SOSIAALI- JA TERVEYSMINISTERIÖ

Hallitusneuvos Joni Komulainen

Eduskunta
Sosiaali- ja terveysvaliokunta

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

SOSIAALI- JA TERVEYSMINISTERIÖN VASTINE SOSIAALI-JA TERVEYSVALIOKUNNALLE

Eduskunnan sosiaali- ja terveysvaliokunta on pyytänyt vastinetta hallituksen esityksestä eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain 60 §:n muuttamisesta annetuista asiantuntijalausunnoista.

Tietoturvalliselta käyttöympäristöltä edellytettävien vaatimusten voimaantulo

Kansaneläkelaitos on lausunnossaan tuonut esille, että he pitävät perusteltuna siirtymäsäännöksen muuttamista lain tietoturvalliselta käyttöympäristöltä edellytettävien vaatimusten osalta siten, että vaatimuksia sovellettaisiin vasta 1.1.2023. Kansaneläkelaitos pitää edelleen 12.4.2021 antamansa lausunnon kantaansa perusteltuna. Kelan mielestä esitys määräajaksi annetusta tietoluvasta 30.4.2022 saakka on kuitenkin perusteltu. Kela haluaa kuitenkin tuoda esiin, että tutkimuksen jatkuvuus on kyettävä turvaamaan riittävällä ohjeistuksella tilanteessa, kun tutkimus jatkuu määräaikaisen tietoluvan päättyessä.

Varsinaissuomen sairaanhoitopiiri toteaa lausunnossaan, että siirtymäajan pitäisi olla pidempi, vähintään kaksi vuotta, ja tänä aikana pitäisi kriittisesti arvioida, millaiset vaatimukset ovat realistisia, tutkimusta tukevia ja tietosuoja-asetuksen kanssa yhteensopivia. Käyttöympäristövaatimukset ovat tällaisenaan ristiriidassa EU:n yleisen tietosuoja-asetuksen tavoitteiden kanssa, joka ilmenee esim. suoraan 1 artiklan 3-kohdasta: ”Henkilötietojen vapaata liikkuvuutta unionin sisällä ei saa rajoittaa eikä kieltää syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä.” Näin ollen kyseinen säädös on ristiriidassa EU-lainsäädännön kanssa, eikä tällaiseen ole annettu kansallista liikkumavaraa.

Varsinaissuomen sairaanhoitopiiri toteaa myös, että toisiolain edellyttämiä järjestelmiä on myös joissain tilanteissa mahdotonta käytännössä rakentaa. Miten Findata tai kukaan muukaan rakentaa järjestelmän, joka mahdollistaa minkä tahansa tietojen tehokkaan käsittelyn, kun otetaan huomioon, että tiedot voivat olla missä muodossa tahansa (genomitieto, video, audio, teksti jne.)? Lisäksi on syytä huomioida myös se, että osa tiedoista voi olla tutkimuslaitekohtaisia, ja että niitä pitää voida käsitellä mitä erilaisimmilla ohjelmistoilla lisenssi- ja yhteensopivuus

SOSIAALI- JA TERVEYSMINISTERIÖ

vaatimuksineen. Lisäksi tietoihin pitäisi voida yhdistää mitä tahansa toisiolain ulkopuolista tietoa, sykemittaridataa, elämäntapatietoja jne. yms. Näin iso ja perustavanlaatuinen ongelma ei tule ratkeamaan vuoden tai varmasti kahdenkaan vuoden siirtymäajan aikana ja he pitävät tärkeänä, että siirtymäajan pidennys saadaan mahdollisimman pian voimaan, jotta he välttyvät tieteellisten tutkimusten estymiseltä.

