Helsingin kaupunki, sosiaali- ja terveystoimiala

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?

kyllä pääosin

Avoimet huomiot koskien kysymystä 1

Tietosuoja-asiat pitää ratkaista ja tarkoituksenmukainen tausta-järjestelmä toteuttaa tai muokata olemassa olevista.

Kaiken kaikkiaan suunniteltu sovellus vaikuttaa lupaavalta lisältä epidemian hallinnassa ja esitetyn suunnitelman pohjalta voidaan edetä. Mobiilisovellus tai älytekniikka itsessään ei pandemiaa kuitenkaan ratkaise vaan ratkaisua tulee hakea testaamisesta, vasta-aineista ja rokotteesta. Tartunnanjäljityksen kokonaisuutta ei mitenkään voi jättää tämän varaan. Kuten esityksessä todetaan, tartunnan varmentaminen tapahtuu aina terveydenhuollon ammattihenkilön toimesta.

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

kyllä pääosin

Avoimet huomiot koskien kysymystä 2

Tietojen säilyttäminen vahvasti salattuna pitää todentaa eri ekosysteemejä vasten ja varmistaa käyttöjärjestelmän tuki vahvalle salaukselle. Tietojen hävittäminen pitää varmistaa aukottomasti myös siinä tapauksessa, että käyttäjän laite rikkoutuu, poistetaan käytöstä, varastetaan tai laite vaihtaa omistajaa.

Tietosuojan kannalta on perusteltua, että tiedot ovat hajautettuina käyttäjien päätelaitteissa ja että tiedot siirtyvät keskitettyyn taustajärjestelmään vasta kun tartunta on varmistettu. On perusteltua tietosuoja-asetuksen sekä komission huhtikuussa 2020 antamien suosituksien kannalta, että käsittelyperuste on laissa, mutta sovelluksen käyttö perustuu vapaaehtoisuuteen/suostumukseen.

Epäselväksi jää, miten henkilötietojen käsittely jatkuu, jos rekisteröity peruu suostumuksen.

Rekisteröityjen informointi on järjestettävä kokonaisuudessaan riittävällä tarkkuudella ja ymmärrettävästi.

Tietosuoja on aina riski. Tietojen salauksen toimivuus eri alustoilla on aina kysymysmerkki. Lisäksi toistaiseksi tuntemattomien haavoittuvuuksien hyödyntäminen tietovarkauksissa voi altistaa käyttäjät vakaville tietosuojaongelmille, jos lähikontaktit voidaan jollakin tavoin yhdistää henkilöihin.

Rekisteröidyn oikeuksien toteutumiseen ei ole otettu esityksessä kantaa. (Esimerkiksi sovelluksen käyttäjän oikeus päästä omiin tietoihinsa.)

Vaikutustenarviointi lainsäädäntövaiheessa on esityksessä mainitusti tarpeellinen ja se olisi hyvä saattaa tietosuojavaltuutetun ennakkokuulemismenettelyyn. Esityksen perusteella on epäselvää, onko tietosuoja-asetuksessa tarkoitettu laillinen käsittelyperuste 9 artiklan 2 kohdan a alakohta (suostumus) vai i alakohta (käsittely on kansallisen lain perusteella tarpeen kansanterveyteen liittyvän yleisen edun vuoksi). On selvää, että sovelluksen käyttäminen on vapaaehtoista, mutta jos peruste on suostumus, on epäselvää, miten suostumuksen peruminen, oikeus tulla unohdetuksi yms. on tarkoitus toteuttaa. Tarkoituksenmukaisinta olisi varmasti, että käsittelyperuste olisi 9 artiklan 2 kohdan a alakohta ja tietojen luovuttaminen perustuisi henkilön antamaan suostumukseen, mutta se olisi käsittelyn kansallisessa laissa säädetty lisäedellytys, ei asetuksen mukainen käsittelyperuste. I alakohtaan perustuvan käsittelyn osalta kansallisessa laissa on säädettävä asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn oikeuksien ja vapauksien, erityisesti salassapitovelvollisuuden, suojaamiseksi. Esityksestä ei käy ilmi, miten tämä aiotaan toteuttaa. Esityksen perusteella vaikuttaisi siltä, että suuri merkitys on sillä, miten henkilön suostumus pyydetään ja mitä se kattaa, tämä pitäisi kirjata riittävällä tarkkuudella lakiin.

Hajautettu malli on ehdottomasti tietosuojan toteutumisen kannalta keskitettyä mallia parempi vaihtoehto. Tietojen säilyminen ainoastaan puhelimissa ja poistuminen määritellyn ajan jälkeen, jos altistumista ei tapahdu, turvaa tietojen minimointivaatimusta hyvin. Liitteen 2 mukaan ” Riippuen valitusta

toteutustavasta taustajärjestelmä voidaan toteuttaa ilman tietoa henkilön yksilöivästä tunnisteesta tai niin, että taustajärjestelmään jää jokin yksilöivä tieto henkilöstä, kuten puhelinnumero. Vain taustajärjestelmä voi yhdistää pseudonymisoidun tunnisteen ja yksilön todellisen henkilöllisyyden.”

Tämä kohta on ristiriidassa esityksessä kuvatun kanssa, sillä jos pseudonyymin purkaminen tapahtuu henkilön itsensä toimesta terveydenhuollosta saadulla avauskoodilla ei ole tietosuojanäkökulmasta perusteltua kerätä pseudonyymin lisäksi henkilön puhelinnumeroa.

3. Onko muistiossa tunnistetut lainsäädäntömuutokset riittävät?

kyllä pääosin

Avoimet huomiot koskien kysymystä 3

Lain valmistelussa tulisi määritellä, mikä on uuden rekisterin suhde tartuntatautilain mukaisiin rekistereihin, mukaan lukien kuntien ylläpitämiin 39 §:n mukaisiin tapauskohtaisiin rekistereihin, esim. kattaako henkilön suostumus tietojen luovuttamiseen tietojen siirron näihin rekistereihin. Eri toimijoiden tiedonsaantioikeudet kunnat mukaan lukien tulee määritellä selkeästi laissa siten, että ne täyttävät tiedonhallintalain asettamat vaatimukset rajapintojen rakentamiselle. Lisäksi tulisi määritellä selkeästi onko kuntien mahdollista tehdä tietojohtamista applikaation tiedoilla, vai onko tämä mahdollista vain THL:lle.

4. Mahdolliset yksilöidyt säädösmuutosehdotukset

Ei kommentteja.

5. Mitä hyötyjä arvioitte sovelluksella olevan ja mille tahoille?

Laajasti käyttöönotettuna ja käytettynä sovellus olisi yhteiskunnan kokonaisedun mukainen. Se hyödyttäisi todennäköisesti myös yksittäisiä kansalaisia tautiin varautumisen ja asianmukaisen ohjeistuksen saamisen näkökulmista.

Sovelluksen saaminen väestön käyttöön riittävän kattavasti (3,3 miljoonaa applikaation lataamista, 60% väestöstä) on haasteellista. Australiassa arvioidaan tarvittavan 40 % kattavuutta; Norjassa jopa 70%. Islannissa on päästy 17.4. mennessä 37% kattavuuteen. Väestön valmius käyttöön ottoon vaihtelee huomattavasti eri maiden välillä.

6. Millaisia riskejä valmisteluun tai sovelluksen käyttöön voi kohdistua?

Covid-19-infektoituneen lähikontaktin oikea määrittäminen ja tämän tekninen toteutus on kriittistä. Bluetoothin tarkkuus ei ehkä riitä lähikontaktien määrittelyyn ja Bluetooth voi myös olla asetuksiltaan sellainen, että se sammuttaa itsensä, jos laiteliitosta ei olla tekemässä määritellyn ajan puitteissa. Sovelluksen pitäisi osata hallita siis tätä Bluetoothin asetusta. Tekstissä viitataan lisäksi johonkin Bluetoothiin liittyvään riskiin Applen laitteilla, mutta tätä ei avata tarkemmin.

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

Jäljityssovelluksesta kannattaisi saman tien rakentaa sellainen, että sen pohjalta voisi toteuttaa kansallisen terveystiedon arkiston ”Kanta” kanssa yhteensopivan tiedonkeruusovelluksen, jonka kautta kansalainen voi itse ja oma-aloitteisesti tallentaa ja päivittää terveys- ja (liikkumis)tietojaan Kantaan ja myös hallinnoida omien tietojensa näkyvyyttä ja käytettävyyttä terveydenhuollon ammattilaisille, kuten terveyskeskus- tai työterveyslääkäreille ja –hoitajille. Sovelluksessa tulisi olla tätä varten rajapinnat Applen, Googlen, Polarin ja muiden vastaavien valmistajien terveys- tai liikkumissovelluksiin.

Bluetooth-teknologia ei ole mitenkään riskitön, mutta toiminee tässä parhaiten. Tästä seuraa, että kaikkien käyttäjien matkapuhelimiin kertyy valtavasti tietoa käyttäjien lähikontakteista. Tietosuojamielessä tämä on todella merkittävä riski ja esimerkiksi sopivan haittaohjelman kautta varastettuna tieto olisi väärinkäyttämiselle erittäin altista.

Tiedon hajautettu tallentaminen parantaa tietosuojaa ja tiedon luotettavuutta, koska sen väärentäminen on huomatavan vaikeaa. Jäljityssovelluksessa on kuitenkin pakko olla joku tunniste, jolla lähikontaktit rekisteröityvät. Sovelluksen tunnistetta ei saa mitenkään voida yhdistää myöskään käyttäjän laitteeseen. Tekstissä huomioidaan vain henkilöiden tunnistaminen. Laitteen tunnistaminen paljastaa myös käyttäjän.

Nyt suunnitellussa ratkaisussa tieto ei siirtyisi automaattisesti terveydenhuollon tietojärjestelmiin. Taustajärjestelmän olisi hyvä olla joku nykyisin laajasti käytössä oleva terveydenhuollon sovellus, joka jo valmiiksi toimii samanlaisessa käytössä. Esimerkiksi SAI, joka tukee mm. Helsinkiä Covid-19 –tartuntaketjujen selvittämisessä. Taustajärjestelmä voi toki olla joku muukin, mutta silloin tarvitaan rajapintoja ja manuaalista työtä, mikä ei ole tässä tilanteessa toivottava vaihtoehto.

Järjestelmän toiminnan pitää käyttäjän suostumuksen ohella perustua myös siihen, että käyttäjät tosiasiallisesti käyttävät järjestelmää tarkoitetulla tavalla. Käyttäjien sitouttaminen on varmasti jonkinlainen haaste, mutta se on kaikkein oleellisin asia koko idean toimivuuden kannalta.

Viranomaisten tuottaman järjestelmän luotettavuus esim. suurien laitevalmistajien omiin sovelluksiin tai muiden toimijoiden sovelluksiin verrattuna ei ole mikään itsestään selvyys. Kaupalliset ratkaisut joka tapauksessa kilpailevat viranomaisten ratkaisujen kanssa. Koko kappale 3 on kirjoitettu aika optimistiseen sävyyn viranomaisen toiminnan ja suosion kannalta.

Järjestelmän teknisen kehittämisen aikataulu 6-8 viikkoa kuulostaa todella optimistiselta ja oikeasti tässä aikataulussa toteutunee määrittely ja yksi kehityssprintti, joita varmaan tarvitaan jatkossa useita. Lopputuloksena tällä aikataululla lienee toimiva demo. Käyttöönottoaikataulu kesäkuussa 2020 on erittäin optimistinen, jos halutaan tässä asiakirjassa kuvattu tietosuojan ja luotettavuuden taso sekä liittymät taustajärjestelmiin ja kaikki testattuna ja sertifioituna. Käyttöönottoa nopeuttaa, mikäli lainsäädäntöhanketta ja sovelluskehitystä tehdään samanaikaisesti.

Miksi taustajärjestelmän pitäisi olla uusi? Miksi ei tukeuduta olemassa oleviin samaa tarkoitusta (tartuntatautien jäljitys) tekeviin järjestelmiin (kuten SAI) tai olemassa olevan arkkitehtuurin päälle toteutettavaan laajennukseen (kuten Kanta)?

Muutoksessa on huomioitava erityisryhmien (esimerkiksi vammaisten, kehitysvammaisten, lasten) mahdollisuudet sovelluksen käyttöön muilla tavoin kuin mobiililaitteilla, jotta sovelluksen käyttäminen voisi toteutua mahdollisimman yhdenvertaisesti.

Esityksessä on käytetty pseudonymisointi-termiä tulkinnanvaraisesti esimerkiksi sivun 4 viimeisessä virkkeessä. Pseudonymisoitu tieto on henkilötietoa.

Toimeenpanon kustannusarvio jää sikäli vajaaksi, että ylläpidon kustannuksista ja maksajasta ei ole esitetty edes alustavaa arviota.

Pellinen Jukka
Helsingin kaupunki, sosiaali- ja terveystoimiala - Juha Jolkkonen, toimialajohtaja