Sisäministeriö
Inrikesministeriet

Lausunto
05.05.2020

SM2013996
00.02.04
SMDno-2020-1086

Sosiaali- ja terveysministeriö

Lausuntopyyntö VN/10058/2020

Sisäministeriön lausunto esityksestä kontaktien jäljityssovelluksen käyttöönotosta Covid-19-epidemian hallinnan tueksi

Sosiaali- ja terveysministeriö on pyytänyt sisäministeriöltä lausuntoa lähikontaktien jäljityssovelluksen käyttöönotosta Covid-19-epidemian hallinnan tueksi. Pyydettynä lausuntonaan sisäministeriö toteaa seuraavaa.

Tausta

Sosiaali- ja terveysministeriö on valmistellut etenemisesityksen lähikontaktien jäljityssovelluksen käyttöönottoon Covid-19-epidemian hallinnan tueksi. EU-komission suositus 8.4.2020 mobiiliteknologian käytöstä Covid-19-kriisissä toteaa, että jäljityssovelluksilla on oletettavasti saavutettavissa hyötyjä kriisin hallinnassa. Koska useat Euroopan maat ovat kehittäneet jäljitysratkaisuja, Suomenkin lähestymistavan kehittämisessä on tukeuduttu alustaviin kokemuksiin näiden sovellusten avulla saavutettavista hyödyistä sekä niihin liittyvistä haasteista.

Ensisijainen hyödynsaaja on tartunnalle altistunut henkilö, joka saa sovelluksen kautta varoituksen mahdollisesta altistumisestaan. Hän voi jakaa tämän tiedon terveydenhuollolle ja toimia saamiaan ohjeita noudattaen ennen kuin terveydenhuoltohenkilöstö ottaa häneen yhteyttä muita tarvittavia toimenpiteitä varten. Keskeiset haasteet liittyvät tietosuoja- ja tietoturvaperiaatteiden toteuttamiseen.

Tavoitteena on tukea tartuntatautien jäljitystyötä terveydenhuollossa ja tartuntaketjujen katkaisemista mobiiliteknologiaan perustuvaa, lähikontakteja rekisteröivää sovellusta hyödyntämällä. Sovellus on vapaaehtoinen, ja tiedon käyttö perustuu henkilön suostumukseen. Testausten määrän merkittävästä kasvattamisesta saadaan enemmän hyötyjä tehokkaammalla altistuneiden henkilöiden tavoittamisella ja nopeammalla auttamisella. Jäljityssovelluksen keräämien lähikontaktitietojen pohjalta voidaan lyhentää aikaa altistuneiden oirearvioon ja testaukseen.

Kirkkokatu 12, Helsinki
PL 26, 00023 Valtioneuvosto
Vaihde 0295 480 171 | kirjaamo@intermin.fi | www.intermin.fi

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

- **kyllä X**
- kyllä pääosin
- ei pääosin
- ei
- ei kantaa

Avoimet huomiot koskien kysymystä 1:

Sisäministeriö toteaa, että mobiilisovellus on tarkoituksenmukainen ja kustannustehokas tapa jäljittää tartuntaketjuja, joka säästää myös tarvittavan henkilökunnan määrää. Huomiona todetaan, että mobiililaitteiden yleisyys ja esityksessä kuvatulla sovelluksella saatavan tiedon nopea välittäminen tukevat testausstrategiaa. Siten sovelluksen avulla saatavat tiedot todennäköisesti tehostavat toimia Covid19-epidemian hallinnassa. Edellytyksinä ovat sovelluksen helppo saatavuus, käytettävyys ja laaja käyttö. Huomiona todetaan kuitenkin lisäksi, että kaikilla matkapuhelinverkkoa käyttävillä ei ole älypuhelimia.

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

- kyllä
- **kyllä pääosin X**
- ei pääosin
- ei
- ei kantaa

Avoimet huomiot koskien kysymystä 2:

Etenemisehdotuksessa todetaan, että henkilötietojen käsittely perustuisi lakiin, mutta koska jäljityssovelluksen käyttö olisi vapaaehtoista, olisi henkilöllä oikeus olla suostumatta tällaiseen tietojen käsittelyyn.

