Tietosuoja yhteishankkeissa

Jukka Tuomela, tietosuojavastaava

Olli Repo, lakimies

Anna Rytivaara, tietosuoja-asiantuntija

Esityksen sisältö

1. Tietosuoja tutkimuksessa
2. Tietosuojasta sopiminen yhteishankkeissa
   - Käsittelijöiden roolit ja vastuut
   - Sopimukset
     - Käsittelysopimus (DPA)
     - Yhteisrekisterinpitäjyyssopimus
     - Siirtosopimukset
3. Henkilötietojen siirrot ETA-alueen ulkopuolelle

Tietosuoja tutkimuksessa

Tietosuoja tutkimuksessa

- Tietosuojan tehtävä:
  - Osoittaa **milloin ja millä edellytyksillä** henkilötietoja voidaan käsitellä
- Olennaiset kysymykset (yksinkertaistetusti):
  - **Käsitelläänkö henkilötietoja?**
  - **Mihin tarkoitukseen henkilötietoja käsitellään?**
  - **Kuka henkilötietoja käsittelee?**

Tietosuoja yliopistossa

- Henkilötietojen suoja on jokaisen oikeus;
- Henkilötietojen suojan toteuttaminen on jokaisen yliopistoyhteisön jäsenen velvollisuus
- Käsittelyn vastuut, periaatteet ja toimintatavat vahvistettu yliopiston tietosuojapolitiikassa.
- Tutkimuksen tietosuojan perusohjeet ja -dokumentaatio julkisilla sivuilla
- Yhteystiedot:
  - intranet: https://intra.tuni.fi/handbook/2686/2725?
  - sähköposti: dpo@tuni.fi
  - yliopiston tietosuojatiimi:
    - tietosuojavastaava Jukka Tuomela
      - varalla lakimies Olli Repo ja Juha Malmivaara
    - tietosuoja-asiantuntija Anna Rytivaara

Tietosuojaan liittyvä keskeinen lainsäädäntö

- EU:n yleinen tietosuoja-asetus (GDPR)
  - suoraan sovellettavaa oikeutta kaikissa EU/ETA-maissa
  - joiltain osin sisältää kansallista liikkumavaraa
- Tietosuojalaki (1050/2018)
  - kansallisen liikkumavaran käyttö Suomessa
  - yleisen edun mukainen tehtävä määritelty
    - tieteellinen ja historiallinen tutkimus
    - arkistointi
- Laki viranomaisten toiminnan julkisuudesta (621/1999) ”Julkisuuslaki”
  - tietolupa, mahdollista saada myös salassa pidettäviin viranomaisten asiakirjoihin ja henkilörekistereihin
  - sosiaali- ja terveystietojen toisiokäyttö (oma laki)

Mihin tarkoitukseen henkilötietoja käsitellään?

- Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla; käsittely on lainmukaista ainoastaan, mikäli sillä on laissa säädetty käsittelyperuste.
- Käsittelyn tarkoitus määrittää pitkälti soveltuvan käsittelyperusteen; soveltuva käsittelyperuste määrittää pitkälti käsittelyyn liittyvät rekisteröidyn oikeudet:

- Yliopiston tutkimustoiminnassa käsittelytarkoitus pääsääntöisesti (yleisen edun mukainen) tieteellinen tutkimus; tarkoituksen täsmennys tutkimussuunnitelmassa, DMP:ssä..; kuvaus tietosuojailmoituksessa ja muussa informaatiodokumentaatiossa (suostumuslomake, tutkimustiedote).
- Ohjeeksi kysyjälle
  - Tutkimuksen tietosuojan julkinen sivu

Määritelmiä: henkilötietojen käsittely (GDPR, artikla 4)

- *Henkilötietojen käsittelyllä* tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten
    - tietojen keräämistä,
    - tallentamista ja säilyttämistä,
    - järjestämistä ja jäsentämistä,
    - muokkaamista tai muuttamista,
    - hakua, kyselyä,
    - käyttöä,
    - tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville,
    - tietojen yhteensovittamista tai yhdistämistä,
    - rajoittamista, poistamista tai tuhoamista

