Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

Lausunto

28.07.2022

Asia: VN/33623/2021

Lausuntopyyntö luonnoksesta hallituksen esitykseksi eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta

Lausunnonantajan lausunto

Mahdollistaako luonnoksessa hallituksen esitykseksi esitetty ratkaisuehdotus suomalaisten rekisteritietojen käytön kansainvälisessä tutkimusyhteistyössä?

Jos ei, perustele miksi [Hallituksen esityksessä ehdotetaan muutettavaksi lain sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019, toisiolaki) koskevia vaatimuksia. Hallituksen esityksessä keskeisiä muutoksia on Tietolupaviranomaisen määräysten muuttaminen aikaisempaa enemmän kansainvälisiä standardeja hyödyntäväksi ja tietoturvallisten käyttöympäristöjen vaatimustenmukaisuuden arviointeja voisivat toteuttaa Traficomin hyväksymien tietoturvallisuuden arviointilaitosten lisäksi akkreditoidut sertifiointielimet. Sertifiointielimelle ehdotetaan myös oikeutta valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. Valvira toteaa, että sertifiointielimelle ehdotettu oikeus valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset on kokonaan uusi tehtäväkokonaisuus, joka aikaisemmin on toteutettu viranomaistehtävänä. Kokonaan uuden tehtäväkokonaisuuden siirto yksityiselle sertifiointielimelle tulisi aiheuttamaan merkittävää ja osin myös ennakoimatonta kustannusten nousua niiden arvioimia tietoturvallisia käyttöympäristöjä käyttäville tutkijatahoille. Tämä ei edistäisi tavoitetta rekisteritietojen hyödyntämisestä kansainvälisessä tutkimusyhteistyössä. Hallituksen esityksessä ei ole esitetty arvioita tehtäväkokonaisuuden siirrosta aihetuvista kustannuksista tietoturvallisia käyttöympäristöjä hyödyntäville tahoille. Tulee huomioida, että osa sertifiointielimelle ehdotetuista tehtävistä on luonteeltaan jatkuvaa toimintaa.]

Onko jokin ehdotuksessa esitetty muu toteuttamisvaihtoehto parempi kuin esitetty ratkaisuehdotus?

2) Yhteiseurooppalaiset ratkaisut [Hallituksen esitysluonnoksessa tuodaan esille Euroopan komission toukokuussa 2022 julkaisema ehdotus eurooppalaisen terveysdata-avaruudesta (EHDS). EHDS-säädösehdotus koskee myös terveystietojen toisiokäyttöä ja ehdotus sisältää säännökset tietoturvallisista käsittely-ympäristöistä. Ehdotuksen käsittely ja säädöksen mukaisten käsittely-ympäristöjen käyttöönotto arvioidaan kuitenkin vievän aikaa. Valvira toteaa, että myös hallituksen esityksessä ehdotettu eteneminen tulee viemään huomattavasti aikaa. Hallituksen esityksessä ehdotetun lainsäädännön muutoksen hyväksymisen jälkeen on Tietolupaviranomaisen aloitettava valmistelu määräyksien muuttaminen kansainvälisiä standardeja ja menettelyjä hyödyntäväksi. Myös

akkreditoitujen sertifiointielinten valinta ja hyväksyminen tulevat viemään aikaa. Valvira katsoo, että parempi vaihtoehto ehdotetulle ratkaisulle on odottaa yhteiseurooppalaisia ratkaisuja ja samanaikaisesti pyrkiä vaikuttamaan yhteiseurooppalaisen ratkaisun valmisteluun. Toisiolain muuttaminen lyhyeksi aikaa juuri ennen eurooppalaisen terveysdata-avaruuden (EHDS) tuoman uuden sääntelyn johtaa tilanteeseen, jossa säädökset muuttuisivat useasti verrattain lyhyen ajan sisällä.]

Mitä muita ratkaisuvaihtoehtoja olisi mahdollista esittää kansainvälisen tutkimusyhteistyön toteuttamiseksi? Perustelut ratkaisuvaihtoehdolle.

-

Muut hallituksen esityksen luonnosta koskevat huomiot.

Hallituksen esityksessä kohdassa 4.2.2 Vaikutukset viranomaisten toimintaan arvioidaan vaikutusta Valviran toimintaan: ”Ehdotus vaikeuttaisi Valviralle nykyisessä lainsäädännössä annettua tehtävää valvoa ja edistää sitä, että tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. On todennäköistä, että Valviralla ei olisi käytännöllisesti katsoen mahdollisuutta valvoa muiden kuin Suomessa sijaitsevien tietoturvallisen käyttöympäristöjen vaatimustenmukaisuutta. Lisäksi valvontaan kuuluvia tarkastuksia ei olisi mahdollista toteuttaa Suomen ulkopuolella… Valvira voisi antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta.”

