HUS-Yhtymä

Lausunto

06.09.2023 VN/23585/2023, HUS/5668/2023

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?

Hyötyinä mainitsemme seuraavat seikat:

Tietosuoja-asetus on luonut yhteisiä pelisääntöjä EU:n sisällä lääketieteelliseen tutkimukseen.

Tietosuoja-asetuksen myötä erilaiset toimijat ovat kiinnittäneet rekisteröityjen informointiin paremmin huomiota. Tietosuojaselosteet ovat kattavampia ja laadukkaampia verrattuna aikaan ennen tietosuoja-asetuksen soveltamisen alkamista. Vastaavasti henkilötietojen käsittelyä koskevien sopimusten laatu on parantunut tietosuoja-asetuksen myötä.

Yleisesti tietosuoja-asetus on parantanut yksityishenkilöiden yksityisyyden suojaa.

Haasteina tuomme esiin seuraavat asiat:

Tietosuoja-asetusta kuvastaa se, että suomenkielisessä asetuksessa käsite asianmukainen esiintyy eri sijamuodoissaan 136 kertaa. Tämä ilmentää sitä, että asetuksen teksti on osin vaikealukuista ja tulkinnan varaista. Esim. mitä ovat asianmukaiset suojatoimenpiteet? Tähän voidaan esittää monenlaisia käsityksiä. Tulkinnat samasta asiasta voivat myös vaihdella eri EU-jäsenmaittain.

Tietosuoja-asetuksen 4 artiklan henkilötiedon määritelmä on aiheuttanut sen, että anonymisoidun tiedon tuottaminen on mahdotonta esim. lääketieteellisessä tutkimuksessa. Jos tutkimusaineistosta on poistettu henkilöiden tunnisteet sekä muut tunnistamisen mahdollistavat elementit, mutta niiden

palauttamiseen liittyvä avainkoodi on aineiston luovuttajan hallussa, katsotaan aineisto aina pseydonymisoiduksi henkilötiedoksi, jota koskee kaikki tietosuoja-asetuksen vaatimukset, vaikka luovutuksen vastaanottajalla ei olisi realistisia mahdollisuuksia tunnistaa henkilöitä kohtuullisilla keinoilla. Henkilötietojen luovuttaja taas ei voi tuhota avainkoodeja tutkimuksen ollessa kesken. Tutkimustoimintaa vaikeuttaa edelleen kansallinen toisiolaki, jonka mukaisesti anonymisoitua tietoa voi tuottaa vain kansallinen tietolupaviranomainen Findata. STM on linjannut anonymisoidun potilastiedon eri tavalla kuin EU-tuomioistuinten päätöksissä on linjattu. Anonymisoituna tietona tulisi pitää sellaista tietoa, josta henkilöiden tunnistaminen ei ole mahdollista ilman lainvastaisia keinoja. Liian tiukalle viety tulkinta hankaloittaa tutkimusta. Tämän osalta viittaamme alla olevaan päätökseen:

“If the data recipient does not have any additional information enabling it to re-identify the data subjects and has no legal means available to access such information, the transmitted data can be considered anonymized and therefore not personal data. The fact that the data transmitter has the means to re-identify data subjects is irrelevant and does not mean that the transmitted data is automatically also personal data for the recipient.”

EUR-Lex - 62020TJ0557 - EN - EUR-Lex (europa.eu)

EU General Court Clarifies When Pseudonymized Data is Considered Personal Data | Inside Privacy

Käytännössä edellä mainitut seikat estävät tutkimusaineistojen vertailun kansainvälisesti.

Yleisenä haasteena on se, että tietosuoja-asetusta sovelletaan kaikkeen henkilötietojen käsittelyyn, oli sitten kyseessä esim. verkkokaupan asiakasrekisteri, kunnan kotiseutuyhdistyksen jäsenrekisteri, harrastelijateatterin jäsenluettelo tai erityiset henkilötietoryhmät kuten salassa pidettävät sairaalan potilasasiakirjat. Tietosuoja-asetus on ikään kuin ”one size fits for all”. Kokemuksemme perusteella erityisiä henkilötietoryhmiä koskevia artikloita tulisi täsmentää erityisesti henkilötietojen luovutuksen osalta. On ristiriitaista, että johdanto-osassa (43) todetaan, että suostumusta ei tulisi käyttää tilanteessa, jossa rekisterinpitäjä on viranomainen. Toisaalta kuitenkin 6 ja 9 artiklassa suostumus on käsittelyperusteena.

Erityisesti harvinaissairauksien tutkimuksessa suostumus on usein käytännössä ainoa käytettävissä oleva käsittelyperuste, mutta tietosuoja-asetuksen vaatimusten mukaisen suostumuksen laatiminen on vaikeata, koska suostumuksessa pitäisi pystyä kertomaan kaikki mahdolliset henkilötietojen tulevaisuuden käyttötarkoitukset kuten tietojen luovutus tutkimuskäyttöön. Usein kansainvälisessä tutkimuksessa oikeus saada tutkimusyhteisön tutkimustuloksia on sidottu vastavuoroisuusperiaatteeseen eli tällöin tiedon saajan tulisi myös luovuttaa tutkimusta hyödyntävää aineistoa tiedeyhteisön käyttöön. Tällöin on mahdotonta etukäteen arvioida, mitä mahdollisia tieteellisiä tutkimuksia tulevaisuudessa käynnistyy ja mihin yksittäisiin tutkimustarkoituksiin luovutettavia tietoja käytettäisiin.

Ristiriitaa ilmentää tietosuoja-asetuksen 5 artiklan 1 b) kohta: ”ne on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten

kanssa yhteensopimattomalla tavalla; myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota 89 artiklan 1 kohdan mukaisesti yhteensopimattomaksi alkuperäisten tarkoitusten kanssa (”käyttötarkoitussidonnaisuus”);”

Edellä mainittu 5 artiklan 1 b) kohta mahdollistaa henkilötietojen käsittelyn ”myöhempää yleisen edun mukaista tieteellistä tutkimusta varten”, mutta tietoisen suostumuksen vaatimuksena taas on, että rekisteröidylle tulisi pystyä kertomaan kaikki tulevat käyttötarkoitukset. Tulevaisuuden tieteellisen tutkimuksen käyttötarkoituksia on mahdotonta yksilöidä etukäteen.

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

Yhtenä yksittäisenä haasteena voidaan mainita vakuutusyhtiön oikeus saada kuolleen henkilön potilasasiakirjoja vapaaehtoisissa vakuutuksissa. Olemme tulkinneet lakia potilaan asemasta ja oikeuksista 785/1992 ja sen 13 § 5) kohtaa siten, että vakuutusyhtiöllä ei olisi tähän säädökseen vedoten oikeutta saada yllä kuvatussa tilanteessa elinaikaa koskevia potilaskertomustietoja. Tiedossamme ei ole muuta tähän nimenomaiseen asiaan liittyvää erityislainsäädäntöä.

Vakuutusyhtiöt vetoavat tietosuojalain 6 §:n 1 mom. 1) kohtaan, mutta tämä ei voi olla luovutuksen peruste, koska tietosuojalaki täydentää tietosuoja-asetusta, jota taas ei sovelleta kuolleiden henkilöiden henkilötietoihin.

Kuolleen henkilön potilastietojen luovutusta säätelee näin ollen vain em. potilaslaki (785/1992) ja sen 13 § 5) kohta, jossa ei ole mainintaa vakuutusyhtiön oikeudesta saada kuolleen henkilön potilasasiakirjoja.

Tietosuoja-asetus ja tietosuojalaki ovat aiheuttaneet entistä enemmän byrokratiaa ja niiden tulkinta vaatii yhä enemmän erityisasiantuntemusta, jonka vuoksi terveydenhuollon ammattihenkilöiden on vaikea ymmärtää vaatimuksia ja miten ne tulisi toteuttaa. Lainsäädäntö on osittain yhtenäistänyt tulkintoja, mutta erityisesti kansainvälisissä yhteyksissä esiintyy hyvinkin erilaisia tulkintoja.