Tietosuojan perusdokumentaatio

- **Henkilötietojen käsittelyn suunnittelu:**
  - Ohje: Tutkimuksen tietosuojapolku
  - Ohje/asiakirjamalli: Tietosuojan tarkastuslista
  - Datapalvelu, tutkimuspalvelut omalta osaltaan (DMP:n kuvaukset, H2020 Ethics, tutkimussuunnitelma)
- **Käsittelyperiaatteiden toteuttaminen ja käsittelyyn liittyvien riskien arviointi**
  - Asiakirjamalli: Perusmuotoinen riskiarvio (Art. 32 käsittelyn turvallisuuden arviointi)
  - Asiakirjamalli: Tietosuojaa koskeva vaikutustenarviointi (”DPIA”, Art. 32 käsittelyn turvallisuuden arviointi ja Art. 35 tietosuojaa koskeva vaikutustenarviointi)
  - Ohje: Riskien arviointi
  - Ohje: Vaikutustenarviointi (DPIA), täyttöohje kirjattu lisäksi suoraan asiakirjamalliin
  - Ohje: Tietosuojaviranomaisen ennakkokuuleminen (Art. 36 ennakkokuulemismenettely)

Tietosuojan perusdokumentaatio (jatkuu)

- **Tutkittavan informointi**
  - Asiakirjamalli: Tieteellisen tutkimuksen tietosuojailmoitus (Art. 12—14 informointivelvoite)
  - Asiakirjamalli: Tutkimustiedote
  - Asiakirjamalli: Suostumuslomakemalli (tutkimuseettiset vaatimukset)
  - Asiakirjamalli: Käsittelytoimien seloste (Art. 30 dokumentointivelvoite, sisällytetty tutkimuksen tietosuojailmoitukseen päällekkäisen dokumentaation välttämiseksi)
  - Ohje: Tutkimuksen tietosuojailmoituksen täyttöohje
- **Henkilötietojen käsittelystä sopiminen**
  - Tietojenkäsittelysopimus (Art. 28 sopimisvelvoite käsittelytoimien ulkoistuksissa)
  - Yhteisrekisterinpitäjäsopimus (Art. 26 mukainen dokumentaatio tutkimusyhteistyötä varten)
- **Opinnäytetutkimus**
  - Asiakirjamalli Opinnäytetutkimuksen tietosuojailmoitus (Art. 12—14 informointivelvoite)
  - Ohje: Henkilötietojen käsittely opinnäytetutkimuksessa
  - Ohje: Henkilötietojen käsittely opinnäytetutkimuksen ohjaajalle

Tietosuojasta sopiminen yhteishankkeissa

Kuka henkilötietoja käsittelee?

- Onko hanketta suunnittelemassa yksi vai useampi taho? Mitkä osapuolten **käsittelyroolit** ovat? Kerätäänkö aineisto rekisteröidyltä vai saadaanko aineistoa muualta? Toteuttaako tutkimuksen tekijä kaikki käsittelytoimet itse, vai hankitaanko tutkimuksen toteuttamiseksi palveluita (ml. tukipalvelut kuten alustaratkaisut, litterointipalvelut..) muilta tahoilta?
- Ohjeeksi kysyjälle
  - Tutkimuksen tietosuojan julkiset sivut
- Tietovirtakaavion laatiminen ei ole pakollista
  - kuvaus osapuolista, osapuolten rooleista ja tiedon liikkeistä helpottaa kuitenkin huomattavasti sekä tutkijan että tukipalvelujen toimintaa

Tutkimuksen tietovirrat

Roolit: rekisterinpitäjä(t)

- Rekisterinpitäjä (controller):
  - taho, joka määrittelee käsittelyn tarkoituksen ja keinot (”omistaa tiedot”).
  - luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin
  - yliopiston hankkeissa ja hankinnoissa pääsääntöisesti yliopisto
- Yhteisrekisterinpitäjä (joint controllers):
  - vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot.
  - usein esimerkiksi kansallisissa tai kansainvälisissä konsortioissa tai yhteishankkeissa, jossa eri osapuolet päättävät yhdessä tutkimuksessa käsiteltävien henkilötietojen tarkoituksesta ja keinoista.
- ”Controllers in common”
  - vähintään kaksi rekisterinpitäjää käsittelee samaa henkilötietoaineistoa, mutta määrittää itsenäisesti käsittelyn tarkoitukset ja keinot.

