ESiOR Oy

Lausunto

29.07.2022

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 kyllä, perustele miksi [Pääosin kyllä, mutta muissa huomioissa esitämme tähän liittyviä seikkoja. Ehdotus keskittyy tähän tilanteeseen, mutta ohittaa tilanteet, joissa ulkomaalaista dataa saadaan Suomeen - se olisi toivottavaa tutkimuksen lisääntymisen tavoitteelle Suomessa.]

Onko jokin ehdotuksessa esitetty muu toteuttamisvaihtoehto parempi kuin esitetty ratkaisuehdotus?

3) Näiden vaihtoehtojen yhdistelmä [Yhdistelmä suositeltava; tässä vaiheessa on oleellista lain kehittäminen toimivammaksi ja varautuminen yhteiseurooppalaiseen ratkaisuun, kuten EHDS. Pääosin lisäykset ovat hyviä, mutta toisiolaissa on muitakin puutteita, joita nostamme esille muissa huomioissa.]

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

Pitäisi huomioida tilanteet, joissa dataa tuodaan Suomeen - se tulisi olla osatavoitekin. Se lisäisi tutkimusta, kehittäisi kansantaloutta ja kasvattaisi Suomen mainetta erinomaisena tutkimusmaana.

On epäselvää, miksi esityksessä lähdetään liikkeelle siitä, että viemme tiedon ja osaamisen Suomesta muualle, mutta emme toisi sitä ollenkaan Suomeen (tai ainakin se vaihtoehto ehdotuksessa ohitetaan kokonaan)?

Muut hallituksen esityksen luonnosta koskevat huomiot.

ESiOR Oy kiittää mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta (diaarinumero VN/33623/2021).

ESiOR Oy tarjoaa mm. terveystalous-, vaikuttavuustutkimus- ja market access -palveluita aina tutkimuksen tai mallinnuksen suunnittelusta sen julkaisuun saakka. Asiakkailta tulleiden tarpeiden ja oman kokemuksensa perusteella ESiOR on kehittänyt myös Suomessa sijaitsevan private cloud -tyyppisen tietoturvallisen käyttöympäristön (SPE, secure processing environment) nimeltään SPESiOR, joka on auditoitu ja listattu Valviran Toini-rekisteriin hyväksytyksi SPE:ksi jo ennen toisiolain siirtymäajan päättymistä 1.5.2022. SPESiOR mahdollistaa myös mm. uuden tiedon keruun, siirron, analysoinnin ja säilyttämisen SPE-tasoista tietoturvaa noudattaen.

Esitämme alla huomioita esitysluonnoksesta. Ehdotamme tällaisten esitysluonnosten jakelua tulevaisuudessa kaikille Valviran Toini-listan mukaisille organisaatioille, joilla on tietoturvallinen käyttöympäristö.

Luonnoksen mukaan ehdotettu laki on tarkoitettu tulemaan voimaan 1. päivänä joulukuuta 2023. Keskustelimme että onko siirtymäaika riittävä, jos muutokset ovat merkittäviä? Eurooppalaisen harmonisointiehdotuksen (EHDS, European Health Data Space) aikataulu vaikuttanee myös, jos ja kun yhteiseurooppalaista harmonisointia toteutetaan kansallisesti.

Lausuntopyynnöstä puuttuu oleellinen näkökohta: Mahdollistaako luonnoksessa hallituksen esitykseksi esitetty ratkaisuehdotus ulkomaalaisten rekisteritietojen käytön Suomessa? Miksi asia on ohitettu kokonaan?

Taustan osalta toisiolaki edellyttää, että Suomesta saatava tietoaineisto luovutetaan ainoastaan toisiolain vaatimusten mukaisesti auditoituun tietoturvalliseen käyttöympäristöön ja Tietolupaviranomaisen voimassa oleva määräys rajoittaa käyttöympäristöt EU/ETA-alueelle.

