Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain tietoturvallisia käyttöympäristöjä koskevia vaatimuksia niin, että vaatimukset mahdollistaisivat toisiolaissa tarkoitettujen tietojen luovuttamisen muihin kuin Suomessa sijaitseviin tietoturvallisiin käyttöympäristöihin. Muutoksen tarkoituksena on mahdollistaa suomalaisten rekisteritietojen käyttö kansainvälisessä tutkimusyhteistyössä, samalla kuitenkin varmistaen tietoturvan ja tietosuojan korkean tason.

Ehdotettu laki on tarkoitettu tulemaan voimaan 1. päivänä joulukuuta 2023.

_____

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Pääministeri Sanna Marinin hallituksen ohjelman 2019 tavoitteena on muun muassa edistää sosiaali- ja terveystietojen joustavaa ja laajamittaista hyödyntämistä, samalla kuitenkin rekisteröityjen tietosuojan korkeasta tasosta huolehtien.

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019, jäljempänä *toisiolaki*) on tullut voimaan 1.5.2019. Toisiolain tarkoituksena on luoda edellytykset sosiaali- ja terveydenhuollon palvelutoiminnassa syntyvien henkilötasoisten asiakastietojen sekä muiden terveyteen ja hyvinvointiin liittyvien henkilötietojen käytölle tilastointiin, tutkimukseen, kehittämis- ja innovaatiotoimintaan, opetukseen, tietojohtamiseen, viranomaisohjaukseen ja -valvontaan sekä viranomaisten suunnittelu- ja selvitystehtäviin. Laki mahdollistaa sosiaali- ja terveydenhuollon asiakas- ja potilastiedon hyödyntämisen muussa kuin kyseisen tiedon alkuperäisessä käyttötarkoituksessa.

Toisiolaissa asetetaan vaatimukset tietoturvallisille käyttöympäristöille, joilla tarkoitetaan toisiolain 3 §:n 11 kohdan mukaan teknisiä, organisatorisia ja fyysisiä tietojen käsittelyn toimintaympäristöjä, joiden tietoturvallisuus on varmistettu asianmukaisin hallinnollisin ja teknisin toimin. Tietoturvallisiin käyttöympäristöihin voidaan luovuttaa henkilötietoja toisiolain 3 §:n 8 kohdassa tarkoitetun tietoluvan nojalla.

Toisiolain 60 §:n 1 momentissa säädetään siirtymäajasta, jonka mukaan lain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sovelletaan 1 päivästä toukokuuta 2022. Siirtymäajan jälkeen toisiolaissa tarkoitettuja henkilötietoja voidaan luovuttaa tietoluvan nojalla käsiteltäväksi ainoastaan Sosiaali- ja terveysalan tietolupaviranomaisen (jäljempänä *Tietolupaviranomainen*) tietoturvallisessa käyttöympäristössä (Kapseli-käyttöympäristö[1]) tai muussa toisiolain mukaisesti auditoidussa tietoturvallisessa käyttöympäristössä. Aggregoitua tilastotietoa taas voidaan luovuttaa vapaasti tietopyynnön perusteella.

Vaatimus henkilötietojen käsittelystä toisiolain mukaisessa tietoturvallisessa käyttöympäristössä voi aiheuttaa haasteen erityisesti kansainväliselle tutkimusyhteistyölle, jossa haluttaisiin käyttää Suomesta saatavaa sosiaali- ja terveystietoa osana muista maista kerättävää tietoaineistoa. Lääketieteen tutkimus on luonteeltaan kansainvälistä ja tutkimusta tehdään hyvin usein kansainvälisissä konsortioissa. Toisiolaki edellyttää, että Suomesta saatava tietoaineisto luovutetaan ainoastaan toisiolain vaatimusten mukaisesti auditoituun tietoturvalliseen käyttöympäristöön. Toisiolaki ei ota kantaa, missä käyttöympäristö maantieteellisesti sijaitsee, mutta Tietolupaviranomaisen voimassa oleva määräys rajoittaa käyttöympäristöt EU/ETA-alueelle.[2] Osa tietoturvallisia käyttöympäristöjä koskevia toisiolain vaatimuksia voidaan täyttää vain kansallisen lainsäädännön ja kansallisten viranomaisten määräyksiä noudattamalla.[3] Käyttöympäristön tietoturvallisuus tulee osoittaa Liikenne- ja viestintäviraston (jäljempänä *Traficom*) hyväksymän tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Käytännössä tietoturvaa koskevia

[1] ks. https://findata.fi/kapseli/

[2] ks. https://findata.fi/palvelut-ja-ohjeet/maaraykset/

[3] Tulee ottaa kuitenkin huomioon, että kansalliset kriteeristöt, kuten VAHTI ja KATAKRI perustuvat yleisiin tietoturvaperiaatteisiin ja osittain kansainvälisiin standardeihin, kuten ISO/IEC 27001 –standardiin.

arviointeja tekevät Suomessa Traficomin Kyberturvallisuuskeskuksen erikseen hyväksymät arviointilaitokset.

Vaikka tietoturvallinen käyttöympäristö voi Tietolupaviranomaisen määräyksen mukaan sijaita EU/ETA-alueella, käytännössä kaikki toisiolain mukaiset käyttöympäristöt sijaitsevat tällä hetkellä Suomessa. Ulkomaisilla toimijoilla ei ole kattavaa tietoa toisiolain auditointivelvoitteesta, eikä kukaan ulkomainen toimija ole ryhtynyt auditoimaan omia järjestelmiään toisiolain perusteella. Tutkimusten siirtymistä suuressa määrin Tietolupaviranomaisen tai muiden suomalaisten toimijoiden käyttöympäristöihin ei pidetä todennäköisenä vaihtoehtona. Tämän seurauksena on mahdollista, että suomalaisen datan hyödyntäminen kansainvälisessä tutkimusyhteistyössä ja siten suomalaisten tutkijoiden mahdollisuus osallistua tutkimusyhteistyöhön vaikeutuu.

1.2 Valmistelu

Hallituksen esitys on valmisteltu virkamiestyönä sosiaali- ja terveysministeriössä. Hallituksen esityksen valmistelun tukena on toiminut kansainvälisten tietoluovutusten työryhmä (VN/16772/2021). Työryhmän tavoitteena oli selvittää ja arvioida kansainvälisiin luovutuksiin sovellettavia tietoturvaa koskevia toisiolain säännöksiä yhteistyössä tietoturva- ja tietosuoja-asiantuntijoiden, toisiolakia ohjaavien ja valvovien viranomaisten sekä muiden alan keskeisten sidosryhmien kanssa.

Hallituksen esityksen valmistelun tueksi sosiaali- ja terveysministeriö tilasi selvityksen kansainvälisistä standardeista ja menettelyistä, joiden perusteella olisi mahdollista täyttää toisiolaissa ja Tietolupaviranomaisen määräyksessä asetettuja vaatimuksia tietoturvallisille käyttöympäristöille.

Sosiaali- ja terveysministeriö järjesti hallituksen esitysluonnoksesta lausuntokierroksen 10.6.2022-29.7.2022. Täydennetään lausuntokierroksen perusteella.

Hallituksen esityksen valmisteluasiakirjat ovat julkisessa palvelussa osoitteessa https://stm.fi/hankkeet tunnuksella STM154:00/2021.

2 Nykytila ja sen arviointi

2.1 Yleistä

Toisiolain tavoitteena on mahdollistaa sosiaali- ja terveydenhuollon toiminnassa sekä sosiaali- ja terveysalan ohjaus-, valvonta-, tutkimus- ja tilastotarkoituksessa tallennettujen henkilötietojen tehokas ja tietoturvallinen käsittely sekä niiden yhdistäminen Kansaneläkelaitoksen, Väestörekisterikeskuksen, Tilastokeskuksen ja Eläketurvakeskuksen henkilötietoihin. Toisiolain yhtenä keskeisenä tarkoituksena on suojata kaikessa sosiaali- ja terveystietojen toissijaisessa käsittelyssä henkilötiedot siten, että kansalaisten luottamusta voidaan vahvistaa suhteessa heidän tietojensa käsittelyyn toissijaisessa käyttötarkoituksessa. Toisiolaki mahdollistaa aiempaa paremman tietoturvan sosiaali- ja terveydenhuollon arkaluonteisten henkilötietojen toissijaisessa käsittelyssä.

Tietoturvallinen käyttöympäristö on yksi toisiolain keskeisistä suojatoimista, jolla mahdollistetaan arkaluonteisten henkilötietojen käsittely turvallisessa ympäristössä ja turvataan yksilön henkilötietojen suojaa. Muita keskeisiä suojatoimia on kuvattu toisiolain 60 §:n muuttamista koskevassa hallituksen esityksessä (HE 96/2021 vp) sivuilla 29-30. Tietoturvallisella käyttöympäristöllä voidaan estää väärinkäytöksiä ja toteuttaa kyberturvallisuutta henkilötietojen käytössä

toisiotarkoitukseen. Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (jäljempänä *tietosuoja-asetus*) edellytetään riittäviä suojatoimia, kun käsitellään arkaluonteisia ja erityisiin henkilötietoryhmiin henkilötietoja.

Toisiolain 60 §:ssä asetettiin siirtymäaika, jonka jälkeen henkilötietoja voidaan luovuttaa vain tietoturvalliseen käyttöympäristöön käsiteltäviksi. Toisiolain valmistelun yhteydessä arvioitiin, että tietoturvallisten käyttöympäristöjen rakentaminen veisi hyväksymisen jälkeen noin kaksi vuotta ja siirtymäajaksi esitettiin tällöin 1.5.2021. Siirtymäaikaa siirrettiin vuodella eteenpäin lailla sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta (793/2021), jolloin siirtymäajaksi asetettiin 1.5.2022.

Hallituksen esityksen toisiolain 60 §:n muuttamisesta (HE 96/2021 vp) valmistelussa oltiin tunnistettu, että tutkijoille tarkoitettuihin tietojärjestelmiin ei oltu toteutettu kaikkia toisiolaissa edellytettyjä tietosuoja- ja turvavaatimuksia ja 1.5.2021 mennessä kenelläkään muulla toimijalla kuin Tietolupaviranomaisella ei ollut käytössään toisiolain 20 §:n edellyttämää tietoturvallista käyttöympäristöä, jonne tietoaineistoja voisi luovuttaa luvansaajan käsiteltäväksi. Siirtymäajan siirrolla haluttiin turvata terveydenhuollon tutkimuksen jatkuminen ja antaa lisäaikaa toimijoille auditoida omiin käyttötarpeisiinsa sopivia tietoturvallisia käyttöympäristöjä.

Toisiolaki mahdollistaa useampien tietoturvallisten käyttöympäristöjen perustamisen, kunhan ne täyttävät toisiolaissa asetetut tietoturvavaatimukset. Useampia tietoturvallisia käyttöympäristöjä tarvitaan, jotta tutkimuksen tekijät voivat valita tutkimukseensa sopivimman käyttöympäristön ja erilaiset käyttöympäristöt voivat erikoistua tiettyjen aineistojen käsittelyyn. Esimerkiksi yliopistosairaalat voivat tarvita tutkimukseen tietoaineistoa, jonka käsittelyyn tarvitaan erityisosaamista ja erityislaitteistoa. Esimerkkinä voi mainita terveydenhuollon kuvantamisaineistot (esimerkiksi röntgenkuvat, ultraäänikuvat ja EKG-tallenteet), jotka kuuluvat aineistona toisiolain soveltamisalan piiriin. Kuvantamisaineiston käsittely edellyttää laitteistoja ja ohjelmistoja, joita on vain terveydenhuollon toimijoilla. Kuvantamisaineiston käsittely edellyttää myös lähes aina sitä, että käsittelyn tekee tai siihen osallistuu kyseiseen alaan erikoistunut lääkäri.

Tämän hallituksen esityksen valmistumisen aikaan tietoturvallisia käyttöympäristöjä on auditoitu Tietolupaviranomaisen tietoturvallisen käyttöympäristön lisäksi kuusi; Helsingin ja Uudenmaan sairaanhoitopiirin kuntayhtymän HUS Acamedic, Istekki Oy:n T3 Tutkijan työtila, ESiOR Oy:n SPESiOR, Helsingin yliopiston FinnGen Sandbox, CSC Tieteen tietotekniikan keskus Oy:n SD Desktop ja Tilastokeskuksen Fiona-käyttöympäristö. Käyttöympäristöt rekisteröidään Sosiaali- ja terveysalan lupa- ja valvontaviraston (jäljempänä *Valvira*) toisiokäyttöympäristöjen rekisteriin.[4]

Nykyinen sääntely mahdollistaa suomalaisen rekisteritiedon käytön kansainvälisessä tutkimusyhteistyössä, jos tutkijat käyttävät tietojen käsittelyssä toisiolain mukaisesti auditoituja käyttöympäristöjä. Tutkijoiden on mahdollista etäyhteydellä saada pääsy joko Tietolupaviranomaisen tai muun suomalaisen toimijan auditoituun käyttöympäristöön ja käsitellä suomalaisia rekisteritietoja siellä. Jotta tutkija voisi joustavasti yhdistää ja analysoida rekisteritietoja suhteessa muihin tutkimuksessa käsiteltäviin tietoihin, tutkijan tai tutkimusryhmän tulisi siirtää tutkimuksen tietoaineisto kokonaisuudessaan suomalaiseen käyttöympäristöön. Kaikkien tutkimuksessa käsiteltävien tietoaineistojen tuominen ja käsittely toisiolain mukaisessa käyttöympäristössä on

[4] https://www.valvira.fi/terveydenhuolto/toisiolain-mukaiset-tietoturvalliset-kayttoymparistot/toisio-kayttoymparistojen-rekisteri

mahdollista nykyisen sääntelyn puitteissa. Suomalaisen rekisteritiedon käyttöä kansainvälisessä tutkimusyhteistyössä edistäisi se, että tutkijoiden käyttämiä käyttöympäristöjä auditoitaisiin tietoturvallisuuden arviointilaitosten toimesta toisiolain ja Tietolupaviranomaisen määräyksen vaatimusten mukaisesti EU- ja ETA-alueella. Ulkomaiset toimijat eivät kuitenkaan ole tähän mennessä ryhtyneet auditoimaan käyttöympäristöjään toisiolain mukaisesti.

Suomalaisten rekisteritietojen käyttöä kansainvälisessä tutkimusyhteistyössä voitaisiin edistää muuttamalla toisiolain tietoturvallisia käyttöympäristöjä koskevia vaatimuksia niin, että toisiolaissa tarkoitettuja tietoja olisi mahdollista luovuttaa myös Suomen ulkopuolella sijaitseviin käyttöympäristöihin.

2.2 Standardi, sertifiointi ja akkreditointi

Sertifioinneilla ja auditoinneilla valvotaan vaatimusten toteutumista ja luodaan luottamusta. Standardoinnin avulla voidaan kehittää toiminnan laatua, turvallisuutta ja läpinäkyvyyttä. Standardoinnin vaikuttavuuden kannalta keskeisessä asemassa ovat standardien kansainvälisyys, standardointiprosessin avoimuus, nopeus, ennustettavuus, joustavuus ja standardoinnin kohde. Standardoinnin vaikutusta on mahdollista tehostaa sertifioinnilla, joka kertoo siitä, että standardissa asetetut vaatimukset täyttyvät. Myös saatavuus vaikuttaa standardien käytön laajuuteen ja vaikuttavuuteen. Auditointien laadun varmistamisessa tärkeää on myös akkreditointi eli auditointeja tekevien tahojen pätevyyden toteaminen.[5]

Tietoturvallisuutta standardoidaan monilla eri toimialoilla sekä eurooppalaisella että kansainvälisellä tasolla. Virallisella standardoinnilla tarkoitetaan kansainvälisiä, eurooppalaisia ja kansallisia standardointiorganisaatioita, joiden jäsenyys on maakohtaista. Viralliset standardointiorganisaatiot, kuten kansainvälinen standardointielin ISO (International Organization for Standardization), ovat vakiintuneita ja tunnettuja. Esimerkkeinä standardeista voidaan mainita ISO/IEC 27001 ja CSA STAR. Kansainvälinen tietoturvallisuuteen liittyvä virallinen vaatimusstandardi on tietoturvan hallintajärjestelmästandardi ISO/IEC 27001, joka on kansainvälisesti yksi tunnetuimmista ja käytetyimmistä organisaation tietoturvallisuuden hallinnan standardeista. CSA STAR taas on pilvipalveluntarjoajille kehitetty kansainvälisesti tunnustettu sertifiointi, joka perustuu amerikkalaisen voittoa tavoittelemattoman organisaation Cloud Security Alliancen kehittämään Cloud Controls Matrixiin.[6]

Sertifiointi on määritelmän mukaan vaatimustenmukaisuuden arviointia. Vaatimustenmukaisuuden todistettavasti täyttäville toteutuksille voidaan myöntää hyväksyntä eli sertifikaatti, jonka myöntää puolueeton kolmas osapuoli. Sertifikaatteja voidaan myöntää esimerkiksi IT-palvelunhallintajärjestelmille, pilvipalvelun tarjoajille ja teknisille ratkaisuille. Sertifioinnin taustalla on usein asiakasvaatimus. Sertifikaatti on joissain tilanteissa myös kilpailutekijä, jonka avulla voidaan erottautua kilpailijoista riskittömämpänä vaihtoehtona.[7]

Sertifiointiorganisaatio arvioi, täyttääkö sertifioitava järjestelmä sertifiointivaatimuksissa esitetyt vaatimukset. Arvioinnin perusteella sertifiointiorganisaatio antaa todistuksen, jossa todetaan

[5] Traficom: Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin 2019, s. 3 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf.
[6] Traficom: Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin, s. 7-8.
[7] Traficom: Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin, s. 13.

johtamisjärjestelmän, tuotteen, prosessin tai henkilön täyttävän määrätyt vaatimukset. Sertifiointi on voimassa määritellyn ajan, minkä jälkeen voidaan tehdä uudelleensertifiointi.[8]

Akkreditointi tarkoittaa pätevyyden toteamista puolueettomasti ja riippumattomasti. Akkreditoidut sertifiointielimet ovat puolueettomia ja sertifioinnin kohteesta riippumattomia kolmannen osapuolen toimijoita, joilla tulee olla kansainvälisissä standardeissa määritelty pätevyys ja muut edellytykset toimintaansa varten.[9] Jokaisessa EU-maassa on EU-lainsäädännön mukaisesti kansallinen akkreditointielin ja Suomessa akkreditointielimenä toimii FINAS (Finnish Accreditation Service).