Roolit: rekisterinpitäjän vastuu

- Rekisterinpitäjällä on kokonaisvastuu tietosuojalainsäädännön noudattamisesta
  - Rekisterinpitäjä vastaa henkilötietojen käsittelyn lainmukaisuudesta
    - Omassa toiminnassaan sekä
    - Käyttäessään ulkopuolisen palveluntarjoajan palveluja, myös niiden sitouttamisesta noudattamaan tietosuojalainsäädäntöä, **alikäsittelijätilanteet** huomioiden
  - Yliopisto rekisterinpitäjä/käsittelijänä vastaa
    - Oman henkilöstönsä kouluttamisesta ja ohjeistamisesta (GDPR art. 29)
    - Ulkopuolisten palveluntarjoajien ohjeistamisesta

Roolit: käsittelijä

- Käsittelee henkilötietoja rekisterinpitäjän puolesta ja lukuun
  - Osatutkimus palveluhankintana
  - Internet-pohjaiset säilytysalustat
  - Kysely- ja analysointipalvelut
  - Muut tukipalvelut, kuten litterointi, käännöspalvelut
  - Yliopiston ulkopuoliset tutkijat, opinnäytetöiden tekijät
- Oikeushenkilöiden lisäksi myös esim. luonnollinen henkilö, virasto…
- Yliopiston hankkeissa ja hankinnoissa pääsääntöisesti toimittaja/palveluntarjoaja

Milloin sovitaan?

- ”Jos käsittely on määrä suorittaa rekisterinpitäjän lukuun”
  - Kun käytetään henkilötietojen käsittelijöitä (”alihankkijoita”), suoraan EU:n yleiseen tietosuoja-asetukseen (28 artikla) perustuva velvollisuus määrittää henkilötietojen käsittelyä
    - => Kirjallinen **käsittelysopimus** pakko tehdä
- ”Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot"
  - Mikäli kyse on **yhteisrekisteristä** (Art. 26; useampi rekisterinpitäjä määrittää yhdessä käsittelyn tarkoitukset ja keinot), keskinäiset vastuualueet on määriteltävä “keskinäisellä järjestelyllä”
    - → Yhteisrekisterinpitäjyyssopimus, yhdistetty tietosuojailmoitus vai muu tapa?
- Huom. usein erillistä sopimista edellyttävät mm.
  - Datan luovutukset
  - Käyttöoikeuksien myöntäminen
  - Arkistointi

Sopimustyypit

- Käsittelysopimus (**Data Processing Agreement**, DPA)
  - Käsittelyn ”ulkoistus” rekisterinpitäjä → rekisterinpitäjä
- Yhteisrekisterinpitäjäsopimus (**Joint Controller Agreement**) JCA
  - Yhteiskäsittely rekisterinpitäjä & rekisterinpitäjä
- Siirtosopimukset (**Data**/Material **Transfer Agreement**)
  - Datan luovutus rekisterinpitäjä → rekisterinpitäjä

→ Jos hankkeeseen osallistuvien tahojen roolit ja vastuut ovat selvät (tutkimussuunnitelma, DMP), sopimusten laatimisessa on kyse enää sovittujen toimintatapojen dokumentoinnista

- Huom. tukipalveluilla on tukirooli; tässäkin suunnittelu ja riittävät taustatiedot ovat olennaisia

Käsittelysopimukset (Data Processing Agreement, DPA)

Käsittelysopimus (28 artikla)

3. Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella tai muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Tässä sopimuksessa tai muussa oikeudellisessa asiakirjassa on säädettävä erityisesti, että henkilötietojen käsittelijä

a) käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti, mikä koskee myös henkilötietojen siirtoja kolmanteen maahan tai kansainväliselle järjestölle, paitsi jos henkilötietojen käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaaditaan, missä tapauksessa henkilötietojen käsittelijä tiedottaa rekisterinpitäjälle tästä oikeudellisesta vaatimuksesta ennen käsittelyä, paitsi jos tällainen tiedottaminen kielletään kyseisessä laissa yleistä etua koskevien tärkeiden syiden vuoksi;

b) varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus;

c) toteuttaa kaikki 32 artiklassa vaaditut toimenpiteet;

d) noudattaa 2 ja 4 kohdassa tarkoitettuja toisen henkilötietojen käsittelijän käytön edellytyksiä;

e) ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat III luvussa säädettyjen rekisteröidyn oikeuksien käyttämistä;

f) auttaa rekisterinpitäjää varmistamaan, että 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonteen ja henkilötietojen käsittelijän saatavilla olevat tiedot;

g) rekisterinpitäjän valinnan mukaan poistaa tai palauttaa käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, paitsi jos unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään henkilötiedot;

h) saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen tässä artiklassa säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja sallii rekisterinpitäjän tai muun rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit, kuten tarkastukset, sekä osallistuu niihin.

