Heidi Kivekäs

Lausunto

25.07.2022

TRAFICOM/278294/03.03.00/2022

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?

-

Onko jokin ehdotuksessa esitetty muu toteuttamisvaihtoehto parempi kuin esitetty ratkaisuehdotus?

-

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

-

Muut hallituksen esityksen luonnosta koskevat huomiot.

Käyttöympäristöjen tietoturvallisuus ja tietoturvallisuuden valvonta

Toisiolain muuttamista koskevan esityksen tarkoituksena on mahdollistaa terveystietojen tutkimuskäyttö myös Suomen ulkopuolella sijaitsevissa käyttöympäristöissä. Nykyisin käyttöympäristön tietoturvallisuuden voi osoittaa vain Liikenne- ja viestintäviraston hyväksymän arviointilaitoksen myöntämällä todistuksella ja arvio tehdään Tietolupaviranomaisen määräystä vasten. Esityksessä esitetään, että jatkossa käyttöympäristön tietoturvallisuuden voisi osoittaa myös akkreditoidun sertifiointielimen myöntämällä todistuksella ja arvio voitaisiin tehdä kansainvälisiä standardeja vasten. Suomessa akkreditoinnin tekisi FINAS. Tietolupaviranomainen voisi antaa tarkempia määräyksiä menettelyistä, standardeista ja niistä sertifiointielimistä, jotka voivat tehdä arvioita.

Liikenne- ja viestintävirasto pitää toisiolain tavoitteiden kannalta keskeisenä, että tietoja käsitellään tietoturvallisissa käyttöympäristöissä ja että käyttöympäristöjen turvallisuus on arvioitu asianmukaisesti ja yhtenäisesti riippumatta siitä, kuka arvioinnin on tehnyt.

Liikenne- ja viestintävirasto pitää toisiolain tavoitteiden kannalta keskeisenä, että tietoja käsitellään tietoturvallisissa käyttöympäristöissä ja että käyttöympäristöjen turvallisuus on arvioitu asianmukaisesti ja yhtenäisesti riippumatta siitä, kuka arvioinnin on tehnyt. Perusperiaatteena voidaan pitää sitä, että suomalaisen henkilötietojen käsittelyllä tulisi olla samat vaatimukset koko EUalueella ja myös vastaanottajan käyttöympäristön tietoturvallisuus tulisi kyetä todentamaan. Virasto korostaa tietoturvan ja tietosuojan huolellista suunnittelua ja toteuttamista digitaalisissa ympäristöissä erityisesti kriittisillä toimialoilla, kuten sosiaali- ja terveysalalla. Puutteellisesta tietoturvasta johtuvat tietovuodot ja tietojen suojan vaarantuminen voivat aiheuttaa merkittävää vahinkoa ja kustannuksia kuin myös henkisiä kärsimyksiä tietovuodon uhreiksi joutuneille. Virasto korostaa, että ennakolliset panostukset tietoturvaan ja -suojaan sekä niiden arviointeihin ovat kustannuksiltaan huomattavasti pienempiä kuin kustannukset, vahingot ja mahdolliset henkiset kärsimykset, joita voi aiheutua tietomurron tai tietojen vuotamisen johdosta. Ilman tietoa toisiolain myötä annettavien määräyksien sisällöstä ei ole mahdollisuutta arvioida tietoturvavaatimusten ja -suojauskontrollien riittävyyttä. Asetettavien tietoturvavaatimusten ja -suojauskontrollien lisäksi käyttöympäristöjen tietoturvallisuuden valvontaan ja valvonnan toimivuuteen on myös syytä kiinnittää erityistä huomioita.

Esityksessä ehdotetaan, että sertifiointielinten tehtävänä on valvoa ja edistää sitä, että niiden arvioimat käyttöympäristöt täyttävät tietoturvaa ja -suojaa koskevat vaatimukset. Epäselväksi kuitenkin jää se, mitä sertifiointielinten valvontatehtävät sisältävät ja mikä on niiden ja VALVIRA:n välinen tehtävänjako käyttöympäristöjen tietoturvan ja -suojan valvonnassa. Epäselväksi jää myös se, minkä nojalla viranomaiselle kuuluva valvontatehtävä voitaisiin antaa muulle kuin viranomaiselle eli tässä tapauksessa sertifiointielimelle. On myös epäselvää, miten valvonta toteutetaan ulkomailla sijaitseviin käyttöympäristöihin, joihin lähtökohtaisesti sovelletaan muun maan kuin Suomen lainsäädäntöä ja joihin VALVIRA:n toimivaltuudet eivät lähtökohtaisesti päde. Erityisesti tilanne muuttuu haastavaksi, jos käyttöympäristöjen fyysistä turvallisuutta tulisi arvioida paikan päällä tai jos palvelut ovat sijoitettu pilviympäristöihin.