Akkreditointi viestii asiakkaille toiminnan pätevyydestä, uskottavuudesta ja luotettavuudesta sekä yhdenmukaistaa vaatimusten tulkintaa ja lisää yhteentoimivuutta. Lisäksi sillä edistetään Euroopan sisämarkkinoiden toimintaa varmistamalla, että akkreditoidun toimijan tuottamien palvelujen laatuun ja standardin tulkintaan voidaan luottaa kansainvälisesti. Näistä syistä sertifioinneissa tulisi käyttää vain akkreditoituja toimijoita.[10]

ISO 27001 –standardi

Kansainvälisen standardisoimisjärjestön tietoturvan hallintajärjestelmästandardi ISO 27001 on kansainvälinen virallinen vaatimusstandardi, jonka kohteena on tietoturvan johtamisjärjestelmä. ISO 27001 –standardiin kuuluu keskeisesti johdon sitoutuminen tietoturvallisuuteen, jatkuva parantaminen ja riskipohjainen tietoturvan hallintakeinojen valinta. Standardi on laadittu niin, että hallintajärjestelmään voidaan liittää muitakin tietoturvan hallintakeinoja (kontrolleja) kuin ISO 27001 liitteen mukaisia keinoja.

ISO 27001 –standardi on kansainvälisesti yleinen, luotettu ja vakiintunut standardi. Sertifioituja organisaatioita on yli 40 000 ja Suomessa ISO 27001 -sertifiointeja on voimassa noin 100. Akkreditoituja ISO 27001 sertifiointielimiä on lähes joka maassa. Sertifiointielimet voivat sertifioida myös muissa kuin niiden sijaintimaassa olevia tietoturvallisuuden johtamisjärjestelmiä.[11]

CSA STAR –standardi

Cloud Security Alliancen (CSA) Security, Trust, Assurance and Risk Registry (STAR) –standardi on suunnattu erityisesti pilvipalveluntarjoajille välineeksi osoittaa tarjoamiensa palveluiden vaatimustenmukaisuutta. Sertifioinnissa hyödynnetään ISO/IEC 27001 –tietoturvan hallintajärjestelmästandardin vaatimuksia yhdessä CSA:n Cloud Controls Matrix (CCM) -menetelmän kanssa. CSA STAR –standardi on yleistymässä oleva standardi, mutta ei kuitenkaan kovin tavallinen pienillä toimijoilla.

STAR-sertifiointi perustuu ISO/IEC 27001 -standardin ja pilvipalvelun valvontamatriisissa esitettyjen kriteerien saavuttamiseen, eli CCM:ssä esitettyjä hallintakeinoja voidaan pitää ISO 27001 -standardin mukaisina lisäkontrolleina. Näin ollen mikään CCM-arviointia koskeva sertifikaatti ei ole voimassa ilman siihen liittyvää ISO 27001 -sertifikaattia, jonka soveltamisala on vähintään yhtä suuri kuin STAR-sertifioinnin.[12]

---

[8] Ks. https://www.finas.fi/akkreditointi/Sivut/default.aspx

[9] Ks. https://www.finas.fi/akkreditointi/Akkreditointialueet/Sivut/Sertifiointiorganisaatiot.aspx

[10] Traficom: Luottamuksen lähteillä Näkökulmia tietoturvan standardointiin ja sertifiointiin, s. 14.

[11] Nixu Certification Oy selvitys huhtikuu 2022.

[12] Nixu Certification Oy selvitys huhtikuu 2022.

2.3 Toisiolaissa asetetut vaatimukset tietoturvallisille käyttöympäristöille

Toisiolain 18 §:ssä asetetaan yleisiä tietoturvavaatimuksia toisiokäytölle. Käsittelyn riittävä tietoturvallisuus on varmistettava riskienhallinnalla, pääsynhallinnalla, aktiivisella valvonnalla sekä noudattamalla tietoturvallisuuden ja tietosuojan toteutuksesta ja valvonnasta vastaavan viranomaisen määräyksiä ja ohjeita. Erityistä huomiota on kiinnitettävä käyttörajoitusten sekä salassapitovelvoitteen toteuttamiseen.

Toisiolain 20 – 30 §:ssä asetetaan vaatimukset tietoturvallisille käyttöympäristöille. Toisiolain 20 §:n 1 momentin mukaan Tietolupaviranomainen ylläpitää yksin tai yhdessä muiden viranomaisten kanssa tietoturvallista käyttöympäristöä, jossa voidaan varmistaa Tietolupaviranomaisen tai muun toisiolaissa tarkoitetun viranomaisen toisiolain nojalla luovuttamien tietojen tietoturvallinen, luvan mukainen käsittely.

Tietoturvallinen käyttöympäristö sisältää muun muassa päätelaitteet, palvelimet, työasemat, käyttöjärjestelmä- ja varusohjelmistot sekä hallinta- ja tietoturvakäytännöt, jotka eivät ole osa tietojärjestelmää tai tietojärjestelmäpalvelua. Tietoturvalliseen käyttöympäristöön sisältyvät myös tietoturvaprosessien hallinto ja johtamisjärjestelmä kattaen henkilöstö-, laitteisto-, tietoliikenne-, käyttö- ja ohjelmistoturvallisuuden sekä fyysisen turvallisuuden (HE 159/2017 vp, s. 93).

Toisiolain 20 §:n mukaan henkilötiedot luovutetaan ensisijaisesti Tietolupaviranomaisen tietoturvalliseen käyttöympäristöön. 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. Tietolupaviranomainen tai muu toisiolaissa tarkoitettu viranomainen saa tällöin luovuttaa tiedot hakijalle vain, jos käyttöympäristö täyttää toisiolain 20 §:n 2 momentissa ja 21–29 §:ssä säädetyt edellytykset.

Toisiolain 21 §:n 1 momentin mukaan tietoturvallisen käyttöympäristön käyttäjät on tunnistettava luotettavasti sekä todennettava. Toisiolain 22 §:ssä säädetään tietoturvallisen käyttöympäristön käyttäjien käyttöoikeuksista, ja 22 §:n 3 momentin mukaan Tietolupaviranomainen antaa määräykset niistä perusteista, joiden mukaisesti palveluntarjoajan on määriteltävä luvansaajan käyttöoikeudet asiakastietoihin.

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).

Toisiolain 24 §:n 1 momentin mukaan tietoturvallisen käyttöympäristön on täytettävä tietoturvaa ja tiedonsiirron yhteentoimivuutta koskevat vaatimukset, jotka perustuvat viranomaisten antamiin määräyksiin, suosituksiin ja näiden osoittamiin, tietoturvalliseen käyttöympäristöön soveltuviin standardeihin. Toisiolain 24 §:n 2 momentin mukaan Tietolupaviranomainen antaa

tarkemmat määräykset muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista. Vaatimuksissa on edellytettävä vastaavaa tietoturvan tasoa kuin Tietolupaviranomaisen omassa käyttöympäristössä vaaditaan.

Tietoturvalliset käyttöympäristöt tulee auditoida toisiolain tietoturvaa koskevien vaatimusten mukaisesti tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaisten arviointilaitosten toimesta. Toisiolain 25 §:n mukaan käyttöympäristön tietoturvallisuus on osoitettava 26 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Tietolupaviranomainen voi antaa tarkempia määräyksiä tietoturvallisuuden osoittamisessa noudatettavista menettelyistä.

Toisiolain 26 §:ssä asetetaan vaatimukset käyttöympäristöjen tietoturvallisuuden arvioinnille. Toisiolain 26 §:n 1 momentin mukaan tietoturvallisuuden arviointilaitos arvioi toisiolain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Arviointiperusteina on käytettävä Tietolupaviranomaisen määräyksiä turvalliselle käyttöympäristölle asetettavista vaatimuksista.

Toisiolain 26 §:n 2 momentin mukaan, jos käyttöympäristö täyttää toisiolain mukaiset tietoturvallisuusvaatimukset, tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan arvioinnista palveluntarjoajalle todistus sekä siihen liittyvä tarkastusraportti. Jos arviointi tai uudelleenarviointi koskee vain käyttöympäristön osaa, arviointilaitoksen antamaan todistukseen on selkeästi merkittävä, mikä osa käyttöympäristöstä on arvioitu.

Toisiolain 26 §:n 3 momentin mukaan arviointilaitoksen myöntämä todistus on voimassa enintään viisi vuotta. Tietoturvallisuuden arviointilaitos voi vaatia palveluntarjoajalta kaikki arvioinnin sekä todistuksen laatimisen ja ylläpitämisen edellytyksenä olevat tiedot. Todistuksen antamiseen sovelletaan muutoin tietoturvallisuuden arviointilaitoksista annetun lain 9 §:n 3 momenttia.

Toisiolain 27 §:ssä säädetään edellytyksistä, joilla arviointilaitos voi peruuttaa myöntämänsä todistuksen. Toisiolain 28 §:n mukaan tietoturvallisuuden arviointilaitoksen on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle tiedot kaikista myönnetyistä, muutetuista, täydennetyistä, määräajaksi tai kokonaan peruutetuista tai evätyistä todistuksista sekä 27 §:n mukaisista kehotuksista ja rajoituksista. Lisäksi tietoturvallisuuden arviointilaitoksen on pyydettäessä annettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle kaikki tarvittavat lisätiedot.

Toisiolain 29 §:n 1 momentin mukaan palveluntarjoajan on seurattava toisiolain muutoksia ja tehtävä käyttöympäristöön muutosten edellytyksenä olevat korjaukset. 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.

Toisiolain 30 §:ssä säädetään Sosiaali- ja terveysalan lupa- ja valvontaviraston tehtävästä valvoa ja edistää sitä, että tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. Sosiaali- ja terveysalan lupa- ja valvontavirasto ylläpitää julkista rekisteriä sille ilmoitetuista, vaatimukset täyttävistä käyttöympäristöistä. Sosiaali- ja terveysalan lupa- ja valvontavirastolla on oikeus tehdä valvonnan edellytyksenä olevia tarkastuksia.

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. 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.

2.4 Tietolupaviranomaisen määräyksessä asetetut vaatimukset tietoturvallisille käyttöympäristöille

Toisiolain 24 §:n 2 momentin mukaan Tietolupaviranomainen antaa tarkemmat määräykset muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista. Ensimmäinen tietoturvallisia käyttöympäristöjä koskeva määräys julkaistiin 5.10.2020. Tietolupaviranomainen julkaisi päivitetyn version määräyksestä 19.1.2022.[13]

Määräystä sovelletaan 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.

Määräyksen mukaisten vaatimusten toteuttaminen on 1.5.2022 lähtien edellytyksenä sille, että tietoja voidaan luovuttaa luvansaajan käsiteltäväksi toissijaisiin tarkoituksiin muussa kuin Tietolupaviranomaisen tietoturvallisessa käyttöympäristössä toisiolain 20 §:n 3 momentin mukaisesti.

Mikäli tietolupahakemuksessa pyydetään luovuttamaan tietoaineistoja käsiteltäviksi muussa kuin Tietolupaviranomaisen tietoturvallisessa käyttöympäristössä, hakemuksessa on toisiolain 20 §:n 3 momentin mukaan erikseen perusteltava syyt, joiden vuoksi tämä on välttämätöntä. Tietolupaviranomainen tai muu toisiolaissa tarkoitettu viranomainen saa tällöin luovuttaa tiedot hakijalle vain, jos käyttöympäristö täyttää 20 § 2 momentissa ja 21–29 §:ssä säädetyt edellytykset. Jos toisiolain 44 §:n 3 momentissa tarkoitettu yksittäinen rekisterinpitäjä on tehnyt omiin rekistereihinsä sisältyviä tietoja koskevan tietolupapäätöksen, sen tulee luovuttaa tietoaineisto luvansaajan käsiteltäväksi aina toisiolain 20 §:ssä tarkoitettuun tietoturvalliseen käyttöympäristöön.

Määräyksen vaatimusten toteutuminen osoitetaan toisiolain 26 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Todistus myönnetään tarkastusraportin havaintojen perusteella. Jotta todistus voidaan myöntää, tarkastusraportti ei saa sisältää yhtään määräyksen mukaan vakavaksi poikkeamaksi luokiteltavaa havaintoa.

Poikkeamien luokittelu tapahtuu osana tietoturvallisuuden arviointilaitoksen suorittamaa arviointia niin, että poikkeamat on luokiteltu vakavien, keskitason ja lievien poikkeamien perusteella. Mikäli tarkastusraportissa todetaan yksi tai useampi määräyksen mukaan keskitason poikkeamaksi luokiteltava havainto, tulee tarkastusraportin sisältää myös arviointilaitoksen hyväksymä korjaussuunnitelma, jossa on asetettu myös määräaika korjaussuunnitelman mukaisen

[13] https://findata.fi/palvelut-ja-ohjeet/maaraykset/

uudelleenarvioinnin valmistumiselle. Uudelleenarviointi on suoritettava hyväksytysti viimeistään 6 kuukauden kuluessa tarkastusraportin valmistumisesta. Muiden kuin vakavien poikkeamien ei arvioida yhdessä muodostavan vakavaksi luokiteltavaa poikkeamaa.

Arvioinnin toteuttava ja todistuksen myöntävä tietoturvallisuuden arviointilaitos arvioi soveltuvatko palveluntarjoajan tietoturvallista käyttöympäristöä koskevat, voimassa olevat tietoturvallisuuteen liittyvät todistukset määräyksessä esitettyjen vaatimustenmukaisuuden osoittamiseen. Arvioitavan kohteen osat, joita olemassa oleva todistus ei kata, tulee erikseen arvioida. Arviointilaitos tarkastaa palveluntarjoajan voimassa olevan todistuksen voimassaoloajan ja asettaa tarvittaessa rajoituksen tämän määräyksen perusteella myönnettävän todistuksen voimassaoloajalle.

Tietoturvavaatimuksissa on viitattu muun muassa tietoturvallisuuden auditointityökaluun viranomaisille (KATAKRI[14]) ja pilvipalveluiden turvallisuuden arviointikriteeristöön (PiTuKri[15]). Arviointilaitoksella on mahdollisuus perustaa arviointi PiTuKrin vaatimuksiin KATAKRI:n sijaan kohdissa, joissa se arvioitavan kohteen osalta on tarkoituksenmukaista. Tietoturvavaatimuksissa viitataan myös tietosuoja-asetukseen ja Euroopan parlamentin ja neuvoston asetukseen (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta. Lisäksi vaatimuksissa mainitaan ISO/IEC 27001 –standardi.

Tietoturvallisella käyttöympäristöllä on oltava nimetty palveluntarjoaja, joka vastaa siitä, että tietoturvallinen käyttöympäristö ja sen tuottamiseen osallistuvat osapuolet noudattavat määräyksessä asetettuja vaatimuksia. Palveluntarjoaja voi käyttää alihankkijoita esimerkiksi tietoteknisten palveluiden tuottamiseksi, mutta palveluntarjoaja vastaa aina tietoturvallisen käyttöympäristön vaatimustenmukaisuudesta. Käytännössä palveluntarjoajan ja käytettävän alihankkijan välillä on oltava sitova sopimussuhde.

