Kansaneläkelaitos

Lausunto

01.06.2020 Kela 54/010/2020

Asia: VN/10579/2020

Lausuntopyyntö: Luonnos hallituksen esityksestä laiksi tartuntatautilain väliaikaisesta muuttamisesta: koronavirusepidemian tartuntaketjujen jäljittämistä ja katkaisua tehostava altistuneiden tunnistusjärjestelmä

Lausunnonantajan lausunto

Vastaajatahon virallinen nimi

Kansaneläkelaitos

Vastauksen kirjanneen henkilön nimi

Mia Mustonen

Vastauksen vastuuhenkilön yhteystiedot

Marina Lindgren

marina.lindgren@kela.fi

Onko vastaaja

joku muu

Kysymyksiä esityksen tavoitteista ja vaikutuksista

Voidaanko ehdotetulla altistuneiden tunnistusjärjestelmällä mielestänne tehostaa koronavirusepidemian tartuntaketjujen jäljittämistä ja katkaisua?

-

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

-

Onko esityksestä aiheutuvat taloudelliset vaikutukset arvioitu asianmukaisesti?

-

Onko esityksestä aiheutuvat muut vaikutukset arvioitu asianmukaisesti?

-

Mahdolliset yksilöidyt pykälämuutosehdotukset

Ehdotuksenne 43 a §:n muutoksiksi (Terveyden ja hyvinvoinnin laitoksen tehtävät)

-

Ehdotuksenne 43 b §:n muutoksiksi (Kansaneläkelaitoksen tehtävät)

-

Ehdotuksenne 43 c §:n muutoksiksi (Altistuneiden tunnistusjärjestelmän yhteydessä tapahtuva tietojen käsittely)

-

Ehdotuksenne 43 d §:n muutoksiksi (Suhde 22 §:ssä säädettyyn ilmoitusvelvollisuuteen)

-

Ehdotuksenne 43 e §:n muutoksiksi (Altistuneiden tunnistusjärjestelmästä saadun altistumistiedon käsitteleminen)

-

Ehdotuksenne 43 f §:n muutoksiksi (Altistuneiden tunnistusjärjestelmän toteutuksen ohjaus)

-

Ehdotuksenne 43 g §:n muutoksiksi (Altistuneiden tunnistusjärjestelmän tietoturvallisuuden arvioiminen)

-

Ehdotuksenne 43 h §:n muutoksiksi (Valvonta)

-

Voimaantulosäännös: Ovatko esityksen voimaantulo- ja voimassaoloajat perusteltuja esityksen tavoitteiden saavuttamiseksi?

-

Muut huomiot esityksestä

Mahdolliset muut näkemyksenne esityksestä?

Henkilötietojen käsittelystä ja tietosuojanäkökulmia

Esityksessä on monipuolisesti käyty asiaa läpi, mutta esitystä tulee täsmentää mm. pseudotunnisteen osalta. Kelan näkemyksen mukaan järjestelmään tallennettava tunniste ei ole

pseudotunniste vaan satunnaisluku, joka ei sisällä henkilötietoa. Järjestelmässä ei myöskään ole muuta sellaista tietoa, joka yhdistämällä tähän satunnaislukuun voisi johtaa henkilötietojen paljastumiseen.

Säilytysajat

Esityksessä esitetään, että taustajärjestelmään tallennettu pseudotunnus hävitettäisiin 14 vuorokauden kuluttua. Esityksestä ei selkeästi käy esille kenen/mistä pseudotunnuksesta on kyse, pseudotunnuksen säilytysvastuu ja pseudotunnuksen avainparin säilytysaika. Pyydetään tarkentamaan pseudotunnuksen ja avainparin suojaustoimenpiteet ja vastuu säilyttämisestä.

Pyydetään täsmentämään tiedon säilytysaika, tiedon lokituksen periaatteet ja lokin säilytysaika mahdollisia teknisiä virhe- ja häiriöselvitystä, jälkivalvontaa ja rekisteröidyn oikeuksien toteuttamista varten.

Pyydetään tarkentamaan esitystä Kelan ylläpitämän taustajärjestelmään tallentuneen tiedon ja lokitietojen arkistointia riittävällä säilytysajalla. Arkistoidun tiedon käyttötarkoitukseksi tulisi säätää vain tekninen virheselvitys ja poikkeamaselvitystyö, jälkivalvonta sekä rekisteröidyn oikeuksien turvaaminen.

