

Asia: VN/33623/2021

Lausuntopyyntö luonnoksesta hallituksen esitykseksi eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain muuttamisesta

Lausunnonantajan lausunto

Mahdollistaako luonnoksessa hallituksen esitykseksi esitetty ratkaisuehdotus suomalaisten rekisteritietojen käytön kansainvälisessä tutkimusyhteistyössä?

Jos ei, perustele miksi [Lainsäädännön asettamat velvoitteet ovat olleet välttämätön onnistumisen edellytys toisiokäytön tietosuojan myönteisen kehityksen kannalta - samalla tavalla kuin EU:n yleinen tietosuoja-asetus on vienyt velvoittavana lainsäädäntönä tietosuojan kehitystä eteenpäin EU:ssa. Kansallisella tasolla tavoitteeseen pääseminen on edennyt 5.10.2020 julkaistun määräyksen jälkeen tilanteeseen, jossa vaatimusten mukaisia käyttöympäristöjä on nyt keväällä käytössä seitsemän kappaletta Findatan Kapseli-ympäristön lisäksi. Käyttöympäristöjen tietoturva-vaatimukset (auditointikriteerit) ovat osa toisiolain asettamia raameja, ja on oletettavaa, ettei Suomesta käsin tapahtuvalla pelkällä käyttöympäristöä koskevien tietoturva-vaatimusten muotoilulla saavuteta toivottua vaikutusta, ellei tukena ole jäsenmaata määräävää lainsäädäntöä. Kynnys ryhtyä noudattamaan suomalaisia vaatimuksia ulkomailla sijaitsevien käyttöympäristöjen tietoturvasuuden osoittamisessa – vaikkakin käytettäisiin kansainvälisiä sertifiointistandardeja - on korkea, koska vaatimustenmukaisuuden toteuttaminen ja auditointi aiheuttavat kustannuksia ja vievät aikaa. Kuten esityksessä todetaan, EU:ssa ei ole tällä hetkellä lainsäädäntöä tai EU:ssa yhteisesti sovittuja käytänteitä, joita olisi mahdollista käyttää tietoturvallisten käyttöympäristöjen tietoturvasuuden arviointiin. Yhteiseurooppalaisten standardien puuttuessa Findata ei tässä tilanteessa näe ratkaisuksi käyttöympäristöjen auditointikriteeristön päivittämistä.]

Onko jokin ehdotuksessa esitetty muu toteuttamisvaihtoehto parempi kuin esitetty ratkaisuehdotus?

3) Näiden vaihtoehtojen yhdistelmä [Valmistelussa olevan EHDS-regulaation myötä on EU-tasolla toivottavasti kehittymässä terveysdatan vaihdon mahdollistavaa infrastruktuuria ja tietoturva-vaatimusten yhtenäistämistä. Toisioaineistojen luvittaminen osaksi kansainvälistä toisessa maassa tapahtuvaa tutkimusta olisi syytä huomioida toisiolaissa omana käyttötapauksenaan, jossa tietoturvan ja tietosuojan varmistaminen toteutetaan hyödyntäen kulloinkin voimassaolevaa ja sitovaa EU-lainsäädäntöä sanktioineen sekä määrittämällä tietoluvan myöntävälle viranomaiselle selkeät sopimusehdot, joita luvansaajan (rekisterinpitäjä) ja käyttöympäristön palveluntarjoajan on ennen luvan myöntämistä sitouduttava noudattamaan. Findata haluaa korostaa, että ulkomaisten tutkijoiden on mahdollista analysoida rekisteriaineistoja Findatan Kapselissa ja muissa auditoiduissa

käyttöympäristöissä joko omissa tutkimushankkeissaan tai osana suomalaista tutkimusryhmää. Kapselin käyttö ei ole sidottu paikkaan, vaan tunnistautumisen jälkeen tietoluvassa mainitut henkilöt voivat käyttää etätöppöytää myös muista maista käsin. Ulkomaisten käyttäjien osuus vuoden 2022 ensimmäisellä neljänneksellä oli noin 8% Kapselin käyttäjistä.]

Mitä muita ratkaisuvaihtoehtoja olisi mahdollista esittää kansainvälisen tutkimusyhteistyön toteuttamiseksi? Perustelut ratkaisuvaihtoehdolle.

Ratkaisuehdotuksemme muissa maissa sijaitseviin käyttöympäristöihin tapahtuvien tietoluovutusten osalta on seuraava:

KV-tutkimuksista tehdään toisilakiin erillinen käyttötapaus. Käyttöympäristön tietoturva-vaatimusten ja sertifiointimenettelyjen sijaan keskitytään salassa pidettävien henkilötietoaineistojen käsittelyn suojaukseen voimassa olevan velvoittavan lainsäädännön (GDPR) tukemana. Avainkohdat ovat:

Roolit: Vain tietolupaviranomainen voi myöntää tietolupia ulkomaisiin käyttöympäristöihin ja toteuttaa toisioaineistojen siirtoja ulkomaille. Tietolupakäsittelyssä arvioidaan erityisen kriittisesti tiedonhyödyntämissuunnitelman asianmukaisuutta käyttötapaukseen nähden.