Palveluntarjoajan on myös tunnistettava mahdollinen henkilötietojen kasautumisvaikutus ja huomioitava tämä tarjoamansa käyttöympäristön suojauksessa. Kasautumisvaikutus voi syntyä esimerkiksi tilanteissa, joissa käyttöympäristössä on tarkoitus säilyttää useita henkilötietoaineistoja ja/tai aineistojen koot muodostuvat suuriksi. Valvira ylläpitää julkista rekisteriä sille ilmoitetuista vaatimukset täyttävistä käyttöympäristöistä.

Tietolupaviranomaisen määräyksessä asetetaan tekniset vaatimukset tunnistautumiselle, käyttäjien ja käyttöoikeuksien hallinnalle, ympäristön suojaamiselle, lokitukselle, ympäristön hallinnalle ja valvonnalle ja aineistojen poistolle käyttöympäristöstä, sekä vaatimukset toimijan luotettavuudelle, tietosuojalle, toimitiloille ja henkilöstölle.

---

[14] Katakri on viranomaisten auditointityökalu, jota viranomainen voi käyttää arvioidessaan kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Katakria voidaan käyttää auditointityökaluna arvioitaessa yrityksen turvallisuusjärjestelyjä yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Sitä voidaan käyttää myös apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä. Ks. https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille.

[15] Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. Kriteeristö on tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin. Kriteeristö on laadittu Suomen kansallisten tarpeiden näkökulmasta. Ks. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri.

3 Tavoitteet

Hallituksen esityksen tavoitteena on mahdollistaa suomalaisten rekisteritietojen käyttö kansainvälisessä tutkimusyhteistyössä, samalla kuitenkin varmistaen tietoturvan ja tietosuojan korkean tason. Esityksessä ehdotetaan muutettavaksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain tietoturvallisia käyttöympäristöjä koskevia vaatimuksia niin, että vaatimukset mahdollistaisivat toisiolaissa tarkoitettujen tietojen luovuttamisen muihin kuin Suomessa sijaitseviin tietoturvallisiin käyttöympäristöihin.

Tietoturvallisten käyttöympäristöjen tulee täyttää tietosuojan ja tietoturvan korkean tason varmistamiseksi toisiolaissa ja Tietolupaviranomaisen määräyksessä asetetut tietoturvaa koskevat vaatimukset. Korkean tietoturvan ja tietosuojan varmistaminen on erityisen tärkeää, kun käsitellään arkaluonteisia ja erityisiin henkilötietoryhmiin kuuluvia tietoja.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Hallituksen esityksessä ehdotetaan muutettavaksi toisiolain tietoturvallisia käyttöympäristöille asetettuja vaatimuksia niin, että toisiolain ja Tietolupaviranomaisen asettamia vaatimuksia olisi mahdollista täyttää myös Tietolupaviranomaisen määräyksessä määriteltyjä kansainvälisiä standardeja ja menettelyjä noudattamalla. Lisäksi 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 rekisteriin.

Toisiolaissa säädettäisiin tietoturvallisille käyttöympäristöille asetettavista vaatimuksista ainoastaan yleisellä tasolla ja tarkemmat määräykset vaatimuksista antaisi Tietolupaviranomainen toisiolain 24 §:n mukaisesti. Tietolupaviranomaisen määräystä kehitettäisiin niin, että siinä asetettuja vaatimuksia olisi mahdollista täyttää kansallisten vaatimusten lisäksi myös kansainvälisiä standardeja ja menettelyjä noudattamalla. Tietolupaviranomaisen olisi mahdollista joustavasti päivittää vaatimuksia tietoturvallisille käyttöympäristöille, jolloin ne mahdollistaisivat uusimpien standardien ja menettelyjen huomioimisen käyttöympäristöjen arvioinnissa.

Tietolupaviranomainen voisi määräyksessään määritellä ne akkreditoidut sertifiointielimet, joilla katsotaan olevan riittävät edellytykset arvioida tietoturvallisten käyttöympäristöjen vaatimustenmukaisuutta toisiolain ja Tietolupaviranomaisen määräyksessä asetettujen vaatimusten perusteella.

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.

Ehdotetut muutokset ovat perusteltuja, sillä kansainvälisten standardien ja lisäarviointien yhdistelmä varmistaisi tietoturvan ja tietosuojan korkean tason, jota edellytetään tietojen luovuttamiseksi tietoturvalliseen käyttöympäristöön. Tietolupaviranomainen ja muut toisiolaissa tarkoi-

tetut viranomaiset voisivat luovuttaa tietoaineistoja tietopyynnön perusteella sekä tietoturvallisuuden arviointilaitosten auditoimiin käyttöympäristöihin, että akkreditoitujen sertifiointielinten auditoimiin käyttöympäristöihin, jotka olisi merkitty Valviran toisiokäyttöympäristöjen rekisteriin.

4.2 Pääasialliset vaikutukset

4.2.1 Taloudelliset vaikutukset

Ehdotuksella voi olla taloudellisia vaikutuksia yrityksille ja muille toimijoille, kuten tutkimusyhteisöille, jotka auditoivat tietoturvallisen käyttöympäristön toisiolain mukaisesti tai käsittelevät henkilötietoja käyttöympäristössä. Useampien tietoturvallisten käyttöympäristöjen avaaminen lisää kilpailua ja mahdollistaa käyttöympäristöjen erikoistumisen tietynlaisten tietojen käsittelyyn. Lisäksi useampien käyttöympäristöjen avaaminen voisi laskea käyttäjiltä perittäviä maksuja tietojen käsittelystä käyttöympäristössä.

Jo nykyisessä sääntelyssä edellytetään tietoturvallisten käyttöympäristöjen käyttöä silloin, kun luovutetut tiedot ovat henkilötietoja. Ehdotus ainoastaan mahdollistaisi tietoturvallisten käyttöympäristöjen vaatimusten toteuttamisen kansainvälisillä standardeilla ja menettelyillä, ja lisäksi vaatimustenmukaisuus olisi mahdollista todistaa akkreditoidun sertifiointielimen toteuttamalla arvioinnilla.

Tietoturvallisuusvaatimusten toteuttaminen lisää yritysten ja muiden toimijoiden kustannuksia, jos ne toteuttavat toisiolain ja Tietolupaviranomaisen määräyksen mukaisen käyttöympäristön. Toisaalta ehdotuksen tarkoituksena on, että vaatimusten toteuttamisessa olisi mahdollista käyttää yleisesti käytössä olevia kansainvälisiä standardeja ja menettelyjä, joiden käyttöönotto ei aiheuttaisi kohtuuttomia kustannuksia yrityksille tai muille toimijoille. Voidaan myös huomioida, että henkilötietoja käsittelevien toimijoiden tulisi toteuttaa asianmukaisia tietoturvatoimia toiminnassaan jo EU:n tietosuojasääntelyn ja niitä koskevan kansallisen sääntelyn nojalla.

Sertifikaattien hankkiminen, joilla todistetaan kansainvälisen standardin noudattaminen, voi olla helpompaa suuremmille toimijoille kuin keskisuurille ja pienille toimijoille. Sertifioinnin kustannukset voivat olla varsinkin pienemmille toimijoille suuret.[16] Jo nykyiset säännökset aiheuttavat joitain kustannuksia toimijoille, jos ne haluavat auditoida tietoturvallisen käyttöympäristön toisiolain mukaisesti. Kansainvälisten standardien noudattaminen voi tuoda toimijalle kilpailuetua ja maineen luotettavana toimijana, jonka tietosuoja- ja tietoturva-asiat ovat kunnossa.

Suomalaisten toimijoiden olisi edelleen mahdollista todistaa tietoturvallisen käyttöympäristön vaatimustenmukaisuus tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Toisaalta toimija voisi myös päättää käyttää kansainvälisiä standardeja ja sertifiointeja, ja vaatimustenmukaisuus olisi mahdollista todistaa myös akkreditoidun sertifiointielimen antamalla todistuksella. Ehdotus lisäisi joustavuutta tietoturvallisten käyttöympäristöjen vaatimustenmukaisuuden todistamiseen.

[16] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla: Työryhmän loppuraportti 2021, s. 55.

4.2.2 Vaikutukset viranomaisten toimintaan

Ehdotuksella olisi vaikutuksia Tietolupaviranomaisen, toisiolain 6 §:ssä tarkoitettujen viranomaisten sekä Valviran toimintaan.

Tietolupaviranomaisen ja toisiolain 6 §:ssä tarkoitettujen viranomaisten toimintaan ehdotus tulisi vaikuttamaan niin, että niitä voitaisiin pyytää luovuttamaan toisiolaissa tarkoitettuja tietoja muihin kuin Suomessa sijaitseviin tietoturvallisiin käyttöympäristöihin. Viranomaisten tulisi tällöin tarkistaa, että tietoluvan pyytäjällä on käytössään toisiolain mukainen tietoturvallinen käyttöympäristö, joka on lisätty Valviran ylläpitämään toisiokäyttöympäristöjen rekisteriin.

Ehdotuksen toteuttaminen edellyttäisi Tietolupaviranomaisen määräyksen uudistamista ja tähän liittyvää selvitystyötä liittyen kansainvälisten standardien ja määräyksessä asetettujen vaatimusten vastaavuudesta. Kansainvälisten standardien ja menettelyjen vastaavuudesta määräyksessä asetettuihin nähden tulisi laatia vastaavuustaulukko, jonka avulla olisi mahdollista määrittää, mitkä määräyksessä asetetut vaatimukset olisi mahdollista täyttää kansainvälisiä standardeja tai menettelyjä noudattamalla. Lisäksi selvitystyössä tulisi arvioida, miltä osin Tietolupaviranomaisen määräyksessä asetettuja vaatimuksia ei ole mahdollista täyttää kansainvälisillä standardeilla ja kuinka monta vaatimusta tulisi arvioida lisäarvioinnilla. 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.[17]

Tietolupaviranomaisen määräyksen uudistamis- ja selvitystyön, mukaan lukien vastaavuustaulukon laatimisen voidaan arvioida vaativan resursseja noin 640 tuntia ja arvioitu kustannus olisi noin 150 000 euroa.[18]

Valviran toimintaan ehdotus tulisi vaikuttamaan niin, että myös muut kuin tietoturvallisuuden arviointilaitosten arvioimat tietoturvalliset käyttöympäristöt olisi mahdollista hyväksyä toisiokäyttöympäristöjen rekisteriin akkreditoidun sertifiointielimen antaman todistuksen perusteella. Lisäksi Valvira vastaanottaisi todistusten lisäksi tarkastusraportteja arvioinneista.

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.

Tämän vuoksi 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.

Ehdotetut muutokset liittyvät Valviran nykyisiin tehtäviin ja eivät näin ollen aiheuttaisi Valviralle merkittäviä lisätehtäviä tai kustannuksia.

[17] Nixu Certification Oy:n arvio huhtikuu 2022.
[18] Nixu Certification Oy:n arvio huhtikuu 2022.

4.2.3 Muut yhteiskunnalliset vaikutukset

4.2.3.1 Vaikutukset kansalaisten asemaan ja toimintaan yhteiskunnassa

Ehdotuksella olisi vaikutuksia henkilöiden yksityiselämän suojaan ja henkilötietojen suojaan. Toisiolain hallituksen esityksessä HE 159/2017 vp on arvioitu toisiokäytöstä aiheutuvia vaikutuksia kansalaisten asemaan. Toisiolain tarkoituksena on parantaa rekisteröityjen henkilötietojen suojaa asettamalla tietoturvavaatimuksia henkilötietojen käsittelylle toisiotarkoituksessa. Henkilötietoja voidaan käsitellä ainoastaan tietoturvallisessa käyttöympäristössä, jossa tietoturva on varmistettu asianmukaisin hallinnollisin ja teknisin toimin sekä tietojärjestelmien asianmukaisin standardein.

Ehdotuksessa ei muutettaisi tätä perusperiaatetta, vaan henkilötietoja olisi edelleen mahdollista luovuttaa ainoastaan toisiolain ja Tietolupaviranomaisen vaatimukset täyttäviin käyttöympäristöihin. Ainoastaan keinot, joilla vaatimustenmukaisuus olisi mahdollista todistaa, muuttuisivat ja monipuolistuisivat. Lähtökohtana on, että kansainvälisillä standardeilla ja menettelyillä osoitettu vaatimustenmukaisuus takaisi vähintään yhtä hyvän tietoturvan tason kuin nykyiset kansalliset vaatimukset.

4.2.3.2 Vaikutukset tutkimus- ja kehittämistoimintaan

Ehdotuksella voisi olla vaikutuksia tutkimus- ja kehittämistoimintaan. Myös nykyinen toisiolaki mahdollistaa kansainvälisen tutkimusyhteistyön etäkäyttöyhteydellä, mutta ehdotettu ratkaisu saattaisi lisätä kansainvälisen tutkimusyhteistyön edellytyksiä helpottamalla tietoturvallisten käyttöympäristöjen perustamista myös Suomen ulkopuolelle. Ehdotus saattaisi myös edistää suomalaisen rekisteridatan käyttöä kansainvälisessä tutkimusyhteistyössä ja parantaa suomalaisten tutkijoiden mahdollisuuksia osallistua tutkimusyhteistyöhön.

4.2.3.3 Sosiaali- ja terveysvaikutukset

Ehdotuksella ei olisi suoria vaikutuksia ihmisten terveyteen ja hyvinvointiin. Ehdotus voisi kuitenkin pidemmällä aikavälillä tuottaa etuja suomalaisten sosiaali- ja terveydenhuollon asiakkaiden hoidossa, sillä ehdotuksen mahdollistama kansainvälinen tutkimusyhteistyö suomalaisilla rekisteritiedoilla voisi mahdollistaa uusien hoitomuotojen ja –keinojen kehittämisen suomalaisten potilaiden tarpeisiin. Nykyisessä sääntelyssä riskinä on, että uusimpia tutkimustuloksia ja hoitomuotoja ei kehitetä suomalaisten tarpeiden mukaisesti ja suomalaisten tutkijoiden on vaikeaa toteuttaa tutkimusta osana kansainvälistä tutkimusyhteistyötä.

4.2.3.4 Tietoyhteiskuntavaikutukset

Ehdotuksella olisi vaikutuksia henkilötietojen suojaan ja tietoturvaan. Toisiolain hallituksen esityksessä HE 159/2017 vp on arvioitu laista aiheutuvia vaikutuksia henkilötietojen suojaan. Ehdotus ei muuttaisi toisiolaissa asetettuja henkilötietojen käsittelyn perusteita tai tarkoituksia, tai muita henkilötietojen käsittelyn edellytyksiä, mutta se mahdollistaisi aiempaa useamman tietoturvallisen käyttöympäristön perustamisen ja tietojen luovuttamisen myös Suomen ulkopuolella sijaitsevaan tietoturvalliseen käyttöympäristöön. Henkilötietojen suojaan kohdistuvat riskit voisivat lisääntyä, sillä suomalaisilla viranomaisilla ei olisi mahdollisuutta valvoa kaikkia tietoturvallisia käyttöympäristöjä, ja ulkomaisten käyttöympäristöjen tietoturvan arviointi ja valvonta olisi akkreditoitujen sertifiointielimien vastuulla.

Näin ollen tässä esityksessä on tarpeen arvioida suunniteltujen muutosten vaikutukset henkilötietojen suojalle. Toisiolaissa tarkoitettujen henkilötietojen käsittely perustuu tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohtaan ja erityisten henkilötietoryhmien osalta käsittely perustuu käyttötarkoituksesta riippuen 9 artiklan 2 kohdan g, h tai j alakohtaan. Toisiolaissa on tarkkaan määritelty ne käsittelytarkoitukset, joihin tietoja saa toisiotarkoituksessa käsitellä. Tietolupaviranomainen tai muu toisiolaissa tarkoitettu viranomainen tarkistaa tietolupapyynnön vastaanottaessaan, että se täyttää toisiolain ja tietosuojalainsäädännön vaatimukset. Ehdotus ei muuta näitä vaatimuksia, vaan henkilötietojen käsittely perustuu edelleen toisiolaissa määriteltyihin käyttötarkoituksiin ja toisiolaissa tarkoitetun viranomaisen myöntämään tietolupaan.

Toisiolaissa tarkoitetut henkilötiedot ovat arkaluonteisia ja erityisiin henkilötietoryhmiin kuuluvia tietoja, joiden vuoksi niiden suojaamiselle on tietosuojalainsäädännössä asetettuja erityisiä vaatimuksia. Toisiolaissa on tunnistettu sosiaali- ja terveystietojen erityinen arkaluonteisuus, minkä vuoksi henkilötietoja on mahdollista luovuttaa ainoastaan toisiolain vaatimukset täyttäviin käyttöympäristöihin. Toisiolaki sisältää myös muita suojatoimia, joilla henkilötietoja suojataan ja näitä suojatoimia on kuvattu toisiolain muuttamista koskevassa hallituksen esityksessä (HE 96/2021 vp) sivuilla 29-30.

Toisiolaissa säädetään asianmukaisista ja erityisistä suojatoimista rekisteröityjen oikeuksien ja vapauksien turvaamiseksi. Tässä ehdotuksessa ei muutettaisi toisiolaissa säädettyjä suojatoimia henkilötietojen käsittelylle. Henkilötietojen käsittelyä suojaisi edelleen tietoturvallisen käyttöympäristön käyttö. Kaikkia tietoturvallisia käyttöympäristöjä koskisivat samat toisiolaissa ja Tietolupaviranomaisen määräyksessä asetetut vaatimukset sijainnista riippumatta. Ainoastaan vaatimustenmukaisuuden osoittamisen tapa muuttuisi niin, että vaatimustenmukaisuus olisi mahdollista todistaa tietoturvallisuuden arviointilaitoksen auditoinnin lisäksi myös akkreditoidun sertifiointielimen antaman todistuksen perusteella ja kansainvälisiä standardeja tai menettelyjä noudattamalla.

Ehdotuksessa mahdollistettaisiin tietojen luovuttaminen aiempaa sujuvammin Suomen ulkopuolella sijaitsevaan käyttöympäristöön. Myös nykyinen toisiolaki mahdollistaa käyttöympäristön perustamisen Suomen ulkopuolelle ja Tietolupaviranomaisen määräyksen mukaan käyttöympäristön tulee sijaita EU/ETA-alueella. Ehdotuksessa ei rajoitettaisi tietoturvallisten käyttöympäristöjen sijoittautumispaikkaa. Näin ollen olisi mahdollista, että käyttöympäristö olisi mahdollista perustaa myös EU:n ulkopuolelle. Henkilötietojen siirroista kolmansiin maihin säädetään tietosuoja-asetuksen V luvussa. Jos henkilötietoja tultaisiin siirtämään kolmansiin maihin, tulisi siirron täyttää tietosuoja-asetuksen V luvussa asetetut vaatimukset.

Henkilötietojen käsittelytoimet olisivat tarpeellisia, jotta kansainvälinen tutkimusyhteistyö suomalaisilla rekisteritiedoilla olisi mahdollista ja tietoja olisi mahdollista siirtää muihin kuin Suomessa sijaitseviin käyttöympäristöihin. Käsittelytoimien oikeasuhtaisuutta perustelisi se, että henkilötietoja suojataan toisiolaissa usein eri tavoin ja henkilötietoja olisi mahdollista käsitellä edelleen ainoastaan auditoiduissa tietoturvallisissa käyttöympäristöissä.

Muutoksen myötä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat riskit voisivat lisääntyä. Nämä riskit aiheutuisivat erityisesti siitä, että kansallisten viranomaisten mahdollisuudet valvoa muualla kuin Suomessa sijaitsevia käyttöympäristöjä olisivat vähäiset. Vaatimustenmukaisuuden arviointeja voisivat toteuttaa akkreditoidut sertifiointielimet, joiden toimintaa määrittelisi EU-lainsäädäntö ja kunkin maan kansallinen lainsäädäntö. Myös julkaistavien tietojen anonymisoinnin varmistamiseen tulisi kiinnittää erityistä huomiota, sillä Tietolupaviranomaisen mahdollisuudet varmistaa kansainvälisissä tutkimusyhteistyössä julkaistavien tietojen ano-

nymisointi ovat hyvin rajalliset ja näin ollen esityksessä ehdotetaankin, että Tietolupaviranomainen voisi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta.

Toisiolaki ja Tietolupaviranomaisen määräys sisältävät suoja- ja turvallisuustoimia ja mekanismeja, joilla varmistetaan henkilötietojen suoja. Muualla kuin Suomessa sijaitsevien käyttöympäristöjen tietoturvallisuus tulisi todentaa akkreditoidun sertifiointielimen antamalla todistuksella, jolla osoitetaan, että toisiolakia ja Tietolupaviranomaisen määräystä noudatetaan. Lainsäädännössä ja Tietolupaviranomaisen määräyksessä asetetut ehdot varmistaisivat sen, että henkilötietojen tietosuoja ja tietoturva olisi turvattu, ja että henkilötietojen käsittelyssä otettaisiin huomioon rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut.

Tässä hallituksen esityksessä on mahdollista arvioida henkilötietojen käsittelyyn kohdistuvia riskejä vain yleisellä tasolla. Tietosuoja-asetuksen mukaisesti rekisterinpitäjien tulee toteuttaa ennen käsittelyä tietosuoja-asetuksen 35 artiklan mukainen tietosuojaa koskeva vaikutustenarviointi, jos käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Vaihtoehto 1: Toisiolaissa asetettujen vaatimusten pitäminen ennallaan

Yhtenä vaihtoehtona esitetylle ratkaisulle olisi pitää toisiolaissa asetetut tietoturvallisia käyttöympäristöjä koskevat vaatimukset ennallaan. Tällöin kansainvälinen tutkimusyhteistyö suomalaisilla rekisteritiedoilla olisi mahdollista toteuttaa niin, että tutkija ottaisi etäyhteyden auditoituun suomalaiseen käyttöympäristöön ja käsittelisi toisiolain nojalla pyydettyjä tietoja tässä käyttöympäristössä. Tietojen analysointi ja yhdistäminen muihin tutkimuksessa kerättyihin tietoihin olisi mahdollista, jos tutkija siirtäisi koko tutkimusaineiston suomalaiseen käyttöympäristöön.

Kansainvälistä tutkimusyhteistyötä edistäisi se, että ulkomaiset toimijat alkaisivat auditoimaan käyttöympäristöjään toisiolain mukaisesti EU- ja ETA-alueella. Tähän mennessä ulkomaiset toimijat eivät ole aloittaneet toisiolain mukaisia auditointeja.

Vaihtoehto 2: Yhteiseurooppalaiset ratkaisut

Euroopan unionissa on tällä hetkellä käynnissä hankkeita, joiden tarkoituksena on helpottaa datan käyttöä erilaisiin yhteisen edun mukaisiin tavoitteisiin, kuten tieteelliseen tutkimukseen. Euroopan komission vuonna 2020 julkistaman datastrategian tarkoituksena on laajentaa datan, mukaan lukien terveysdatan, käyttöä Euroopan unionissa. Datastrategiassa ehdotetaan Euroopan terveysdata-avaruuden (European Health Data Space, EHDS) luomista osana Euroopan datapolitiikkaa.

Euroopassa ei tällä hetkellä ole yhteisiä käytäntöjä terveystietojen toissijaiseen käyttöön. Tietosuoja-asetuksen 9 artiklan 4 kohdan mukaan jäsenmaat voivat ottaa käyttöön lisäehtoja, mukaan lukien rajoituksia, jotka koskevat geneettisten tietojen, biometristen tietojen tai terveystietojen käsittelyä, joka on osaltaan johtanut hajanaisiin käytäntöihin EU:ssa.

EU:ssa ei ole tällä hetkellä lainsäädäntöä tai yhteisesti sovittuja käytänteitä, joita olisi mahdollista käyttää tietoturvallisten käyttöympäristöjen tietoturvallisuuden arviointiin. EU:ssa on

käynnissä useita hankkeita erityisesti pilvipalveluiden turvallisuuden varmentamiseksi. Näitä ovat esimerkiksi EUSEC:n pilvipalveluiden kriteeristöjen arviointi ja ristiinhyväksyntä.[19] EU:n kyberturvallisuusvirasto ENISA[20] on julkaissut ehdotetun kriteeristön pilvipalveluiden kyberturvallisuudelle (EUCS).[21] EUCS tarjoaisi valmistuessaan yhteisen pilvipalveluiden kriteeristön Euroopan unioniin. ENISA on myös julkaissut terveydenhoidon pilvipalveluiden tietoturvaa käsittelevän muistion.[22]

Euroopan komissio julkaisi ehdotuksen eurooppalaisen terveysdata-avaruuden (EHDS) luomisesta toukokuussa 2022. Eurooppalaisen data-avaruuden luominen on yksi Euroopan komission poliittisista painopisteistä vuosina 2019–2025. EHDS:n tarkoituksena on parantaa erilaisten terveystietojen vaihtamista ja saatavuutta (muun muassa sähköiset terveyskertomukset, genomidata ja potilasrekisteritiedot) ja tukea terveydenhuollon tarjoamista (tietojen ensisijainen käyttö) sekä terveysalan tutkimusta ja terveyspolitiikan laadintaa (toissijainen käyttö).

EHDS-säädösehdotuksen yleisenä tavoitteena on parantaa EU-kansalaisten mahdollisuutta hallita omia terveystietojaan. Ehdotuksen tarkoituksena on luoda oikeudellinen kehys, joka sisältää luotettavat EU- ja jäsenvaltiotason hallintomekanismit ja turvallisen tietojen käsittely-ympäristön, jonka avulla tutkijat, päätöksentekijät ja sääntelyviranomaiset EU- ja jäsenvaltiotasolla voisivat vastaanottaa ja käsitellä terveystietoja edistääkseen yksilöiden parempaa diagnoosia, hoitoa ja hyvinvointia sekä luodakseen parempia ja tietoon perustuvia toimintaperiaatteita.

EHDS-säädösehdotus koskee myös terveystietojen toisiokäyttöä ja siinä säännellään mekanismeista, joilla terveystietoja olisi mahdollista jakaa EU:n jäsenmaissa yhteisten käytäntöjen avulla. Ehdotus sisältää säännökset tietoturvallisista käsittely-ympäristöistä, joissa olisi mahdollista käsitellä ehdotuksen nojalla jaettavia terveystietoja tunnisteellisessa muodossa. EHDS tulisi voimaantullessaan luomaan säännökset, joilla mahdollistetaan eurooppalainen ja mahdollisesti myös kansainvälinen tutkimusyhteistyö terveystiedoilla. Suomella onkin mahdollisuus vaikuttaa tulevan EHDS-säädöksen toteuttamistapaan niin, että sillä edistetään kansainvälistä tutkimusyhteistyötä suomalaisilla rekisteritiedoilla. Vaihtoehtona ehdotetulle ratkaisulle olisikin odottaa yhteiseurooppalaisia ratkaisuja ja vaikuttaa niihin. Ehdotuksen käsittely ja säädöksen mukaisten käsittely-ympäristöjen käyttöönotto tulee kuitenkin viemään aikaa.

5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot

Ulkomaista lainsäädäntöä ja ulkomailla käytettyjä keinoja arvioitiin toisiolain hallituksen esityksen (HE 159/2017 vp) yhteydessä sivuilla 32-58 ja hallituksen esityksen toisiolain 60 §:n muuttamisesta (HE 96/2021 vp) yhteydessä sivulla 21.

Toisiolakia vastaavaa sääntelyä tietoturvallisista käyttöympäristöistä ei ole säädetty muissa maissa, ja Suomi onkin tämän suhteen edelläkävijä. Aiemmassa kappaleessa tuotiin esille, että Euroopan komissio on julkaissut ehdotuksen eurooppalaisesta terveysdata-avaruudesta, johon kuuluu myös sääntely tietoturvallisista käsittely-ympäristöistä.

[19] Ks. https://www.sec-cert.eu/
[20] Ks. https://www.enisa.europa.eu/
[21] Ks. Candidate scheme European Cybersecurity Certification Scheme for Cloud Services.
[22] Ks. https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services.

Suomen itsenäisyyden juhlarahasto Sitran koordinoima TEHDAS (Towards the European Health Data Space) Joint Action –hanke on selvittänyt raportissaan terveystietojen toisiokäytön sääntelyä Euroopassa.[23]

Raportissa todetaan, että Euroopan hallinto- ja terveystietojärjestelmissä on eroja ja EU:n jäsenvaltioissa on kansallisia terveystiedon hallintamalleja keskitetyistä malleista hajautettuihin ja federoituihin järjestelmiin. Raportin mukaan yhteisesti sovitun toissijaisen käytön määritelmän puute muodostaa esteen rajat ylittävälle datan jakamiselle. Toissijaisella käytöllä ei ole oikeusperustaa kaikissa EU-maissa, eikä selvää rajanvetoa ensisijaisen ja toissijaisen käytön välillä ole.

Lisäksi eri maiden väliset erot tietosuoja-asetuksen tulkinnassa ja kansallisten lisäsääntöjen olemassaolo voivat hankaloittaa terveystietojen toissijaista käyttöä yli jäsenvaltioiden rajojen. Päällekkäisten lakien olemassaolo EU:ssa ja kansallisella tasolla on johtanut eroihin datan jakamisen tulkinnassa ja soveltamisessa eri puolilla Eurooppaa.

Kansallisten tietosuojaviranomaisten ja Euroopan tietosuojaneuvosto EDPB:n ohjeistusta ja tulkintakäytäntöä tietosuoja-asetuksesta kertyy koko ajan lisää. Tällä hetkellä eri maissa sovelletaan erilaisia sääntöjä, jotka voivat viivästyttää ja vaikeuttaa rajat ylittävää tutkimusta ja tiedon jakamista, koska suostumus- ja terveystietojen jakamista koskevat säännöt ovat epäselviä. Myös erilaisten yhteentoimivuusstandardien käyttö Euroopassa tekee tietojen ja tutkimustulosten vertailusta ja jakamisesta haastavaa.

TEHDAS-raportissa ehdotetaan yhdeksi ratkaisuksi ongelmiin tietoturvallista käyttöympäristöä. Komissio voisi antaa ohjeistuksia tietoturvallisten käyttöympäristöjen vaatimuksista ja määritelmistä. Jäsenvaltiot voisivat hyväksyä tunnustamisperiaatteen rajat ylittävien tietoturvallisten käyttöympäristöjen toiminnan ja toimintojen välillä.

Euroopan komissio on julkaissut muistion EU:n jäsenvaltioiden terveystietoja koskevien säännösten arvioinnista tietosuoja-asetuksen valossa.[24] Muistion mukaan kaikissa jäsenvaltioissa on olemassa mekanismi, jonka avulla tutkijat voivat käsitellä terveystietoja, jotka on kerätty alun perin toisessa tarkoituksessa. Toisiokäytön hyväksynnässä on yleensä mukana jonkinlainen tutkimuseettinen komitea tai joissain tapauksissa hyväksynnän tietojen käsittelylle antaa keskitetty viranomainen. Usein kansallinen tietosuojaviranomainen on mukana hyväksymisprosessissa. Noudatettavan mekanismin määrittävät usein tutkimuksen luonne, tiedot tai tutkimuksen toteuttaja. Tietosuoja-asetuksen noudattamiseksi käytetään yleisesti sekä anonymisointi- että pseudonymisointityökaluja, tietopyynnön luonteesta riippuen.

6 Lausuntopalaute

Kohtaa täydennetään lausuntopalautteen perusteella.

7 Säännöskohtaiset perustelut

3 §. *Määritelmät*.

---

[23] TEHDAS Joint Action Report on secondary use of health data through European case studies.
[24] Assessment of the EU Member States' rules on health data in the light of GDPR, ks. https://ec.europa.eu/newsroom/sante/items/702120/en.

Sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 3 §:n 21 kohtaan ehdotetaan lisättäväksi uusi määritelmä sertifiointielimistä. Sertifiointielimellä tarkoitettaisiin yhdenmukaisten kansainvälisten ja eurooppalaisten arviointiperusteiden mukaisesti akkreditoitua arviointielintä, jonka on hyväksynyt EU:n asetuksen 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista mukainen kansallinen akkreditointielin.

Sertifiointielimen tulisi olla akkreditoitu yhdenmukaisten kansainvälisten ja eurooppalaisten arviointiperusteiden mukaisesti, kuten esimerkiksi ISO/IEC 17021 standardilla ja sitä täydentävällä ISO/IEC 27006 – standardilla. Akkreditoinnin suorittaisi akkreditointielin, joka hyväksyisi sertifiointielimen kansainvälisten ja eurooppalaisten arviointiperusteiden mukaisesti. Akkreditointielin tarkoittaisi tässä yhteydessä EU:n asetuksen 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista mukaisesti nimettyä kansallista akkreditointielintä.

