Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain siirtymäsäännöstä siten, että lain tietoturvalliselta käyttöympäristöltä edellytettäviä vaatimuksia sovellettaisiin vasta 1 päivästä toukokuuta 2022. Ennen mainittua ajankohtaa tietoja voitaisiin kuitenkin luovuttaa luvansaajan käsiteltäväksi lain nojalla, vaikka tietolupahakemuksessa ei osoitettaisi laissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle. Tietojen luovuttaminen edellyttäisi tällöin määräajaksi annettua tietolupaa, joka olisi voimassa enintään 30 päivään huhtikuuta 2022. Lisäksi siirtymäsäännöstä esitetään muutettavaksi siten, että lain merkittäviin kliinisiin löydöksiin perustuvia oikeuksia, velvoitteita ja toimenpiteitä sovellettaisiin 1 päivästä tammikuuta 2024.

Laki on tarkoitettu tulemaan voimaan mahdollisimman pian.

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Pääministeri Sanna Marinin hallituksen ohjelman 2019 tavoitteena on, että Suomi on kansainvälisesti houkutteleva paikka opiskella, tutkia ja investoida.

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019, jäljempänä toisiolaki) on tullut voimaan 1.5.2019.

Toisiolain tarkoituksena on luoda ajanmukaiset ja yhdenmukaiset 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 nykyistä laajemman sosiaali- ja terveydenhuollon asiakas- ja potilastiedon hyödyntämisen muussa kuin kyseisen tiedon alkuperäisessä käyttötarkoituksessa sosiaali- ja terveydenhuollon palvelujärjestelmässä.

Toisiolain keskeinen päätavoite edellä kuvatun tiedon laajemman hyödyntämisen ohella 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. Tämä vahvistaa osaltaan myös luottamusta sosiaali- ja terveydenhuollon palvelujärjestelmään yleisesti.

Sosiaali- ja terveysvaliokunta on mietinnössään (StVM 37/2018 vp) pitänyt välttämättömänä, että sosiaali- ja terveydenhuollon arkaluonteisia henkilötietoja käsitellään tietoturvallisesti siten, että ne eivät paljastu sivullisille. Sosiaali- ja terveysalan tietolupaviranomaisen (jäljempänä Tietolupaviranomainen) perustamisessa sekä ehdotettujen lakien toimeenpanossa tulee valiokunnan näkemyksen mukaan hyödyntää tarvittavaa korkean tason osaamista siten, että huomioidaan teknologian kehitys. Tietolupaviranomaisen käynnistäminen sekä toiminnan suunnittelu tulee sosiaali- ja terveysvaliokunnan näkemyksen mukaan toteuttaa siten, että siinä turvataan korkeatasoinen tietosuojan ja tietoturvan osaaminen sekä kokonaisuudessaan riittävät voimavarat.

Sosiaali- ja terveysvaliokunta on edellä mainitussa 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.

Tietoturvallinen käyttöympäristö on toisiolain hallituksen esitykseen (HE 159/2017 vp) kirjoitettu keskeinen toimi, joka turvaa yksilön henkilötietojen suojaa. Tietoturvallisella käyttöympäristöllä on merkittävä rooli väärinkäytösten estämisessä ja kyberturvallisuuden toteuttamisessa. Se on myös kilpailuetu Suomelle, koska voimme siten osoittaa, että täällä huolehditaan vahvasti

arkaluonteisten henkilötietojen suojasta.[1] Myös 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 *yleinen tietosuoja-asetus*) edellytetään riittäviä suojatoimia, kun käsitellään arkaluonteisia henkilötietoja.

Toisiolain 60 §:n 1 momentissa säädetään siirtymäajasta, jonka jälkeen Tietolupaviranomainen voisi luovuttaa luvansaajalle tunnisteellisia tietoja vain 20 §:n 3 momentissa tarkoitettuun tietoturvalliseen käyttöympäristöön käsiteltäviksi. 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. Sanotun pykälän 3 momentin mukaan, jos tietolupahakemuksessa pyydetään luovuttamaan tietoaineistoja käsiteltäviksi muussa kuin 1 momentissa tarkoitetussa 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.

Tunnisteellisia henkilötietoja luovutetaan tyypillisesti tutkimustarkoituksissa yhdistettäviksi terveydenhuollon potilasasiakirjoissa oleviin tietoihin. Tällöin niitä usein käsitellään toimintayksikön omissa, tutkijoille tarkoitetuissa tietojärjestelmissä, joissa ei toistaiseksi ole toteutettuna kaikkia edellytettyjä tietosuoja- ja turvavaatimuksia. Siirtymäajan tarkoitus oli turvata se, ettei terveydenhuollon tutkimus tyrehdy lain voimaantultua. Asianomaisten toimintayksiköiden olisi kuitenkin velvollisuus huolehtia, että tutkijoiden käyttämät tietojärjestelmät vastaavat viimeistään siirtymäajan päätyttyä 20 §:n 3 momentissa asetettuja vaatimuksia.

Lain valmistelun yhteydessä arvioitiin, että tietoturvallisten käyttöympäristöjen rakentaminen veisi hyväksymisen jälkeen noin kaksi vuotta ja siirtymäajaksi esitettiin 1.5.2021, joka on nyt myös toisiolain 60 §:ssä säädetty siirtymäaika.

Tietolupaviranomaiselta saadun tiedon mukaan 1.5.2021 mennessä ei kenelläkään toimijalla, Tietolupaviranomaista itseään lukuun ottamatta, ole toisiolain 20 §:n edellyttämää tietoturvallista käyttöympäristöä, jonne tietoaineistoja voisi luovuttaa luvansaajan käsiteltäväksi. Myöskään ulkomaisilla toimijoilla ei ole kattavaa tietoa tästä auditointivelvoitteesta, eikä kukaan ulkomainen toimija ole ryhtynyt auditoimaan omia järjestelmiä toisiolain mukaisiksi. Tietolupaviranomaisen käyttöympäristö ei myöskään vielä pysty käsittelemään kaikkea sellaista tietoaineistoa, joita erityisesti lääketieteen tutkimuksessa olisi tarve käsitellä. Esimerkkinä voi mainita terveydenhuollon kuvantamisaineistot (esimerkiksi röntgenkuvat, ultraäänikuvat ja EKG-tallenteet), jotka kuuluvat aineistona toisiolain soveltamisalan piiriin. Kuvantamisaineistot edellyttävät käytännössä 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. Tämänkin vuoksi on tärkeää, että muun muassa merkittävimmät terveydenhuollon toimijat Suomessa ehtivät auditoida omat käyttöympäristöt vaatimuksia vastaaviksi ja siten pystyvät käsittelemään näitä erityisiä tietoaineistoja myös omissa ympäristöissään.

[1] ks. asiantuntijalausunto tietoturvasta https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-229672.pdf

Toisiolain 55 §:n mukaan tietoluvan saajalla on oikeus ilmoittaa Tietolupaviranomaisen nimeämälle vastuuhenkilölle kliinisesti merkittävästä löydöksestä, jonka perusteella olisi mahdollista ehkäistä tietyn potilaan terveyteen liittyvää riskiä tai parantaa merkittävästi hoidon laatua.

Jos ilmoituksen perusteena olevat tiedot ovat pseudonymisoituja, sanotun vastuuhenkilön on selvitettävä, ketä tai keitä tieto koskee. Kun Tietolupaviranomaisen vastuuhenkilöllä on tiedossaan henkilö tai henkilöt, joita ilmoitus koskee, vastuuhenkilön on toimitettava ilman aiheetonta viivytystä tiedot Terveyden ja hyvinvoinnin laitoksen nimeämälle asiantuntijalle. Asiantuntijan on yhteistyössä laitoksen nimeämien muiden asiantuntijoiden kanssa arvioitava tiedon merkittävyys ja sen pohjalta toteutettavissa olevien toimenpiteiden odotettavissa oleva hyöty. Jos hyöty arvioidaan niin ilmeiseksi, että tutkittava olisi tärkeää saada hoidon piiriin, Terveyden ja hyvinvoinnin laitoksen asiantuntijan on ilmoitettava löydöksestä kunkin henkilön terveydenhuollosta alueellisesti terveydenhuoltolain (1326/2020) nojalla vastuussa olevalle toimintayksikölle. Toimintayksikön on otettava yhteys potilaaseen ja selvitettävä, haluaako tämä tiedon kliinisesti merkittävästä löydöksestä ja sen perusteella mahdollisesti tehtävistä tutkimus- ja hoitotoimenpiteistä sekä niistä odotettavissa olevasta hyödystä.

Potilaalla on oikeus kieltää kliinisesti merkittävän löydöksen perusteella tehtävät yhteydenotot. Kielto kirjataan asiakastietolain 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun. Potilas voi tehdä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toimintayksikössä taikka sähköisesti asiakastietolain 19 §:ssä tarkoitetun kansalaisen käyttöliittymän välityksellä.

Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tutkijoiden tietoturvallisiin käyttöympäristöihin, lain edellyttämiä muutokset olisi perusteltua yhdistää uuden asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koskeviin muutosehdotuksiin. Muutoksia ei ole tehty, mutta muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan 1. päivänä tammikuuta 2024.[2]

1.2 Valmistelu

Hallituksen esitys on valmisteltu sosiaali- ja terveysministeriön ja Tietolupaviranomaisen sisäisenä virkamiestyönä.

Sosiaali- ja terveysministeriö järjesti 12.4.2021 kuulemistilaisuuden keskeisille toisiolain rekisterinpitäjille ja viranomaisille, jossa esiteltiin toisiolain 60 §:n 1 momentin siirtymäsäännökseen esitettävät muutokset. Kuulemistilaisuuteen osallistui 68 henkilöä. Kuulemistilaisuuden lisäksi luonnoksesta hallituksen esitykseksi on voinut antaa kirjallisen lausunnon 13.4.2021 mennessä. Lausuntoja esitykseen saapui yhteensä 28 kappaletta.

[2] Kelan ja THL:n näkemyksen mukaan kyseessä on todella laaja uusi prosessi, jossa on monia toimijoita ja työkaluja (Findata, tutkijat, uusi tutkijoiden käyttöliittymä, kansalaiset, Kanta-palvelut, terveydenhuolto, potilastietojärjestelmät). Terveydenhuoltoon ja valtakunnallisiin tietojärjestelmäpalveluihin kohdistuu seuraavana kahtena vuonna lukuisia muita lainsäädännön toimeenpanovaatimuksia mm. asiakastietolain muutosten toimeenpano, henkilötunnusuudistus 1.1.2023 mennessä sekä sote-uudistuksen edellyttämä toimeenpano.

Hallituksen esityksen valmisteluasiakirjat ovat julkisessa palvelussa osoitteessa https://stm.fi/hanke?tunnus=STM047:00/2021.

2 Nykytila ja sen arviointi

Yleisen tietosuoja-asetuksen 42 artiklan mukaisia hyväksyttyjä tietosuojasertifiointimekanismeja ei vielä ole käytössä. Auditointia voidaan kuitenkin pitää esiasteena tietoturvaa tai tietosuojaa koskevan sertifikaatin hankkimiseksi. Sertifikaatti toimii todistuksena sekä sovellettavien standardien että auditoinnissa käytettyjen kriteerien ja vaatimusten täyttämisestä. Näiden käyttöä olisi syytä kannustaa eri toimialoilla täydentämään rekisterinpitäjän sisäistä valvontaa ja viranomaisvalvontaa vastaavalla tavalla kuin nyt käytetään tietoturva-auditointeja.[3]

Suomessa hyödynnetään muun muassa kansallista turvallisuusauditointikriteeristöä Katakria. Katakri-kriteeristö itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvavelvoitteisiin. Vaikka Katakri-kriteeristöä käytetään ensisijaisesti turvallisuusluokitellun tiedon käsittelyn arviointien yhteydessä, kriteeristöä voidaan hyödyntää myös yksityisen ja julkisen sektorin muussa turvallisuustyössä ja sen kehittämisessä. Lisäksi Kyberturvallisuuskeskus on laatinut pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri), jonka tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa.

Myös terveydenhuollon B-luokan järjestelmien auditointi on vähäistä. Auditointien vähäinen käyttöaste osalla toimialoista on vaikuttanut siihen, että prosessien, toimintojen ja tietojärjestelmien tietoturvallisuuden taso voi vaihdella merkittävästi eri toimialoilla. Prosessien ja toimintojen auditoinnin pitäisi olla luonnollinen osa kriittisten toimialojen riskinhallintaa.

Auditointien määrän lisääminen edellyttää sääntelyn tarkastelun ohella toimintakulttuurin muutosta niin julkisella kuin yksityisellä sektorilla. Kaikki auditointitoiminta edellyttää toiminnan kohteelta rahallisia panostuksia. Tämän osalta tulee kuitenkin huomioida, että auditoinnin yksityiskohtaisuus ja tarkistettavan kohteen laajuus vaikuttavat suoraan kyseessä olevan auditoinnin kustannuksiin. Näin ollen yksittäisten, kriittisiksi tunnistettujen, tietojärjestelmien tai prosessien auditoinnit ovat kokoluokaltaan moninkertaisesti pienempiä panostuksia kuin suuryrityksen tai kunnan digitaalisen palveluympäristön laajamittainen auditointi.

Tietoturvaa koskevia auditointeja tekevät Suomessa Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, erikseen hyväksytyt arviointilaitokset (muun muassa KPMG ja Nixu), eräät tietoturvayritykset ja organisaatioiden sisäiset riippumattomat toimijat. Korkeimmasta tarkastusta-

[3] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla työryhmän loppuraportti https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162783/LVM_2021_1.pdf?sequence=1&isAllowed=y. Työryhmässä on arvioitu, että myös tietosuojaa koskevien arviointien osalta erityisesti yleisen tietosuoja-asetuksen mukaisten tietosuojan sertifiointimekanismien käyttöä olisi mahdollista lisätä. Loppuraportissa todetaan, että ”ulkopuolisten sertifiointielinten myöntämät tietosuojasertifioinnit olisivat yksi tietosuoja-asetuksen mukainen keino rekisterinpitäjän osoittaa, että tietosuoja-asetusta ja erityisesti käsittelyn turvallisuuteen liittyviä vaatimuksia noudatetaan. Ulkopuolisten riippumattomien sertifiointielinten tekemät arviot lisäisivät toiminnan uskottavuutta, laajentaisivat merkittävästi kyvykkyyksiä arvioida säännösten mukaisuutta (valvontaa) ja samalla se toisi rekisterinpitäjille tärkeää osaamista tietosuojan kehittämiseen. Tämä edellyttäisi sertifiointielinten akkreditointia, joka on tietosuojavaltuutetun tehtävä, sekä tietosuojan sertifioinnin liiketoiminnan käynnistämistä.”

sosta vastaavat Kyberturvallisuuskeskus ja erikseen hyväksytyt arviointilaitokset, joita on Suomessa tällä hetkellä vain muutamia. Toimijoiden omavalvonta ja sisäset riippumattomat auditoinnit ja tarkastukset eivät vastaa ulkopuolisen arviointilaitoksen tekemää tarkastusta, mutta ne voidaan nähdä yhtenä lisäkeinona tietoturvan ja tietosuojan parantamiseksi. Lisäksi yksityisen sektorin toimijoilta on mahdollista hankkia erilaisia koulutus- ja konsultointipalveluita tietoturvan ja tietosuojan parantamiseksi.