Tietojen kerääminen rekisteriin tiettyä sairautta koskien ja tutkimusta varten on tulkittu eri maissa eri tavoin. Suomessa datan käyttö on mahdollista vain edellyttäen, että kaikki käyttötarkoitukset ovat tiedossa ja käyttö on ajallisesti rajattu. Joissain Euroopan maissa suostumusta ei ole tulkittu näin vaan on voitu toimittaa dataa ilman sanottuja edellytyksiä useita tulevia tutkimuksia varten. Euroopan tasoisesta rekisteristä, jossa tietoja voidaan käyttää myös tutkimukseen, on saatu laajoja epidemiologisia selvityksiä ja etenkin harvinaisten sairauksien kohdalla vain näin saadaan riittäviä aineistokokoja.

Siten henkilön omalla suostumuksella – laajallakin ja tulevaisuuteen kohdistuvalla – tulisi olla suurempi painoarvo. Se, mitä GDPR tarkoittaa nimenomaisella suostumuksella yhtä tai useampaa käyttötarkoitusta varten on tulkinnanvarainen kysymys. Voitaisiin ajatella, että nimenomainen suostumus on kyseessä silloinkin, kun se annetaan tiettyä tautia koskeviin tutkimuksiin EU:n alueella, edellyttäen tietenkin, että henkilö on kykenevä ymmärtämään suostumuksen merkityksen ja häntä on informoitu mahdollisista riskeistä.

Tässä esteenä on myös toisiolain vaatimus kansallisen auditointilaitoksen hyväksymästä tietoturvallisesta käyttöympäristöstä, joka koskee pseydonymisoitua tietoa. Anonymisoitu tieto taas on niin ylätason tietoa (usein luonteeltaan tilastollista), että sillä ei ole tieteellistä arvoa esim. tietyn sairauden tutkimuksessa. Lisäksi anonymisoitua potilastietoa ei voi tuottaa kuin Findata, jolla ei ole teknistä kyvykkyyttä tuottaa anonymisoitua potilastietoa ja myös STM:n linjaukset ovat tehneet sen mahdottomaksi, koska linjauksissa mitään jäännösriskiä ei ole hyväksytty.

Nostamme esiin tietosuojalain 31 §:n kolmannen kohdan: Käsiteltäessä henkilötietoja tieteellistä tai historiallista tutkimustarkoitusta varten voidaan tietosuoja-asetuksen 15, 16, 18 ja 21 artiklassa säädetyistä rekisteröidyn oikeuksista tarvittaessa poiketa edellyttäen, että:

3) henkilötietoja käytetään ja luovutetaan vain historiallista tai tieteellistä tutkimusta taikka muuta yhteensopivaa tarkoitusta varten sekä muutoinkin toimitaan niin, että tiettyä henkilöä koskevat tiedot eivät paljastu ulkopuolisille.

Tähän liittyy myös tietosuojalain 32 §: Yleisen edun mukaisia arkistointitarkoituksia varten tapahtuvaa henkilötietojen käsittelyä koskevat poikkeukset ja suojatoimet

Käsiteltäessä henkilötietoja yleisen edun mukaisia arkistointitarkoituksia varten 4 §:n 4 kohdan tai tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohdan nojalla voidaan tietosuoja-asetuksen 15, 16 ja 18–21 artiklassa tarkoitetuista rekisteröidyn oikeuksista poiketa tietosuoja-asetuksen 89 artiklan 3 kohdassa säädetyin edellytyksin.

Jos tutkimusaineisto on säilytettävä määräajan verifiointia varten, onko kyse 32 § mukaisesta yleisen edun mukaisesta arkistointitarkoituksesta?

Kiinnitämme huomiota tietosuojalain 6 §:n 1 mom. 8 kohtaan:

”Erityisiä henkilötietoryhmiä koskeva käsittely

Tietosuoja-asetuksen 9 artiklan 1 kohtaa ei sovelleta:

8) tutkimus- ja kulttuuriperintöaineistojen käsittelyyn yleishyödyllisessä arkistointitarkoituksessa geneettisiä tietoja lukuun ottamatta.”

Tästä nousee kysymys, mikä on käsittely- ja säilytysperuste geneettisille tiedoille, kun em. säädös sulkee geneettiset tiedot pois? Tutkimuksen verifiointi edellyttää, että myös geneettisiä tietoja on säilytettävä tutkimuslainsäädännön ja hyvien kansainvälisten tutkimuskäytäntöjen edellyttämä aika.

27 § 1 mom.: akateemisen ilmaisun tarkoituksia varten? Tätä ei ole määritelty. Mihin säädöstä voidaan soveltaa henkilötietojen käsittelyssä esim. lääketieteellisessä tutkimuksessa?

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?

STM:n yksilökohtaisten tietojen anonymisointiin liittyvät linjaukset tulisi muuttaa yleiseurooppalaisen tulkinnan ja EU-tuomioistuinten päätösten mukaisiksi.

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?

Katsomme, että terveydenhuollossa rekisteröityjen oikeudet ja suojaaminen ovat korostuneet mutta tiedon vapaa liikkuvuus EU-alueella on vaikeutunut osin johtuen GDPR:n tulkinnoista ja osin toisiolaista, joka lisää edellytyksiä tiedon käsittelylle ja niille ympäristöille missä tietoa voi käsitellä. Erityisesti toisiolain vaatimus tietoturvallisesta käyttöympäristöstä ei edistä tiedon liikkuvuutta vaan estää sen. Toisiolakiin tulee tehdä muutoksia, jotta se edistäisi kansainvälistä tutkimusta.

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

Suomen toisiolaki aiheuttaa hankaluuksia, koska potilaan (rekisteri)tietoa (esim. alun perin terveydenhuoltoa varten kerätyt potilastiedot) ei suoranaisesti saa sen puitteissa käyttää tieteelliseen tutkimukseen tai luovuttaa “tavallisen tutkimusdatan” tapaan muulle toimijalle, edes potilaan suostumuksella. Toisiolaki vaatii, että terveysdata siirretään hyväksyttyyn tietoturvalliseen käyttöympäristöön tutkimusta varten, mikä on huomattavasti hankalampaa. Toisaalta voidaan tulkita GDPR:n mahdollistavan, että potilas antaa suostumuksensa terveydenhuollon yhteydessä kerätyn datan käyttöön, mikä ohittaa toisiolain (EU-oikeuden ensisijaisuus). Jos taas potilaalta ei voida pyytää suostumusta, joudutaan asia toteuttamaan toisiolain kautta ja ulkomaiset yhteistyökumppanit eivät aina halua käsitellä dataa toisiolain mukaisessa kansallisen arviointilaitoksen hyväksymässä tietoturvallisessa käyttöympäristössä.

Esimerkkinä voidaan mainita eurooppalainen yliopistosairaala tai tutkimuslaitos, jolla on tietoturvallisuuden ISO 27001 sertifikaatti. Tietoja ei voida kuitenkaan voida siirtää tutkimuskumppanin tekniseen ympäristöön, koska sitä ei ole auditoinut toisiolain mukainen kansallinen arviointilaitos, vaikka tutkimuskumppanilla on vahva näyttö siitä, että sen tietojenkäsittely-ympäristö on tietoturvallisuuden hallintamenettelyiden osalta sertifioitu. Tutkimuskumppani on syystä haluton tilaamaan kustannuksia aiheuttavan suomalaisen arviointilaitoksen sertifioinnin.

Yhtenä erityiskysymyksenä nostamme esiin asiakastietolain (784/2021) ja sote voimaanpanolain (616/2021) säädökset koskien potilaskertomustietojen luovutusta. Tietosuoja-asetuksen 1 artiklassa on kerrottu asetuksen tavoitteet. Lienee sanomatta selvää, että tietosuoja-asetuksen tavoitteet huomioiden myös Suomen kansallisessa lainsäädännössä potilastietojen luovuttaminen terveydenhuollon toimintayksilöltä toiselle tulisi tapahtua yhdenmukaisilla periaatteilla.

Asiakastietolaki ja sote-voimaanpanolain 64 a §:n väliaikainen tiedonsaantioikeus (voimassa 31.12.2024) asettaa kuitenkin kansalaiset ja hyvinvointialueiden ammattihenkilöt eriarvoiseen asemaan riippuen siitä, asuvatko henkilöt Uudellamaalla vai muualla Suomessa. Tätä voidaan valaista kahdella käytännön esimerkillä:

Vantaalainen henkilö hakeutuu kotoaan kilometrin päähän oman hyvinvointialueen (Vantaa-Keravan hyvinvointialue) terveysasemalle, jossa hänelle tehdään lähete HUS-yhtymään (oma erillinen erikoissairaanhoidon hyvinvointialue ja oma rekisterinpitäjä). Henkilö menee kotoaan 1,5 kilometrin päähän HUS-yhtymän Peijaksen sairaalaan ensimmäiselle vastaanotolle. Tässä tilanteessa hän siirtynyt hyvinvointialueelta toiselle (eri rekisterinpitäjät) ja hänellä on oikeus tehdä asiakastietolain 18 §:n luovutuskielto Vantaa-Keravan tietoihin sekä myös HUS-yhtymän erikoissairaanhoidon tietoihin.

Verrataan tilannetta Nokian kunnassa asuvaan henkilöön, joka menee terveysongelman vuoksi ensin Pirkankaan hyvinvointialueen Nokian terveysasemalle, jossa hänestä tehdään lähete Tampereen yliopistolliseen sairaalaan (edelleen Pirkanmaan hyvinvointialue). Kansalainen ei voi tehdä luovutuskieltoja perusterveydenhuollon tietoihin tai erikoissairaanhoidon tietoihin, koska sekä perusterveydenhuolto että erikoissairaanhoito ovat samaa hyvinvointialuetta ja kyse on yhdestä rekisterinpitäjästä. Mikäli yliopistosairaala tai terveyskeskus käsittelevät tavalla tai toisella toisen osapuolen laatimia hoidon kannalta tarpeellisia tietoja, on kyse rekisterinpitäjän sisäisestä tietojen käsittelystä, ei luovutuksesta. Uudellamaalla taas tietojen siirtäminen HUS-yhtymän ja perusterveydenhuollon välillä on nimenomaan luovutusta, jonka edellytykset ovat

1. Kanta-palveluihin tallennettu asiakastietolain mukainen luovutuslupa tai

2. Sote-voimaanpanolain 64 a §:n mukainen väliaikainen tiedonsaantioikeus (Kanta-informointi ver. 1.1 tallennettu tahdonilmaisupalveluun eikä potilas ole tehnyt luovutuskieltoa)

3. nimenomainen suostumus (koskee tietoja, jotka eivät esim. ole saatavilla Kannasta tai muutoin sähköisessä muodossa, esim. lasten kasvukäyrät, kuulokäyrät)

Huomionarvoista on, että esimerkkinä käytetyllä Pirkanmaan hyvinvointialueella tietoja voidaan siirtää ja käsitellä perusterveydenhuollon ja erikoissairaanhoidon välillä ilman asiakastietolain mukaista luovutuslupaa tai potilaslain mukaista suostumusta. Edelleen nostamme esiin, että rekisteröity ei voi asettaa Pirkanmaan hyvinvointialueen sisällä luovutuskieltoja, kun taas Uudellamaalla rekisteröity voi asettaa luovutuskiellot eri hyvinvointialueiden tietoihin kuten erikoissairaanhoidon (HUS-yhtymä) ja perusterveydenhuollon (esim. Vantaa-Keravan hyvinvointialue) välille.

Sosiaali- ja terveysvaliokunta on kiinnittänyt asiaan huomiota:

Sosiaali- ja terveysvaliokunta toisti asiakastietolaista antamassaan lausunnossa (STVM 48/2022) aiemman kantansa (StVM 9/2022 vp , s. 5—6) ja kiinnittää vakavaa huomiota siihen, että Uudenmaan aluetta koskeva potilastietojen käsittely on väliaikaisen sääntelyn voimassaoloaikana ratkaistava kestävällä tavalla toistaiseksi voimassa olevalla sääntelyllä siten, että terveydenhuollon ammattihenkilöillä on sujuva pääsy potilasturvallisuuden kannalta olennaisiin tietoihin potilaan tietosuojaa kunnioittaen. Valiokunta ehdotti asiassa lausumaa, jonka eduskunta hyväksyi (EV 300/2022 vp HE 246/2022 vp).

Väliaikaisen tiedonsaantioikeuden määräaikaisuus aiheuttaa osaltaan epävarmuutta Uudenmaan hyvinvointialueilla.

Edellä olevan perusteella ja asiakkaiden ja potilaiden yhdenvertaisuuden ja oikeuksien turvaamiseksi sekä asiakas- ja potilasturvallisuuden varmistamiseksi HUS-yhtymä esittää, että asiakastietolakiin lisätään säädös, jonka mukaisesti Uudenmaan hyvinvointialueiden, Helsingin kaupungin ja HUS-yhtymän potilastietojen käsittely tapahtuisi samalla periaatteella kuin muilla hyvinvointialueilla, eli perusterveydenhuollon ja erikoissairaanhoidon välillä ei tarvita luovutuslupaa eikä potilailla olisi mahdollista tehdä luovutuskieltoa.

Toisiolain tietojohtamista koskeva säädös § 41 asettaa Uudenmaan ja muun Suomen hyvinvointialueet eriarvoiseen asemaan. Esim. Pohjois-Pohjanmaan hyvinvointialue (POHDE) on yksi rekisterinpitäjä ja toisiolain mukainen palvelunantaja, joka voi käyttää asiakastietoja esim. perusterveydenhuollon ja erikoissairaanhoidon hoitoketjujen ja yhteentoimivuuden analysointiin.

Sen sijaan 41 § 3 mom. estää Uudenmaan hyvinvointialueiden perusterveydenhuollon ja erikoissairaanhoidon (HUS-yhtymä) potilashoidon analysoinnin, koska 3 momentti rajoittaa tietojohtamisen vain hyvinvointialueiden omiin rekistereihin tallennettuihin tietoihin. Säädöksen kummallisuus on potilastiedot, ”joita HUS-yhtymä tuottaa rahoitusvastuun perusteella hyvinvointialueen lukuun.” Jos HUS-yhtymä tuottaa sille lainsäädännössä määrättyjä tehtäviä, on HUS-yhtymä myös tietojen rekisterinpitäjä.

Uudenmaan terveydenhuollon toiminnan johtaminen ja suunnittelu edellyttää vastaavaa sääntelyä kuin muilla hyvinvointialueilla.

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

Tuomme esiin haasteena sen, että Suomessa lääketieteellisessä tutkimuksessa ja kliinisessä lääketutkimuksessa käsittelyperusteena on kansallisen lainsäädännön mukaan (laki lääketieteellisestä tutkimuksesta 488/1999 21 a § ja laki kliinisestä lääketutkimuksesta 983/2021 33 §) tietosuoja-asetuksen 6 ja 9 artiklan mukainen yleinen etu.

Sen sijaan usein eurooppalaisilla tutkimuskumppaneilla käsittelyperusteena on tietosuoja-asetuksen mukainen suostumus. Lisäksi tutkimuskumppaneiden käsitys tietoisesta suostumuksesta on lavea verrattuna suomalaiseen tulkintaan (kts. tietosuojavaltuutetun toimiston sivu https://tietosuoja.fi/rekisteroidyn-suostumus), jonka mukaisesti rekisteröidylle on pystyttävä yksilöimään kaikki käsittelytarkoitukset sekä kaikki tutkimuksen edellyttämät tietojen luovutukset.

Lienee sanomatta selvää, että edellä mainittu tilanne aiheuttaa hämmennystä ja ristiriitoja jäsenvaltioiden välisessä tutkimuksessa.

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

Kyllä, ne ovat selventäneet osittain tiettyjä erityiskysymyksiä. Huomionarvoista kuitenkin on, että jos asetuksen soveltaminen vaatii lukuisia erillisiä soveltamisohjeita, tämä kertoo implisiittisesti siitä, että itse asetusteksti on vaikeasti hahmotettava ja tulkittavissa usealla tavalla.

Erityisen tärkeää olisi saada EDPB:n soveltamisohje koskien tieteellisten tutkimusten aineistojen säilyttämistä ja niiden myöhempää yleisen edun mukaista hyödyntämistä (5 artiklan 1 b) kohta).

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?

-

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

-

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?

Henkilötiedon määritelmä aiheuttaa sen, että joudutaan raskaisiin sopimusprosesseihin, vaikka aineisto olisi luovuttajan näkökulmasta anonyymiä eikä vastaanottajalla ole tosiasiallisia mahdollisuuksia tunnistaa henkilöitä kohtuullisilla keinoilla. Tämä aiheuttaa samalla myös monimutkaisia teknisiä järjestelyitä aineistojen toimittamisessa. Kolmansissa maissa olevien sopimuskumppaneiden on vaikea ymmärtää, miksi heidän on sitouduttava EU-komission vakiolausekesopimukseen, vaikka heidän näkökulmastaan heille luovutettavasta aineistosta ei ole mahdollista tunnistaa henkilöitä.

Rekisterinpitäjille on annettu kohtuuttoman suuri vastuu arvioida muiden maiden tietosuojalainsäädäntöä (ns. TIA-arviointi). Esim. Kanadassa voi olla aluekohtaisia lainsäädännön eroja julkisen hallinnon toimijoilla kuten sairaaloilla tai tutkimuslaitoksilla.

TSA:n 4 artiklan mukaan geneettinen tieto on henkilötietoa, mutta mikä on tosiasiassa geneettistä tietoa, joka mahdollistaa henkilön tunnistamisen? Kaikki geneettinen tieto ei mahdollista henkilön tunnistamista. Kuitenkin tietosuoja-asetuksen 4 artiklaa tulkitaan herkästi niin, että kaikki geneettinen tieto on aina henkilötietoa.

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?

-

Kommentit yleisen tietosuoja-asetuksen I lukuun – Yleiset säännökset

Rekisterinpitäjän määrittely on sekava. Tämä tuodaan esiin alempana kohdassa kommentit IV lukuun.

Kommentit yleisen tietosuoja-asetuksen II lukuun – Periaatteet

Jo aikaisemmin olemme todenneet, että 5 artiklan 1 b) kohtaa tulisi täsmentää EDPB:n soveltamisohjeella (tutkimukseen kerätyn aineisto hyödyntäminen myöhemmin muissa tutkimuksissa).

11 artikla on malliesimerkki siitä, että asetuksen teksti on vaikeasti hahmotettavaa:

”Jos tämän artiklan 1 kohdassa tarkoitetuissa tapauksissa rekisterinpitäjä pystyy osoittamaan, ettei se pysty tunnistamaan rekisteröityä, rekisterinpitäjän on ilmoitettava asiasta rekisteröidylle, jos tämä on mahdollista.”

Jos rekisterinpitäjä ei pysty tunnistamaan rekisteröityä, kuinka käytännössä on mahdollista ilmoittaa rekisteröidylle, että häntä ei voida tunnistaa?

Kommentit yleisen tietosuoja-asetuksen III lukuun – Rekisteröidyn oikeudet

Informointivelvollisuus laaja ja yksityiskohtainen, mutta sen tulisi kuitenkin olla tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tämä ei ole todellakaan helppoa, koska jo rekisterinpitäjän käsitteestä on monenlaisia tulkintoja.

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

Tässä luvussa kiteytyy tietosuoja-asetuksen perusongelma seuraavasti: kolmen keskeisen käsitteen (rekisterinpitäjä, käsittelijä, yhteisrekisterinpitäjä) määrittelemiseen ei riitä asetuksen teksti, vaan EDPB on julkaisut em. käsitteiden soveltamista varten yli 50 sivuisen ohjeen (EDPB guidelines 07/2020). Lainvalmistelutyötä ei voi pitää onnistuneena, jos kolmen keskeisen käsitteen ymmärtäminen vaatii erillisen massiivisen ohjeen. Tähän on viitattu myös kohdassa Ovatko Euroopan tietosuojaneuvoston antamat ohjeet auttaneet käytännön soveltamistilanteisiin liittyvien ratkaisujen tekemisessä? Hyvin valmisteltu lainsäädäntö on itsessään niin selkeä, että erillisiä soveltamisohjeita ei tarvita.

36 artiklan mukainen ennakkokuuleminen ei käytännössä toimi, vastauksen saaminen valvontaviranomaiselta kestää usein niin kauan, että varsinainen hanke kuten tutkimus viivästyy ja esim. mahdollinen tutkimuksen rahoitus jää saamatta. Tilannetta korjaisi säädös määräajasta.

Tietoturvaloukkausten ilmoittamisesta valvontaviranomaisille tulisi luoda nykyistä kattavampia käytännesääntöjä toimialoittain. Isossa sosiaali- tai terveydenhuollon toimintayksikössä, jossa henkilökuntamäärä sekä asiakas- tai potilasmäärä on suuri, tietoturvaloukkauksia tapahtuu väistämättä inhimillisten erehdysten ja vahinkojen vuoksi. Valvontaviranomainen vaikuttaa olevan pulassa suurten ilmoitusmäärien vuoksi, tästä kertoo pitkät ilmoitusten käsittelyajat ja vakiomuotoiset vastaukset. Herää väistämättä kysymys, mikä on niukat resurssit huomioon ottaen

järkevää ja toteuttaa tietosuosuoja-asetuksen periaatteita. Tärkeintä varmaankin on, että rekisteröity saa tiedon häntä koskevasta tietoturvaloukkauksesta. Toimialakohtaiset nykyistä tarkemmat käytännesäännöt voisivat kirkastaa sitä, milloin ilmoittaminen ei ole tarpeellista ja säästäisi näin sekä rekisterinpitäjän että valvontaviranomaisen resursseja.

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

Tässä kohdassa jo otsikko ilmentää tietosuoja-asetuksen käsitteiden tulkinnan varaisuutta. Mitä eroa on tiedon siirrolla ja luovutuksella? Tai onko siirto jotakin muuta kuin luovutusta? Jälleen kerran asiaa kuvastaa, että 46 artiklan 2 kohdan a) alakohdan 3 kohdan b) alakohdan soveltamisesta on annettu erillinen EDPB:n ohje (guidelines 2/2020). Siis yhden artiklan kahden alakohdan soveltaminen edellyttää erillistä ohjetta.

Tähän liittyy myös EDPB:n guidelines 05/2021, jossa todetaan seuraavasti: Since the GDPR does not provide for a legal definition of the notion “transfer of personal data to a third country or to an international organization, it is essential to clarify this notion.” Jälleen kerran asetuksen yhtä keskeistä käsitettä (tässä tapauksessa siirto) ryhdytään määrittelemään vasta erillisessä soveltamisohjeessa.

Yhdysvaltojen osalta tilanne muuttuu jatkuvasti. 10.7.2023 on tullut voimaan DPF-kehys, jonka tulevaisuus on epävarma. Jos tietojen siirto toteutetaan voimassa olevan DPF-kehyksen avulla, mitkä ovat rekisterinpitäjän vastuut, jos DPF-kehys myöhemmin kumoutuu? Rekisterinpitäjän kannalta jatkuva epävarmuus on sietämätön tilanne, koska valvontaviranomaisen kanta on usein se, että rekisterinpitäjä vastaa aina kaikesta, vaikka olisi toiminut tiettynä hetkenä voimassa olleen hyväksytyn menettelyn mukaisesti.

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

89 artikla antaa liikkumavaraa henkilötietojen käsittelylle tutkimustoiminnassa, mutta sen käytännön soveltamista voidaan tulkita monella tavoin. Olisi toivottavaa, että EDPB antaisi ko. artiklasta soveltamisohjeen.

Hämäläinen Petri
HUS-Yhtymä - HUS-yhtymä