Esityksessä ehdotetaan, että Tietolupaviranomainen voisi antaa tarkempia määräyksiä sertifiointielimistä, jotka voivat arvioida sitä, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset.

21 §. *Tietoturvallisen käyttöympäristön käyttäjien tunnistaminen*.

Lain 21 §:n 2 momentti, jonka mukaan sosiaali- ja terveysministeriön asetuksella voidaan antaa tarkempia säännöksiä tunnistamisen ja todentamisen teknisestä toteuttamisesta, ehdotetaan kumottavaksi. Sähköisen tunnistamisen ja todentamisen teknisestä toteuttamisesta säädetään muun muassa EU:n asetuksessa 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta sekä vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa 617/2009.

23 §. *Tietoturvallisen käyttöympäristön suojaaminen*.

Lain 23 §:n 1 momenttia ehdotetaan muutettavaksi niin, että siinä viitataan tiedonhallintalain (906/2019) 4 luvussa säädettyihin tietoturvallisuusvaatimuksiin ja Tietolupaviranomaisen määräykseen. Aiempi viittaus julkisuuslain 36 §:ään on vanhentunut. Nykyiset valtion viranomaisten tietoturvallisuutta koskevat velvoitteet löytyvät tiedonhallintalaista. Tiedonhallintalain myötä julkisuuslain nojalla annettu asetus tietoturvallisuudesta valtionhallinnossa (681/2010) kumottiin.

Tiedonhallintalain säännökset voivat velvoittaa ainoastaan Suomessa sijaitsevien käyttöympäristöjen palveluntarjoajia. Tämän vuoksi toisiolain 23 §:n 1 momenttiin ehdotetaan lisättäväksi, että tietoturvallinen käyttöympäristö tulisi suojata noudattaen, mitä Tietolupaviranomaisen määräyksessä edellytetään. Tietolupaviranomaisen määräyksessä asetettaisiin tiedonhallintalain edellytyksiä vastaavat vaatimukset käyttöympäristöjen suojaamiselle.

25 §. *Tietoturvallisen käyttöympäristön tietoturvallisuuden osoittaminen*.

Lain 25 §:n 1 momenttia ehdotetaan muutettavaksi niin, että käyttöympäristön tietoturvallisuus olisi mahdollista osoittaa tietoturvallisuuden arviointilaitoksen antaman todistuksen lisäksi sertifiointielimen antamalla todistuksella.

Lain 25 §:n 2 momenttia ehdotetaan muutettavaksi niin, että Tietolupaviranomainen voisi antaa tarkempia määräyksiä tietoturvallisuuden osoittamisessa noudatettavista menettelyistä sekä

niistä sertifiointielimistä, jotka voivat arvioida sitä, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset.

26 §. *Tietoturvallisuuden arviointi*.

Esityksessä ehdotetaan muutettavaksi lain 26 §:n 1 momenttia niin, että tietoturvallisuuden arviointilaitoksen lisäksi myös sertifiointielin voisi arvioida toisiolain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset.

Lain 26 §:n 2 momenttia ehdotetaan muutettavaksi niin, että myös sertifiointielin voisi antaa suorittamastaan arvioinnista palveluntarjoajalle todistuksen sekä siihen liittyvän tarkastusraportin, jos käyttöympäristö täyttää toisiolain mukaiset tietoturvallisuusvaatimukset. Jos arviointi tai uudelleenarviointi koskee vain käyttöympäristön osaa, sertifiointielimen antamaan todistukseen olisi selkeästi merkittävä, mikä osa käyttöympäristöstä on arvioitu.

Lain 26 §:n 2 momenttia ehdotetaan muutettavaksi niin, että sekä arviointilaitoksen että sertifiointielimen myöntämä todistus olisi voimassa enintään kolme vuotta. Todistuksen voimassaoloajan lyhentäminen viidestä vuodesta kolmeen vuoteen olisi perusteltua, sillä viidessä vuodessa tietoturvallisuusympäristö- ja vaatimukset ehtivät muuttua huomattavasti ja kolme vuotta on alalla vakiintunut käytäntö useimmissa todistuksissa. Esimerkiksi ISO 27001 ja CSA Star sertifiointi ovat voimassa kolme vuotta ja seuranta-auditointeja tehdään vuosittain.

Lisäksi lain 26 §:n 2 momenttia ehdotetaan muutettavaksi niin, että myös sertifiointielin voisi vaatia palveluntarjoajalta kaikki arvioinnin sekä todistuksen laatimisen ja ylläpitämisen edellytyksenä olevat tiedot. Kuitenkin vain arviointilaitoksen todistuksen antamiseen sovellettaisiin muutoin tietoturvallisuuden arviointilaitoksista annetun lain 9 §:n 3 momenttia. Sertifiointielimen todistuksen antamiseen sovellettaisiin muutoin Tietolupaviranomaisen määräystä.

27 §. *Arviointilaitoksen myöntämän todistuksen peruuttaminen*.

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.

28 §. *Tietoturvallisuuden arviointilaitoksen ja sertifiointielimen ilmoittamisvelvollisuus*.

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.

29 §. *Tietoturvallisen käyttöympäristön käyttöönoton jälkeinen seuranta*.

Lain 28 §:n 1 momenttia ehdotetaan muutettavaksi 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

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

Lain 29 §:n 2 momentin mukaisesti palveluntarjoajan on säilytettävä vaatimustenmukaisuutta koskevat ja muut valvonnan edellytyksenä olevat tiedot vähintään viisi vuotta tietoturvallisen käyttöympäristön tuotantokäytön päättymisestä.

30 §. *Tietojärjestelmien valvonta ja tarkastukset*.

Lain 30 §:n 1 momenttia ehdotetaan muutettavaksi niin, että sertifiointielimien tehtävänä olisi valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset.

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 §. *Tietoluvan nojalla luovutetuista tiedoista johdettujen tulosten julkaiseminen*.

Lain 52 §:ää ehdotetaan muutettavaksi niin, että pykälään lisättäisiin uusi 3 momentti, jonka mukaan Tietolupaviranomainen voi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta.

Toisiolaissa on asetettu Tietolupaviranomaisen tehtäväksi vastata julkaistavien tietojen anonymisoinnin varmistamisesta. Tietolupaviranomainen voi perustellusta syystä lupapäätöksessään myöntää luvansaajalle oikeuden toteuttaa itse julkaistavien edellä mainittujen tietojen anonymisoinnin ehdolla, että ne toimitetaan jälkikäteen Tietolupaviranomaisille.

Ehdotuksen mukaan Tietolupaviranomainen voisi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta. Määräyksessä olisi mahdollista tarkemmin määrittää, miten julkaistavien tietojen anonymisointi tulisi varmistaa luvansaajan toimesta.

8 Lakia alemman asteinen sääntely

Toisiolain 24 §:n 2 momentin mukaan Tietolupaviranomainen antaa tarkemmat määräykset muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista. Esityksessä ehdotetaan muutettavaksi toisiolain 25 §:n 2 momenttia niin, että Tietolupaviranomainen voisi antaa tarkempia määräyksiä tietoturvallisuuden osoittamisessa noudatettavien menettelyjen lisäksi niistä sertifiointielimistä, jotka voivat arvioida sitä, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Lisäksi toisiolain 52 §:ää ehdotetaan muutettavaksi niin, että pykälään lisättäisiin uusi 3 momentti, jonka mukaan Tietolupaviranomainen voi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta.

Esityksessä ehdotetun ratkaisun toteuttamiseksi Tietolupaviranomaisen tietoturvallisia käyttöympäristöjä koskevaa määräystä tulisi muuttaa niin, että siinä asetetut vaatimukset on mahdollista täyttää myös kansainvälisiä standardeja ja menettelyjä noudattamalla ja vaatimustenmukaisuuden arviointi on mahdollista suorittaa akkreditoidun sertifiointielimen toimesta.

Toisiolain hallituksen esityksen (HE 159/2017 vp) sivuilla 176-177 on käsitelty Tietolupaviranomaisen määräyksenantovaltuuksia. Tietolupaviranomaisen määräyksenantovaltuutta tietoturvallisille käyttöympäristöille asetettavista vaatimuksista perustellaan sillä, että määräyksenantovaltuudet koskevat pääosin teknisiä yksityiskohtia, joiden antaminen sopii luontevasti Tietolupaviranomaisen tehtäviin. Lisäksi teknisten ja tarkempien määräysten antaminen on hallituksen esityksen mukaan välttämätöntä, koska tekninen kehitys etenee nopeasti ja koska määräysten antaminen edellyttää tietoturvalliseen käyttöympäristöön liittyvää erityisasiantuntemusta

Esityksessä ehdotetaan säädettäväksi Valviralle oikeus antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta. Muutosta perustellaan sillä, että kansallisen viranomaisen edellytykset valvoa muualla kuin Suomessa sijaitsevia käyttöympäristöjä ovat vähäiset ja tämän vuoksi sertifiointielimien tehtävänä olisi valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietoturvaa koskevat vaatimukset. Valviran olisi mahdollista antaa tarkempia määräyksiä siitä, miten sertifiointielimien valvontatehtävä tultaisiin toteuttamaan.

9 Voimaantulo

Ehdotetaan, että laki tulee voimaan 1.12.2023. Ehdotuksen voimaantulo edellyttää Tietolupaviranomaisen määräysten muuttamista ja näiden muutosten toteuttamisessa arvioidaan kestävän noin vuosi.

10 Toimeenpano ja seuranta

Sosiaali- ja terveysvaliokunta on toisiolain hallituksen esityksessä (HE 159/2017) antamassaan mietinnössään todennut, että valtioneuvoston on tarpeen seurata ja arvioida sääntelyn toimeenpanoa ja toimivuutta huolellisesti siten, että lainsäädäntö vastaa teknisen kehityksen muutosten mukanaan tuomiin tarpeisiin siten, että varmistetaan tietojen toissijaisen käytön sujuva toteutus, korkean tason tietoturva arkaluonteisten sosiaali- ja terveystietojen käsittelylle sekä tietojen toissijaisen käytön vaikuttavuus sosiaali- ja terveydenhuollon palvelujärjestelmälle. Valiokunta korosti, että ehdotetun järjestelmän kokonaisuuden sekä sitä sääntelevän lainsäädännön toimivuutta tulee seurata ja arvioida huolellisesti myös silloin, kun toiminta on jo käynnissä, jotta toiminnassa hyödynnetään asianmukaisella tavalla teknologian kehitystä turvaamaan henkilötietojen suoja. Tarvittaessa lainsäädäntöä tulee myös muuttaa.

Hallituksen näkemyksen mukaan toisiolain toimeenpanoa tulee edelleen seurata yhdessä valvovien viranomaisten ja toisiolain 8 §:n 4 momentin mukaisen korkean tason asiantuntijaryhmän kanssa varmistaen, että toiminnassa hyödynnetään asianmukaisella tavalla teknologian kehitystä turvaamaan henkilötietojen suoja.

Esityksessä ehdotetun ratkaisun toteuttamiseksi on tarpeen toimeenpanna ja seurata Tietolupaviranomaisen määräyksen muuttamiseksi tarvittavia toimenpiteitä. Näihin toimenpiteisiin sisältyisi vastaavuustaulukon laatiminen Tietolupaviranomaisen määräyksessä asetettuja vaatimusten ja kansainvälisissä standardeissa ja menettelyissä asetettujen vaatimusten välillä. Lisäksi 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.

11 Suhde muihin esityksiin

11.1 Esityksen riippuvuus muista esityksistä

Esitys ei liity tällä hetkellä annettuihin tai valmisteilla oleviin hallituksen esityksiin.

11.2 Suhde talousarvioesitykseen

Esityksellä on vaikutus Tietolupaviranomaisen budjettiin. Esityksessä ehdotetun ratkaisun toteuttamiseksi Tietolupaviranomaisen tulisi uudistaa tietoturvallisia käyttöympäristöjä koskevaa määräystään ja tämä arviointi- ja uudistamistyö edellyttää resursseja.

12 Suhde perustuslakiin ja säätämisjärjestys

Yksityiselämän suoja

Toisiolain hallituksen esityksessä (HE 159/2017) on arvioitu erityisesti esityksen suhdetta yksityiselämän suojaan ja julkisuusperiaatteeseen ja julkisen vallan käyttöön.

Hallituksen esityksessä toisiolain muuttamisesta (HE 96/2021 vp) on käsitelty esityksen suhdetta yksityiselämän suojaan ja käyty läpi perustuslakivaliokunnan lausuntokäytäntöä liittyen henkilötietojen käsittelyyn, lailla säätämisen vaatimukseen, tiedonsaantioikeuksiin ja arkaluonteisten tietojen käsittelyyn. Alla kuvataan tiivistetysti esitykseen liittyvä perustuslakivaliokunnan käytäntö.

Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Säännös viittaa tarpeeseen turvata yksilön yksityiselämän suoja henkilötietojen käsittelyssä eli henkilötietojen suoja sisältyy osittain yksityiselämän suojan piiriin. Henkilötietojen suojasta voidaan säätää tarkemmin lailla, mutta samalla on turvattava tietosuoja sellaisella tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuuden kannalta.

Eduskunnan perustuslakivaliokunta on lausunnoissaan (PeVL 8/1995 vp, PeVL 26/1996 vp sekä PeVL 7, 28 ja 29/1997 vp) ottanut kantaa hallitusmuodon 8 §:n 1 momentissa (nykyinen perustuslain 10 §:n 1 momentti) säädettyyn henkilötietojen käsittelyn lailla säätämisen velvollisuuteen. Valiokunta on todennut, että henkilötietojen suojaa koskevan perusoikeussäännöksen kannalta tärkeitä sääntelykohteita ovat ainakin rekisteröinnin tavoite, rekisteröitävien henkilötietojen sisältö, niiden sallitut käyttötarkoitukset mukaan luettuna tietojen luovutettavuus ja tietojen säilytysaika henkilörekisterissä sekä rekisteröidyn oikeusturva samoin kuin näiden seikkojen sääntelemisen kattavuus ja yksityiskohtaisuus lain tasolla. Myöhemmissä lausunnoissaan (PeVL 12/2002 vp, 14/2002 vp, 51/2002 vp ja 11/2008 vp) valiokunta on uudistanut näkemystään ja todennut, että lailla säätämisen vaatimus koskee myös mahdollisuutta luovuttaa henkilötietoja teknisen käyttöyhteyden avulla.

Henkilötietojen käsittelyä koskevan lainsäädännön on oltava kattavaa, täsmällistä ja tarkkarajaista. Perustuslakivaliokunta on lisäksi kiinnittänyt useissa lausunnoissaan huomiota siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tiedonsaantioikeus sidotaan tietojen välttämättömyyteen. Viranomaisen tietojensaantioikeus ja tietojenluovuttamismahdollisuus ovat valiokunnan mukaan voineet liittyä jonkin tarkoituksen kannalta "tarpeellisiin tietoihin", jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisältöjä ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus "tietojen välttämättömyydestä" jonkin tarkoituksen kannalta (esim. PeVL 10/2014 vp, s. 6/II, PeVL 17/2016

vp, s. 2—3, PeVL 38/2016 vp, s. 2). Lisäksi mahdollisuudesta yhdistää rekisteritietoja on säädettävä lailla (PeVL 17/2007 vp ja PeVL 30/2005 vp).

Perustuslakivaliokunnan mukaan on lähtökohtaisesti riittävää perustuslain 10 §:n 1 momentin kannalta, että sääntely täyttää EU:n yleisessä tietosuoja-asetuksessa asetetut vaatimukset. Valiokunnan mukaan henkilötietojen suoja tulee turvata ensisijaisesti EU:n yleisen tietosuoja-asetuksen ja kansallisen yleislainsäädännön nojalla. Kansallisen erityislainsäädännön säätämiseen tulee siten suhtautua pidättyvästi ja rajata sellainen vain välttämättömään tietosuoja-asetuksen salliman kansallisen liikkumavaran puitteissa (ks. PeVL 14/2018 vp, s. 4—5).

Perustuslakivaliokunnan mukaan on kuitenkin selvää, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksenkin edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä suurempi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn osalta (ks. PeVL 14/2018 vp, s. 5).

Perustuslakivaliokunta on painottanut arkaluonteisten tietojen käsittelyn aiheuttamia uhkia. Valiokunnan mielestä arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille (ks. PeVL 13/2016 vp, s. 4, PeVL 14/2009 vp, s. 3/I). Myös EU:n yleisen tietosuoja-asetuksen 51 johdantokappaleen mukaan asetuksen 9 artiklassa tarkoitettuja erityisiä henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, koska niiden käsittelyn asiayhteys voisi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille. Valiokunta on tämän johdosta kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on rajattava täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään ja sääntelyn on oltava tietosuoja-asetuksen mahdollistamissa puitteissa yksityiskohtaista ja kattavaa (PeVL 65/2018 vp, s. 45, PeVL 15/2018 vp, s. 40). Valiokunta painotti kuitenkin tietosuojalain arvion yhteydessä, että sääntelyn tarpeen osalta on syytä kiinnittää huomiota myös asetuksessa omaksuttuun riskiperusteiseen lähestymistapaan, ja korosti, että myös arkaluonteisten henkilötietojen käsittelyä koskevan sääntelyn kohdalla on syytä pyrkiä selkeään ja ymmärrettävään lainsäädäntöön (PeVL 14/2018 vp, s. 6).

Perustuslakivaliokunta on painottanut, että väärinkäytön estävät tietoturvajärjestelyt ovat toimivia ja käytettävissä heti, kun järjestelmä otetaan käyttöön. Valiokunnan mielestä käsittelyn välttämättömyyden ja muun lainmukaisuuden jälkikäteinen ja tehokas valvonta esimerkiksi lokitietojen avulla on sinänsä välttämätöntä, mutta ei kuitenkaan riittävä tae. Valiokunta on korostanut, että tietojen suojaamista oikeudettomalta käytöltä ei voi perustaa vain rekisterinpitäjää tai tietojen käsittelijää koskevan virkavastuun tai muun seuraamusjärjestelmän varaan (PeVL 65/2018 vp, s. 47, PeVL 51/2018 vp, s. 5, PeVL 52/2018 vp, s. 4).

Tässä hallituksen esityksessä ehdotettu ratkaisu olisi merkityksellinen perustuslain 10 §:n 1 momentissa turvatun yksityiselämän ja henkilötietojen suojan kannalta. Ehdotettu sääntely on merkityksellistä myös EU:n perusoikeuskirjan kannalta. EU:n perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja ja 8 artiklassa jokaisen oikeus henkilötietojensa suojaan. Ehdotus mahdollistaisi toisiolaissa tarkoitettujen henkilötietojen luovuttamisen muualla kuin Suomessa sijaitsevaan tietoturvalliseen käyttöympäristöön. Esitetty ratkaisu voisi lisätä rekisteröidyille aiheutuvia riskejä verrattuna nykytilaan, jossa tietoturvalliset käyttöympäristöt auditoidaan Traficomin Kyberturvallisuuskeskuksen hyväksymien tietoturvallisuuden arviointilaitosten toimesta. Ehdotuksella ei kuitenkaan ole tarkoitus muuttaa toisiolaissa tietoturvallisilta käyttöym-

päristöiltä edellytettyä tietoturvan tasoa, vaan korkea tietoturvan ja tietosuojan taso varmistettaisiin toisiolaissa ja Tietolupaviranomaisen määräyksessä edellytetyillä tietoturvavaatimuksilla.

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.

Henkilötietojen suojan kannalta tulee myös ottaa huomioon, että tietoturvallinen käyttöympäristö ei ole ainoa toisiolaissa säädetty keino varmistaa henkilötietojen tietoturva ja tietosuoja, vaan toisiolakiin sisältyy useita henkilötietoja suojaavia mekanismeja. Lisäksi toisiolaissa olisi edelleen voimassa periaate, jonka mukaan toisiolaissa tarkoitetut tiedot luovutetaan ensisijaisesti aina Tietolupaviranomaisen omaan tietoturvalliseen käyttöympäristöön.

Hallituksen esityksessä toisiolain muuttamisesta (HE 96/2021 vp) on kuvattu toisiolain tietosuojaa ja tietoturvaa koskevia järjestelyitä, jotka suojaavat toisiotarkoituksessa käsiteltäviä henkilötietoja. Toisiolaki sisältää mahdollisimman tarkkarajaisesti ne käyttötarkoitukset, joihin tietoja voidaan luovuttaa, sekä perusteet joilla luovutuspäätös tulee ratkaista. Toisiolakiin sisältyy merkittäviä määrä teknisiä ja muita turvatakeita, joiden avulla voidaan varmistua siitä, että luovutuksensaaja käsittelee henkilötietoja rekisteröidyn yksityiselämän suojaa turvaten. Näitä ovat esimerkiksi tietojen kokoamis-, yhdistämis- ja esikäsittelypalvelu, tunnisteiden hallinnointipalvelu, tietopyyntöjen hallintajärjestelmä ja tietoturvallinen käyttöpalvelu.

Rekisteröidyn oikeuksia ja vapauksia suojataan muun muassa siten, että henkilötietoja voidaan käsitellä vain viranomaisen myöntämän tietoluvan perusteella ja luvansaajaa koskisi salassapitovelvollisuus. Toisiolain salassapitopykälässä on kysymys salassapitosäännösten laajentamisesta koskemaan myös muuta kuin viranomaistoimintaa. Lisäksi pykälässä kielletään pääsääntöisesti tietojen käyttö yksittäistä henkilöä koskevassa päätöksenteossa. Salassapitovelvollisuuden tarkoituksena on samalla turvata yksilöiden henkilötietojen suojaa perusoikeutena.

Henkilötiedot tulee anonymisoida tai pseudonymisoida aina, kun se on käyttötarkoituksen kannalta mahdollista. Tietolupaviranomaisen ja muiden toisiolain mukaisesti tietolupia myöntävien viranomaisten sekä Valviran on omalta osaltaan seurattava ja valvottava, että niiden myöntämien lupien ehtoja noudatetaan. Toisiolain 56 §:n mukaan, jos Tietolupaviranomaisella tai toisiolain mukaisesti tietolupia myöntävällä viranomaisella on perusteltua syytä epäillä, että sen myöntämän tietoluvan perusteella tietoja käsittelevä ei käsittele henkilötietoja lain mukaisesti, sen on viipymättä tehtävä ilmoitus tietosuojavaltuutetulle.

Toisiolaki ja Tietolupaviranomaisen määräys yhdessä muodostavat henkilötietojen suojaa turvaavan kokonaisuuden, jota täydentää myös muu sovellettava kansallinen ja eurooppalainen lainsäädäntö. Toisiolailla on ollut tarkoitus panna toimeen sen alaan kuuluvilta osin EU:n yleinen tietosuoja-asetus ja ottaa huomioon myös muu alaan liittyvä Euroopan unionin sääntely. Toisiolailla annetaan tietosuoja-asetusta täydentävät säännökset kansallisen liikkumavaran puitteissa.

Ehdotuksessa annettaisiin tietosuoja-asetusta täydentäviä säännöksiä kansallisen liikkumavaran puitteissa. Kansallinen liikkumavara pohjautuu tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohtaan sekä erityisten henkilötietoryhmien osalta 9 artiklan 2 kohdan g, h ja j alakohtaan. Tietosuoja-asetuksen 6 artiklan 3 kohdan mukaan jäsenvaltion lainsäädäntö voi sisältää erityisiä

säännöksiä, joilla mukautetaan tietosuoja-asetuksen sääntöjen soveltamista. Erityiset säännökset voivat sisältää yleisiä edellytyksiä, jotka koskevat rekisterinpitäjän suorittaman tietojenkäsittelyn lainmukaisuutta, käsiteltävien tietojen tyyppiä, asianomaisia rekisteröityjä, yhteisöjä joille ja tarkoituksia joihin henkilötietoja voidaan luovuttaa, käyttötarkoitussidonnaisuutta, säilytysaikoja; sekä käsittelytoimia ja -menettelyjä, mukaan lukien laillisen ja asianmukaisen tietojenkäsittelyn varmistamiseen tarkoitetut toimenpiteet. Lisäksi tietosuoja-asetuksen 9 artiklan 4 kohdan mukaan jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön lisäehtoja, mukaan lukien rajoituksia, jotka koskevat geneettisten tietojen, biometristen tietojen tai terveystietojen käsittelyä.

Esityksessä ehdotetut säännökset toimisivat tietosuoja-asetuksen edellyttäminä suojatoimina rekisteröidyn perusoikeuksien ja etujen suojaamiseksi. Ehdotetut säännökset sisältyvät näin ollen tietosuoja-asetuksessa jäsenvaltioille annettuun kansalliseen liikkumavaraan.

Edellä esitetyn perusteella ehdotetut säännökset turvaavat yksityiselämän suojan sekä henkilötietojen suojan vaatimukset perustuslain ja tietosuoja-asetuksen edellyttämällä tavalla.

Julkisen vallan käyttö

Perustuslain 124 §:ssä säädetään hallintotehtävän antamisesta muulle kuin viranomaiselle. Sen mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia.

Perustuslain 124 §:n perustelujen sekä perustuslakivaliokunnan tulkintakäytännön mukaan ”julkisella hallintotehtävällä” viitataan ”julkisen vallan käyttöä” laajempaan kokonaisuuteen. Julkinen hallintotehtävä voi olla luonteeltaan myös palvelutehtävä, joka ei välttämättä sisällä julkisen vallan käyttöä tai julkisen vallan käytön osuus siinä voi olla vähäinen.

Lisäksi perustuslain 124 §:n mukaan merkittävää julkista valtaa sisältävää tehtävää voi hoitaa vain viranomainen. Tällaista merkittävää julkista valtaa saattaisi sisältyä muun muassa käyttölupaharkintaan ja tietojen luovuttamista tämän lain perusteella koskeviin muihin päätöksiin. Julkisen hallintotehtävän hoitaminen on pykälän perusteella pääsääntöisesti viranomaisen tehtävä ja se voidaan antaa muille kuin viranomaisille vain rajoitetusti.

Perustuslakivaliokunnan tulkintakäytännöstä ilmenee, että perustuslain 124 §:n mukaisella hallintotehtävän antamisella muulle kuin viranomaiselle voi etenkin yksityisen oikeusasemaan olennaisesti vaikuttavissa tilanteissa olla vain viranomaistoimintaa täydentävä ja avustava luonne. Perustuslakivaliokunnan käytännössä on arvioitu muun muassa oikeusapu- ja edunvalvontapalveluja (PeVL 16/2016 vp), oleskelulupatehtäviä (PeVL 62/2014 vp), passin antamista koskevan menettelyn ulkoistamista (PeVL 6/2013 vp), viranomaisten turvallisuusverkkotoiminnan antamista valtionyhtiölle (PeVL 8/2014 vp), rautatieliikenteen vaatimuksenmukaisuuden teknisen arvioinnin ja tarkastustehtävien antamista yksityiselle oikeushenkilölle (PeVL 16/2002 vp). Kyse on ollut viranomaistoiminnalle edellytyksiä luovasta, teknisluontoisesta tai epäitsenäisestä toimintakokonaisuudesta.

Perustuslakivaliokunta on käytännössään jakanut 124 §:n mukaisen arvioinnin kolmeen osaan. Jako perustuu perustuslain esitöihin. Valiokunta on edellyttänyt, että kyseessä ei ole merkittävän julkisen vallan siirto, tehtävän siirto on tarkoituksenmukainen mm. hallinnon tehokkuuden ja muiden hallinnon sisäisten tarpeiden sekä myös yksityisten henkilöiden ja yhteisöjen tarpeiden vuoksi ja siirrettäessä huolehditaan perusoikeuksien, oikeusturvan ja muiden hyvän hallinnon vaatimusten turvaamisesta.

Hallituksen esityksessä toisiolain muuttamisesta (HE 96/2021 vp) on käsitelty julkisen vallan käyttöä ja tietoturvallisten käyttöympäristöjen perustamista suhteessa perustuslain 124 §:ään. Toisiolain 20 §:ssä tarkoitetun tietoturvallisen käyttöympäristön voi perustaa muukin kuin viranomainen, myös yksityisoikeudellinen oikeushenkilö. Käyttöympäristössä käsitellään henkilötietoja.

Tietolupaviranomaisen tietoturvallinen käyttöympäristö on aina ensisijainen paikka, johon henkilötiedot luovutetaan. Tietolupaviranomaisen käyttöympäristön ei pitäisi rajoittaa sinänsä perustuslainmukaisen käyttötarkoituksen toteutumista. Tämän vuoksi on tarkoituksenmukaista, että tietoja voi käsitellä muussakin kuin Tietolupaviranomaisen käyttöympäristössä. Lisäksi nykysääntelyn valossa arkaluonteistenkin henkilötietojen käsittely on ollut mahdollista muussa kuin viranomaisen käyttöympäristössä. Käsittelijöiltä on luonnollisesti edellytetty salassapitovelvollisuutta.

Vaikka tietoja voidaan siirtää muuhun kuin Suomessa sijaitsevaan tietoturvalliseen käyttöympäristöön, rekisteröidyn perusoikeudet eivät saisi näissä tilanteissa vaarantua. Tietoturvallisen käyttöympäristön tietoturvallisuudelle asetettaisiin henkilötietojen suojaamiseksi lain 21—29 §:ssä vähimmäisvaatimukset, jotka sen olisi täytettävä. Tietoturvallisuuden arviointilaitos tai akkreditoitu sertifiointielin suorittaisi järjestelmille auditoinnin, jolla varmistuttaisiin vähimmäisvaatimusten täyttymisestä. Akkreditoitu sertifiointielin valvoisi niitä järjestelmiä, jotka se on arvioinut. Luvansaajaa sitoisi lisäksi salassapitovelvollisuus. Tietolupaviranomainen toisiolaissa säädetyin edellytyksin valvoo sitä, että henkilötietoja käsitellään lain ja lupaehtojen mukaisesti. Näin kyettäisiin huolehtimaan siitä, että henkilötietoja käsitellään asianmukaisesti.

Perustuslain 10 §:ssä ei edellytetä, että henkilötietoja käsittelee viranomainen. Käytännössä yksityiset tahot käsittelevät henkilötietoja huomattavassa määrin ja myös arkaluonteisia henkilötietoja. Teknisiä viranomaisten henkilötietojen käsittelyyn liittyviä tehtäviä hoitavat yksityisoikeudellisetkin oikeushenkilöt esimerkiksi sopimuksen nojalla.

Norminantovaltuudet

Perustuslain 80 §:n 1 momentin mukaan ministeriö ja valtioneuvosto voivat antaa asetuksia perustuslaissa tai muussa laissa säädetyn valtuuden nojalla. Lailla on kuitenkin säädettävä yksilön oikeuksien ja velvollisuuksien perusteista sekä asioista, jotka perustuslain mukaan muuten kuuluvat lain alaan. Perustuslain 80 §:n 2 momentin mukaan muu viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä määrätyistä asioista, jos siihen on sääntelyn kohteeseen liittyviä erityisiä syitä eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella. Valtuuden tulee olla soveltamisalaltaan täsmällisesti rajattu. Perustuslaista johtuvista syistä valtuuden kattamat asiat on määriteltävä tarkasti laissa. Valtuutuksen säätämiselle laissa on perustuslakivaliokunnan lausuntokäytännössä kohdistettu vaatimuksia sääntelyn täsmällisyydestä ja tarkkarajaisuudesta (PeVL 19/2002 vp, s. 5, PeVL 1/2004 vp, s. 2 ja PeVL 17/2010 vp, s. 2).

Esityksessä ehdotetaan säädettäväksi määräyksenantovaltuuksia Tietolupaviranomaiselle ja Valviralle. Toisiolain 25 §:n 2 momenttia ehdotetaan muutettavaksi niin, että Tietolupaviranomainen voisi antaa tarkempia määräyksiä niistä sertifiointielimistä, jotka voivat arvioida sitä, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Lisäksi lain 52 §:ää ehdotetaan muutettavaksi niin, että pykälään lisättäisiin uusi 3 momentti, jonka mukaan Tietolupaviranomainen voisi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta.

Edellä mainitut Tietolupaviranomaiselle ehdotetut määräyksenantovaltuudet koskevat pääosin teknisiä yksityiskohtia, joiden antaminen sopii luontevasti Tietolupaviranomaisen tehtäviin. Tarkempien määräysten antaminen sertifiointielimistä olisi tarpeellista, sillä Tietolupaviranomainen määrittelisi tietoturvallisia käyttöympäristöjä koskevassa määräyksessään ne kansainväliset standardit ja menettelyt, joiden perusteella voidaan todistaa toisiolaissa ja Tietolupaviranomaisen määräyksessä asetettujen vaatimusten toteutumista. Nämä standardit ja menettelyt määrittelisivät myös sitä, mitkä akkreditoidut sertifiointielimet voisivat arvioida käyttöympäristön vaatimustenmukaisuutta. Tarkempien määräysten antaminen anomymisoinnin varmistamisesta olisi tarpeellista, jotta Tietolupaviranomainen voisi tehokkaasti varmistaa myös muualla kuin Suomessa sijaitsevien toimijoiden julkaisujen anonymisoinnin.

