Terveyden ja hyvinvoinnin laitos THL

Lausunto

06.09.2023 THL/3969/4.00.00/2023

Asia: VN/23585/2023

Lausuntopyyntö yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista

Lausunnonantajan lausunto

Mitkä ovat olleet yleisen tietosuoja-asetuksen soveltamiseen liittyvät merkittävimmät hyödyt ja haasteet?

Tietosuoja-asetus on yhtenäistänyt tutkimuskäytäntöjä Suomessa ja jäsenvaltioiden välillä. Yhtenä esimerkkinä henkilötietojen käsittelyperusteena erityisesti yleisen edun mukainen tieteellinen tutkimus on kasvattanut suosiota suostumukset sijasta, mikä on voinut selkeyttää ja helpottaa tutkimuskäytäntöjä. Toisaalta suostumus henkilötietojen käsittelyperusteena sotketaan välillä ns. eettiseen suostumukseen tutkimukseen osallistumiseksi.

Tutkimusaineistojen käsittely-ympäristöjen tietoturva on jossain tapauksissa parantunut ja yhtenäistynyt. Rekisteröityjen oikeudet ovat vahvistuneet. Sanktiot ja julkiset seuraamukset kannustuvat lainmukaiseen toimintaan.

Merkittävä haaste on jäsenmaiden erilaiset tulkinnat tietosuoja-asetuksen määritelmistä ja asetuksen soveltamisesta. Esimerkkinä jossain jäsenmaissa on liberaali aggregoidun tiedon tulkinta. Tutkimusaineiston taulu voi sisältää uniikkeja muuttujayhdistelmiä, mutta jos siinä ei ole suoria tai epäsuoria tunnistetietoja niin tietoja ei silti pidetä henkilötietoina. Suomessa henkilötiedon määritelmää on tulkittu tiukemmin, mikä voi vaikeuttaa tutkimusaineistojen hyödyntämistä ja erityisesti kv-tutkimuksen tekemistä. Lisäksi erilainen henkilötiedon määritelmä on merkittävä ongelma erityisesti tutkimusyhteistyössä Yhdysvaltalaisten organisaatioiden kanssa.

Vaikeat tai tiukat tietosuojasuojalainsäädännön tulkinnat tai hankalat toimintatavat voivat myös haitata viranomaistehtävien ja -vastuiden hoitamista erityisesti terveysturvallisuuden sekä väestötasoisen terveyden ja hyvinvoinnin toimenpiteiden alalla. Pahimmillaan eteen tulevat tilanteet voivat vaarantaa jossain tapauksissa mahdollisuuksia väestön hengen ja terveyden suojeluun.

Tietosuoja-asetus on lisännyt byrokratian määrää ja tarvetta laatia erilaisia tietosuojadokumentteja, mikä aiheuttaa tutkimushallinnolle resurssipaineita ja tutkijoille vaikeuksia soveltaa tietosuoja-asetusta. Tietosuojaviranomaisilta tai EDPB:ltä ei ole saatu riittävästi tukea asetuksen tulkintaan ja tulkintavastuut on jätetty yksittäisille tutkimusorganisaatioille. Edelleen esimerkiksi yhteisrekisterinpitäjillä voi olla poikkeavia tulkintoja tietosuoja-asetuksen peruskäsitteistä, jolloin aikaa hukataan perusmääritelmien käsittelyyn.

Onko tietosuojalaki koettu yleisesti toimivaksi? Minkälaisia haasteita sen soveltamisessa on ilmennyt?

Vanhemmat tutkimusaineistot ja rekisteröidyn oikeudet: Tietosuojalain 31 §:ssä sallitaan tietyin ehdoin poikkeuksia 15, 16, 18 ja 21 artiklan mukaisiin rekisteröidyn oikeuksiin. THL:n tutkimuksissa käsitellään kuitenkin yleensä 9(1) artiklassa tarkoitettuja henkilötietoja (eli mm. terveyttä koskevia tietoja), joten rekisteröidyn oikeuksista poikkeaminen edellyttää lisäksi joko vaikutustenarvioinnin laatimista tai käytännesääntöjen noudattamista. Käytännesääntöjä ei ole ja vanhempiin tutkimusaineistoihin ei ole aina tehty vaikutustenarviointia. Tilanne voi aiheuttaa haasteita, kun vanhoihin tutkimusaineistoihin kohdistuu tarkastuspyyntö. Yleisesti ottaen rekisteröityjen oikeuksien ymmärtäminen ja toteuttaminen poikkeuksineen tieteellisen tutkimuksen kontekstissa on erittäin vaativa kokonaisuus, jonka ymmärtäminen edellyttää tutkimukseen perehtynyttä tietosuojajuristia tai -asiantuntijaa.