Lakiehdotuksessa on kiinnitetty erityistä huomioita tiedon siirrolle Suomesta ulkomaille. Mutta lähtökohtaisesti tilanne olisi parempi, jos tieto siirtyisi ulkomailta Suomeen tietoturvalliseen käyttöympäristöön. Tämän asian huomiointi ja tukeminen pitäisi olla ehdotuksessa ja toimintastrategiana merkittävästi isommassa roolissa, kun halutaan lisätä tutkimusta Suomessa sekä Suomen mainetta erinomaisena tutkimusmaana. Suomessa on kuitenkin useita tietoturvallisia käyttöympäristöjä (Toini-rekisteri), joilla on erilaisia käyttötarkoituksia ja ominaisuuksia.

Näiden osalta on lisäksi hyvä huomioida se, että EU/ETA-alueen ulkopuolelle tapahtuva aineistonsiirto tietoturvalliseen käyttöympäristöön vaatisi aika paljon muutoksia ja sopimuksia. Suomalaiset ja ulkomaalaiset toimijat ja julkiset tai yksityiset toimijat eivät saa joutua ainakaan suomalaisen aineiston osalta eriarvoiseen tilanteeseen, jossa olisi käytössä erilaiset määräykset tai määräykset, jotka jotenkin estäisivät tai heikentäisivät nykyisen Toini-listatun tietoturvallisen käyttöympäristön käyttöä.

Nykyisellään suomalaisten ja muiden maiden rekisteritietojen käyttöä kansainvälisessä tutkimusyhteistyössä voitaisiin edistää muuttamalla toisiolain tietoturvallisia käyttöympäristöjä koskevia vaatimuksia niin, että kansainvälinen auditointi olisi paikallisen auditoinnin lisäksi

mahdollinen käyttöympäristölle. Myös ulkomaisilla toimijoilla ja heidän tietoturvallisilla käyttöympäristöillään tulee olla samat tietoturva- ja muut vaatimukset kuin suomalaisilla ympäristöillä.

Standardi, sertifiointi ja akkreditointi: ISO/IEC 27001 on kansainvälisesti yksi tunnetuimmista ja käytetyimmistä organisaation tietoturvallisuuden hallinnan standardeista, jonka asema tulisi säilyttää. Fyysisen turvallisuuden osalta on oltava Katakria tms. vastaavat/soveltuvat vaateet, jotta datojen sijainnit ja niihin pääsyt sekä esim. katastrofien hallinta tulee oikeasti varmistettua. Koronatilanteen muututtua ei ole esteitä suorittaa fyysisiä auditointeja. Jos päädytään vaihtamaan standardeja, tulee huomioida riittävä siirtymäaika toimijoille toteutumiseksi. Lisäksi tulee huomioida, että sertifiointikustannukset muodostavat suuria kustannuksia organisaatioille. Tulevaisuudessa tarvittaisiin listaus EU:n tasolla akkreditoiduista palveluntarjoajista, jotta tietoturvallisia käyttöympäristöjä on helpompi löytää.

Toisiolain 20 §:n mukaan henkilötiedot luovutetaan ensisijaisesti Tietolupaviranomaisen omaan tietoturvalliseen käyttöympäristöön (Kapseli). Tämä kohta tulisi poistaa laista, koska kohta on ristiriidassa lakimuutoksen tavoitteiden kanssa, laissa ei tulisi eriarvoistaa tietoturvallisia käyttöympäristöjä asetelmaan Kapseli ja muut ympäristöt, ja lisäksi tämä asetelma voi olla omiaan luomaan monopolitilannetta. Tietoturvallisten käyttöympäristöjen käyttötarkoitusten piirissä hyväksytyt ympäristöt täyttävät säännösten perusteella vähintään samat säädökset kuin Kapseli, joten lainkohdalle ei ole perustetta. Markkinoilla on myös yksityisomisteinen ympäristö SPESiOR ja eri ympäristöillä on hieman erilaisia ominaisuuksia ja käyttötarkoituksia käytännön toiminnan kannalta.

