Tampereen yliopisto
Tampere University

Tutkimuksen suppea riskiarvio

Ohje
Tampereen yliopisto
Tietosuojavastaava dpo@tuni.fi
Helmikuu 2021

Tietosuojariskien arviointi

- Riskienarviointiprosessi etenee vaiheittain:
  i. Suppea riskiarvio
  ii. Tietosuojavaikutusten arviointi (DPIA)
  iii. Valvontaviranomaisen ennakkokuuleminen
- i) **Suppea tietosuojariskien arviointi** tehdään aina ennen kuin henkilötietoja ryhdytään käsittelemään.
- ii) Mikäli suppea tietosuojariskien arviointi osoittaa, että tutkimuksen yhteydessä suoritettava henkilötietojen käsittely aiheuttaa korkean riskin rekisteröidylle, tulee henkilötietojen käsittelyn osalta tehdä lisäksi **tietosuojavaikutusten arviointi (DPIA)**.
- Iii) Mikäli rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi, DPIA:n jälkeen lisäksi toteutettava valvontaviranomaisen **ennakkokuuleminen**.

Suppea riskiarvio

- Tavoite on tunnistaa jo suunnitteluvaiheessa:
  - **riskit,** joita henkilötietojen käsittely voi tutkittavalle aiheuttaa sekä
  - **toimenpiteet,** joihin asianmukaisen käsittelyn turvaamiseksi on ryhdyttävä
- Riskiarvio tehdään ennen henkilötietojen käsittelyn aloittamista
- Riskejä arvioidaan käsittelytoimittain ja rekisteröidyn näkökulmasta
  - Ei siis varsinaisesti tutkimushankkeen, organisaation tai tutkijan itsensä näkökulmasta
- Riskiarvio on dokumentoitava. Riskiarviossa arvioidaan ja kirjataan:
  - Mitä tutkittavan vapauksia tai oikeuksia henkilötietojen käsittely voi vaarantaa?
  - Mitä vahinkoja tutkittavalle voi aiheutua suunnitellusta henkilötietojen käsittelystä?
  - Millä toimenpiteillä tutkittavalle aiheutuva riski poistetaan tai sitä pienennetään?

Määritelmiä: henkilötieto (GDPR, artiklat 4, 9-10)

- *Henkilötiedoilla* tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', 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
- *Erityiset henkilötietoryhmät* ovat tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista
  - Myös: Rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyvät henkilötiedot

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,
    - 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

Tampereen yliopisto
Tampere University

Seuraavat kalvot mukailevat Tampereen yliopiston suppean riskiarvion mallipohjaa.

Suppean riskien arvioinnin ulottuvuudet

- Arvioi kunkin käsittelytoimen osalta:
  - Käsittelyyn liittyvä **riski**
  - Riskin **todennäköisyys** (epätodennäköinen, mahdollinen, todennäköinen, lähes varma)
  - Riskin **vakavuus** (vakava, tunnistettuja vaikutuksia, vähäisiä vaikutuksia)
  - **Toimenpide** riskin vähentämiseksi
  - **Jäännösriski**. Jäännösriskillä tarkoitetaan tutkittavalle aiheutuvaa riskiä sen jälkeen, kun suojatoimenpiteet on toteutettu (matala, keskimääräinen, korkea)
- Arvioi riskejä ja seurauksia **rekisteröidyn eli tutkittavan näkökulmasta.**

Suppean riskien arvioinnin ulottuvuudet

Loukkauksen tai haitan vakavuus	Vakava	Matala riski	Korkea riski	Korkea riski
	Tunnistettuja vaikutuksia	Matala riski	Keskimääräinen riski	Korkea riski
	Vähäisiä vaikutuksia	Matala riski	Matala riski	Matala riski
		Kaukainen	Mahdollinen	Hyvin mahdollinen
		Loukkauksen tai haitan todennäköisyys		

Riskit

- Vahinkoa voi aiheutua erityisesti siitä, että henkilötietoja *katoaa, häviää, tai niihin saa pääsyn taho, jolla ei ole oikeutta käsitellä tutkittavan henkilötietoja*.
- Mahdolliset vahingot voivat olla muun muassa **taloudellisia** (kuten petoksen tai identiteettivarkauden kohteeksi joutuminen tietovuodon vuoksi), **fyysisiä** (kuten väkivalta tai sen uhka) tai **aineettomia** (kuten maineen tai yksityisyyden suojan menetys).
- Riski on sitä suurempi, mitä vakavampi seuraus on yksilön kannalta ja mitä todennäköisempää seurauksen toteutuminen on:
    - **riski = seurauksen vakavuus x seurauksen todennäköisyys**