Käyttöympäristöjen arviointi- ja sertifiointielimet

Valtioneuvoston periaatepäätöksessä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (TITUKRI) esitettiin, että arviointilaitosten määrää kasvatettaisiin ja hyväksymismenettelyä tehostettaisiin. Toisiolakiin esitetyt muutokset akkreditoidun sertifiointielimen hyödyntämisestä käyttöympäristöjen tietoturvallisuuden arvioinnissa voidaan lähtökohtaisesti katsoa olevan linjassa periaatepäätöksen kanssa edellyttäen, että sertifiointielinten arviointitoiminnan korkeaan laatuun ja ammattitaitoon kiinnitetään huomiota Tietolupaviranomaisen määräyksissä. Määräyksissä on myös syytä huomioida EU:n kyberturvallisuusasetus ja sen nojalla valmistelussa olevat sertifiointikehykset soveltuvin osin.

Toisiolakiin esitetyt muutokset käytännössä ohjaisivat Suomessa tietojärjestelmien ja tietoliikennejärjestelyjen arviointia entistä enemmän malliin, jossa:

1. Liikenne- ja viestintäviraston hyväksymillä ja KATAKRI- ja VAHTIpätevyyden omaavilla arviointilaitoksilla olisi automaattisesti pätevyys tehdä arviointeja ja antaa todistuksia toimialasta ja pätevyysalueesta riippumatta (eli arviointilaitoksista tulisi niin sanotusti yleispäteviä arviointielimiä tehdä ja antaa todistuksia toimialasta ja pätevyysalueesta riippumatta) sen lisäksi, että ne voisivat tehdä nykyisen tavoin arviointeja turvallisuusluokitellun tiedon käsittelyyn tarkoitetuille tietojärjestelmille ja tietoliikennejärjestelyille.

2. FINAS:n akkreditoimilla ja hyväksymillä sekä tietyn yksittäisen toimialan pätevyysalueen (esim. pätevyys tehdä arivointeja ja antaa todistuksia toisiolain mukaisille käyttöympäristöille) omaavilla arviointi- ja sertifiointielimillä olisi mahdollisuus tehdä arviointeja ja antaa todistuksia tietyllä yksittäisellä pätevyysalueella pois lukien KATAKRI- ja VAHTI-pätevyysalueet, joihin pätevyyden voi saada vain Liikenne- ja viestintäviraston arviointilaitokselle antaman hyväksynnän kautta.

Liikenne- ja viestintävirasto suhtautuu lähtökohtaisesti myönteisesti tällaiseen malliin. Tällaisessa mallissa on tärkeää, että FINAS:lle ja toisiolakia valvoville viranomaisille varataan riittävät resurssit valvoa mahdollisia käyttöympäristöjen arviointeja tekeviä serfiointielimiä ja antaa neuvontaa niille toisiolaissa ja toisiolain nojalla annettavissa määräyksissä asetetuista tietoturvallisuuden vaatimuksista käyttöympäristöille. Toisiolakia valvovien viranomaisten tulee varautua myös antamaan arviointilaitoksille neuvoa toisiolain ja sen nojalla annettavien määräyksien tietoruvallisuudelle asettamista vaatimuksista. Liikenne- ja viestintäviraston arviointilaitosten neuvonta kohdistuu ennen kaikkea teknisiin arviointimenetelmiin, ei toimialakohtaisissa lainsäädännössä asetettuihin tietoturvallisuuden vaatimuksiin.

Muut huomiot

Virasto pitää perusteltuna sitä, että toisiolaissa säädettäisiin tietoturvallisille käyttöympäristöille asetettavista vaatimuksista ainoastaan yleisellä tasolla ja tarkemmat määräykset vaatimuksista antaisi Tietolupaviranomainen toisiolain 24 §:n mukaisesti. Tietoturva- ja tietosuojauhkat kehittyvät nopeasti ajassa kuin myös tietoturvaa ja -suojaa koskeva standardointi. Määräykset, alemman tason säädöksinä mahdollistavat nopean reagoimisen tunnistettuihin tietoturva- ja tietosuojauhkiin kuin myös standardointiin tehtyihin muutoksiin. Virasto pitää kannatettavana, että arviointiperusteena hyödynnetään EU:n kyberturvallisuusasetuksen mukaisia tulevia sertifiointijärjestelmiä ja muita EU:n laajuisia kehikoita, kuten European Health Data Space, EHDS:ää.

Kivekäs Heidi