Helsingin yliopisto esittää harkittavaksi, että siirtymäaika olisi jopa pidempi. Tarkoittaen, että tietoturvallisen käyttöympäristön vaatimuksia sovellettaisiin vasta 1 päivästä toukokuuta 2025. Siirtymäajan pituutta tulisi tarkastella tarkemmin yleiseurooppalaisten toimintamallien ja kehityksen näkökulmasta. Tämä edellyttää ehdotettua pidempää siirtymäaikaa (4v). Muualla kuin Suomessa ei ole olemassa
Suomalaiset kriteerit täyttäviä tietoturvallisia käyttöympäristöjä. Tietoturvallisen käyttöympäristön vaatimukset tulevat Helsingin yliopiston lausunnon mukaan vaikeuttamaan kansainvälistä lääketieteen tutkimusyhteistyötä. Euroopan komissiolla on valmisteilla europpalaista terveysdata-avaruutta (European Health Data Space) koskeva lainsäädäntöhanke, jonka komissio on käynnistynyt vuoden 2021 aikana. Lisäksi Euroopan parlamentti ja neuvosto ovat 25. marraskuuta 2020 antaneet ehdotuksen asetuksesta eurooppalaisesta datanhallinnosta (Data Governance Act).

Sosiaali- ja terveysministeriö toteaa vastauksenaan seuraavaa:

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. 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. Toisiolain mukaista 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.[1]

Tietolupaviranomainen antoi toisiolain mukaisen määräyksen (1/2020) tietoturvallisista käyttöympäristöistä 5.10.2020.[2] Määräyksen antaminen ja sen sisältö oli

[1] ks. Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla, jossa todetaan, että kaikille kriittisille toimialoille on oltava lakisääteiset tietoturvavaatimukset ja vaatimuksenmukaisuutta tulee arvioida säännöllisesti.
[2] https://www.findata.fi/uploads/2020/10/20ddc0dd-findata-maarays-1-2020-muiden-palveluntarjoajien-tietoturvallisille-kayttoymparistoille-asetettavat-vaatimukset.pdf

SOSIAALI- JA TERVEYSMINISTERIÖ

hyvin alan keskeisillä toimijoilla tiedossa ja määräysluonnoksesta saatiin paljon lausuntopalautetta. Tietolupaviranomaiselta saadun tiedon mukaan määräystä ja sen toimeenpanoon liittyviä toisiolain edellyttämiä toimia käytiin 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. 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 lukuun ottamatta, ollut toisiolain 20 §:n edellyttämällä todettua tietoturvallista käyttöympäristöä, jonne tietoaineistoja olisi voinut luovuttaa luvansaajan käsiteltäväksi. Tämä hetkisen tiedon mukaan Tietolupaviranomaisella ja Tilastokeskuksella on toisiolain edellyttämä tietoturvallinen käyttöympäristö. Nykyinen tilanne on johtanut siihen, että 1.5.2021 alkaen toisiolain tietoluvalla toteutettavat käyttötarkoitukset (muun muassa tieteellinen tutkimus henkilötiedoilla) ovat muuttunut mahdottomaksi toteuttaa, koska ei ole käyttötarkoitukseen sopivia auditoituja tietoturvallisia käyttöympäristöjä, jonne tietoaineiston voisi tietoluvan perusteella luovuttaa.[3] Tietolupaviranomaisen käyttöympäristö ei vielä pysty käsittelemään kaikkea sellaista tietoaineistoa, joita erityisesti lääketieteen tutkimuksessa olisi tarve käsitellä. 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. Asiasta saatujen tietojen mukaan alan keskeisiä toimijoita ovat tilanneet auditoinnin ja aloittaneet auditoinnin valmistelun.[4] Ministeriö kannustaa, että kaikki alan keskeiset toimijat toimisivat etupainotteisesti käyttöympäristöjen auditoinnin aloittamiseksi.

Tietoturvallisia käyttöympäristöjä koskeva vaatimus on ollut keskeinen toisiolain ehdotus. Se on lähes sellaisenaan ollut jo ihan ensimmäisissä toisiolain lakiluonnoksissa 2015-2016 ja lausuntokierroksella ja toisiolain moninaisissa valmistelun

[3] Sen sijaan tämä ei estä toisiolain kaikkia käyttötarkoituksia tietopyynnöillä, tietojohtamista, kehittämis- ja innovaatiotoimintaa tai sosiaali- ja terveydenhuollon viranomaisohjaus ja –valvontaa.