Toisiolain 24 §:n mukaan tietoturvallisen käyttöympäristön on täytettävä tietoturvaa ja tiedonsiirron yhteentoimivuutta koskevat vaatimukset, jotka perustuvat viranomaisten antamiin määräyksiin, suosituksiin ja näiden osoittamiin, tietoturvalliseen käyttöympäristöön soveltuviin standardeihin. Tietolupaviranomainen antaa tarkemmat määräykset muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista. Vaatimuksissa on edellytettävä vastaavaa tietoturvan tasoa kuin Tietolupaviranomaisen omassa käyttöympäristössä vaaditaan. Toisiolain 25 §:n mukaan käyttöympäristön tietoturvallisuus on osoitettava toisiolain 26 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Tietolupaviranomainen voi antaa tarkempia määräyksiä tietoturvallisuuden osoittamisessa noudatettavista menettelyistä.

Tietolupaviranomainen antoi toisiolain mukaisen määräyksen (1/2020) tietoturvallisista käyttöympäristöistä 5.10.2020.[4] Tietolupaviranomaiselta saadun tiedon mukaan tämän jälkeen määräystä ja sen toimeenpanoon liittyviä toisiolain edellyttämiä toimia on käyty loppuvuoden 2020 aikana läpi Liikenne- ja viestintäviraston (Traficom) ja Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) kanssa. Tietolupaviranomaisen mukaan tämä yhteinen läpikäynti on ollut tarpeen, jotta Traficom on pystynyt muokkaamaan omaa ohjeistustaan arviointilaitoksille ja ottamaan huomioon ohjeistuksessa uuden määräyksen. Valvira on tarvinnut tiedon määräyksen sisällöstä, jotta se on pystynyt viemään eteenpäin tietoturvallisten käyttöympäristöjen julkista rekisteriä. Tietolupaviranomaisen mukaan on tarvittu yhteistä läpikäyntiä ja yhteydenpitoa arviointilaitoksiin. Arviointilaitosten kanssa on ollut tarve käydä uutta määräystä läpi, jotta syntyy käsitys siitä, mitä määräyksen sisältämät vaatimukset tarkoittavat auditoinnille.

Tämä kuvattu läpikäynti on kestänyt noin 4 kuukautta. Se on ollut välttämätöntä määräyksen täytäntöönpanoon kannalta. Sitä ei myöskään olisi voitu aloittaa ennen kuin Tietolupaviranomainen olisi antanut määräyksen ja ennen kuin olisi ollut tiedossa, minkälaisia vaatimuksia määräys sisältäisi. Valmistelun aikana syntyi myös perustellumpi käsitys, minkälainen työmäärä vaaditaan sekä kuinka kauan auditointi uuden määräyksen perusteella ennakoidaan kestävän. Ainakin osa vaatimuksista ovat uusia auditoiville arviointilaitoksille, koska määräys sisältää sellaisia vaatimuksia, joita ei esimerkiksi ole sisällytetty nykyisiin sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007, jäljempänä *asiakastietolaki*) mukaisiin terveydenhuollon A-luokan tietojärjestelmien vaatimuksiin. Tietolupaviranomaiselta saadun tiedon mukaan arviointilaitokset ovat arvioineet, että määräyksen mukainen auditointi kestää noin kaksi kalenterikuukautta. Auditointi edellyttää myös valmistautumista ennen kuin varsinaiseen auditointiin voidaan ryhtyä. Muun muassa tekniset kuvaukset ja dokumentaatiot tulee olla laadittuna, riittävän kattavia ja ne tulee arkistoida. Auditoitavan toimijan tulee myös itse käydä läpi määräyksen vaatimukset ja varmistaa, että sen toimintatavat ovat määräyksen mukaisia. Vasta tämän jälkeen voidaan ryhtyä varsinaiseen auditointiin.

[4] https://www.findata.fi/uploads/2020/10/20ddc0dd-findata-maarays-1-2020-muiden-palveluntarjoajien-tietoturvallisille-kayttoymparistoille-asetettavat-vaatimukset.pdf

Tietolupaviranomainen on myöntänyt tietolupia 1.4.2020 alkaen yksilötasoiseen aineistoon. Lupaharkinnassa on otettu huomioon, että Tietolupaviranomaisen oma käyttöympäristö on ensisijainen ympäristö, jonne tietoaineistoja voi luovuttaa. Siirtymäajan aikana on kuitenkin mahdollista luovuttaa tietoaineisto myös muuhun kuin Tietolupaviranomaisen ympäristöön. Laissa ei ole erityisiä säännöksiä siitä, missä tilanteissa tai millä perustein tietoaineisto voidaan siirtymäajan voimassa ollen luovuttaa muualle kuin Tietolupaviranomaisen ympäristöön. Toisiolain mukaan ennen 1.5.2021 tietoja voidaan luovuttaa luvansaajan käsiteltäväksi, vaikka tietolupahakemuksessa ei osoitettaisi lain 20 §:n 3 momentissa ja 21–34 §:ssä tietoturvalliselta käyttöympäristöltä edellytettäviä vaatimuksista tietojen käsittelylle. Toisiolain 43 §:n 4 momentin mukaan lupa voidaan antaa, jos on ilmeistä, ettei tiedon antaminen loukkaa niitä etuja, joiden suojaksi salassapitovelvollisuus on säädetty. Lupaan on lisäksi liitettävä tietojen käsittelyn suojaustoimenpiteitä koskevat riskien mukaiset vaatimukset ja muut yksityisen edun suojaamiseksi tarpeelliset määräykset. Toisiolain 18 § sisältää yleiset tietoturvavaatimukset, jotka ovat olleet voimassa jo heti lain voimaantultua. Sen mukaan, kun henkilötietoja käsitellään tämän lain nojalla, 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.

Lainsäädäntö sisältää siten vaatimuksia tietoturvasta ja -suojasta ja näiden varmistamisesta myös siirtymäajalle. Samanaikaisesti Tietolupaviranomaisen on otettava huomioon lain toinen tavoite, joka on ollut tutkimustoiminnan turvaaminen ja lupakäytäntöjen nopeuttaminen. Tietolupaviranomainen on luovuttanut tietoaineistoja muuhun kuin sen omaan käyttöympäristöön seuraavissa tilanteissa:

- Jos kyseessä on ollut jo käynnissä oleva tutkimushanke, jossa on haettu Tietolupaviranomaiselta esimerkiksi jatkoaikaa. Tietolupaviranomainen myöntää jatkoajan tilanteessa, joissa alkuperäinen tutkimuslupa on koskenut useiden rekisterinpitäjien aineistoja. Näissä tilanteissa aineisto sijaitsee jo jossakin käyttöympäristössä, sen mukaan kuin mitä alkuperäinen lupa tai luvat ovat määritelleet.

- Tietolupaviranomainen ei ole edellyttänyt, että jatkoajan vuoksi tutkimusaineisto tulisi siirtää toiseen paikkaan, siis tietolupaviranomaisen ympäristöön. Myös sensitiivisten tietoaineistojen siirto tai liikuttelu muodostaa itsessään riskiä tietoturvalle ja -suojalle. Tutkimusaineistot voivat olla hyvinkin laajoja, ja osa aineistoista voi olla myös paperisia muodoltaan. Tietolupaviranomainen ei käsittele paperia, vaan sen käsittely pohjautuu täysin sähköiseen käsittelyyn ja siihen, että aineistot ovat sähköisiä.

- Tietolupaviranomainen on antanut luvan tietoaineistojen käsittelyyn myös silloin, kun luvansaajana on toiminut ja tietojen sijaintipaikkana on ollut terveydenhuollon toiminnanharjoittaja. Tällaisella toimijalla on jo itsellään hallinnassa merkittäviä määriä sensitiivistä tietoa, ja sitä koskevat myös muun lainsäädännön vaatimukset tietojen tietoturvallisesta käsittelystä. Lisäksi on voinut olla kyse kuvantamisaineistoista, joita ei voida käsitellä Tietolupaviranomaisen omassa käyttöympäristössä.

Tietolupaviranomainen ei ole antanut tietolupaa tietojen käyttöön, jos se on harkinnut saamiensa tietojen pohjalta, että tietojen käsittely ehdotetussa paikassa aiheuttaisi liian suurta riskiä tietoturvalle tai -suojalle. Tällaisia tapauksia on voinut olla esimerkiksi silloin, jos luvanhakija on ilmoittanut, että aineistoa pidetään usb-muistitikuilla tutkimuksen harjoittajan työhuoneessa. Tilanteissa, joissa tietoaineistoa on haluttu siirtää ulkomaille, on Tietolupaviranomainen harkinnut tapaus kerrallaan, miltä tilanne näyttää tietosuojan ja tietoturvan kannalta.

Lain valmistelun yhteydessä arvioitiin, että tietoturvallisten käyttöympäristöjen rakentaminen veisi hyväksymisen jälkeen noin kaksi vuotta ja siirtymäajaksi esitettiin 1.5.2021. Tietolupaviranomaiselta saadun tiedon mukaan 1.5.2021 mennessä ei kenelläkään toimijalla, Tietolupaviranomaista itseään lukuun ottamatta, ole toisiolain 20 §:n edellyttämää tietoturvallista käyttöympäristöä, jonne tietoaineistoja voisi luovuttaa luvansaajan käsiteltäväksi. Nykyinen tilanne johtaa siihen, että 1.5.2021 alkaen usea tutkimus uhkaa loppua tai muuttua mahdottomaksi, koska ei ole tietoturvallisia käyttöympäristöjä, jonne tietoaineiston voisi tietoluvan perusteella luovuttaa. Tietolupaviranomaisen käyttöympäristö ei kuitenkaan vielä pysty käsittelemään kaikkea sellaista tietoaineistoa, joita erityisesti lääketieteen tutkimuksessa olisi tarve käsitellä. Esimerkkinä voi mainita terveydenhuollon kuvantamisaineistot (esimerkiksi röntgenkuvat), jotka kuuluvat aineistona toisiolain soveltamisalan piiriin. Kuvantamisaineistot edellyttävät käytännössä 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. Tämänkin vuoksi on tärkeää, että muun muassa merkittävimmät terveydenhuollon toimijat Suomessa ehtivät auditoida omat käyttöympäristöt vaatimuksia vastaaviksi ja siten pystyvät käsittelemään näitä erityisiä tietoaineistoja myös omissa ympäristöissään. Asiantuntija-arvioiden mukaan tämä voisi tapahtua 1.5.2022 mennessä. Lisäksi erityisesti kansainvälisten tutkimusten turvaamista ja tietoturvaa koskevat haasteet on tuotu esille hallituksen esityksen kohdassa toimeenpano ja seuranta.

Toisiolain 55 §:n mukaan tietoluvan saajalla on oikeus ilmoittaa Tietolupaviranomaisen nimeämälle vastuuhenkilölle kliinisesti merkittävästä löydöksestä, jonka perusteella olisi mahdollista ehkäistä tietyn potilaan terveyteen liittyvää riskiä tai parantaa merkittävästi hoidon laatua.

Potilaalla on oikeus kieltää kliinisesti merkittävän löydöksen perusteella tehtävät yhteydenotot. Kielto kirjataan asiakastietolain 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun. Potilas voi tehdä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toimintayksikössä taikka sähköisesti asiakastietolain 19 §:ssä tarkoitetun kansalaisen käyttöliittymän välityksellä.

Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tutkijoiden käyttämiin tietoturvallisiin käyttöympäristöihin, lain edellyttämät muutokset eivät ole valmiita 1.5.2021 mennessä vaan edellyttävät paljonenemmän työtä ja aikaa. Muutokset olisi lisäksi perusteltua yhdistää uuden asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koskeviin muutosehdotuksiin. Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan muutokset olisi toteutettavissa aikaisintaan siten, että toisiolain 55 § voisi astua voimaan 1. päivänä tammikuuta 2024.

3 Tavoitteet

Esityksen tavoitteena on, että toisiolain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sovellettaisiin vasta, kun alan keskeiset toimijat ovat voineet ilman aiheetonta viivytystä auditoida tietoturvalliset käyttöympäristönsä. Hallituksen näkemyksen mukaan tämä tulee tapahtua etupainotteisesti ilman aiheetonta viivytystä, mutta kuitenkin viimeistään 1 päivästä toukokuuta 2022. On oletettava, että viimeistään silloin alan toimijoiden tietoturvalliset käyttöympäristöt on auditoitu toisiolain edellyttämällä tavalla siten, että luvansaajan auditoituun tietoturvalliseen käyttöympäristöön tietoaineistoja voisi luovuttaa toisiolain mukaisesti. Ennen mainittua ajankohtaa tietoja voitaisiin kuitenkin luovuttaa luvansaajan käsiteltäväksi toisiolain 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä

tietojen käsittelylle. Tietojen luovuttaminen edellyttäisi tällöin 43 §:n 4 momentin nojalla määräajaksi annettua tietolupaa, joka on voimassa enintään 30 päivään huhtikuuta 2022. Tämä sen takia, jotta voitaisiin varmistaa, että siirtymäajan jälkeen tietoaineistojen käsittely tapahtuisi vain tietoturvallisissa käyttöympäristöissä. Toisaalta siirtymäajan aikanakin tietoaineistoja voisi luovuttaa lain 43 §:n 4 momentin mukaisella tietoluvalla käyttöympäristöön, jos jo täyttäisi tietoturvalliselta käyttöympäristöltä edellytettävät vaatimukset.

Sen sijaan toisiolain 60 §:n 1 momentissa olevaa siirtymäaikaa koskien lain 19 §:ää lokitiedoista ei tässä yhteydessä esitetä muutettavaksi. Lokitietoja koskeva vaatimus on keskeinen keino, joilla rekisteröity, rekisterinpitäjä ja viranomaiset voivat seurata ja valvoa henkilötietojen käsittelyä. Lisäksi vastaava velvoite koskee viranomaisia jo julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, jäljempänä tiedonhallintalaki) perusteella.[5] Tietolupaviranomainen itse kerää edellä mainittua lokitietoa.

Koska toisiolain 55 §:n merkittäviin kliinisiin löydöksiin perustuvien oikeuksien, velvoitteiden ja toimenpiteiden täytäntöönpano edellyttää muutoksia myös potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvallisiin käyttöympäristöihin, lain edellyttämiä muutoksia ei ole mahdollista toteuttaa 1.5.2021 mennessä. Muutokset olisivat lisäksi perusteltua yhdistää uuden asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koskeviin muutosehdotuksiin. Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan muutokset olisi tehtävissä siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Keskeisenä ehdotuksena on, että toisiolain 60 §:n 1 momentin siirtymäsäännöstä muutetaan siten, että toisiolain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sovellettaisiin vasta, kun alan keskeiset toimijat ovat voineet ilman aiheetonta viivytystä auditoida tietoturvalliset käyttöympäristönsä.

Tietoturvallinen käyttöympäristö on toisiolain hallituksen esitykseen kirjoitettu keskeinen toimi, joka turvaa yksilön henkilötietojen suojaa. Tietoturvallisella käyttöympäristöllä on merkittävä rooli väärinkäytösten estämisessä ja kyberturvallisuuden toteuttamisessa. Se on myös kilpailuetu Suomelle, koska voimme siten osoittaa, että täällä huolehditaan vahvasti arkaluonteisten henkilötietojen suojasta. Myös yleisessä tietosuoja-asetuksessa edellytetään riittäviä suojatoimia, kun käsitellään arkaluonteisia henkilötietoja.