Onko yleisen tietosuoja-asetuksen mahdollistamaa sääntelyliikkumavaraa käytetty EU:ssa ja Suomessa tarkoituksenmukaisella tavalla? Jos ei, miten ja minkälaisia tilanteita varten tietosuoja-asetuksen sääntelyliikkumavaraa tulisi käyttää eri tavoin kuin on tehty?

Suomessa tai EU:ssa ei tulisi tehdä liian tiukkoja tulkintoja tietosuojalainsäädännöstä, jos liikkumavaraa on käytettävissä. Esimerkkinä tutkimusaineistojen käsittely selkeytyisi tai mahdollistuisi huomattavasti, jos yksiselitteisesti ohjeistettaisiin tai säädettäisiin, EU-oikeuskäytäntöön (T-557/20, SRB v EDPS ja C-582/14, Breyer) nojautuen, että pseudonymisoitu henkilötieto voi olla ei-henkilötietoa toiselle osapuolelle, jos henkilön tunnistaminen ei olisi käytännössä mahdollista.

Vaihtoehtoisesti tietosuoja-asetuksen mukainen tutkimusaineistojen henkilötiedon käsite tulisi olisi yhtenäinen Yhdysvaltojen HIPAA:n ”protected health information” tai Common Rulen ”identifiable private information” kanssa. Nykytulkinnat johtavat tietyissä tapauksissa mahdottomiin tilanteisiin. Esimerkkinä USA:n NIH on merkittävä tutkimusrahoituksen myöntäjä, mutta tutkimusaineistojen jakaminen NIH:lle voi olla jossain tilanteissa käytännössä mahdotonta, koska mahdollisia siirtomekanismeja ei ole. Sama tilanne voi koskea myös kansainvälisiä järjestöjä, kuten WHO:ta.

Lainsäädännössä tulisi mahdollistaa mekanismi, jolla toisessa jäsenmaassa hyväksytään toisessa maassa jo hyväksytty käsittely-ympäristö liittyen terveystietojen toisiokäyttöön. Lisäksi tarvittaisiin mekanismi, jolla nämä aineistot voidaan yhdistää yhdessä maassa. Tulisi välttää tilannetta, jossa eri valtioista toisiokäyttöön luvitettuja tietoja pitäisi käsitellä jokaista erillisissä käsittely-ympäristöissä.

Millä toimialoilla yleistä tietosuoja-asetusta on pantu täytäntöön tehokkaasti ja onnistuneesti huomioiden asetukselle asetetut tavoitteet edistää rekisteröityjen oikeuksien ja vapauksien toteutumista sekä edistää tiedon vapaata liikkuvuutta EU-alueella?

Toimeenpano on ehkä ollut tehokkainta aloilla, joissa tietosuojaan liittyvät kysymykset ovat yksinkertaisia tai tilanteet joihin tietosuojaviranomaisten on helppo puuttua. Viranomaisten tulisi kohdistaa resurssit suurimpia riskejä sisältäviin tapauksiin.

Minkälaisia haasteita on ilmennyt yleisen tietosuoja-asetuksen ja kansallisen lainsäädännön tai muun EU-lainsäädännön yhteensovittamisessa eri soveltamistilanteissa?

