Kuva- ja signaalitiedon anonymisointi ja anonymiteetti sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (522/2019) mukaisessa käsittelyssä

Sosiaali- ja terveystietojen toissijaisen käytön tietosuojan asiantuntijaryhmä (VN/23353/2022) linjaa seuraavaa kuva- ja signaalitiedon anonymisoinnista ja anonymiteetista sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019, jäljempänä ”toisiolaki”) mukaisessa käsittelyssä. Tämä linjaus ei koske genomi- ja geneettistä dataa. Linjaus ei ota kantaa anonymisoinnissa käytettäviin työkaluihin tai teknisiin ratkaisuihin.

Tausta

- Toisiolaissa käytetyt määritelmät perustuvat vahvasti EU:n yleisen tietosuoja-asetuksen (2016/679) mukaisiin määritelmiin. Anonymisoinnin osalta lähtökohtana pidetään tietosuoja-asetuksen henkilötiedon määritelmää, asetuksen johdanto-osan 26-kohdan mukaista tulkintaohjetta, Unionin tuomioistuimen oikeuskäytäntöä, Euroopan tietosuojaneuvoston ohjeita, tietosuojaryhmän (WP29) laatimia, tietosuojaneuvoston hyväksymiä ohjeita sekä tietosuojan asiantuntijaryhmän aiempaa linjausta[1] anonyymin tiedon määritelmästä. Yleisen tietosuoja-asetuksen (2016/679) mukainen minimointiperiaate tulee ottaa huomioon ja tietojen määrä ja tarkkuus arvioida suhteessa käyttötarkoitukseen. Aineistoa rajaamalla ja kuvien resoluutiota vähentämällä voidaan myös vähentää tunnistamiseen liittyvää riskiä.
- Toisiolain mukaan tietoluvan perusteella luovutettavan henkilötietoaineiston anonymisoinnista vastaa Tietolupaviranomainen, siitä riippumatta, mikä taho on myöntänyt tietoluvan. Tietolupaviranomainen vastaa luovutettavien tietojen anonymisoinnista ja niiden luovuttamisesta luvansaajan käsiteltäväksi, poikkeuksena tilastoviranomaisten tietojen käsittely toisiolain 7 § mukaisesti. Tietoluvan saaja voi tuottaa anonyymit julkaistavat tulokset, kun Tietolupaviranomainen myöntää tähän oikeuden. Tietolupaviranomainen vastaa kuitenkin julkaistavien tietojen anonymisoinnin varmistamisesta.
- Tietoa käsittelevän tahon tulee seurata anonymisoidun aineiston tunnistettavuuteen liittyvää riskiä säännöllisesti. Aineiston käsittelyyn tulee soveltaa tietosuojasääntelyä, jos anonyymi aineisto muuttuu henkilötiedoksi.

Kuva- ja signaalitiedon anonymisointi ja anonymiteetti

- Kuva- ja signaalitiedon anonymiteettia tulee tarkastella ensisijaisesti vastaanottajan näkökulmasta. Suhteessa alkuperäiseen rekisterinpitäjään tiedot ovat yleisen tietosuoja-asetuksen (2016/679) näkökulmasta lähtökohtaisesti edelleen henkilötietoja, jos kyseinen rekisterinpitäjä säilyttää alkuperäiset henkilötiedot itsellään. Muulle taholle sama tieto voi kuitenkin olla anonyymiä[2]. Kun tietoa julkaistaan, vastaanottajajoukko on rajaamaton. Tällöin tietojen riittävään anonymisointiin tulee kiinnittää erityistä huomiota.
- Yksittäisen kuvan tai signaalitietokuvion (esim. sydänfilmi ilman aikaleimaa) perusteella on useissa tapauksissa käytännössä mahdotonta tunnistaa yksittäistä henkilöä ilman kyseisen kuvan tai

signaalitiedon etsimistä potilastietojärjestelmästä, mikä on lähtökohtaisesti kiellettyä. Tällaista kuvaa voidaan pitää anonyymina, jos kuvassa ei ole potilaan tunnistetietoja mukana, eikä vastaanottaja voi yhdistää kuvaa potilaan tunnistetietoihin tai muuhun tietoon henkilön tunnistamiseksi keinoin, joita joku voisi kohtuullisen todennäköisesti käyttää.