Valvira toteaa, että sen toimivalta viranomaisena ei ulotu Suomen rajojen ulkopuolelle. Valvira katsoo, että sen toimivalta ei ulotu antamaan sitovaa määräystä ulkomaalaiselle sertifiointielimelle, joka arvioisi ulkomailla sijaitsevaa tietoturvallista käyttöympäristöä. Lisäksi Valviralla ei olisi keinoja seurata tai varmistua noudatettaisiinko annettua määräystä. Sekä sertifiointielin että tietoturvallinen käyttöympäristö voivat sijaita myös EU/Eta-alueen ulkopuolella. Valviran näkemyksen mukaan hallituksen esityksessä Valviralle ehdotettu mahdollisuus antaa määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta ei siten toteuta hallituksen esityksen lähtötavoitetta hyödyntää rekisteritietoja, samalla kuitenkin rekisteröityjen tietosuojan korkeasta tasosta huolehtien.

Hallituksen esityksessä annetaan sertifiointielimien tehtäväksi toteuttaa arviointeja sekä valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. Valviran näkemyksen mukaan hallituksen esityksessä ei ole riittävästi arvioitu sitä, voidaanko toisiolain 30 §:n mukainen valvontatehtävä antaa luonnoksessa ehdotetulla tavalla sertifiointielimelle, ottaen huomioon mitä perustuslain (731/1999) 124 §:ssä säädetään hallintotehtävän antamisesta muulle kuin viranomaiselle. Hallituksen esityksen mukaan sertifiointielin voisi toteuttaa arviointeja ja siten myös suorittaa valvontaa Suomessa.

Hallituksen esitys asettaa Suomessa sijaitsevat tietoturvallisuuden arviointilaitokset ja sertifiointielimet keskenään eriarvoiseen asemaan. Suomalaisia tietoturvallisuuden arviointilaitoksia sitoo laki tietoturvallisuuden arviointilaitoksista (1405/2011) ja Traficomin antama ohje tietoturvallisuuden arviointilaitoksille. Hallituksen esityksessä suomalaista tietoturvallisuuden

arviointilaitosta säädeltäisiin siten enemmän kuin sertifiointielintä myös silloin kuin ulkomainen sertifiointielin toimisi Suomessa arvioidessaan tietoturvallisia käyttöympäristöjä.

Hallituksen esityksen mukaan Valviran tulee hyväksyä tietoturvallisia käyttöympäristöjä toisiokäyttöympäristöjen rekisteriin akkreditoidun sertifiointielimen antaman todistuksen perusteella. Lisäksi Valvira vastaanottaisi todistusten lisäksi tarkastusraportteja arvioinneista. Valvira toteaa, että sillä ei ole toimivaltaa Suomen rajojen ulkopuolelle. Hallituksen esityksessä ehdotettu toimintamalli johtaa siten siihen, että ulkomaalaisen sertifiointielimen Valviralle lähettämien dokumenttien oikeellisuutta ei olisi käytännössä mahdollista tarkastaa tai kyseenalaistaa. Sama koskisi myös sertifiointielimen tuottamia tarkastusraportteja. Vaikka tarkastusraportissa nostettaisiin esille merkittävä tietoturvariski ulkomailla sijaitsevassa käyttöympäristössä, niin Valviralla ei olisi toimivaltaa mitenkään siihen puuttua. Siten Valvira toimisi ehdotetussa toimintamallissa käytännössä vain kirjaamona vastaanottaessaan sertifiointilaitoksen lähettämiä dokumentteja ulkomailla sijaitsevista käyttöympäristöistä. Hallituksen esityksessä ei ole avattu vastuu tai toimivaltakysymyksiä ulkomailla tapahtuvan mahdollisen tietomurron tai muun vastaavan tapahtuessa.

Hallituksen esityksessä ehdotetaan 26§:ssä ”Sertifiointielin arvioi tämän lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Esityksen 30§:ssä ehdotetaan ”Sertifiointielimien tehtävänä on valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset.” Valvira toteaa, että hallituksen esityksen mukaan sertifiointielin itse ensin arvioi käyttöympäristöjen tietoturvallisuutta koskevia vaatimuksia ja tämän arvioinnin suorittamisen jälkeen asettuu osittain myös itse valvomaan niitä samoja kokonaisuuksia, joita se itse oli arvioimassa. Sertifiointielin vaikuttaisi siten valvovan myös sen itsensä tekemää työtä. Ehdotettuja pykäliä tulisi tarkastella myös valvontatoimivallan ja mahdollisen eturistiriidan näkökulmasta.

Elo Marko
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira