechts over een beperkte afstand worden overgedragen. Zo snel mogelijk personen identificeren die zich in de nabijheid van een besmette persoon hebben bevonden, is een belangrijke factor om de besmettingsketen te doorbreken. Het vaststellen van nabijheid is afhankelijk van de afstand en de duur van een contact en moet uit epidemiologisch oogpunt worden bekeken. Het is bijzonder belangrijk de besmettingsketen te doorbreken om een opflakking van besmettingen in de exitfase van de crisis te voorkomen.

Nabijheidsgegevens kunnen daarvoor noodzakelijk zijn. Voor het meten van de nabijheid en het nauwe contact blijken Bluetooth Low Energy (BLE)-communicaties tussen toestellen nauwkeuriger en dus geschikter dan het gebruik van geolocatiegegevens (GNSS/GPS of cellulaire locatiegegevens). BLE voorkomt dat tracering kan worden gebruikt (in tegenstelling tot geolocatiegegevens). De Commissie beveelt dan ook aan gegevens van BLE-communicaties (of gegevens die door gelijkwaardige technologie zijn gegenereerd) te gebruiken om nabijheid vast te stellen.

Locatiegegevens zijn niet noodzakelijk voor gebruik in functionaliteiten inzake contacttracering, aangezien deze niet tot doel hebben de bewegingen van personen te volgen of voorschriften af te dwingen. Daarnaast zou het rekening houdend met het beginsel van gegevensminimalisatie moeilijk zijn de verwerking van locatiegegevens te rechtvaardigen en kunnen er problemen op het gebied van veiligheid en privacy ontstaan. Om deze reden adviseert de Commissie in dit verband geen gebruik te maken van locatiegegevens.

Ongeacht de gebruikte technische middelen voor het bepalen van nabijheid lijkt het niet noodzakelijk het exacte tijdstip van het contact of de plaats (indien beschikbaar) op te slaan. Toch zou het nuttig kunnen zijn de dag van het contact op te slaan om te weten of het contact plaatsvond wanneer de persoon symptomen ontwikkelde (of 48 uur eerder⁽¹³⁾) en om het follow-upbericht te sturen met bijvoorbeeld advies over de duur van de zelfquarantaine.

Nabijheidsgegevens mogen alleen worden gegenereerd en verwerkt als er een daadwerkelijk risico op besmetting bestaat (afhankelijk van de nauwe aard en de duur van het contact).

Opgemerkt zij dat de noodzaak en de evenredigheid van de gegevensverzameling bijgevolg zullen afhangen van factoren zoals de mate waarin testfaciliteiten beschikbaar zijn, met name wanneer maatregelen zoals afzondering reeds waren opgelegd. Personen die in nauw contact met een besmette persoon zijn geweest, kunnen op twee manieren worden gewaarschuwd:

Volgens de eerste aanpak wordt via de app automatisch een waarschuwing naar de nauwe contacten verzonden wanneer een gebruiker – met goedkeuring of bevestiging van de gezondheidsinstantie, bijvoorbeeld via een QR- of TAN-code – in de app invoert dat hij of zij positief is getest (gedecentraliseerde verwerking). De inhoud van het waarschuwingsbericht moet bij voorkeur door de gezondheidsinstantie worden vastgesteld. Volgens de tweede aanpak worden de arbitraire tijdelijke identificatiecodes op een backendserver bij de gezondheidsinstantie opgeslagen (backendserver-oplossing). Gebruikers kunnen niet onmiddellijk worden geïdentificeerd via deze gegevens. Via de identificatiecodes ontvangen gebruikers die in nauw contact met een positief geteste gebruiker zijn geweest, een waarschuwing op hun toestel. Indien de gezondheidsinstanties ook via telefoon of sms in contact wensen te treden met gebruikers die in nauw contact met een besmette persoon zijn geweest, moeten zij van die gebruikers toestemming krijgen voor gebruik van hun telefoonnummers.

⁽¹³⁾ De besmette persoon kan de besmetting doorgeven 48 uur voordat de symptomen optreden.

