Microsoft Oy

Lausunto

05.05.2020

Asia: VN/10058/2020, STM053:00/2020

Lausuntopyyntö esityksestä kontaktien jäljityssovelluksen käyttöönotosta Covid-19-epidemian hallinnan tueksi

Kysymykset

1. Muistiossa esitellään mobiilisovellus tukemaan tartuntatautien jäljitystyötä ja tartuntaketjujen katkaisemista. Onko tämä tarkoituksenmukainen tapa jäljittää tartuntaketjuja?

-

Avoimet huomiot koskien kysymystä 1

-

2. Onko esityksessä asianmukaisesti otettu huomioon henkilötietojen ja yksityisyyden suojaan liittyvät näkökohdat?

-

Avoimet huomiot koskien kysymystä 2

-

3. Onko muistiossa tunnistetut lainsäädäntömuutokset riittävät?

-

Avoimet huomiot koskien kysymystä 3

-

4. Mahdolliset yksilöidyt säädösmuutosehdotukset

-

5. Mitä hyötyjä arvioitte sovelluksella olevan ja mille tahoille?

-

6. Millaisia riskejä valmisteluun tai sovelluksen käyttöön voi kohdistua?

-

7. Muut huomiot muistiosta ja liitteestä. Voit esittää myös näkemyksiä jäljitysprosessissa tarvittavaan tiedonhallinnan ja tietojärjestelmien kehitykseen.

Kiitämme mahdollisuudesta ja kunnioittaen haluamme lausua seuraavaa.

Meneillään olevassa Covid-19 kriisin yhteydessä hallitukset, kansanterveysviranomaiset ja yritykset tekevät tärkeää työtä, jonka avulla voidaan löytää tie, jolla yhteiskuntaa jälleenrakennetaan kohti ns uutta normaalia. Kuten kaikilla muillakin nykyaikaisen elämän osa-alueilla, digitaalisia teknologioita käytetään todennäköisesti seurantaan, jäljittämiseen ja testaukseen. Tämä vaatii erityistä huolellisuutta, sillä arkaluonteisia tietoja sijainnistamme ja terveydentilastamme voi olla mukana.

Näiden teknisten ratkaisujen kehittämisen ja toteuttamisen kannalta tietosuojan varmistaminen on ratkaisevan tärkeää. Tässä on seitsemän tietosuojan periaatetta, joita haluamme korostaa.

1. Suostumus. Tietoja tulee kerätä vain suostumuksella ja niitä tulee käyttää tavalla, joka kerrotaan selkeästi niin, että osallistuvat henkilöt voivat tehdä informoidun päätöksen. Selkeän ja käyttäjäystävällisen tiedon avulla edistetään vapaaehtoista osallistumista ja voidaan varmistaa, että kaikki teknologian kanssa vuorovaikutuksessa olevat tekevät informoituja valintoja osallistuakseen tietojen keräämiseen ja ovat tietoisia tietojen keräämisen tarkoituksesta, kerättävien tietojen tasosta, tietojen säilytysajasta ja tietojen keruun eduista.

2. Käyttötarkoitus. Kerätään tietoja vain Covid-19:ään liittyvää kansanterveydellistä tarvetta varten. Yksilö omistaa yksilöltä kerätyt tiedot. Yleisesti ottaen kansanterveysviranomaisten olisi käytettävä näitä tietoja ainoastaan tarkoitettuun kansanterveydelliseen tarkoitukseen, ei muihin asiaan liittymättömiin syihin.

3. Minimointi. Kerätään mahdollisimman vähän tietoa. Kansanterveysviranomaisten tähän tarkoitukseen (kuten jäljittäminen) keräämät tiedot, tulisi rajoittaa ainoastaan tarvittaviin erityistietoihin, ja niitä olisi kerättävä ja käytettävä ainoastaan niin kauan kuin kansanterveysalan asiantuntijat ovat ne määrittäneet tarpeellisiksi.

4. Tietojen sijainti. Annetaan yksilöille vaihtoehtoja siitä, missä heidän tietojaan säilytetään. Tietojen on oltava täysin yksilön hallinnassa, mukaan lukien se, että henkilö voi valita, mihin tiedot tallennetaan (esimerkiksi käyttäjän omaan laitteeseen tai pilvipalveluun).

5. Tietojen suojaaminen. Huolehditaan asianmukaisista suojaustoimista tietojen suojaamiseksi. Käytössä olisi oltava luotettavat tietoturvakontrollit, kuten anonymisointi, salaus, hajautetut

identiteetit tai vastaavat toimenpiteet, joilla suojellaan käyttäjien tietoja paljastumiselta ja hakkerointiyrityksiltä.

6. Tietojen jakaminen. Tietoja ei jaeta ilman suostumusta ja jaetut tiedot minimoidaan. Henkilön tietoja tai terveydentilaa ei saa jakaa henkilön kontaktien tai muiden kanssa varmistamatta ensin henkilön suostumusta. Jos tällainen jakaminen on lakisääteisten vaatimusten mukaista, jakaminen olisi rajoitettava tiukasti lain soveltamisalalle ja vain siinä määrin kuin se on ehdottoman välttämätöntä.

7. Tietojen poistaminen. Velvoitetaan poistamaan tiedot heti, kun ne eivät enää ole tarpeen (käyttötarkoitus).palvelimelleenipalveluun. Covid-19 jäljittämistä varten kansanterveysviranomaisille ja muille siirretyt kopioit tiedoista olisi poistettava, jos niistä ei enää ole hyötyä kansanterveydellisissä tarkoituksissa. Viranomaisten tai muiden ei tulisi säilyttää mitään henkilöidenn tietoja tuleviin, toisiinsa liittymättömiin tarkoituksiin.

Tänä päivänä on olemassa enemmän työkaluja ja menetelmiä kuin koskaan – kuten esimerkiksi Differential Privacy, Federated Learning (koneoppimisen hajautettu malli), hajautettu identiteetinhallinta, tietosuojan varmistavat jäljitysprotokollat ja avoimen lähdekoodin repositoryt sekä muita teknologioita tietosuojan varmistamiseen ja hallinnointiin.

Kun otetaan huomioon kasvava kiinnostus mahdollisuudesta hyödyntää teknologiaa pandemian lieventämisessä, toteamme, että COVID-19 tilanteeseen liittyvät ongelmat ja mahdollisuudet ovat monimutkaisia. Teknisiä edistysaskeleita, kuten matkapuhelinten käyttöä erilaisten tietojen keräämiseen, on tarkasteltava laajemmassa yhteydessä, kuten se, miten mielekkäästi ihmiset jakavat tietoja, testausresurssien saatavuus, menetelmien tehokkuus sekä niin kotimaisten kuin kansainvälisten sääntöjen kehittyminen. HuolenaiheinatTeknologiaan ovat myös muun muassa moniin tekijöihin perustuva järjestelmällisen syrjinnän mahdollisuus. Esimerkiksi eri väestöryhmät voivat kohdata erilaisia haasteita yrittäessään osallistua terveyskeskeisiin ohjelmiin ja hankkeisiin, jotka perustuvat teknologian saavutettavuuteen ja osaamiseen iän, koulutuksen ja tulotason mukaan.

5.5.2020

Susanna Mäkelä, yhteiskuntasuhdejohtaja

Mikko Viitaila, teknologiajohtaja

Microsoft Oy

Viitaila Mikko
Microsoft Oy