EU:N YLEINEN TIETOSUOJA-ASETUS

Jarkko Reittu
Tietosuojavastaava, Lakimies
Helsingin yliopisto, Yleishallinto
jarkko.reittu@helsinki.fi

ESITYKSEN SISÄLTÖ

1. YLEISTÄ ASIAA TIETOSUOJA-ASETUKSESTA
- Henkilötietojen käsittelyn peruskäsitteet
- EU:n tietosuoja-asetuksesta
- Rekisterinpitäjän velvollisuuksista
- 72h raportointivelvollisuus tietoturvaloukkauksissa
- Rekisteröidyn oikeudet
- Oikeussuojasta ja seuraamuksista

2. KUINKA VALMISTAUTUA ASETUKSEEN KÄYTÄNNÖSSÄ?

HENKILÖTIETOJEN KÄSITTELYN PERUSKÄSITTEET

- **Henkilörekisterillä** tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuva henkilötietoja sisältävää tietojoukko, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta
- **Rekisterinpitäjä**
  - yksi tai useampi
  - henkilö, yhteisö, laitos tai säätiö
  - jonka käyttöä varten henkilörekisteri perustetaan
  - ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty
- **Henkilötietojen käsittelijä**
  - luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin,
  - joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

HENKILÖTIETOJEN KÄSITTELYN PERUSKÄSITTEET

- Tietosuoja on otettava huomioitava aina kun **käsitellään henkilötietoja.**
- **Henkilötiedoilla** tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.
    - **Pseudonymisoitua** henkilötietoa käsitellään henkilötietona. Pseudonymisointi on vain yksi henkilötietojen suojakeino.
- **Käsittelyllä** tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.
- Erotettava toisistaan henkilötieto, arkaluonteinen henkilötieto, henkilötunnus ja lapsia koskevat henkilötiedot.

HENKILÖTIETOJEN KÄSITTELYN PERUSKÄSITTEET

- **Geneettisellä tiedolla** tarkoitetaan **henkilötietoja**, jotka liittyvät luonnollisen henkilön perittyihin tai hankittuihin ominaisuuksiin, jotka on saatu kyseisen luonnollisen henkilön biologisesta näytteestä analysoimalla, erityisesti kromosomien DNA:sta tai RNA:sta tai muusta vastaavia tietoja tarjoavasta tekijästä tehdyllä analyysilla.
- **Terveyttä koskeviin henkilötietoihin** kuuluvat seuraavat tiedot:
  1. Kaikki henkilön terveydentilaa koskevat tiedot
  2. Kaikki henkilön entisestä, nykyisestä tai tulevasta fyysisen terveyden tai mielenterveyden tilasta paljastavat tiedot
  3. Terveyspalvelujen saamista varten tai niiden tarjoamisen yhteydessä kerätyt tiedot, mm.
     a) henkilölle annettu numero, symboli tai erityistuntomerkki, jolla hänet voidaan tunnistaa yksiselitteisesti terveydenhuollon piirissä
     b) kehon osan tai kehosta peräisin olevan aineen testaamisesta tai tutkimisesta saadut tiedot, kuten geneettiset tiedot ja biologiset näytteet
     c) kaikki tiedot esimerkiksi sairauksista, vammoista, sairauden riskistä, esitiedoista tai annetuista hoidoista
     d) tieto rekisteröidyn fyysisestä tai lääketieteellisestä tilanteesta riippumatta siitä, mistä lähteestä tiedot on saatu, esimerkiksi lääkäriltä tai muulta terveydenhuollon ammattilaiselta, sairaalalta, lääkinnällisestä laitteesta tai diagnostisesta in vitro -testistä

HENKILÖTIETOJEN KÄSITTELYN PERUSKÄSITTEET

- **Erityisiin henkilötietoryhmiin** (eli arkaluonteisiin tietoihin) kuuluvat seuraavat tiedot:
  - rotu tai etninen alkuperä
  - poliittiset mielipiteet
  - uskonnollinen tai filosofinen vakaumus
  - ammattiliiton jäsenyys
  - geneettiset tai biometriset tiedot, jotka on kerätty henkilön yksiselitteistä tunnistamista varten
  - terveyttä koskevat tiedot
  - seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot

TIETOSUOJALAINSÄÄDÄNNÖN SOVELTAMINEN?

- SOVELLETAAN
  - Henkilötietojen automaattiseen käsittelyyn tai
  - Jos muodostuu henkilörekisteri tai sen osa
- EI SOVELLETA
  - Jos henkilötietojen käsittelyä suorittaa luonnollinen henkilö henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin
- SOVELLETAAN RAJOITETUSTI
  - Henkilötietojen käsittelyyn toimituksellisia, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten
- EI KOSKE KUOLLEITA
  - Huom.! Julkisuuslain salassapitösäännökset voivat koskea myös kuolleita

EU:N YLEINEN TIETOSUOJA-ASETUS ELI GDPR

- Tietosuoja-asetus on jo voimassa, mutta soveltaminen alkaa **25.5.2018**
- Tietosuoja-asetus on suoraan sovellettavaa oikeutta; kansallista liikkumavaraa erityisesti tutkimuksen osalta
- Nykyinen henkilötietolaki korvataan tietosuojalailla
- Kesällä annettiin OM:n muistio kansallisen lainsäädännön muutoksista, erityislainsäädäntö valmisteluun aikaisintaan syksyllä. **http://urn.fi/URN:ISBN:978-952-259-612-3**
- Suurimmat muutokset
  - Rekisterinpitäjän osoitusvelvollisuus (accountability)
  - Rekisteröidyn oikeudet laajenevat ja rekisterinpitäjän velvollisuudet kasvavat
  - 72 h raportointivelvollisuus tietoturvaloukkauksista
  - Oikeussuojakeinot ja seuraamukset ankaroituvat
  - Velvollisuus nimittää tietosuojavastaava (mm. viranomaiset, henkilötietoja paljon käsittelevät)

ARTIKLA 5 - HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAT PERIAATTEET

Henkilötietojen käsittelylle asetetut vaatimukset:

- Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Täsmällisyys
- Säilytyksen rajoittaminen
- Tietojen eheys ja luottamuksellisuus

➢ **Osoitusvelvollisuus, että vaatimukset täyttyvät**

OIKEUSPERUSTA ARTIKLA 6 MUKAAN

- Artikla 6: käsittelyn lainmukaisuus
  a) Suostumus
  b) Sopimuksen täytäntöönpano / toimeksianto
  c) ”Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi”
  d) Tarpeen rekisteröidyn elintärkeän edun suojaamiseksi
  e) ”Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi”
  f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.
    – paikkaa yhteysvaatimuksen puuttumista
    – edellyttää etujen, haittojen ja suojatoimien suhteuttamista
    – ei sovellu viranomaisiin!

HENKILÖTIETOJEN KÄSITTELYN TULEE PERUSTUA SUUNNITELMAAN

- Vain käyttötarkoituksen kannalta tarpeellisten henkilötietojen käsittely on mahdollista (**käyttötarkoitussidonnaisuus** & **tietojen minimoinnin periaate)**
- Henkilötietojen käsittely on suunniteltava etukäteen alusta loppuun perustuen riskiarvioon:
  - Mitä henkilötietoja kerätään? Miten henkilötietoja kerätään?
  - Mikä on oikeusperuste henkilötietojen käsittelylle?
  - Kuinka henkilötietoja käsitellään ja säilytetään?
  - Kuinka huolehditaan tietoturvasta?
  - Kuinka henkilötietojen käsittelyä valvotaan?
  - Kuinka on hoidettu henkilötietojen luovutukset ja siirrot?
  - Mitä henkilötiedoille tapahtuu käyttötarkoituksen päättymisen jälkeen?
  - Kuinka rekisteröidyn oikeudet toteutuvat?