Tietojen tallentaminen väliaikaiseen rekisteriin

Pyydetään täsmentämään terveydenhuollon toimintayksikön perustamaan väliaikaisen rekisterin suojaustoimenpiteet, käyttöoikeusvaltuudet, käytön lokitus ja valvonta. Jos tiedot tulisi poistaa viivytyksettä tulisi huomioida tietoturvallisuusvaatimukset. Rekisterin suojaustoimenpiteisiin tulisi kiinnittää huomio.

Avauskoodi

Esityksessä esitetään, että terveydenhuollosta lähetettäisiin avauskoodi käyttäjän puhelimeen. Tästä nimenomaisesta kokonaisuudesta pyydetään säätämään tietoturvallisuusvaatimuksin.

Lokienhallinta

Lokien ja lokienhallinnan vaatimuksia pyydetään tarkentamaan. Tietoja yhdistämällä muodostuu terveystieto, joka kuuluu erityiseen henkilötietoryhmään, jolloin rekisterinpitäjän tulee soveltaa artikla 9 suojaustoimenpiteitä.

Rekisteröidyn ja ylläpitäjän tiedon käsittelyn lokittaminen on osa varmistua tiedon muuttumattomuudesta ja eheydestä. Kelan taustajärjestelmän häiriö- ja virheselvitystyöstä ja ylläpitotehtävistä tulisi siten tallentaa ylläpitäjän käyttöloki, jolla todennetaan Kelan toimihenkilöiden tietojen käsittely ja varmistetaan heidän oikeusturva. Järjestelmän käytön jälkivalvonnan, tietojen oikeellisuuden ja rekisteröidyn oikeuksien toteuttamiseksi tulisi tästä olla tarkempaa säätelyä (vrt. Kyberturvakeskus ja Vahti-ohje).

Esityksessä ei ole huomioitu taustajärjestelmään tallennettujen tietojen lokienhallinnan toteutusta. Esityksessä pyydetään kiinnittämään huomiota myös siihen, että esityksessä ei ole mainintaa käyttölokeista, luovutuslokeista, niiden tietosisällöistä ja säilytysajasta.

Rekisteröidyn oikeudet

Rekisterinpitäjänä Terveyden ja hyvinvoinnin laitos huolehtii rekisterinpitäjälle yleisessä tietosuoja-asetuksessa asetetuista vaatimuksista, kuten esimerkiksi rekisteröidyn oikeuksien toteuttamisesta ja rekisteröityjen asianmukaisesta informoinnista.

Tietosuoja-asetuksen artikla 15 sovelletaan rekisteröidyn pääsystä omiin tietoihin. Esitystä pyydetään tarkentamaan artikla 15 toteuttamiseksi. THL:n vastuu luovuttaa rekisteröidyn tiedot pyydettäessä tai ohjata tehtävä lakisääteisenä Kelalle. Tietojen luovuttaminen rekisteröidylle tulisi toteutua tietoturvavaatimukset täyttäen teknisesti.

Esitystä pyydetään tarkentamaan rekisteröidyn oikeuden toteuttamiseksi lisäksi seuraavilta osin: oikeutta vaatia poistaa tietonsa järjestelmästä, virheellisen tiedon korjaaminen, oikeutta siirtää tiedot toiseen järjestelmään.

Virhetilanteet ja ylläpitotehtävät

Esitystä pyydetään tarkentamaan Kelan oikeudesta käsitellä järjestelmään tallennettua tietoa tietyissä tapauksissa. Tunnistusjärjestelmän ylläpitäjänä ja henkilötietojen käsittelijänä Kelalla tulisi olla oikeus käsitellä tietoa häiriö- ja virheselvitysten laajuudessa ja ylläpitotehtävien toteuttamiseksi.