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

SOSIAALI- JA TERVEYSMINISTERIÖ

läpikäynneissä ja itse hallituksen esityksessä vuodesta 2017 lähtien. Tietoturvallisten käyttöympäristöjen mallina toimivat jo olemassa olevat sairaanhoitopiirien ja biopankkien tietoallasratkaisut. Alan toimijoilla on siis vuosikausia ollut mahdollisuus varautua näihin ympäristöihin ja kehittää tietoturvan tasoa vaikka sinällään itse tarkennetut Tietolupaviranomaisen asettamat vaatimukset valmistuivat 5.10.2020. Itse tietoturvavaatimukset ovat saman tyyppisiä riskiperusteiseen arvioon perustuvia vaatimuksia kuin esimerkiksi jo arviointilaki asettaa valtion viranomaisille.

Tästä hallituksen esityksessä annetuissa lausunnoissaan kaikki alan keskeiset ministeriöt ja viranomaiset (ohessa muutamia otteita heidän lausunnoistaan), *Kansaneläkelaitosta* lukuun ottamatta, edellyttivät, että sosiaali- ja terveysalan toimijoiden digitaalisten käyttöympäristöjen ja tietojen käsittelyn tietoturvallisuus tulisi varmistaa mahdollisimman pian. Ohessa on seuraavaksi muutamia heidän keskeisiä huomiota.

Muun muassa *Liikenne- ja viestintäministeriön* mukaan esitysluonnoksessa ehdotettua vuoden lisämääräaikaa tietoturvallisen käyttöympäristön soveltamiseksi ei tulisi ainakaan pidentää esitetystä. Liikenne- ja viestintäministeriö katsoi lausunnossaan, että ehdotetun uuden siirtymäajan aikana alan toimijoiden tulee kiinnittää erityistä huomiota toimintansa ja käytössä olevien tietojärjestelmiensä tietoturvallisuuteen toisiolain 18 §:n yleisten tietoturvavaatimusten mukaisesti.

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 erityisesti kriittisillä toimialoilla, kuten sosiaali- ja terveysalalla. Puutteellisesta tietoturvasta johtuvat tietovuodot ja tietojen suojan vaarantuminen voivat aiheuttaa merkittävää vahinkoa ja kustannuksia. *Traficom* korostaa, että ennakolliset panostukset tietoturvaan ja arviointeihin ovat kustannuksiltaan huomattavasti pienempiä kuin kustannukset ja vahingot, joita voi aiheutua tietomurron tai tietojen vuotamisen johdosta. *Traficom* lausunnossaan kannusti 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. Sosiaali- ja terveysministeriö yhtyy TrafiComin näkemykseen.

Myös *apulaistietosuojavaltuutettu* katsoi lausunnossaan, että siirtymäajan jatkamista voidaan pitää perusteltuna ottaen huomioon, että tietoaineistojen käsittely Tietolupaviranomaisen ylläpitämässä tietoturvallisessa käyttöympäristössä ei kaikissa tapauksissa ole mahdollista.

Myös *Valvira* piti lausunnossaan tärkeänä, että sosiaali- ja terveystietojen toissijaista käyttöä tekevillä organisaatioilla on tosiasiallinen mahdollisuus saattaa omat käyttöympäristönsä lain ja sitä tarkentavan määräyksen vaatimusten tasolle.

SOSIAALI- JA TERVEYSMINISTERIÖ

Ministeriö yhtyy Valviran näkemykseen, että käyttöympäristöihin tarvittavat muutokset ovat mittavia ja edellyttävät merkittävästi aikaa, henkilöresursseja ja taloudellisia resursseja. Ministeriön näkemyksen mukaan tämän takia toimenpiteet käyttöympäristöjen auditoinniksi tulisi välittömästi käynnistää. 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 siirtymäajan muutosta perusteltuna.

Myös oikeusministeriö piti lausunnossaan selvänä, että tietojärjestelmät olisi saatettava lain säännösten edellyttämälle tasolle ilman aiheetonta viivytystä.