Toisiolain 20 §:n 3 momentin mukaan, jos tietolupahakemuksessa pyydetään luovuttamaan tietoaineistoja käsiteltäviksi muussa kuin Tietolupaviranomaisen käyttöympäristössä, hakemuksessa on erikseen perusteltava syyt, joiden vuoksi tämä on välttämätöntä. Tämä kohta tulisi olla väljempi – riittää, kunhan tietoturvallinen käyttöympäristö on hyväksytty (Toini-rekisteri) ja sen käyttötarkoitus on sopiva. Jos laissa pidetään mukana mainittu perusteiden välttämättömyys, tarvitaan tarkempi määritelmä, millä perusteella tietoaineistojen käsittely voidaan tehdä muualla kuin Tietoturvaviranomaisen käyttöympäristössä ja esimerkkejä. Lähtökohtaisesti rekisterinpitäjillä on tässä iso merkitys ja ainakin yksittäinen rekisterinpitäjä voi vaikuttaa suoraan ympäristön valintaan. Muita seikkoja ovat ainakin ympäristön tekniset ominaisuudet ja saatavuus (aikataulu) sekä asiakkaan tai sponsorin vaatimukset.

Tietolupaviranomainen tai muu toisiolaissa tarkoitettu viranomainen saa tällöin luovuttaa tiedot hakijalle vain, jos käyttöympäristö täyttää toisiolain 20 §:n2 momentissa ja 21–29 §:ssä säädetyt edellytykset. Tämä lain kohta on toimiva ja tulee säilyttää.

Toisiolain 23 §:n 1 momentin mukaan tietoturvallinen käyttöympäristö on suojattava valtion viranomaisten tietoturvallisuutta koskevien velvoitteiden mukaisesti noudattaen, mitä julkisuuslain

36 §:ssä ja mainitun pykälän 1 momentin nojalla annetussa valtioneuvoston asetuksessa säädetään. Tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta valtionhallinnossa säädetään nykyään julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, jäljempänä tiedonhallintalaki) 4 luvussa. Tiedonhallintalain 18 §:ssä säädetään turvallisuusluokiteltavista asiakirjoista valtionhallinnossa. Turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä ja turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvistä tietoturvallisuustoimenpiteistä säädetään tarkemmin valtioneuvoston asetuksella asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Mutta voidaanko turvallisuusluokittelua soveltaa terveysdataan?

Tietoturvallisen käyttöympäristön olennaisista muutoksista on ilmoitettava tietoturvallisuuden arviointilaitokselle. Arviointilaitoksen myöntämä todistus on uudistettava, jos käyttöympäristöön tehdään merkittäviä muutoksia tai jos käyttöympäristöä koskevia vähimmäisvaatimuksia on muutettu tavalla, jonka edellytyksenä on uusi arviointi. Mutta mitä tarkoitetaan olennaisilla muutoksilla?

Toisiolain 52 §:ssä säädetään tietoluvan nojalla luovutetuista tiedoista johdettujen tulosten julkaisemisesta. Kun tietoluvan nojalla on luovutettu tietoja käsiteltäviksi tietoturvallisessa käyttöympäristössä ja niiden pohjalta tuotettuja tuloksia halutaan julkaista, Tietolupaviranomainen vastaa julkaistavien tietojen anonymisoinnin varmistamisesta. Tietolupaviranomainen voi kuitenkin perustellusta syystä lupapäätöksessään myöntää luvansaajalle oikeuden toteuttaa itse julkaistavien edellä mainittujen tietojen anonymisoinnin ehdolla, että ne toimitetaan jälkikäteen Tietolupaviranomaisille.

Olisi hyvä tarkentaa, mitä tarkoittaa julkaiseminen – onko se tiedon tuontia tietoturvallisen käyttöympäristön ulkopuolelle? Ja mikä on perusteltu syy, että luvansaajalle myönnetään oikeus toteuttaa itse julkaistavien tietojen anonymisointi? Ainakin yksittäisen rekisterinpitäjän luvittaman tiedon osalta pitäisi anonymisoinnin varmistaminen olla mahdollista automaattisesti muuallakin kuin Tietolupaviranomaisella ehdolla, että tiedot toimitetaan jälkikäteen Tietolupaviranomaisille. Anonymisoinnin varmistamisen menetelmien osalta riittänee Tietolupaviranomaisen käyttämät anonymisoinnin varmistamisen menetelmät.