3.5 Beperking van openbaarmaking van/toegang tot gegevens

— Functionaliteit inzake informatie:

Er kan geen andere op eindapparatuur opgeslagen of voor die eindapparatuur toegankelijke informatie met gezondheidsinstanties worden uitgewisseld dan die welke noodzakelijk is om de informatiefunctie te vervullen. Aangezien deze functionaliteit alleen maar in een communicatiemiddel voorziet, krijgen de gezondheidsinstanties geen toegang tot andere gegevens.

— Functionaliteiten inzake symptoomcontrole en telegeneeskunde:

De functionaliteit inzake symptoomcontrole kan voor de lidstaten nuttig zijn om burgers voor te lichten over de vraag of zij moeten worden getest, om informatie over afzondering te verstrekken en om mee te delen wanneer en hoe zij toegang krijgen tot gezondheidszorg, met name voor risicogroepen. Deze functionaliteit kan ook een aanvulling vormen op de surveillance van de eerstelijnszorg en kan helpen om de besmettingsgraad voor COVID-19 na te gaan bij de bevolking. Daarom kan worden beslist dat de bevoegde gezondheidsinstanties en nationale epidemiologische instanties toegang moeten krijgen tot de door de patiënt verstrekte informatie. Het ECDC kan van de nationale instanties voor epidemiologische surveillance geaggregeerde gegevens ontvangen.

Indien ervoor wordt gekozen contact met gezondheidsfunctionarissen mogelijk te maken in plaats van via de app zelf, moeten aan de nationale gezondheidsinstanties indien nodig ook de telefoonnummers van de gebruikers van de app worden doorgegeven.

— Functionaliteiten inzake contacttracering en waarschuwing:

— Gegevens van de besmette persoon

De apps genereren op bijna willekeurige wijze efemere en regelmatig veranderende identificatiecodes van de telefoontoestellen die in contact staan met de gebruiker. Een optie is dat de identificatiecodes op het toestel van de gebruiker worden opgeslagen (zogenaamde gedecentraliseerde verwerking). Een andere optie kan erin bestaan dat deze arbitraire identificatiecodes worden opgeslagen op de server waartoe de gezondheidsinstanties toegang krijgen (zogenaamde backendserver-oplossing). De gedecentraliseerde oplossing stemt meer overeen met het minimalisatiebeginsel. De gezondheidsinstanties mogen alleen toegang krijgen tot nabijheidsgegevens van op het toestel van een besmette persoon, zodat zij in staat zijn mensen te contacteren die risico op besmetting lopen.

Deze gegevens zullen pas ter beschikking van de gezondheidsinstanties worden gesteld nadat de besmette persoon (na het ondergaan van een test) deze gegevens proactief met hen uitwisselt.

De besmette persoon mag niet worden geïnformeerd over de identiteit van de personen met wie hij/zij potentieel epidemiologisch relevant contact heeft gehad en die zullen worden gewaarschuwd.

— Gegevens van de personen die in (epidemiologisch) contact met de besmette persoon zijn geweest.

De identiteit van de besmette persoon mag niet worden bekendgemaakt aan de personen met wie hij/zij epidemiologisch contact heeft gehad. Het volstaat om hen in kennis te stellen van het feit dat zij tijdens de afgelopen 16 dagen epidemiologisch contact met een besmette persoon hebben gehad. Zoals hierboven opgemerkt, mogen gegevens over de tijd en de plaats van dergelijke contacten niet worden opgeslagen. Het is dan ook niet nodig of mogelijk deze gegevens door te geven.

De nationale gezondheidsinstanties moeten ten behoeve van het traceren van de epidemiologische contacten van een appgebruiker die besmet blijkt te zijn alleen in kennis worden gesteld van de identificatiecode van de persoon met wie de besmette persoon contact heeft gehad in de periode vanaf 48 uur voor het begin van de symptomen tot 14 dagen na het begin van de symptomen, op basis van de nabijheid en de duur van het contact.

Het ECDC kan van de nationale instanties geaggregeerde gegevens ontvangen voor epidemiologische surveillance betreffende in samenwerking met de lidstaten vastgestelde indicatoren.

