15.6.2020

Eduskunta

Liikenne- ja viestintävaliokunta

Lausunto: HE 101/2020 vp Hallituksen esitys eduskunnalle laiksi tartuntatautilain väliaikaisesta muuttamisesta

F-Secure kiittää mahdollisuudesta lausua hallituksen esityksestä tartuntalain väliaikaisesta muuttamisesta ja ehdotuksesta säätää covid-19-epidemian aiheuttaneen koronaviruksen tartuntaketjujen katkaisua tehostavasta tietojärjestelmästä koronavirukselle mahdollisesti altistuneiden tavoittamiseksi.

F-Secure pitää hyvänä, että koronaviruksen tartuntaketjujen jäljittämisen ja katkaisemisen tueksi suunnitellusta tietojärjestelmästä säädetään lailla, ratkaisu toteutetaan hajautettuna, vapaaehtoisuuteen pohjautuvana sekä ajallisesti ja vain tähän yhteen selkeästi määriteltyyn käyttötarkoitukseen rajattuna. Tärkeä osa mobiilisovelluksen luotettavuutta on sen lähdekoodin julkaisu avoimesti, jotta sen toimintaa voidaan arvioida riippumattomasti.

Esityksessä korostetaan tietojärjestelmän (mobiilisovellus ja taustajärjestelmä) tietoturvaa. Tämä on ensiarvoisen tärkeää. Vahva tietoturva lisää kansalaisten luottamusta ratkaisuun ja kannustaa osaltaan mobiilisovelluksen käyttöönottoon. On siis tärkeää, että tietoturvatestauksen asiantuntijat voivat testata sovelluksen ja siihen mahdollisesti tehtävät päivitykset ja käydä läpi ratkaisun tietoturva-arkkitehtuurin kokonaisuuden.

Esityksessä kuvattu toiminnallisuus vastaa Applen ja Googlen poikkeuksellisessa yhteistyössä kehittämän Exposure Notification -rajapinnan toimintaa. Pidämme perusteltuna kehittää mobiilisovellus Applen ja Googlen rajapintaa käyttäen. Tämä on itseasiassa Apple iOS-laitteiden osalta käytännössä ainoa mahdollinen tapa toteuttaa mobiilisovellus.

Osa mobiilisovelluksen ominaisuuksista määräytyy rajapinnan (ja täten Applen ja Googlen) päätöksistä eikä niihin voi välttämättä vaikuttaa sovelluskehityksessä. Muun muassa tästä syystä olisi tärkeää, että lain tasolla ei määritetä sellaisista teknisistä yksityiskohdista, joiden muuttuminen saattaa tehdä järjestelmästä lainvastaisen, vaikka ne eivät todellisuudessa vaikuttaisikaan tietosuojan tasoon ja joihin ei kansallisen sovelluksen puitteissa voida vaikuttaa. Asioita, jotka määräytyvät ainakin osin rajapinnan mukaan ovat esimerkiksi tietojen säilytysaika laitteessa (Applen määritelmän mukaan tällä hetkellä 14 päivää) sekä rajapintatoteutuksen tallentamat ja käsittelemät tiedot, joita käytetään esimerkiksi altistusriskiarvioon.

F-Secure Corporation Tammasaarenkatu 7 P.O. Box 24 FI-00181 Helsinki Finland
Tel: +358 9 2520 0700 www.f-secure.com
Business id 0705579-2 Registered office Helsinki

Lain tasolla voisi olla perusteltua määrätä vain siitä, että järjestelmä takaa pseudonymiteetin esitöissä kuvatulla tasolla käyttäjien välillä sekä tartunnan raportointiin asti myös viranomaisille päin, eikä nimetä laissa tarkasti niitä teknisiä tietoja, joita laitteessa saa tallentaa ja käsitellä. Näin mahdollistettaisiin vaikka se, että rajapinta käyttäisi ja käsittelisi tulevaisuudessa esimerkiksi riskiarvion parantamiseen liikesensori- ja älykellodataa ilman, että kyseinen data lähetetään laitteesta ulos. Laite pystyisi esimerkiksi päättelemään, onko se todellisuudessa ollut käyttäjän mukana, autossa, jne. Koska tietoa ei jaettaisi laitteesta ulos, vaikutus tietosuojaan ei olisi merkittävä. Applen ja Googlen rajapinnan tekemää altistusriskiarviota ei ole huomioitu esityksen 43 c pykälän 2 momentin 2 kohdassa.