- Anonyymista kuvasta tai signaalitietokuviosta tulee olla poistettu henkilöön viittaavat tunnistetiedot, kuten nimi, henkilötunnus, syntymäaika, tarkka ikä, kuvauspäivämäärä sekä muut tunnistamisen mahdollistavat metatietokentät. Tunnistamisriskiä voidaan vähentää rajauksin ja resoluution vähentämisen avulla.
    - Anonyymiin kuva- ja signaalitietoon voidaan liittää yleisiä lisätietoja (esim. potilaan karkea ikäluokka ja löydöksen luokittelutietoja), kunhan kokonaisuus pysyy anonyyminä.
    - Tunnistettavuutta arvioitaessa erityistä harkintaa tulee käyttää seuraavanlaisiin tietoihin, joihin liittyy huomattava tunnistamisen riski: kasvokuva (lähtökohtaisesti pidettävä tunnistettavana), kasvojen muodon paljastava magneettikuva, hammaskartta, sormenjälki, silmän iiris, kämmenen kuva, kuva jostain erittäin harvinaisesta löydöksestä sekä kuva ihossa olevasta tatuoinnista (lista ei ole kattava).
    - Jos kuva- tai signaalitietokuvio esittää ominaisuutta, joka vaihtelee mittauksesta toiseen (esim. verenpaine), on tunnistettavuuden riski pienempi.
    - Anonyymiin kuva- tai signaalitietoon ei voi liittyä pseudotunnisteita, jotka vastaanottajan on mahdollista yhdistää tiettyihin tutkimushenkilöihin.
- Yleisen tietosuoja-asetuksen (2016/679) sekä Unionin tuomioistuimen ratkaisukäytännön mukaan tulee arvioida, onko tietoja käsittelevällä taholla käytettävissään laillisia keinoja, joita se kohtuullisen todennäköisesti voisi käyttää, tunnistamaan yksilöitä. Tunnistamisen kohtuullisuutta arvioitaessa tulisi ottaa huomioon kaikki objektiiviset tekijät, kuten tunnistamisesta aiheutuvat kulut, tunnistamiseen tarvittava aika sekä käsittelyajankohtana käytettävissä oleva teknologia ja tekninen kehitys. Asiantuntijaryhmä on muodostanut Unionin tuomioistuimen ratkaisukäytännön perusteella[3] tulkinnan, että laittomia keinoja ei pidetä kohtuullisina. Vaikka esimerkiksi alkuperäinen rekisterinpitäjä voisi hallussaan olevista kuva- ja signaalitietovarannoista löytää täysin samanlaisen kuvan tai kuvion, jolloin yhdistäminen tunnistetietoihin ja täten tunnistaminen on mahdollista, tulee henkilötietojen käsittelyä koskeva sääntely sovellettavaksi vain, jos rekisterinpitäjä ryhtyy käsittelemään tällaista muuta käyttötarkoitusta varten käsiteltyä tietoa. Tällaiseen käsittelyyn ei rekisterinpitäjällä tai muulla taholla yleensä ole laillista perustetta. Lisäksi yhdistäminen olisi useimmiten myös teknisesti kohtuuttoman vaikeaa. Arviointi sen osalta, voiko laillinen peruste tietojen yhdistämiselle olla, tulee tehdä tapauskohtaista harkintaa käyttäen.
- Kuva- ja signaalitiedon anonymiteettia arvioitaessa tulee aina käyttää tapauskohtaista harkintaa ja suorittaa asianmukainen dokumentoitu riskinarviointi sekä tarvittaessa tietosuojaa koskeva vaikutustenarviointi. Anonymisointiin liittyvillä tapauskohtaisilla olosuhteilla on olennainen merkitys henkilön tunnistettavuuden ja henkilötietojen anonymisoinnin tehokkuuden arvioinnissa. Mahdollisuus yhdistää muuta aineistoa kuva- tai signaalitietoon lisää tunnistamisen riskiä. Mitä enemmän tietoa liitetään, sitä suuremmaksi kasvaa riski sille, että yksilö voidaan tunnistaa. Anonymiteettiä ja siihen liittyviä riskejä kokonaisuutena arvioitaessa on otettava huomioon muut aineistot, joissa esiintyy samoja kuva- tai signaalitietoja.

Viitteet

[1] Periaatepäätös: Pseudonymisointi, anonymisointi ja suorien tunnisteiden käyttö sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (522/2019) mukaan. https://stm.fi/documents/1271139/2013549/Pseydonymisointi_anonymisointi_linjaus.pdf/a00821ea-0b18-ff44-ee0d-d7080215820a/Pseydonymisointi_anonymisointi_linjaus.pdf?t=1603108675223

