Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

Lausunto

17.01.2020

Dnro

TRAFICOM/526056/03.03.00/2019

Asia: VN/12603/2019

Lausuntopyyntö luonnoksesta hallituksen esitykseksi eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä eräiksi siihen liittyviksi laeiksi

1. Asiakas- ja potilastietojen käsittely ja luovuttaminen

Onko asiakas- ja potilastietojen käsittelystä ja luovuttamisesta säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

-

2. Tahdonilmaukset

Tiedonhallintapalvelua koskevaan 11 §:ään on lisätty uusi kohta liittyen muihin asiakkaan sosiaali- ja terveydenhuoltoon kytkeytyviin palveluihin ja asiakastietojen käsittelyyn liittyvistä tahdonilmauksista. Tiedonhallintapalveluun voisi tallentaa esimerkiksi henkilön vastustuksen hänen tietojensa käytöstä biopankkitoiminnassa. Onko tahdonilmauksista käsittelystä ja luovuttamisesta säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

-

3. Erityissuojattavat asiakirjat

Lain 9 §:stä poistettaisiin sosiaali- ja terveysministeriön asetuksenantovaltuus siitä, mitkä asiakasasiakirjat on luokiteltava erityistä suojausta edellyttäviksi. Lain mukaan Terveyden ja hyvinvoinnin laitos antaisi määräykset valtakunnallisten tietojärjestelmäpalvelujen toteutuksen edellyttämistä tietojärjestelmien olennaisista vaatimuksista ja määrittää asiakasasiakirjojen tietosisällöt ja tietorakenteet sekä tietorakenteissa valtakunnallisesti hyödynnettävät koodistot. Pitäisikö erityissuojattavista asiakirjoista säätää asiakastietolaissa ja potilasasiakirja-asetuksessa? Onko erityissuojattavista asiakirjoista säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

-

4. Omatietovaranto

Lain 12 §:ssä säädettäisiin, että henkilö voi antaa suostumuksensa siihen, että palvelunantajalle voidaan luovuttaa omatietovarannossa olevia hyvinvointitietoja sosiaali- ja terveyspalvelujen toteuttamiseksi. Onko hyvinvointitietojen luovuttamisesta säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

-

5. Omatietovaranto

Lain 19 ja 21 §:ssä säädettäisiin, että henkilöllä on oikeus saada omat asiakas- ja potilastietonsa omatietovarantoon ja edelleen hyvinvointisovelluksiin hyödynnettäviksi. Onko asiakas- ja potilastietojen luovuttamisesta omatietovarantoon säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa? Pitäisikö omatietovarantoon liittyvät hyvinvointisovellukset sertifioida?

-

6. Valtakunnallisten tietojärjestelmäpalvelujen käytöstä perittävät maksut

Esityksen 47 §:ssä esitetään muutettavaksi valtakunnallisten tietojärjestelmäpalveluiden käytöstä perittävien maksujen perusteita siten, että Kansaneläkelaitoksen tulisi toimittaa arvio seuraavien neljän vuoden kustannuksista yhden vuoden sijasta. Muutoksella tavoitellaan sitä, että merkittävien, valtakunnallisten tietojärjestelmäpalveluiden hoidon edellyttämien investointien kustannukset voidaan huomioida useamman vuoden jaksotuksella niin, etteivät kustannukset kasaannu yksittäiselle vuodelle. Onko maksuihin liittyvistä menettelyistä säädetty riittävän selkeästi ja tarkasti? Jos ei ole, miten säännöstä pitäisi muuttaa?

-

7. Rekisteröidyn oikeus rajoittaa käsittelyä

Olisiko asiakastietolaissa säädettävä siitä, että rekisteröidyn oikeutta käsittelyn rajoittamiseen voitaisiin rajoittaa silloin, kun rekisteröity kiistää henkilötietojen paikkansapitävyyden (EU:n yleinen tietosuoja-asetus 18 art 1 kohta a alakohta)?

-

8. Muut huomiot

Voitte kirjoittaa muut huomionne tähän

Liikenne- ja viestintävirasto Traficom on voimassa olevan sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007, jäljempänä Asiakastietolaki) 3 §:n 1 momentin 9 kohdassa mainittu viranomainen, joka hyväksyy tietoturvallisuuden arviointilaitokset, joille ko. laissa säädetään tehtäviä.

Traficom esittää lausuntonaan lakiuudistuksesta seuraavaa:

1. Viestintävirasto on nykyisin Liikenne- ja viestintävirasto

Hallituksen esityksessä viitataan joissakin kohdin Viestintävirastoon. 1.1.2019 voimaantulleen lakimuutoksen jälkeen Viestintävirastoa ei kuitenkaan enää ole, vaan Liikenteen turvallisuusvirasto Trafi ja Viestintävirasto sekä osa Liikennevirastoa yhdistyivät 1.1.2019 ja muodostavat nyt Liikenne- ja viestintäviraston (Traficom).

Lain Liikenne- ja viestintäministeriön hallinnonalan virastouudistuksen täytäntöönpanoa sekä virastojen tehtävien uudelleenorganisointia koskevan lainsää-dännön voimaanpanosta 4 §:n mukaan: "Lain 1 §:ssä mainitun Liikenne- ja viestintävirastosta annetun lain 2 ja 3 §:ssä tarkoitettuun tehtäväalaan kuuluva tehtävä, joka on muualla laissa säädetty Liikenteen turvallisuusviraston, Viestintäviraston, Liikenneviraston, Ilmailuhallinnon, Telehallintokeskuksen, Autorekisterikeskuksen, Ajoneuvohallintokeskuksen, Rautatieviraston, Merenkulkulaitoksen tai lääninhallituksen hoidettavaksi, siirtyy Liikenne- ja viestintävirastolle 1 päivänä tammikuuta 2019 tämän lain mukaisesti." Näin ollen, vaikka joissakin laeissa lukeekin edelleen "Viestintävirasto", on käytännössä toimivaltainen viranomainen tällöin Liikenne- ja viestintävirasto.

2. Tietojärjestelmän määrittely

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (1406/2011) määritellään tietojärjestelmä siten, että sillä tarkoitetaan (2 §:n 1 momentin 1 kohta): tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä. Tätä vakiintunutta määritelmää on käytetty myös julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, jäljempänä tiedonhallintalaki). Lakiesityksessä on käytetty tietojärjestelmästä uutta määritelmää, joka poikkeaa myös voimassa olevasta Asiakastietolain tietojärjestelmän määrittelystä. Lakiesityksessä ehdotetaan tietojärjestelmän määrittelyksi "ohjelmistoa, järjestelmää tai osajärjestelmää, joka valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi asiakastietojen sähköiseen käsittelyyn, asiakasasiakirjojen tallen-tamiseen ja ylläpitoon tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja". Yhdenmukaisuuden vuoksi Traficom kannattaisi läheisemmin tiedonhallintalain määrittelylle perustuvaa tietojärjestelmän määrittelyä esim. "tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä, jota valmistajan suunnittelemien ominaisuuksien mukaisesti on tarkoitettu käytettäväksi asiakastietojen sähköiseen käsittelyyn, asiakasasia-kirjojen tallentamiseen ja ylläpitoon tai valtakunnallisiin tietojärjestelmäpalveluihin liittämiseen tai jolla sosiaali- ja terveydenhuollon ammattihenkilö voi hyödyntää hyvinvointitietoja".

3. Vaatimustenmukaisuustodistuksen voimassaoloaika

Sekä voimassa olevassa Asiakastietolaissa että sen ehdotetussa muutoksessa (36 §:n 3 momentti) säädetään vaatimustenmukaisuustodistuksen voimassaolo-ajaksi enintään viisi vuotta. Sekä Suomessa että kansainvälisesti tietojärjestelmille tehdyt tarkastukset ovat voimassa korkeintaan

kolme vuotta. Tämä johtuu siitä, että tietoturvallisuuden alalla kehitys on nopeaa. Näin ollen, vaikka tieto-järjestelmän todettaisiin nyt täyttävän sille asetetut vaatimukset, on todennä-köistä, että jollei tietojärjestelmää ole päivitetty tai muuten kehitetty, sen tietoturvallisuuden taso on viidessä vuodessa tippunut huomattavan paljon, eikä sitä voida enää pitää tietoturvallisena. Ei ole olemassa perustetta, miksi sosiaali- ja terveydenhuollon alalla tietojärjestelmien tietoturvallisuuden annettaisiin heikentyä viiden vuoden ajan. Päinvastoin, tietojärjestelmiä tulisi tarkastaa vähintäänkin yhtä usein kuin muillakin yhteiskunnan aloilla. Tämän vuoksi ehdottamme, että ehdotettua 36 §:ää muutettaisiin siten, että vaatimustenmukaisuustodistukset olisivat voimassa vain enintään kolme vuotta. Samoin vaatimustenmukaisuustodistuksen voisi jatkaa enintään kolmeksi vuodeksi kerrallaan.

4. Rekisteri sertifioiduista tietojärjestelmistä

Ehdotetussa 29 §:n 2 momentissa, kuten nykyisessäkin Asiakastietolaissa säädetään, että Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) ylläpitää julkista rekisteriä sille ilmoitetuista sosiaali- ja terveydenhuollon tietojärjestelmistä.

Ehdotamme, että tämä rekisterin tekninen ylläpitovastuu siirrettäisiin Valviralta Kansaneläkelaitokselle (Kela). Kelalla on asiaan vaadittavaa osaamista. Lisäksi rekisterin ylläpito tukisi Kelaa sen työssä sote-tietojärjestelmien sertifiointiprosessin osana. Kela nimittäin suorittaa tietojärjestelmien yhteistestauksen ja varmistaa näin, että tietojärjestelmän voi liittää osaksi Kanta-palvelua.

5. Vaatimustenmukaisuustodistuksen laatiminen

Ehdotetun Asiakastietolain mukaan luokkaan A kuuluvan tietojärjestelmän vaatimustenmukaisuuden todentaminen tapahtuisi

1. tietojärjestelmäpalvelun tuottajan vakuutuksella siitä, että järjestelmä täyttää kaikki olennaiset toiminnallisuutta koskevat vaatimukset

2. Kelan järjestämällä hyväksytyllä yhteistestauksella ja

3. tietoturvallisuuden arviointilaitoksen tekemällä tietoturvallisuuden arvi-oinnilla (kriteeristönä THL:n asiasta antama määräys 1/2015).

Kaikkien edellä mainittujen edellytysten täyttyessä tietoturvallisuuden arviointi-laitos myöntäisi tietojärjestelmälle vaatimustenmukaisuustodistuksen. Tämä vastaa voimassa olevan Asiakastietolain sääntelyä.

Ehdotamme, että luokkaan A kuuluvien tietojärjestelmien olennaisten vaatimusten todentaminen eli vaatimustenmukaisuustodistuksen myöntäminen siirrettäisiin yksityisiltä yrityksiltä eli Traficomin hyväksymiltä tietoturvallisuuden arviointilaitoksilta viranomaistoimijalle eli Kelalle. Arviointilaitokset antaisivat edelleenkin todistuksen tietojärjestelmän tietoturvallisuudesta (kohta 3 yllä), mutta Kela arvioisi koko kokonaisuutta eli yllä mainittujen ehtojen 1-3 täyttymistä. Kohdan 3 täyttyminen osoitettaisiin Kelalle tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Tämä tukisi Kelan roolia sertifiointiprosessissa, kuten yllä aiemmin on kuvattu. Sote-tietojärjestelmien sertifiointiprosessi on nykyisin pirstaloitunut useammalle organisaatiolle: Kelalle, Valviralle, tietoturvallisuuden arviointilaitoksille ja Terveyden ja hyvinvoinnin laitokselle (THL). Olisi erittäin tärkeää, että yhdellä organisaatiolla olisi kokonaisnäkymä prosessiin ja sen lopputulokseen. Kelan asema sertifiointiprosessissa huomioon ottaen, tämä rooli sopisi parhaiten sille. Lisäksi olisi asianmukaista, että sertifiointiprosessin tulokset yhteen dokumenttiin kokoava taho olisi viranomainen eli Kela. Nykyisin prosessia on hankaloittanut myös se, ettei viranomaisillä ole tietoa siitä, mikä Traficomin hyväksymistä tietoturvallisuuden arviointilaitoksista on arvioimassa mitäkin tietojärjestelmää. Tehtävän keskittäminen Kelalle selkeyttäisi tätäkin asiaa. Tarkoituksenmukaista ja kustannustehokkainta olisi, että arviointilaitokset voisivat keskittyä tietoturvallisuuden arviointiin (yllä kohta 3) ja viranomainen hoitaisi lainsäädännössä edellytettyjen hallinnollisten edellytysten valvontaa. Traficomin näkemyksen mukaan Kelalla olisi myös intressi hoitaa vaatimustenmukaisuustodistusten myöntämistä, sillä se hyödyttäisi sen roolia sertifiointiprosessissa.

Ehdottamamme muutos toteutuisi, jos 1) lakiehdotuksen 36 §:n 2 momentti muutettaisiin kuulumaan esimerkiksi seuraavasti: "Jos luokkaan A kuuluva tieto-järjestelmä täyttää käyttötarkoituksensa mukaiset olennaiset tietoturvallisuusvaatimukset, tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan tietoturvallisuuden arvioimisesta tuottajalle todistus ja siihen liittyvä tarkastus-raportti. Arviointi tai uudelleenarviointi on suoritettava…" ja 2) lakiehdotuksen 34 §:n 1 momentti muutettaisiin kuulumaan esimerkiksi seuraavasti "Luokkaan A kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava sertifioinnilla eli tietojärjestelmäpalvelun tuottajan antamalla selvityksellä siitä, että järjestelmä täyttää käyttötarkoituksensa mukaiset toiminnallisuutta koskevat vaatimukset, hyväksytyllä yhteistestauksella ja 36 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Kansaneläkelaitos myöntää sertifioidulle tietojärjestelmälle vaatimustenmukaisuustodistuksen. Tietojärjestelmäpalvelun tuottaja vastaa siitä, että tietojärjestelmä on sertifioitu."

Lisäksi 36 §:n 3 momenttia, 37 §:ää ja 38 §:ää tulisi vastaavasti muuttaa niin, että niissä vaatimustenmukaisuustodistus-sana vaihdettaisiin todistus-sanaksi.

von Fieandt-Lehtonen Anna