Ohjeet 4/2020 sijaintitietojen käytöstä ja kontaktien jäljitysvälineistä covid-19-pandemian yhteydessä

Annettu 21. huhtikuuta 2020

hyväksytty

Versioyhteenveto

Versio 1.1	5. toukokuuta 2020	Vähäisiä korjauksia
Versio 1.0	21. huhtikuuta 2020	Ohjeiden hyväksyminen

Sisällysluettelo

Euroopan tietosuojaneuvosto, joka

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan e alakohdan,

ottaa huomioon ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETAn sekakomitean päätöksellä N:o 154/2018[1],

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

ON ANTANUT SEURAAVAT OHJEET:

1 JOHDANTO JA ASIAYHTEYS

1 Hallitukset ja yksityiset toimijat ovat aikeissa käyttää datavetoisia ratkaisuja osana toimiaan covid-19-pandemiaan vastaamiseksi, mikä herättää lukuisia yksityisyyteen liittyviä huolenaiheita.

2 Euroopan tietosuojaneuvosto korostaa, että tietosuojaa koskeva oikeudellinen kehys on suunniteltu joustavaksi, joten se on tehokas väline sekä pandemian rajoittamiseen että ihmisoikeuksien ja perusvapauksien suojelemiseen.

3 Euroopan tietosuojaneuvosto on vakaasti sitä mieltä, että tietosuoja on välttämätöntä käsiteltäessä henkilötietoja covid-19-pandemian hallitsemiseksi. Sen avulla voidaan rakentaa luottamusta ja luoda edellytykset ratkaisujen sosiaaliselle hyväksynnälle ja taata näiden toimien tehokkuus. Koska virus ei tunne rajoja, olisi suotavaa kehittää yhteinen eurooppalainen lähestymistapa tämänhetkiseen kriisiin tai ainakin ottaa käyttöön yhteentoimivat puitteet.

4 Tietosuojaneuvosto katsoo yleisesti ottaen, että covid-19-taudin torjunnassa hyödynnettävää dataa ja teknologiaa olisi käytettävä yksilöiden voimaannuttamiseen kontrolloimisen, leimaamisen tai lannistamisen sijaan. Lisäksi vaikka data ja teknologia voivat olla tärkeitä välineitä, niihin liittyy luontaisia rajoituksia ja niillä voidaan vain tehostaa muita kansanterveystoimenpiteitä. Yleisten tehokkuuden, tarpeellisuuden ja oikeasuhteisuuden periaatteiden on ohjattava kaikkia jäsenvaltioiden ja EU:n toimielinten toimia, joihin liittyy henkilötietojen käsittelyä covid-19-taudin torjumiseksi.

5 Näissä ohjeissa selvennetään sijaintitietojen ja kontaktien jäljitysvälineiden oikeasuhteisen käytön edellytyksiä ja periaatteita kahta erityistä tarkoitusta varten:

- sijaintitietojen käyttö pandemian vastatoimien tukena: tietojen avulla mallinnetaan viruksen leviämistä, jotta voidaan arvioida eristystoimenpiteiden yleistä tehokkuutta
- kontaktien jäljitys: tarkoituksena on ilmoittaa yksilöille, jos he ovat olleet sellaisen henkilön läheisyydessä, joka on myöhemmin todettu viruksen kantajaksi. Näin pyritään katkaisemaan tartuntaketjut mahdollisimman varhaisessa vaiheessa.

6 Kontaktien jäljityssovellusten tehokkuus pandemian hallinnassa riippuu monista tekijöistä, joita ovat muun muassa se prosenttiosuus väestöstä, jonka tulisi asennetaa sovellus, ja se, miten kontaktin läheisyys ja kesto määritellään. Lisäksi tällaisten sovellusten on oltava osa

1 Viittauksilla "jäsenvaltioihin" tarkoitetaan näissä ohjeissa ETAn jäsenvaltioita.

pandemian torjuntaa koskevaa kattavaa kansanterveysstrategiaa, johon kuuluu myös testaus ja sitä seuraava kontaktien manuaalinen jäljittäminen epäilysten poistamiseksi. Sovellusten käyttöä olisi täydennettävä tukitoimenpiteillä sen varmistamiseksi, että käyttäjille annettavat tiedot asetetaan oikeaan asiayhteyteen ja että ilmoituksista on hyötyä kansalliselle terveysjärjestelmälle. Muussa tapauksessa nämä sovellukset eivät ehkä saavuta täyttä vaikutustaan.

7 Tietosuojaneuvosto korostaa, että yleinen tietosuoja-asetus ja direktiivi 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) sisältävät täsmällisiä sääntöjä, joiden nojalla voidaan sallia anonyymien tai henkilötietojen käyttö viranomaisten ja muiden kansallisten ja EU:n tason toimijoiden tukena SARS-CoV-2-viruksen leviämisen seurannassa ja hillitsemisessä.[2]

8 Euroopan tietosuojaneuvosto on jo ottanut kantaa siihen, että kontaktien jäljityssovellusten käytön olisi oltava vapaaehtoista eikä sen pitäisi perustua henkilöiden yksittäisten liikkeiden jäljittämiseen vaan pikemminkin käyttäjiä koskevaan läheisyysdataan.[3]

[2] Katso edellinen Euroopan tietosuojaneuvoston lausunto covid-19-epidemiasta.
[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 SIJAINTITIETOJEN KÄYTTÖ

2.1 Sijaintitietojen lähteet

9 Sijaintitietoja viruksen leviämisen ja eristystoimenpiteiden yleisen tehokkuuden mallintamiseen on saatavilla kahdesta pääasiallisesta lähteestä:

- sähköisten viestintäpalvelujen tarjoajien (kuten matkaviestintäoperaattorien) palvelujensa tarjoamisen yhteydessä keräämät tiedot ja
- tietoyhteiskunnan palvelujen tarjoajien sellaisten sovellusten keräämät sijaintitiedot, joiden toiminnot edellyttävät tällaisten tietojen käyttöä (esim. navigointi ja kuljetuspalvelut).

10 Euroopan tietosuojaneuvosto muistuttaa, että sähköisten viestintäpalvelujen tarjoajilta saatuja sijaintitietoja[4] voidaan käsitellä ainoastaan sähköisen viestinnän tietosuojadirektiivin 6 ja 9 artiklan tarkoituksessa. Tämä tarkoittaa, että näitä tietoja voidaan välittää viranomaisille tai kolmansille osapuolille vain, jos palveluntarjoaja on anonymisoinut ne. Käyttäjän päätelaitteen maantieteellisen sijainnin osoittavia tietoja, jotka eivät ole liikennetietoja, voidaan välittää vain käyttäjän ennakkosuostumuksella.[5]

11 Suoraan päätelaitteelta kerättyihin tietoihin, myös sijaintitietoihin, sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa. Näin ollen tietojen tallentaminen käyttäjän laitteelle tai jo tallennettujen tietojen käyttö on sallittua vain, jos i) käyttäjä on antanut suostumuksensa[6] tai ii) tallentaminen ja/tai käyttö on ehdottoman välttämätöntä käyttäjän nimenomaisesti pyytämän tietoyhteiskunnan palvelun kannalta.