Ensimmäisen alakohdan h alakohdan osalta henkilötietojen käsittelijän on välittömästi ilmoitettava rekisterinpitäjälle, jos hän katsoo, että ohjeistus rikkoo tätä asetusta tai muita unionin tai jäsenvaltion tietosuojasäännöksiä.

Käsittelysopimus (28 artikla)

- Take-awayt:
  - Käsittelyä ”on määritettävä” sopimuksella tai muulla asiakirjalla
  - ”Vahvistettava”:
    - Käsittelyn kohde ja kesto
    - käsittelyn luonne ja tarkoitus
    - henkilötietojen tyyppi ja rekisteröityjen ryhmät
    - Rekisterinpitäjän oikeudet ja velvollisuudet
  - ”Säädettävä erityisesti”:
    - dokumentoidut ohjeet
    - salassapito
    - 32 artiklan mukaiset tietoturvaseikat
    - alikäsittelijöiden rooli
    - avustamisvelvollisuus
    - vaikutustenarviointi, ennakkokuuleminen
    - Tietoturvaloukkauksiin reagoiminen
    - auditointi
    - yleinen tiedonantovelvollisuus (ml. tieto virheellisestä ohjeistuksesta)
    - toiminta käsittelyn päätyttyä

Käsittelysopimus (28 artikla)

- Käytännössä:
  1. Tietojenkäsittelysopimus (DPA)
     - => Sopimisvelvoite, kohde, osapuolten vastuut
  2. Rekisterinpitäjän dokumentoitu ohjeistus
     - => tietoturva- ja tietosuojavaatimukset
       - hankinnoissa ns. (”tt-excel”) ja toiminnalliset vaatimukset
       - tutkimuksessa käytännössä vapaamuotoinen kuvaus, yleensä sopimustekstissä tai sopimuksen liitteenä, tutkimusyhteistyössä myös tutkimussuunnitelmassa
       - Huom. ”sitoutuu käsittelemään tietosuoja-asetuksen mukaisesti” ei pelasta.

Käsittelysopimus (28 artikla)

- Yliopiston käsittelysopimuksen mallipohja
  - Lähtökohtaisesti täytettävä mallipohjan ”keltaiset kohdat”, eli
    - Käsittelyn kohde
    - Käsittelyn laatu ja tarkoitus
    - Käsittelyn kohteena olevat rekisteröityjen ryhmät ja henkilötietotyypit
    - Substanssiosaaja täyttää → täyttäminen ei ole hankintahenkilöstön ja/tai lakipalveluiden tehtävä
  - Sopimusmallista riippuen kuvaus voidaan tehdä myös erillisellä liitteellä

Käsittelysopimus (28 artikla)

- Yleiset kipukohdat (selvä teema – raha ratkaisee):
  - Kuluvastuut
    - avustamisvelvollisuus,
    - käsittelyohjeistuksen päivitys,
    - auditoinnin kulut
  - Vahingonkorvausvastuu
    - Art. 82?
    - JIT/JYSE vakioratkaisu
    - Vaikka vastuunrajoituksesta olisi sovittu, salassapito-exclusion?
- Arviointi läht.koht. lakipalveluiden yleisen sopimuspolitiikan mukaisesti
- Poikkeaminen vakioehdoista = vastuuyksikön liiketoimintapäätös
  - Tietosuojatiimi (tai lakipalvelut, hankinnat..) ei ”kuittaa ok:ksi”

Yhteisrekisterinpitäjäsopimukset (Joint Controller Agreement, JCA)

Yhteisrekisterinpitäjyyssopimus (26 artikla)

26 artikla

Yhteisrekisterinpitäjät

1. Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Ne määrittelevät keskinäisellä järjestelyllä läpinäkyvällä tavalla kunkin vastuualueen tässä asetuksessa vahvistettujen velvoitteiden noudattamiseksi, erityisesti rekisteröityjen oikeuksien käytön ja 13 ja 14 artiklan mukaisten tietojen toimittamista koskevien tehtäviensä osalta, paitsi jos ja siltä osin kuin rekisterinpitäjiin sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä määritellään rekisterinpitäjien vastuualueet. Järjestelyn yhteydessä voidaan nimetä rekisteröidyille yhteyspiste.

