

Privaon

Privacy as a Service

privaon.com



**TIETOSUOJAA KOSKEVA
VAIKUTUSTENARVIOINTI**

Terveyden ja hyvinvoinninlaitos (THL)

~~LUKU 5: Riskitaulukko SALASSA PIDETTÄVÄ – Julkl (621/1999) 24.1 §:n 7 k~~

1. Yhteenveto

Covid-19-tartuntaketjujen jäljitystyön ja tartuntaketjujen katkaisemisen tehostamiseksi kehitettävän jäljityssovelluksen yhteyteen suunnitellulle henkilötietojen käsittelylle tehtiin tietosuoja koskeva vaikutustenarviointi heinä-elokuussa 2020. Vaikutustenarvioinnin toimitti tietosuoja-alan asiantuntijayritys Privaon Oy. Tämä dokumentti sisältää kuvauksen suunnitelluista henkilötietojen käsittelytoimenpiteistä, arvion henkilötietojen käsittelyn oikeasuhtaisuudesta ja tarpeellisuudesta, sekä kuvauksen tunnistetuista rekisteröityjen vapauksiin ja oikeuksiin kohdistuvista riskeistä ja toimenpiteistä, joilla riskeihin puututaan.

Tietosuoja koskeva vaikutustenarviointi tulee tietosuoja-asetuksen mukaan tehdä silloin, jos tietyn tyyppinen henkilötietojen käsittely todennäköisesti aiheuttaa käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Vaikutustenarvioinnissa tulee arvioida suunniteltujen käsittelytoimien vaikutuksia henkilötietojen suojalle. Vaikutustenarviointi auttaa rekisterinpitäjänä toimivaa Terveystietojen ja hyvinvoinnin laitosta tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Vaikutustenarviointi on tarkoitettu jatkuvaksi riskienhallintatoimenpiteeksi ja sitä on tarvittaessa päivitettävä, mikäli henkilötietojen käsittely tai siitä aiheutuvat riskit muuttuvat. Tämä vaikutustenarviointi on osa tietosuoja-asetuksen mukaista rekisterinpitäjän osoitusvelvollisuutta.

Tehdyn vaikutustenarvioinnin perusteella käsittely on suunniteltuihin käsittelytarkoituksiin nähden oikeasuhteista ja tarpeellista. Arvioitu käsittely on lainmukaista ja se perustuu tartuntatautilain väliaikaisen muutoksen rekisterinpitäjälle määrittämien tehtävien toteuttamiseen. Suunnitellut käsittelytoimet noudattavat tehokkaasti tietosuoja-asetuksen mukaisia tietosuojaperiaatteita. Vaikutustenarvioinnissa tunnistettujen tietosuojariskien todennäköisyyttä ja vaikutuksia rekisteröityjen oikeuksille ja vapauksille on lievennetty asianmukaisin tietosuoja- ja tietoturvatoinenpitein. Suunniteltujen käsittelytoimien ei tunnistettu aiheuttavan korkeita riskejä rekisteröityjen vapauksille ja oikeuksille.

Vaikutustenarvioinnin keskeisimmät havainnot liittyvät tunnistettuun riskiin siitä, että rekisteröidylle toimitettava altistumisilmoitus perustuu virheelliseen tietoon, tai tartunnan saaneelle tarkoitettu avauskoodi toimitetaan väärälle rekisteröidylle. Rekisteröity voi virheellisen tai väärin toimitetun tiedon perusteella aloittaa omaehtoisen karanteenin tai muulla tavoin omaehtoisesti rajoittaa toimintaansa merkittäväällä tavalla. Toisena keskeisenä huomiona tunnistettiin, että koska suunniteltujen käsittelytoimien luonteesta johtuen rekisterinpitäjä käsittelee tietoa, joka voi paljastaa rekisteröidyn mahdollisen altistumisen tai todetun tartunnan, vaikuttaa kyseisten tietojen arkaluonteisuus merkittävästi mahdollisen inhimillisestä tai teknisestä virheestä johtuvan tietoturvaloukkauksen vakavuuteen. Koska kehitettävälle mobiilisovellukselle ei aseteta ikärajaa, Privaon suosittelee, että henkilötietojen käsittelystä rekisteröidylle toimitettavan tiedon ymmärrettävyyteen, helppolukuisuuteen ja saatavuuteen kiinnitetään erityistä huomiota.

Tarkempi kuvaus vaikutustenarvioinnissa tunnistetusta riskeistä ja niiden vaikutuksista, sekä Privaonin suosituksista riskien lieventämiseksi on kirjattu tästä dokumentista löytyvään arvioon rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä. Suositukset esitettiin rekisterinpitäjälle ja osallistujille myös vaikutustenarvioinnin lopputapaamisessa.

Vaikutustenarviointi toteutettiin Privaonin tarjoamana työpajapohjaisena palveluna, jossa Privaonin tietosuoja-asiantuntijat Toni Leppänen ja Hanna Parviainen, sekä vanhempi tietosuoja-asiantuntija Sini Mickelsson avustivat rekisterinpitäjää arvioimaan käsittelytoimien vaikutuksia henkilötietojen suojalle. Vaikutustenarviointi perustuu vaikutustenarvioinnin osallistujien antamaan kuvaukseen ja työpajatyöskentelyyn. Rekisterinpitäjän edustajina vaikutustenarviointiin osallistui sen kohteena olevan henkilötietojen käsittelyn tuntevaa henkilöstöä. Tarkempi listaus vaikutustenarviointiin osallistuneista henkilöistä on löydettävissä vaikutustenarvioinnin yleiskuvauksesta.

2. Tietosuoja koskeva vaikutustenarviointi

Yleiskuvaus vaikutustenarvioinnista

Terveyden ja hyvinvoinnin laitos (THL) on kansallinen asiantuntijalaitos, jonka tarkoituksena on tarjota luotettavaa tietoa terveys- ja hyvinvointialan päätöksenteon ja toiminnan tueksi. THL:n tavoitteena on kehittää valtakunnallinen mobiilisovellus, joka tukee sosiaali- ja terveysministeriön (STM) määrittämää Covid-19-testausstrategiaa: testaa-jäljitä-eristä-hoida. Kehitettävän mobiilisovelluksen avulla voidaan tukea Covid-19-tartuntaketjujen jäljitystyötä terveydenhuollossa ja tartuntaketjujen katkaisemista.

Tämän tietosuoja koskevan vaikutustenarvioinnin (jäljempänä "vaikutustenarviointi" tai "arviointi") kohteena ovat kehitettävän mobiilisovellusratkaisun yhteyteen suunnitellut henkilötietojen käsittelytoimet. Vaikutustenarvioinnin piiriin kuuluu mobiilisovelluksen ja sen taustajärjestelmän lisäksi altistumisilmoitukseen liittyvä prosessi, jossa tartunnalle mahdollisesti altistunut käyttäjä ohjataan ottamaan yhteyttä terveydenhuoltoon Omaolo-palvelun yhteydenottopyyntölomakkeen tai oirearvioinnin kautta. Kuitenkin varsinainen yhteydenottopyyntöjen ja oirearvioiden käsittely SoteDigi Oy:n rekisterinpitäjyyden alaisuudessa ja terveydenhuollon ammattilaisten toimesta kunnallisissa potilastietojärjestelmissä jää tämän arvioinnin ulkopuolelle. Omaolo-palvelusta on laadittu erillinen vaikutustenarviointi. Tämän arvioinnin piiriin kuuluu lisäksi avauskoodien luonti -toiminnallisuus, joka ei ole osa potilastietojärjestelmäksi luokiteltavaa kokonaisuutta.

