APULAISOIKEUSKANSLERI

23.6.2022 OKV/1678/21/2022

OKV/1678/21/2022-OKV-2

Sosiaali- ja terveysministeriö

Viite:
Sosiaali- ja terveysministeriön lausuntopyyntö, Dnro VN/33623/2021, säädösvalmisteluhankeen tunniste STM154:00/2021

Asia:
Lausunto luonnoksesta hallituksen esitykseksi eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (toisiolaki) muuttamisesta

Toisiolain tavoitteena on luoda edellytykset sosiaali- ja terveydenhuollon asiakastietojen hyödyntämiselle myös muissa kuin niiden ensisijaisessa käyttötarkoituksessa.

Lausuttavana olevan hallituksen esityksen tavoitteena on mahdollistaa suomalaisten sosiaali- ja terveydenhuollon rekisteritietojen käyttö kansainvälisessä tutkimusyhteistyössä ja varmistaa samalla tietoturvan ja tietosuojan korkea taso. Tavoitteen toteuttamiseksi hallituksen esityksessä ehdotetaan muutettavaksi toisiolain tietoturvallisille käyttöympäristöille asetettuja vaatimuksia niin, että toisiolain ja Tietolupaviranomaisen asettamat vaatimukset olisi mahdollista täyttää myös Tietolupaviranomaisen määräyksessä määriteltyjä kansainvälisiä standardeja ja menettelyjä noudattamalla. Tietoturvallisten käyttöympäristöjen vaatimustenmukaisuuden arviointeja voisivat toteuttaa Traficomin hyväksymien tietoturvallisuuden arviointilaitosten lisäksi akkreditoidut sertifiointielimet. Akkreditoitu sertifiointielin toimittaisi todistuksen tietoturvallisen käyttöympäristön vaatimustenmukaisuudesta Sosiaali- ja terveysalaln lupa- ja valvontavirastolle (Valvira), joka lisäisi tiedon käyttöympäristöstä ylläpitämäänsä toisiokäyttöympäristöjen rekisteriin.

PL 20, 00023 Valtioneuvosto Puhelin 0295 16001 kirjaamo.okv@gov.fi

www.okv.fi

Esityksen säätämisjärjestysperusteluissa (12 Suhde perustuslakiin ja säätämisjärjestysperustelut, s. 25) todetaan, että esitetty ratkaisu voisi lisätä rekisteröidyille aiheutuvia riskejä verrattuna nykytilaan, jossa Traficomin Kyberturvallisuuskeskuksen hyväksymät tietoturvallisuuden arviointilaitokset auditoivat tietoturvalliset käyttöympäristöt.

Esityksen vaikutusten arvioinnissa (4.2.3.4 Tietoyhteiskuntavaikutukset, s. 16-17) todetaan muun muassa, että muutoksen myötä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat riskit voisivat lisääntyä. Nämä riskit aiheutuisivat esityksen mukaan erityisesti siitä, että kansallisten viranomaisten mahdollisuudet valvoa muualla kuin Suomessa sijaitsevia käyttöympäristöjä olisivat vähäiset. Vaatimustenmukaisuuden arviointeja voisivat esityksen mukaan toteuttaa akkreditoidut sertifiointielimet, joiden toimintaa määrittelisi EU-lainsäädäntö ja kunkin maan kansallinen lainsäädäntö.

Esityksen mukaan julkaistavien tietojen anonymisoinnin varmistamiseen tulisi kiinnittää erityistä huomiota, sillä Tietolupaviranomaisen mahdollisuudet varmistaa kansainvälisissä tutkimusyhteistyössä julkaistavien tietojen anonymisointi ovat hyvin rajalliset ja näin ollen esityksessä ehdotetaankin, että Tietolupaviranomainen voisi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta.

Toisiolain 30 §:n mukaan Valvira valvoo tietoturvallisten käyttöympäristöjen vaatimustenmukaisuutta ja se voi tehdä valvonnan edellytyksenä olevia tarkastuksia. Esityksen mukaan pykälään lisättäisiin säännös, jonka mukaan sertifiointielimien tehtävänä olisi valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. Toisiolain 30 §:n 5 momentin mukaan Sosiaali- ja terveysalan lupa- ja valvontaviranomainen (pitäisi ilm. olla –virasto) voisi antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta.

Pykälää koskevien yksityiskohtaisten perustelujen (s. 22) mukaan tietoturvallisten käyttöympäristöjen vaatimustenmukaisuuden valvonta on toisiolaissa asetettu Valviran tehtäväksi. Kuitenkin käytännössä kansallisen viranomaisen edellytykset valvoa muualla kuin Suomessa sijaitsevia käyttöympäristöjä ovat esityksen mukaan vähäiset. Sen vuoksi Valviran olisi mahdollista antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta. Määräyksessä olisi esityksen mukaan mahdollista määrätä tarkemmin esimerkiksi siitä, miten muiden kuin Suomessa sijaitsevien käyttöympäristöjen valvonta tultaisiin toteuttamaan.

Esityksessä jää epäselväksi, mitä toisiolain 30 §:n 1 momenttiin sisältyvää säännös sertifiointielinten velvollisuudesta valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset, käytännössä tarkoittaa. Perusteluissa lähinnä toistetaan säännöksen sanamuoto. Säännöstä olisi syytä konkretisoida ja sen tarkoitusta ja soveltamiskeinoja tulisi selvittää esityksen perusteluissa.