Siirtymäsäännöksen tarkoituksena on ohjata alan keskeisiä toimijoita toimimaan siten, että käsiteltävien arkaluontoisten henkilötietojen käsittelyssä edellytettävä tietoturvan taso voidaan varmistaa. *Kansaneläkelaitokselta* oli toisiolain valmistelun aikana ja eduskuntakäsittelyn aikana kysytty lukuisia kertoja näkemyksiä toisiolain siirtymäsäännöksistä. Se ei silloin arvioinut, että tietoturvallisia käyttöympäristöjä koskeva voimaantulo olisi liian tiukka. Myös Kansaneläkelaitoksen tulee toimia kyseisen määräajan mukaisesti siltä osin, kun sillä on etuustietoja varten tietoturvallinen käyttöympäristö valmistumassa. Sen sijaan Kanta-tietoja varten on jo olemassa Tietolupaviranomaisen (Findata) ympäristö, koska Tietolupaviranomainen, eikä siis Kansaneläkelaitos, päättää Kanta-tietojen tietoluvista.

Ministeriö yhtyy *Kansaneläkelaitoksen* näkemykseen, että Tietolupaviranomaisen (Findata) ja viranomaisasemassa olevien rekisterinpitäjien eli muiden tietolupaviranomaisten tulee varmistaa tutkimuksen jatkuvuus riittävällä ohjeistuksella tilanteessa, kun tutkimus jatkuu määräaikaisen tietoluvan päättyessä. Ministeriö haluaa korostaa, että tämä vaatimus jatkuvuuden varmistamisesta ei kuitenkaan koske pelkästään tieteellistä tutkimusta vain kaikkia toisiolain mukaisia käyttötarkoituksia, joita tietoluvilla luvitetaan.

Varsinaissuomen sairaanhoitopiiri toteaa lausunnossaan virheellisesti, että käyttöympäristövaatimukset ovat tällaisenaan ristiriidassa EU:n yleisen tietosuoja-asetuksen tavoitteiden kanssa, joka ilmenee esim. suoraan 1 artiklan 3-kohdasta: ”Henkilötietojen vapaata liikkuvuutta unionin sisällä ei saa rajoittaa eikä kieltää syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä.” Näin ollen kyseinen säädös on ristiriidassa EU-lainsäädännön kanssa, eikä tällaiseen ole annettu kansallista liikkumavaraa. Ministeriö toteaa, että *Varsinais-suomen sairaanhoitopiirin* ilmeinen väärinkäsitys on valitettavan yleinen. Toisiolaki on syntynyt perustuslakivaliokunnan myötävaikutuksella ja lain tietosuoja-asetuksen mukaisuus on varmistettu sosiaali- ja terveysvaliokunnassa. Lisäksi toisiolain valmisteluun on osallistunut tietosuojavaltuutetun toimiston edustajia ja tietosuojavaltuutettu, Euroopan tietosuojaneuvosto ja EU:n komissio ovat hyvinkin tietoinen toisiolaista. Euroopan tietosuojaneuvosto on lisäksi tutustunut toisiolakiin maavierailun yhteydessä. Helsingin yliopiston lausunnossakin mainitussa EU-yhteistyössä toisiolaki on toiminut mallina ja sen tietosuoja-asetuksen mukaisuutta on myös siinä yhteydessä arvioitu. Toisiolain säännökset koskevat samalla tavalla kaikkia EU:n toimijoita. Toisiolain alaiset henkilötiedot liikkuvat siis

SOSIAALI- JA TERVEYSMINISTERIÖ

samojen sääntöjen perusteella unionin sisällä ja tietoaineistoja voidaan tietoturvallisella etäyhteydellä käsitellä Suomen rajojen ulkopuolelta. Tietoturvallista käyttöympäristöä koskeva vaatimus perustuu tietosuoja-asetuksen 9 artiklan 4 kohtaan: "Jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön lisäehtoja, mukaan lukien rajoituksia, jotka koskevat geneettisten tietojen, biometristen tietojen tai terveystietojen käsittelyä." Tietosuoja-asetuksen 9 artiklan 4 kohdan perusteella asetetut lisäehdot ovat siis sallittuja ja toisiolailla ei rajoiteta henkilötietojen vapaata liikkumista toisin kuin esimerkiksi tällä hetkellä Tanskassa tai Ranskassa, jotka eivät luovuta henkilötietoja (kuten esimerkiksi terveystietoja) maan rajojen ulkopuolella. Kuten oikeusministeriökin toteaa tästä hallituksen esityksestä antamassaan lausunnossa: "*toisiolaissa säädetyt vaatimukset, jotka liittyvät tietoturvalliseen käyttöympäristöön, ovat oleellisia suojatoimenpiteitä rekisteröidyn oikeuksien turvaamiseksi*."