REKISTERINPITÄJÄN VELVOLLISUUKSISTA

- **Osoitusvelvollisuus:** Rekisterinpitäjän on pystyttävä osoittamaan **kirjallisesti**, että rekisterinpitäjä noudattaa tietosuojalainsäädäntöä, henkilötietojen käsittelyä koskevia periaatteita sekä toteuttaa lainsäädännön edellyttämät rekisteröityjen oikeudet
- Vastuuta ei voida ulkoistaa; rekisterinpitäjä on 24 artiklan mukaisesti vastuussa siitä, että se toteuttaa tietosuoja-asetuksen edellyttämät **tekniset** ja **organisatoriset** toimenpiteet
  - Toimenpiteet tulee mitoittaa riskiperustaisen arvioinnin perusteella
  - Organisatoriset toimenpiteet: organisaation hallinnollinen tietosuoja, kuten tietosuojapolitiikat ja käytännöt, tietosuojaohjeet ja toimintamallit, sertifikaatit
  - Tekniset toimenpiteet: tietoturva, tekniset suojaustoimenpiteet uusin teknologia ja kustannukset huomioiden
- Artikla 25: Sisäänrakennettu ja oletusarvoinen tietosuoja
- Artikla 30: Kirjanpitovelvollisuus kaikista henkilötietojen käsittelyprosesseista
- Artikla 35: Tietosuojan vaikutustenarviointi pakollinen tietyissä tilanteissa

SISÄÄNRAKENNETTU JA OLETUSARVOINEN TIETOSUOJA

- Tietosuoja ja tietoturva on otettava huomioon jo suunnitteluvaiheessa
- Huolehdittava, että henkilötietoja käsitellään tietoturvallisessa ja tietosuojavaatimukset täyttävässä ympäristössä
- Toteuttamisessa voidaan käyttää esimerkiksi seuraavia toimenpiteitä:
  - Henkilötietojen pseudonymisointi
  - Riittävät suojatoimet
  - Koulutus, ohjeet, määräykset, sitoumukset ja sopimukset
  - Prosessit, käytännesäännöt, sertifikaatit
  - Tiedon salaaminen
  - Auditoinnit
  - Tekniset rajoitukset ja valvonta

ILMOITUSVELVOLLISUUS TIETOTURVALOUKKAUKSISTA 72H SISÄLLÄ

- Ilmoitus tehdään tietosuojaviranomaisella ja rekisteröidylle
- 33 artiklan mahdollistama poikkeus: jos tiedot on salattu, ilmoitusta ei tarvitse tehdä rekisteröidylle
- Tarkempaa ohjeistusta odotetaan tietosuojaviranomaisilta

HUONEENTAULU REKISTERÖITYJEN OIKEUKSISTA

- Oikeus saada läpinäkyvää informaatiota (Artikla 12-14, Artikla 19)
  - Silloin, kun henkilötiedot kerätään suoraan rekisteröidyltä
  - Silloin, kun henkilötiedot kerätään muualta kuin rekisteröidyltä
- Oikeus saada pääsy tietoihin (*tarkastusoikeus, Artikla 15*)
- Oikeus tietojen oikaisemiseen (*virheen oikaisu, Artikla 16*)
- Oikeus tietojen poistamiseen (”oikeus tulla unohdetuksi”, Artikla 17)
- Oikeus käsittelyn rajoittamiseen (Artikla 18)
- Oikeus siirtää tiedot järjestelmästä toiseen (Artikla 20)
- Vastustamisoikeus (Artikla 21)
- Automatisoidut yksittäispäätökset; profilointi mukaan luettuna
- Oikeus tulla informoiduksi henkilötietojen tietoturvaloukkauksista
- Lasten erityisasema
- Oikeus saada valvontaviranomaiselta apua
- Oikeus luottaa tietoturvaan

OIKEUSSUOJA JA SEURAAMUKSET

- Artikla 82: Oikeus korvauksen saamiseen
  - Rekisteröidyllä on oikeus saada täysi korvaus rekisterinpitäjältä tai henkilötietojen käsittelijältä tietosuoja-asetuksen rikkomisesta aiheutuneesta vahingosta
  - Rekisterinpitäjällä ankara vastuu
  - Henkilötietojen käsittelijällä toissijainen vastuu
- Artikla 83: Hallinnolliset sakot ja muut seuraukset
- max. 20 milj.euroa tai 4 % edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta
  - ”Kukin jäsenvaltio voi asettaa sääntöjä siitä, voidaanko viranomaisille tai julkishallinnon elimille määrätä kyseisessä jäsenvaltiossa hallinnollisia sakkoja ja missä määrin”
- Huomautus, varoitus, määräys, käsittelynrajoitus

KUINKA VALMISTAUTUA ASETUKSEEN KÄYTÄNNÖSSÄ?

KUINKA VALMISTAUTUA TIETOSUOJA-ASETUKSEEN?