Jatkovalmistelussa tulee määriteltäväksi henkilötietojen käsittelyn tietosuojasäädösten mukaiset perusteet. Viranomaistoiminnassa suostumuksen käyttämistä käsittelyn perusteena ei yleensä ole pidetty mahdollisena tai ainakaan suositeltavana. Lähtökohtana on ollut, ettei viranomainen toiminnassaan käsittele henkilötietoja suostumuksen perusteella. Ehdotuksessa henkilön suostumus on kuitenkin keskeisessä ja suorastaan ratkaisevassa asemassa, kun ehdotuksessa korostetaan vapaaehtoisuutta eri vaiheissa. Ehdotuksen perusteella käsittelyperusteita vaikuttaisi olevan eri vaiheissa useampia. Suostumuksen käytön yhdistäminen viranomaisia koskevaan lainsäädäntöön ja esimerkiksi rekisterinpitäjän ja käsiteltävien tietoryhmien sääntelyyn vaatii tarkkuutta ja uudenlaista lähestymistapaa.

Jos jatkovalmistelussa kuitenkin edelleen nojataan suostumus-termiin, sisäministeriö esittää, että suostumusta koskevissa kirjauksissa voitaisiin käyttää muotoilua ”*tosiasiallinen suostumus*” sekä avata sille oikeuskäytännössä ja -kirjallisuudessa vakiintunut sisältö.

Kun suostumuksen antajasta tulee rekisteröity, kysymys on terveystiedoista ja koska rekisterinpitäjänä on viranomainen, on jatkovalmistelussa syytä kiinnittää erityistä huomiota siihen, minkä sisältöisenä ja millä tavoin suostumuksen antajaa informoidaan hänen tietojensa käsittelystä. Henkilötietojen käsittelyyn suostumuksen perusteella liittyy myös oikeus annetun suostumuksen peruuttamiseen.

Henkilötietojen suojan ja sovellusta kohtaan tunnettavan luottamuksen kannalta on tärkeää, että jäljityssovelluksen taustajärjestelmää, sen toiminnallisuuksia ja hallinnointia käsitellään jatkovalmistelussa avoimesti ja ymmärrettävästi. Etenemisehdotuksessa jäljityssovelluksen taustajärjestelmässä tapahtuvasta henkilötietojen käsittelystä onkin vasta alustavia suunnitelmia. Taustajärjestelmälle on varmasti mahdollista saada myös sen keskeistä merkitystä tarkemmin kuvaava nimitys.

Esityksessä esitetyt linjaukset ja periaatteet (hajautettu malli, käyttö perustuu vapaaehtoisuuteen, useampi suostumus eri vaiheissa, ei sisällä paikkatietoa jne.) ovat oikeita ja ottavat huomioon henkilötietojen ja yksityisyyden suojaan liittyviä näkökohtia. Jäljityssovelluksen suunnittelun tekniset yksityiskohdat ja toteutuksen oikeellisuus ja virheettömyys ovat kuitenkin erittäin tärkeitä, koska viimekädessä nämä ratkaisevat onko lopputulos käyttäjien henkilötietojen, yksityisyyden suojan ja tietoturvan näkökulmasta turvallinen. Pienikin virhe salaus-, pseudonymisointi-, satunnaisuus tai muissa vastaavissa teknisissä suunnittelun tai toteutuksen yksityiskohdissa voi tehdä ratkaisusta turvattoman ja johtaa laajaan käyttäjien yksityisyyden loukkaamisen. Ilman tarkempia teknisiä tietoja ratkaisun turvallisuutta ei pysty arvioimaan.

Sisäministeriö toteaa, että ehdotettu Kyberturvallisuuskeskuksen arviointi toteutukselle on erittäin hyvä.

3. Onko muistiossa tunnistetut lainsäädäntömuutokset riittävät?

- kyllä
- kyllä pääosin
- ei pääosin
- ei
- **ei kantaa X**

Avoimet huomiot koskien kysymystä 3:

Esityksessä on tunnistettu riittävät lainsäädäntömuutokset tämän hetkisten tietojen pohjalta. Muistion mukaan jäljityssovellus ja sen taustajärjestelmä toteutetaan perusoikeuksista, tietosuojasta ja tietoturvasta huolehtien ja sovelluksen käyttötarkoituksesta, siihen liittyvästä toimivallasta ja henkilötietojen käsittelystä säädetään lainsäädännöllä. Etenemisehdotus kuvaa vasta sovelluksen lähtökohtia, toimintamallia ja reunaehtoja. Lainsäädäntömuutosten riittävyyteen koko toteutuksen osalta ei näin ollen ole tässä vaiheessa mahdollista ottaa kantaa.

Avoimina huomioina todetaan, että sovelluksen käyttötarkoitus huomioiden on perusteltua korostaa sen käytön perustumista lakiin. Mahdollisen lainsäädännön on yksilöitävä käyttötarkoitus, kerättävien tietojen käyttötarkoitussi-

donnaisuus, rekisterinpitäjä sekä tietojen säilyttämisen kesto, tuhoaminen ja kansainvälinen käyttö yksiselitteisesti.

Lisäksi todetaan, että jossain määrin vaikeaselkoisena ja hieman ristiriitaisena voidaan pitää etenemisehdotuksessa (s. 8) lainsäädäntömuutoksia koskevaa ajatusta, että ”henkilötietojen käsittely perustuisi lakiin, mutta koska jäljitys-sovelluksen käyttö olisi vapaaehtoista, olisi henkilöllä oikeus olla suostumatta tällaiseen tietojenkäsittelyyn.”

4. Mahdolliset yksilöidyt säädösmuutosehdotukset

Ei esityksiä

5. Mitä hyötyjä arvioitte sovelluksella olevan ja mille tahoille?

Sovelluksen avulla on mahdollista seurata epidemian määrällistä kehitystä ja tehtyjen rajoitustoimien vaikutusta ihmisten toimintaan.

6. Millaisia riskejä valmisteluun tai sovelluksen käyttöön voi kohdistua?

Huomiota tulisi kiinnittää myös käytettyyn terminologiaan, jota kannattaisi mahdollisimman varhaisessa vaiheessa valmistelua avata ja selkeyttää. Tällaisia ovat esimerkiksi ehdotuksessa käytetyt ilmaisut ”pseudonomisoitu tunniste” ja ”tiedon käsittely aggregoidussa muodossa”. Lisäksi jatkovalmistelussa voitaisiin arvioida myös tarvetta ja mahdollisuuksia tietojen anonymisointiin.

Etenemisehdotuksessa hahmotellaan muita jäljityssovelluksen avulla toteutettavissa olevia toiminnallisuuksia, kuten luotettavan terveysinformaation ja ohjeiden jakaminen. Sovelluksen toiminnallisuudet on kuitenkin jo säädösvaiheessa esitettävä riittävän selkeästi ja tarkkarajaisesti. Tällä voidaan arvioida olevan merkitystä myös siihen, kuinka aktiivisesti ihmiset ottavat sovelluksen käyttöön. Kysymyksessä on ensisijaisesti lähikontakteja rekisteröivä mobiilisovellus eikä epäselvyyttä voi jäädä siitä, mitä muita toiminnallisuuksia sovelluksella mahdollisesti toteutetaan.

Lisäksi todetaan, että esityksen sivulla 8 mainittu teknisen toteuttamisen aikataulu on varsin kireä. Aikataulussa pysyminen edellyttänee teknisen toteuttamisen onnistumista ilman ennakoimattomia viivästyksiä, mikä on epätodennäköistä tietoteknisessä hankkeessa. Ehdotetun sovelluksen on esitetyssä käyttötarkoituksessa täytettävä tietoturvataso, auditointi ja ennen tuotantokäyttöä suoritettava testaus.

Kuten muissakin tietojärjestelmissä ja niihin liittyvissä sovelluksissa, myös tässä tapauksessa on huomioitava tietojärjestelmän omistajan ja rekisterinpitäjän kyky vastata lainsäädännön velvoitteisiin. Käytännössä tämä tarkoittaa voimavaroja tietojärjestelmän ja sovelluksen suorituskyvyn riittävyyden varmistamiseen, kerättyjen tietojen käsittelyyn (tallentaminen, varmuuskopiointi, käsittely) sekä ylläpitävää kehittämistä. Edellä mainitut liittyvät suoraan rahoitukseen, joka tarvitaan hankkeen toteuttamiseen. Rahoituksen tulee olla jatkuvaa, koska Covid-19-epidemian jatkumisen pituus ei ole tiedossa.

Sovelluksen tuottama tietojoukko, vaikkakin salattuna, pseudonymisoituna ja aggregoituna, tulee todennäköisesti muodostamaan kohteen tietomurroille ja sitä kautta saatavan tiedon hyväksikäytölle. Toinen näkökulma on itse sovellukseen kohdistuvat hyökkäykset.

Jäljityssovelluksen perustuminen avoimeen lähdekoodiin mahdollistaa toteutuksen yksityiskohtien oikeellisuuden varmistamisen. Tämä on tärkeää, mikäli toteutuksessa päädytään käyttämään valmiita komponentteja tai kirjastoja, jotka on toteutettu muualla kuin Suomessa.