Viitaten *Varsinaissuomen sairaanhoitopiirin* lausunnossa esitettyyn huomioon, ettei kaikkia lain mukaisia ympäristöjä voisi edes rakentaa, ministeriö toteaa, että lain valmistelun yhteydessä käytettiin nimenomaan mallina olemassa olevia ja tulevia tietoaltaita ja kuultiin alan parhaimpia asiantuntijoita. Tarkoituksena on nimenomaan se, että Suomeen muodostuu tietoturvallisten käyttöympäristöjen verkosto, joissa on kaikissa sama korkea tietoturvan taso, mutta ne kilpailevat välineistöllä. Myös omia välineistöjä voidaan tuoda ympäristöihin edellyttäen, että niiden tietoturvallisuus voidaan varmistaa. On kuitenkin selvää, että myös rekisterinpitäjien ja alan keskeisten toimijoiden tulee aktiivisesti kehittää järjestelmiään ja toimia yhteisin tietorakentein. Kaikki tieto ei ole vielä ole yhtenäistä ja kaikki järjestelmät eivät vielä ole keskenään yhteensopivia, mutta tietoluvilla aineistoja voidaan kuitenkin yhdellä tietoluvalla luvittaa ja kehittää nykyistä federoitua mallia. Tämä edellyttää kaikilta toisiolain alaisilta toimijoilta aktiivisia toimia ja resursseja tähän työhön. Tämä tekeminen osa joka tapauksessa keskeistä tekemistä, jota on pitänyt tehdä ennen toisiolain voimaantuloa, jotta rekisteriaineistot olisi paremmin hyödynnettävissä myös paikallisesti.

Helsingin yliopiston lausuntoon viitaten ministeriö toteaa, että se on alusta alkaen seurannut yleiseurooppalaista toisiokäytön lainsäädännön kehittymistä. Ministeriö on positiivisena huomiona pannut merkille, että Helsingin yliopiston lausunnossa mainituissa Data Governance Act –luonnoksessa, kuten myös European Health Data Space -työssä mallina on käytetty Suomen toisiolakia. Etenkin Data Governance Act -luonnos muistuttaa rakenteeltaan hyvinkin keskitettyjen tietolupaviranomaisten mallia. Suomi on osallistunut aktiivisesti erityisesti European Health Data Space työhön Sitran toimiessa joint actionin vetäjänä sosiaali- ja terveysministeriön lukuun. Myös tässä työssä on kiinnitetty huomiota tietosuoja-asetuksen mukaisten leimojen ja tietoturvaa ja tietosuojaa koskevien käytänteiden tärkeyteen. Toisiolain mukainen auditointihan on ensiaste mainittujen leimojen saamiselle ja suomalainen osaaminen näissä asioissa on kilpailuetu.

Sosiaali- ja terveysministeriössä ollaan perustamassa 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 käyttöym-

SOSIAALI- JA TERVEYSMINISTERIÖ

päristöihin. 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. Suomi seuraa yleiseurooppalaista kehitystä, mutta tämän hallituksen esityksen valmistelun yhteydessä kuultujen keskeisten viranomaisten näkemysten mukaan tietoturvallista käyttöympäristöä koskevaa vaatimusta ei voi siirtää tulevaisuuteen siten kuten Helsingin yliopisto lausunnossaan esittää. Toisin kuin *Helsingin yliopiston* lausunnossaan todetaan, Tietolupaviranomaiset asettamat, osittain Katakriin ja osittain Pitukriin, perustuvat kansalliset tietoturvavaatimukset ovat asiasisällöltään kansainvälisesti yleisesti hyväksyttyjä vaatimuksia, jotka toimivat esiasteena myös ISO 27 001 standardin käyttöönotolle.

Merkittäviä kliinisiä löydöksiä koskeva siirtymäsäännös

Tietolupaviranomainen toteaa lausunnossaan kannattavansa toisiolain 55 § :n siirtymäsäännöksen muutosta, mutta esittää harkittavaksi, voisiko siirtymäaika olla esitettyä lyhyempi. *Tietolupaviranomaisen* mukaan toisiolain 55 §:n mukainen mainittu prosessi on pystytetty ja toimintavalmis lukuun ottamatta 5 momentissa tarkoitettua tiedonhallintapalvelua (Kela), jonka kautta potilas voi toteuttaa oikeuttaan kieltää yhteydenotto.