1. Kartoita ja analysoi henkilötietoja käsittelevät prosessit
2. Analysoi käsiteltävät henkilötiedot ja käsittelyperusteet
3. Päivitä henkilörekisteriselosteet
4. Tarkasta sopimukset
5. Selvitä GDPR:n asettamat vaatimukset tietojärjestelmille
6. Kouluttaudu
7. Seuraa aktiivisesti yliopistotason ohjeistusta

1. KARTOITA HENKILÖTIETOJA KÄSITTELEVÄT PROSESSIT

- Missä henkilötietoja käsitellään?
- Mistä henkilötiedot on kerätty?
- Kuinka henkilötietoja käsitellään ja säilytetään? Kenellä on pääsy tietoihin?
- Henkilötietojen luovutukset ja siirrot (erityisesti ETA:n ulkopuolelle)
- Henkilötietojen muokkaaminen
- Varmuuskopiot
- Henkilötietojen arkistointi tai hävittäminen

2. ANALYSOI KÄSITELTÄVÄT HENKILÖTIEDOT JA KÄSITTELYPERUSTEET

- Henkilötietojen käsittelyn tulee olla suunniteltua
  - Henkilötiedon luokittelu (henkilötieto/arkaluonteinen henkilötieto/henkilötunnus)
  - Selvitä henkilötietojen käyttötarkoitus
    - Vain tarpeellisia ja virheettömiä henkilötietoja voidaan käsitellä (minimisointiperiaate)
    - Tuhoa käyttötarkoituksen kannalta tarpeettomat henkilötiedot
  - Selvitä henkilötietojen käsittelyn oikeusperusta
  - Suunnittele henkilötietojen koko elinkaari
  - Onko tietoturva asetuksen edellyttämällä tasolla?
  - Toteutuvatko rekisteröidyn oikeudet?
- GDPR:n mukainen kirjanpitovelvollisuus kaikista henkilötietojen käsittelyprosesseista artikla 30 mukaisesti

3. PÄIVITÄ REKISTERISELOSTEET

- Voimassa olevan lainsäädännön mukaan ”Rekisterinpitäjän on pidettävä rekisteriseloste jokaisen saatavilla.”
- Henkilörekisteriselosteet/tietosuojaselosteet ovat kerätty tällä hetkellä yliopiston Kirjaamon WWW-sivuille: https://www.helsinki.fi/fi/yliopisto/tietosuojaselosteet-0
- Tietosuoja-asetus **EI** sisällä nykyisen henkilötietolain mukaista velvollisuutta koskien rekisteriselosteita
  - Mutta rekisterinpitäjällä on
    a) 30 artiklan mukainen velvollisuus pitää kirjaa käsittelytoimista (Huom. Suomennos on huono ”Seloste käsittelytoimista” vs. ”Records of processing activities”); ei ainakaan täysin julkinen, koska voi sisältää salassapidettävää tietoa mm.”mahdollisuuksien mukaan yleinen kuvaus 32 artiklan 1 kohdassa tarkoitetuista teknisistä ja organisatorisista turvatoimista.”
    b) 12 artiklan mukainen rekisteröidyn informointivelvollisuus

4. TARKASTA SOPIMUKSET

- Kiinnitä huomiota erityisesti henkilötietojen siirtoon* ETA:n ulkopuolelle
  - Toteutuu erityisesti pilvipalveluita käytettäessä
  - Huomioi myös mahdolliset tukipalvelutilanteet, jossa annetaan etätukea ETA-alueen ulkopuolelta
  - Käytännön vaihtoehdot tällä hetkellä:
    1. Rekisteröidyn yksiselitteinen suostumus
    2. **Vain USA**: Privacy Shield, epävarmalla pohjalla USA:n tiedustelulainsäädännön vuoksi
    3. Komission määrittelemät riittävän tietosuojan maat tällä hetkellä: **Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay**
    4. **Komission mallisopimuslausekkeet**, tällä hetkellä paras vaihtoehto. Mallisopimuslausekkeet ovat myös vaarassa *(Irish Data Protection Commissioner v. Facebook and Max Schrems)*
- Uusi velvollisuus: Data Processing Agreement (DPA)

* Huom.! Henkilötietojen siirto ei ole sama asia kuin henkilötietojen luovuttaminen