Hallituksen näkemyksen mukaan tämä tulee tapahtua etupainotteisesti ilman aiheetonta viivytystä, mutta kuitenkin viimeistään 1 päivästä toukokuuta 2022. On oletettava, että viimeistään silloin alan keskeisten toimijoiden tietoturvalliset käyttöympäristöt on auditoitu toisiolain edellyttämällä tavalla siten, että luvansaajan auditoituun tietoturvalliseen käyttöympäristöön tietoaineistoja voisi luovuttaa toisiolain mukaisesti. Ennen mainittua ajankohtaa tietoja voitaisiin kuitenkin luovuttaa luvansaajan käsiteltäväksi toisiolain 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvallista

[5] Ko. hallituksen esityksen (HE 284/2018 vp) valmistelussa tuotiin kuitenkin lokitietojen keräämisen osalta lausunnoissa esille, että ehdotettu vaatimus lokitietojen keräämisestä, jos tietojärjestelmässä käsitellään henkilötietoja tai salassa pidettäviä tietoja, on kohtuuttoman raskas ja kallis vaatimus toteuttaa nykyisiin tietojärjestelmiin.

käyttöympäristöä tietojen käsittelylle. Tietojen luovuttaminen edellyttäisi tällöin 43 §:n 4 momentin nojalla määräajaksi annettua tietolupaa, joka on voimassa enintään 30 päivään huhtikuuta 2022. Tämä sen takia, jotta voitaisiin varmistaa, että siirtymäajan jälkeen tietoaineistojen käsittely tapahtuisi vain tietoturvallisissa käyttöympäristöissä. Myös siirtymäajan aikana tietoaineistoja voidaan käsitellä tietoturvallisessa käyttöympäristössä määräaikaisen tietoluvan, jonka voimassa oloa ei kuitenkaan ole rajoitettu, perusteella.

Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan, koska toisiolain 55 §:n sekä 21-29 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvallisiin käyttöympäristöihin, lain edellyttämiä muutokset edellyttävät paljon enemmän aikaa kuin lain valmistelun yhteydessä on arvioitu ja toiminnallisuutta ei ole mahdollista toteuttaa 1.5.2021 mennessä.

Lain 55 §:n edellyttämät muutokset olisi perusteltua yhdistää asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koskeviin muutosehdotuksiin. Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024. Tämän takia esitetään, että lain 55 §:ää kliinisistä löydöksistä sovellettaisiin 1 päivästä tammikuuta 2024.

Sen sijaan toisiolain 60 §:n 1 momentissa olevaa siirtymäaikaa koskien lain 19 §:ää lokitiedoista ei tässä yhteydessä esitetä muutettavaksi. Lokitietoja koskeva vaatimus on keskeinen keino, joilla rekisteröity, rekisterinpitäjä ja viranomaiset voivat seurata ja valvoa henkilötietojen käsittelyä. Lisäksi vastaava velvoite koskee viranomaisia jo tiedonhallintalain perusteella.[6] Tietolupaviranomainen itse kerää edellä mainittua lokitietoa.

4.2 Pääasialliset vaikutukset

Tietoturvavaikutukset

Esitys mahdollistaa sen, että useampi toimija saa oman käyttöympäristönsä auditoiduksi. Tämä parantaa mahdollisuuksia sille, että toisiolaissa tarkoitettuja tietoturvallisia käyttöympäristöjä syntyisi useita. Uusissa auditoitavissa käyttöympäristöissä voidaan räätälöidä myös sellaisia tietojen käsittelymahdollisuuksia tai erikoistua johonkin tiettyyn käsittelyyn, joka ei välttämättä olisi tällä hetkellä mahdollista Tietolupaviranomaisen omassa käyttöympäristössä.

Suurin tietoturvaa koskeva vaikutus olisi, että kaikki toisiolain perusteella tietoluvan perusteella luvitettavat tietoaineistot luovutettaisiin vain toisiolain tarkoittamiin auditoituihin tietoturvallisiin käyttöympäristöihin, siirtyisi vuodella eteenpäin. Vuoden siirtymäaika mahdollistaa siis sen, että tietoja voitaisiin käsitellä vuoden ajan lisää myös sellaisissa käyttöympäristöissä, joita ei ole auditoitu.

Vaikka toisiolaissa säädetty tietoturvallinen käyttöympäristö on keskeinen asia tietoturvaa ja tietosuojaa varmistamassa, ei se kuitenkaan ole ainoa keino varmistaa tietoturva ja tietosuoja.

[6] Kyseisen hallituksen esityksen (HE 284/2018 vp) valmistelussa tuotiin kuitenkin lokitietojen keräämisen osalta lausunnoissa esille, että ehdotettu vaatimus lokitietojen keräämisestä, jos tietojärjestelmässä käsitellään henkilötietoja tai salassa pidettäviä tietoja, on kohtuuttoman raskas ja kallis vaatimus toteuttaa nykyisiin tietojärjestelmiin.

Ensinnäkin siirtymäajan siirrosta huolimatta tietoaineisto luovutetaan ensisijaisesti aina Tietolupaviranomaisen omaan tietoturvalliseen käyttöympäristöön.

Tietolupaviranomainen on tehnyt ajalla 1.4.2020-21.3.2021 yhteensä 88 tietolupapäätöstä, jotka koskevat uuden tutkimuksen aloittamista ja niihin tarvittavia toisiolain alaisia tietoja. Näistä yhteensä 47:ssa on päätetty, että tieto sijoitetaan Tietolupaviranomaisen tietoturvalliseen käyttöympäristöön. Muualle luovutuksista on tehty yhteensä 41 päätöstä. Muualle luovutuksista hyvin suuressa osassa on ollut kyse joko Terveyden ja hyvinvoinnin laitoksen (THL) omista tutkimushankkeista tai siitä, että tieto on luovutettu Tilastokeskuksen vastaavaan tietoturvalliseen ympäristöön (”Fiona”). Lisäksi tieto-aineistoa on luovutettu yliopistosairaaloiden omiin tietoympäristöihin, tai suomalaisten yliopistojen hallinnoimiin käyttöympäristöihin. Vain muutamissa, yksittäisissä tilanteissa tieto on luovutettu joko yksityisen toimijan hallintaan tai ulkomaille. Valtaosa muualle luovutettujen tietojen hallinnoijista ovat joko kotimaisia viranomaisia tai kotimaisia yliopistosairaaloita. Yliopistosairaalat hallinnoivat jo perustehtävänsä vuoksi suurta määrää terveystietoa ja niiden käyttämät potilastietojärjestelmät kuuluvat asiakastietolain perusteella A-luokan järjestelmien piiriin.

Kliinisesti merkittävän löydöksen perusteella tehtävät muutokset toteutuvat tietoturvallisesti, mutta vasta siirtymäajan jälkeen.

Tietosuojavaikutukset

Esityksellä katsotaan olevan rajoitettu vaikutus tietosuojaan, koska kyse on vain siirtymäsäännösten muuttamisesta.

Tietolupaviranomainen on ottanut käyttöön omassa lupatoiminnassa jo nyt useita tietosuojaa parantavia toimenpiteitä, joita ei aikaisemmin ole ollut käytössä. Tietolupaviranomainen vaikuttaa siten jo nyt toiminnallaan tietoturvaa ja -suojaa parantavasti.

Tietolupaviranomainen käy luvanhakijan kanssa hyvin tarkasti läpi, mitä tietoja ja kuinka paljon haettavaan käyttötarkoitukseen tarvitaan. On tavanomaista, että hakemusprosessin aikana tieto-aineisto tarkentuu merkittävästi siitä, mitä on alun perin haettu. Tietolupaviranomainen arvioi, tarvitaanko haettuun käyttötarkoitukseen niin paljoa tietoa kuin on haettu, ja onko haettava tieto käyttötarkoitukseensa sopivaa.

Tietolupapäätöksessä Tietolupaviranomainen yksilöi muuttujakohtaisesti ne tiedot, joiden käyttöön se antaa luvan. Tämäkin parantaa tietosuojaa. Luvat myönnetään vain määräaikaisina, keskimäärin korkeintaan viiden vuoden määräajaksi. Lupaan liitetään erilliset lupaehdot, jotka sisältävät määräyksiä tietosuojan ja turvan suojaamisen näkökulmasta. Jos ehtoja ei noudateta, on Tietolupaviranomaisella oikeus perua myöntämänsä lupa. Tietoluvan peruuttamisia ei ole ollut, mutta muutamissa tilanteissa Tietolupaviranomainen on huomauttanut hakijaa lupaehtojen noudattamisen tärkeydestä. Tietolupaviranomaisen näkemyksen mukaan sen laatimat lupapäätökset ja niihin liitettävät lupaehdot ovat tarkemmalla tasolla kuin mitä on ollut tilanne lupapäätösten suhteen ennen toisiolakia.

Tiedot kerätään ja luovutetaan luvanhakijalle ensisijaisesti siten, että aineisto tulee ensin Tietolupaviranomaiselle, joka yhdistää tietoaineistot sekä pseudonymisoi ne. Aineiston lähettäminen tapahtuu toisiolaissa säädettyä sähköistä tietoturvallista käyttöpalvelua pitkin. Vain pseudonymisoitu tietoaineisto luovutetaan luvansaajalle.

Tietolupaviranomaisen tekemässä lupapäätöksessä yksilöidään ne henkilöt, jotka saavat pääsyn tietoaineistoon. Kun tämä tietoaineisto sitten luovutetaan luvansaajalle, on edellytyksenä se, että käyttöoikeuden saaneet henkilöt tunnistetaan vahvasti.

Yleisessä tietosuoja-asetuksessa säädetään rekisteröityjen oikeuksista. Tietolupaviranomainen on ottanut käyttöön tammikuussa 2020 menettelyitä rekisteröityjen oikeuksien toteuttamiseksi. Asiasta on tuolloin keskusteltu Tietosuojavaltuutetun toimiston kanssa, joka on pitänyt tärkeänä, että rekisteröityjen oikeuksia ryhdytään toteuttamaan tehokkaasti. Tietolupaviranomainen on luonut internet-sivuilleen oman sivuston koskien rekisteröityjen oikeuksien toteuttamista. Tietolupaviranomainen on vastaanottanut tähän saakka yhteensä 201 vastustamisilmoitusta. Osa vastustamisilmoituksia on koskenut huoltajien tekemiä vastustamisia alaikäisistä lapsistaan.

Tietolupaviranomainen merkitsee vastustamisen tiedoksi ja suodattaa muilta rekisterinpitäjiltä saaduista aineistoista ne henkilöt pois, jotka ovat tehneet vastustamisilmoituksen. Sen sijaan tämä vastustamistieto ei välity muille rekisterinpitäjille, jotka tekevät itse päätöksiä omista aineistoistaan. Vastaavasti muille rekisterinpitäjille tehdyt mahdolliset vastustamisilmoitukset eivät tule Tietolupaviranomaisen tietoon. Tämä johtuu siitä, että toisiolaissa ei ole säädetty oikeutta muille rekisterinpitäjille eikä Tietolupaviranomaiselle saada rekisteröityjen oikeuksien toteuttamistarkoituksessa salassa pidettävää tietoa.

Pyyntöjä saada pääsy omiin tietoihin on tehty yhteensä 20 kappaletta.

Tietolupaviranomaiselta saadun näkemyksen mukaan muille rekisterinpitäjille ei ole kuitenkaan vastaavia ilmoituksia tai pyyntöjä juurikaan tehty. Tietolupaviranomainen on kannustanut muita rekisterinpitäjiä tähän sekä tarjonnut myös omaa toimintamallia asiassa hyödynnettäväksi. Terveyden- ja hyvinvoinnin laitos on ottanut myös rekisteröityjen oikeuksien toteuttamisen käyttöönsä.

Tietolupaviranomainen on ottanut rekisteröityjen oikeuksien toteuttamisessa kaikki ne keinot käyttöönsä, joihin sillä on laillinen oikeus ja velvollisuus. Tietolupaviranomaisen näkemyksen mukaan rekisteröityjen oikeuksia toteutetaan Tietolupaviranomaisen toimesta toisiolain voimaantultua aktiivisemmin kuin mikä tilanne oli ennen toisiolain voimaatuloa.

Potilaalla on oikeus kieltää kliinisesti merkittävän löydöksen perusteella tehtävät yhteydenotot siirtymäajan jälkeen. Potilas voi tehdä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toimintayksikössä taikka sähköisesti asiakastietolain tarkoitetun kansalaisen käyttöliittymän välityksellä.

Taloudelliset vaikutukset

Siirtymäajan pidentämisellä arvioidaan olevan pääosin myönteisiä vaikutuksia tietoturvallisia käyttöympäristöjä kehittävien organisaatioiden kustannuksiin. Nykyisten järjestelmien kehittäminen entistä paremmiksi huomioiden Tietolupaviranomaisen määräys tietoturvallisten käyttöympäristöjen vaatimuksista voidaan tehdä tarkoituksenmukaisella aikataululla, mikä merkitsee kustannussäästöjä verrattuna tilanteeseen, jossa joudutaan tekemään suuria kertainvestointeja kiireessä. Myös käyttöympäristöjen auditointien kustannusten arvioidaan pysyvän kohtuullisempina siirtymäajan pidentymisen vuoksi. Arviointilaitosten perimien kustannusten on tällä hetkellä kuitenkin raportoitu kasvaneen jopa kolminkertaiseksi alkuperäisiin kustannusarvioihin verrattuna. Tämän arvioidaan ainakin osittain johtuvan arviointipalveluiden kovasta kysynnästä ja arviointilaitosten henkilöresurssien niukkuudesta.

Arviointilaitosten alustavien arvioiden mukaan yksi auditointi maksaisi toimijalle useita kymmeniä tuhansia euroja. Alustavien arvioiden mukaan auditointi edellyttäisi vähimmillään noin 40 henkilötyöpäivän työajan asiaan perehtyneeltä tietoturvan auditoijalta. Helsingin ja Uudenmaan sairaanhoitopiiri on esittänyt arvioita, jonka mukaan sen oman tietoaltaan auditointi tarkoittaa miljoonien eurojen kustannuksia. Suurin kustannuserä ei ole varsinainen auditointi, vaan se, jos tai kun auditoitavaa järjestelmää joudutaan muokkaamaan määräysten kriteerien mukaiseksi. Tästä kustannustasosta ei ole vielä kattavia arvioita, koska auditointeja vasta aloitetaan. Lisäksi käyttöympäristöjen palveluntarjoajille aiheutuisi kustannuksia maksuista, joita perittäisiin Valviralle tehtävistä ilmoituksista, joiden perusteella tiedot käyttöympäristöistä tallennettaisiin Valviran ylläpitämään julkiseen rekisteriin. Maksut olisivat 300 eurosta 1200 euroon.