12 Sähköisen viestinnän tietosuojadirektiivissä säädetyistä oikeuksista ja velvollisuuksista voidaan kuitenkin poiketa direktiivin 15 artiklan nojalla, jos se on välttämätöntä, asianmukaista ja oikeasuhteista demokraattisen yhteiskunnan tiettyjen tavoitteiden saavuttamiseksi.[7]

13 Jotta tietoyhteiskunnan palveluntarjoajan (esimerkiksi käyttöjärjestelmän tai jonkin aikaisemmin asennetun sovelluksen kautta) keräämiä sijaintitietoja voitaisiin käyttää uudelleen mallintamistarkoituksessa, tiettyjen lisäedellytysten on täytyttävä. Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa noudattaen kerättyjä tietoja voidaan käsitellä edelleen vain rekisteröidyn lisäsuostumuksella tai sellaisen unionin oikeuden tai jäsenvaltion lainsäädännön perusteella, joka muodostaa demokraattisessa yhteiskunnassa välttämättömän ja oikeasuhteisen toimenpiteen yleisen tietosuoja-asetuksen[8] 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi.

2.2 Keskiössä anonymisoitujen sijaintitietojen käyttö

14 Tietosuojaneuvosto korostaa, että käsiteltäessä sijaintitietoja olisi aina suosittava anonymisoituja tietoja henkilötietojen sijaan.

15 Anonymisoinnilla tarkoitetaan sitä, että tiettyjen tekniikoiden avulla poistetaan mahdollisuus kohtuudella toteutettavissa olevin keinoin yhdistää tiedot tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Kohtuullisuuden arvioinnissa on otettava huomioon sekä objektiiviset tekijät (aika, tekniset keinot) että asiayhteyteen liittyvät tekijät, jotka voivat

---

[4] Ks. sähköisen viestinnän tietosuojadirektiivin 2 artiklan c kohta (”paikkatieto”).
[5] Ks. sähköisen viestinnän tietosuojadirektiivin 6 ja 9 artikla.
[6] Sähköisen viestinnän tietosuojadirektiivissä suostumuksella tarkoitetaan samaa kuin yleisessä tietosuoja-asetuksessa, ja sen on täytettävä kaikki yleisen tietosuoja-asetuksen 4 artiklan 11 kohdassa ja 7 artiklassa vahvistetut suostumuksen edellytykset.
[7] Ks. sähköisen viestinnän tietosuojadirektiivin 15 artiklan tulkinnan osalta myös yhteisöjen tuomioistuimen asiassa C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29.1.2008 antama tuomio.
[8] Ks. verkottuneiden ajoneuvojen yhteydessä tapahtuvasta henkilötietojen käsittelystä annettujen ohjeiden 1/2020 kohta 1.5.3.

vaihdella tapauskohtaisesti (tapauksen harvinaisuus, kun otetaan huomioon henkilötiheys, tietojen luonne ja määrä). Jos tiedot eivät täytä arvioinnin kriteerejä, niitä ei siinä tapauksessa ole anonymisoitu ja niihin sovelletaan edelleen yleistä tietosuoja-asetusta.

16 Anonymisoinnin pätevyys arvioidaan kolmen kriteerin perusteella, jotka ovat i) muista erottaminen (henkilö voidaan erottaa suuremmasta ryhmästä tietojen perusteella), ii) yhdistettävyys (kaksi samaa henkilöä koskevaa tietuetta voidaan yhdistää toisiinsa) ja iii) päättely (henkilöstä voidaan suurella todennäköisyydellä päätellä tietoja, jotka eivät aiemmin olleet tiedossa).

17 Anonymisoinnin käsite ymmärretään helposti väärin, ja usein sitä pidetään erheellisesti pseudonymisointina. Anonymisoituja tietoja voidaan käyttää rajoituksetta, mutta pseudonymisoituihin tietoihin sovelletaan yhä yleistä tietosuoja-asetusta.

18 Tehokasta anonymisointia varten on monia mahdollisuuksia, mutta niihin on suhtauduttava tietyin varauksin.[9] Yksittäisiä tietoja ei voida anonymisoida vaan ainoastaan kokonaisia tietojoukkoja. Näin ollen mitä tahansa yksittäisen tietorakenteen muuttamista (salaus-tai muulla matemaattisella menetelmällä) voidaan parhaimmillaankin pitää vain pseudonymisointina.

19 Anonymisointiprosesseista ja tietojen jälleentunnistamisyrityksistä tehdään aktiivisesti tutkimusta. On olennaisen tärkeää, että anonymisointiratkaisuja toteuttava rekisterinpitäjä seuraa alan viimeisintä kehitystä erityisesti (teleoperaattoreilta ja/tai tietoyhteiskunnan palveluntarjoajilta saatujen) sijaintitietojen osalta, sillä ne ovat tunnetusti vaikeasti anonymisoitavissa.

20 Monet tutkimukset[10] ovat itse asiassa osoittaneet, että *anonymisoituina pidetyt sijaintitiedot* eivät välttämättä todellisuudessa olekaan anonyymejä. Henkilöiden liikkuvuustietojen jäljet ovat luontaisesti varsin korreloivia ja ainutlaatuisia. Näin ollen ne voivat tietyissä olosuhteissa olla alttiita uudelleentunnistamista koskeville yrityksille.

21 Yksittäistä tietorakennetta, joka osoittaa henkilön sijainnin merkittävän ajanjakson aikana, ei voida täysin anonymisoida. Tämä voi pitää paikkansa myös silloin, jos tallennettujen maantieteellisten koordinaattien tarkkuutta ei alenneta riittävästi, jos tietueen tarkemmat tiedot poistetaan tai jos säilytetään vain niiden paikkojen sijainnit, joissa rekisteröity oleskelee huomattavia aikoja. Tämä koskee myös heikosti aggregoituja sijaintitietoja.

22 Jotta anonymisointi onnistuu, sijaintitietoja on käsiteltävä huolellisesti niin, että ne täyttävät kohtuullisuuden arvioinnin kriteerit. Tällaiseen käsittelyyn kuuluu näin ollen se, että sijaintitietojoukkoja tarkastellaan kokonaisuutena ja että käsitellään kohtuullisen suuresta yksilöiden joukosta saatuja tietoja. Käsittelyssä käytetään saatavilla olevia päteviä anonymisointitekniikoita, jotka on pantava asianmukaisesti ja tehokkaasti täytäntöön.

23 Kun otetaan huomioon, että anonymisointiprosessit ovat monimutkaisia, anonymisointimenetelmän läpinäkyvyys on erittäin suotavaa.

---

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

3 KONTAKTIEN JÄLJITYSSOVELLUKSET

3.1 Yleinen oikeudellinen analyysi

24 Luonnollisten henkilöiden sijainnin ja/tai heidän välistensä kontaktien järjestelmällinen ja laajamittainen seuranta loukkaa vakavasti henkilöiden yksityisyyttä. Seuranta voidaan oikeuttaa ainoastaan sillä, että käyttäjät hyväksyvät vapaaehtoisesti kunkin asiaan kuuluvan käyttötarkoituksen. Tämä tarkoittaisi erityisesti sitä, että henkilöille, jotka päättävät olla käyttämättä tai eivät voi käyttää tällaisia sovelluksia, ei aiheudu siitä mitään haittaa.