3.6 Bepaling van de precieze doeleinden van de verwerking

De doeleinden van de verwerking dienen in de rechtsgrondslag (Unierecht of lidstatelijk recht) te zijn vastgesteld. Het doeleinde moet specifiek zijn, zodat er geen twijfel bestaat over het soort persoonsgegevens dat moet worden verwerkt om het gewenste doeleinde te bereiken, en het doeleinde moet uitdrukkelijk worden vermeld. .

Het precieze doeleinde dan wel de precieze doeleinden zullen afhangen van de functionaliteiten van de app. Elke functionaliteit van een app kan meerdere doeleinden hebben. Teneinde de betrokkenen volledige zeggenschap over hun gegevens te verschaffen, beveelt de Commissie aan om verschillende functionaliteiten niet te bundelen. In ieder geval moet de betrokkene de mogelijkheid hebben om te kiezen tussen verschillende functionaliteiten die een elk een afzonderlijk doeleinde nastreven.

De Commissie raadt het gebruik van onder de hierboven beschreven voorwaarden verzamelde gegevens voor andere doeleinden dan de bestrijding van COVID-19 af. Indien doeleinden als wetenschappelijk onderzoek en statistieken nodig zijn, moeten deze worden opgenomen in de oorspronkelijke lijst van doeleinden en duidelijk worden meegedeeld aan de gebruikers.

— Functionaliteit inzake informatie:

Het doel van deze functionaliteit is het verstrekken van de informatie die vanuit het oogpunt van de gezondheidsinstanties in de context van de crisis relevant is.

— Functionaliteiten inzake symptoomcontrole en telegeneeskunde:

De functionaliteit inzake symptoomcontrole kan een indicatie geven welk aandeel van de personen die bij COVID-19 passende symptomen melden daadwerkelijk besmet is (bijvoorbeeld door bij alle of een willekeurig aantal personen met dergelijke symptomen een monster af te nemen en dat te testen, indien daar capaciteit voor is). Bij de omschrijving van dit doeleinde moet duidelijk worden gemaakt dat de persoonlijke gezondheidsgegevens worden verwerkt om i) de betrokkene de mogelijkheid te bieden om aan de hand van een aantal vragen die worden gesteld zelf te beoordelen of hij/zij symptomen van COVID-19 heeft, of ii) medisch advies te krijgen indien hij/zij symptomen van COVID-19 heeft.

— Functionaliteiten inzake contacttracering en waarschuwing:

Loutere vermelden dat het doeleinde “preventie van verdere besmettingen met COVID-19” is, is niet specifiek genoeg. In dit geval beveelt de Commissie aan het doeleinde of de doeleinden nader te specificeren in de zin van: “bewaren van de contacten van de personen die de app gebruiken en die mogelijk blootgesteld zijn geweest aan besmetting met COVID-19 om degenen te waarschuwen die eventueel besmet kunnen zijn”.

3.7 Strikte beperkingen voor gegevensopslag vaststellen

Het beginsel van de beperking van de opslag vereist dat persoonsgegevens niet langer worden bewaard dan nodig is. De termijnen moeten worden gebaseerd op medische relevantie (afhankelijk van het doeleinde van de app: de incubatietijd enz.) en op realistische periodes voor administratieve stappen die eventueel moeten worden ondernomen.

— Functionaliteit inzake informatie:

Indien bij de installatie van deze functionaliteit gegevens worden verzameld, moeten deze onmiddellijk worden verwijderd. Het bewaren van dergelijke gegevens is niet gerechtvaardigd.

— Functionaliteiten inzake symptoomcontrole en telegeneeskunde:

De gezondheidsinstanties moeten dergelijke gegevens uiterlijk na één maand (incubatietijd plus marge) verwijderen, of nadat de betrokkene is getest en het resultaat negatief is. Gezondheidsinstanties kunnen gegevens langer bewaren ten behoeve van surveillancerapportage en onderzoek, mits deze geanonimiseerd zijn.

— Functionaliteiten inzake contacttracering en waarschuwing:

Nabijheidsgegevens moeten worden verwijderd zodra deze niet meer noodzakelijk zijn voor de alarmering van personen. Dergelijke gegevens moeten uiterlijk na één maand (incubatietijd plus marge) worden verwijderd, of nadat de betrokkene is getest en het resultaat negatief is. Gezondheidsinstanties kunnen nabijheidsgegevens langer bewaren ten behoeve van surveillancerapportage en onderzoek, mits deze geanonimiseerd zijn.