Yhtenä toteutusvaihtoehtona on hyödyntää jäljityssovelluksessa Applen ja Googlen kehittämää alustapalvelua (”Privacy-Preserving Contact Tracing”), joka on tulossa iOS ja Android käyttöjärjestelmiin. On todennäköistä, että jäljitysratkaisusta tulee toimivampi (käyttökokemus, virheettömyys, virran kulutus) ja turvallisempi (salaus-, pseudonymisointi-, Bluetooth- yms. ratkaisut) tätä mobiilikäyttöjärjestelmien ominaisuutta hyödyntämällä. Sovelluksen käyttö edellyttää Bluetooth-teknologian aktivointia laitteissa ja laajassa mittakaavassa se todennäköisesti lisää aktiivisten Bluetooth laitteiden määrää, sellaisetkin henkilöt jotka muuten eivät käyttäisi Bluetooth-yhteyksiä nyt sen aktivoivat puhelimessaan. Samaan aikaan on tiedossa, että Bluetooth-teknologiassa ja laitetoteutuksissa on ollut useita haavoittuvuuksia eikä läheskään kaikilla käyttäjillä ole asennettuna laitteisiinsa viimeisiä ongelmat korjaavia päivityksiä. Sovelluksen käyttö lisää laajassa mittakaavassa Bluetooth-teknologian kautta muodostuvaa uhkaa mobiililaitteille. Riskien pienentämiseksi sovelluksen tiedottamisen yhteydessä tulisi esim. muistuttaa laitteiden päivitysten tarpeellisuudesta. Järjestelmän poistuessa käytöstä on tärkeää, ettei käyttäjien laitteisiin jää asennettuja aktiivisia jäljityssovelluksia jotka jatkavat kontaktien kartoitusta. Järjestelmän tulee mahdollistaa sovelluksen toiminnan ja tiedonkeruun lopettaminen tai estäminen, vaikka käyttäjä ei itse aktiivisesti muistaisikaan poistaa sovellusta.

Esityksessä mainittu kerätyn tiedon kansanvälinen käyttö puolestaan edellyttänee erikseen rakennettavia rajapintoja tietojoukkojen luovuttamiseen.

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

Sovelluksen kehittämisessä ja sen aikataulutuksessa on huomioitava valtiota sitova hankkeiden kilpailutukseen liittyvä lainsäädäntö sekä valtion tietojärjestelmien arkkitehtuuri. Edellä mainitut voivat aiheuttaa muutoksia aikataulutukseen ja rajoituksia sovelluksen toiminnallisuuteen.

Sovelluksen kehittämiseen liittyvään budjetointiin liittyvänä huomiona todetaan, että valitun palveluntuottajan ja sovelluksenkehittäjän käyttämä tietojärjestelmien/sovellusten kehittämistapa ja vaatimusmäärittelyn laajuus vaikuttavat oleellisesti aikataulutukseen. Kevyempi vaatimusmäärittely nopeuttaa varsinaisen ohjelmointityön aloittamista. Riskeinä ovat kuitenkin vaatimusmäärittelyn aiheuttamat puutteet tietoturvassa ja toiminnallisuudessa sekä vaatimusmäärittelyn täydentämisestä seuraavat lisäkustannukset ja toteutuksen viivästyminen.

Jäljityssovelluksessa ja taustajärjestelmässä, kuten missä tahansa sovelluksessa tai järjestelmässä, todennäköisesti ilmenee korjattavia virheitä ja mahdollisesti myös tietoturvaan liittyviä päivitystä edellyttäviä ongelmia. Sovelluksen kehitysprosessissa tulee varmistaa, että ongelmien ilmoittamiseen on käytettävissä toimivat kanavat ja yhteystiedot, mahdolliset ongelmat havaitaan viivytyksettä, niihin pystytään tekemään korjaukset nopeasti ja päivitetty versio saadaan jaeltua mahdollisimman tehokkaasti. Eteen tulevat tietoturvaan liit-

tyvät ongelmat ja näistä johtuvat päivitykset kannattaa ottaa suunnittelun lähtökohdaksi eikä olettaa virheetöntä toteutusprosessia. Kannatta myös harkita voisiko sovellus itse huomauttaa käyttäjälle vanhentuneesta versiostaan tai jos se havaitsee/tunnistaa päivittämättömän ja haavoittuvan mobiilikäyttöjärjestelmän version jossa ohjelmaa suoritetaan.

Lisäksi tämän tyyppisten sovellusten osalta olisi hyvä ottaa huomioon sovelluksen uudelleenkäyttömahdollisuus vastaavissa muissa tilanteissa. Käyttöoikeudet, lisenssit ja muut asiaan liittyvät tekniset järjestelyt mm. tietokantojen koko tulisi suunnitella siten, että tämä on mahdollista.

Kansliapäällikkö Kirsi Pimiä

Johtava asiantuntija Hanne Huvila

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Sisäministeriö 05.05.2020 klo 14:07. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Tiedoksi

Sisäministeri Ohisalo
Valtiosihteeri Parviainen
Erityisavustajat Kerman ja Laaksonen
SM/PO
SM/PEO
SM/KTY
SM/HKO