SOSIAALI- JA TERVEYSMINISTERIÖ

Hallitusneuvos Joni Komulainen

Eduskunta
Perustuslakivaliokunta

Asia: HE 96/2021 vp Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta

SOSIAALI- JA TERVEYSMINISTERIÖN LAUSUNTO PERUSTUSLAKIVALIOKUNNALLE

Eduskunnan perustuslakivaliokunta on pyytänyt asiantuntijalausuntoa hallituksen esityksestä eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta.

Sosiaali- ja terveysministeriö toteaa lausuntonaan seuraavaa:

Nykytila ja tausta

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 aiempaa huomattavasti laajemman sosiaali- ja terveydenhuollon asiakas- ja potilastiedon hyödyntämisen muussa kuin kyseisen tiedon alkuperäisessä käyttötarkoituksessa sosiaali- ja terveydenhuollon palvelujärjestelmässä.[1]

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 mah-

[1] ks. tarkemmin https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L2P6 ja https://findata.fi/palvelut/aineistot/#yleinen

SOSIAALI- JA TERVEYSMINISTERIÖ

dollistaa 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. 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.

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.

SOSIAALI- JA TERVEYSMINISTERIÖ

Suomessa hyödynnetään muun muassa kansallisen turvallisuusviranomainen NSA:n kansallista turvallisuusauditointikriteeristö Katakria.[2] 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.

Tietoturvaa koskevia auditointeja tekevät Suomessa Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, erikseen Traficomin hyväksymät arviointilaitokset (muun muassa KPMG ja Nixu), eräät tietoturvayritykset ja organisaatioiden sisäiset riippumattomat toimijat. Korkeimmasta tarkastustasosta 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.[3] 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.[4] 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.

Toisiolain 60 §:n 1 momentissa säädetään siirtymäajasta, jonka jälkeen Tietolupaviran-omainen voisi luovuttaa luvansaajalle tunnisteellisia tietoja vain 20 §:n 3

---

[2] https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

[3] ks. Valtioneuvoston periaatepäätös LVM/2021/44 https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82

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

SOSIAALI- JA TERVEYSMINISTERIÖ

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. Siirtymä-ajan tarkoitus oli turvata se, ettei sosiaali- ja terveydenhuollon tutkimus ja moni muu toisiolain käyttötarkoitus esty lain voimaantultua. Asianomaisten toimintayksiköiden olisi kuitenkin velvollisuus huolehtia, että 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.

Tietolupaviranomainen antoi toisiolain mukaisen määräyksen (1/2020) tietoturvallisista käyttöympäristöistä 5.10.2020.[5] 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.

---

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

SOSIAALI- JA TERVEYSMINISTERIÖ

Tämä kuvattu läpikäynti on kestänyt noin 4 kuukautta. Ja auditointiin olisi jäänyt aikaa ennen lain siirtymäsäännöksen (1.5.2021) voimaantuloa noin 4-5 kuukautta.

Tietolupaviranomaiselta saadun tiedon mukaan 1.5.2021 mennessä ei kenelläkään toimijalla, Findataa lukuunottamatta, ollut toisiolain 20 §:n edellyttämällä todettua tietoturvallista käyttöympäristöä, jonne tietoaineistoja olisi voinut luovuttaa luvansaajan käsiteltäväksi. Tämä hetkisen tiedon mukaan vain Tietolupaviranomaisella ja Tilastokeskuksella on toisiolain edellyttämä tietoturvallinen käyttöympäristö. Nykyinen tilanne johtaa siihen, että 1.5.2021 alkaen usea sosiaali- ja terveydenhuollon tutkimus ja useat muutkin toisiolain mukaiset käyttötarkoitukset ovat muuttunut mahdottomaksi toteuttaa, koska ei ole käyttötarkoitukseen sopivia auditoituja tietoturvallisia käyttöympäristöjä, jonne tietoaineiston voisi tietoluvan perusteella luovuttaa. Tietolupaviranomaisen käyttöympäristö ei 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.[6] Lisäksi ulkomaisilla toimijoilla ei ole kattavaa tietoa auditointivelvoitteesta, eikä kukaan ulkomainen toimija ole ryhtynyt auditoimaan omia järjestelmiä toisiolain perusteella.[7]

55 § Merkittäviin kliinisiin löydöksiin perustuvat oikeudet, velvoitteet ja toimenpiteet

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, vas-

---

[6] Huhtikuussa 2021 auditoinnit olivat jo tilannet Istekki, PSHP, HUS, PSSHP, Terveystalo ja auditointiin olivat valmistautuneet VSHP, HY (ml FIMM ja Finngen), Tampereen YO ja HY.