[2]Se, että sama tieto voi näyttäytyä yhdelle toimijalle henkilötietona samalla kun toisella toimijalla ei ole käytettävissään kohtuullisia keinoja yhdistää tietoa tiettyyn henkilöön liittyväksi, rakentuu sisälle henkilötiedon käsitettä koskevaan Unionin tuomioistuimen ratkaisukäytäntöön. Ratkaisukäytännössä on arvioitu eri tahoilla olevia keinoja tietojen yhdistämiseksi tiettyä henkilöä koskevaksi sekä näiden eri tahojen käytössä olevien keinojen kohtuullisuutta. Ratkaisukäytännön perusteella näyttää olevan tarpeen arvioida tietojen vastaanottajan käytettävissä olevia keinoja. Katso esimerkiksi tuomio 19.10.2016, Breyer, C-582/14, EU:C:2016:779 kohdat 44–45 sekä tuomio 9.11.2023, C-319/22, EU:C:2023:837 kohta 49, jotka ohjaavat arvioimaan tilannetta eri toimijoiden näkökulmista sen sijaan, että tuomioistuin toteaisi suoraan kysymyksessä olevan henkilötiedon käsittely kaikissa tilanteissa riippumatta tietoja käsittelevien tahojen käytettävissä olevista keinoista. Asiantuntijaryhmä huomioi lisäksi, että vastaavasti on todettu Unionin yleisen tuomioistuimen tuomiossa 26.4.2023, SRB v. EDPS, T-557/20, EU:T:2023:219 kohdat 101–105 (tuomio ei tätä linjausta annettaessa ole lainvoimainen).

[3]Asiantuntijaryhmän tulkinta on muodostettu Unionin tuomioistuimen ratkaisukäytännön perusteella. Katso Unionin tuomioistuimen tuomio 19.10.2016, Breyer, C-582/14, EU:C:2016:779, jonka kohtien 45–46 mukaan oli selvitettävä, onko mahdollisuus yhdistää dynaaminen IP-osoite mainittuihin internet-yhteyden tarjoajan hallussa oleviin lisätietoihin rekisteröidyn tunnistamiseksi kohtuullisesti toteutettavissa oleva keino. Näin ei ollut muun muassa, kun rekisteröidyn tunnistaminen on kielletty laissa.

Liite 1. Esimerkkejä linjauksen soveltamisen tueksi

Esimerkki 1. Tietoluvan perusteella tapahtuva aineiston käsittely (toisiolaki 14 §, 51 §)

Findata tai yksittäinen rekisterinpitäjä myöntää luvansaajalle oikeuden käyttää kuva- ja signaalitietoa tietoluvan perusteella. Jos aineisto luovutetaan luvansaajalle anonyymissa muodossa, Findata suorittaa anonymisoinnin. Kuva- ja signaalitiedon luovuttaminen suoraan alkuperäiseltä rekisterinpitäjältä toisiolain mukaiseen käyttötarkoitukseen anonyymissa muodossa on mahdollista vain, jos Findata ulkoistaa anonymisoinnin ko. alkuperäiselle rekisterinpitäjälle. Anonymisoinnin suorittamisen ulkoistamisen osalta Findata tekee tapauskohtaista harkintaa ja huolehtii toiminnan juridisesta asianmukaisuudesta. Toisiolain mukaan tietoluvan perusteella luovutettua aineistoa tulee käsitellä tietoturvallisessa käyttöympäristössä, vaikka se olisi anonymisoitua, ellei kyseessä ole aggregoitu tilastotieto. Tietoturvallisen käyttöympäristön ulkopuolella voi käsitellä anonyymia tulosaineistoa toisiolain 52§ mukaisesti (ks. esimerkit 2 ja 3).

Jos tietoluvalla myönnetään oikeus käsitellä kuva- ja signaalitietoa pseudonymisoituna, luvan myöntänyt taho vastaa aineiston pseudonymisoinnista.

Esimerkki 2. Anonyymin aineiston käsittely ilman toisiolain mukaista tietolupaa

Jos kuva- ja signaalitieto on valmiiksi anonyymissa muodossa (esim. rekisterinpitäjä on anonymisoinut aineiston muun lain perusteella kuin toisiolaki, tai aineisto on toisiolain mukaisen käsittelyn perusteella syntynyt anonymisoitu tulos tai tietopyynnön perusteella luovutettu tilastoaineisto), sen käsittelyyn ei sovelleta tietosuojasääntelyä eikä toisiolakia.

Esimerkki 3. Tietoluvan perusteella myönnetystä aineistosta tuotettujen tulosten käsittely (toisiolaki 52 §)

Kun luvansaaja käsittelee kuva- ja signaalitietoa tietoluvan perusteella, luvansaaja vastaa rekisterinpitäjän ominaisuudessa käsittelemästään aineistosta sekä tuottamistaan tuloksista. Luvansaaja voi tuottaa anonyymit julkaistavat tulokset, kun Tietolupaviranomainen myöntää tähän oikeuden. Tietolupaviranomainen vastaa julkaistavien tietojen anonymisoinnin varmistamisesta.

Kuva- ja signaalitiedoista sekä mahdollisista lisätiedoista muodostuvan anonyymin tulosaineiston voi koostaa ja julkaista 1) hakemalla tietoluvan, 2) muodostamalla anonyymin tulosaineiston, 3) varmistamalla tulosaineiston anonymiteetin Tietolupaviranomaisen toimesta ja 4) julkaisemalla tulokset.