Terveysrekistereitä ja terveystietoja koskeva tutkimus toimi tehokkaammin ennen tietosuoja-asetusta. Nyt tietojen siirtämisessä ollaan lähinnä pattitilanteessa, jossa tietoja ei voida yhdistää kohtuullisella vaivalla ja kohtuullisilla kuluilla tai ollenkaan. Tämä johtaa siihen, että kukin maa/alue analysoi oman datansa ja tiedot yhdistetään meta-analyysin avulla. Meta-analyysi toimii, jos on riittävään yleinen ilmiö. Sen sijaan harvinaisissa altistumisissa ja päätetapahtumissa voi olla tilanne, että on maita/alueita joissa on nolla tapausta, jolloin riskiestimaatteja ei voida laskea. Esimerkiksi lääketurvallisuustutkimuksessa tämä johtaa siihen, että yhdessä maassa/alueella voi olla vaikka kuinka paljon lääkitysturvallisuutta tukevaa dataa (lääkkeen käyttäjiä, mutta ei yhtään haitallista tapahtumaa) ja se tieto jää huomiotta, koska nollalla tapauksella ei voi laskea riskiestimaattia. Eli lääkitysturvallisuutta koskevat signaalit vääristyvät haittojen suuntaan. Kun kyseessä on harvinainen altiste ja päätetapahtuma on ensisijaisen tärkeää, että aineistot voidaan yhdistää jolloin kaikki henkilöt tuottavat seuranta-aikaa, vaikka ei olisikaan yhtään haittatapahtumaa.

Lisäksi toisiolain on koettu estävän tutkimusta jossain tapauksissa. Haasteita on havaittu usealla tasolla. Findatan käsittelyajat ovat pitkät ja aineistojen hyödyllisyys ja käytettävyys ovat heikentyneet. Aiemmin rekisterivastaavat arvioivat tutkimussuunnitelmat etukäteen, nyt tämä vaihe puuttuu ja mitä tahansa voi tulla toteutukseen. Aineistojen hinnat ovat nousseet liian korkeiksi ja rekisteritutkimukseen ei ole aina varaa. Findatan sääntö, että alle 5 havaintojen tuloksia ei voida esittää tekee harvinaisten altisteiden ja päätetapahtumien tutkimisesta vaikeaa, ellei mahdotonta. Samoin Findatan tulkinta aggregoidusta datasta (vain taulukkomuotoista yli 5 havaintoa per solu) tekee synteettisten datan hyödyntämisen tutkimuskäytössä mahdottomaksi. Se, että Suomessa hyväksytään vain suomalaisten viranomaisten auditoima käsittely-ympäristö tekee kv-tutkimuksen mahdottomaksi. Suomi on pieni väestö ja markkina maailman laidalla, meidän vahvuus on nimenomaan siinä, että tietoja voitaisiin yhdistää vähintään Pohjoismaiden tasolla. Kv-toimijat eivät ole kiinnostuneita hankkimaan Suomesta hyväksyntää käsittely-ympäristölleen, jos jossakin toisessa Euroopan maassa pelkästään yhden sairaalan catchment area on 20 miljoonaa henkilöä. On myös kestämätöntä, ettei esim. toisen tilastoviranomaisen (kuten Statistics Denmark) käsittely-ympäristö kelpaa Suomessa.

Haasteelliseksi on myös koettu kansallisen biopankkilain ja toisiolain erilaiset tulkinnat terveystiedon määritelmän osalta suhteessa muihin jäsenvaltioihin. Joissakin jäsenvaltioissa määritelmä käsittää myös biopankkidatan ja genomidatan ja meillä on em. koskien erillislainsäädäntö ja nämä eivät ole sisällöiltään kaikilta osin yhteneväisiä.

Onko eri jäsenvaltioiden tietosuojalainsäädäntöjen eroavaisuuksiin ja täytäntöönpanoon liittyen tunnistettu haasteita? Jos on, minkälaisia haasteita?

Jossain jäsenvaltioissa on säädetty tai ohjeistettu, ettei esimerkiksi henkilötietojen käsittelyperuste voi olla mikään muu kuin suostumus, mikä aiheuttaa ongelmia tai suorastaan esteitä, kun tehdään kv-tutkimusta ja toisessa jäsenvaltiossa käsittelyperusteeksi onkin valittu joku muu vaihtoehto.

Myös eri osapuolten rooleista joudutaan käymään välillä pitkiäkin neuvotteluita, koska osapuolille ei ole selvää käsitteet henkilötietojen käsittelijä, rekisterinpitäjä tai yhteisrekisterinpitäjä. Välillä on myös poikkeavia näkemyksiä eri osapuolten välillä siitä, onko pseudonymisoitu henkilötieto tai kahteen kertaan pseudonymisoitu henkilötieto henkilötietoa vai ei.

Ovatko Euroopan tietosuojaneuvoston antamat ohjeet auttaneet käytännön soveltamistilanteisiin liittyvien ratkaisujen tekemisessä? Mitä yleisen tietosuoja-asetuksen tulkintaa koskevia ohjeita vielä tarvittaisiin?

Kullekin maalle on muodostunut omat käytäntönsä tulkinnoista, vaikka ohjeet ovat olleet kaikille samat, joten kuinka lisäohjeilla käytäntöjä saataisiin yhtenäistettyä? Eli soveltamisohjeiden sijaan käsitteiden tulisi olla yhteneväisiä ja regulaation tulisi olla niin selvä, ettei se jätä tulkinnanvaraa.

EDPB:n artiklaa 15 koskeva ohje (Guidelines 01/2022 on data subjects rights – Right of access) on tietosuoja-asetuksen tulkinnassa tiukka ja käytännön soveltamistilanteissa haastava, kun otetaan huomioon THL:n käsittelemien henkilötietojen suuri määrä sekä ohjeen linjaukset suhteessa mm. tietopyyntöjen rajaamiseen, pseudonymisoituihin aineistoihin sekä artiklan 12 tulkintaan.

EDPB:n ohjetta liittyen tieteelliseen tutkimukseen on odotettu jo useampi vuosi.

Onko edustamanne organisaatio ollut mukana laatimassa yleisen tietosuoja-asetuksen 40 artiklan mukaisia käytännesääntöjä tai harkinnut niiden laatimista? Mitkä ovat käytännesääntöjen laatimiseen liittyviä merkittävimpiä hyötyjä ja haasteita?

Suomalaiset yliopistot, korkeakoulut, tutkimuslaitokset ja yliopistosairaalat alkoivat laatimaan yhteistyössä tieteellistä tutkimusta koskevia käytännesääntöjä vuonna 2017 laajennetussa TUTTI-ryhmässä. THL:n tietosuojavastaava on aktiivisesti mukana kesken olevassa laatimistyössä.

Tieteellistä tutkimusta koskeva käytännesääntötyö on toistaiseksi keskeytetty, kunnes EDPB:n tieteellistä tutkimusta koskevaa ohjeistus valmistuu. Lisäksi käytännesääntötyön haasteina on koettu epäselvä ohjeistus käytännesääntöjen laatimisesta, tarkoituksesta ja muodosta. Käytännesääntötyön oheistuotteena hyödyllistä on ollut tiedon jakaminen tietosuojalainsäädännön soveltamisesta ja oikeustapauksista, luotu yhtenäisiä tulkinta- ja toimintakäytäntöjä sekä luotu verkostoja tutkimuksen juristien ja tietosuojavastaavien välillä.

Onko yleisen tietosuoja-asetuksen täytäntöönpanoon liittyvä seuraamusjärjestelmä Suomessa tehokas ja tarkoituksenmukainen? Mitä merkittävimpiä hyötyjä ja haasteita seuraamusjärjestelmään liittyy?

Voidaan myös pitää haasteena ja epäkohtana, ettei seuraamusmaksua ei voida määrätä valtion viranomaisille, liikelaitoksille ym. eli käytännössä ei kenellekään niille tahoille, jotka kaikkein eniten ovat tekemisissä arkaluonteisen henkilötiedon kanssa. Eli jos jotakin virheitä em. toimesta tapahtuu, niin toiminta saattaa jatkua ilman merkittäviä muutoksia käytännön toimintatavoissa. Kansalaiset voivat kokea tilanteen epäoikeudenmukaiseksi eikä osoita, että seuraamusmaksujen määrääminen olisi oikeasuhtaista ja varottavaa. Seuraamusmaksut ovat olleet Suomessa aika pieniä verrattuna muihin jäsenvaltioihin.

Toistaiseksi sanktiot eivät ole Suomessa koskeneet julkista puolta, mutta hallitusohjelman mukaisesti tilanne tullee muuttumaan. Olisi hyödyllistä selvittää, minkälaisia kokemuksia julkisen puolen sanktioista on ollut muissa jäsenmaissa? Ja millä tavalla em. asiantilan muuttaminen vaikuttaisi esim. ylemmän johdon virkavastuisiin? Käytännön toteuttaminen hallinnossa ei varmastikaan tulisi olemaan "läpihuutojuttu". Olisiko tässä sanktioasiassa kuitenkin EU-tason yhtenäisyys ja yhteiset käytänteet parempi kuin jokaisen jäsenvaltion n kpl variaatioita sanktioiden soveltamisessa julkiseen hallintoon?

Ovatko yleisen tietosuoja-asetuksen kansainväliset tiedonsiirtomekanismit toimivia vai tulisiko niitä kehittää edelleen ja miten niitä tulisi kehittää edelleen? Mitkä ovat olleet kansainvälisiin tiedonsiirtoihin liittyvät merkittävimmät hyödyt ja haasteet?

Schrems-tuomioiden jatkumo ja EU-US-siirtomekanismien kaatuminen aina vuorollaan on aiheuttanut epäselvyyttä ja oikeusvarmuuden puutetta yhdysvaltalaisten palveluntarjoajien kohdalla. Tilannetta ei ole helpottanut se, ettei todellisia vaihtoehtoja US-palveluntarjoajalle ole aina edes tarjolla. Uusi tiedonsiirtokehys ei ole myöskään pysyvä ratkaisu, sillä järjestelyn odotetaan kaatuvan taas EU-tuomioistuimissa. Lisäksi tietosuojaviranomaiset puuttuvat kv-tiedonsiirtoihin hyvin satunnaisesti, mitä ei voida pitää toivottavana tilanteena, varsinkaan jos käsillä olleesta ”pakkotilanteeseen” liitetään vielä virkavastuuasiat. EU:n ja USA:n tulisi luoda aidosti toimiva mekanismi EU-US -tiedonsiirtoihin liittyen.

Onko yleisen tietosuoja-asetuksen ns. laajennettu alueellinen soveltamisala, joka kattaa myös EU:n markkinoilla toimivien kolmansien maiden toimijoiden suorittaman henkilötietojen käsittelyn, toiminut tarkoituksenmukaisella tavalla? Olisiko yleisen tietosuoja-asetuksen täytäntöönpanoon liittyvää yhteistyötä kolmansien maiden kanssa tarpeen kehittää ja miten?

Tieteellisen tutkimuksen kontekstissa kolmansien maiden tai kv-organisaatioiden voi olla vaikeaa ymmärtää GDPR:n laajennettua soveltamisalaa, eikä asiaa aina haluta hyväksyä tai ymmärtää, varsinkaan kun esim. henkilötiedon määritelmät voivat erota merkittävällä tavalla EU:n ja kolmannen maan välillä. Tilanteeseen liittyy myös tulkintaepäselvyyksiä, kuten kuinka tietojen pysyvät luovutukset kolmanteen maahan kv-organisaatiolle tulisi käsittää? Tai kuinka hallitaan tietojen luovutukset kolmannesta maasta eteenpäin?

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

-

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

-

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

-

Kommentit yleisen tietosuoja-asetuksen IV lukuun – Rekisterinpitäjä ja henkilötietojen käsittelijä

-

Kommentit yleisen tietosuoja-asetuksen V lukuun – Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille

-

Kommentit yleisen tietosuoja-asetuksen IV lukuun – Riippumattomat valvontaviranomaiset

-

Kommentit yleisen tietosuoja-asetuksen VII lukuun – Yhteistyö ja yhdenmukaisuus

-

Kommentit yleisen tietosuoja-asetuksen VIII lukuun – Oikeussuojakeinot, vastuu ja seuraamukset

-

Kommentit yleisen tietosuoja-asetuksen IX lukuun – Tietojenkäsittelyyn liittyviä erityistilanteita koskevat säännökset

-

Reittu Jarkko
Terveyden ja hyvinvoinnin laitos THL