Vaikutustenarvioinnin tavoitteena on arvioida järjestelmällisesti käsittelytoimia, jotka voivat aiheuttaa luonnollisten henkilöiden oikeuksien ja vapauksien kannalta korkean riskin. Arvioitavat käsittelytoimet ja niistä rekisteröidyn vapauksille ja oikeuksille syntyvät riskit saattavat tulevaisuudessa muuttua, jolloin myös vaikutustenarviointi tulee uusia ja päivittää. Vaikutustenarviointi toteutetaan Privaonin tarjoamana työpajapohjaisena palveluna, jossa Privaonin tietosuoja-asiantuntijat Toni Leppänen ja Hanna Parviainen, sekä vanhempi tietosuoja-asiantuntija Sini Mickelsson avustavat rekisterinpitäjää arvioimaan käsittelytoimien vaikutuksia henkilötietojen suojalle.

Vaikutustenarvioinnin toteuttaminen jakaantuu neljään eri vaiheeseen. Ensimmäinen vaihe alkaa vaikutustenarvioinnin aloitustapaamisella, jossa määritetään vaikutustenarvioinnin kohde ja jossa vaikutustenarvioinnin osallistujat kuvaavat arvioinnin kohteena olevia käsittelytoimia. THL:n toimittaman vaikutustenarvioinnin kohteeseen liittyvän ennakkomateriaalin ja aloitustapaamisen keskusteluiden perusteella laaditaan kuvaus henkilötietojen käsittelystä. Vaikutustenarvioinnin toisessa vaiheessa järjestetään työpaja, jossa arvioidaan käsittelytoimien tarpeellisuutta ja oikeasuhtaisuutta, sekä tietosuojaperiaatteiden ja rekisteröityjen oikeuksien toteutumista arvioinnin kohteen mukaisessa henkilötietojen käsittelyssä. Kolmas vaihe käsittää riskiarviointityöpajan, jossa arvioidaan henkilötietojen käsittelytoimista rekisteröityjen oikeuksille ja vapauksille kohdistuvia riskejä. Neljännessä vaiheessa pidetään lopputapaaminen, jossa käydään läpi määritetyt toimenpiteet ja suositukset riskien hallitsemiseksi. Vaikutustenarviointi perustuu siihen osallistuneiden henkilöiden antamiin kuvauksiin ja työpajatyöskentelyyn.

Vaikutustenarviointiin osallistuneet henkilöt:

Antto Seppälä, hankepäällikkö, Gofore
Andrei Lauren, tietoturvapäällikkö ja tietosuojavastaavan sijainen, THL
Heikki Siltala, pääarkkitehti (aloituspalaverissa Mika Pihlajamäen sijaisena), THL
Mika Pihlajamäki, tietoarkkitehti, THL
Jarkko Reittu, tietosuojavastaava, THL
Jani Harju, ratkaisuarkkitehti, SoteDigi Oy
Jenni Siermala, tietoturvapäällikkö, SoteDigi Oy
Leena Soininen, lääketieteellinen johtaja, SoteDigi Oy
Niklas Murtola, toteutusprojektin projektipäällikkö, Solita Oy
Toni Iltanen, tuoteomistaja, Codecontrol Oy
Joni Fred, projektipäällikkö, Kela

Rosa Jokela, suunnittelun asiantuntija, Kela Karri Maijanen, tietoturva-arkkitehti, Kela Anna-Maija Nurminen-Lempinen, suunnittelun asiantuntija, Kela Toni Leppänen, tietosuoja-asiantuntija, Privaon Oy Hanna Parviainen, tietosuoja-asiantuntija, Privaon Oy Sini Mickelsson, vanhempi tietosuoja-asiantuntija, Privaon Oy
Rekisterinpitäjä
Terveystieteiden tutkimuskeskus, THL PL 30 00271 Helsinki puh. 020 610 6000
Tietosuojavastaava
Jarkko Reittu, tietosuoja(a)thl.fi puh. 029 524 7474.
Kuvaus ennakkomateriaaleista ja muusta arviointiin liittyvästä dokumentaatiosta
Vaikutustenarviointiin sisältyvä materiaali ja dokumentaatio: - mobiilisovelluksen tietosuojailmoitus - mobiilisovelluksen toiminallinen mallinnus - mobiilisovellusratkaisun kehitystyön projektisuunnitelma sekä muu projektin yhteistyötilassa saatavilla ollut materiaali - sovelluskehittäjän laatima uhkamallinnus
Kuvaus vaikutustenarvioinnin kohteeseen liittyvästä erityislainsäädännöstä
EU:n yleinen tietosuoja-asetus (EU) 2016/679 Tietosuojalaki 1050/2018 Tartuntatautilaki 1227/2016 (ml. laki tartuntatautilain väliaikaisesta muuttamisesta) Laki potilaan asemasta ja oikeuksista 17.8.1992/785

3. Kuvaus henkilötietojen käsittelystä

Kuvaus henkilötietojen käsittelytarkoituksesta

Vaikutustenarvioinnin kohteena ovat seuraavat henkilötietojen käsittelytarkoitukset:

- Henkilötietoja käsitellään Covid-19-tartuntaketjujen katkaisemiseksi ja sovellusta käyttävien sekä tartunnalle mahdollisesti altistuneiden henkilöiden tavoittamiseksi ja informoimiseksi;
- Henkilötietoja käsitellään Covid-19-epidemian seurannan ja tietojärjestelmän toiminnan arvioinnin kannalta tarpeellisiin tilastollisiin tarkoituksiin.

Kuvaus henkilötietojen käsittelyn luonteesta

Terveiden ja hyvinvoinninlaitoksen (THL) tavoitteena on kehittää valtakunnallinen mobiilisovellus, joka tukee sosiaali- ja terveysministeriön (STM) määrittämää Covid-19-testausstrategiaa: testaa-jäljitä-eristähoida. Kehitystyön taustalla on valtioneuvoston päätös hybridistrategiasta Covid-19-epidemian hillitsemiseksi. Hybridistrategian avulla pyritään estämään Covid-19-viruksen leviämistä yhteiskunnassa, turvaamaan terveydenhuollon kantokyky ja suojelemaan erityisesti riskiryhmiin kuuluvia ihmisiä. Tavoitteena on, että hybridistrategian avulla epidemiaa onnistutaan tehokkaasti hillitsemään niin, että se haittaa mahdollisimman vähän ihmisiä, yrityksiä, yhteiskuntaa ja perusoikeuksien toteutumista. Kehitettävän mobiilisovelluksen avulla voidaan tukea sekä Covid-19-tartuntaketjujen jäljitystyötä terveydenhuollossa että tartuntaketjujen katkaisemista.

Vaikutustenarvioinnin kohteena oleva henkilötietojen käsittely tapahtuu kehitettävän mobiilisovelluksen (jäljempänä myös "sovellus" tai "jäljitysovellus") ja sen taustajärjestelmän yhteydessä, sekä osana käsittelytarkoituksia palvelevaa prosessia, jossa mahdollisesti altistuneet sovelluksenkäyttäjät ohjataan Omaolo-palvelun yhteydenottolomakkeelle ja oirearvioon. Sovelluksessa ja taustajärjestelmässä käsitellään henkilötiedoksi luokiteltavia pseudotunnisteita, joiden avulla sovelluksen käyttäjä yksilöidään. Mobiilisovelluksen pseudotunniste vaihtuu noin 15 minuutin välein.¹ Tietojen käyttö ja siirto mobiilisovelluksen ja taustajärjestelmän välillä edellyttää sovelluksen käyttäjän suostumusta. Suostumus annetaan sovelluksessa. Mobiilisovellus on kaikille käyttäjille maksuton ja sen käyttö perustuu vapaaehtoisuuteen.

Kun sovelluksen ladanneiden henkilöiden mobiililaitteet kohtaavat, sovellukset tallentavat toistensa yksilölliset pseudotunnisteet, mikäli kohtaaminen tapahtuu altistumisen mahdollistavalla etäisyydellä. Kehitettävä mobiilisovellus hyödyntää muiden mobiililaitteiden etäisyyden tunnistamisessa, kohtaamisen keston mittaamisessa ja pseudotunnisteiden tallentamisessa bluetooth-teknologiaa.