De gegevens moeten op het toestel van de gebruiker worden opgeslagen en alleen gegevens die door de gebruikers zijn meegedeeld en die noodzakelijk zijn om het doeleinde te bereiken, moeten worden geüpload naar de server die beschikbaar is voor de gezondheidsinstanties wanneer deze optie werd gekozen (d.w.z. alleen de gegevens van “nauwe contacten” van een persoon die positief op besmetting met COVID-19 is getest, worden naar de server geüpload).

3.8 Beveiliging van de gegevens waarborgen

De Commissie beveelt aan de gegevens in versleutelde vorm op het eindtoestel van de betrokkene op te slaan, waarbij gebruik wordt gemaakt van geavanceerde encryptietechnieken. Indien de gegevens op een centrale server worden opgeslagen, moet de toegang, waaronder de administratieve toegang, worden geregistreerd.

Nabijheidsgegevens mogen alleen in versleuteld en gepseudonimiseerd formaat op het eindtoestel van de betrokkene worden gegenereerd en opgeslagen. Teneinde traceren door derden uit te sluiten, moet activering van bluetooth mogelijk zijn zonder dat andere locatiediensten moeten worden geactiveerd.

Tijdens het verzamelen van nabijheidsgegevens via BLE verdient het de voorkeur regelmatig veranderende tijdelijke gebruiker-ID's te genereren en op te slaan en niet de daadwerkelijke toestel-ID op te slaan. Deze maatregel biedt extra bescherming tegen afluisteren en traceren door hackers en maakt de identificatie van personen moeilijker.

De Commissie beveelt aan de broncode van de app openbaar te maken en beschikbaar te stellen voor toetsing.

Aanvullende maatregelen om de verwerkte gegevens te beveiligen, kunnen worden overwogen, met name wat betreft automatische verwijdering of anonimisering van de gegevens na een bepaald tijdstip. In het algemeen moet de mate van beveiliging zijn afgestemd op de hoeveelheid verwerkte persoonsgegevens en de gevoeligheid daarvan.

Elke gegevensoverdracht van het persoonlijke toestel naar de nationale gezondheidsinstanties moet worden versleuteld.

Wanneer in de nationale wetgeving is bepaald dat de verzamelde persoonsgegevens ook voor wetenschappelijk onderzoek kunnen worden verwerkt, moet er in beginsel gebruik worden gemaakt van pseudonimisering.

3.9 De juistheid van de gegevens waarborgen

Het waarborgen van de juistheid van de verwerkte persoonsgegevens is niet alleen een voorwaarde voor de efficiëntie van de app, maar is ook een vereiste in het kader van de wetgeving inzake de bescherming van persoonsgegevens.

In dit verband is de juistheid van de informatie over de vraag of er contact met een besmette persoon (epidemiologische afstand en duur) is geweest, van essentieel belang, teneinde het risico op fout-positieve resultaten zo klein mogelijk te houden. Daarbij gaat het om scenario's waarbij twee gebruikers van de app contact hebben op straat, in het openbaar vervoer of in een gebouw. Het is onwaarschijnlijk dat het gebruik van locatiegegevens op basis van mobiele telefoonnetwerken daartoe accuraat genoeg is.

Daarom is het raadzaam gebruik te maken van technologieën die een nauwkeurigere beoordeling van het contact mogelijk maken (zoals bluetooth).

3.10 Betrokkenheid van gegevensbeschermingsautoriteiten

De gegevensbeschermingsautoriteiten moeten volledig worden betrokken bij de ontwikkeling van de app en daarover worden geraadpleegd, en zij moeten de uitrol ervan toetsen. Aangezien de verwerking van gegevens in het kader van de app zal worden aangemerkt als verwerking op grote schaal van bijzondere categorieën gegevens (gezondheidsgegevens), wijst de Commissie op artikel 35 van de algemene verordening gegevensbescherming betreffende de gegevensbeschermingseffectbeoordeling.

ISSN 1977-0995 (elektronische uitgave)
ISSN 1725-2474 (papieren uitgave)



Bureau voor publicaties van de Europese Unie
2985 Luxemburg
LUXEMBURG

