

AINEISTOJEN JAKAMISEN MYYTEISTÄ JA HAASTEISTA

Tietosuojaavastaava Jarkko
Reittu



ESITYKSEN KOHDE

- Kuinka tietosuojalainsäädäntö rajoittaa aineistojen avointa julkaisemista
- Tässä esityksessä ei tarkastella esim. aineiston omistusoikeuksiin tai immateriaalioikeuksiin liittyviä kysymyksiä, jotka voivat myös olla erittäin hankalia avoimen julkaisemisen kannalta
- Esitetyt tulkinnat ovat omiani, eivätkä välttämättä edusta THL:n virallista linjaa

AINEISTON JAKAMISEEN LIITTYVÄT TIETOSUOJAAHAASTEET

- Käyttötarkoitussidonnaisuuden periaate: Henkilötietoja voidaan käyttää vain siihen tarkoitukseen mihin ne on alkujaan kerätty
 - Poikkeus: Tieteellinen tutkimus on kuitenkin yhteensopiva alkuperäisen käyttötarkoituksen kanssa
 - Jos tietoja aiotaan käyttää muuhun kuin alkuperäiseen tarkoitukseen, tulee asiasta informoida asianmukaisesti (artiklat 12-14)
 - Jos tiedot on kerätty henkilöltä itseltään, tulee käyttötarkoituksen muutoksesta informoida **aktiivisesti**, eikä tästä veloitteesta voida poiketa
- Henkilötietoja saa käsitellä vain niin kauan kuin se on tarpeen
- Aineiston jakaminen (tai arkistointi) ei saa johtaa tutkittavan kannalta ennakoimattomaan henkilötietojen käsittelyyn

AINEISTON JAKAMISEEN LIITTYVÄT TIETOSUOJAAHAASTEET (JATKUU)

- Viranomaisten rekistereistä saatujen tietojen käyttö on sallittua vain lupaehtojen mukaiseen tarkoitukseen
 - Käyttö on tyypillisesti rajoitettu vain tietopyynnössä yksilöityä tutkimustarkoitusta varten
 - Tutkimusryhmä ei voi luovuttaa näihin tietoihin suurempaa oikeutta mitä sillä itsellään on
- Tutkittavalta voidaan pyytää laaja suostumus koskien tiettyä tutkimusalaa
 - Suostumuksella on aina reunaehdot, jotka rajoittavat tietojen käyttöä
 - Suostumus on oltava peruutettavissa

AINEISTON JAKAMISEEN LIITTYVÄT TIETOSUOJAAHAASTEET (JATKUU)

- Tietojen minimoinnin periaate rajoittaa henkilötietojen käsittelyn vain tarkoituksen kannalta tarpeellisiin henkilötietoihin
- Henkilötietojen siirto EU/ETA:n ulkopuolelle on mahdollista vain riittävien suojaustoimenpiteiden toteutuessa. Jos henkilötietojen siirto perustuu suostumukseen, tulee tutkittavalle kertoa ennakkoon riittävästi tietojen siirtoon liittyvistä riskeistä.
- Rekisterinpitäjän tulee toteuttaa asianmukaiset tekniset ja organisatoriset suojaustoimenpiteet
- Täysin avoin henkilötietoja sisältävän tutkimusaineiston julkaiseminen ei näyttäisi olevan mahdollista

AINEISTON VAPAAN JAKAMISEN VAIHTOEHDOT

1. Aineiston jakaminen rajoitetaan pyydettyyn suostumukseen
2. Julkaistaan vain kuolleiden henkilöiden tietoja
 - Joskus kuolleita koskevat tiedot voivat koskea myös elossa olevia henkilöitä
3. Henkilö voisi myös itse saattaa henkilötiedot nimenomaisesti julkiseksi
 - Kuinka tämä voidaan toteuttaa käytännössä?
4. Henkilötietoja sisältävä aineisto anonymisoidaan pysyvästi, jolloin tietojen käsittelyyn ei sovelleta tietosuojalainsäädäntöä