Lain 30 §:ään ehdotetaan lisättäväksi uusi 5 momentti, jonka mukaan Valvira voisi antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta. Määräyksessä olisi mahdollista määrätä tarkemmin esimerkiksi siitä, miten muiden kuin Suomessa sijaitsevien käyttöympäristöjen valvonta tultaisiin toteuttamaan.

Ehdotetut valtuutussäännökset on pääosin rajoitettu koskemaan ainoastaan teknisluonteisia yksityiskohtia. Yksilöiden oikeusaseman perusteet taas määräytyisivät lain säännösten perusteella. Ehdotuksen norminantovaltuuksien ei edellä esitetyillä perusteilla voida katsoa olevan ristiriidassa perustuslain 80 §:n kanssa.

Hallitus katsoo edellä esitetyillä perusteilla, että esitys on sopusoinnussa perustuslain kanssa, minkä vuoksi ehdotettu laki voidaan käsitellä tavallisen lain säätämisjärjestyksessä. Hallitus pitää kuitenkin suotavana, että perustuslakivaliokunta antaisi asiasta lausunnon.

Ponsi

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäväksi seuraava lakiehdotus:

Lakiehdotus

Laki

sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019) 21 §:n 2 momentti,

muutetaan lain 3 §:n 20 kohta, 23 §:n 1 momentti, 25—28 §, 29 §:n 1 momentti, 30 §:n 1 momentti, sekä

lisätään lain 3 §:ään uusi 21 kohta, 30 §:ään uusi 5 momentti ja 52 §:ään uusi 3 momentti seuraavasti:

3 §

Määritelmät

Tässä laissa tarkoitetaan:

— —

20) *tietoturvallisuuden arviointilaitoksella* sellaista yritystä, yhteisöä ja viranomaista, jonka Liikenne- ja viestintävirasto on hyväksynyt tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) perusteella arvioimaan sitä, täyttääkö tietojärjestelmä tietoturvallisuutta koskevat vaatimukset;

21) *sertifiointielimellä* yhdenmukaisten kansainvälisten ja eurooppalaisten arviointiperusteiden mukaisesti akkreditoitua arviointielintä, jonka EU:n asetuksen 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista mukainen kansallinen akkreditointielin on hyväksynyt.

23 §

Tietoturvallisen käyttöympäristön suojaaminen

Tietoturvallinen käyttöympäristö on suojattava valtion viranomaisten tietoturvallisuutta koskevien velvoitteiden mukaisesti noudattaen, mitä julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 4 luvussa säädetään ja mitä Tietolupaviranomaisen määräyksessä edellytetään.

— —

25 §

Tietoturvallisen käyttöympäristön tietoturvallisuuden osoittaminen

Käyttöympäristön tietoturvallisuus on osoitettava 26 §:n mukaisella tietoturvallisuuden arviointilaitoksen tai sertifiointielimen antamalla todistuksella.

Tietolupaviranomainen voi antaa tarkempia määräyksiä tietoturvallisuuden osoittamisessa noudatettavista menettelyistä sekä niistä sertifiointielimistä, jotka voivat arvioida sitä, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset.

26 §

Tietoturvallisuuden arviointi

Tietoturvallisuuden arviointilaitos arvioi tämän lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Sertifiointielin arvioi tämän lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Arviointiperusteina on käytettävä Tietolupaviranomaisen määräyksiä turvalliselle käyttöympäristölle asetettavista vaatimuksista.

Jos käyttöympäristö täyttää tämän lain mukaiset tietoturvallisuusvaatimukset, tietoturvallisuuden arviointilaitoksen tai sertifiointielimen on annettava suorittamastaan arvioinnista palveluntarjoajalle todistus sekä siihen liittyvä tarkastusraportti. Jos arviointi tai uudelleenarviointi koskee vain käyttöympäristön osaa, arviointilaitoksen tai sertifiointielimen antamaan todistukseen on selkeästi merkittävä, mikä osa käyttöympäristöstä on arvioitu.

Arviointilaitoksen tai sertifiointielimen myöntämä todistus on voimassa enintään kolme vuotta. Tietoturvallisuuden arviointilaitos tai sertifiointielin voi vaatia palveluntarjoajalta kaikki arvioinnin sekä todistuksen laatimisen ja ylläpitämisen edellytyksenä olevat tiedot. Arviointilaitoksen todistuksen antamiseen sovelletaan muutoin tietoturvallisuuden arviointilaitoksista annetun lain 9 §:n 3 momenttia.

27 §

Arviointilaitoksen ja sertifiointielimen myöntämän todistuksen peruuttaminen

Jos tietoturvallisuuden arviointilaitos tai sertifiointielin toteaa, että käyttöympäristö ei ole täyttänyt tai ei enää täytä tässä laissa säädettyjä vaatimuksia tai että todistusta ei muutoin olisi tullut myöntää, laitoksen on kehotettava palveluntarjoajaa korjaamaan puutteet. Arviointilaitos tai sertifiointielin voi peruuttaa todistuksen määräajaksi tai kokonaan taikka myöntää sen rajoitettuna, jollei palveluntarjoaja korjaa puutteellisuuksia arviointilaitoksen tai sertifiointielimen asettamassa määräajassa. Määräajan pituutta määritettäessä on otettava huomioon käyttöympäristön korjaamiseksi tarvittava kohtuullinen aika.

28 §

Tietoturvallisuuden arviointilaitoksen ja sertifiointielimen ilmoittamisvelvollisuus

Tietoturvallisuuden arviointilaitoksen ja sertifiointielimen on 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 tietoturvallisuuden arviointilaitoksen ja sertifiointielimen on pyydettäessä annettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle kaikki tarvittavat lisätiedot.

29 §

Tietoturvallisen käyttöympäristön käyttöönoton jälkeinen seuranta

Palveluntarjoajan on seurattava ja arvioitava ajantasaisella järjestelmällisellä menettelyllä tietoturvallisesta käyttöympäristöstä sen tuotantokäytön aikana saatavia kokemuksia. Palveluntarjoajan on seurattava tämän lain ja Tietolupaviranomaisen määräyksen muutoksia ja tehtävä käyttöympäristöön muutosten edellytyksenä olevat korjaukset. Käyttöympäristön olennaisista muutoksista on ilmoitettava tietoturvallisuuden arviointilaitokselle tai sertifiointielimelle. Arviointilaitoksen tai sertifiointielimen myöntämä todistus on uudistettava, jos käyttöympäristöön tehdään merkittäviä muutoksia tai jos käyttöympäristöä koskevia vähimmäisvaatimuksia on muutettu tavalla, jonka edellytyksenä on uusi arviointi.

— —

30 §

Tietojärjestelmien valvonta ja tarkastukset

Sosiaali- ja terveysalan lupa- ja valvontaviraston tehtävänä on valvoa ja edistää sitä, että tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. Sertifiointielimien tehtävänä on valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. Sosiaali- ja terveysalan lupa- ja valvontavirasto ylläpitää julkista rekisteriä sille ilmoitetuista, vaatimukset täyttävistä käyttöympäristöistä.

— —

Sosiaali- ja terveysalan lupa- ja valvontaviranomainen voi antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta.

52 §

Tietoluvan nojalla luovutetuista tiedoista johdettujen tulosten julkaiseminen

— —

Tietolupaviranomainen voi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta.

_____

Tämä laki tulee voimaan päivänä kuuta 2022.

_____

Helsingissä x.x.2022

Pääministeri

Sanna Marin

Perhe- ja peruspalveluministeri Aki Lindén

Liite
Rinnakkaisteksti

Laki

sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti muutetaan sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019):

Voimassa oleva laki	*Ehdotus*
3 §	3 §
Määritelmät	*Määritelmät*
Tässä laissa tarkoitetaan:	Tässä laissa tarkoitetaan:
1) *asiakastiedolla* lain mukaan salassa pidettävää, tietosuoja-asetuksen 4 artiklan 1 kohdan mukaista henkilötietoa, joka on tallennettu sosiaali- ja terveydenhuollon tai etuuskäsittelyn asiakassuhteessa asiakasrekisteriin tai asiakkuuteen liittyvään hallinnolliseen rekisteriin;	1) *asiakastiedolla* lain mukaan salassa pidettävää, tietosuoja-asetuksen 4 artiklan 1 kohdan mukaista henkilötietoa, joka on tallennettu sosiaali- ja terveydenhuollon tai etuuskäsittelyn asiakassuhteessa asiakasrekisteriin tai asiakkuuteen liittyvään hallinnolliseen rekisteriin;
2) *henkilötietojen ensisijaisella käyttötarkoituksella* sellaista käyttötarkoitusta, jossa henkilötiedot on alun perin tallennettu;	2) *henkilötietojen ensisijaisella käyttötarkoituksella* sellaista käyttötarkoitusta, jossa henkilötiedot on alun perin tallennettu;
3) *henkilötietojen toissijaisella käyttötarkoituksella* henkilötietojen käsittelyä muussa käyttötarkoituksessa kuin 2 kohdan tarkoittamassa ensisijaisessa käyttötarkoituksessa;	3) *henkilötietojen toissijaisella käyttötarkoituksella* henkilötietojen käsittelyä muussa käyttötarkoituksessa kuin 2 kohdan tarkoittamassa ensisijaisessa käyttötarkoituksessa;
4) *kehittämis- ja innovaatiotoiminnalla* teknisen ja liiketoimintatiedon sekä olemassa olevan muun tiedon soveltamista ja käyttöä yhdessä tässä laissa tarkoitettujen henkilötietojen kanssa, kun tavoitteena on kehittää uusia tai merkittävästi parannettuja tuotteita, prosesseja tai palveluja;	4) *kehittämis- ja innovaatiotoiminnalla* teknisen ja liiketoimintatiedon sekä olemassa olevan muun tiedon soveltamista ja käyttöä yhdessä tässä laissa tarkoitettujen henkilötietojen kanssa, kun tavoitteena on kehittää uusia tai merkittävästi parannettuja tuotteita, prosesseja tai palveluja;
5) *tietojohtamisella* tiedon käsittelemistä palvelunantajan asiakas-, palvelu- ja tuotantoprosesseissa toiminnan, tuotannon ja talouden ohjauksen, johtamisen ja päätöksenteon tukena;	5) *tietojohtamisella* tiedon käsittelemistä palvelunantajan asiakas-, palvelu- ja tuotantoprosesseissa toiminnan, tuotannon ja talouden ohjauksen, johtamisen ja päätöksenteon tukena;
6) *sosiaali- ja terveydenhuollon viranomaisohjauksella* kansallisten sosiaali- ja terveydenhuollon viranomaisten lainsäädäntöön pe-	6) *sosiaali- ja terveydenhuollon viranomaisohjauksella* kansallisten sosiaali- ja terveydenhuollon viranomaisten lainsäädäntöön pe-

Voimassa oleva laki

rustuvaa alan toimijoiden ohjausta, joka pohjautuu tarkoitukseen koottuihin henkilö- ja tilastotietoihin taikka tietoihin, jotka on yksittäistapauksessa saatu ohjaus- tai valvontatehtävää varten;

7) *sosiaali- ja terveydenhuollon viranomaisvalvonnalla* kansallisten sosiaali- ja terveydenhuollon viranomaisten lainsäädäntöön perustuvaa sosiaali- ja terveydenhuollon ammattihenkilöiden ja toimintayksiköiden valvontaa;

8) *tietoluvalla* tämän lain mukaisesti myönnettyä lupaa käsitellä luvassa määriteltyjä salassa pidettäviä henkilötietoja luvassa mainittuun käyttötarkoitukseen;

9) *tietopyynnöllä* pyyntöä saada tämän lain mukaiseen käyttötarkoitukseen tässä laissa tarkoitetuista henkilötiedoista muodostettua aggregoitua tilastotietoa;

10) *tietoturvallisella käyttöpalvelulla* tietoturvallista ratkaisua, jonka kautta osapuolet voivat luovuttaa ja vastaanottaa käyttörajoituksen alaisia tietoja;

11) *tietoturvallisella käyttöympäristöllä* teknistä, organisatorista ja fyysistä tietojen käsittelyn toimintaympäristöä jossa tietoturvallisuus on varmistettu asianmukaisin hallinnollisin ja teknisin toimin;

12) *tietopyyntöjen hallintajärjestelmällä* järjestelmää, jonka välityksellä tietoluvan hakija tai tietoja tämän lain perusteella muutoin pyytävä toimittaa tietolupahakemuksen tai tämän lain mukaisen tietopyynnön ja sen liitteet viranomaiselle ja jossa tietolupaa tai tietopyyntöä koskeva päätös annetaan tiedoksi luvan hakijalle;

13) *palvelunantajalla* sosiaali- tai terveydenhuoltoa taikka sosiaali- tai terveyspalveluja järjestävää, tuottavaa tai toteuttavaa viranomaista taikka yksityistä palvelujen tuottajaa, jota tarkoitetaan yksityisistä sosiaalipalveluista annetussa laissa (922/2011) tai yksityisestä terveydenhuollosta annetussa laissa (152/1990);

14) *palvelunjärjestäjällä* sosiaali- tai terveydenhuollon palvelunantajaa, jolla on:

Ehdotus

rustuvaa alan toimijoiden ohjausta, joka pohjautuu tarkoitukseen koottuihin henkilö- ja tilastotietoihin taikka tietoihin, jotka on yksittäistapauksessa saatu ohjaus- tai valvontatehtävää varten;

7) *sosiaali- ja terveydenhuollon viranomaisvalvonnalla* kansallisten sosiaali- ja terveydenhuollon viranomaisten lainsäädäntöön perustuvaa sosiaali- ja terveydenhuollon ammattihenkilöiden ja toimintayksiköiden valvontaa;

8) *tietoluvalla* tämän lain mukaisesti myönnettyä lupaa käsitellä luvassa määriteltyjä salassa pidettäviä henkilötietoja luvassa mainittuun käyttötarkoitukseen;

9) *tietopyynnöllä* pyyntöä saada tämän lain mukaiseen käyttötarkoitukseen tässä laissa tarkoitetuista henkilötiedoista muodostettua aggregoitua tilastotietoa;

10) *tietoturvallisella käyttöpalvelulla* tietoturvallista ratkaisua, jonka kautta osapuolet voivat luovuttaa ja vastaanottaa käyttörajoituksen alaisia tietoja;

11) *tietoturvallisella käyttöympäristöllä* teknistä, organisatorista ja fyysistä tietojen käsittelyn toimintaympäristöä jossa tietoturvallisuus on varmistettu asianmukaisin hallinnollisin ja teknisin toimin;

12) *tietopyyntöjen hallintajärjestelmällä* järjestelmää, jonka välityksellä tietoluvan hakija tai tietoja tämän lain perusteella muutoin pyytävä toimittaa tietolupahakemuksen tai tämän lain mukaisen tietopyynnön ja sen liitteet viranomaiselle ja jossa tietolupaa tai tietopyyntöä koskeva päätös annetaan tiedoksi luvan hakijalle;

13) *palvelunantajalla* sosiaali- tai terveydenhuoltoa taikka sosiaali- tai terveyspalveluja järjestävää, tuottavaa tai toteuttavaa viranomaista taikka yksityistä palvelujen tuottajaa, jota tarkoitetaan yksityisistä sosiaalipalveluista annetussa laissa (922/2011) tai yksityisestä terveydenhuollosta annetussa laissa (152/1990);

14) *palvelunjärjestäjällä* sosiaali- tai terveydenhuollon palvelunantajaa, jolla on:

Voimassa oleva laki

a) viranomaisena velvollisuus huolehtia siitä, että asiakas saa hänelle lain tai viranomaisen päätöksen mukaan kuuluvan palvelun tai etuuden; taikka

b) yksityisenä palvelunantajana velvollisuus huolehtia siitä, että yksityisesti palvelun ostava asiakas saa kuluttajansuojaa koskevien säännösten mukaisen, hänelle kuuluvan palvelun;

15) *palveluntuottajalla* palvelunantajaa, joka palvelunjärjestäjän kanssa tehdyn sopimuksen perusteella tai muutoin palvelunjärjestäjän lukuun tuottaa sosiaali- tai terveyspalvelua;

16) *palveluntarjoajalla* toimijaa, joka tarjoaa asiakkailleen tietoturvalliseen käyttöympäristöön liittyviä palveluita;

17) *tiedonhyödyntämissuunnitelmalla* tutkimussuunnitelmaa, hankesuunnitelmaa ja vastaavaa suunnitelmaa, josta ilmenevät lupahakemuksessa tarkoitettujen tietojen käyttötarkoitus, niiden rekisterinpitäjä ja käsittelijät, käsittelyn oikeudellinen peruste sekä tietojen käsittelyn tietosuojaan ja tietoturvaan liittyvät olennaiset seikat kattaen koko tietojen elinkaaren mukaan lukien tietojen säilytys sekä hävittäminen tai arkistointi;

18) *aggregoidulla tilastotiedolla* tilastomuotoista, luotettavasti anonymisoitua tietoa;

19) *valmisaineistolla* aineistokokonaisuutta, jotka 4 §:ssä tarkoitettu Sosiaali- ja terveysalan tietolupaviranomainen on koostanut yhden tai useamman kuin yhden organisaation tiedoista ja yhdistänyt yhdeksi aineistoksi taikka tallentanut siten, että aineistojen tunnistetiedot on koodattu yhdenmukaisella koodilla;

20) *tietoturvallisuuden arviointilaitoksella* sellaista yritystä, yhteisöä ja viranomaista, jonka Liikenne- ja viestintävirasto on hyväksynyt tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) perusteella arvioimaan sitä, täyttääkö tietojärjestelmä tietoturvallisuutta koskevat vaatimukset.