Toisiolain 55 §:n toteuttamisesta aiheutuu kustannuksia palvelunantajille potilastietojärjestelmien kehittämisestä, Kansaneläkelaitokselle valtakunnallisten tietojärjestelmäpalveluiden kehittämisestä ja tutkijayhteisölle tutkijoiden käyttämien tietojärjestelmien kehittämisestä. Muutokset on kuitenkin perustelua kustannustehokkaasti yhdistää asiakastietolain (HE 212/2020) tahdonilmaisupalvelua ja kieltoja koskeviin muutoksiin. Mikäli asian vaatimat tekniset muutokset tehtäisiin vain valtakunnallisiin tietojärjestelmäpalveluihin ja muusta Kanta-kehittämisestä erillään, siitä aiheutuisi vähintään 500 000 euron kustannukset. Toisiolain 55 §:n toimeenpano aiheuttaa myös vähäisiä kustannuksia Tietolupaviranomaiselle ja Terveyden ja hyvinvoinnin laitokselle. Sinällään pelkän siirtymäajan muuttamisesta ei kuitenkaan aiheudu kustannuksia.

Viranomaisvaikutukset

Esityksellä ei lisättäisi viranomaisten hallinnollista taakkaa. Tietoturvallisten käyttöympäristöjen palveluntarjoajille aiheutuisi kuitenkin tietoturvallisten käyttöympäristöjen auditoinnista kustannuksia.

Tietolupia myöntävillä viranomaisilla säilyisi edelleen harkintavalta siitä, siirretäänkö luvitettava tietoaineisto Tietolupaviranomaisen omaan käyttöympäristöön vai muualle. Tältä osin voimassa ollut tilanne jatkuisi vielä vuoden. Harkintavallan jatkaminen vuodella helpottaa lupaharkintaa, tilanteessa, jossa tietoturvallisia käyttöympäristöjä ei vielä ole ehtinyt syntyä.

Toisiolain 6 §:n 1-8 kohdassa mainituilla organisaatioilla ja viranomaisilla on kuitenkin toisiolain 10 §:n perusteella mahdollisuus käyttää Tietolupaviranomaisen tietoturvallista käyttöympäristöä. Tietolupaviranomaisen tietoturvallinen käyttöympäristö ei kuitenkaan esimerkiksi vielä pysty käsittelemään tietyntyyppistä tietoaineistoa, esimerkiksi geenitietoa, joka on volyymiltaan massiivista. Tietolupaviranomaisen ympäristössä ei myöskään voida käsitellä terveydenhuollon kuvantamisaineistoja, esimerkiksi röntgenkuvia. Kuvantamistiedon käsittelyyn tarvitaan omat, terveydenhuollon käytössä olevat laitteet. Tällaisia laitteistoja on vain sairaaloilla. Siten tietolupia myöntävä viranomainen on vaikeassa tilanteessa, jos ainoa mahdollinen ympäristö on Tietolupaviranomaisen käyttöympäristö, mikäli luvitettava aineisto olisi sen laatuista, jota ei kyseisessä ympäristössä voida näistä syistä käsitellä.

Toisiolain 55 §:n voimaan tulon siirtämisellä ei ole viranomaisvaikutuksia. Vaikutukset aiheutuvat vasta, kun 55 §:n mukaisia oikeuksia, velvoitteita ja toimenpiteitä aletaan soveltaa.

Vaikutukset yritysten toimintaan

Esityksellä ei ole merkittävä vaikutuksia yritysten toimintaan, koska kyse on vain siirtymäaikojen siirtämisestä. Esityksellä ei lisättäisi yritysten hallinnollista taakkaa, koska kyse on siirtymäajan siirtämisestä. Tietoturvallisten käyttöympäristöjen palveluntarjoajille aiheutuisi kuitenkin tietoturvallisten käyttöympäristöjen auditoinnista kustannuksia. Käytännössä nämä aiheutuvat lisäkustannukset siirrettäneen niiden käyttäjiltä perittäviin maksuihin. Lisäksi käyttöympäristöjen palveluntarjoajille aiheutuisi kustannuksia maksuista, joita perittäisiin Valviralle tehtävistä ilmoituksista, joiden perusteella tiedot käyttöympäristöistä tallennettaisiin Valviran ylläpitämään julkiseen rekisteriin. Maksut olisivat 300 eurosta 1200 euroon.

Toisiolain 55 §:n voimaantulosäännöksen siirtämisellä ei ole vaikutuksia yritysten toimintaan.

Vaikutukset kansalaisten asemaan

Esityksellä olisi vaikutuksia kansalaisten asemaan lähinnä heidän henkilötietojensa suojan suhteen. Rekisteröityjen henkilöiden asema paranisi siirtymäajan jälkeen nykyisestä toisiolaissa tarkoitetuilla tietoturvatoimenpiteillä, jotka ovat lähtökohtana kaikessa toisiolain mukaisessa henkilötietojen käsittelyssä.

Esityksessä ehdotettu tietojen käsittelyn lähtökohta on, että tietoja käsitellään siirtymäajan jälkeen tietoturvallisessa käyttöympäristössä, mikä merkitsee, että tietojen käsittely toteutetaan teknisessä ja fyysisessä ympäristössä, jossa tietoturva on varmistettu asianmukaisin hallinnollisin ja teknisin toimin sekä tietojärjestelmien asianmukaisin standardein. Tämä merkitsee tietojen käsittelyä tietoturvallisessa ympäristössä, johon käyttäjille annetaan käyttöoikeuksia.

Tietolupahakemusten ja niiden perusteella luovutettavien tietojen keskitetty hallinnointi ja käsittely tietoturvallisten käyttöyhteyksien välityksellä tietoturvallisessa käyttöympäristössä vähentää olennaisesti tietojen käsittelyyn liittyviä riskejä rekisteröityjen kannalta. Lisäksi tietojen käsittelyn valvonnasta on säädetty aiempaa tarkemmalla tasolla. Tarkemmat säännökset mahdollistaisivat sen, että rekisteröityjen oikeusturva toteutuu aiempaa paremmin. Rekisterinpitäjät on velvoitettu kuvaamaan tietoaineistonsa. Kun tietoaineistot on kuvattu nykyistä paremmin, myös rekistereiden yleiset tietosisällöt ovat avoimemmin kaikkien tarkasteltavissa.

Se, että ihmisille on järjestetty kanava Tietolupaviranomaisen kautta vastustaa tietojensa käsittelyä toisiotarkoituksessa, turvaa osaltaan sitä, että henkilöt, jotka eivät luota tietojensa olevan turvassa tai eivät ylipäätänsä halua tietojaan käytettävän toisiolaissa säädettyihin tarkoituksiin, voivat tällaisen vastustamisilmoituksen tehdä.

Toisiolain 55 §:n voimaantulon siirtämisellä ei ole suoranaisia vaikutuksia kansalaisiin. Mahdollisuus kliinisten löydösten perusteella ottaa yhteyttä kansalaisiin ja kansalaisen oikeus kieltää nämä yhteydenotot siirtyvät esitettävän siirtymäajan verran.

Vaikutukset sosiaali- ja terveyspalvelujärjestelmään

Vaikutuksia on arvioitu toisiolain hallituksen esityksessä (HE 159/2017). Sosiaali- ja terveydenhuollon palvelujärjestelmä on suurien muutosten edessä sote-uudistuksen tullessa voimaan vuoden 2023 alussa. Palvelujärjestelmän muutoksen suunnittelun ja seurannan kannalta on tärkeätä, että tietojen käyttöprosesseja saadaan muutettua ehdotetun lakiesityksen mukaiseen tietoturvaa korottavaan suuntaan.

Toisiolaki mahdollistaa tutkimusedellytysten lisääntymisen ja luo siten pohjaa korkeatasoisille tieteellisille tutkimusympäristöille ja niistä syntyville uusille innovaatioille. Uudet palveluinnovaatiot luovat edellytyksiä palvelujärjestelmän kehittymiselle asiakaslähtöisempään suuntaan ja luovat pohjaa yksilöllisemmän hoito- ja palvelukulttuurin syntymiselle.

Palvelurakenteen kehittämisen kannalta on tärkeää saada tutkimustietoa vaikuttavista hyvinvointiin ja terveyteen liittyvistä teknologioista, jotka voivat korvata esimerkiksi laitoshoitoa ja siten siirtää palvelurakenteen painopistettä laitoksista ihmisten koteihin. Tällä painopisteen muutoksella on iso merkitys siinä, miltä tulevaisuuden palvelurakenne näyttää ja millaiseksi sitä pitäisi rakentaa. Lakiesitys mahdollistaa myös tutkimuksen ja tuotekehityksen ympärille rakentuvan tietoturvallisten ympäristöjen ekosysteemin syntymisen, mistä erikokoiset yksityiset ja julkiset toimijat voisivat hyötyä. Ekosysteemin syntymisen edellytyksenä on se, että laadukkaita rekisteriaineistojamme voidaan hyödyntää nopeasti ja siten, että tietojen käyttöönotosta syntyvät kustannukset ovat kohtuullisia.

Sote-uudistus painottaa sosiaali- ja terveydenhuollon integraatiota. Se hyödyttää palvelujärjestelmän näkökulmasta kaikkia asiakkaita, jotka käyttävät enemmän kuin yhtä palvelua. Kaikkein eniten se auttaa paljon palveluja käyttäviä asiakkaita ja potilaita. Vaikka lakiesitys sosiaali-ja terveydenhuollon järjestämisestä helpottaa näiden asiakas- ja potilasryhmien saamien palveluiden seuraamista ja myös palveluketjujen seuraamista, se ei sinällään ratkaise kaikkia tiedonkeruuseen ja tietoturvaan liittyviä haasteita, vaan tarvitsee pohjakseen ehdotetun kaltaiset tietoturvalliset käyttöympäristöt.

Toisiolain 55 §:n voimaantulon siirtämisellä ei ole suoranaisia vaikutuksia sosiaaliset ja terveyspalvelujärjestelmään. Mahdollisuus kliinisten löydösten perusteella ottaa yhteyttä kansalaisiin ja kansalaisen oikeus kieltää nämä yhteydenotot siirtyy. Siirtymäajan jälkeen toisiolain 55 §:n muutoksilla on toisiolain hallituksen esityksessä (HE 159/2017) todettuja vaikutuksia.

Vaikutukset lapsiin ja sukupuolten tasa-arvoon

Esityksellä ei arvioida olevan erityisiä lapsiin tai sukupuolten tasa-arvoon kohdistuvia vaikutuksia.

Vaikutukset työllisyyteen ja työelämään

Esityksellä on työllisyyttä lisäävä vaikutus, sillä luvanhakijoiden tulee rakentaa ja auditoida siirtymäajan aikana toisiolain mukaiset tietoturvalliset käyttöympäristöt tai hankkia vastaava palvelu Tietolupaviranomaiselta tai muilta toimijoilta. Tällä on sekä alan toimijoita, luvan hakijoita ja arviointilaitosten työmäärää lisäävä ja siten välillisesti työllisyyttä lisäävä vaatimus. Tietoturvallista käyttöympäristöä ei auditoida vain kerran vaan teknologian ja toimintakentän muutosten myötä auditointi on uusittava.

Toisiolain 55 §:n voimaantulon siirtämisellä on työllisyyttä lisäävä vaikutus, koska sen mukaiset oikeudet, velvoitteet ja toimenpiteet on toteutettava sosiaali- ja terveysalan tietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tutkijoiden käyttämiin järjestelmiin.

Vaikutukset rikoksentorjuntaan ja turvallisuuteen

Siirtymäajan siirrolla ei sinällään ole rikoksentorjuntaan lisäävä vaikutusta. Tietoturvallisilla ympäristöjä koskevilla vaatimuksilla, auditoinnilla ja lokitusvaatimuksella on kuitenkin sinällään jo rikosten torjuntaa edesauttava vaikutus. Tietoturvalliset ympäristöt ovat yksi monista keinoista turvallisuuden korottamiseen ja varmistamiseen. Täytäntöönpanossa tulee kuitenkin huolehtia, että on olemassa toimivia tietoturvaa varmistavia ratkaisuja ennen kuin laissa esitetty siirtymäsäännös astuu voimaan.

Toisiolain 55 §:n voimaantulon siirtämisellä on rikoksentorjuntaan ja turvallisuutta lisäävä vaikutus, koska siirtymäajan jälkeen toteutetaan toisiolain 55 §:n mukaiset oikeudet, velvoitteet ja toimenpiteet, mutta tietoturvallisesti ja tietosuoja huomioon ottaen ja turvaten kansalaisen itsemääräämisoikeuden.

Vaikutukset tietoyhteiskuntaan

Vaikutuksia on arvioitu jo toisiolain hallituksen esityksessä (HE 159/2017). Sinällään siirtymäajan muuttamisella ei ole merkittäviä vaikutuksia tietoyhteiskuntaan. Sinällään toisiolailla turvataan sosiaali- ja terveysalan tutkimus- ja innovaatiotyön jatkuminen kansallisesti sekä suomalaisten mahdollisuus osallistua kansainväliseen kehitykseen samalla kun rekisteritiedon hyödyntämisen tietosuojan ja -turvan pitkäjänteistä parantamistyötä jatketaan.

Tutkimus- ja innovaatiotoiminta tuottaa uusia hoitoja, lääkkeitä, terveysteknologian ratkaisuja, parempia toimintamalleja ja prosesseja sosiaali- ja terveydenhuoltoon. Samalla alan osaaminen kehittyy ja syntyy uutta ja kasvavaa kansainvälistä vientiä. Lääkeyritysten tutkimusinvestoinnit Suomeen olivat vuonna 2019 186 miljoonaa euroa. Terveysteknologian viennin arvo vuonna 2019 oli 2,4 miljardia euroa. Kasvua edelliseen vuoteen verrattuna 5,7 prosenttia. Terveysteknologian vienti on vahvasti ylijäämäistä. Tutkivan lääke- ja terveysekosysteemin työllisyysvaikutus vuonna 2018 oli noin 14 000 työllistä. Suoran rekisteritutkimuksen osuus kokonaisvaikutuksista on suhteellisen pieni. Sosiaali- ja terveystietojen hyödyntämisellä muun tutkimuksen osana on kuitenkin merkittävä vaikutus tutkimus- ja innovaatiomahdollisuuksiin.

Tutkimus- ja innovaatiotoiminnan osittainen pysähtyminen siirtymäajaksi sekä siitä seuraavat kerrannaisvaikutukset tuleville vuosille olisivat merkittävät, vaikka euromääräisiä vaikutuksia ei osata arvioida. Hoitojen, lääkkeiden, terveysteknologian laitteiden ja alan toimintamallien kehitys vaikeutuisi merkittävästi. Asiakassuhteet tutkimuskonsortioihin ja alan suurasiakkaisiin vaarantuisivat, työllisyys ja vientitulot laskisivat sekä alan myönteinen kehityssuunta vaarantuisi.

Tutkimus ja innovaatiot kasvattavat välillisesti ihmisten hyvinvointia ja terveyttä. Tutkimusyhteistyön avulla suomalaisten käyttöön saadaan alan uusinta osaamista ja hoitoja, joiden saapuminen Suomeen voisi muuten viedä vuosia. Rekisteritiedon hyödyntämisessä tapahtuva katkos haittaa siten mahdollisuuksia hyödyntää uusia, parhaita keinoja ja työkaluja vaikuttaa ihmisten hyvinvointiin ja terveyteen.