25 Jotta voidaan varmistaa osoitusvelvollisuus, kontaktien jäljityssovellusten tietojen rekisterinpitäjä olisi määriteltävä selkeästi. Tietosuojaneuvosto katsoo, että rekisterinpitäjiä voisivat olla kansalliset terveysviranomaiset.[11] Myös muita rekisterinpitäjiä voidaan harkita. Joka tapauksessa, jos kontaktien jäljityssovellusten käyttöönottoon osallistuu useita toimijoita, niiden roolit ja vastuualueet on määriteltävä selkeästi alusta alkaen ja selitettävä käyttäjille.

26 Lisäksi käyttötarkoitusten on käyttötarkoitussidonnaisuuden periaatteen mukaisesti oltava riittävän yksityiskohtaisia, jotta tietojen myöhempi käsittely covid-19-terveyskriisin hallintaan liittymättömissä tarkoituksissa (esim. kaupallisissa tai lainvalvontatarkoituksissa) ei ole mahdollista. Kun tarkoitus on määritelty selkeästi, on varmistettava, että henkilötietojen käyttö on asianmukaista, välttämätöntä ja oikeasuhteista.

27 Kontaktien jäljityssovellusten yhteydessä olisi tarkasteltava huolellisesti tietojen minimoinnin periaatetta sekä sisäänrakennettua ja oletusarvoista tietosuojaa:

- kontaktien jäljityssovellukset eivät edellytä yksittäisten käyttäjien sijainnin jäljittämistä, vaan sen sijaan olisi käytettävä läheisyysdataa
- koska kontaktien jäljityssovellukset voivat toimia ilman henkilöiden suoraa tunnistamista, olisi toteutettava asianmukaiset toimenpiteet jälleentunnistamisen estämiseksi
- kerättyjen tietojen olisi sijaittava käyttäjän päätelaitteella, ja vain olennaisia tietoja olisi kerättävä, kun se on ehdottoman välttämätöntä.

28 Euroopan tietosuojaneuvosto toteaa käsittelyn lainmukaisuuden osalta, että kontaktien jäljityssovelluksiin liittyy päätelaitteelle jo tallennettujen tietojen säilyttäminen ja/tai käyttö ja tähän säilyttämiseen ja käyttöön sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa. Jos nämä toimet ovat ehdottoman välttämättömiä, jotta sovelluksen tarjoaja voi toimittaa käyttäjän nimenomaisesti pyytämän palvelun, käsittely ei edellytä käyttäjän suostumusta. Jos toimet eivät ole ehdottoman välttämättömiä, tarjoajan on pyydettävä käyttäjän suostumus.

29 Tietosuojaneuvosto huomauttaa lisäksi, että kontaktien jäljityssovellusten käytön vapaaehtoisuus ei tarkoita, että henkilötietojen käsittelylle olisi välttämättä annettu suostumus. Kun viranomaiset tarjoavat palvelua lakisääteisen toimeksiannon perusteella ja laissa asetettujen vaatimusten mukaisesti, tietojen käsittelyn asianmukaisin oikeusperuste on yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdassa vahvistettu käsittelyn tarpeellisuus yleistä etua koskevan tehtävän suorittamiseksi.

30 Yleisen tietosuoja-asetuksen 6 artiklan 3 kohdassa selvennetään, että 6 artiklan 1 kohdan e alakohdassa tarkoitetun käsittelyn oikeusperusteena on rekisterinpitäjään sovellettava unionin oikeus tai jäsenvaltion lainsäädäntö. Käsittelyn tarkoitus määritellään kyseisessä käsittelyn oikeusperusteessa tai, 1 kohdan e alakohdassa tarkoitetussa käsittelyssä, sen on

[11] Ks. myös Euroopan komission antamat ”Covid-19-pandemian torjuntaa tukevien sovellusten tietosuojaa koskevat ohjeet”, 16.4.2020 C(2020) 2523 final.

oltava tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.[12]

31 Oikeusperusteeseen tai lainsäädäntötoimenpiteeseen, joka toimii lainmukaisena perustana kontaktien jäljityssovellusten käytölle, olisi kuitenkin sisällytettävä tarkoituksenmukaisia suojatoimia, mukaan lukien viittaus sovelluksen käytön vapaaehtoisuuteen. Siihen olisi sisällytettävä myös selkeästi yksilöity henkilötietojen käyttötarkoituksen määrittely ja nimenomaiset myöhemmän käsittelyn rajoitukset sekä asianomaisten rekisterinpitäjien selkeä määrittäminen. Lisäksi olisi yksilöitävä tietoryhmät ja tahot (sekä tarkoitukset, joita varten henkilötietoja voidaan luovuttaa). Tietojen käytön asteesta riippuen oikeusperusteeseen tai lainsäädäntötoimenpiteeseen olisi sisällytettävä myös ylimääräisiä suojatoimia käsittelyn luonne, laajuus ja tarkoitukset huomioon ottaen. Euroopan tietosuojaneuvosto suosittelee sisällyttämään siihen mahdollisimman pian myös perusteet sen määrittämiseksi, milloin sovellus lakkautetaan, ja sen, mikä taho on siitä vastuussa.

32 Jos tietojen käsittely kuitenkin perustuu toiseen oikeusperusteeseen, kuten 6 artiklan 1 kohdan a alakohdassa tarkoitettuun suostumukseen, rekisterinpitäjän[13] on varmistettava, että tällaisen oikeusperusteen pätevyyttä koskevat tiukat edellytykset täyttyvät.

33 Lisäksi sovelluksen käyttö covid-19-pandemian torjunnassa voi johtaa terveystietojen (esimerkiksi tartunnan saaneen henkilön tilaa koskevat tiedot) keräämiseen. Tällaisten tietojen käsittely[14] on sallittua, kun se on tarpeen kansanterveyteen liittyvän yleisen edun vuoksi yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan i alakohdassa vahvistettujen edellytysten mukaisesti tai mainitun asetuksen 9 artiklan 2 kohdan h alakohdassa[15] vahvistettuja terveydenhuollon tarkoituksia varten. Oikeusperusteesta riippuen käsittelyn perustana voi myös olla nimenomainen suostumus (yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohta).

34 Alkuperäisen tarkoituksen mukaisesti yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan j alakohdassa sallitaan terveystietojen käsittely tieteellisiä tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

35 Tämänhetkistä terveyskriisiä ei pidä käyttää mahdollisuutena ottaa käyttöön suhteettomia tietojen säilyttämistä koskevia valtuuksia. Säilytystä koskevissa rajoituksissa olisi otettava huomioon todelliset tarpeet ja lääketieteellinen merkitys (tähän voi sisältyä epidemiologisiin syihin perustuvia näkökohtia, kuten itämisaika), ja henkilötietoja olisi säilytettävä vain covid-19-kriisin ajan. Yleisenä sääntönä on, että kriisin jälkeen kaikki henkilötiedot olisi poistettava tai anonymisoitava.

36 Euroopan tietosuojaneuvosto katsoo, että tällaiset sovellukset eivät voi korvata vaan ainoastaan tukea julkisen terveydenhuollon ammattihenkilöiden suorittamaa manuaalista kontaktien jäljittämistä. He voivat selvittää, johtavatko läheiset kontaktit todennäköisesti viruksen leviämiseen vai eivät (esimerkiksi henkilön ollessa vuorovaikutuksessa asianmukaisin suojavarustein varustautuneen henkilön, kuten kassatyöntekijän, tai ilman suojavarusteita olevan henkilön kanssa). Tietosuojaneuvosto korostaa, että menettelyjen ja prosessien, mukaan lukien kontaktien jäljittämissovellusten asianmukaisten algoritmien, olisi oltava asiantuntevan henkilöstön tarkassa valvonnassa, jotta voidaan rajoittaa väärien positiivisten tai negatiivisten tulosten esiintymistä. Erityisesti toteutettavia toimia koskevien neuvojen antamista ei saisi toteuttaa ainoastaan automaattisesti.