HUS pitää toisiolain 55 § viivästettyä käyttöönottoa ongelmallisena. Vaikka Kantapalveluissa määriteltyä ennakkokieltoa ei vielä voisikaan toteuttaa, 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. *HUS*:ssa tämä ominaisuus on jo käytössä. Lain henkeä ei siis rikottaisi.

HUS:n lausunnon mukaan Findata on jo tietoluvittanut 55 §:n käyttöä hyväksikäyttävää tutkimusta ainakin HUSissa. Kyseinen tutkimus on läpikäynyt monipolvisen, pian 2 v 10 kk kestäneen arvion, jonka aikana mm. HUSin eettinen toimikunta on valtakunnallista eettistä toimikuntaa TUKIJAa konsultoituaan todennut, että tutkimus on selkeästi eettinen. Se noudattaa myös hallituksen, eduskunnan ja EU:n hyväksymiä linjauksia tekoälytutkimuksille.

HUS:n lausunnossa tiedustellaan myös

a) Mitkä ovat näiden asiantuntijoiden oikeudelliset vastuut?

b) Mikä on asiantuntijoiden ja tutkittavan oikeusturva? Rekisteritutkimuksen tuloksena syntyy tieteellistä tietoa, joka voi paljastaa näitä puutteita ja niiden mahdollista vakavuutta.

c) Pykälä ei myöskään ota kantaa siihen, kauanko kyseinen prosessi saa kestää.

Sosiaali- ja terveysministeriö toteaa vastauksenaan seuraavaa:

SOSIAALI- JA TERVEYSMINISTERIÖ

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 tiedonhallinta-palveluun. Potilas voi tehdä kiellon kirjallisesti missä tahansa julkista terveydenhuoltoa tuottavassa toimintayksikössä taikka sähköisesti asiakastietolain 19 §:ssä tarkoitetun kansalaisen käyttöliittymän välityksellä.

Toisiolain 55 § on eduskunnassa alun perin hyväksytty, sillä edellytyksellä, että potilas (eli tietosuoja-asetuksen mukainen rekisteröity) voisi käyttää asiakastietolain ja toisiolain mukaista kielto-oikeutta ja tietosuoja-asetuksen mukaisia oikeuksia. Nyt tässä hallituksen esityksessä esitetään vain ko. pykälän voimaantulon siirtämistä, ei siis sisällöllistä muutosta, koska eduskunta on hyväksynyt pykälän aikoinaan kokonaisuutena. Mikäli pykälä saatettaisiin voimaan siten, että tuota tiedollista itsemääräämisoikeutta ei voida varmistaa, sääntelyn hyväksyttävyydestä ja erityisesti sen perustuslain 10 §:n ja tietosuoja-asetuksen mukaisuudesta tulisi pyytää vähintään perustuslakivaliokunnan, tietosuojavaltuutetun ja oikeusministeriön lausunto tai jopa täydentävä hallituksen esityksenä. Asia on myös eettisesti hyvin tärkeä ja rekisteröidyn itsemääräämisoikeus pitää pystyä turvaamaan. Saman tyyppistä lainsäädäntöä on suunnitteilla myös biopankkilain uudistamisen yhteydessä.

Kuten apulaistietosuojavaltuutettu on lausunnossaan todennut, tätä siirtymäaikaa ei tulisi jatkaa pidempään kuin on perustellusti tarpeen, *jotta* rekisteröityjen *oikeus saada pääsy itseään koskeviin henkilötietoihin ja mahdollisuus kieltää yhteydenotot voisi toteutua ilman aiheetonta viivytystä myös merkittäviä kliinisiä löydöksiä koskevien tietojen osalta.*

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, määrityksiä ja vaatimuksia ei ole tehty, mutta muutokset olisi toteutettavissa siten, että toisiolain 55 § voisi astua voimaan 1. päivänä tammikuuta 2024.