[7] Kansainvälisten tutkimusten turvaamista ja tietoturvaa koskevat haasteet on tuotu esille hallituksen esityksen kohdassa ”Toimeenpano ja seuranta”.

SOSIAALI- JA TERVEYSMINISTERIÖ

tuuhenkilön 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 tiedonhallinta-palveluun. 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.

Esityksen pääasiallinen sisältö

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. 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

SOSIAALI- JA TERVEYSMINISTERIÖ

aikana tietoaineistoja voisi luovuttaa tietoturvalliseen käyttöympäristöön. Sen osalta ei esitetä määräaikaista sääntelyä tietoluvan kestosta

Sen sijaan toisiolain 60 §:n 1 momentissa olevaa siirtymäaikaa koskien lain 19 §:ää loki-tiedoista 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. Tietolupaviranomainen itse kerää edellä mainittua lokitietoa.

55 § Merkittäviin kliinisiin löydöksiin perustuvat oikeudet, velvoitteet ja toimenpiteet

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 vaan edellyttävät paljon enemmän työtä ja aikaa. Lausuntojen mukaan muutokset olisi perusteltua yhdistää uuden asiakastietolain hallituksen esityksessä (HE 212/2020 vp) esitettyyn tahdonilmaisupalvelua ja kieltoja, koskeviin muutosehdotuksiin. Muutokset olisi tehtävissä siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024. Hallitus esittää edellä mainitun takia siirtymäsäännöstä muutettavaksi siten, että lain merkittäviin kliinisiin löydöksiin perustuvia oikeuksia, velvoitteita ja toimenpiteitä sovellettaisiin 1 päivästä tammikuuta 2024.

Esityksen perustuslain mukaisuus

Toisiolain hallituksen esityksessä (HE 159/2017) ja tämän hallituksen esityksen säätämisjärjestysperusteluissa on arvioitu yksityiskohtaisesti erityisesti esitysten 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.

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

SOSIAALI- JA TERVEYSMINISTERIÖ

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 (HE 96/2021 vp) tietosuoja- ja tietoturvavaikutuksia koskevissa kohdissa on kuvattu tietosuojaa ja tietoturvaa koskevista järjestelyistä, jotka ovat jo nyt kattavasti voimassa.

SOSIAALI- JA TERVEYSMINISTERIÖ

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. Li-säksi sen olisi raportoitava 53 §:n mukaisesti tietosuojavaltuutetulle tietojen käsittelystä.

SOSIAALI- JA TERVEYSMINISTERIÖ

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 suojatoimi 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. Toisiolain 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 innovaatio-toiminnan 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

SOSIAALI- JA TERVEYSMINISTERIÖ

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.

Yhteenveto

Myös ennen siirtymäsäännöksen voimaantuloa perustuslain 10 §:n turvaama oikeus yksityiselämään ja henkilötietojen suojaan pyritään 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 kiinnitettään jo nyt käyttörajoitusten sekä salassapitovelvoitteen toteuttamiseen.

Jotta voitaisiin varmistaa, että esitetyn siirtymäajan 1.5.2022 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

SOSIAALI- JA TERVEYSMINISTERIÖ

toisiolain 51 §:n 3 momentissa tarkoitettua tietoturvallista käyttöympäristöä tietojen käsittelylle. Sen sijaan myös siirtymäajan aikana tietoaineistoja voisi luovuttaa tietoturvalliseen käyttöympäristöön.

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.[8]

Toisiolain 55 §:n mukaisilla menettelyillä ja tahdonilmaisuilla turvataan yksityisyyden suojaa, kun 55 § astuisi voimaan. Kansaneläkelaitokselta ja Terveyden ja hyvinvoinnin laitokselta saadun tiedon mukaan toisiolain 55 §:n edellyttämät muutokset potilastietojärjestelmiin, valtakunnallisiin tietojärjestelmäpalveluihin ja tutkijoiden käyttämiin tietoturvallisiin käyttöympäristöihin eivät ole valmiita. Muutokset olisi tehtävissä siten, että toisiolain 55 § voisi astua voimaan aikaisintaan 1. päivänä tammikuuta 2024. Hallitus esittää tämä takia siirtymäsäännöstä muutettavaksi siten, että lain merkittäviin kliinisiin löydöksiin perustuvia oikeuksia, velvoitteita ja toimenpiteitä sovellettaisiin 1 päivästä tammikuuta 2024.

[8] 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.