Mobiilisovellusten yhteistestaus ja sertifiointi

Riippumatta siitä mihin järjestelmään mobiilisovellus liittyisi ja tallentaisi tietoa, tulee huomioida yleiset sertifiointi-, yhteistestaus- ja tietoturvavaatimukset ja näiltä osin esitykseen pyydetään tarkennuksia. Mobiilisovellusten yhteistestaukset Kelan taustajärjestelmän kanssa on siten huomioitava ja edellytettävä. Vaatimusten tarkoitus on, että sovellus on tietoturvallinen, se toteuttaa tietosuojaa ja mobiilisovellus tai mobiilit taustajärjestelmät eivät välitä tietoja ulkopuolisille.

Miten on huomioitu puhelimessa olevan tiedon turvaaminen ja puhelimen omistajan turvallisuus esim. jos puhelin häviää, varastetaan, joutuu muiden käsiin esim. perheessä tai jos puhelin laitetaan kierrätykseen (sovelluksen käytön päättyminen)?

Poikkeamailmoitukset

Tietosuoja-asetuksen velvoitteiden mukaisesti rekisterinpitäjänä THL:n on vastuu ilmoittaa tietoturvapoikkeamista tietosuojavaltuutetulle. Esityksessä pyydetään nostamaan esille, että sovelluskehittäjällä on velvollisuus ilmoittaa tietoturvaan tai tietosuojaan laitetta koskevasta poikkeamasta Valviralle.

Lisäksi esityksessä olisi hyvä huomioida Valviran ja Tietosuojavaltuutetun oikeudesta saada valvontatehtävän hoitamiseksi järjestelmästä tarvittavat tiedot.

Tietosuojan vaikutustenarviointi

Esityksessä mainitaan, että ”vaikutustenarvioinnin tekee rekisterinpitäjä, jollei vaikutustenarviointia ole yleisen tietosuoja-asetuksen 35 artiklan 10 kohdan mukaisesti jo tehty yleisen vaikutustenarvioinnin osana henkilötietojen käsittelyn oikeusperusteen hyväksymisen yhteydessä”.

Esityksen kohtaan pyydetään selkeyttämistä, koska esityksestä jää epäselväksi tehdäänkö vaikutustenarviointi oikeusperusteen hyväksymisen yhteydessä vai jääkö se rekisterinpitäjän tehtäväksi.

Riski- ja uhka-analyysi

Esityksessä ei tuoda tarpeeksi selvästi esille sitä, että vaikutustenarvioinnissa pitää tehdä huolellinen uhka- ja riskianalyysi, koska tunnistusjärjestelmällä puututaan perustuslaillisiin yksilön vapauksiin. Esimerkiksi tartunnan saanut ja altistunut voidaan määrätä karanteeniin, jossa yksilön vapauksia rajoitetaan. Tällaisissa tilanteissa ei saisi tapahtua väärää arviointia ja/tai tiedon väärinkäytöksiä. Väärästä arviosta tai tiedon väärinkäytöstä rekisteröityä vastaan voi seurata suuria henkisiä vaurioita ja/tai taloudellisia menetyksiä. Tapahtuma voisi muodostua esimerkiksi tilanteessa, jos tartunta- tai altistusmääritys on annettu virheellisesti tai käyttäjän puhelin joutuu vääriin käsiin. On jo nyt tiedossa, että virustestit eivät ole täysin luotettavia. Lisäksi bluetooth-menetelmän käytön riskit ja uhat pitää arvioida huolellisesti. Bluetooth esim. kuluttaa puhelimen akkua ja sen ollessa päällä ulkopuolinen voi mahdollisesti hakkeroida yhteyden ja saada käsiinsä pseudotunnuksen.

Alaikäisen asema

Alaikäisen asema, oikeudet ja yksityisyyden suoja, etenkin 15-vuotta täyttäneiden osalta, jää epäselväksi esityksessä.

Pyydetään huomioimaan käytännön esimerkkejä alaikäisen oikeuksien toteuttamiseksi. Esimerkiksi, jos alaikäinen saa altistusmerkinnän puhelimeensa ja alaikäinen ei halua ryhtyä asian suhteen toimenpiteisiin perustuen esitettyyn vapaaehtoisuuteen, mitä seuraamuksia tapahtumakulusta voisi olla, kun vanhempi käyttää huoltajan oikeutta toimenpiteisiin ryhtyäkseen vasten alaikäisen tahtoa (esim. pakottaa virustestiin)?

Mustonen Mia
Kansaneläkelaitos