Pseudotunnisteet sekä kohtaamiset tallentuvat mobiililaitteisiin käyttöjärjestelmätasolle. Sovellus vertaa kohtaamiensa pseudotunnisteita taustajärjestelmästä löytyvään tietoon tartunnan saaneiden henkilöiden sovellusten pseudotunnisteista. Mikäli sovellus tunnistaa kohdanneensa tartunnan saaneelle henkilölle kuuluvan pseudotunnisteen, tallentuu tartunnan saaneen pseudotunniste hetkellisesti myös altistuneen henkilön sovellukseen. Taustajärjestelmä voi päiväkohtaisen avaimen avulla tunnistaa kaikki tietyllä mobiililaitteella päiväkohtaisesti kuuluneet pseudotunnisteet, jotta mahdolliset altistumiset on mahdollista kartoittaa.

¹ Näiden 15 minuutin välein vaihtuvien mobiililaittekohtaisten pseudotunnisteiden luomisen sekä altistumistietojen laskemisen mahdollistaa käyttöjärjestelmätasolla toimiva mobiilisovelluksesta erillinen Google/Apple Exposure Notification (GAEN) -rajapinta. Pseudotunnisteiden vaihtaminen ja tallentuminen mobiililaitteisiin edellyttää, että sovelluksen käyttäjä on sallinut GAEN-rajapinnan käyttöönoton mobiililaitteellaan. GAEN-rajapinnan käyttäminen on todettu sovelluksen kehitysvaiheessa edellytykseksi sille, että sovellus voidaan toteuttaa tietoturvasuosin ns. hajautettuun malliin perustuen, jossa tietoa kohtaamisista ja altistumisista ei välitetä yksittäiseen keskitettyyn tietokantaan. GAEN-toteutuksen tietosuojat ei ole ollut tämän vaikutustenarvioinnin kohteena. Kansainvälisesti tarkasteltuna GAEN-toteutuksesta on kuitenkin löydetty arvioita toteutuksen tietosuojariskeistä. Tämän vaikutustenarvioinnin yhteydessä on tunnistettu, että teknologian käyttöön liittyy tietosuojariskejä.

Jos sovellus huomaa olleensa lähikontaktissa tartunnan saaneen henkilön pseudotunnuksen kanssa, sovellus ilmoittaa käyttäjälleen mahdollisesta altistumisesta. Sovelluksen käyttäjälle ei esitetä tartunnan saaneen pseudotunnistetta tai tietoja mahdollisen altistumisen ajankohdasta. Altistumisilmoituksen yhteydessä sovelluksen käyttäjä ohjataan ottamaan yhteyttä hänen kotikuntansa THL:n kanssa sopimaan yhteydenottokanavaan joko puhelimitse tai sähköisen Omaolo-asiointipalvelun kautta, mikäli Omaolo-palvelu on kotikunnassa käytössä. Tämän jälkeen tartunnalle mahdollisesti altistunut henkilö voi halutessaan jakaa tiedon mahdollisesta altistumisestaan, mahdollisista oireistaan sekä yhteystietonsa (nimi, puhelinnumero, kotikunta ja tarvittaessa tilapäinen asuinpaikka) terveydenhuoltoon.

Mikäli sovellusta käytävällä henkilöllä todetaan varmennettu Covid-19-tartunta, voi tartunnan saanut henkilö pyytää diagnoosin saamisen yhteydessä terveydenhuollon ammattilaista toimittamaan sovellukseen syötettävän 12 merkkiä pitkän numerosarjan, jota kutsutaan avauskoodiksi. Avauskoodin tarkoituksena on viestiä sovellukselle, että käyttäjällä, johon tietyt pseudotunnisteet linkittyvät, on todettu tartunta. Tällöin pseudotunnisteiden kohtaamisten avulla voidaan tunnistaa altistuneet käyttäjät ja lähettää heille altistumisilmoitus. Terveydenhuollon ammattihenkilö käyttää avauskooditoiminnallisuuksia Omaolossa olevan käyttöliittymän avulla. Avauskoodi on voimassa neljä tuntia sen luomisesta. Ensisijaisesti koodi toimitetaan tekstiviestillä, mutta terveydenhuollon ammattilainen voi lukea avauskoodin ja antaa ohjeet sen käyttöön tartunnan saaneelle myös puhelimesta.

Avauskoodin sisältävä tekstiviesti lähetetään Kelan hallinnoimasta tekstiviestipalvelusta. Tekstiviestissä tartunnan saanutta ohjataan syöttämään avauskoodi sovellukseen. Tämän jälkeen sovelluksen käyttäjä voi halutessaan syöttää avauskoodin sovellukseen. Avauskoodin syöttämisen jälkeen sovellus lähettää kohdatut pseudotunnisteet eteenpäin taustajärjestelmälle. Sovelluksen käyttäjä saa ilmoituksen tietojen lähettämisestä ja tiedon sovelluksen lukittumisesta. Avauskoodi liitetään henkilön puhelinnumeroon: puhelinnumero ja avauskoodi kulkevat yhdessä tekstiviestipalvelussa.

Käsittelytarkoituksia varten käsitellään rekisteröityjen terveydentilaan liittyviä tietoja, joiden katsotaan yleisen tietosuojasetuksen artiklan 9 mukaisesti kuuluvan niin kutsuttuihin erityisiin henkilötietoryhmiin. Tällaisten henkilötietojen katsotaan olevan erityisen arkaluonteisia rekisteröityjen perusoikeuksien ja -vapauksien kannalta ja niiden käsittely voi asiayhteydestä riippuen aiheuttaa huomattavia riskejä yksilön perusoikeuksille ja -vapauksille.

Rekisteröityjen voidaan lähtökohtaisesti todeta olevan epätasapainoisessa asemassa suhteessa rekisterinpitäjään, sillä rekisterinpitäjänä toimii viranomainen. Epätasapaino korostuu erityisesti niiden rekisteröityjen kohdalla, joilla on todettu varmistettu tartunta tai epäily mahdollisesta altistumisesta. Tästä johtuen rekisteröityjen voidaan katsoa olevan heikommassa asemassa suhteessa rekisterinpitäjään. On myös huomioitavaa, että rekisteröityjen piiriin kuuluu todennäköisesti myös alaikäisiä henkilöitä, sillä sovellukselle ei ole määritetty ikäraja. Sovelluksen käytön ja yhteydenottopyynnön yhteydessä henkilön ikää ei tunnisteta.

Kuvaus henkilötietojen käsittelyn laajuudesta

Sovelluksen toiminta-alue on Suomi ja se on lähtökohtaisesti kaikkien ladattavissa, joiden käytössä on Android tai iOS -käyttöjärjestelmää hyödyntävä mobiililaitte. Jotta mobiilisovellus palvelisi määriteltyjä henkilötietojen käsittelytarkoituksia rekisterinpitäjän toivomalla tavalla, on rekisterinpitäjän tavoitteena, että mahdollisimman suuri osa väestöstä ottaisi sovelluksen käyttöön. Potentiaalisten rekisteröityjen määrän sekä sovelluksen käytön maantieteellisen kattavuuden vuoksi henkilötietojen käsittelyn voidaan katsoa olevan laajaa.

Mobiilisovelluksessa ja taustajärjestelmässä käsitellään seuraavia henkilötietotyyppisiä:

- sovelluksen käyttäjien pseudotunnisteet;
- käyttäjien mobiililaitteiden kohtaamisten kestot;
- tieto mahdollisesta altistumisesta;

- tieto tunnistetusta tartunnasta (avauskoodi); sekä
- puhelinnumero (käsitellään Kelan tekstiviestipalvelussa).