HUS:n lausunnossa on ilmeinen väärinkäsitys heidän todetessaan, että toisiolain mukainen kielto-oikeus ominaisuus olisi jo käytössä. Teknisiä ja toiminnallisia lainsäädännöstä johtuvia vaatimuksia ei ole edes vielä asetettu toimijoille. Ei ole mitenkään mahdollista, että HUS toimisi lainsäädännön asettamien vaatimusten mukaisesti, koska vaatimuksia ei ole asetettu ja lisäksi kielto-oikeus tulee olla toteutettavissa täysimääräisesti heti alusta alkaen sekä palvelunantajan luona että myös asiakastietolain mukaisen kansalaisen käyttöliittymän (Omakanta) kautta kuten apulasitietosuojavaltuutettukin on lausunnossaan edellyttänyt.

SOSIAALI- JA TERVEYSMINISTERIÖ

Koska toisiolain 55 § on ollut voimassa vasta 1.5.2021 alkaen, niin ei liene mahdollista, mikäli tietolupa on myönnetty ennen ko. ajankohtaa, että tietolupaviranomainen olisi voinut tietoluvittaa 55 §:n perusteella tutkimusta HUSissa. Tietosuojavaltuutetulla on tarvittaessa oikeus kieltää henkilötietojen käsittely, mikäli se tapahtuu toisiolain säännösten kuten esimerkiksi 55 §:n vastaisesti. Tekoälyn käytössä tulee lisäksi ottaa huomioon perustuslakivaliokunnan tekoälyn käyttöä koskevat kannanotot ja tekoälytekniikoihin liittyvät tietoturvariskit.

HUS:n lausunnossa esiin nostetut vastuukysymykset ja kestoa koskevat kysymykset määräytyvät jo voimassa olevan yleis- ja erityislainsäädännön perusteella. Kuten HUS:n lausunnosta on pääteltävissä, kunhan rekisteröidyn oikeudet voidaan toteuttaa 1.1.2024, toisiolain 55 §:n monet erilaiset hyödyt voidaan lunastaa täysimääräisesti.

Muita huomioita

HUS toteaa myös, että Suomessa tehdyt kansalliset erityisratkaisut tietoturvallisista käyttöympäristöistä ja tulkinnat henkilötiedon ja sen anonymisoinnin osalta vaikeuttavat vakavasti kansainvälistä yhteistyötä.

Oulun yliopiston lausunnossa todetaan, toisiolaissa on edelleen valtavia puutteita liittyen tutkimuksen konkreettiseen tekemiseen. Vaikuttaa siltä, että tutkimustyötä tekeviä ei ole riittävästi kuultu lakia valmisteltaessa, eikä vaikutuksia konkreettiseen tutkimustyön tekemiseen ole selvitetty kunnolla. Lakia valmisteltaessa on mitä ilmeisimmin oltu tietämättömiä siitä, miten laajaa ja moninaista tutkimuskenttää laki koskee. Lakiin päätyneet ratkaisut ovat monelta osin erittäin huonoja ja epäselviä. Esimerkiksi luvitukseen, tietoympäristöön, rekisteritietoaineistojen käyttöön/yhdistämiseen muiden tutkimusaineistojen kanssa liittyvät asiat ovat vähintään hankalia, elleivät mahdottomia, ja ovat jo nyt luoneet esteitä tutkimuksen tekemiselle.

Sosiaali- ja terveysministeriö toteaa vastauksenaan seuraavaa:

Kuten edellä on jo todettu, sosiaali- ja terveysministeriössä ollaan perustamassa 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.

Henkilötiedon käsitemäärittely tapahtuu tietosuoja-asetuksen perusteella ja yleiseurooppalaiseen tulkintakäytäntöön perustuen. Toisiolaissa henkilötietoa ei tämän takia erikseen määritellä. Lisäksi pseudonymisointi on määritelty muualla kuin toisiolaissa. Toisiolain 8 §:n 4 momentin mukaisen korkean tason asiantuntijaryhmän pseudonymisointia koskeva tulkintalinjaus koskien henkilötietojen käsittelyä tietoturvallisessa käyttöympäristössä on yleiseurooppalaisesti kovinkin maltillinen ja antaa toisiolain soveltajille enemmän mahdollisuuksia. Ano-

SOSIAALI- JA TERVEYSMINISTERIÖ

nymisointitekniikoihin liittyvät riskit tuotiin monin eri tavoin esille toisiolain eduskuntakäsittelyn yhteydessä. Eduskuntakäsittelyssä tehdyt ratkaisut perustuivat Suomen johtavien anonymisointi- ja tekoälyprofessorien asiantuntijanäkemyksiin.

Oulun yliopiston lausunnossa, kuten myös useammassa muussa lausunnoissa on unohdettu, että tieteellinen tutkimus (ja erityisesti lääketieteellinen tutkimus) on vain yksi toisiolain mahdollistamista monista käyttötarkoituksista, joihin sosiaali- ja terveydenhuollon toiminnassa sekä sosiaali- ja terveysalan ohjaus-, valvonta-, tutkimus- ja tilastotarkoituksessa tallennettuja henkilötietoja voi yhdistää esim. Kansaneläkelaitoksen, Väestörekisterikeskuksen, Tilastokeskuksen ja Eläketurvakeskuksen henkilötietoihin. Monet toisiolain mahdollisuudet vain odottavat tutkijoita ja toisiolain muihin käyttötarkoitukseen tietoaineistoja käsitteleviä. Oulun yliopiston lausunnossa esitetty väite, että tutkijoita ei ole kuultu lainsäädännön valmistelussa ei pidä paikkaansa. Lainvalmistelu oli kaiken kaikkiaan erittäin avointa ja vuorovaikutteista sidosryhmien kanssa ja ehkäpä voisi toimia kaikelle muullekin lainvalmistelulle (ks. liite). Tutkijoita nimenomaan on kuultu valmistelun kaikissa vaiheissa.

Toisiolaki mahdollistaa uudella tavalla rekisteritietojen käytön ja varmistaa tietosuojan. Samalla toimintamallit tietojen luvituksessa ja luovuttamisessa ovat muuttuneet. Uudet toimintamallit on saatava kaikkien tietoon, ja lisäksi niiden kehittämisessä on vielä runsaasti jatkotyötä. Uudet toimintamallit ja esimerkiksi vaatimus tietoturvallisista käyttöympäristöistä voi tehdä tutkijan työstä myös paikoin aikaisempaa erilaisempaa, mutta toisaalta tietoturvalliset käyttöympäristöt tarjoavat tutkijoille paljon uusia mahdollisuuksia tarjoamalla alan parhaimmat välineistöt ja keskitetyt ympäristöt, joissa arkaluonteisten henkilötietojen käsittely voi tapahtua tehokkaasti ja tietoturvallisesti. Toimintamallit on kuitenkin pystyttävä yhdessä tekemään niin sujuviksi kuin tietoturva ja –suoja huomioiden on mahdollista.

On esitetty, että toisiolaki vaikeuttaa erityyppisten tutkimusten, kuten harvinaissairauksien tutkimuksen tekemistä tai terveysteknologian kehittämistä. Toisiolain myötä muuttuneet toimintatavat voivat tehdä tutkimuksesta joissakin tilanteissa osin aikaisempaa erilaisempaa. Tässä asiassa on kuitenkin esiintynyt myös paljon väärinkäsityksiä. Toisiolaki ei esimerkiksi estä harvinaissairauksien tutkimusta. Toisiolaki ei edes säädä näistä tietokannoista. Myös terveysteknologian tutkiminen on mahdollista.

On tärkeää, että toisiolain tuomat mahdollisuudet ja hyödyt otetaan maksimaalisesti käyttöön. Julkisuudessa olleissa vetoomuksissa esiin nostetut huolenaiheet kun eivät pääsääntöisesti ole johtuneet itse toisiolaista vaan esimerkiksi tietosuoja-asetuksesta tai potilaslain uudistamisen tarpeista tai monen lain saman aikaiseen soveltamiseen liittyvistä haasteista. Sosiaali- ja terveysministeriö on käynnistänyt selvityksen toisiolain vaikutuksista, jotta kuitenkin edellä mainitut myös tutkijoiden huolet ja ongelmat tulevat käsitellyiksi. Tavoitteena on tunnistaa lain vaikutukset ja arvioida tarpeita jatkotoimenpiteisiin.

LIITE **Liite toisiolain valmistelusta**