4. DATA PROCESSING AGREEMENT

- Laadittava henkilötietojen käsittelijän ja rekisterinpitäjän välille, kun tietoja käsitellään rekisterinpitäjän puolesta ja lukuun
  - Tietojärjestelmäsopimukset, **Huom.! Henkilötietojen tallennus on henkilötietojen käsittelyä**
  - Materiaalinsiirtosopimukset (MTA), esim. analyysit rekisterinpitäjän puolesta
  - Tutkimussopimukset
  - Mahdollisesti myös tutkijan ja yliopiston välille, kun tutkija on rekisterinpitäjä ja yliopisto henkilötietojen käsittelijä. Kenellä on pääasiallinen vastuu sopimisesta?
- Myös vanhat sopimukset käytävä läpi, jos tietojen käsittely jatkuu myös 25.5.2018 jälkeen
- Rekisterinpitäjän tulee varmistaa, että suunniteltu henkilötietojen käsittelijä täyttää tietosuoja-asetuksen asettamat vaatimukset henkilötietojen käsittelylle.
- Tietosuoja-asetuksen mukaisesti rekisterinpitäjän ja henkilötietojen käsittelijän välille on laadittava osapuolia sitova **kirjallinen sopimus**, jossa **vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet.**
- Kirjallisen sopimuksen tekemättä jättämisestä uhkana sakko, max. 10 000 000 euroa tai 2 % edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta

4. DATA PROCESSING AGREEMENT - JATKUU

- Sovittava kirjallisesti edellä kuvatun lisäksi:
  1. Käsiteltävä tietoja rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti
  2. Salassapitoehto
  3. Tietoturvasta huolehtiminen 32 artiklan mukaisesti
  4. DPA:n sopimusehtojen ulottaminen myös alihankkijoihin
  5. Rekisterinpitäjää tukevat toimenpiteet, joilla turvataan rekisteröidyn oikeuksien toteutuminen
  6. Avustaminen 32-36 artiklassa säädettyjen velvollisuuksien toteuttamiseksi
  7. Henkilötietojen palauttaminen tai hävittäminen rekisterinpitäjän pyynnöstä
  8. Tarvittavien tietojen toimittaminen rekisterinpitäjälle osoitusvelvollisuuden toteuttamiseksi

4. DATA PROCESSING AGREEMENT - JATKUU

- Helsingin yliopistolla on oma DPA-sopimusmalli
- Katso myös ohje ” Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja”, ohjeen lopusta löytyy suomenkielinen DPA-sopimusmalli: https://www.hansel.fi/media/filer_public/1d/2c/1d2c32ab-bb9a-49c0-b75c-da64871d1df9/tietosuojaohje.pdf
- Voidaan ottaa tarvittaessa pääsopimuksen liitteeksi
- Ehdot eivät ole lähtökohtaisesti neuvoteltavissa, koska sisältö määräytyy tietosuoja-asetuksen mukaan
- Haasteita DPA:n käyttöönotossa:
  - Ei välttämättä mene läpi isojen toimijoiden kanssa
  - Kuinka saadaan pienet toimijat ymmärtämään tietosuoja-asetuksen asettamat velvollisuudet

5. SELVITÄ GDPR:N ASETTAMAT VAATIMUKSET TIETOJÄRJESTELMILLE

- Onko tietosuojan vaikutustenarviointi (PIA/DPIA) tarpeellinen?
- Onko rekisteröidyn oikeuksien toteutumiseen varauduttu, esim. tietopyynnöt ja tietojen siirrot?
  - Esim. vastaus tietopyyntöön annettava GDPR:n mukaan ilman aiheetonta viivytystä, mutta max. 1 kk sisällä. Huom. julkisuuslain mukaisiin tietopyyntöihin vastattava 14 pv. sisällä.
- 72 H Data Breach Notification
  - Huom.! Tietojen salaaminen tärkeää -> ei ilmoitusvelvollisuutta rekisteröidylle
- Tarkasta järjestelmän tietoturvavaatimukset (perustuttava riskiperustaiseen arvioon)
  - Riskiarvioon vaikuttavat
    - Käsiteltävien tietojen määrä
    - Käsiteltävien tietojen laatu (henkilötieto, arkaluonteinen henkilötieto, henkilötunnus)
    - Tietosuojaloukkausten vaikutukset
- Käytön valvonta: logimerkintä henkilötietojen käsittelystä (kuka teki ja mitä)

KYSYMYKSIÄ?

https://www.helsinki.fi/