---

[12] Ks. johdanto-osan 41 kappale.

[13] Rekisterinpitäjien (erityisesti viranomaisten) on kiinnitettävä erityistä huomiota siihen, että suostumusta ei voida pitää vapaaehtoisesti annettuna, jos henkilöllä ei ole todellista mahdollisuutta kieltäytyä sen antamisesta tai peruuttaa sitä ilman, että siitä aiheutuu hänelle haittaa.

[14] Käsittelyn on perustuttava unionin oikeuteen tai jäsenvaltion lainsäädäntöön, jossa säädetään asianmukaisista ja täsmällisistä toimenpiteistä rekisteröidyn oikeuksien ja vapauksien, erityisesti salassapitovelvollisuuden, suojaamiseksi.

[15] Ks. yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan h alakohta.

37 Jotta voidaan varmistaa algoritmien oikeudenmukaisuus, luotettavuus ja laajemmin niiden lainmukaisuus, niiden on oltava tarkastettavissa ja riippumattomien asiantuntijoiden olisi arvioitava niitä säännöllisesti. Sovelluksen lähdekoodi olisi julkaistava mahdollisimman laajaa tarkastelua varten.

38 Vääriä positiivisia tuloksia esiintyy aina tietyssä määrin. Koska infektioriskin tunnistamisella voi luultavasti olla suuri vaikutus yksilöihin esimerkiksi niin, että he pysyvät omaehtoisessa karanteenissa kunnes he ovat saaneet negatiivisen testituloksen, on välttämätöntä tarjota mahdollisuus oikaista tiedot ja/tai myöhemmät analyysien tulokset. Tätä olisi tietenkin sovellettava vain skenaarioihin ja täytäntöönpanoihin, joiden yhteydessä tietoja käsitellään ja/tai säilytetään niin, että niiden oikaiseminen on teknisesti mahdollista ja edellä mainitut haittavaikutukset ovat todennäköisiä.

39 Euroopan tietosuojaneuvosto katsoo myös, että ennen tällaisen välineen käyttöönottoa on tehtävä tietosuojaa koskeva vaikutustenarviointi, koska käsittelyyn katsotaan liittyvän todennäköisesti korkea riski (terveystiedot, ennakoitu laajamittainen käyttöönotto, järjestelmällinen seuranta, uuden teknisen ratkaisun käyttö).[16] Tietosuojaneuvosto suosittelee vahvasti tietosuojaa koskevien vaikutustenarviointien julkaisemista.

3.2 Suositukset ja toiminnalliset vaatimukset

40 Tietojen minimoinnin periaatteen mukaisesti – sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden[17] noudattamisen ohella – on käsiteltävien tietojen määrä rajoitettava mahdollisimman pieneksi. Sovelluksen ei pitäisi kerätä toisiinsa liittymättömiä tai tarpeettomia tietoja, joita voivat olla muun muassa siviilisääty, viestintätunnisteet, laitteen hakemiston nimikkeet, viestit, puhelulokit, sijaintitiedot ja laitteen tunnisteet.

41 Sovellusten lähettämiin tietoihin saa sisältyä vain joitakin sovelluksen tuottamia ja sille ominaisia yksilöllisiä ja pseudonyymejä tunnisteita. Tunnisteet on uusittava säännöllisesti viruksen leviämisen estämiseen soveltuvalla tiheydellä, ja niiden on oltava sisällöltään riittäviä rajoittamaan yksilön tunnistamisen ja fyysisen jäljittämisen riskiä.

42 Kontaktien jäljittämisessä voidaan noudattaa keskitettyä tai hajautettua lähestymistapaa.[18] Kumpaakin olisi pidettävä toteuttamiskelpoisena vaihtoehtona, edellyttäen että käytössä on riittävät turvatoimet, sillä niillä kummallakin on etuja ja haittoja. Näin ollen sovelluksen kehittämisen käsitteellisessä vaiheessa olisi aina tarkasteltava perusteellisesti kumpaakin lähestymistapaa, punniten huolellisesti niiden kummankin vaikutuksia tietosuojaan/yksityisyyteen ja mahdollisia yksilön oikeuksiin kohdistuvia vaikutuksia.

43 Kontaktien jäljitysjärjestelmän käyttämien palvelinten on kerättävä ainoastaan sellaisen käyttäjän kontaktihistoria tai pseudonyymit tunnisteet, joka on terveysviranomaisten arvioinnin perusteella ja hänen oman vapaaehtoisen toimintansa tuloksena diagnosoitu tartunnan saaneeksi. Palvelimen on säilytettävä luettelo tartunnan saaneiden käyttäjien pseudonyymeistä tunnisteista tai heidän kontaktihistoriansa vain sen ajan, joka on tarpeen altistumisesta ilmoittamiseksi tartunnan mahdollisesti saaneille käyttäjille, eikä palvelin saa yrittää tunnistaa mahdollisesti tartunnan saaneita käyttäjiä.

44 Sellaisen maailmanlaajuisen kontaktien jäljitysmenetelmän käyttöönotto, johon kuuluu niin sovellusten kuin manuaalisen jäljityksen käyttöä, saattaa joissakin tapauksissa edellyttää lisätietojen käsittelyä. Nämä lisätiedot olisi säilytettävä käyttäjän päätelaitteella, ja niitä olisi

---

[16] Ks. Euroopan tietosuojaneuvoston hyväksymät entisen tietosuojatyöryhmän antamat ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”

[17] Ks. Euroopan tietosuojaneuvoston ohjeet 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta

[18] Hajautettu lähestymistapa on yleisesti ottaen yhdenmukaisempi tietojen minimoinnin periaatteen kanssa.

käsiteltävä vain, kun se on ehdottoman välttämätöntä ja käyttäjä on antanut siihen etukäteen nimenomaisen suostumuksensa.

45 Palvelimille ja sovelluksiin tallennettujen tietojen sekä sovellusten ja etäpalvelimen välisen tiedonvaihdon turvaamiseksi on käytettävä uusimpia kryptografian tekniikoita. Lisäksi on käytettävä sovelluksen ja palvelimen välistä molemminpuolista todentamista.

46 Jotta SARS-CoV-2-tartunnasta voidaan ilmoittaa käyttäjille sovelluksessa, tarvitaan asianmukainen vahvistus. Se voidaan saada esimerkiksi käyttämällä kertakäyttöistä koodia, joka on liitetty tartunnan saaneen henkilön pseudonymisoituun henkilöllisyyteen ja testauslaitokseen tai terveydenhuollon ammattihenkilöön. Jos vahvistusta käyttäjän tilasta ei voida saada suojatulla tavalla, tietoja ei pitäisi käsitellä olettaen tilan olevan vahvistettu.

47 Rekisterinpitäjän on yhteistyössä viranomaisten kanssa ilmoitettava selkeästi linkistä, jonka kautta voi ladata virallisen kansallisen kontaktien jäljityssovelluksen. Näin pyritään vähentämään sitä riskiä, että yksilöt käyttäisivät kolmannen osapuolen sovellusta.

4 PÄÄTELMÄT

48 Maailmaa koettelee merkittävä kansanterveyskriisi. Se edellyttää voimakkaita toimia, joiden vaikutukset ulottuvat myös tämän hätätilanteen jälkeiseen aikaan. Automaattinen tietojenkäsittely ja digitaaliteknologia voivat olla keskeisiä osatekijöitä covid-19-taudin torjunnassa. On kuitenkin varottava niin kutsuttua salpavaikutusta. Velvollisuutemme on varmistaa, että kaikki näissä poikkeuksellisissa olosuhteissa toteutetut toimenpiteet ovat tarpeellisia, ajallisesti rajoitettuja ja mahdollisimman vähäisiä ja että niitä tarkastellaan säännöllisesti ja tosiasiallisesti ja arvioidaan tieteellisesti.

49 Euroopan tietosuojaneuvosto korostaa, että meidän ei tulisi joutua tekemään valintaa kriisin tehokkaan ratkaisemisen ja perusoikeuksien suojelun välillä: voimme saavuttaa ne molemmat. Sitä paitsi tietosuojaperiaatteilla voi olla hyvin tärkeä rooli viruksen torjunnassa. EU:n tietosuojalainsäädännössä sallitaan henkilötietojen vastuullinen käyttö terveydensuojelun tarkoituksessa ja varmistetaan, että yksilön oikeuksia ja vapauksia ei heikennetä prosesseissa.

Euroopan tietosuojaneuvoston puolesta

Puheenjohtaja

(Andrea Jelinek)

LIITE – KONTAKTIEN JÄLJITYSSOVELLUKSET – ANALYYSI JA OHJEITA

0. Vastuuvapauslauseke

Seuraavat ohjeet eivät ole määräämiä eivätkä tyhjentäviä, ja niiden ainoana tarkoituksena on antaa yleisiä ohjeita kontaktien jäljityssovellusten suunnittelijoille ja toteuttajille. Muiden kuin tässä kuvattujen ratkaisujen käyttö on mahdollista ja lainmukaista, kunhan ne ovat asiaa koskevan oikeudellisen kehyksen (eli yleisen tietosuoja-asetuksen ja sähköisen viestinnän tietosuojadirektiivin) mukaisia.

On myös huomattava, että nämä ohjeet ovat yleisluonteisia. Näin ollen tässä asiakirjassa esitettyjä suosituksia ja velvoitteita ei pidä pitää tyhjentävinä. Kaikki arvioinnit on tehtävä tapauskohtaisesti, ja tietyt sovellukset saattavat edellyttää lisätoimenpiteitä, joita ei käsitellä näissä ohjeissa.

1. Tiivistelmä

Sidosryhmät useissa jäsenvaltioissa harkitsevat *kontaktien jäljityssovellusten* käyttöä auttaakseen väestöä saamaan selville, ovatko he olleet kontaktissa SARS-Cov-2-tartunnan saaneen henkilön kanssa.

Vielä ei ole vahvistettu, millä edellytyksillä tällaiset sovellukset edistäisivät tehokkaasti pandemian hallintaa. Nämä edellytykset olisi vahvistettava ennen sovellusten käyttöönottoa. Ohjeiden antaminen on siitä huolimatta hyödyllistä, jotta voidaan välittää olennaisia tietoja alkuvaiheen sovelluskehitystiimeille ja taata henkilötietojen suoja jo varhaisesta suunnitteluvaiheesta lähtien.

On huomattava, että nämä ohjeet ovat yleisluonteisia. Näin ollen tässä asiakirjassa esitettyjä suosituksia ja velvoitteita ei pidä pitää tyhjentävinä. Kaikki arvioinnit on tehtävä tapauskohtaisesti, ja tietyt sovellukset saattavat edellyttää lisätoimenpiteitä, joita ei käsitellä näissä ohjeissa. Tarkoituksena on antaa yleisiä ohjeita kontaktien jäljityssovellusten suunnittelijoille ja toteuttajille.

Jotkin kriteerit saattavat mennä tietosuojakehyksestä johtuvia tiukkoja vaatimuksia pidemmälle. Niiden tavoitteena on varmistaa mahdollisimman suuri läpinäkyvyys, jotta kontaktien jäljityssovellukset saavat sosiaalisen hyväksynnän.

Kontaktien jäljityssovellusten julkaisijoiden olisi näin ollen otettava huomioon seuraavat kriteerit:

- Sovelluksen käytön on oltava täysin vapaaehtoista. Se ei saa olla edellytyksenä lainsäädännössä vahvistettujen oikeuksien käytölle. Yksityishenkilöillä on aina oltava täysi mahdollisuus hallita tietojaan, ja heidän olisi voitava vapaasti valita, käyttävätkö he sovellusta.
- On todennäköistä, että kontaktien jäljityssovelluksista aiheutuu luonnollisten henkilöiden oikeuksien ja vapauksien kannalta korkea riski ja että ennen niiden käyttöönottoa on tehtävä tietosuojaa koskeva vaikutustenarviointi.
- Tiedot sovelluksen käyttäjien läheisyydestä toisiinsa voidaan saada ilman heidän paikantamistaan. Tämän tyyppinen sovellus ei edellytä eikä siihen näin ollen pitäisi sisältyä sijaintitietojen käyttöä.
- Kun käyttäjällä diagnosoidaan SARS-CoV-2-virustartunta, ilmoitus olisi lähetettävä vain henkilöille, joiden kanssa käyttäjä on ollut läheisessä kontaktissa sellaisen epidemiologisesti merkityksellisen ajanjakson aikana, jolta kontaktin jäljitystiedot säilytetään.

- Tällaisen sovelluksen toiminta saattaa, valitun arkkitehtuurin mukaan, edellyttää keskitetyn palvelimen käyttöä. Tässä tapauksessa, tietojen minimoinnin ja sisäänrakennetun tietosuojan periaatteiden mukaisesti, keskitetyn palvelimen prosessoimien tietojen määrän olisi oltava mahdollisimman pieni:
    - Kun käyttäjällä diagnosoidaan tartunta, tietoja hänen läheisistä kontakteistaan tai hänen sovelluksensa lähettämistä tunnisteista voidaan kerätä vain hänen suostumuksellaan. Käyttöön on otettava menetelmä, jolla voidaan varmentaa, että henkilöllä todella on tartunta, ilman että häntä tunnistetaan. Teknisesti tämä voitaisiin toteuttaa siten, että kontakteille ilmoitetaan vasta, kun terveydenhuollon ammattihenkilö on vahvistanut tartunnan, esimerkiksi kertakäyttöisen koodin avulla.
    - Rekisterinpitäjän ei saisi olla mahdollista tunnistaa tartunnan saaneiksi diagnosoituja käyttäjiä tai tällaisten käyttäjien kanssa läheisessä kontaktissa olleita henkilöitä keskuspalvelimelle tallennettujen tietojen perusteella. Niiden perusteella ei myöskään saisi olla mahdollista päätellä kontaktien yhteyksiä, jotka eivät ole tarpeen olennaisten kontaktien määrittämiseksi.
- Tällaisen sovelluksen toiminta edellyttää, että lähetetään tietoja, joita toisten käyttäjien laitteet lukevat, ja tällaisten lähetysten vastaanottamista:
    - Riittää, että käyttäjien mobiililaitteet (tietokoneet, tabletit, älykellot jne.) vaihtavat pseudonyymejä tunnisteita esimerkiksi Bluetooth Low Energy -tekniikan välityksellä.
    - Tunnisteet on tuotettava uusimpia kryptografisia menetelmiä käyttäen.
    - Ne on uusittava säännöllisesti, jotta voidaan vähentää fyysisen seurannan ja tietojen yksilöihin yhdistämisen riskiä.
- Tällainen sovellus on suojattava teknisten prosessien turvallisuuden takaamiseksi. Erityisesti on huomioitava seuraavaa:
    - Sovellus ei saa välittää käyttäjille tietoja, joiden perusteella he voivat päätellä muiden käyttäjien henkilöllisyyden tai näiden saaman diagnoosin. Keskuspalvelin ei saa tunnistaa käyttäjiä eikä päätellä heitä koskevia tietoja.

Vastuuvapauslauseke: Edellä mainitut periaatteet liittyvät ainoastaan *kontaktien jäljityssovellusten* ilmoitettuun tarkoitukseen eli siihen, että sovellukset ilmoittavat automaattisesti virukselle mahdollisesti altistuneille henkilöille heidän altistuksestaan (ilman että heitä tarvitsee tunnistaa). Toimivaltainen valvontaviranomainen voi valvoa sovelluksen operaattoreita ja infrastruktuuria. Näiden ohjeiden noudattaminen kokonaan tai osittain ei välttämättä riitä varmistamaan, että tietosuojakehystä noudatetaan kaikilta osin.

2. Määritelmät

Kontakti	Kontaktien jäljityssovellusten yhteydessä kontaktilla tarkoitetaan käyttäjää, joka on ollut vuorovaikutuksessa viruksenkantajaksi todetun käyttäjän kanssa niin, että vuorovaikutuksen kesto ja etäisyys aiheuttavat merkittävän altistumisriskin. Terveysviranomaisten on laskettava altistuksen kestoa ja

	henkilöiden välistä etäisyyttä koskevat parametrit, jotka voidaan tämän jälkeen asettaa sovellukseen.
Sijaintitiedot	Sijaintitiedoilla tarkoitetaan sähköisessä viestintäverkossa käsiteltäviä tai sähköisen viestintäverkon käsittelemiä tietoja, jotka ilmaisevat yleisesti saatavilla olevan sähköisen viestintäpalvelun (sellaisena kuin se on määritelty sähköisen viestinnän tietosuojadirektiivissä) käyttäjän päätelaitteen maantieteellisen sijainnin, sekä muista mahdollisista lähteistä saatuja tietoja, jotka liittyvät seuraaviin: • päätelaitteen leveys- ja pituusaste ja korkeus merenpinnasta • käyttäjän matkan suunta tai • sijaintietojen tallentamisen ajankohta.
Vuorovaikutus	Kontaktien jäljityssovellusten yhteydessä vuorovaikutuksella tarkoitetaan toisiaan (ajallisesti ja sijainnillisesti) lähellä olevien laitteiden välistä tietojenvaihtoa käytetyn viestintätekniikan (kuten Bluetooth) mahdollistamissa rajoissa. Tämä määritelmä ei sisällä vuorovaikutuksessa olevien kahden käyttäjän sijaintia.
Viruksenkantaja	Tässä asiakirjassa viruksenkantajalla tarkoitetaan käyttäjiä, jotka ovat saaneet positiivisen virustestituloksen ja virallisen diagnoosin lääkäriltä tai terveysasemalta.
Kontaktien jäljitys	Henkilöillä, jotka ovat olleet (epidemiologien määrittelemien kriteerien mukaisessa) läheisessä yhteydessä virustartunnan saaneen henkilön kanssa, on merkittävä riski saada tartunta ja tartuttaa puolestaan muita. Kontaktien jäljitys on taudintorjuntamenetelmä, jossa laaditaan luettelo kaikista viruksenkantajan läheisyydessä olleista henkilöistä, jotta voidaan tarkistaa heidän tartuntariskinsä ja ryhtyä tarvittaviin terveydenhoidollisiin toimenpiteisiin.

3. Yleistä

GEN-1	Sovelluksella on täydennettävä perinteisiä kontaktinjäljitystekniikoita (erityisesti tartunnan saaneiden henkilöiden haastatteluja), eli sen on oltava osa laajempaa kansanterveysohjelmaa. Sitä on käytettävä vain siihen saakka, kunnes uusien tartuntojen määrää voidaan hallita pelkillä manuaalisilla kontaktinjäljitystekniikoilla.

GEN-2	Viimeistään silloin, kun toimivaltaiset viranomaiset päättävät palaamisesta normaaliin elämään, on otettava käyttöön menettely, jolla lopetetaan tunnisteiden kerääminen (yleinen sovelluksen aktivoinnin poistaminen, ohjeet sovelluksen asennuksen poistamiseksi, sovelluksen asennuksen automaattinen poistaminen jne.) ja aloitetaan kerättyjen tietojen poistaminen kaikista tietokannoista (mobiilisovellukset ja palvelimet).
GEN-3	Sovelluksen ja sen taustapalvelimen lähdekoodin on oltava avoimia ja teknisten eritelmien on oltava julkisia, jotta asianomaiset osapuolet voivat tarkastaa koodin ja tarvittaessa edistää koodin parantamista, mahdollisten virheiden korjaamista ja henkilötietojen käsittelyn läpinäkyvyyden varmistamista.
GEN-4	Sovelluksen käyttöönottovaiheiden on oltava sellaisia, että sen tehokkuus kansanterveyden näkökulmasta voidaan varmistaa asteittain. Tätä tarkoitusta varten on alkuvaiheessa laadittava arviointisuunnitelma, jossa määritellään sovelluksen tehokkuutta mittaavat indikaattorit.

4. Tarkoitus

PUR-1	Sovelluksen ainoana tarkoituksena on oltava kontaktien jäljittäminen niin, että SARS-CoV-2-virukselle mahdollisesti altistuneille henkilöille voidaan ilmoittaa altistuksesta ja heistä voidaan huolehtia. Sitä ei saa käyttää muuhun tarkoitukseen.
PUR-2	Sovellusta ei saa käyttää muuhun kuin sen ensisijaiseen tarkoitukseen eli siihen, että sillä valvotaan karanteeni- tai eristystoimenpiteiden ja/tai lähikontaktien välttämistä koskevan säännön noudattamista.
PUR-3	Sovelluksen avulla ei saa tehdä päätelmiä käyttäjien sijainnista heidän kanssakäymisensä perusteella ja/tai muilla keinoin.

5. Toiminnalliset näkökohdat

FUNC-1	Sovelluksessa on oltava toiminto, jonka avulla käyttäjille voidaan ilmoittaa heidän mahdollisesta altistumisestaan. Altistumista koskeva tieto perustuu läheisyyteen tartunnan saaneen käyttäjän kanssa hänen positiivista testitulostaan edeltäneiden X päivän aikana. (Terveysviranomaiset määrittelevät X-arvon.)
FUNC-2	Sovelluksella on annettava suosituksia virukselle mahdollisesti altistuneille käyttäjille. Sillä on välitettävä heille ohjeita, ja heidän on voitava pyytää sitä kautta neuvoja. Tällaisissa tapauksissa ihmisen osallistuminen on pakollista.
FUNC-3	Algoritmia, joka mittaa tartuntariskiä ottamalla huomioon etäisyyttä ja aikaa koskevat tekijät ja määrittää, milloin kontakti on kirjattava kontaktien jäljitysluetteloon, on voitava säätää turvallisesti niin, että siinä otetaan huomioon viimeisimmät tiedot viruksen leviämisestä.

FUNC-4	**Käyttäjille on viruksen itämisajan kuluessa ilmoitettava, jos he ovat altistuneet virukselle,** tai heidän on saatava säännöllisesti tietoa mahdollisesta altistumisestaan.
FUNC-5	Sovelluksen on oltava yhteentoimiva muissa jäsenvaltioissa kehitettyjen sovellusten kanssa, jotta eri jäsenvaltioissa matkustaville käyttäjille voidaan toimittaa tehokkaasti ilmoituksia.

6. Tiedot

DATA-1	Sovelluksen on voitava lähettää ja vastaanottaa tietoja likiverkkotekniikan, kuten Bluetooth Low Energy -tekniikan, välityksellä, jotta kontakteja voidaan jäljittää.
DATA-2	Näihin lähetettyihin tietoihin on sisällyttävä sovelluksen tuottamia, sille ominaisia näennäissatunnaisia tunnisteita, jotka ovat kryptografisesti vahvoja.
DATA-3	Näennäissatunnaisten tunnisteiden välisten ristiriitojen riskin olisi oltava riittävän pieni.
DATA-4	Näennäissatunnaiset tunnisteet on uusittava riittävän usein. Näin rajoitetaan sitä riskiä, että keskuspalvelimen operaattorit, muut sovelluksen käyttäjät tai pahantahtoiset kolmannet osapuolet voisivat tunnistaa yksilöitä, seurata heitä fyysisesti tai yhdistää tietoja yksilöihin. Käyttäjän sovelluksen on luotava nämä tunnisteet mahdollisesti keskuspalvelimen tuottaman alkuarvon perusteella.
DATA-5	Tietojen minimoinnin periaatteen mukaan sovellus saa kerätä vain sellaisia tietoja, jotka ovat ehdottoman välttämättömiä kontaktien jäljitystä varten.
DATA-6	Sovellus ei saa kerätä sijaintitietoja kontaktinjäljitystarkoituksessa. Sijaintitietoja voidaan käsitellä ainoastaan, jotta sovellus voi olla vuorovaikutuksessa muissa maissa käytettävien samankaltaisten sovellusten kanssa, ja käsittely on rajattava tarkasti siihen, mikä on ehdottoman välttämätöntä tätä käyttötarkoitusta varten.
DATA-7	Sovellus ei saa kerätä muita terveystietoja kuin niitä, jotka ovat ehdottoman välttämättömiä sovelluksen käyttötarkoitusta varten, paitsi vapaaehtoiselta pohjalta ja ainoastaan siihen tarkoitukseen, että autetaan käyttäjälle ilmoittamiseen liittyvässä päätöksenteossa.
DATA-8	Käyttäjää on informoitava, mitä kaikkia henkilötietoja kerätään. Tällaisia tietoja on kerättävä ainoastaan käyttäjän luvalla.

7. Tekniset ominaisuudet

TECH-1	Sovelluksen olisi käytettävä saatavilla olevaa tekniikkaa, kuten likiverkkotekniikkaa (esim. Bluetooth Low Energy), sovellusta käyttävän laitteen läheisyydessä olevien käyttäjien havaitsemiseen.
TECH-2	Sovelluksen olisi säilytettävä käyttäjän kontaktihistoria laitteella ennalta määritellyn rajoitetun ajan.
TECH-3	Sovellus voi käyttää keskuspalvelinta joidenkin toimintojen suorittamiseen.
TECH-4	Sovelluksen arkkitehtuurin on perustuttava mahdollisimman pitkälti käyttäjien laitteisiin.
TECH-5	Virustartunnan saaneiden käyttäjien kontaktihistoria tai heidän omat tunnisteensa olisi välitettävä keskuspalvelimelle käyttäjien aloitteesta, kun asianmukaisen sertifioinnin saanut terveydenhuollon ammattihenkilö on vahvistanut heidän tilansa.

8. Turvallisuus

SEC-1	SARS-CoV-2-tartunnan saaneiden käyttäjien tila on varmennettava sovelluksessa esimerkiksi käyttämällä kertakäyttöistä koodia, joka on liitetty testauslaitokseen tai terveydenhuollon ammattihenkilöön. Jos varmennusta ei voida saada suojatulla tavalla, tietoja ei saa käsitellä.
SEC-2	Tiedot on välitettävä keskuspalvelimelle suojattua kanavaa pitkin. Käyttöjärjestelmän tarjoajien toimittamien ilmoituspalvelujen käyttö olisi arvioitava huolellisesti, eikä käyttö saisi johtaa tietojen luovuttamiseen kolmansille osapuolille.
SEC-3	Pyynnöt eivät saa olla sellaisia, että pahantahtoiset käyttäjät voisivat käsitellä niitä vilpillisesti.
SEC-4	Sovelluksen ja palvelimen välisen ja sovellusten välisen tiedonvaihdon turvaamiseksi sekä yleisesti sovelluksiin ja palvelimille tallennettujen tietojen suojaamiseksi on käytettävä uusimpia kryptografisia tekniikoita. Tällaisia tekniikoita ovat esimerkiksi seuraavat: symmetrinen ja epäsymmetrinen salaus, tiivistysfunktiot, Private Membership Test (PMT) -protokollat, Private Set Interaction (PSI) -protokollat, Bloom-suodattimet, Private Information Retrieval (PRI) -protokolla, homomorfinen salaus jne.
SEC-5	Keskuspalvelin ei saa säilyttää käyttäjien, mukaan lukien positiivisen diagnoosin saaneiden ja kontaktihistoriansa tai omat tunnisteensa välittäneiden käyttäjien, verkkoyhteyden tunnisteita (kuten IP-osoitteita).
SEC-6	Palvelimen on todennettava sovellus, jotta voidaan estää toisena henkilönä esiintyminen tai väärennettyjen käyttäjäprofiilien luominen.
SEC-7	Sovelluksen on todennettava keskuspalvelin.
SEC-8	Palvelimen toiminnot olisi suojattava toistohyökkäyksiltä.

SEC-9	Keskuspalvelimen lähettämät tiedot on allekirjoitettava, jotta niiden alkuperä ja luotettavuus voidaan todentaa.
SEC-10	Pääsy kaikkiin keskuspalvelimelle tallennettuihin tietoihin, jotka eivät ole julkisesti saatavilla, on rajattava ainoastaan valtuutettuihin henkilöihin.
SEC-11	Laitteen käyttöjärjestelmätason lupien hallinnoijan on pyydettävä ainoastaan niitä lupia, joita tarvitaan viestintämoduuleihin pääsemiseen ja niiden käyttämiseen tarvittaessa sekä tietojen tallentamiseen päätelaitteelle ja tietojen vaihtamiseen keskuspalvelimen kanssa.

9. Henkilötietojen ja luonnollisten henkilöiden yksityisyyden suoja

Muistutus: seuraavat ohjeet koskevat sovellusta, jonka ainoana käyttötarkoituksena on kontaktien jäljitys.

PRIV-1	Tietojen vaihdossa on kunnioitettava käyttäjien yksityisyyttä (ja erityisesti tietojen minimoinnin periaatetta).
PRIV-2	Sovelluksen avulla ei saa olla mahdollista tunnistaa käyttäjiä suoraan näiden käyttäessä sovellusta.
PRIV-3	Sovelluksen avulla ei saa olla mahdollista jäljittää käyttäjien liikkeitä.
PRIV-4	Sovelluksen ei tule antaa käyttäjille mitään tietoja muista käyttäjistä (eikä etenkään siitä, ovatko he viruksenkantajia).
PRIV-5	Keskuspalvelimeen on luotettava vain rajallisesti. Keskuspalvelimen hallinnoinnissa on noudatettava selkeästi määritettyjä sääntöjä ja toteutettava kaikki tarvittavat toimenpiteet keskuspalvelimen turvallisuuden varmistamiseksi. Keskuspalvelimen sijainnin olisi oltava sellainen, että toimivaltainen valvontaviranomainen voi valvoa sitä tehokkaasti.
PRIV-6	Tietosuojaa koskeva vaikutustenarviointi on tehtävä, ja se olisi julkistettava.
PRIV-7	Sovelluksen olisi ilmoitettava käyttäjälle ainoastaan hänen mahdollisesta altistumisestaan sekä altistumiskertojen ajankohdat ja lukumäärät, mahdollisuuksien mukaan paljastamatta tietoja muista käyttäjistä.
PRIV-8	Käyttäjien ei tule voida tunnistaa virusta kantavia käyttäjiä eikä saada tietoa heidän liikkeistään sovelluksen välittämien tietojen perusteella.
PRIV-9	Terveysviranomaisten ei tule voida tunnistaa mahdollisesti altistuneita käyttäjiä sovelluksen välittämien tietojen perusteella ilman käyttäjien lupaa.
PRIV-10	Sovellusten keskuspalvelimelle tekemissä pyynnöissä ei saa paljastaa mitään tietoja viruksenkantajasta.
PRIV-11	Sovellusten keskuspalvelimelle tekemissä pyynnöissä ei saa antaa tarpeettomia tietoja käyttäjästä, paitsi mahdollisesti, ja jos se on välttämätöntä, hänen pseudonyymi tunnisteensa ja yhteystietoluettelonsa.
PRIV-12	Tietoja ei tule voida yhdistää yksilöihin.
PRIV-13	Käyttäjien on voitava käyttää oikeuksiaan sovelluksen välityksellä.
PRIV-14	Sovelluksen asennuksen poistamisen on poistettava myös kaikki paikallisesti kerätyt tiedot.
PRIV-15	Sovelluksen olisi kerättävä ainoastaan sovelluksen esiintymien tai samankaltaisten yhteentoimivien sovellusten välittämiä tietoja. Muihin sovelluksiin ja/tai likiverkkoa käyttäviin laitteisiin liittyviä tietoja ei saa kerätä.
PRIV-16	Jotta voidaan välttää tietojen jälleentunnistaminen keskuspalvelimessa, on otettava käyttöön välityspalvelimia. Tällaisten palvelimien (*non-colluding server*) tarkoituksena on sekoittaa useiden käyttäjien (sekä viruksenkantajien että pyynnön esittäjien lähettämiä) tunnisteita ennen kuin ne jakavat ne

	keskuspalvelimen kanssa. Tällä pyritään estämään se, että keskuspalvelin saa käyttäjien tunnisteita (kuten IP-osoitteita).
PRIV-17	Sovellus ja palvelin on kehitettävä ja konfiguroitava huolellisesti niin, että mitään tarpeettomia tietoja ei kerätä (esimerkiksi palvelimen lokitietoihin ei tulisi sisällyttää tunnisteita) ja että voidaan välttää se, että kolmansien osapuolten ohjelmankehityspaketit keräävät tietoja muihin tarkoituksiin.

Useimmat tämänhetkisen keskustelun kohteina olevista kontaktien jäljityssovelluksista noudattavat periaatteessa kahta lähestymistapaa, kun käyttäjällä vahvistetaan tartunta: joko ne lähettävät palvelimelle analysoimalla saadut kontaktihistoriatiedot tai ne lähettävät luettelon lähetetyistä omista tunnisteistaan. Seuraavassa esitetyt periaatteet perustuvat näihin kahteen lähestymistapaan. Vaikka näissä ohjeissa käsitellään juuri näitä lähestymistapoja, se ei tarkoita sitä, etteivätkö muut lähestymistavat olisi mahdollisia tai jopa suositeltavia. Tällaisia voivat olla esimerkiksi lähestymistavat, joissa käytetään päästä päähän -salausta tai muita turvallisuutta tai yksityisyyttä parantavia teknologioita.

9.1. Periaatteet, joita sovelletaan vain silloin, kun sovellus lähettää palvelimelle yhteystietoluettelon:

CON-1	Keskuspalvelimen on kerättävä SARS-CoV-2-tartunnan saaneiden käyttäjien kontaktihistoria näiden vapaaehtoisen toiminnan seurauksena.
CON-2	Keskuspalvelin ei saa ylläpitää eikä levittää luetteloa tartunnan saaneiden käyttäjien pseudonyymeistä tunnisteista.
CON-3	Keskuspalvelimelle tallennettu kontaktihistoria on poistettava, kun käyttäjille on ilmoitettu heidän olleen tartunnan saaneen henkilön läheisyydessä.
CON-4	Käyttäjän laitteelta ei saa lähteä mitään tietoja, paitsi jos tartunnan saaneeksi todettu käyttäjä jakaa kontaktihistoriansa keskuspalvelimen kanssa tai lähettää palvelimelle pyynnön mahdollisen altistumisensa selvittämiseksi.
CON-5	Paikallisiin historiatietoihin sisältyvät tunnisteet on poistettava X päivän kuluttua niiden keräämisestä. (Terveysviranomaiset määrittelevät X-arvon.)
CON-6	Eri käyttäjien toimittamia kontaktihistorioita ei saa käsitellä edelleen esimerkiksi niin, että niiden ristiinkorreloinnin avulla laadittaisiin läheisyyksiä osoittavia maailmanlaajuisia karttoja.
CON-7	Palvelimen lokitiedot on minimoitava, ja niiden käsittelyssä on noudatettava tietosuojavaatimuksia.

9.2. Periaatteet, joita sovelletaan vain silloin, kun sovellus lähettää palvelimelle luettelon omista tunnisteistaan:

ID-1	Keskuspalvelimen on kerättävä SARS-CoV-2-tartunnan saaneiden käyttäjien sovellusten lähettämät tunnisteet käyttäjien vapaaehtoisen toiminnan seurauksena.

ID-2	Keskuspalvelin ei saa ylläpitää eikä levittää tartunnan saaneiden käyttäjien kontaktihistoriatietoja.
ID-3	Keskuspalvelimelle tallennetut tunnisteet on poistettava, kun ne on jaettu muille sovelluksille.
ID-4	Käyttäjän laitteelta ei saa lähteä mitään tietoja, paitsi jos tartunnan saaneeksi todettu käyttäjä jakaa tunnisteensa keskuspalvelimen kanssa tai lähettää palvelimelle pyynnön mahdollisen altistumisensa selvittämiseksi.
ID-5	Palvelimen lokitiedot on minimoitava, ja niiden käsittelyssä on noudatettava tietosuojavaatimuksia.