Ehdotus

a) viranomaisena velvollisuus huolehtia siitä, että asiakas saa hänelle lain tai viranomaisen päätöksen mukaan kuuluvan palvelun tai etuuden; taikka

b) yksityisenä palvelunantajana velvollisuus huolehtia siitä, että yksityisesti palvelun ostava asiakas saa kuluttajansuojaa koskevien säännösten mukaisen, hänelle kuuluvan palvelun;

15) *palveluntuottajalla* palvelunantajaa, joka palvelunjärjestäjän kanssa tehdyn sopimuksen perusteella tai muutoin palvelunjärjestäjän lukuun tuottaa sosiaali- tai terveyspalvelua;

16) *palveluntarjoajalla* toimijaa, joka tarjoaa asiakkailleen tietoturvalliseen käyttöympäristöön liittyviä palveluita;

17) *tiedonhyödyntämissuunnitelmalla* tutkimussuunnitelmaa, hankesuunnitelmaa ja vastaavaa suunnitelmaa, josta ilmenevät lupahakemuksessa tarkoitettujen tietojen käyttötarkoitus, niiden rekisterinpitäjä ja käsittelijät, käsittelyn oikeudellinen peruste sekä tietojen käsittelyn tietosuojaan ja tietoturvaan liittyvät olennaiset seikat kattaen koko tietojen elinkaaren mukaan lukien tietojen säilytys sekä hävittäminen tai arkistointi;

18) *aggregoidulla tilastotiedolla* tilastomuotoista, luotettavasti anonymisoitua tietoa;

19) *valmisaineistolla* aineistokokonaisuutta, jotka 4 §:ssä tarkoitettu Sosiaali- ja terveysalan tietolupaviranomainen on koostanut yhden tai useamman kuin yhden organisaation tiedoista ja yhdistänyt yhdeksi aineistoksi taikka tallentanut siten, että aineistojen tunnistetiedot on koodattu yhdenmukaisella koodilla;

20) *tietoturvallisuuden arviointilaitoksella* sellaista yritystä, yhteisöä ja viranomaista, jonka Liikenne- ja viestintävirasto on hyväksynyt tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) perusteella arvioimaan sitä, täyttääkö tietojärjestelmä tietoturvallisuutta koskevat vaatimukset*;*

21) ***sertifiointielimellä*** *yhdenmukaisten kansainvälisten ja eurooppalaisten arviointiperusteiden mukaisesti akkreditoitua arviointielintä, jonka EU:n asetuksen 765/2008 tuot-*

Voimassa oleva laki	*Ehdotus*
	teiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista mukainen kansallinen akkreditointielin on hyväksynyt.
23 §	23 §
Tietoturvallisen käyttöympäristön suojaaminen	*Tietoturvallisen käyttöympäristön suojaaminen*
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.	Tietoturvallinen käyttöympäristö on suojattava valtion viranomaisten tietoturvallisuutta koskevien velvoitteiden mukaisesti noudattaen, mitä *julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 4 luvussa säädetään ja mitä Tietolupaviranomaisen määräyksessä edellytetään.*
Käyttöympäristön on mahdollistettava lokitietojen kerääminen luovutettujen tietojen käytöstä seurantaa ja valvontaa varten 19 §:n mukaisesti.	Käyttöympäristön on mahdollistettava lokitietojen kerääminen luovutettujen tietojen käytöstä seurantaa ja valvontaa varten 19 §:n mukaisesti.
25 §	25 §
Tietoturvallisen käyttöympäristön tietoturvallisuuden osoittaminen	*Tietoturvallisen käyttöympäristön tietoturvallisuuden osoittaminen*
Käyttöympäristön tietoturvallisuus on osoitettava 26 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla todistuksella.	Käyttöympäristön tietoturvallisuus on osoitettava 26 §:n mukaisella tietoturvallisuuden arviointilaitoksen *tai sertifiointielimen* antamalla todistuksella.
Tietolupaviranomainen voi antaa tarkempia määräyksiä tietoturvallisuuden osoittamisessa noudatettavista menettelyistä.	Tietolupaviranomainen voi antaa tarkempia määräyksiä tietoturvallisuuden osoittamisessa noudatettavista menettelyistä *sekä niistä sertifiointielimistä, jotka voivat arvioida sitä, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset*.
26 §	26 §
Tietoturvallisuuden arviointi	*Tietoturvallisuuden arviointi*
Tietoturvallisuuden arviointilaitos arvioi tämän lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö	Tietoturvallisuuden arviointilaitos arvioi tämän lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö

Voimassa oleva laki	*Ehdotus*
tietoturvallisuutta koskevat vaatimukset. Arviointiperusteina on käytettävä Tietolupaviranomaisen määräyksiä turvalliselle käyttöympäristölle asetettavista vaatimuksista.	tietoturvallisuutta koskevat vaatimukset. *Sertifiointielin arvioi tämän lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset.* Arviointiperusteina on käytettävä Tietolupaviranomaisen määräyksiä turvalliselle käyttöympäristölle asetettavista vaatimuksista.
Jos käyttöympäristö täyttää tämän lain mukaiset tietoturvallisuusvaatimukset, tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan arvioinnista palveluntarjoajalle todistus sekä siihen liittyvä tarkastusraportti. Jos arviointi tai uudelleenarviointi koskee vain käyttöympäristön osaa, arviointilaitoksen antamaan todistukseen on selkeästi merkittävä, mikä osa käyttöympäristöstä on arvioitu.	Jos käyttöympäristö täyttää tämän lain mukaiset tietoturvallisuusvaatimukset, tietoturvallisuuden arviointilaitoksen *tai sertifiointielimen* on annettava suorittamastaan arvioinnista palveluntarjoajalle todistus sekä siihen liittyvä tarkastusraportti. Jos arviointi tai uudelleenarviointi koskee vain käyttöympäristön osaa, arviointilaitoksen *tai sertifiointielimen* antamaan todistukseen on selkeästi merkittävä, mikä osa käyttöympäristöstä on arvioitu.
Arviointilaitoksen myöntämä todistus on voimassa enintään viisi vuotta. Tietoturvallisuuden arviointilaitos voi vaatia palveluntarjoajalta kaikki arvioinnin sekä todistuksen laatimisen ja ylläpitämisen edellytyksenä olevat tiedot. Todistuksen antamiseen sovelletaan muutoin tietoturvallisuuden arviointilaitoksista annetun lain 9 §:n 3 momenttia.	Arviointilaitoksen *tai sertifiointielimen* myöntämä todistus on voimassa enintään *kolme* vuotta. Tietoturvallisuuden arviointilaitos *tai sertifiointielin* voi vaatia palveluntarjoajalta kaikki arvioinnin sekä todistuksen laatimisen ja ylläpitämisen edellytyksenä olevat tiedot. *Arviointilaitoksen todistuksen* antamiseen sovelletaan muutoin tietoturvallisuuden arviointilaitoksista annetun lain 9 §:n 3 momenttia.
27 §	27 §
Arviointilaitoksen myöntämän todistuksen peruuttaminen	*Arviointilaitoksen **ja sertifiointielimen** myöntämän todistuksen peruuttaminen*
Jos tietoturvallisuuden arviointilaitos toteaa, että käyttöympäristö ei ole täyttänyt tai ei enää täytä tässä laissa säädettyjä vaatimuksia tai että todistusta ei muutoin olisi tullut myöntää, laitoksen on kehotettava palveluntarjoajaa korjaamaan puutteet. Arviointilaitos voi peruuttaa todistuksen määräajaksi tai kokonaan taikka myöntää sen rajoitettuna, jollei palveluntarjoaja korjaa puutteellisuuksia arviointilaitoksen asettamassa määräajassa. Määräajan pituutta määritettäessä on otettava huomioon	Jos tietoturvallisuuden arviointilaitos *tai sertifiointielin* toteaa, että käyttöympäristö ei ole täyttänyt tai ei enää täytä tässä laissa säädettyjä vaatimuksia tai että todistusta ei muutoin olisi tullut myöntää, laitoksen *tai sertifiointielimen* on kehotettava palveluntarjoajaa korjaamaan puutteet. Arviointilaitos *tai sertifiointielin* voi peruuttaa todistuksen määräajaksi tai kokonaan taikka myöntää sen rajoitettuna, jollei palveluntarjoaja korjaa puutteellisuuksia arviointilaitoksen *tai sertifiointieli-*

Voimassa oleva laki	*Ehdotus*
käyttöympäristön korjaamiseksi tarvittava kohtuullinen aika.	*men* asettamassa määräajassa. Määräajan pituutta määritettäessä on otettava huomioon käyttöympäristön korjaamiseksi tarvittava kohtuullinen aika.
28 §	28 §
Tietoturvallisuuden arviointilaitoksen ilmoittamisvelvollisuus	*Tietoturvallisuuden arviointilaitoksen **ja sertifiointielimen** ilmoittamisvelvollisuus*
Tietoturvallisuuden arviointilaitoksen on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle tiedot kaikista myönnetyistä, muutetuista, täydennetyistä, määräajaksi tai kokonaan peruutetuista tai evätyistä todistuksista sekä 27 §:n mukaisista kehotuksista ja rajoituksista. Lisäksi tietoturvallisuuden arviointilaitoksen on pyydettäessä annettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle kaikki tarvittavat lisätiedot.	Tietoturvallisuuden arviointilaitoksen *ja sertifiointielimen* on 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 tietoturvallisuuden arviointilaitoksen *ja sertifiointielimen* on pyydettäessä annettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle kaikki tarvittavat lisätiedot.
29 §	29 §
Tietoturvallisen käyttöympäristön käyttöönoton jälkeinen seuranta	*Tietoturvallisen käyttöympäristön käyttöönoton jälkeinen seuranta*
Palveluntarjoajan on seurattava ja arvioitava ajantasaisella järjestelmällisellä menettelyllä tietoturvallisesta käyttöympäristöstä sen tuotantokäytön aikana saatavia kokemuksia. Palveluntarjoajan on seurattava tämän lain muutoksia ja tehtävä käyttöympäristöön muutosten edellytyksenä olevat korjaukset. 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.	Palveluntarjoajan on seurattava ja arvioitava ajantasaisella järjestelmällisellä menettelyllä tietoturvallisesta käyttöympäristöstä sen tuotantokäytön aikana saatavia kokemuksia. Palveluntarjoajan on seurattava tämän lain ja Tietolupaviranomaisen määräyksen muutoksia ja tehtävä käyttöympäristöön muutosten edellytyksenä olevat korjaukset. Käyttöympäristön olennaisista muutoksista on ilmoitettava tietoturvallisuuden arviointilaitokselle *tai sertifiointielimelle*. Arviointilaitoksen *tai sertifiointielimen* myöntämä todistus on uudistettava, jos käyttöympäristöön tehdään merkittäviä muutoksia tai jos käyttöympäristöä koskevia vähimmäisvaatimuksia on muutettu tavalla, jonka edellytyksenä on uusi arviointi.
Palveluntarjoajan on säilytettävä vaatimustenmukaisuutta koskevat ja muut valvonnan edellytyksenä olevat tiedot vähintään viisi vuotta tietoturvallisen käyttöympäristön tuotantokäytön päättymisestä.	Palveluntarjoajan on säilytettävä vaatimustenmukaisuutta koskevat ja muut valvonnan edellytyksenä olevat tiedot vähintään viisi

Voimassa oleva laki

30 §

Tietojärjestelmien valvonta ja tarkastukset

Sosiaali- ja terveysalan lupa- ja valvontaviraston tehtävänä on valvoa ja edistää sitä, että tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. Sosiaali- ja terveysalan lupa- ja valvontavirasto ylläpitää julkista rekisteriä sille ilmoitetuista, vaatimukset täyttävistä käyttöympäristöistä.

Sosiaali- ja terveysalan lupa- ja valvontavirastolla on oikeus tehdä valvonnan edellytyksenä olevia tarkastuksia. Tarkastuksen suorittamiseksi tarkastajalla on oikeus päästä kaikkiin tiloihin, joissa harjoitetaan tässä laissa tarkoitettua toimintaa tai säilytetään tämän lain noudattamisen valvonnan kannalta merkityksellisiä tietoja. Tarkastusta ei kuitenkaan saa tehdä pysyväisluonteiseen asumiseen käytettävissä tiloissa.

Tarkastuksessa on esitettävä kaikki tarkastajan pyytämät asiakirjat, jotka ovat tarpeellisia tarkastuksen toimittamiseksi. Lisäksi tarkastajalle on annettava maksutta hänen pyytämänsä jäljennökset tarkastuksen toimittamiseksi tarpeellisista asiakirjoista.

Sosiaali- ja terveysalan lupa- ja valvontaviraston on säilytettävä tarkastuksesta laadittava tarkastuskertomus kymmenen vuoden ajan tarkastuksen suorittamisesta.

Ehdotus

vuotta tietoturvallisen käyttöympäristön tuotantokäytön päättymisestä.

30 §

Tietojärjestelmien valvonta ja tarkastukset

Sosiaali- ja terveysalan lupa- ja valvontaviraston tehtävänä on valvoa ja edistää sitä, että tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset. *Sertifiointielimien tehtävänä on valvoa ja edistää sitä, että niiden arvioimat tietoturvalliset käyttöympäristöt täyttävät tietosuojaa ja tietoturvaa koskevat vaatimukset*. Sosiaali- ja terveysalan lupa- ja valvontavirasto ylläpitää julkista rekisteriä sille ilmoitetuista, vaatimukset täyttävistä käyttöympäristöistä.

Sosiaali- ja terveysalan lupa- ja valvontavirastolla on oikeus tehdä valvonnan edellytyksenä olevia tarkastuksia. Tarkastuksen suorittamiseksi tarkastajalla on oikeus päästä kaikkiin tiloihin, joissa harjoitetaan tässä laissa tarkoitettua toimintaa tai säilytetään tämän lain noudattamisen valvonnan kannalta merkityksellisiä tietoja. Tarkastusta ei kuitenkaan saa tehdä pysyväisluonteiseen asumiseen käytettävissä tiloissa.

Tarkastuksessa on esitettävä kaikki tarkastajan pyytämät asiakirjat, jotka ovat tarpeellisia tarkastuksen toimittamiseksi. Lisäksi tarkastajalle on annettava maksutta hänen pyytämänsä jäljennökset tarkastuksen toimittamiseksi tarpeellisista asiakirjoista.

Sosiaali- ja terveysalan lupa- ja valvontaviraston on säilytettävä tarkastuksesta laadittava tarkastuskertomus kymmenen vuoden ajan tarkastuksen suorittamisesta.

Sosiaali- ja terveysalan lupa- ja valvontaviranomainen voi antaa tarkempia määräyksiä tietoturvallisten käyttöympäristöjen valvonnasta.

Voimassa oleva laki	*Ehdotus*
52 §	52 §
Tietoluvan nojalla luovutetuista tiedoista johdettujen tulosten julkaiseminen	*Tietoluvan nojalla luovutetuista tiedoista johdettujen tulosten julkaiseminen*
Kun tietoluvan nojalla on luovutettu tietoja käsiteltäviksi 20 §:ssä tarkoitetussa tietoturvallisessa käyttöympäristössä ja niiden pohjalta tuotettuja tuloksia halutaan julkaista, vastaa Tietolupaviranomainen 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.	Kun tietoluvan nojalla on luovutettu tietoja käsiteltäviksi 20 §:ssä tarkoitetussa tietoturvallisessa käyttöympäristössä ja niiden pohjalta tuotettuja tuloksia halutaan julkaista, vastaa Tietolupaviranomainen 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.
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.	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.
	Tietolupaviranomainen voi antaa tarkempia määräyksiä julkaistavien tietojen anonymisoinnin varmistamisesta.
	Tämä laki tulee voimaan päivänä kuuta 20 .