Tietolupaviranomainen tuottaa anonymisoidut tulokset ja luovuttaa ne luvansaajalle vapaasti julkaistaviksi tämän tekemän pyynnön ja pyyntöön liitetyn ehdotuksen perusteella riippumatta siitä, onko tietoluvan myöntänyt yksittäinen rekisterinpitäjä vai Tietolupaviranomainen. Sanamuodon osalta on todettava, että käytännössä Tietolupaviranomainen ei itse tuota anonymisoituja tuloksia. Mutta Tietolupaviranomainen varmistaisi siis kaikki anonymisoinnit niiden luvittajasta riippumatta. Jos tutkimus tehdään yhden rekisterinpitäjän aineistoon, Tietolupaviranomainen vastaa edelleen anonymisoinnista? Koskettaako tämä myös Tilastokeskusta, jonka aineistoista osa sisältää sosiaali- tai terveystietoa? Askarruttaa että miksi tietolupaviranomainen tulee mukaan yhden rekisterinpitäjän prosessiin, jossa lupaa Tietolupaviranomaiselta ei vaadita? Lisäksi tuleeko saatu yksittäisen rekisterinpitäjän tietolupa toimittaa samalla anonymisoitavan aineiston kanssa Tietolupaviranomaiselle? Tulisiko lakia muuttaa näiltä osin?

Tietolupaviranomaisen määräyksessä asetetut vaatimukset tietoturvallisille käyttöympäristöille ovat käytössä kaikkiin niihin toisiolaissa säädettyihin käyttötarkoituksiin, joihin tarvitaan tietolupa. Näitä käyttötarkoituksia ovat tieteellinen tutkimus, tilastointi, opetus sekä viranomaisen suunnittelu- ja selvitystehtävä. Opetuksen osalta määräys koskee opetusaineiston valmistamista, ei varsinaista opetusta.

Tämän osalta olisi hyvä huomioida EHDS-kehitys ja ottaa kehitys- ja innovaatiotoiminta mukaan käyttötarkoituksena sekä tarkastella tiedolla johtamista niin, että se Suomessa oikeasti voi toteutua.

Tietoturvavaatimuksissa on viitattu muun muassa tietoturvallisuuden auditointityökaluun viranomaisille (KATAKRI14) ja pilvipalveluiden turvallisuuden arviointikriteeristöön (PiTuKri15). PiTuKrin ja KATAKRI:n soveltaminen tulisi kirjata tarkemmin määräykseen. Fyysisen turvallisuuden arviointi tulee olla osa säädöksiä, koska mm. tiedon sijainti ja pääsynhallinta ovat ensiarvoisen tärkeitä esim. katastrofihallinnan osalta. Nykytilanteessa ei ole esteitä soveltuville fyysisille auditoinneille.

Tietoturvallisten käyttöympäristöjen vaatimustenmukaisuuden arviointeja voisivat toteuttaa Traficomin hyväksymien tietoturvallisuuden arviointilaitosten lisäksi akkreditoidut sertifiointielimet. Akkreditoitu sertifiointielin toimittaisi todistuksen tietoturvallisen käyttöympäristön vaatimustenmukaisuudesta Valviralle, joka lisäisi tiedon käyttöympäristöstä ylläpitämäänsä toisiokäyttöympäristöjen Toini-rekisteriin. Tässä on hyvä huomioida, että tietoturvallisen käyttöympäristön auditointi ei ole helppo tehtävä. Akkredioidun sertifiointielimen tuleekin ymmärtää paikalliset ja tarvittaessa myös kansainväliset vaatimukset. TEHDAS/EHDS-kehityksen vaikutus merkittävä, joten on syytä vaikuttaa siihen, että EU-tasoiset vaatimukset ovat linjassa paikallisten vaatimusten kanssa.

Tietolupaviranomaisen olisi mahdollista joustavasti päivittää vaatimuksia tietoturvallisille käyttöympäristöille, jolloin ne mahdollistaisivat uusimpien standardien ja menettelyjen huomioimisen käyttöympäristöjen arvioinnissa. Tärkeää tässä on huomioida riittävä suunnittelu, resurssit ja se että jo auditoidut ja Toini-listatut tietoturvalliset käyttöympäristöt tai käynnissä olevat tutkimukset eivät vaarannu liian nopeilla muutoksilla (lisäksi huomioidaan riittävä siirtymäaika). Erityisesti tietoturvaa tai sen hallintaa mahdollisesti heikentäviin muutoksiin tulee suhtautua riittävällä vakavuudella.

Vaikuttaa hyvältä, että Tietolupaviranomaisen määräyksessä listattaisiin soveltuvat kansainväliset standardit ja menettelyt, joita olisi mahdollista lukea hyväksi määräyksessä asetettujen vaatimusten täyttämiseksi. Lisäksi määräyksessä kuvattaisiin, mitä vaatimuksia ei ole mahdollista täyttää kansainvälisiä standardeja ja menettelyjä noudattamalla ja joiden täyttymistä tulisi näin ollen arvioida erikseen. Kansainvälisten standardien ja lisäarviointien yhdistelmän perusteella voitaisiin arvioida, täyttääkö tietoturvallinen käyttöympäristö toisiolaissa ja Tietolupaviranomaisen määräyksessä asetetut vaatimukset.

Ehdotuksella voi olla taloudellisia vaikutuksia yrityksille ja muille toimijoille, kuten tutkimusyhteisöille, jotka auditoivat tietoturvallisen käyttöympäristön toisiolain mukaisesti tai käsittelevät henkilötietoja käyttöympäristössä. Ehdotuksen mukaan useampien tietoturvallisten käyttöympäristöjen avaaminen lisää kilpailua ja mahdollistaa käyttöympäristöjen erikoistumisen tietynlaisten tietojen käsittelyyn.

Tulee kuitenkin tarkastella kriittisesti taloudellisia vaikutuksia. Lainsäädännön tai julkisen toiminnan ei pidä estää tai hankaloittaa entisestään tutkimusta tai yritysten toimintaa.

Tietoturvallisten käyttöympäristöjen erikoistuminen on erittäin suositeltava kehityssuunta.

Ehdotuksen mukaan useampien tietoturvallisten käyttöympäristöjen avaaminen voisi laskea käyttäjiltä perittäviä maksuja tietojen käsittelystä käyttöympäristössä. Valitettavasti tämä ei välttämättä suoraan laske käyttäjiltä perittäviä kustannuksia. Vaikutus voi olla jopa päinvastainen. Käyttäjiltä perittäviin maksuihin vaikuttavat ainakin tietoturvallisen käyttöympäristön kehittämiseen vaadittavien kustannusten kuten tarvittava osaaminen sekä useiden auditointien ja eri sertifiointien suorittamisen jyvittäminen, käytetty teknologia, datan sijainti, todellinen laskentateho ja -tila, tietoturvan taso (minimi vai parempi), sisältyvät palvelut ja tuki sekä kaupallisten ohjelmistojen ohjelmistolisenssit (yleensä kaupallisessa tai sponsoroidussa tutkimuksessa voidaan käyttää kaupallisten ohjelmistojen osalta ainoastaan kaupallisia lisenssejä).

Viranomaisten tulisi tällöin tarkistaa, että tietoluvan pyytäjällä on käytössään toisiolain mukainen tietoturvallinen käyttöympäristö, joka on lisätty Valviran ylläpitämään Toini-toisiokäyttöympäristöjen rekisteriin. Olisi erittäin hyvä, jos valvonta ja vastuu olisi yhdellä viranomaisella. Mutta onko niin, että tällä hetkellä vastuu on todellisuudessa rekisterin pitäjillä? Ja tämän kirjauksen myötä vastuu siirtyy Tietolupaviranomaiselle? Lauseesta ei suoraan käy ilmi ketä viranomaistahoja tällä tarkoitetaan, mutta olisi selkeämpää, jos arviointi toteutetaan yhden viranomaisen tai yhden rekisterinpitäjän datan ollessa kyseessä yhden rekisterinpitäjän toimesta.

Tällä hetkellä Tietolupaviranomaisen määräyksen ja kansainvälisten standardien suora vastaavuus on pientä, ja vastaavuutta tulisikin nostaa muuttamalla määräystä enemmän kansainvälisten standardien mukaiseksi, jotta ehdotettu ratkaisu olisi toteutettava. Tämä on siis kannatettavaa toimintaa, mutta on huomioitava jo olemassa olevat tietoturvalliset käyttöympäristöt ja organisaatioille aiheutuvat muutokset.

Tietolupaviranomaisen määräyksen uudistamis- ja selvitystyön, mukaan lukien vastaavuustaulukon laatimisen voidaan arvioida vaativan resursseja noin 640 tuntia ja arvioitu kustannus olisi noin 150 000 euroa. Mikä on budjettiarvio nykyisen tietoturvallisen käyttötilan vaatimasta muutoksesta sen omistavalle organisaatiolle?

Ehdotuksessa asetettaisiin sertifiointielimien tehtäväksi valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. Valvira

voisi antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta. Mutta miten valvotaan, että kaikilla sertifiointielimillä eri maissa on samanlaiset tavat auditoida tietoturvalliset käyttöympäristöt? Tämä osio on hieman epäselvä, ja vaikuttaa siltä, että millään suomalaisella organisaatiolla ei välttämättä olisi oikeutta valvoa ulkomaalaisia ympäristöjä, vaikka siellä olisi Suomen dataa tai Suomessa olevia ulkomaalaisen sertifiointielimen auditoimaa ympäristöä. Jos luotetaan pelkästään sertifikaattiin, tulee vaatimukset olla selvät ja raportit näiltä auditointitoimijoilta riittävät. Valvira voisi kyllä halutessaan vaatia esim. tarkistusraportteja tai haavoittuvuuden testausraportteja, ja varmistaa että vakavia puutteita ei ole, mutta tällöin prosessi SPE:n haltijan, Tietolupaviranomaisen ja Valviran välille tulisi luoda. Toinen lisäidea voisi olla, että olisi yleinen velvollisuus informoida Valviraa poikkeamista.

Tietoyhteiskuntavaikutusten osalta henkilötietojen suojaan kohdistuvat riskit voivat lisääntyä kansainvälisessä yhteistyössä erityisesti, jos suomalaisia datoja toimitetaan ulkomaille, sillä suomalaisilla viranomaisilla ei olisi mahdollisuutta valvoa kaikkia tietoturvallisia käyttöympäristöjä, ja ulkomaisten käyttöympäristöjen tietoturvan arviointi ja valvonta olisi akkreditoitujen sertifiointielimien vastuulla. Parempi olisi, jos dataa tuotaisiin ulkomailta suomalaisiin tietoturvallisiin käyttöympäristöihin entistä enemmän. EU:n tasolla tarvitaan Valviran listausta vastaava lista tietoturvallisista käyttöympäristöistä – ja mielellään niistä tieto siirtyisi jollakin tasolla kansallisille listoille, kuten Toiniin; ilman moninkertaisia maksuja. Ja minimissään tarvitaan edelleen lista Suomen osalta suomalaiselle datalle hyväksytyistä ympäristöistä.

Toteuttamisvaihtoehdoista vaihtoehto 1: Toisiolaissa asetettujen vaatimusten pitäminen ennallaan. Ehdotamme että pitäydyttäisiin tässä vaiheessa pääosin nykyisessä vaihtoehdossa yksi. Mutta lähdettäisiin kuitenkin ajan kanssa ja proaktiivisesti valmistautumaan vaihtoehdon 2 (Yhteiseurooppalaiset ratkaisut) tuloon. Jos määräystä lähdetään muuttamaan tässä vaiheessa, kun EHDS:n valmistelu on vielä kesken (kommentointi päättyi eilen osoitteessa: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-Digital-health-data-and-services-the-European-health-data-space_en), vaarana on useampi ja kenties merkittävä muutosprosessi tietoturvallisen käyttöympäristön määräykseen. Toisaalta Suomi on ollut vahvasti ja kärkipäässä luomassa suuntaviivoja terveysdatan tietoturvalliseen ja tietosuojan huomioivaan kehitykseen, joten EHDS:n vaatimusten huomiointi pitäisi olla mahdollista. Ajan kanssa kansainvälisen säännöstön noudattaminen kansalliset erityispiirteet huomioiden (mm. Suomessa on saatavissa todella paljon sosiaali- ja terveysdataa, joten EHDS-minimi Suomessa tuskin riittää, ja yleisesti ottaen digitalisaation aste ja tietoturva ovat Suomessa korkealla tasolla) lienee toimivin ratkaisu.

Vaihtoehto 2: Yhteiseurooppalaiset ratkaisut, kuten EHDS. Suomalaiset toimijat ovat olleet aktiivisesti mukana EU-tason kehittämisessä (mm. TEHDAS), mutta edelleen tulee seurata EU:n tasolla tapahtuvaa poliittista päätöksentekoa. Tärkeää on, että suomalainen lainsäädäntö vastaa vähintään EU:n lainsäädäntöä. Vaihtoehtona ehdotetulle ratkaisulle yksi olisikin odottaa yhteiseurooppalaisia ratkaisuja ja erityisesti yrittää vaikuttaa niihin. Ehdotuksen käsittely ja säädöksen mukaisten tietoturvallisten käsittely-ympäristöjen käyttöönotto tulee kuitenkin viemään aikaa. Olisikin tarkasteltava eksplisiittisesti Suomen valtion, yritysten, tutkimusten, potilaiden ja kansalaisten näkökulmasta eri vaihtoehtojen hyödyt ja haitat. Mistä vaihtoehdosta on eriten arvoa

kaikille osapuolille? Näkemyksemme perusteella tämä olisi yhdistelmä vaihtoehtoja 1 ja 2 eli vaikuttaminen ja valmistautuminen EHDS-kaltaiseen toimintaan sekä nykyisen toimintaympäristön turvaaminen.

Samoin kuin EHDS-suunnitelmassa, myös TEHDAS-raportissa ehdotetaan yhdeksi ratkaisuksi ongelmiin tietoturvallista käyttöympäristöä (SPE). Komissio voisi kuitenkin antaa tarkempia ohjeistuksia SPE-vaatimuksista ja -määritelmistä. Jäsenvaltiot voisivat hyväksyä tunnustamisperiaatteen rajat ylittävien SPE:en toiminnan ja toimintojen välillä. Tietolupaviranomaisen ja lainsäätäjän onkin hyvä seurata TEHDAS-hankkeen ehdotuksia ja tuloksia.

Lain 26 §:n 2 momenttia ehdotetaan muutettavaksi niin, että sekä arviointilaitoksen että sertifiointielimen myöntämä todistus olisi voimassa enintään kolme vuotta. Epäselvää on, miten muutos toteutetaan niiden ympäristöjen osalta, jotka ovat jo saaneet viiden vuoden voimassaolon? Vanhan lain aikana myönnettyjä ei tulisi muuttaa vaan pitää 5 vuotta; tämän lain voimaan tulon jälkeen sovellettaisiin uusilla ympäristöillä 3 vuoden sääntöä.

Eräs hyvä seikka EHDS-lakiehdotuksessa on mm. se, että se tuo esim. auditointivaatimusten osalta tunnisteellista tietoa sisältävät terveydenhuollon tietojärjestelmät (EHR) niiden ensisijaiskäytön osalta lähemmäs toisiokäytön pseudonyymiä (tai tulkinnasta riippuen) anonyymiä tietoa sisältäviä sertifioituja tietoturvallisia käyttötiloja, joihin pääsy on erittäin tiukasti kontrolloitu ja perustuu aina erilliseen lupaan.

Lain 27 §:ää ehdotetaan muutettavaksi niin, että myös sertifiointielimen on kehotettava palveluntarjoajaa korjaamaan puutteet, jos sertifiointielin toteaa, että käyttöympäristö ei ole täyttänyt tai ei enää täytä toisiolaissa säädettyjä vaatimuksia tai että todistusta ei muutoin olisi tullut myöntää. Sertifiointielin voisi myös peruuttaa todistuksen määräajaksi tai kokonaan taikka myöntää sen rajoitettuna, jollei palveluntarjoaja korjaa puutteellisuuksia sertifiointielimen asettamassa määräajassa.

Lain 28 §:ää ehdotetaan muutettavaksi niin, että myös sertifiointielimen olisi ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle tiedot kaikista myönnetyistä, muutetuista, täydennetyistä, määräajaksi tai kokonaan peruutetuista tai evätyistä todistuksista ja 26 §:n mukaisista tarkastusraporteista sekä 27 §:n mukaisista kehotuksista ja rajoituksista. Lisäksi sertifiointielimen olisi pyydettäessä annettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle kaikki tarvittavat lisätiedot.