PERUSKÄSITTEISTÄ

- *Henkilötiedoilla* tarkoitetaan kaikkia tietoja, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön
- *Henkilötietojen käsittelyllä* tarkoitetaan toimia, jotka kohdistuvat henkilötietoihin
- Tietosuoja-asetusta sovelletaan
 - automaattiseen tietojenkäsittelyyn sekä
 - manuaaliseen käsittelyyn, kun henkilötiedot muodostavat osan rekisteristä tai joiden on tarkoitus muodostaa osa rekisteristä
 - Ei sovelleta kuolleisiin henkilöihin tai oikeushenkilöihin (yritykset)
 - Huom. Tiedot voivat silti olla salassa pidettäviä

TUNNISTETTAVUUDESTA

- **Tunnistettavissa olevana** pidetään luonnollista henkilöä, joka voidaan **suoraan** tai **epäsuorasti** tunnistaa erityisesti tunnistetietojen perusteella, kuten
 - nimi, henkilötunnus, sijaintitieto, verkkotunnistetieto taikka yksi tai useampi tunnusomainen fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä
- Tunnistettavuutta arvioidaan muun kuin henkilön itsensä näkökulmasta eli pystyykö ulkopuolinen tunnistamaan tiedoista henkilön joko suoraan tai yhdistämällä tietoihin muita tietoja
- Pelkkä hypoteettinen tai häviävän pieni mahdollisuus tunnistamiseen ei tee tiedoista henkilötietoja. Tunnistaminen tulee olla toteutettavissa **kohtuullisin** tai **laillisin** keinoin.



PSEUDONYMISOINNISTA

”*pseudonymisoimisella* tarkoitetaan henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu”

PSEUDONYMISOINNISTA

- Pseudonymisointi on **prosessi**, jossa poistetaan suorat tunnistetiedot
- Lähtökohtaisesti pseudonymisoitu tieto on henkilötietoa
- Pseudonymisointi on yksi asianmukainen suojatoimi, jota tulisi käyttää, kun henkilötietoja käsitellään tieteellisessä tutkimustarkoituksessa

VOIKO PSEUDONYMISOITU TIETO OLLA MYÖS ANONYYMIA?

- Yleisesti esitetty väite: pseudonymisoitu tieto on **aina** henkilötietoa, vaikka pääsyä koodiavaimiin ei olisi ja koodiavaimet ovat edelleen olemassa
- Tietosuoja-asetuksen mukaan pseudonymisointi on vain määritelmän mukainen prosessi, eikä pseudonymisoidulle tiedolla ole erityistä määritelmää
- Voiko pseudonymisointiprosessin tuloksena syntyä myös anonyymia tietoa (ainakin jonkun toimijan näkökulmasta)?

VOIKO PSEUDONYMISOITU TIETO OLLA MYÖS ANONYYMIA?

- Tapauksessa C-582/14 ”Patrick Breyer” EU:n tuomioistuin linjasi, että sama tieto voi olla anonyymia toiselle osapuolelle, jos tällä toisella osapuolella ei ole käytettävissä **kohtuullisesti toteuttavissa olevia** keinoja, joilla saataisiin lisätietoja henkilön tunnistamiseksi
 - Jos pseudonymisoitu tieto on ilman koodiavaimia aidosti anonyymia eikä koodiavaimia voida saada haltuun kohtuullisesti toteutettavissa olevin laillisin keinoin, voi myös pseudonymisoitu tieto olla anonyymia tietyille osapuolille
- Vaikka Breyer-casen tuomio annettiin tietosuojadirektiivin aikaan, voidaan tuomiota pitää perustellusti edelleen pätevänä

VOIKO PSEUDONYMISOITU TIETO OLLA MYÖS ANONYYMIA?

- Tulkinnat tietosuoja-asetuksesta tekee viime kädessä EU:n tuomioistuin
- Kansallinen lainsäätäjät tai viranomaiset rikkoo EU:n perussopimuksia, jos se tekee tulkintoja tietosuoja-asetuksesta

MILLOIN TIETO ON ANONYYMIA?

Tieto on anonyymia jos:

- tiedosta ei voida suoraan tunnistaa henkilöä **ja**
- ei ole **kohtuullisen todennäköistä**, että henkilö voidaan tunnistaa
 - tiedoista itsestään tai
 - yhdistämällä tietoihin muita tietoja (esim. hankkimalla pseudonymisoidun tiedon koodiavaimet laillisia menetelmiä käyttäen)

LISÄTIETOJA

- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fi.pdf
- <http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN>
- <https://www.sciencedirect.com/science/article/pii/S0267364918300153>
- <https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm>