Insta Secrays 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?

ei kantaa

Avoimet huomiot koskien kysymystä 1

Toimiessaan sovellus voi täydentää muuta jäljitystyötä ja potentiaalisesti nopeuttaa altistumisista ilmoittamista sekä auttaa ilmoittamaan altistumisesta sellaisille henkilöille, joita jäljityksellä ei muutoin ole mahdollista tavoittaa. Käytännössä sovelluksen toimivuuteen liittyy kuitenkin runsaasti epävarmuutta. Muistiossa viitatun 60 prosentin käyttöasteen saavuttaminen vaikuttaa tämänhetkisen tiedon ja muista maista peräisin olevien kokemusten valossa epätodennäköiseltä. Valmistelussa tulisikin arvioida, onko sovelluksesta saatavissa hyötyjä myös siinä tapauksessa, että käyttöaste jää (merkittävästikin) alle tavoitteen tai vaihtelee alueellisesti tai ikä- ja käyttäjäryhmittäin. Sovelluksen hyödyntäminen edellyttää lisäksi huomattavan laajaa testaamista, käytännössä myös kaikkien lieväoireisten.

Muistion mukaan ”sovellukseen määritellään terveysviranomaisen arvioon perustuen, mikä on Covid-19-taudin lähikontakti eli kontaktin etäisyys ja kohtaamisen kesto (tämän hetkisen tiedon valossa esim. 2 metriä ja 15 minuuttia)” (s. 5). Muistion kirjaus saattaa antaa epärealistisen kuvan siitä, millä tarkkuudella kontaktien etäisyyksiä pystytään tosiasiassa määrittelemään. Bluetooth LE -teknologiaa ei ole suunniteltu eikä tarkoitettu etäisyyden mittaamiseen, ja parhaimmillaankin kyse on signaalin lähetys- ja vastaanottotehon voimakkuuden perusteella tapahtuvasta päättelystä, jonka tarkkuuteen olosuhteet voivat merkittävällä tavalla vaikuttaa.

Riskinä siis yhtäältä on, että merkittävä määrä todellisia altistumisia jää pimentoon, mutta toisaalta että sovellus tunnistaa huomattavan määrän myös ns. vääriä positiivisia ja aiheuttaa siten

tarpeetonta kuormitusta terveydenhuoltoon. Väärien positiivisten määrä voi myös käyttäjien näkökulmasta heikentää luottamusta sovellukseen ja sitä kautta vähentää sovelluksen käyttöä.

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

ei pääosin

Avoimet huomiot koskien kysymystä 2

Muistiossa on otettu huomioon useita käyttäjien yksityisyyden suojan kannalta keskeisiä seikkoja. Muistiossa on kuitenkin paikoin epäselvyyksiä, jotka hankaloittavat tarkempaa arviointia, ja lukuisat yksityisyyden suojan kannalta olennaiset asiat ovat riippuvaisia jatkovalmistelusta.

Muistiossa viitataan kontaktitietojen tallentamiseen hajautetusti käyttäjien laitteisiin (s. 4). Liitteessä 2 toisaalta viitataan myös vaihtoehtoon, jossa taustajärjestelmään tallennetaan tietoja, joiden perusteella pseudonymisoitu tunniste voidaan yhdistää henkilöllisyyteen, eli ns. keskitettyyn malliin (ja tästä nimenomaan sellaiseen, jossa keskitetysti tallennetaan myös henkilöllisyystieto). Myös muistiossa viitataan yhteystietojen jakamiseen, joskin on epäselvää, mitä tällä käytännössä tarkoitetaan. Ei siten ole yksiselitteisen selvää, mitä mallia muistiossa esitetään. Pidämme välttämättömänä, että eteneminen tapahtuu hajautetun mallin mukaisesti, sillä altistustiedon yhdistäminen käyttäjän henkilöllisyyteen ei ole tarpeen sovelluksen ydintoiminnallisuuksien ja hyötyjen kannalta. Hajautettu malli on sekä tietoturvan että käyttäjien yksityisyyden suojan kannalta merkittävästi parempi ratkaisu, ja yksinkertaistaa tarvittavaa toteutusta.

Toiminnallisiin periaatteisiin tulisi sisällyttää edellytys käyttää mobiilikäyttöjärjestelmien tarjoamia valmiita rajapintoja, käytännössä Applen ja Googlen yhteistyössä kehittämää. Valmiiden rajapintojen hyödyntäminen edesauttaa myös komission suosituksessa mainittua sovellusten yhteentoimivuutta eri jäsenvaltioiden kesken sekä nopeuttaa sovelluksen kehitystyötä, lisää sen luotettavuutta ja turvallisuutta sekä vähentää kehitystyön kustannuksia. Valmistajien antamien ja Julkisuudessa olleiden tietojen perusteella Applen ja Googlen tarjoamassa rajapinnassa on otettu sisäänrakennettuna huomioon lukuisia tietoturvan ja käyttäjien yksityisyyden suojan kannalta merkittäviä suojakeinoja. Rajapintojen käyttämisellä vältetään myös muutoin eteen tulevat ongelmat esimerkiksi käyttöjärjestelmien virransäästöön ja käyttäjien yksityisyyden suojaan liittyvien ominaisuuksien kannalta (näitä ominaisuuksia ja niiden sovelluksille asettamia rajoituksia kuvataan muistiossa ”potentiaaliseksi riskiksi”).

Muistiossa on tunnistettu tarve tehdä tietosuojaa koskeva vaikutustenarviointi. Muistion mukaan vaikutustenarviointi ”voidaan tehdä lakiehdotuksen yhteydessä rekisterinpitäjän tekemän vaikutustenarvioinnin sijasta” (s. 8). Tietosuoja-asetuksen 35 artiklan 10 kohta sallii tietyin edellytyksin arvioinnin tekemisen oikeusperusteen hyväksymisen yhteydessä. Jo lakiehdotuksen valmistelun ja käsittelyn yhteydessä tulisi nähdäksemme arvioida käsittelyn vaikutuksia erityisesti edellytettävien suojatoimien kannalta, mutta jatkovalmistelussa on syytä pohtia, onko tarkoituksenmukaista tehdä vaikutustenarviointi vain lainsäädäntövaiheessa. Erityisesti on tarpeen kiinnittää huomiota siihen, voidaanko lakia valmisteltaessa ottaa riittävällä tavalla ja riittävällä

tarkkuudella huomioon ne seikat, joita huolellisesti toteutetussa vaikutustenarvioinnissa tulisi tarkastella.

Muistiossa mainittu sovelluksen toteutus avoimen lähdekoodin pohjalta sekä ehdotettu Kyberturvallisuuskeskuksen tekemä sovelluksen tietoturva-auditointi ovat kannatettavia.

Muistiossa esitettyjen toiminnallisten periaatteiden mukaan tieto on pseudonymisoitua ja aggregoitua (s. 5-6). On epäselvää, mihin aggregoidulla tiedolla tässä yhteydessä viitataan. Edellä mainittu muistion kohta koskee yleisesti sovelluksen keräämää tietoa, ja kontaktien jäljityksessä tarpeen on nimenomaisesti yksilötason tieto. Aggregoitu tieto voisi tulla kyseeseen lähinnä tilastointitarkoituksiin, mihin muistiossa viitataan muussa yhteydessä (s. 11).

3. Onko muistiossa tunnistetut lainsäädäntömuutokset riittävät?

ei pääosin

Avoimet huomiot koskien kysymystä 3

Henkilötietojen käsittelyn osalta muutosten riittävyyden arviointia hankaloittaa se, että muistiossa ei esimerkiksi arvioida käsittelyn oikeusperustetta tietosuoja-asetuksen näkökulmasta tai oteta kantaa siihen, ovatko tarvittavat lainsäädäntömuutokset tarkoitettu määräaikaisiksi.

Käsittelyperusteen osalta muistiossa viitataan sekä lakisääteiseen henkilötietojen käsittelyyn että henkilöiden suostumuksen tarpeeseen. Muistion mukaan yhtäältä ”henkilötietojen käsittely siis perustuisi lakiin, mutta koska jäljityssovelluksen käyttö olisi vapaaehtoista, olisi henkilöllä oikeus olla suostumatta tällaiseen tietojenkäsittelyyn” (s. 7-8). Toisaalta, jäljityssovelluksen käyttö ”on henkilölle vapaaehtoista ja perustuu henkilön suostumukseen” (s. 5). Suostumukseen viitataan myös esimerkiksi tietojen välittämisessä terveysviranomaisille (s. 7).

Mitä ilmeisimmin käsittelystä on tarkoitus säätää siten, että tietosuoja-asetuksen näkökulmasta kyse on 6 artiklan 1 kohdan c tai e alakohdissa tarkoitetusta käsittelystä sekä erityisten henkilötietoryhmien osalta 9 artiklan 2 kohdan g tai i alakohdassa tarkoitetusta käsittelystä. Muistion mukaan ”henkilötietojen käsittely siis perustuisi lakiin” (s. 7). Sääntelypohja on jatkovalmistelussa syytä tuoda yksiselitteisesti esiin. Myös tietojen käyttötarkoituksista on syytä säätää tarkkarajaisesti ja yksiselitteisesti laissa, tai vaihtoehtoisesti pyytää käyttäjältä nimenomainen suostumus kuhunkin mahdolliseen eri käyttötarkoitukseen.

Muistion mukaan ”jäljityssovelluksen toteuttaminen viranomaislähtöisenä ja suostumukseen perustuvana toimintana edellyttää tietosuoja-asetuksen mukaisesti lainsäädäntöä, koska viranomaisen ja henkilön välillä on usein selkeä vallan epätasapaino” (s. 7). Muistiossa on sinänsä asianmukaisesti tunnistettu viranomaisen ja yksilön välinen vallan epätasapaino, joka voi olla ongelmallinen tietosuoja-asetuksen 7 artiklan mukaisen suostumuksen edellytysten kannalta. Vallan

epätasapaino ei kuitenkaan automaattisesti tarkoita, etteikö myös rekisterinpitäjänä toimivan viranomaisen käsittely voisi perustua suostumukseen, jos 7 artiklan edellytykset esimerkiksi suostumuksen vapaaehtoisuudesta täyttyvät (vrt. rekisterinpitäjän oikeutettu etu, joka on eksplisiittisesti suljettu pois viranomaisilta 6 artiklassa).

Muistiossa kuvatut toiminnallisuudet edellyttävät tietojen tallentamista käyttäjän päätelaitteelle, mutta muistiossa ei ole arvioitu asiaa sähköisen viestinnän tietosuojadirektiivin 5 artiklan ja sähköisen viestinnän palveluista annetun lain 205 §:n vaatimusten kannalta. Komission tiedonannossa (2020/C 124 I/01) esitetyn näkemyksen mukaan tietojen tallentaminen käyttäjän päätelaitteelle tämänkaltaisten sovellusten yhteydessä edellyttää suostumusta (näin siis myös silloin, kun kyse ei ole henkilötiedoista, tai kun henkilötietojen käsittelyn perusteena ei ole suostumus). Kiinnitämme tässä yhteydessä huomiota myös siihen, että direktiivin mukainen suostumus tarkoittaa nykyisin samaa kuin tietosuoja-asetuksen mukainen suostumus.

Muistiossa käytetään suostumuksen käsitettä useissa yhteyksissä. Niissä tapauksissa, joissa ei yksiselitteisesti ole tarkoitus viitata suostumukseen joko tietosuoja-asetuksen 6 tai 9 artiklan mukaisena oikeusperusteena taikka sähköisen viestinnän palveluista annetun lain mukaisena edellytyksenä tietojen tallentamiselle, olisi selkeintä välttää suostumus-termin käyttöä ja puhua sen sijaan esimerkiksi sovelluksen käyttämisen ja tietojen luovuttamisen vapaaehtoisuudesta.

Muistiossa käsitellään lyhyesti myös tietojen säilytysaikoja koskevia periaatteita. Nähdäksemme myös tietojen säilytysajasta on tarpeen säätää lailla.

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.

-

Valo Janne
Insta Secrays Oy