Sopimus: Henkilötietoaineiston vastaanottavan palveluntarjoajan ja tietolupaviranomaisen kanssa tehdään vakio-tyyppinen tietosuojasopimuksen vaatimukseen kytketty sopimus:

-Tietolupaviranomainen määrittää sopimuksen sisällön.

-Sopimus on oltava voimassa ennen tietoluvan myöntämistä koskien kyseistä käyttöympäristöä.

-Sopimuksessa edellytetään vaatimusten huomiointia myös mahdollisesti käytettävien tiedonkäsittelijöiden (IT-toimittajat) osalta.

-Sopimuksen liitteenä on käyttöympäristöltä edellytettävä vaikutusten arviointi (DPIA), jossa on tehty hyväksytty riskiarvio käyttöympäristön suojaukseen liittyville keskeisille teknisille, fyysisille ja organisatorisille osille. Vaikutustenarviointi uusitaan vuosittain ja toimitetaan tietolupaviranomaiselle.

-Käyttöympäristön palveluntarjoajalla on sopimuksessa nimettynä tietosuojavastaava, joka valvoo henkilötietojen käsittelyä sekä neuvoo henkilötietoja käsitteleviä työntekijöitä heidän velvoitteistaan ja tiedottaa heille niistä.

-EU/ETA-ulkopuolelle tapahtuvissa siirroissa noudatetaan vallitsevia Euroopan tietosuojaneuvoston ohjeita.

Aineistojen suojaus:

-Aineistoja ei koskaan luovuteta ulkomaille suoria henkilötunnisteita sisältävinä vaan aineistot pseudonymisoidaan ennen siirtoa tietolupaviranomaisen toimesta.

-Siirto tapahtuu salattuna palveluntarjoajalle tietolupaviranomaisen tietoturvallista käyttöpalvelua käyttäen.

Valvonta: Valvira ylläpitää rekisteriä sopimuksen omaavista ulkomaisista käyttöympäristöistä. Tietolupaviranomainen toimittaa laaditun sopimuksen Valviralle

Sanktiot: Tietosuojarikkomuksia käsitellään ja niihin liittyvät seuraamusmaksut määrätään tietosuojaviranomaisten toimesta.

Kustannukset: Maksuasetus säädetään kattamaan tietolupaviranomaisen palveluntarjoajan kanssa tehtävän sopimuksen kulut sekä muut syntyvät kustannukset. Palveluntarjoajalle asetetaan rekisteröitymismaksu.

Jatkokehitys: Menettelytavat kehitetään vastaamaan EU-tasoisia EHDS-vaatimuksia niiden voimaantulon edetessä.

Ratkaisuehdotuksen mukainen toiminta edellyttää toisilakiin muutoksen, jolla annetaan tietolupaviranomaiselle päätäntävalta säätää tarkemmin em. menettelytavoista.

Muut hallituksen esityksen luonnosta koskevat huomiot.

Pyydämme huomioimaan myös toisoin (52 §) tietolupaviranomaiselle asettaman vaatimuksen varmistaa käyttöympäristössä tuotettujen tulosten anonymisointi. Vaatimus kohdistuu ainoastaan tietolupaviranomaiseen, riippumatta siitä kuka on myöntänyt tietoluvan tai missä käyttöympäristössä käsittely on tapahtunut. Käytännössä tietolupaviranomaisen on varmistettava siis kaikkien käyttöympäristöjen tulosten anonymiteetti, mikä lisää merkittävästi resurssitarpeita.

Ehdotus: Tietoluvan saaja on aineiston rekisterinpitäjä ja vastaa aina tietolupaehtojen mukaisesta anonymisoinnin toteuttamisesta. Tietolupaviranomainen puuttuu havaittuihin ja tietolupaviranomaiselle tiedoksi saatettuihin poikkeamiin. Tietolupaviranomaisella on oikeus tehdä anonymisointiin liittyviä tarkastuksia. Tilanteissa, joissa luvansaajalle luovutettu toisoinlain alainen aineisto sisältää suoria henkilötunnisteita, aineisto toimitetaan aina tietoluvan myöntäjälle tarkastettavaksi ennen julkaisua.

Lanu Heikki
Terveysten ja hyvinvoinnin laitos THL - Sosiaali- ja terveysalan
tietolupaviranomainen Findata