Toisiolailla on ollut selkeä myönteinen vaikutus tietosuojaan ja -turvaan sosiaali- ja terveystietojen käytössä tutkimus- ja innovaatiotoiminnassa. Siirtymäajan jatkamisella varmistetaan tämän myönteisen kehityksen jatkuminen. Alan toimijat, kuten rekisterinpitäjät ja tutkijat, ovat ryhtyneet kiinnittämään entistä enemmän huomiota tietosuojaan ja -turvaan omassa toiminnas-

saan. Lain edellytysten mukainen tietojärjestelmien kehittäminen on käynnissä ja keskeiset toimijat ovat käynnistäneet tietoturvallisten käyttöympäristöjen auditointiprosesseja. Tietosuojan ja -turvan kehittäminen on pitkäjänteistä, jatkuvaa toimintaa.

Merkittäviin kliinisiin löydöksiin perustuvat oikeudet, velvoitteet ja toimenpiteet toteutettaisiin tietoyhteiskunnan palveluita hyväksikäyttäen. Kiellon voisi siirtymäajan jälkeen tehdä sekä palvelunantajan luona mutta myös asiakastietolain mukaisen kansalaisen käyttöliittymän (Omakanta) kautta.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Vaihtoehto 1: Palataan entisiin käytäntöihin

Tietoturvallinen käyttöympäristö on toisiolain hallituksen esitykseen kirjoitettu keskeinen toimi, joka turvaa yksilön henkilötietojen suojaa. Jos vaatimuksesta luovuttaisiin, putoaisi koko toisiolain keskeinen pohja. Tietoturvallisella käyttöympäristöllä on merkittävä rooli väärinkäytösten estämisessä ja kyberturvallisuuden toteuttamisessa. Se on myös kilpailuetu Suomelle, koska voimme siten osoittaa, että täällä huolehditaan vahvasti arkaluonteisten henkilötietojen suojasta. Myös yleisessä tietosuoja-asetuksessa edellytetään riittäviä suojatoimia, kun käsitellään arkaluonteisia henkilötietoja.

Vaikka toisiolain tietoturvan taso on korkea, ei toisiolain tarkoituksena ole ollut vaikeuttaa tieteellistä tutkimusta vaan päinvastoin edistää sitä. Toisiolaissa on samanaikaisesti mahdollistettu tietojen käyttö toisiolaissa todettuun moneen eri käyttötarkoituksiin ja huolehdittu siitä, että rekisteröityjen henkilötietojen suoja ja luottamus sosiaali- ja terveydenhuoltopalveluihin sekä toisaalta toissijaista käyttöä kohtaan voidaan turvata. Tämä on ehdoton edellytys sille, että arkaluonteisia tietoja voidaan käsitellä toisiolain käyttötarkoituksiin.

Oppivan tekoälyn ja reidentifikaatiotekniikoiden kehityksen myötä edes anonymisointi anonymisointihetkellä tunnettuja anonymisointitekniikoita käyttäen ei enää automaattisesti takaa, etteikö henkilöitä tai heihin liitettäviä tietoja kyettäisi jälkikäteen selvittämään useita eri anonymisoituja tietoaineistoja yhdistelemällä.

Turvallisten käyttöympäristöjen etuna on muun muassa se, että tietoaineistoja ei käytetä eikä säilytetä niitä käsittelevien omassa tietokoneessa, vaan käsittelykapasiteetiltaan huomattavasti tehokkaammassa käyttöympäristössä, jossa tutkijoilla ja muilla tietoja käsittelevillä on käytettävissään parhaat tekniset välineet. Luonnollisesti turvallisen käyttöympäristön hankkimisesta aiheutuu rakentamiskustannuksia, mutta käyttökustannukset ovat kohtuullisia riittävällä tietoturvan tasollakin. Kyse on yhteiskunnan infrastruktuurin rakentamisesta digitaalitaloutta varten. Olisikin tärkeää, että eri tutkimuslaitoksille ja yliopistoille turvattaisiin taloudelliset edellytykset hankkia käyttöönsä ajanmukaiset, tietoturvalliset käyttöympäristöt edistämään kansallisen tutkimusinfrastruktuurin houkuttelevuutta sekä parantamaan sen tietoturvallisuutta ja samalla tutkimuksen teknisesti toteutettavia edellytyksiä.

Turvalliset käyttöympäristöt ovat kilpailutekijä. Niitä tarjoavat tahot voivat profiloitua kansainvälisestikin ja muun muassa kilpailla osaavista tutkijoista, koska hankkeet toteutetaan laadukkailla tietoaineistoilla ja aineistot käsitellään tietoturvallisessa ympäristössä, mikä säästää niitä hyödyntävien tahojen laite- ja muita kustannuksia. Muun muassa Turussa Auria-Tietopalvelulla

on hyviä kokemuksia tietoturvallisista ”hauskoista, hienoista ja työtä säästävistä” käyttöympäristöistä, joilla on säästetty ylimääräistä työtä, käytettävissä on viimeisimmät työvälineet ja toiminta on tietoturvallista.

Mikään ei myöskään estä yliopistotutkijaa käyttämästä esimerkiksi yliopistollisen sairaalan tarjoamaa auditoitua tietoturvallista käyttöympäristöä. Laissa ei velvoiteta muita kuin Tietolupaviranomaista perustamaan tietoturvallisen käyttöympäristön. Jokainen toimija ei siis tarvitse omaa järjestelmäänsä tietojen turvalliseen käsittelyyn.

Kansaneläkelaitokselta ja Tietolupaviranomaiselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvallisiin käyttöympäristöihin, lain edellyttämät muutoksia ei ole mahdollista toteuttaa 1.5.2021 mennessä. Toisiolain 55 §:n mukaiset yhteydenotot ja kieltooikeus eivät olisi mahdollista, mikäli palattaisiin vanhoihin käytänteisiin.

Mikäli palattaisiin vanhoihin käytänteisiin, niin siitä huolimatta olisi edelleen rekisteröityjen oikeuksia ja erityisesti tietosuojaa ja tietoturvaa suojaamassa yleinen tietosuoja-asetus, tietosuojalaki, tiedonhallintalaki, Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011), tilastolaki (280/2004) ja edellä mainittujen lakien ja toisiolain perusteella jo nyt toteutetut tietosuojaa ja tietoturvaa lisäävät toimenpiteet. Käyttöympäristöjen tietoturvaa voisi korottaa lisäksi vapaaehtoisilla auditoinneilla ja sertifikaateilla.

Mikäli palattaisiin vanhoihin käytäntöihin, riskinä on, että kliinisten merkittävien löydösten perusteella potilaisiin otettaisiin yhteyttä ilman lakiperustaa ja potilaiden perustuslaillista tiedollista itsemääräämisoikeutta loukaten.

Vaihtoehto 2: Siirretään siirtymäaikaa esityksen sijaan vain kuudella kuukaudella

Mikäli siirtymäaikaa siirretään vain kuudella kuukaudella, tilanne olisi tietoturvan tason nostamisen osalta sinällään osin parempi kuin tällä hetkellä, mutta on kuitenkin oletettavaa, etteivät kaikki alan keskeiset toimijat olisi vielä auditoineet heidän ympäristöjään. Sen sijaan myös siirtymäajan aikana tietosuojaa ja tietoturvaa turvaisivat useat Tietolupaviranomaisen toisiolain perusteella käyttöönottamat toimenpiteet ja edellä mainituista laeista johtuvat tietosuoja- ja tietoturvavaatimukset. Ratkaisevaa on sekä arviointilaitoksen valmiudet ja resurssit, mutta myös arvioitavien järjestelmien määrä ja kyvykkyydet ja eri toimijoiden valmiudet aloittaa tietoturvallisen käyttöympäristönsä auditoinnit. Arviointilaitokset ovat ilmaisseet valmiudet hoitaa auditoinnit vuoden sisällä edellyttäen, että arvioitavia käyttöympäristöjä tulee tasaisia määriä arvioitavaksi, eikä vain painottuen kevääseen 2022.

Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvallisiin käyttöympäristöihin, lain edellyttämiä muutoksia ei ole mahdollista tehdä 1.5.2021, eikä 1.5.2022. Kansaneläkelaitokselta saadun tiedon mukaan muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024.

Vaihtoehto 3: Sidotaan siirtymäaikaa sote-uudistuksen voimaantuloon 1.1.2023.

Useassa sote-uudistusta koskevassa lausunnossa on todettu, että mitään muita suuria muutoksia ei tulisi asettaa sosiaali- ja terveysalan toimijoille samaan aikaan sote-uudistuksen määräaikojen

kanssa, koska suurin osa resursseista menee sote-uudistuksen valmisteluun. Osa lausunnonantajista puolsi tätäkin pidempää siirtymäaikaa kuten esimerkiksi toukokuuhun 2024 tai kunnes asiaa koskeva EU lainsäädäntö täsmentyy.

Kansaneläkelaitokselta ja Tietolupaviranomaiselta saadun tiedon mukaan, koska toisiolain 55 §:n vaatimat muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvallisiin käyttöympäristöihin, lain edellyttämiä muutoksia ei ole mahdollista tehdä 1.5.2021, eikä 1.1.2023. Kansaneläkelaitokselta saadun tiedon mukaan muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024. Itse asiassa muun muassa sote-uudistuksen vuoksi Kansaneläkelaitos ja Terveyden ja hyvinvoinnin laitos suosittelee siirtymäajaksi 1.1.2025.

Vaihtoehto 4: Yhteiseurooppalaiset ratkaisut

Yleisen tietosuoja-asetuksen 42 artiklan mukaisia hyväksyttyjä tietosuojasertifiointimekanismeja ei vielä ole käytössä. Näiden käyttöä olisi syytä kannustaa eri toimialoilla täydentämään rekisterinpitäjän sisäistä valvontaa ja viranomaisvalvontaa vastaavalla tavalla kuin nyt käytetään tietoturva-auditointeja.

Ulkopuolisten sertifiointielinten myöntämät tietosuojasertifioinnit olisivat yksi yleisen tietosuoja-asetuksen mukainen keino rekisterinpitäjän osoittaa, että tietosuoja-asetusta ja erityisesti käsittelyn turvallisuuteen liittyviä vaatimuksia noudatetaan. Ulkopuolisten riippumattomien sertifiointielinten tekemät arviot lisäisivät toiminnan uskottavuutta, laajentaisivat merkittävästi kyvykkyyksiä arvioida säännösten mukaisuutta (valvontaa) ja samalla se toisi rekisterinpitäjille tärkeää osaamista tietosuojan kehittämiseen. Tämä edellyttäisi sertifiointielinten akkreditointia, joka on tietosuojavaltuutetun tehtävä, sekä tietosuojan sertifioinnin liiketoiminnan käynnistämistä.

Kansallisessa sote-tietojen toisiokäytössä ovat koko ajan olleet lähtökohtana yhteiset kansainväliset ja eurooppalaiset käytännöt ja ratkaisut. Kansainvälinen ja eurooppalainen kehitys on kuitenkin vielä niin yleisellä tasolla ja käytännöt eri maissa vaihtelevat niin paljon, että tietojen tietoturvallista luovuttamista käyttöympäristöihin ei voida varmistaa pelkästään niiden avulla. Tietolupaviranomaisen määräys tietoturvallisen käyttöympäristön vaatimuksista konkretisoi keskeiset ratkaisut, joita tietosuojan ja -turvan osalta tulee noudattaa. Määräys perustuu muun muassa ISO 27001 Tietoturvajohtamisen standardiin ja kansalliseen tietoturvallisuuden auditointityövälineeseen viranomaisille Katakriin.

Yleiseurooppalaisia toimintamalleja ja ratkaisuja henkilötason terveystietojen eurooppalaiseen tiedonvaihtoon ja hyödyntämiseen toisiokäytössä selvitetään parhaillaan komission European Health Data Space yhteishankkeessa. Komission on myös ilmoittanut käynnistävänsä European Health Data Space lainsäädäntöhankkeen vuoden 2021 aikana. Tämä lainsäädäntö luon mahdollisesti tulevaisuudessa sellaiset yleiseurooppalaiset toimintamallit ja arviointikäytännöt, joiden avulla myös käyttöympäristöjen tietoturvallisuus voidaan varmistaa koko Euroopan Unionin alueella. Toistaiseksi tällaisia yleiseurooppalaisia ratkaisuja ei kuitenkaan ole olemassa.

Yleiseurooppalaiset ratkaisut eivät tuo ratkaisua merkittäviin kliinisiin löydöksiin perustuviin oikeuksien, velvoitteiden ja toimenpiteiden kansalliseen toteuttamiseen.

Merkittäviin kliinisten löydöksiin liittyvää sääntelyä ei ole vastaavanlaisesti muissa maissa. Alan yleiseurooppalaista sääntelyä tulee seurata, mutta lyhyellä aikavälillä olisi tarkoituksenmukaista seurata vastaavaa biopankkilakiin ja genomilakiin mahdollisesti ehdotettavia muutoksia.

5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot

Ulkomaista lainsäädäntöä ja ulkomailla käytettyjä keinoja arviotiin toisiolain hallituksen esityksen (HE 159/2017 vp) yhteydessä sivuilla 32-58 ja edellä yhteiseurooppalaiset ratkaisut vaihtoehdossa. Vastaavia tietoturvallisia auditoituja käyttöympäristöjä kuin toisiolaissa on säädetty, ei kuitenkaan ole vielä muissa maissa.

Sen sijaan kuten työryhmäraportissa[7] on todettu, ”tieto- ja kyberturvallisuuden ja tietosuojan kehittäminen edellyttävät ymmärrystä kybertoimintaympäristön muutoksista kansallisella ja kansainvälisellä tasolla. Kriittisillä toimialoilla tämä edellyttää, että eri toimijat jakavat ja ylläpitävät kybertoimintaympäristön tilannekuvaa koordinoidusti ja kohdennetuin tilannekatsauksin. Toimintaympäristön osalta on tärkeää huomata, että pahantahtoista kybertoimintaa ja -loukkauksia kohdistuu yksityisten yritysten lisäksi valtion instituutioihin. Tekijänä voivat tällöin olla yksityisen toimijan lisäksi valtiotoimija tai sen käyttämä bulvaani. Valtiolähtöisissä loukkauksissa korostuvat haavoittuvuuksien havaitsemisen ja korjaamisen ohella yhteisesti koordinoidut poliittiset toimet ja signaloinnit. Suomi on osallistunut aktiivisesti yhteisen EU-politiikan ja välineiden kehittämiseen ja hyödyntämiseen, joiden avulla edistetään vastuullista valtiokäyttäytymistä kybertoimintaympäristössä. Tällaisia välineitä pahantahtoisen kybertoiminnan torjuntaan EU:n tasolla ovat olleet esimerkiksi kyberdiplomatian työkalupakki ja kyberpakotteet.

Edellä mainittuihin tekijöihin voidaan kansallisen ja kansainvälisen sääntelyn ohella vaikuttaa toimialojen toimintakulttuureja kehittämällä, vapaaehtoisella yhteistyöllä viranomaisten ja palveluiden tarjoajien välillä sekä kehittämällä sekä hyödyntämällä EU-politiikkoja ja välineitä. Lisäksi on tärkeää osallistua aktiivisena osapuolena kansainväliseen yhteistyöhön, jossa edellytetään vastuullista valtiokäyttäytymistä kybertoimintaympäristössä. On selvää, että hallinnonalojen välistä yhteistyötä EU- ja kansainvälisen tason vaikuttamisen tehostamiseksi kehitetään jatkuvasti. Kansainvälisen kybertoimintaympäristön kehitystä koskevaa tilannekuvaa jaetaan hallinnonalojen välillä ja tämä huomioidaan myös Suomen kansallisen toimintaympäristön arvioinnissa. Näitä laajempia kybertoimintaympäristöön liittyviä kysymyksiä ja kansainvälistä yhteistyötä kyberuhkien torjunnassa ei kuitenkaan käsitellä tämän raportin suosituksissa, vaan niihin liittyvää kehitystyötä tehdään jatkuvasti muun muassa kansallisen kyberturvallisuusstrategian toimeenpanon puitteissa.

6 Lausuntopalaute

Sosiaali- ja terveysministeriö järjesti kuulemistilaisuuden 12.4.2021. Kuulemistilaisuuteen osallistui 68 henkilöä. Kuulemistilaisuudessa 19 osallistujaa kannatti esitysluonnosta tietoturvallisten käyttöympäristöjen siirtymäsäännösten muuttamisesta siten, että niitä sovellettaisiin vasta 1 päivästä toukokuuta 2022. Kukaan ei tilaisuudessa suoraan vastustanut siirtymäajan siirtämistä. Sen sijaan erilaisia näkemyksiä oli kuinka paljon siirtymäsäännöstä tulisi muuttaa. Eduskunnan oikeusasiamiehen toimiston edustaja toi esille esityksessä olevat puutteet perusoikeuksien turvaamisen osalta ja tarpeen mahdollisesti palauttaa asia uudelleen valmisteltavaksi.

[7] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Työryhmän loppuraportti ks. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162783/LVM_2021_1.pdf?sequence=1&isAllowed=y

Kuulemistilaisuudessa 17 henkilöä kannatti esitysluonnosta kliinisesti merkittäviin löydöksiin perustuvien oikeuksien, velvoitteiden ja toimenpiteiden siirtymäsäännösten muuttamisesta siten, että niitä sovellettaisiin vasta 1 päivästä tammikuuta 2024. Kukaan ei ensin suoraan vastustanut siirtymäsäännöksen muuttamista, mutta puheenvuoroista muun muassa HUS vastusti kyseisen siirtymäajan siirtämistä.

Kuulemistilaisuuden lisäksi luonnoksesta hallituksen esitykseksi on voinut antaa kirjallisen lausunnon 13.4.2021 mennessä. Hallituksen esityksen valmisteluasiakirjat ovat julkisessa palvelussa osoitteessa https://stm.fi/hanke?tunnus=STM047:00/2021.

Lausuntoja esitykseen saapui yhteensä 28 kappaletta. Selvä enemmistö kannatti siirtymäsäännösten muuttamista. Enemmistö toisiolain soveltamisalaan kuuluvista organisaatioista, viranomaisista ja rekisterinpitäjistä sekä muun muassa Kuntaliitto ja etujärjestöt ehdottivat jopa paljon pidempiä siirtymäaikoja tietoturvallisille käyttöympäristöille. Osa lausunnonantajista suositteli, että tulisi ottaa huomioon EU:n datapolitiikka, EU:n datatalous ja tuleva tietoaineistojen hallintaa ja terveystietojen data-avaruuksia koskevaa sääntelyä (Data Governance Act ja European Health Data space) ja Euroopan tietosuojaviranomaisen (EDPB) linjauksia ennen kuin tulisi sitoutua kansallisen siirtymäajan jatkamiseen. Lisäksi usea lausunnonantaja toisti, että tietosuojan ja tietoturvan tasoa jo nyt takaa muun muassa yleinen tietosuoja-asetus, tietosuojalaki, tiedonhallintalaki ja moni muukin laki sekä toisiolaissa muun muassa sen 18 §.

Liikenne- ja viestintäministeriön lausunnossa todetaan, että sosiaali- ja terveysalan toimijoiden digitaalisten käyttöympäristöjen ja tietojen käsittelyn tietoturvallisuus tulee varmistaa mahdollisimman pian. Tämän johdosta esitysluonnoksessa ehdotettua vuoden lisämääräaikaa tietoturvallisen käyttöympäristön soveltamiseksi ei tulisi ainakaan pidentää esitetystä. Liikenne- ja viestintäministeriö katsoo, että ehdotetun uuden siirtymäajan aikana alan toimijoiden tulee kiinnittää erityistä huomiota toimintansa ja käytössä olevien tietojärjestelmiensä tietoturvallisuuteen toisiolain 18 §:n yleisten tietoturvavaatimusten mukaisesti. Liikenne- ja viestintäministeriö katsoo esitysluonnoksen mukaisesti, että tulevaisuudessa tulisi arvioida mahdollisia tietoturvaa koskevia lisävaatimuksia, jos tietoaineistoja halutaan luovuttaa tietoturvallisesti muihin kuin Suomessa auditoituihin käyttöympäristöihin. Perusperiaatteena voidaan pitää sitä, että suomalaisen henkilötietojen käsittelyllä tulisi olla samat vaatimukset koko EU-alueella ja myös vastaanottajan käyttöympäristön tietoturvallisuus tulisi kyetä todentamaan. Liikenne- ja viestintäministeriö muistuttaa, että tietoturvallisuuden kehittämiseen osoitetut resurssit ovat pieniä niihin vahinkoihin nähden, jos toimija joutuu esimerkiksi laaja-alaisen tietomurron kohteeksi. Tietoturvan ja tietosuojan merkityksestä on linjattu yksityiskohtaisemmin helmikuussa julkaistussa selvityksessä tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla. Selvityksessä on arvioitu muun muassa tietoturva-auditointien hyötyjä kriittisillä toimialoilla.

Liikenne- ja viestintävirasto (Traficom) pitää toisiolain tavoitteiden kannalta keskeisenä, että tietoja käsitellään tietoturvallisissa käyttöympäristöissä ja että käyttöympäristöt on arvioitu laissa edellytetyllä tavalla. Traficom korostaa tietoturvan ja tietosuojan huolellista suunnittelua ja toteuttamista digitaalisissa ympäristöissä. Puutteellisesta tietoturvasta johtuvat tietovuodot ja tietojen suojan vaarantuminen voivat aiheuttaa merkittävää vahinkoa ja kustannuksia. Traficom kannustaa organisaatioita toteuttamaan tietoturvallisille käyttöympäristöille asetetut vaatimukset mahdollisimman pikaisesti, jotta varmistetaan toisiolain mukaisten tietojen turvallinen ja sujuva käyttö. Arviointiprosessiin on varattava riittävästi aikaa. Traficom muistuttaa, että lain edellyttämät vaatimukset eivät kerran toteutettuna välttämättä anna riittävää suojaa, vaan toteutettuja ratkaisuja on myös arvioitava säännöllisesti riskiperusteisesti koko niiden elinkaaren ajan.

Valtiovarainministeriön lausunnossa todetaan, että ministeriö pitää siirtymäkauden jatkamista sellaisenaan vuoteen 2022 ongelmallisena. Toimijoilla on ollut kaksi vuotta aikaa toteuttaa tietojärjestelmiinsä lain edellyttämät muutokset, eikä kuitenkaan, tietolupaviranomaisen ympäristöä lukuun ottamatta, yhtään tietojärjestelmää ole toteutettu lain vaatimalle tasolle. Valtiovarainministeriön näkemyksen mukaan on suuri riski, ettei vuoden siirtymäkauden jatkon päätyttyä ole edelleenkään saatu toteutettua ja sertifioitua järjestelmiä lain edellyttämälle tasolle. Tällöin siirtymäkauden jatkon päätyttyä ongelma on vastaava eikä siirtymäkauden jatkuva ohjaa toimijoita toimimaan lain vaatimusten mukaisesti. Tästä johtuen tulisi arvioida, mikä on realistinen aika, jossa toimijat ehtivät päivittää järjestelmänsä ja mitoittaa siirtymäkausi sen mukaisesti. Siirtymäkaudella tietolupaviranomaiselle tulisi myöntää oikeus antaa riskiarvioon perustuvia määräaikaisia toimijakohtaisia poikkeamia lain 20 §:n 3 momentin vaatimuksista. Poikkeaman myöntäminen voisi hyvin siirtymäkaudella perustua tiedonkäyttäjien itsearvioon, jolloin tarkastuslaitosten toimintaa ei kuormiteta turhaan. Tämä pienentäisi siirtymäkauden aiheuttamia riskejä tietoturvalle ja tietosuojalle ja tekisi siitä hallittua. Tiedon käyttäjien tietoja tietosuojakontrollien riittävyys riskeihin nähden tulisi arvioitua. Samalla tietosuojaviranomaiselle muodostuisi näkymä siihen, miten hyvin tiedonkäyttäjien tietoturva- ja tietosuojaratkaisut täyttävät lain vaatimukset ja tiedonkäyttäjille luotaisiin painetta saada tietojärjestelmänsä lain vaatimalle tasolle.

Eduskunnan apulaisoikeusasiamiehen lausunnon mukaan esitysluonnoksessa ehdotettu muutos on ristiriidassa niiden vaatimusten kanssa, joita sekä perustuslakivaliokunta että sosiaali- ja terveysvaliokunta asettivat arkaluonteisten henkilötietojen tietoturvan varmistamiseksi toisiolakia koskevaa hallituksen esitystä käsitellessään. Valtiosääntöoikeudellisesti on merkityksellistä, että toisiolaki on mahdollistanut yksityiselämän ytimeen ulottuvien arkaluonteisten henkilötietojen laajamittaisen käsittelyn alkuperäisestä käyttötarkoituksesta poikkeaviin tarkoituksiin, mukaan lukien kehittämis- ja innovaatiotoiminta. Apulaisoikeusasiamies pitää tietoturvallista käyttöympäristöä keskeisenä säädösperusteisena toimena, jolla turvataan yksityiselämän suojaa ja rekisteröidyn oikeuksia käsiteltäessä arkaluonteisista henkilötiedoista muodostuvia tietovarantoja. Apulaisoikeusasiamies katsoo, että tietoturvallista käyttöympäristöä koskeva sääntely on kriittisen tärkeä edellytys tietovarantojen käytön sallittavuudelle ja valtiosääntöiselle hyväksyttävyydelle. Tietoturvallista käyttöympäristöä koskevista vaatimuksista poikkeaminen esitysluonnoksessa ehdotetulla tavalla siirtymäkautta pidentämällä lisäisi vaaraa tietojen joutumisesta vääriin käsiin. Kaikkinainen tietojen väärinkäyttö aiheuttaisi erittäin merkittävää haittaa niin yksittäisille henkilöille kuin toisiolailla luodun järjestelmän luotettavuudelle. Ehdotettu muutos on perustuslain 10 §:n turvaaman oikeuden yksityiselämään ja henkilötietojen suojaan kannalta sillä tavalla ongelmallinen, että esitysluonnos on tietoturvallista käyttöympäristöä koskevin osin palautettava jatkovalmisteluun.

Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) pitää tärkeänä, että sosiaali- ja terveystietojen toissijaista käyttöä tekevillä organisaatioilla on tosiasiallinen mahdollisuus saattaa omat käyttöympäristönsä lain ja sitä tarkentavan määräyksen vaatimusten tasolle. Olemassa oleviin käyttöympäristöihin tarvittavat muutokset ovat mittavia ja edellyttävät merkittävästi aikaa, henkilöresursseja ja taloudellisia resursseja. Toisiolain 60 §:n 1 momentin siirtymäajan muuttaminen mahdollistaa aidosti merkittävimpien käyttöympäristöjen saattamisen lain ja määräyksen edellyttämälle tasolle ja vahvistaa käyttöympäristöjen toteutuksesta vastaavien organisaatioiden sitoutumista pitkäjänteisesti tietoturvaa ja tietosuojaa parantaviin toimenpiteisiin ja teknisiin ratkaisuihin. Valvira pitää ehdotettua siirtämäajan muutosta perusteltuna.

Kansaneläkelaitos ja suurin osa lausujista lausuivat, että toisiolain 55 §:ään tehtävät muutokset olisi perusteltua tehdä samanaikaisesti asiakastietolain (HE 212/2020 vp) muutosten yhteydessä ja siirtää siirtymäaika 1. tammikuuta 2024.

Lausuntojen ja kuulemistilaisuuden johdosta hallituksen esityksen keskeisiä ehdotuksia ei esitetä muutettavaksi. Vaikka siirtymäaikaa päätettäisiinkin siirtää vuodella eteenpäin, perustuslain 10 §:n turvaama oikeus yksityiselämään ja henkilötietojen suojaan pystytään turvaamaan jo voimassa olevan muun lainsäädännön, suojatoimien ja käytänteiden avulla sekä toisiolain 18 §:n mukaisesti riskienhallinnalla, pääsynhallinnalla, aktiivisella valvonnalla sekä noudattamalla tietoturvallisuuden ja tietosuojan toteutuksesta ja valvonnasta vastaavan viranomaisen määräyksiä ja ohjeita. Erityistä huomiota on kiinnitettävä myös käyttörajoitusten sekä salassapitovelvoitteen toteuttamiseen.

Jotta voitaisiin varmistaa, että siirtymäajan jälkeen tietoaineistojen käsittely tapahtuisi vain tietoturvallisissa käyttöympäristöissä, niin lausuntojen johdosta esitystä on muutettu siten, että ennen mainittua ajankohtaa tietoaineistoja voitaisiin luovuttaa vain määräaikaisilla enintään 30.4.2022 voimassa olevilla tietoluvilla luvansaajan käsiteltäväksi, vaikka tietolupahakemuksessa ei osoitettaisi toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle. Sen sijaan myös siirtymäajan aikana tietoaineistoja voisi luovuttaa tietoturvalliseen käyttöympäristöön. Sen osalta ei esitetä määräaikaista sääntelyä tietoluvan kestosta.

Lisäksi säätämisjärjestysperusteluissa on vielä tarkemmin täsmennetty, miten jo nyt voimassa oleva lainsäädäntö asettaa tietosuojaa ja tietoturvan tasoa koskevia vaatimuksia ja miten Tietolupaviranomaisen menettelyt toimivat, kun tietoaineistoja luovutetaan tietoluvan saajille. Toisin kuin apulaisoikeusasiamiehen viittaamassa perustuslakivaliokunnan lausunnossa on todettu, tietoaineistoja ei toisiolain perusteella voida luovuttaa kehittämis- ja innovaatiotoimintaan muuta kuin tietopyynnön perusteella ja vain aggregoituina tilastoina. Säätämisjärjestysperusteluissa on lisäksi käyty läpi lisäsuojatoimia, joita toisiolakiin lisättiin perustuslakivaliokunnan lausunnon jälkeen.

7 Säännöskohtaiset perustelut

60 §. *Siirtymäsäännökset*. Ehdotetun pykälän *1 momenttia* ehdotetaan muutettavaksi siten, että toisiolain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sovellettaisiin 1 päivästä toukokuuta 2022.

Tietoturvallinen käyttöympäristö on toisiolain hallituksen esitykseen kirjoitettu keskeinen toimi, joka turvaa yksilön henkilötietojen suojaa. Tietoturvallisella käyttöympäristöllä on merkittävä rooli väärinkäytösten estämisessä ja kyberturvallisuuden toteuttamisessa. Se on myös kilpailuetu Suomelle, koska voimme siten osoittaa, että täällä huolehditaan vahvasti arkaluonteisten henkilötietojen suojasta. Myös yleisessä tietosuoja-asetuksessa edellytetään riittäviä suojatoimia, kun käsitellään arkaluonteisia henkilötietoja.

Tietolupaviranomaiselta saadun tiedon mukaan 1.5.2021 mennessä ei kenelläkään toimijalla, Tietolupaviranomaista lukuun ottamatta, ole toisiolain 20 §:n edellyttämää tietoturvallista käyttöympäristöä, jonne Tietolupaviranmainen voisi luovuttaa tietoaineiston luvansaajan käsiteltäväksi. Tietolupaviranomaisen käyttöympäristö ei kuitenkaan vielä pysty käsittelemään kaikkea sellaista tietoaineistoa, joita erityisesti lääketieteen tutkimuksessa olisi tarve käsitellä. Esimerkkinä voi mainita terveydenhuollon kuvantamisaineistot (esimerkiksi röntgenkuvat, ultraäänikuvat ja EKG-tallenteet), jotka kuuluvat aineistona toisiolain soveltamisalan piiriin. Kuvantamisaineistot edellyttävät käytännössä laitteistoja ja ohjelmistoja, joita on vain terveydenhuollon toimijoilla. Tämänkin vuoksi on tärkeää, että muun muassa merkittävimmät terveydenhuollon toimijat Suomessa ehtisivät auditoida omat käyttöympäristöt toisiolain ja Tietolupaviranomaisen vaatimuksia vastaaviksi ja siten pystyisivät käsittelemään näitä erityisiä tietoaineistoja myös omissa ympäristöissään. Hallituksen näkemyksen mukaan tämä tulisi tapahtua ilman aiheetonta

viivytystä, mutta kuitenkin viimeistään 1 päivästä toukokuuta 2022. On oletettava, että viimeistään silloin alan toimijoiden tietoturvalliset käyttöympäristöt olisi auditoitu toisiolain edellyttämällä tavalla siten, että luvansaajan auditoituun tietoturvalliseen käyttöympäristöön tietoaineistoja voisi luovuttaa toisiolain mukaisesti. Ennen mainittua ajankohtaa tietoja voitaisiin kuitenkin luovuttaa enintään 30.4.2022 saakka voimassa olevilla 43 §:n 4 momentin mukaisilla määräaikaisilla tietoluvilla luvansaajan käsiteltäväksi toisiolain 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle. Sen sijaan myös siirtymäajan aikana tietoaineistoja voisi luovuttaa käyttöympäristöön, joka jo täyttää lain 20 §:n 3 momentin ja 21–34 §:n tietoturvalliselta käyttöympäristöltä edellytettävät vaatimukset.

Koska toisiolain 55 §:n merkittävää kliinistä löydöstä koskevat tekniset muutokset edellyttävät muutoksia potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tietoturvallisiin käyttöympäristöihin, lain edellyttämät muutokset eivät ole toteutettavissa 1.5.2021 mennessä. Muutokset olisit kustannustehokasta yhdistää asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja koskeviin muutosehdotuksiin. Muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan 1. päivänä tammikuuta 2024. Tämän takia 1 momenttia ehdotetaan muutettavaksi siten, että toisiolain 55 §:ää kliinisistä löydöksistä sovellettaisiin 1 päivästä tammikuuta 2024.

Pykälän *1 momentissa* olevaa siirtymäaikaa toisiolain 19 §:ää lokitiedoista ei tässä yhteydessä ehdoteta muutettavaksi. Lokitietoja koskeva vaatimus on keskeinen keino, joilla rekisteröity, rekisterinpitäjä ja viranomaiset voivat seurata ja valvoa toisiolain soveltamisalaan kuuluvien korostetusti arkaluonteisten henkilötietojen käsittelyä. Lisäksi vastaava velvoite koskee viranomaisia jo tiedonhallintalaissa säädetyllä tavalla.

8 Voimaantulo

Jotta toisiolain mukaisten tietolupien myöntäminen voisi jatkua mahdollisesti keskeytyksettä, laki ehdotetaan tulemaan voimaan mahdollisimman pian, kun se on vahvistettu.

9 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 § 4 momentin korkean tason asiantuntijaryhmän kanssa varmistaen, että toiminnassa hyödynnetään asianmukaisella tavalla teknologian kehitystä turvaamaan henkilötietojen suoja.

Pääministeri Sanna Marinin hallituksen ohjelman 2019 tavoitteena on, että Suomi on kansainvälisesti houkutteleva paikka opiskella, tutkia ja investoida. Hallitusohjelmassa todettu keino olisi muun muassa, että Suomeen laaditaan pitkän aikavälin suunnitelma, jonka avulla TKI-

toimintaympäristö paranee, ja sitä kautta yksityisten ja julkisten investointien ja rahoituksen tasossa tavoitellaan neljän prosentin bruttokansantuoteosuutta. Lisäksi edistetään Suomen houkuttelevuutta kansainvälisten sekä kotimaisten yritysten tutkimus- ja kehitystoiminnan sijoitusmaana ja vahvistetaan suomalaisen tutkimus- ja tiedeyhteisön kansainvälistä kilpailukykyä ja vetovoimaa panostamalla tutkimusympäristöihin ja tutkimusinfrastruktuureihin.

Henkilötietojen käsittelyllä tulisi lähtökohtaisesti olla samat vaatimukset koko EU-alueella, riippumatta siitä, käsitelläänkö henkilötietoja Suomessa vai muualla EU- alueella. Kansainväliset tutkijat voivat käsitellä toisiolain mukaista henkilötason rekisteritietoja ainoastaan Tietolupaviranomaisen tietoturvallisessa käyttöympäristössä tai mahdollisesti muissa siihen mennessä auditoiduissa suomalaisissa käyttöympäristöissä. Aggregoituja aineistoja voidaan kuitenkin luovuttaa vapaasti käyttöön. Lääketieteen tutkimus on luonteeltaan kansainvälistä ja tutkimusta tehdään hyvin usein kansainvälisissä konsortioissa. Vaikeutta syntyy nyt siirtymäajan määräajan jälkeenkin erityisesti kansainvälisten tutkimusten osalta, jossa Suomesta saatava tietoaineisto on vain osa muista maista kerättävää tietoaineistoa, jota tutkimuksessa käytetään. Toisiolaki edellyttää, että Suomesta saatava tietoaineisto luovutetaan vain auditoituun tietoturvalliseen käyttöympäristöön, riippumatta siitä, missä tämä käyttöympäristö sijaitsee maantieteellisesti. Ulkomaisilla toimijoilla ei ole kattavaa tietoa tästä auditointivelvoitteesta, eikä kukaan ulkomainen toimija ole ryhtynyt auditoimaan omia järjestelmiä toisiolain perusteella. Kansainvälisten tutkimusten siirtymistä suuressa määrin Tietolupaviranomaisen tai muiden suomalaisten toimijoiden käyttöympäristöihin ei voida pitää todennäköisenä vaihtoehtona. Kansainvälisillä toimijoilla ei arvioida olevan kiinnostusta suomalaisten vaatimusten mukaiseen oman käyttöympäristönsä auditointiin kuin yksittäistapauksissa. Tilanne on johtamassa siihen, että suomalaisen datan hyödyntäminen kansainvälisessä tutkimuksessa ja siten suomalaisten tutkijoiden mahdollisuus osallistua kansainvälisiin tutkimuksiin vaikeutuu. Tutkimuksissa yhdistyy nykyisin hyvin usein ns. rekisterityyppinen tutkimus, biopankista saatavat näytteet, ja kliininen tutkimus (joko lääketutkimus tai muu lääketieteellinen, kajoava tutkimus). Tutkimuksia ei siis yleensä tehdä per lainsäädäntö, vaan tutkimuksissa yhdistyvät nykyisin useat Suomessa voimassa olevat erilaiset tutkimuslainsäädännöt. Toisiolaki on sote-tietojen ja eräiden niihin liitettävien rekisteritietojen yleislainsäädäntö toisiokäyttöön.

Sosiaali- ja terveysministeriössä on tarkoitus perustaa työryhmä, jossa alan johtavat tieturva- ja tietosuoja-asiantuntijat, toisiolakia ohjaavat ja valvovat viranomaiset ja alan keskeiset toimijat selvittävät, millaisia tietoturvaa koskevia lainsäädännöllisiä vaatimuksia toisiolaissa voitaisiin jatkossa asettaa, mikäli tietoaineistoja halutaan luovuttaa muihin kuin Suomessa auditoituihin tietoturvallisiin käyttöympäristöihin. Tarkoituksena on, että työryhmän työn tuloksena valmistellaan hallituksen esitysluonnos vuoden 2021 aikana kansainvälisiin luovutuksiin sovellettavista tietoturvaa koskevista toisiolain säännöksistä, jolla turvataan myös kansainvälinen tutkimus tietoturvallisesti ja tietosuojaa kunnioittaen.

10 Suhde muihin esityksiin

10.1 Esityksen riippuvuus muista esityksistä

Esityksellä on toisiolain 55 §:n siirtymäajan muuttamisen osalta liittymä asiakastietolain hallituksen esitykseen (HE 212/2020), joka on eduskunnan sosiaali- ja terveysvaliokunnan käsittelyssä. Toisiolain 55 §:n mukaiset muutokset olisi kustannustehokkainta ajoittaa siten, että ne tehtäisiin samalla kuin esitettyyn tahdonilmaisupalveluun ja kieltoihin on esitetty tehtävän muutoksia 1. tammikuuta 2024 mennessä.

10.2 Suhde talousarvioesitykseen

Esityksellä ei katsota olevan merkittävä talousarvioesitysvaikutuksia. Esityksen talousarviovaikutukset on arvioitu toisiolain hallituksen esityksessä (HE 159/2017) ja asiakastietolain hallituksen esityksessä (HE 212/2020 vp). Koska kyse on vain siirtymäajan siirtämisestä, tässä yhteydessä ei ole tarvetta arvioida erityisiä talousarviovaikutuksia.

11 Suhde perustuslakiin ja säätämisjärjestys

Yksityiselämän suoja

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

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).

Ehdotetulla lailla täsmennettäisiin ja täydennettäisiin yleistä tietosuoja-asetusta niiltä osin kuin se on kansallisen liikkumavaran puitteissa mahdollista ja tarkoituksenmukaista.

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).

Yleistä tietosuoja-asetusta yksityiskohtaisemman sääntelyn tarve tulee kuitenkin perustella myös tietosuoja-asetuksen puitteissa tapauskohtaisesti. Tällöin on syytä kiinnittää huomiota myös asetuksessa omaksuttuun riskiperusteiseen lähestymistapaan. Valiokunta on painottanut, että myös arkaluonteisten henkilötietojen käsittelyä koskevan sääntelyn kohdalla on syytä pyrkiä selkeään ja ymmärrettävään lainsäädäntöön (PeVL 14/2018 vp, s. 6).

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).

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).

Tämän hallituksen esityksen tietosuoja- ja tietoturvavaikutuksia koskevissa kohdissa on kuvattu tietosuojaa ja tietoturvaa koskevista järjestelyistä, jotka ovat jo nyt kattavasti voimassa.

Toisiolaissa on säännökset, jotka koskevat sosiaali-, terveys- ja hyvinvointitietojen hyödyntämistä muuhun kuin siihen tarkoitukseen jossa henkilötiedot on alun perin tallennettu. Laki sisältää mahdollisimman tarkkarajaisesti ne käyttötarkoitukset, joihin sanottuja tietoja voidaan luovuttaa, sekä perusteet joilla luovutuspäätös tulee ratkaista. Käyttötarkoituksista on säädetty yksityiskohtaisesti. Henkilötietoja voitaisiin luovuttaa näihin käyttötarkoituksiin salassapitovelvollisuuden estämättä. Henkilötietojen käsittely on lisäksi useissa kohdin sidottu välttämättömyysvaatimukseen.

Toisiolakiin sisältyy merkittäviä määrä teknisiä ja muita turvatakeita, joiden avulla voitaisiin varmistua siitä, että luovutuksensaaja käsittelee tietoja rekisteröidyn yksityiselämän suojaa turvaten silloin, kun pyydetyt tiedot olisi käyttötarkoituksen vuoksi välttämätöntä luovuttaa poikkeuksellisesti henkilötunnuksin tai siten, että rekisteröity voitaisiin muutoin tunnistaa välillisesti.

Rekisteröidyn oikeuksia ja vapauksia suojataan muun muassa siten, että henkilötietoja voisi pääsääntöisesti käsitellä vain viranomaisen myöntämän tietoluvan perusteella ja luvansaajaa koskisi salassapitovelvollisuus. Salassapitovelvollisuus on merkittävä myös perustuslain 12 §:n 2 momentissa säädetyn julkisuusperiaatteen näkökulmasta. Eduskunta on korostanut, että viranomaisten tietojen salassapitoa koskevia säännöksiä tulisi erityislainsäädännön sijaan sisällyttää keskitetysti julkisuuslakiin (PeVL 25/2010 vp, s. 3, PeVL 2/2008 vp, s. 2). Mainitussa 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, ja niiden käsittelylle luotaisiin lain 3 luvun mukaiset palvelut viimeistään 1. toukokuuta 2022. Palveluihin sisältyy tietoturvallinen käyttöympäristö. Henkilötiedot voisi luovuttaa vain tällaiseen käyttöympäristöön 1.5.2022 alkaen. Jotta voitaisiin varmistaa, että siirtymäajan jälkeen tietoaineistojen käsittely tapahtuisi vain tietoturvallisissa käyttöympäristöissä, niin lausuntojen johdosta esitystä on muutettu siten, että ennen mainittua ajankohtaa tietoaineistoja voitaisiin luovuttaa vain määräaikaisilla enintään 30.4.2022 voimassa olevilla tietoluvilla luvansaajan käsiteltäväksi, vaikka tietolupahakemuksessa ei osoitettaisi toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle. Sen sijaan myös siirtymäajan aikana tietoaineistoja voisi luovuttaa käyttöympäristöön, joka jo täyttäisi lain 20 §:n 3 momentin ja 21–34 §:n tietoturvalliselta käyttöympäristöltä edellytettävät vaatimukset.

Tietoluvan myöntäneen viranomaisen olisi valvottava luvan ehtojen noudattamista. Lisäksi sen olisi raportoitava 53 §:n mukaisesti tietosuojavaltuutetulle tietojen käsittelystä.

Rekisteröityjen yhdenvertaisen kohtelun kannalta toisiolaki turvaa sen, että sosiaali- ja terveystietojen sekä muiden yksityiselämän suojan piiriin kuuluvien hyvinvointitietojen hyödyntämistä koskevat tulkintalinjaukset ja päätökset muodostuisivat mahdollisimman yhteneviksi. Keskitetty lupamenettely turvaa yksityiselämän suojaa myös siten, että henkilötietojen käsittelyä voitaisiin minimoida silloinkin, kun saman tiedonhyödyntämissuunnitelman perusteella tarvitaan useiden eri rekisterinpitäjien terveyteen ja hyvinvointiin liittyviä tietoja.

Vaikka toisiolaissa säädetty tietoturvallinen käyttöympäristö on keskeinen toimi tietoturvaa ja tietosuojaa varmistamassa, ei se kuitenkaan ole ainoa keino varmistaa tietoturva ja tietosuoja. Siirtymäajan siirrosta huolimatta toisiolaissa olisi edelleen voimassa se vahva ja selkeä periaate, että tieto luovutetaan ensisijaisesti aina Tietolupaviranomaisen omaan tietoturvalliseen käyttöympäristöön.

Erityisesti on otettava huomioon, että jo yleinen tietosuoja-asetus, tietosuojalaki, tiedonhallintalaki, laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista, laki potilaan asemasta ja oikeuksista (785/1992, potilaslaki), laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000, sosiaalihuollon asiakaslaki), asiakastietolaki ja muun muassa toisiolain 18 § asettaa jo paljon tietosuojaa ja tietoturvaa koskevia vaatimuksia toisiolain mukaisten tietoaineistojen käsittelylle. Toisiolaissa 10 §:ssä on lisäksi useita myös tietoturvan tasoa parantavia palveluita, kuten esimerkiksi tietojen kokoamis-, yhdistämis- ja esikäsittelypalvelu, tunnisteiden hallinnointipalvelu, tietopyyntöjen hallintajärjestelmä ja tietoturvallinen käyttöpalvelu. Toisiolakiin lisättiin perustuslakivaliokunnan lausunnon jälkeen lisäksi useita suojatoimia, jotka ovat jo nyt käytössä. Näitä ovat muun muassa anonymisointitehtävän ja aggregoitujen tilastojen muodostaminen vain Tietolupaviranomaisen tehtäväksi, kehittämis- ja innovaatiotoiminnan käyttötarkoitus on mahdollista vain tietopyynnöillä ja aggregoiduilla tilastoilla, erilliset tietopyyntöä ja tietolupaa koskevat prosessit, tietoluvan perusteella tietoaineisto

ensisijaisesti luovutetaan luvansaajalle Tietolupaviranomaisen käyttöympäristöön ja julkaistavien tulosten anonymiteetin varmistamisprosessi sekä Tietolupaviranomaisen tueksi asetettu korkean tason asiantuntijaryhmä, jonka tehtävänä on laatia anonymisointia, tietosuojaa ja tietoturvaa koskevat Tietolupaviranomaisen toiminnan periaatelinjaukset. Kyseissä asiantuntijaryhmässä on oltava tekoälyn, data-analytiikan, tietoturvan, tietosuojan, alan tutkimuksen, tilastotieteen ja tilastotoimen asiantuntija sekä Tietolupaviranomaisen edustaja.

Siltä osin kuin Tietolupaviranomainen on tietoa luovuttanut muuhun kuin Tietolupaviranomaisen omaan käyttöympäristöön, on suurimmassa osassa tilanteista ollut kyse joko Terveyden ja hyvinvoinnin laitoksen omista tutkimushankkeista tai siitä, että tieto on luovutettu Tilastokeskuksen vastaavaan tietoturvalliseen ympäristöön (”Fiona”). Lisäksi tietoaineistoa on luovutettu yliopistosairaaloiden omiin tietoympäristöihin, tai yliopistojen hallinnoimiin sijainteihin. Vain muutamissa, yksittäisissä tilanteissa tieto on luovutettu joko yksityisen toimijan hallintaan tai ulkomaille. Siten valtaosa muualle luovutettujen tietojen hallinnoijista ovat joko kotimaisia viranomaisia tai kotimaisia erikoissairaanhoidon toimijoita, joiden hallussa on jo muutoinkin merkittävä määrä terveystietoa ja jotka kuuluvat asiakastietolain (159/2007) perusteella A-luokan järjestelmien piiriin.

Tietolupaviranomainen vaikuttaa jo nyt toiminnallaan tietoturvaa ja -suojaa parantavasti. Tietolupaviranomainen harkitsee lupaprosessissa varsin tarkasti useita erilaisia, tietoturvaan ja -suojaan liittyviä seikkoja. Tietolupaviranomainen käy ensinnäkin luvanhakijan kanssa hyvin tarkasti läpi, mitä tietoja ja kuinka paljon haettavaan käyttötarkoitukseen tarvitaan. On hyvin tavanomaista, että hakemusprosessin aikana tietoaineisto tarkentuu merkittävästi siitä, mitä on alun perin haettu. Tietolupaviranomainen ei arvioi tutkimuksen tai muunkaan haettavan käyttötarkoituksen tarpeellisuutta tai tarkoituksenmukaisuutta. Se arvioi kuitenkin, tarvitaanko sanottuun käyttötarkoitukseen niin paljoa tietoa kuin on haettu, ja onko haettava tieto tarkoitukseensa sopivaa.

Tietolupapäätöksessä Tietolupaviranomainen yksilöi muuttujakohtaisesti ne tiedot, joiden käyttöön se antaa luvan. Tämäkin parantaa tietosuojaa. Luvat myönnetään määräaikaisena, keskimäärin korkeintaan viiden vuoden määräajaksi. Lupaa ei siis saa toistaiseksi. Lupaan liitetään erilliset lupaehdot, jotka sisältävät määräyksiä tietosuojan ja turvan suojaamisen näkökulmasta. Jos ehtoja ei noudateta, on Tietolupaviranomaisella oikeus perua myöntämänsä lupa. Tällaisia peruuttamistilanteita ei ole syntynyt, mutta muutamissa tilanteissa Tietolupaviranomainen on huomauttanut hakijaa lupaehtojen noudattamisen tärkeydestä. Tietolupaviranomaisen näkemyksen mukaan sen laatimat lupapäätökset ja niihin liitettävät lupaehdot ovat tarkemmalla tasolla kuin mitä on ollut tilanne lupapäätösten suhteen ennen toisiolakia.

Tiedot kerätään ja luovutetaan luvanhakijalle ensisijaisesti niin, että aineisto tulee ensin Tietolupaviranomaiselle, joka yhdistää aineistot keskenään sekä pseudonymisoi sen. Aineiston lähettäminen tapahtuu toisiolaissa säädettyä sähköistä, tietoturvallista sähköistä kanavaa pitkin. (koska henkilötiedot ovat tutkimusryhmällä tai osalla siitä tiedossa).

Siirtymäajan aikana ala toimijat voivat auditoida ympäristönsä. Lisäksi rekisteröidyillä on käytettävissään myös siirtymäajan aikana kaikki yleisen tietosuoja-asetuksen mukaiset rekisteröidyn oikeudet ja tietoaineistoja käsittelevillä tahoilla jo kaikesta muusta lainsäädännöstä ja toisiolaista seuraavat velvoitteet. Toisiolain 18 §:n mukaan, kun henkilötietoja käsitellään toisiolain nojalla, 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. Voimassa oleva sääntely on itse asiassa tietoturvan ja tietosuojan osalta jo sellaisenaan kattavampaa kuin Euroopan

parlamentin ja neuvoston asetus (EU) N:o 536/2014, annettu 16 päivänä huhtikuuta 2014, ihmisille tarkoitettujen lääkkeiden kliinisistä lääketutkimuksista ja direktiivin 2001/20/EY kumoamisesta.

Toisiolain 55 §:n 5 momentissa säädettäisiin potilaan mahdollisuudesta kieltää kliinisesti merkittävän löydöksen perusteella tehtävät yhteydenotot. Potilas voisi kieltää ne jo ennakolta sähköisesti asiakastietolaissa (159/2007) tarkoitetun kansalaisen käyttöliittymän (Omakanta-palvelu) välityksellä taikka tekemällä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toimintayksikössä, jolloin kielto kirjataan asiakastietolain 14 a §:ssä tarkoitettuun potilaan tiedonhallintapalveluun. Toisaalta potilas voisi kieltäytyä yksittäisen yhteydenoton perusteella ehdotetuista tiedoista, tutkimuksista ja hoidosta. Kielto-oikeudella ja toisiolain 55 §:n mukaisilla menettelyillä turvataan yksityisyyden suoja heti, kun 55 § astuisi voimaan, kuten myös merkittävistä kliinisistä löydöistä ilmoittaminen.

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 lennonvarmistustehtävien jakamista (PeVL 47/2005 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. Toisiolain 20 §:ssä tarkoitetun tietoturvallisen käyttöympäristön voisi perustaa muukin kuin viranomainen, myös yksityisoikeudellinen oikeushenkilö. Käyttöympäristössä käsiteltäisiin henkilötietoja. Säännös on arvioitava henkilötietojen suojaa koskevan perustuslain 10 §:n lisäksi myös perustuslain 124 §:n kannalta.

Siirtymäajan jälkeen Tietolupaviranomaisen tietoturvallinen käyttöympäristö olisi aina ensisijainen paikka, johon henkilötiedot luovutettaisiin. Tietolupaviranomaisen käyttöympäristö ei kuitenkaan välttämättä aina mahdollista tietojen käsittelyä luvansaajan tarpeisiin, koska tietoja voidaan käsitellä niin monella eri tavalla. Eri käyttötarkoituksissa saatetaan tarvita erilaisia työkaluja, joita Tietolupaviranomaisen ei ole aina mahdollista tarjota luvansaajalle. Esimerkiksi tieteellistä tutkimusta voidaan toteuttaa monin eri metodein ja niissä saatetaan tarvita erilaisia analyysityökaluja. Tietolupaviranomaisen käyttöympäristö ei tästä syystä aina käytännössä mahdollistaisi tietojen käsittelyä tietolupaahakemuksessa esitettyyn, sinänsä asialliseen henkilötietojen käyttötarkoitukseen.

Tietolupaviranomaisen käyttöympäristön ei pitäisi rajoittaa sinänsä perustuslainmukaisen käyttötarkoituksen toteutumista. Tämän vuoksi olisi tarkoituksenmukaista, että tietoja voisi 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 voitaisiin siirtää muuhun kuin Tietolupaviranomaisen 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 suorittaisi järjestelmille auditoinnin, millä varmistuttaisiin vähimmäisvaatimusten täyttymisestä. Sosiaali- ja terveysalan lupa- ja valvontaviranomaisen olisi valvottava järjestelmiä. Luvansaajaa sitoisi lisäksi salassapitovelvollisuus. Tietosuojavaltuutettu toimialallaan ja Sosiaali- ja terveysalan käyttölupaviranomainen laissa säädetyin edellytyksin valvoisivat sitä, että henkilötietoja käsitellään lain ja lupaehtojen mukaisesti. Näin kyettäisiin nykytilannetta paremmin 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.

Toisiolain 55 §:ssä säädettäisiin oikeuksista ja velvollisuuksista, joita eri toimijoille syntyisi, jos terveydenhuollon asiakastietoja tai niitä sisältäviä rekisteritietoja toisiolain mukaisesti käsiteltäessä havaittaisiin kliinisesti merkittävä löydös. Pykälän 1 momentin mukaan tietoluvan saajalla, joka käsittelee terveydenhuollon asiakastietoja tai niitä sisältäviä rekisteritietoja ehdotetun lain perusteella, olisi oikeus ilmoittaa kliinisesti merkittävästä löydöksestä. Edellytyksenä olisi, että löydöksen perusteella olisi ilmoittajan ammatillisen käsityksen mukaan mahdollista ehkäistä tietyn potilaan terveyteen liittyvää riskiä tai parantaa merkittävästi hoidon laatua. Kuten edellä on todettu, perustuslain 10 §:ssä ei edellytetä, että henkilötietoja käsittelee viranomainen. Ilmoitus sen sijaan tehtäisiin asian merkittävyyden takia Tietolupaviranomaisen nimeämälle vastuuhenkilölle.

Tietolupaviranomaisen vastuuhenkilön olisi toisiolain 55 §:n 2 momentin mukaan ilmoituksen saatuaan koodattava mahdollisesti pseudonymisoidut tiedot auki ja selvitettävä, ketä tai keitä tieto koskee, sekä toimitettava tiedot ilman aiheetonta viivytystä Terveyden ja hyvinvoinnin

laitoksen nimeämälle asiantuntijalle. Tehtävä on toisiolain hallituksen esityksessä esitetty säädettäväksi asian edellyttämän erityisasiantuntemuksen vuoksi Terveyden ja hyvinvoinnin laitoksen asiantuntijalle, jonka olisi yhteistyössä laitoksen nimeämien muiden asiantuntijoiden kanssa arvioitava tiedon merkittävyys ja sen pohjalta toteutettavissa olevien toimenpiteiden odotettavissa oleva hyöty. Jos hyöty arvioidaan niin ilmeiseksi, että tutkittava olisi tärkeää saada hoidon piiriin, on edellä mainitun asiantuntijan ilmoitettava löydöksestä kunkin henkilön terveydenhuollosta alueellisesti terveydenhuoltolain nojalla vastuussa olevalle toimintayksikölle.

Terveydenhuollon toimintayksikön olisi 55 §:n 4 momentin mukaan tiedon saatuaan otettava yhteys potilaaseen ja selvitettävä, haluaako tämä tiedon kliinisesti merkittävästä löydöksestä ja sen mahdollisesti edellyttämistä tutkimus- ja hoitotoimenpiteistä sekä niistä odotettavissa olevasta hyödystä.

Edellä mainituilla perusteilla lakiehdotus voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä. 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 60 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019) 60 §:n 1 momentti seuraavasti:

60 §

Siirtymäsäännökset

Tämän lain 19 §:ää lokitiedoista sovelletaan 1 päivästä toukokuuta 2021. Tämän lain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sovelletaan 1 päivästä toukokuuta 2022. Ennen mainittua ajankohtaa tietoja voidaan luovuttaa luvansaajan käsiteltäväksi 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle. Tietojen luovuttaminen edellyttää tällöin 43 §:n 4 momentin nojalla määräajaksi annettua tietolupaa, joka on voimassa enintään 30 päivään huhtikuuta 2022. Tämän lain 55 §:ää kliinisistä löydöksistä sovelletaan 1 päivästä tammikuuta 2024.

———————————————————————————————————————

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä 27.05.2021

Pääministeri

Sanna Marin

Perhe- ja peruspalveluministeri Krista Kiuru

Liite
Rinnakkaisteksti

Laki

sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019) 60 §:n 1 momentti seuraavasti:

Voimassa oleva laki	*Ehdotus*
60 §	60 §
Siirtymäsäännökset	*Siirtymäsäännökset*
Tämän lain 19 §:ää lokitiedoista, 20 §:n 3 momenttia ja 21–34 §:ää tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sekä 55 §:ää kliinisistä löydöksistä sovelletaan 1 päivästä toukokuuta 2021. Ennen mainittua ajankohtaa tietoja voidaan luovuttaa luvansaajan käsiteltäväksi 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle.	Tämän lain 19 §:ää lokitiedoista *sovelletaan 1 päivästä toukokuuta 2021. Tämän lain 20 §:n 3 momenttia ja 21–34 §:ää tietoturvalliselta käyttöympäristöltä edellytettävistä vaatimuksista sovelletaan 1 päivästä toukokuuta 2022.* Ennen mainittua ajankohtaa tietoja voidaan luovuttaa luvansaajan käsiteltäväksi 51 §:n 1 ja 2 momentin nojalla, vaikka tietolupahakemuksessa ei osoitettaisi 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle. *Tietojen luovuttaminen edellyttää tällöin 43 §:n 4 momentin nojalla määräajaksi annettua tietolupaa, joka on voimassa enintään 30 päivään huhtikuuta 2022. Tämän lain 55 §:ää kliinisistä löydöksistä sovelletaan 1 päivästä tammikuuta 2024.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20 .