Esityksen perusteella esityksessä tarkoitetut sertifiointielimet arvioisivat muualla kuin Suomessa olevien tietoturvallisten käyttöympäristöjen vaatimustenmukaisuuden, mutta sertifiointielimet eivät olisi suomalaisten viranomaisten valvonnan ulottuvissa, kuten eivät myöskään tietoturvalliset käyttöympäristöt, joiden vaatimustenmukaisuudesta sertifiointielimet antaisivat todistuksen. Esityksen mukaan ulkomailla sijaitsevia käyttöympäristöjen vaatimustenmukaisuutta valvoisi sama taho, joka antaisi niille todistuksen vaatimustenmukaisuudesta.

Esityksen perusteella näyttää siltä, että suomalaisten viranomaisten mahdollisuudet vaikuttaa toisiolain mukaisten tietojen käyttöympäristöjen arviointiin ja valvontaan samoin kuin niitä arvioivien toimijoiden ohjaamiseen ja valvontaan heikkenisivät samalla, kun tietojen käytöstä ihmisten oikeuksille ja vapauksille aiheutuvien riskien arvioidaan kasvavan.

Lisäksi muutos heikentäisi Tietolupaviranomaisen mahdollisuudet varmistaa kansainvälisissä tutkimusyhteistyössä julkaistavien tietojen anonymisointi, joka on nähdäkseni yksi keskeinen tietosuojaa turvaava toimenpide.

Esityksessä on edellä mainitulla tavalla tunnistettu, että muutos voi lisätä riskejä ihmisten oikeuksille ja vapauksille. Toisiolain tarkoittamissa tietoturvallisissa käyttöympäristöissä käsiteltävät tiedot koskevat arkaluonteisia tietoja, jotka kuuluvat perustuslain 10 §:ssä säädetyn yksityiselämän suojan ydinalueeseen. Sen vuoksi esityksessä olisi syytä käsitellä ja arvioida muutoksen mahdollisesti aiheuttamia riskejä perusteellisemmin (esimerkiksi riskien suuruusluokka, todennäköisyys) ja konkreettisemmin (esimerkiksi tilanteet, joissa riskit voivat toteutua ja millaisia ne voisivat olla). Vasta sen jälkeen esitystä olisi aidosti mahdollista arvioida perusoikeuksien suojan kannalta ja siltä kannalta, onko perusoikeuksista poikkeamiselle olemassa hyväksyttävät perusteet. Riskejä olisi mielestäni syytä käsitellä sekä vaikutusten arvioinnissa (myös ihmisiin kohdistuvina vaikutuksina, kohta 4.2.3.1) että säätämisjärjestysperusteluissa, jossa tulisi riskien konkretisoinnin kautta arvioida myös esityksen perustuslainmukaisuus.

Edelliseen liittyen esityksessä olisi lisäksi syytä tuoda esille, miten arviointilaitosten ja sertifiointielinten samoin kuin Suomessa ja ulkomailla sijaitsevien tietoturvallisten käyttöympäristöjen toiminnan seuraaminen, ohjaaminen ja valvominen käytännössä eroaisivat toisistaan ja miten suomalaiset viranomaiset voisivat käytännössä varmistua sertifiointielinten ja ulkomailla sijaitsevien käyttöympäristöjen toiminnan lainmukaisuudesta ja asianmukaisuudesta. Tässä arvioinnissa olisi syytä esimerkiksi tuoda esille, mitkä ovat ne käytännön keinot, joilla Valvira voi suorittaa sille kuuluvaa valvontavelvollisuuttaan. Tämä olisi nähdäkseni perusteltua myös siksi, ettei valvovalle viranomaiselle asetettaisi velvoitteita, joita se ei käytännössä pystyisi toteuttamaan. Valvontavelvoite ei voi olla pelkästään näennäinen etenkin huomioiden ne riskit, joita sosiaali- ja

terveydenhuollon asiakastietojen käsittelystä voi sosiaali- ja terveydenhuollon asiakkaiden oikeuksille aiheutua. Valvontavelvoitteen ja keinot sen toteuttamiseen tulee olla selkeät, jotta valvontaa on mahdollista toteuttaa tehokkaasti.

Tietoturvallisuuden arviointilaitoksista annetun lain 13 §:n mukaan arviointilaitoksen olisi laissa tarkoitettuja tehtäviä hoitaessaan noudattava hallintolakia, julkisuuslakia ja kielilakia. Kyseistä lakia koskevan hallituksen esityksen (HE 45/2011 vp, s. 10) mukaan säädösten soveltamista ei ehdotuksen mukaan olisi sidottu julkisen hallintotehtävän hoitamiseen, vaan säädöksiä sovellettaisiin kaikkiin ehdotetun lain mukaisten tehtävien hoitamiseen. Esityksen perusteella arviointilaitoksen tehtävien on katsottu sisältävän julkisten hallintotehtävin hoitamista.

Toisiolaissa tarkoitetut muualla kuin Suomessa sijaitsevat sertifiointielimet hoitaisivat samoja tehtäviä kuin arviointilaitokset (todistuksen antaminen (25 §), kehotuksen antaminen ja todistuksen peruuttaminen (27 §), ilmoitusvelvollisuus (28 §), todistuksen uudistaminen (29 §), valvonta ja edistäminen (30 §)) Suomessa. Niihin ei kuitenkaan sovellettaisi Suomen lainsäädäntöä eikä siten myöskään hallinnon yleislakeja, joita Suomessa sovelletaan julkisia hallintotehtäviä hoidettaessa. Esitystä tulisi arvioida myös tästä näkökulmasta esityksen säätämisjärjestysperusteluissa.

Tämä asiakirja on allekirjoitettu sähköisesti.

Apulaisoikeuskansleri — Mikko Puumalainen

Esittelijäneuvos — Marjo Mustonen