Nämä 27 §:n ja 28 §:n muutokset ovat kannatettavia, ja ne tulisi kirjata lakiin. Toki tulisi ottaa myös huomioon miten velvoittavaa tämä on sertifiointielimille? Onko jotain sanktioita, jos velvoitetta ei täytetä lain 27 ja 28 §:ien osalta ja miten valvonta oikeasti toteutetaan – onko siihen resursseja?

Kannatettavaa on myös lain 28 §:n 1 momentin muutos niin, että käyttöympäristön olennaisista muutoksista olisi ilmoitettava joko tietoturvallisuuden arviointilaitokselle tai sertifiointielimelle, riippuen siitä, mikä organisaatio käyttöympäristön on arvioinut. Myös sertifiointielimen myöntämä todistus olisi uudistettava, jos käyttöympäristöön tehdään merkittäviä muutoksia tai 22 jos

käyttöympäristöä koskevia vähimmäisvaatimuksia on muutettu tavalla, jonka edellytyksenä on uusi arviointi.

Kaikkia osapuolia tulee kohdella samoin, kun lain 30 §:ään ehdotetaan lisättäväksi uusi 5 momentti, jonka mukaan Sosiaali- ja terveysalan lupa- ja valvontaviranomainen voisi antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta. Tietoturvallisten käyttöympäristöjen vaatimustenmukaisuuden valvonta on toisiolaissa asetettu Valviran tehtäväksi. Kuitenkin käytännössä kansallisen viranomaisen edellytykset valvoa muualla kuin Suomessa sijaitsevia käyttöympäristöjä ovat vähäiset. Tämän vuoksi Valviran olisi mahdollista antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta. Määräyksessä olisi mahdollista määrätä tarkemmin esimerkiksi siitä, miten muiden kuin Suomessa sijaitsevien käyttöympäristöjen valvonta tultaisiin toteuttamaan.

52 §:n muutos on hyvä. Ehdotuksen mukaan Tietolupaviranomainen voisi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta. Määräyksessä olisi mahdollista tarkemmin määrittää/viitata ohjeeseen, miten julkaistavien tietojen anonymisointi tulisi varmistaa luvansaajan toimesta. Tietolupaviranomaisen tulisi julkaista mahdollisesti päivittyvät ohjeet viimeistään ennen kuin laki tulee voimaan.

Esityksen toimeenpano edellyttää yhteistyötä Tietolupaviranomaisen ja Valviran välillä, jotta tietoturvallisten käyttöympäristöjen hyväksyntä päivitettyjen vaatimusten perusteella olisi sujuvaa. Toimeenpano- ja seurantasuunnitelma olisi mahdollista laatia toisiolain 8 §:n 4 momentin mukaisen korkean tason asiantuntijaryhmän toimesta. Toivoisimme asiantuntijaryhmään mukaan myös yritysedustusta ja tutkimuksen asiantuntijoita. EU:n tasolla tapahtuvien muutosten huomiointi on tässä keskeistä.

Kaikkien tietoturvallisten käyttöympäristöjen tulisi edelleen täyttää samat vaatimukset riippumatta niiden maantieteellisestä sijainnista ja siitä, toteuttaako vaatimustenmukaisuuden arvioinnin tietoturvallisuuden arviointilaitos vai akkreditoitu sertifiointielin. Kansainvälisillä standardeilla ja menettelyillä on tarkoitus varmistaa yhtä korkea tietoturvan taso kuin kansallisilla arviointikriteeristöillä. Tämä näkemys tulee varmistaa toimivan lainsäädännön avulla. Toivomme entistä enemmän tilanteita, missä ulkomaalaista dataa tuodaan Suomessa sijaitseviin tai Suomesta hallinnoitaviin tietoturvallisiin käyttöympäristöihin ja niiden analysointia yhdessä Suomen tietojen kanssa.

Kiitos!

Soini Erkki
ESiOR Oy - SPESiOR