Laissa tulisi olla mahdollisuus myös siihen, että jos rajapinnan tietojen säilytysaika mobiililaitteessa muuttuu käyttöjärjestelmävalmistajan muutoksen vuoksi pidemmäksi kuin mainittu 21 päivää, järjestelmä ei muutu saman tien lainvastaiseksi vaan viranomaisilla olisi mahdollisuus hallitusti tehdä päätökset jatkosta. Näin voisi hypoteettisesti käydä, jos esimerkiksi viruksen käyttäytymisestä saadaan uutta tietoa ja Apple ja Google päättävät yksipuolisesti muuttaa tallennusaikaa. Taustajärjestelmän tallennusaikaan, joka myös on tietosuojan kannalta merkittävämpi, tällä ei tietenkään tarvitse olla vaikutusta.

Yksityisyyden suojan varmistamiseksi olisi tärkeää ottaa kantaa myös siihen, miten varmistetaan, että kyseessä on oikea henkilö. Mikäli henkilö käyttää altistumisensa jälkeen järjestelmää henkilötietojen jakamiseen terveysviranomaisille, on tärkeää varmistaa, että henkilö ei anna toisen henkilön tietoja. Teknisesti tämä voitaisiin toteuttaa esimerkiksi niin, että annettuun puhelinnumeroon lähetetään vahvistuskoodi ja tiedot välitetään terveydenhuoltoviranomaisille vasta vahvistuskoodin sovellukseen syöttämisen jälkeen.

Kun tietojärjestelmä poistetaan käytöstä (43 a pykälä 4 momentti), pykälän perusteluissa edellytetään henkilötietojen poistamista ja sovelluksen poistamista sovelluskaupoista. Käytännössä olisi suositeltavaa, että sovelluksessa olisi ominaisuus, jolla se voisi ilmoittaa käyttäjälle olevansa poistettu käytöstä ja ohjeistaa poistamaan sovelluksen laitteesta. Mobiililaite saattaa (käyttöjärjestelmästä riippuen) jatkaa tietojen keräämistä ja oman pseudonyyminsä julkaisua Bluetoothilla niin kauan kuin sovellus on laitteessa, vaikka se olisikin poistettu sovelluskaupoista.

Laissa ja sen esitöissä olisi hyvä huomioida myös kansainvälinen ja Euroopan unionissa tehtävä yhteistyö ja tartuntaketjujen jäljitettävyys myös rajat ylittävissä kohtaamisissa. Esitys ei tällaisenaan mahdollista valtioiden välistä tietojen jakamista. Koska muilla mailla on todennäköisesti käytössään samaan teknologiaan perustuvia ja täten yhteensopivia järjestelmiä, voisi mahdolliseen tiedonjakoon valmistautua esimerkiksi seuraavasti:

- Sallimalla sen, että muiden valtioiden toimivaltaisilta viranomaisilta saadaan vastaanottaa todennetun tartunnan saaneiden tunnisteita ja niitä käsitellään, kuten kansallisesti kerättyjä tunnisteita;

15.6.2020

- Sallimalla sen, että kun henkilö ilmoittaa tartunnastaan sovelluksen kautta, häneltä saadaan kysyä matkustamisesta ulkomailla ja pyytää näissä erillisissä tapauksissa lupa luovuttaa tunnisteet eteenpäin kyseisen maan toimivaltaisille viranomaisille, mikäli Suomen toimivaltainen viranomainen on hyväksynyt vastaanottajan ja tietosuojan taso vastaa Suomen linjauksia.

F-Secure on mielellään käytettävissä ja tuomassa teknistä tietoturva-asiantuntemustamme tietojärjestelmän ja kokonaisratkaisujen suunnitteluun ja käyttöönottoon.

Samu Konttinen
Toimitusjohtaja
F-Secure Oyj

F-Secure Corporation Tammasaarenkatu 7 P.O. Box 24 FI-00181 Helsinki Finland
Tel: +358 9 2520 0700 www.f-secure.com
Business id 0705579-2 Registered office Helsinki