2. Edellä 1 kohdassa tarkoitetusta järjestelystä on käytävä asianmukaisesti ilmi yhteisten rekisterinpitäjien todelliset roolit ja suhteet rekisteröityihin nähden. Järjestelyn keskeisten osien on oltava rekisteröidyn saatavilla.

3. Riippumatta 1 kohdassa tarkoitetun järjestelyn ehdoista rekisteröity voi käyttää tämän asetuksen mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään ja kutakin rekisterinpitäjää vastaan.

Yhteisrekisterinpitäjyyssopimus (26 artikla)

- Take-awayt:
  - Vastuualueet ”määritetään keskinäisellä järjestelyllä läpinäkyvällä tavalla”, erityisesti:
    - rekisteröityjen oikeuksien käyttö,
    - 13 ja artikla 14 mukaisten tietojen toimittaminen,
    - Järjestelyn yhteydessä voidaan nimetä rekisteröidyille yhteyspiste.
  - Muuta:
    - kohde, kesto, tarkoitus, henkilötietojen tyypit, rekisteröityjen ryhmät..
    - kustannustenjako (mahd. hankittavat yhteisjärjestelmät, henkilöstökulut..)
    - erit. tutkimushankkeissa:
      - riskiarvio -> DPIA -> ennakkokuulemismenettely (kuka hoitaa)
      - tietoturva (in transfer, at rest..)
      - toiminta käsittelyn päättyessä
    - tiedonantovelvollisuudet (erit. tietoturvaloukkaukset)
    - vahingonkorvausvastuut (art. 82)? Huom. rekisteröity voi kohdistaa vaatimuksensa kumpaan tahansa.
  - Järjestelyn keskeisten osien on oltava rekisteröidyn saatavilla.
    - Sopimus rekisteröidylle tiedoksi?
    - => Normaali lähtökohta on kirjata ”keskeiset osat” tietosuojailmoitukseen.

Yhteisrekisterinpitäjyyssopimus (26 artikla)

- Yliopiston vakiomuotoinen yhteisrekisterinpitäjäsopimus (FI + EN):
  - https://www.tuni.fi/tutkimuksen-tietosuoja
  - Käytössä mm. Oululla (DIPP-yhteisrekisteri)
  - Sovellettu pilottimielessä useammassa hankkeessa
- Hankekohtaisesti täydennettävä:
  - Kuvaus hankkeen (käsittelyn) tarkoituksesta ja tavoitteista (yleisellä tasolla)
  - Kuvaus henkilötietojen käsittelyn luonteesta ja laajuudesta (tai viittaus tietosuojailmoitukseen)
  - Roolit i) vaikutustenarvioinnissa, ii) informointivelvoitteen toteuttamisessa ja iii) rekisteröidyn oikeuksien käyttämisessä; joko koordinaattorin nimeäminen tai kukin omalta osaltaan; avustamisvelvollisuus
  - Tietoturvatoimenpiteet keräämisessä, säilytyksessä ja siirtämisessä
  - Aineiston käsittely hankkeen päättymisen jälkeen

Yhteisrekisterinpitäjyyssopimus (26 artikla)

- Yleiset kipukohdat:
  - Neuvottelutarvetta ei pääsääntöisesti ole
    - Dokumentoidaan suunnitteluvaiheessa sovittu roolitus
  - Olennaista tiedon käsittelyn kuvaus (tutkija täyttää, datapalvelu/dpo avustaa)
  - Vastuuehdoissa lähtökohta Art. 82: vastuu rekisteröidylle määräytyy kunkin oman toiminnan/laiminlyönnin mukaan; regressioikeus täysimääräinen
    - Huom. 82(4) yhteisvastuu -> jos mahdollista, pyritään purkamaan sopimustasolla
  - Jos hankkeeseen liittyy hankintoja, mahd. valtuutus (yhteishankinnat) tai vastuutus

Yhteisrekisterinpitäjyyssopimus (26 artikla)

- Huom. ei varsinaista sopimispakkoa (vrt. käsittelijätilanteet)
  - Mahdollista on laatia esimerkiksi yhteinen (hyvin laadittu) tietosuojailmoitus, josta roolit ja vastuut ilmenevät
  - Yhteisrekisterinpitäjätilanteiden kannalta relevanttien seikkojen (mm. tekniset suojatoimenpiteet, vastuuasiat, avustamisvelvollisuus..) kirjaaminen kattavasti tietosuojailmoitukseen (sisällön ymmärrettävyys, huom.) on haastavaa -> puoltaa erillisen sopimuksen laatimista

Siirtosopimukset (Data/Material Transfer Agreement)

Siirtosopimukset

- Datansiirtosopimus (DTA) koskee nimensä mukaisesti **dataa** (spss-aineistoa, tietokantoja, exceleitä yms.)
- Materiaalinsiirtosopimus (MTA) taas materiaalia (eli yleensä **näytteitä** kuten solunäytteitä tms).

Siirtosopimukset

- Tietosuojan puolesta huomioitava:
  - **Luovutus on <u>käsittelytoimi</u>**
    - Tarkoitus, käsittelyperuste, tietosuojaperiaatteet huomioitava
  - Kuka luovuttaa kenelle ja mihin tarkoitukseen
    - **Luovuttajalla oltava oikeus luovutukseen**
      - Rekisteröidyn informointi - miten jatkokäyttö huomioitu
      - Käyttötarkoitussidonnaisuus; huom. kuitenkin tutkimuspoikkeus
        - myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota artikla 89 1 kohdan mukaisesti yhteensopimattomaksi alkuperäisten tarkoitusten kanssa
    - **Vastaanottajalla oltava oikeus käsittelyyn**
    - Mahdolliset suojatoimet
      - anonymisointi/pseudonymisointi (anonymisointi siirron edellytys?)
      - laskee riskitasoa molemmilla puolilla

Siirtosopimukset

- Jos kyse on rekisterinpitäjä—rekisterinpitäjä-siirrosta, onko osapuolten vastuista ylipäätään tarve sopia?
  - Kumpikin vastaa rekisterinpitäjänä käsittelystä omalta osaltaan
  - Tietosuojan puolesta siirron/luovutuksen dokumentointi olennaista
- Usein datansiirtosopimus (siirretään esim. spss-aineistoa, tietokantoja, exceleitä) sisältää kuitenkin materiaalinsiirtosopimuksen (siirretään tutkimusmateriaalia, esim. näytteitä) tapaan käyttörajoituksia, ehtoja julkaisuista/viittauksista, ”no warranties” ehtoja.
  - Arviointi lakipalveluiden yleisen sopimuspolitiikan mukaan

Henkilötietojen siirto ETA:n ulkopuolelle

Henkilötietojen siirto ETA:n ulkopuolelle

- Tiedonsiirrot Euroopan talousalueen (ETA) ulkopuolelle
  - Henkilötietojen siirto ETA:n ulkopuolelle edellyttää aina tietosuoja-asetuksessa säädettyjen suojatoimien (**V luku**) noudattamista:

44 artikla

Siirtoja koskeva yleinen periaate

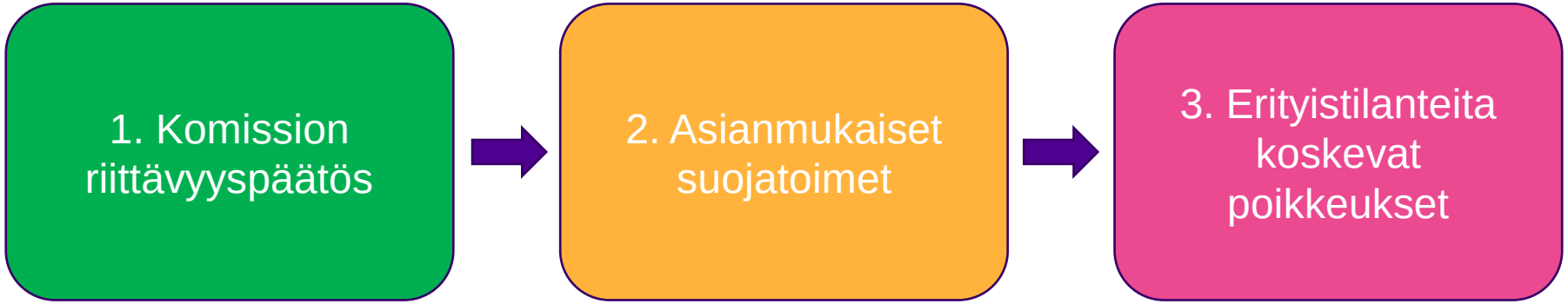
Sellaisten henkilötietojen siirto, joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen, toteutetaan vain jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat tässä luvussa vahvistettuja edellytyksiä ja ellei tämän asetuksen muista säännöksistä muuta johdu; tämä koskee myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle. Kaikkia tämän luvun säännöksiä on sovellettava, jotta varmistetaan, että tällä asetuksella taattua luonnollisten henkilöiden henkilötietojen suojan tasoa ei vaaranneta.

  - esim. henkilötietoaineiston siirto ETA-alueen ulkopuolella toimivalle koordinaattorille tai rahoittajalle (huom. myös pääsy = siirtoa); myös esim. ETA:n ulkopuolella toimivan käsittelijän käyttäminen: pilvipohjaiset säilytyspalvelut, tutkimustietojärjestelmät, myös ”aurinkoa seuraava” asiakaspalvelu, jos pääsy henkilötietoihin

Henkilötietojen siirto ETA:n ulkopuolelle

- Yksinkertaistetusti:
  - Käsittelyn oltava lainmukaista EU-alueella ja
  - Henkilötietojen siirron perustana V luvun siirtomekanismi

- Siirtomekanismien etusijajärjestys



Henkilötietojen siirto ETA:n ulkopuolelle

- Sovellettavat suojatoimet
  - i) Siirto **tietosuojan riittävyyttä koskevan päätöksen perusteella** (Art. 45)
    - Euroopan komission tietosuojan tason riittävyyttä koskevat päätökset
      - ns. ”adequacy decisions”
      - tällä hetkellä mm. Japani, Israel, Kanada (tietyin rajoituksin); Iso-Britannia valmisteilla
      - => voidaan kohdella kuten EU-siirtoja
      - Yhdysvallat olleet mukana ns. ”**Privacy Shield**” -järjestelmällä
  - ii) Siirto **”asianmukaisia suojatoimia” soveltaen** (Art. 46), jos päätöstä ei ole
    - Käytännössä yliopistolla sovellettu ns. ”mallisopimuslausekkeita”
      - Vakiomuotoinen sopimuskokonaisuus, johon ei saa tehdä muutoksia -> helpohko soveltaa
  - iii) Erityistilanteita koskevat poikkeukset (Art. 49)
    - Esim. nimenomainen suostumus, kun riskeistä on kerrottu rekisteröidylle
      - Huom. kyse kuitenkin *poikkeuksesta* -> suostumusta ei pitäisi käyttää toistuvaan tai laajamittaiseen tiedon siirtoon

Henkilötietojen siirto ETA:n ulkopuolelle

- Käytännössä:
  - **Virtuaalityöpöydän käyttö**, mikäli mahdollista
    - Ennakkotieto: KPMG auditoimassa TAU:n virtuaalityöpöydän → toisiolain (552/2019) mukainen tietoturvallinen käsittely-ympäristö
  - Muussa tapauksessa:
    - **Pseudonymisoi** (avain vain TAU:lla, **ei** palveluntarjoajalla tai vastaanottajalla)
    - **Salaa** (salattu säilytys ja lähetys, ohjeistus tai tietoturva@tuni.fi)
    - **Varmista** (tarvittaessa vastaanottajalta, ml. palveluntarjoaja, selvitys käytännöistä)
- Tutkimuksen osalta US-tilanne jossain määrin helpompi (tutkimusorganisaatiot eivät vastaavalla tavalla FISE 702 ja EO 12.333 alaisia)

Kiitos.
Kysymyksiä, kommentteja?