Omaolo-palvelussa olevassa yhteydenottolomakkeessa, jonne mahdollisesti tartunnalle altistuneet rekisteröidyt ohjataan ottamaan yhteyttä, kerätään ja käsitellään seuraavia henkilötietotyypppejä:

- yhteystiedot (etunimi, sukunimi, puhelinnumero, asiointikunta, asiointikieli ja tarvittaessa tilapäinen asuinpaikka).

Terveysdenhuollon ammattihenkilöistä (jäljittäjäkäyttäjät sekä avauskoodin lähettäjät) käsitellään seuraavia henkilötietotyypppejä:

- etu- ja sukunimi;
- yhteystiedot;
- henkilötunnus;
- organisaatio;
- Terhikki-numero (varmennekortin tiedot / ammattihenkilön pätevyys);
- käyttöoikeuden voimassaoloaika;
- lokitieto taustajärjestelmän ammattilaisrajapinnan käytöstä ja avauskoodien luomisesta; sekä
- ammattinimike (vapaaehtoinen).

Henkilötietojen enimmäissäilytysaika sovelluksessa ja taustajärjestelmässä on 21 vuorokautta. Kun käyttäjä poistaa mobiilisovelluksen, kyseisen rekisteröidyn pseudotunniste poistuu mobiililaitteesta mutta ei taustajärjestelmästä. Pseudotunniste poistuu mobiililaitteesta myös silloin, jos rekisteröity poistaa sovelluksen mobiililaitteeltaan. Sähköiset yhteydenottopyynnöt, joiden perusteella terveydenhuolto pyrkii tavoittamaan mahdollisesti altistuneet henkilöt, muodostavat terveydenhuollon toimivaltaisille viranomaisille oman rekisterin. Yhteydenottopyyntöjä ja niiden sisältämiä tietoja säilytetään näissä rekistereissä enintään 21 vuorokautta. Tiedot poistuvat järjestelmästä joko sen jälkeen, kun terveydenhuollon ammattilainen on ollut yhteydessä rekisteröityyn ja sulkee yhteyden, tai, jos rekisteröityyn ei ole oltu yhteydessä, automaattisesti eräajona 21 päivään mennessä yhteydenottopyynnön tekemisestä.

Kuvaus käsittelyn asiayhteydestä

Vaikutustenarvioinnin kohteena oleva henkilötietojen käsittely tapahtuu kehitettävän mobiilisovelluksen ja sovelluksen taustajärjestelmän yhteydessä. Rekisteröidyt voivat ladata sovelluksen sovelluskaupasta Android- tai IOS-käyttöjärjestelmää hyödyntäviin mobiililaitteisiin. Kehitettävän sovelluksen ja taustajärjestelmän toimittaa Solita Oy.

Kela toimii henkilötietojen käsittelijän roolissa rekisterinpitäjän (THL) lukuun siltä osin kuin taustajärjestelmän teknisen alustan ylläpito sitä edellyttää. Kela vastaa THL:n lukuun taustajärjestelmän teknisen alustan ylläpidosta. Kelan tekninen alusta sisältää mm. tietokannat, verkkoyhteydet, ajoympäristön sovelluksille, palomuurin ja kuormanjaon mobiilisovellukselle sekä sen taustajärjestelmille. Taustajärjestelmien ja mobiilisovelluksen kehittäjänä sekä ylläpitäjänä toimii Solita Oy.

Omaolo-palvelu on SoteDigi Oy:n toimittama terveydenhuollon sähköinen asiointipalvelu, jonka avulla rekisteröidyille mahdollistetaan yhteydenottopyyntöjen ja oirearviointien toimittaminen terveydenhuollon ammattilaiselle. Arvioitavien käsittelytoimien osalta SoteDigi toimii henkilötietojen käsittelijän roolissa. Yhteydenottopyynnön tiedot määräytyvät THL:n ohjeistuksen mukaan. Omaolo-palvelun kautta lähetettävän yhteydenottopyynnön perusteella terveydenhuollon ammattilainen pystyy olemaan yhteydessä rekisteröityyn. Mikäli rekisteröity tekee Omaolo-palvelun kautta oirearvion, ohjautuvat

oirearvion tiedot rekisteröidyn kotikunnan perusteella soveltuvan terveydenhuollon potilasrekisterin piiriin.
Omaolo-järjestelmä toimii SoteDigi Oy:n omilla palvelimilla.

4. Arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta

4.1 Käsittelyn oikeasuhteisuutta ja tarpeellisuutta edistävät toimenpiteet

Kuvaus käsittelyn oikeusperusteesta
Vaikutustenarvioinnin kohteen osalta henkilötietojen käsittelyn oikeusperusteena on yleinen etu Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) 6(1)e artiklan mukaisesti. Erityisiin henkilötietoryhmiin kuuluvien tietojen osalta käsittelyn oikeusperusteena toimii tietosuoja-asetuksen 6(1)e artiklan lisäksi tietosuoja-asetuksen 9(2)i artiklan mukainen erityinen oikeusperuste, jonka mukaisesti terveyteen liittyvien tietojen käsittely on sallittua silloin, kun se on tarpeen kansanterveyteen liittyvän yleisen edun vuoksi. Valitut oikeusperusteet on todettu suunniteltuun käsittelyyn soveltuvimmiksi oikeusperustoiksi tartuntatautilain väliaikaisen muutoksen valmisteluasiakirjoissa.² Suunniteltuun käsittelyyn valittujen oikeusperusteiden soveltuvuutta tukevat myös Euroopan tietosuojaneuvoston julkaisemat ohjeet kontaktien jäljitysvälineiden oikeasuhteisen käytön edellytyksistä Covid-19-pandemian yhteydessä.³ Tietojen käyttö ja siirto mobiilisovelluksen ja taustajärjestelmän välillä edellyttää käyttäjän suostumusta. Suostumus ei toimi vaikutustenarvioinnin kohteena olevien käsittelytarkoitusten osalta tietosuoja-asetuksen mukaisena käsittelyn oikeusperusteena, vaan täydentää oikeusperusteita erillisenä suojakeinona rekisteröidyn oikeuksien ja vapauksien suojaamiseksi. Pyydettyä suostumusta avulla pyritään varmistamaan, että rekisteröity on ymmärtänyt henkilötietojen käsittelyn asiayhteyden sovelluksessa ja Omaolo-palvelussa, ja voi paremmin hallita omien henkilötietojensa käsittelyä.
Kuvaus käsittelyn tarkoitusten määrityksestä ja lainmukaisuudesta
Henkilötietoja tullaan käsittelemään ainoastaan tartuntatautilakiin väliaikaisena muutoksena lisätyn 4a-luvun mukaisiin tarkoituksiin, jotka ovat: - Covid-19-tartuntaketjujen katkaiseminen ja sovellusta käyttävien sekä tartunnalle mahdollisesti altistuneiden henkilöiden tavoittaminen ja informointi; - Covid-19-epidemian seurannan ja tietojärjestelmän toiminnan arvioinnin kannalta tarpeelliset tilastolliset tarkoitukset, kuten tilastot sovelluksen käyttöönottoasteesta, arvio kansallisista altistumismääristä, yhteydenottojen ja oirearvioiden lukumäärät, käyttämättä jääneiden avauskoodien lukumäärät, tavallisten yhteydenottojen lukumäärät, yhteydenottojen käsittelyajat, sekä tavoitettujen altistuneiden lukumäärät. Tartuntatautilakiin väliaikaisena muutoksena lisätty 4a-luku edellyttää, ettei vaikutustenarvioinnin kohteena olevia henkilötietoja käytetä myöhemmin poliisitutkinnassa, esitutkinnassa, oikeudenkäynnissä tai muussa lainvalvontaan liittyvässä tarkoituksessa. Tietoja ei myöskään saa käyttää tartuntatautilain 60 §:n mukaisessa päätöksenteossa yksinomaisten perusteena karanteenipäätökselle, eikä muussa Covid-19-tartuntaa koskevaan hoitopäätökseen liittymättömässä julkisen vallan käytössä.

² Hallituksen esitys eduskunnalle laiksi tartuntatautilain väliaikaisesta muuttamisesta (HE101/2020 vp) ja Sosiaali- ja terveystieteiden ministeriön (StVM172020 vp – HE 101/2020 vp)

³ EDPB: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak

Toissijaisia tai muita mahdollisia käyttötarkoituksia ei suunniteltujen käsittelytoimien osalta ole tunnistettu.

Kuvaus henkilötietojen asianmukaisuudesta ja tarpeellisuudesta suhteessa määritettyihin käsittelytarkoituksiin

Tietojen minimointi on ollut mobiilisovellusratkaisun kehitystyössä keskeisenä ja sisäänrakennettuna periaatteena kehitystyön alusta saakka. Mobiilisovelluksen kehitystyön yhteydessä on säännöllisesti kiinnitetty huomiota keinoihin minimoida käsiteltävät henkilötiedot.

Sovelluksessa ja sen taustajärjestelmässä on pyritty teknisten rajausten avulla mahdollisimman minimaaliseen henkilötietojen käsittelyyn henkilötietojen käsittelytarkoitusten tavoitteet huomioon ottaen. Sovelluksen ja sen taustajärjestelmän yhteydessä käsitellään ensisijaisesti vain pseudotunnisteita, joista rekisteröity ei ole suoraan tunnistettavissa. Mobiililaitteessa pseudotunnisteet tallennetaan ainoastaan käyttöjärjestelmätasolle. Sovellus vertaa kohtaamia pseudotunnisteita taustajärjestelmästä löytyvään tietoon tartunnan saaneiden henkilöiden pseudotunnisteista. Mikäli sovellus tunnistaa kohdanneensa tartunnan saaneelle henkilölle kuuluvan pseudotunnisteen, saa sovelluksen käyttäjä ilmoituksen mahdollisesta altistumisesta. Sovelluksen käyttäjälle ei esitetä tartunnan saaneen henkilön pseudotunnistetta tai tietoja mahdollisen altistumisen ajankohdasta. Sovelluksen käyttäjän mobiililaitteelle tallentuneet, kohdatut pseudotunnisteet siirtyvät taustajärjestelmään vain silloin, jos tartunnan saanut henkilö syöttää terveysviranomaisilta saamansa avauskoodin sovellukseen. Käsittelyn tarkoituksia ei ole mahdollista toteuttaa ilman jonkin yksilöivän tiedon ja kohtaamisiin liittyvien tietojen käsittelyä.

Rekisteröityjen puhelinnumeroa käsitellään taustajärjestelmässä vain siinä määrin, kuin se on välttämätöntä tavoittaa rekisteröity yhteydenottopyynnön perusteella tai avauskoodin toimittamiseksi.

Henkilötietojen käsittelyn välttämättömyyttä arvioitaessa suunnitellut käsittelytoimet ovat perusteltavissa ennen kaikkea Covid-19-epidemian hillitsemiseen liittyvien kansanterveydellisten tavoitteiden näkökulmasta. Kehitettävän mobiilisovelluksen tarkoituksena on nopeuttaa virukselle altistuneiden tavoittamista ja tartuntaketjujen katkaisemista. Mobiililaitteen mukana kulkeva sovellus mahdollistaa niiden altistumisen mahdollistavien kohtaamisten tunnistamisen, joita rekisteröity ei itse muista, ole huomionut tai kykene yksilöimään jälkikäteen. Tämä tarkoittaa sitä, että altistumisketjujen tunnistamisessa ei tarvitse nojautua pelkästään rekisteröidyn muistiin tai kertomukseen.

Kuvaus toimenpiteistä sen varmistamiseksi, että henkilötiedot ovat käsittelyn tarkoituksiin nähden täsmällisiä ja tarvittaessa päivitettyjä

Omaolo-palvelun yhteydenottolomakkeelle, jonka kautta mahdollisesti tartunnalle altistuneet rekisteröidyt ohjataan ottamaan yhteyttä, tiedot syöttää rekisteröity itse.

Avauskoodi luodaan vain niille henkilöille, joilla todetaan varmistettu koronavirustartunta. Avauskoodin tuottaminen ja lähettäminen tekstiviestinä oikeaan puhelinnumeroon on jäljittäjäkäyttäjien vastuulla. Jäljittäjäkäyttäjänä toimii vain terveydenhuollon toimintayksiköiden tähän tehtävään nimeämiä terveydenhuollon ammattihenkilöitä. Kun testitulos ilmoitetaan asiakkaalle, samalla kysytään, onko hänellä sovellus käytössä. Mikäli rekisteröity haluaa, että hänelle toimitetaan sovellukseen syötettävä avauskoodi, vahvistaa terveydenhuollon ammattihenkilö rekisteröidyn puhelinnumeron samassa yhteydessä, jossa rekisteröidylle annetaan tieto varmistetusta tartunnasta. Puhelinnumero toimitetaan jäljittäjäkäyttäjälle, joka tarkistaa tässä yhteydessä rekisteröidyltä myös altistumisilmoituksen päivämäärän. Luotu avauskoodi on voimassa neljä tuntia sen luomisesta, jonka jälkeen avauskoodi vanhentuu. Avauskoodin syöttämisen yhteydessä sovellus ei ohjaile käyttäjää siten, että avauskoodin formaatista kerrotaisiin tarkasti. Sovellus ilmoittaa, mikäli syötetty avauskoodi on väärä.

Käsiteltävien henkilötietojen säilymistä ajantasaisena edistää se, että henkilötietojen enimmäissäilytysaika on 21 vuorokautta.

Kuvaus asetetuista määräajoista henkilötietojen poistoa varten tai kuvaus toimenpiteistä säilyttämisen tarpeellisuuden määräaikaistarkastelua varten

Henkilötietojen enimmäissäilytysaika sovelluksessa ja taustajärjestelmässä on 21 vuorokautta (pois lukien varmuuskopiot ammattilaisten käyttöliittymässä tehtyjen toimenpiteiden lokitiedot). Enimmäissäilytysaika määriteltiin tartuntatautilain väliaikaisen muutoksen lainvalmisteluvaiheessa ja se perustuu tämänhetkiseen epidemiologiseen tietoon koronavirustaudin enimmäisitämisajasta, joka on 14 vuorokautta, sekä siihen, että tiedot on välttämätöntä säilyttää mainitun 14 vuorokauden itämisajan lisäksi seitsemän vuorokautta itämisajaa pidemmän ajan, jotta mobiilisovelluksen käyttäjällä on riittävä aika hakeutua testattavaksi ja reagoida saamaansa tartuntatietoon.

Kelan taustajärjestelmässä käsiteltävät tiedot (pseudotunniste, avauskoodi, puhelinnumero) kuuluvat Kelan virtuaalikonevarmistuksen piiriin ja ne poistetaan 21 vuorokauden kuluttua niiden varmistukseen tallennuksesta. Taustajärjestelmässä mobiilisovelluksen tietokanta- ja SMS-palvelimista varmistetaan koko virtuaalipalvelimen levykuva. Varmuuskopiointilla toteutetaan järjestelmän ja järjestelmässä olevan tiedon saatavuus ja eheys koko varmistusajan. Omaolo-palveluun rakennettavassa ammattilaisten käyttöliittymässä tehtävät toimenpiteet (lokietä käyttöliittymän käytöstä ja avauskoodien luomisesta) tallennetaan Kelan lokipalvelimelle ja niitä säilytetään JUHTA-suosituksen mukaisesti 12 vuoden ajan mahdollisten väärinkäytösten selvittämiseksi ja käytönvalvonnan toteuttamiseksi.

Suunniteltujen käsittelytoimien osalta on tehty päätös siitä, että henkilötietojen käsittely määritellyjä käsittelytarkoituksia varten lopetetaan vuoden 2021 maaliskuun loppuun mennessä. Tällöin myös kaikki silloin tallennettuna tai muutoin käsiteltävänä oleva henkilötieto poistetaan. Kun mobiilisovelluksen käyttö lopetetaan, huolehtii THL henkilötietojen poistamisesta ja poistaa mobiilisovelluksen myös sovelluskaupoista. Tämä tietojen poistamisen takaraja ei kuitenkaan koske potilastietojärjestelmään potilaslain mukaisesti tallennettavia henkilötietoja, kuten terveydenhuoltoon toimitettavan oirearvioinnin tietoja, jotka eivät ole tämän vaikutustenarvioinnin kohteena.

Yhteydenottoihin liittyvät tiedot poistetaan heti, kun henkilöön on otettu yhteyttä ja terveydenhuollon ammattilainen on sulkenut yhteydenottopyynnön. Mikäli yhteyttä ei oteta, poistuvat yhteydenottolomakkeen yhteydessä kerätyt henkilötiedot automaattisesti viimeistään 21 vuorokauden kuluttua.

Kuvaus teknisistä ja organisatorisista toimenpiteistä, joilla varmistetaan henkilötietojen asianmukainen turvallisuus ja luottamuksellisuus

Rekisterinpitäjänä THL valvoo käsiteltävien henkilötietojen tietoturvan tasoa THL:n tietoturvallisuuden toimintamallin mukaisesti. Toimintamalliin kuuluvat säännölliset tietoturva-auditoinnit ja sen osana toimii THL:n oma tietoturvatimi. Mobiilisovelluksen auditoimiseen käytetään OWASP Mobile security guideline -kriteeristöä. Taustajärjestelmän auditoimiseen käytetään Katatrin 4. tason kriteeristöä. Kyberturvallisuuskeskus toteuttaa tietoturva-arvioinnin mobiilisovelluskokonaisuuden osalta ennen sovelluksen julkaisua. Kun sovelluksen yleinen käyttö on aloitettu, tehdään sovellukselle mahdollisesti vielä uusi tietoturva-auditointi ja haavoittuvuustestaus.

Omaolo-palvelun osalta organisatorisena toimenpiteenä henkilötietoihin pääsevät vain terveydenhuollon toimintayksiköiden tähän tehtävään nimeämät terveydenhuollon ammattihenkilöt, joita sitoo salassapitovelvollisuus. Omaolo-palvelun sovellusturvallisuutta on arvioitu ulkopuolisen auditoijan toimesta OWASP-kriteeristön sekä muiden alan yleisten tietoturvakriteeristöjen mukaisesti. Omaolo-palvelusta on laadittu oma tietosuojaa koskeva vaikutustenarviointi. Omaolo-palvelun toteutuksessa noudatetaan tämän lisäksi useita standardeja⁴, jotka määrittelevät lääkinnällisten laitteiden käytettävyyttä, riskienhallintaa ja laadunhallintajärjestelmää, sekä terveydenhuolto-ohjelmistotuotteiden turvallisuuden varmistamista.

⁴ IEC 62366-1:2015/COR1:2016, SFS-EN ISO 14971:2019, SFS-EN ISO 13485, IEC 82304-1:2016

Kehitettävän sovelluksen ja taustajärjestelmän toimittava Solita Oy on laatinut oman uhkamallinnuksen sovelluksesta ja sen taustajärjestelmästä. Taustajärjestelmä toimii Kelan teknisellä alustalla, joka sijaitsee Suomessa.

Kuvaus henkilötietojen käsittelyn eri osapuolista ja heidän rooleistaan (käsittelijät, rekisterinpitäjä, yhteisrekisterinpitäjä) sekä suojatoimista asianmukaisen käsittelyn varmistamiseksi

Vaikutustenarvioinnin kohteena olevien käsittelytoimien rekisterinpitäjänä toimii THL. Käsittelytoimiin ei liity yhteisrekisterinpitäjiä.

Kansaneläkelaitos (Kela) vastaa rekisterinpitäjän lukuun taustajärjestelmän ylläpidosta THL:n määrittelemällä tavalla. Kela toimii henkilötietojen käsittelijän roolissa. Vaikutustenarvioinnin tässä vaiheessa ei THL:n ja Kelan välillä ole vielä sovittu käsittelystä tietosuoja-asetuksen artiklan 28 mukaisella käsittelysopimuksella. Käsittelysopimus tulee olemaan osa Kelan ja THL:n välistä ylläpitosopimusta.

Yhteydenottoopyyntöjen sisältävät tiedot sekä jäljittäjäkäyttäjien toimet yhteydenottoopyyntöihin liittyen tallentuvat SoteDigi Oy:n hallinnassa olevaan tietokantaan, jonka rekisterinpitäjä on THL. SoteDigi on henkilötietojen käsittelijän roolissa yhteystietolomakkeen tarjoamisen yhteydessä käsiteltävien henkilötietojen osalta. THL:n ja SoteDigin välillä on sovittu käsittelystä tietosuoja-asetuksen artiklan 28 mukaisella käsittelysopimuksella.

Solita Oy toimittaa mobiilisovelluksen taustajärjestelmän THL:lle ja luovuttaa sen Kelalle asennettavaksi. Tuotantoympäristöön on pääsy vain Kelalla. Solita tulee olemaan mukana sovelluksen ja taustajärjestelmän jatkokehityksessä ja tarjoaa näiden osalta myös teknistä tukea, mutta Solitalla ei tule sovelluksen ja taustajärjestelmän toimittamisen jälkeen olemaan suoraa pääsyä henkilötietoihin. Mobiilisovelluksen jatkokehityksessä tullaan käyttämään ainoastaan kuvitteellista dataa. Solita ja Mediconsultin konsortio toimittaa erillisen hankkeen puitteissa myös terveydenhuollon ammattilaisille Omaolo-palveluun rakennettavan käyttöliittymän.

Kuvaus suojatoimista liittyen kansainvälisiin henkilötietojen siirtoihin

Palvelut, joiden yhteydessä tämän vaikutustenarvioinnin kohteena olevia henkilötietoja käsitellään, tarjotaan vain Suomessa. EU-yhteentoimivuuden käyttöönottoa harkitaan mahdollisesti tulevaisuudessa. Kaikki tuotantodata tulee sijaitsemaan Suomessa. Rekisterinpitäjän tai käsittelijöiden toteuttamia henkilötietojen siirtoja tai luovutuksia EU:n tai ETA:n ulkopuolelle ei ole tunnistettu.

4.2 Rekisteröityjen oikeuksia edistävät toimenpiteet

Kuvaus toimenpiteistä, joilla toimitetaan rekisteröidylle artikla 13 ja artikla 14 mukaiset tiedot

Sovelluksen latauksen yhteydessä rekisteröidylle annetaan sovelluskaupassa tieto sovelluksen käyttöehdoista, jotka sisältävät linkin tietosuojaselosteeseen.

Sovelluksen käyttöönoton yhteydessä rekisteröidylle annetaan sovelluksen ensimmäisellä ohjeistussivulla tietoa sovelluksen yleisistä toimintaperiaatteista. Tämän jälkeen sovellus näyttää rekisteröidylle sovelluksen tietosuojasta kertovan ikkunan, jolla rekisteröidylle kerrotaan yleistä tietoa siitä, millä tavoin henkilötietoja tullaan sovelluksen yhteydessä käsittelemään. Tässä yhteydessä rekisteröityä edellytetään hyväksymään palvelun käyttöehdot sekä vakuuttamaan, että sovellus otetaan käyttöön vapaaehtoisesti. Tämä yleinen sovelluksen toiminnasta ja henkilötietojen käsittelystä annettava informaatio on selkeää ja helppolukuista.

Vaikutustenarviointia varten katselmoitavana olleessa mobiilisovelluksen toiminnallisessa mallinnuksessa tietosuojaselostetta ei tuotu rekisteröidyn tiedoksi sovelluksen käyttöönoton yhteydessä. Kuitenkin

valmiissa sovelluksessa tietosuojaseloste tullaan toimittamaan rekisteröidyille, kun sovelluksen otetaan käyttöön. Lisäksi tietosuojaseloste on rekisteröidyn saatavilla sovelluksen Asetukset-välilehdellä sekä THL:n valitsemissa erillisissä viestintäkanavissa. Tietosuojaseloste sisältää yleisen tietosuoja-asetuksen mukaiset rekisteröidylle annettavat tiedot.

Tietosuojaseloste on ymmärrettävää yleiskieltä, jota rekisteröidyn on helppo lukea ja ymmärtää. Helppolukuisuus edistää myös alaikäisten rekisteröityjen mahdollisuutta ymmärtää käsittelystä toimitettava tieto. Tietosuojaselosteen helppolukuisuutta lisäävät väliotsikot ja lihavoidut tekstit, joilla korostetaan kappaleen keskeisimpiä tietoja (mm. rekisterinpitäjän nimi ja käsittelyn oikeusperuste). Käsittelyn oikeusperusteena olevaa yleistä etua ei ole avattu tarkemmin. Tämä on kuitenkin kerrottu sovelluksen latauksen yhteydessä, jolloin rekisteröidylle kerrotaan, että sovelluksen tavoitteena on ehkäistä koronavirustaudin leviämistä.

Jäljitysovelluksen tietosuojaselosteen lisäksi rekisteröityä informoidaan hänen henkilötietojensa käsittelystä Omaolo-palvelussa. Mikäli rekisteröity haluaa jättää yhteydenottopyynnön, pyydetään häneltä suostumus tietojen välittämiseksi terveydenhuoltoon ja osoitetaan linkki Omaolon tietosuojaselosteeseen. Mikäli rekisteröity haluaa tehdä Omaolon oirearvion, hän hyväksyy Omaolo-palvelun käyttöehdot, Omaolo-palvelun yleisen tietosuojaselosteen sekä evästeiden käytön Omaolo-palvelussa sekä sen, että Omaolo-palvelu arvioi rekisteröidyn hoidon ja palvelun tarvetta ja antaa toimintasuosituksia rekisteröidylle tämän antamien tietojen perusteella.

Omaolo-palvelun tietosuojaseloste on kirjoitettu ymmärrettävällä ja selkeällä yleiskielellä. Jäljitysovellusta koskevat osiot on kirjattu osaksi muuta tietosuojaselostetta. Sovellusta koskevat tiedot ovat löydettävissä, mutta koska käsittelytoimia on monia ja tietosuojaseloste on pitkä, on mahdollista, että rekisteröity joutuu etsimään jäljitysovellusta koskevaa tietoa hetken aikaa.

Kuvaus toimenpiteistä, joilla toimitetaan rekisteröidylle artikla 15 – artikla 22 tiedot (rekisteröidyn oikeudet)

Tietoa rekisteröidylle tietosuoja-asetuksen mukaisesti kuuluvista oikeuksista ei vaikutustenarvioinnin tässä vaiheessa toimiteta rekisteröidylle sovelluksen yhteydessä. Tämä tieto tullaan toimittamaan osana tietosuojaselostetta, jonka laatiminen on kesken. **Tästä syystä käsittelytoimien läpinäkyvyyttä ei voida vaikutustenarvioinnin tässä vaiheessa riittävällä tasolla arvioida.** Kun tietosuojaseloste on valmis, tullaan se toimittamaan rekisteröidylle tiedoksi sovelluksessa, sekä THL:n valitsemissa, erillisissä viestintäkanavissa.

Rekisterinpitäjällä on jo ennen suunniteltuja käsittelytoimia ollut käytössään prosessi, jonka mukaisesti rekisteröityjen pyynnöt käsitellään. Tietosuoja-asetuksen artikla 11 mukaisesti rekisteröidyn oikeuksia ei sovelleta, jos rekisterinpitäjä ei pysty tunnistamaan rekisteröityä luotettavalla tavalla.

Kuvaus toimenpiteistä, joilla varmistetaan rekisteröidyn oikeus saada pääsy tietoihinsa

Lähtökohtaisesti rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy henkilötietoihin tietosuoja-asetuksen artiklan 15 mukaisesti. Kuitenkin, jos käsittelykohteen määrittäminen henkilötietojen käsittely voidaan suorittaa ilman rekisteröidyn tunnistamista, rekisterinpitäjällä ei ole velvollisuutta hankkia lisätietoja ainoastaan rekisteröidyn oikeuksien toteuttamiseksi määritettyjen oikeuksien toteuttamiseksi. Siltä osin kuin rekisterinpitäjä ei pysty tunnistamaan rekisteröityä tiedoista, tarkastusoikeutta ei sovelleta, koska se ei ole mahdollista. Rekisterinpitäjän arvion mukaan sillä ei ole mahdollisuutta tunnistaa rekisteröityä pseudotunnisteen perusteella. Puhelinnumeron osalta rekisteröidyn on mahdollista tarkastaa tietonsa.

Mobiilisovelluksessa käsitellään ensisijaisesti vain 15 minuutin välein vaihtuvia pseudonymisoituja tunnistetta, joiden perusteella rekisteröityä ei ole mahdollista tunnistaa suoraan. Pseudotunnisteen on tarkoitettu rekisteröityjen kohtaamisten – ei yksittäisen rekisteröidyn henkilöllisyyden – tunnistamiseksi.

Avauskoodista tallentuu ainoastaan tieto siitä, onko avauskoodi käytetty. Tietoa siitä, missä laitteessa koodi on käytetty, ei tallenneta.

Omaolo-palveluun rekisteröitynyt käyttäjä voi palvelun käyttöehtojen mukaisesti tarkastaa omat tietonsa palvelun kautta, mutta ei voi nähdä yhteydenottolomakkeella lähetettyjä tietoja, sillä näitä tietoja ei tallenneta Omaloon.

Kuvaus toimenpiteistä, joilla varmistetaan rekisteröidyn oikeus tietojensa oikaisemiseen

Rekisterinpitäjän arvion mukaan sillä ei ole mahdollisuutta luotettavalla tavalla tunnistaa rekisteröityä pseudotunnisteen perusteella. Siltä osin kuin rekisterinpitäjä ei pysty tunnistamaan rekisteröityä tiedoista, oikaisu-oikeutta ei sovelleta, koska se ei ole mahdollista.

Mobiilisovelluksessa tai taustajärjestelmässä ei myöskään käsitellä rekisteröidystä sellaisia tietoja, joita tämän olisi tietojen luonteen puolesta mahdollista oikaista.

Omaolo-palvelussa rekisteröity voi käydä tekemässä oirearvion uudelleen, mikäli hän on antanut virheellisiä tietoja alkuperäisen oirearvion yhteydessä. Jos henkilö on täyttänyt oirearvion Omaolo-palvelussa, ja se on siirtynyt terveydenhuollon potilasrekisteriin, tulee tämän ottaa yhteyttä sairaanhoitopiiriin.

Terveydenhuollon ammattilaisen käyttöliittymän osalta ammattilaisella on oikeus tarkistaa tietonsa ja korjata niitä. Korjaus tapahtuu SoteDigin käyttäjänhallinnassa ja terveydenhuollon ammattilaiset voivat tehdä käyttöoikeuksiin liittyviä pyyntöjä mm. asiakaspalvelun kautta.

Kuvaus toimenpiteistä, joilla varmistetaan rekisteröidyn oikeus tietojen poistamiseen

Tämä oikeus ei tule sovellettavaksi vaikutustenarvioinnin kohteena olevien käsittelytarkoitusten osalta, sillä oikeutta ei tietosuoja-asetuksen artiklan 17(3) b ja c -kohdan mukaisesti sovelleta, jos käsittely on tarpeen:

b) rekisterinpitäjään sovellettavaan unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan, käsittelyä edellyttävän lakisääteisen velvoitteen noudattamiseksi tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten;

c) kansanterveyteen liittyvää yleistä etua koskevista syistä artiklan 9 2 kohdan h ja i alakohdan sekä artikla 9 3 kohdan mukaisesti.

Rekisteröity voi poistaa sovelluksen mobiililaitteesta, jolloin mobiililaitteessa olevat tiedot poistuvat välittömästi ja mahdollisesti taustajärjestelmässä olevat pseudotunnistetiedot poistuvat automaattisesti viimeistään 21 päivän kuluessa.

Kuvaus toimenpiteistä, joilla varmistetaan rekisteröidyn oikeus käsittelyn rajoittamiseen

Rekisterinpitäjän arvion mukaan sillä ei ole mahdollisuutta luotettavalla tavalla tunnistaa rekisteröityä pseudotunnisteen perusteella, vaikka tämä toimittaisi rekisterinpitäjälle lisätietoja. Siltä osin kuin rekisterinpitäjä ei pysty tunnistamaan rekisteröityä tiedoista, rajoitus-oikeutta ei sovelleta, koska se ei ole mahdollista.

Kuvaus toimenpiteistä, joilla varmistetaan rekisteröidyn oikeus siirtää tiedot järjestelmästä toiseen

Tämä oikeus ei tietosuoja-asetuksen artiklan 20(1) kohdan mukaisesti tule sovellettavaksi vaikutustenarvioinnin kohteena olevien käsittelytarkoitusten osalta, sillä käsittely ei perustu rekisteröidyn antamaan suostumukseen eikä rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöönpanoon. Suostumus ei toimi vaikutustenarvioinnin kohteena olevien käsittelytarkoitusten osalta tietosuoja-asetuksen mukaisena käsittelyn oikeusperusteena, vaan täydentää oikeusperusteita erillisenä suoja-keinona rekisteröidyn oikeuksien ja vapauksien suojaamiseksi.

Tätä oikeutta ei tietosuoja-asetuksen artiklan 20(3) kohdan mukaisesti sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten.

Kuvaus toimenpiteistä, joilla varmistetaan rekisteröidyn oikeus erityiseen tilanteeseensa liittyvällä perusteella vastustaa käsittelyä

Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, jonka oikeusperusteena on yleinen etu Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) 6(1)e artiklan mukaisesti. Vaikutustenarvioinnin aikana ei tunnistettu erityisiä henkilökohtaisia tilanteita, joihin vedoten rekisteröity voisi vastustaa käsittelyä. Rekisteröity voi kuitenkin milloin tahansa poistaa mobiilisovelluksen käytöstä.

Tartunnasta ilmoittaneiden pseudotunnisteiden käsittely taustajärjestelmässä on välttämätöntä mahdollisesti altistuneiden henkilöiden varoittamiseksi, joten kerättyjä pseudotunnisteita ei voida poistaa, vaikka rekisteröity vastustaisi käsittelyä.

Kuvaus oikeusperusteesta ja suoja-toimista, mikäli rekisteröity on päätöksen kohteena, joka perustuu pelkästään automaattiseen käsittelyyn, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi

Vaikutustenarvioinnin kohteena olevien käsittelytoimien yhteydessä ei tehdä pelkästään automaattiseen henkilötietojen käsittelyyn perustuvia päätöksiä, joilla olisi oikeusvaikutuksia rekisteröidyn kannalta tai jotka vaikuttaisivat häneen vastaavalla tavalla merkittävästi.

5. Henkilötietojen käsittelyyn liittyvät riskit

Tietosuojaa koskevan vaikutustenarvioinnin avulla rekisterinpitäjä tunnistaa rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä. Alla olevaan taulukkoon on kirjattu vaikutustenarvioinnissa tunnistetut riskit. Riskit on luokiteltu niiden riskitason mukaan. Riskitaso määräytyy riskien vaikutusten todennäköisyyden ja vakavuuden perusteella.⁵ Riskien vaikutusten todennäköisyyttä ja vakavuutta määrittelevät ne toimet, joita rekisterinpitäjä on jo tehnyt rekisteröidyille aiheutuvien riskien lieventämiseksi. Vaikutustenarviointiin dokumentoidaan myös ne suunnitellut toimenpiteet, jotka rekisterinpitäjä aikoo toteuttaa tunnistettujen riskien riskitason laskemiseksi. Jäännösriski on arvio riskitasosta näiden suunniteltujen toimenpiteiden toteuttamisen jälkeen.

Riskitasot esitetään taulukossa seuraavalla yksinkertaisella väriasteikolla:

	Matala riski tai ei riskiä
	Keskinkertainen riski, suositellaan toimenpiteitä
	Korkea riski, vaatii toimenpiteitä

#	Riskin alkuperä ja luonne	Riskin vaikutus rekisteröidyn oikeuksiin ja vapauksiin	Riskin vaikutusten todennäköisyys ja vakavuus	Suunnitellut toimenpiteet	Jäännösriski

⁵ Todennäköisyys ja vakavuus arvioidaan tässä vaikutustenarvioinnissa asteikolla 1-3 seuraavalla tavalla: **todennäköisyys**: 1 = kaukainen, 2 = mahdollinen 3 = hyvin mahdollinen; **vakavuus** 1 = vähäisiä vaikutuksia, 2 = tunnistettuja vaikutuksia, 3 = vakavia vaikutuksia.

--	--	--	--	--	--

[illegible]

--	--	--	--	--	--

--	--	--	--	--	--

--	--	--	--	--	--

--	--	--	--	--	--

--	--	--	--	--	--

Muut tunnistetut jatkotoimenpiteet ja suositukset

Suositellaan, että SoteDigi arvioi Omaolo-palvelusta laaditun erillisen vaikutustenarvioinnin mahdollisen päivitystarpeen.

Suositellaan, yhteydenottopyynnön yhteydessä kerättävän suostumuksen asianmukaisuus arvioidaan, ja siltä osin kuin suostumus kerätään käsittelyn oikeusperusteeksi, varmistetaan, että suostumus täyttää tietosuoja-asetuksen artikla 7 määritellyt edellytykset. Kyseinen suostumusratkaisu ei ole ollut katselmoitavana tämän vaikutustenarvioinnin yhteydessä.

6. Sidosryhmien huomiot

Tietosuojavastaavan huomiot
Vaikutustenarviointi on laadittu tietosuoja-asetuksen 35 artiklan edellyttämällä tavalla. Vaikutustenarvioinnin perusteella ei ole ilmennyt sellaisia rekisteröityjen oikeuksiin ja vapauksiin liittyviä riskejä, jotka estäisivät jäljityssovelluksen käyttöönoton. Lisäksi esiin tulleiden riskien pienentämiseksi on suunniteltu asianmukaisia toimenpiteitä. Vaikutustenarvioinnin perusteella suunniteltuun henkilötietojen käsittelyyn ei myöskään sisälly sellaisia tietosuoja-asetuksen 36 artiklan mukaisia korkeita riskejä, jotka edellyttäisivät tietosuojavaltuutetun ennakkokuulemistä. Vaikutustenarviointia tulee päivittää tarvittaessa.
Rekisteröityjen tai näiden edustajien näkemykset
Vaikutustenarvioinnissa rekisterinpitäjä arvioi tapauskohtaisesti pyydetäänkö rekisteröityjen tai näiden edustajien näkemyksiä käsittelytoimista. Tähän vaikutustenarviointiin ei pyydetty rekisteröityjen tai näiden edustajien näkemyksiä.
Muut sidosryhmät ja heidän huomionsa
Vaikutustenarvioinnissa rekisterinpitäjä arvioi tapauskohtaisesti pyydetäänkö muiden sidosryhmien huomioita käsittelytoimista. Tähän vaikutustenarviointiin ei pyydetty muiden sidosryhmien huomioita.