Tietosuojariskien tunnistaminen

- Millaisia riskejä henkilötietojen käsittelyyn liittyy tutkimuksesi eri vaiheissa? Henkilötietojen käsittelyllä tarkoitetaan kaikkia henkilötietoaineistolle sen käsittelyn elinkaaren aikana tehtäviä toimenpiteitä, kuten *tietojen keräämistä, tallentamista, analysointia, säilyttämistä, luovuttamista, arkistointia, poistamista tai tuhoamista*.
- Arvioi riskejä ja seurauksia **rekisteröidyn eli tutkittavan näkökulmasta.**
- Voit miettiä esimerkiksi
  - Millaisia käsittelytoimia tutkimukseesi sisältyy?
  - Ketkä käsittelevät tietoja tutkimuksen eri vaiheissa?
  - Missä henkilötietoja säilytetään ja missä muodossa?
  - Miten ja minne henkilötietoja siirretään tutkimuksen eri vaiheissa?
  - Kuinka laajasti henkilötietoja käsitellään, yhdistelläänkö eri henkilötietoja keskenään ja käsitelläänkö erityisiä henkilötietoryhmiä?

  → Millaisia riskejä nämä käsittelytoimet aiheuttavat?

Toimenpiteet riskin rajoittamiseksi

- Rekisterinpitäjän on toteutettava on toteutettava ”riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet”.
- Huom. tietosuojaperiaatteiden noudattaminen oletusarvo
- Riskiä voidaan rajoittaa erilaisilla hallinnollisilla ja teknisillä toimenpiteillä, kuten
  - henkilötietojen pseudonymisoinnilla
  - käsittelyyn oikeutetun henkilöpiirin tarkalla määrittelyllä,
  - käyttöoikeuksien tarkalla määrittelyllä
  - tietojen salaamisella säilytyksessä
    - esim. käyttäjätunnus—salasana-yhdistelmä, salattu kovalevy, tiedostojen salaus
  - tietojen salaamisella siirrossa:
    - esim. pääsy tietoturvalliseen käsittely-ympäristöön, sähköpostin ja sen liitteiden salaaminen
- Riskiarvioissa arvioidaan lähtökohtaisesti jäännösriski eli riski, joka jää jäljelle, kun suojatoimenpiteet on suoritettu.
- Lisätietoja: Tietoturvan intranet-sivut

Riskiarvion dokumentointi

- Suppea riskiarvio on **dokumentoitava**
- Suppean riskiarvion voi laatia vapaamuotoisesti ja kirjata esimerkiksi aineistonhallintasuunnitelman, tutkimussuunnitelman, rahoitushakemuksen tai eettisen toimikunnan lupahakemuksen yhteyteen.
- Riskiarviossa voit hyödyntää myös Tampereen yliopiston **riskiarviolomaketta,** joka liitetään projektidokumentaatioon.
- Riskiarvion mallipohja on tutkimuksen tietosuojan sivuilla: https://www.tuni.fi/tutkimuksen-tietosuoja

Käytännön esimerkkejä

- Seuraavissa kalvoissa esitellään esimerkkejä erilaisista tutkimuksista
- Esimerkeissä nostetaan esille seikkoja, jotka voivat aiheuttaa riskin rekisteröidylle
- Esimerkit eivät ole kattavia, vaan niiden tarkoitus on kiinnittää huomiota riskeihin, joita rekisteröidyn oikeuksille ja vapauksille voi aiheutua.

Esimerkkitapaus 1

Tutkija haastattelee tutkimuksessaan 20 ammatillisen koulutuksen opettajaa heidän urapoluistaan. Tutkija tallentaa aineiston omalle henkilökohtaiselle tietokoneelleen ja lähettää haastattelut litteroitavaksi ulkopuoliselle palveluntarjoajalle.

- Riskiarvioinnissa huomioitavia seikkoja:
  - Mitä aiheita haastatteluissa käsitellään? Voiko haastateltavalle koitua haittaa, jos aineisto joutuu vahingossa esimerkiksi hänen työnantajansa käsiin?
  - Siirtoihin liittyvät riskit: Miten aineisto siirretään ulkopuoliselle palveluntarjoajalle ja minne palveluntarjoaja tallentaa aineiston?
  - Toimenpiteitä riskin pienentämiseksi: aineiston pseudonymisointi, tallentaminen yliopiston suosittelemaan tallennuspaikkaan, aineiston suojaus salasanalla ja tallentaminen salattuna, siirtäminen salatulla yhteydellä

Esimerkkitapaus 2

Kansanedustajien perhesuhteita koskeva aineisto koostuu aikakauslehdissä julkaistuista haastatteluista (n=25). Henkilötietoja käsittelee vain väitöskirjatutkija ja hänen ohjaajansa.

- Riskiarvioinnissa huomioitavia seikkoja:
  - Aineisto sisältää erityisiä henkilötietoryhmiä (poliittisia mielipiteitä), jotka rekisteröity on itse saattanut julkiseksi.
  - Aineisto sisältää myös perheenjäsenten henkilötietoja.
  - Toimenpiteitä riskin pienentämiseksi: tallennus- ja siirtotapojen huolellinen suunnittelu

Esimerkkitapaus 3

Tutkimusprojektissa kerätään seksuaalivähemmistöjen terveystietoja viidestä eri maasta ja kolmesta maanosasta. Terveystietoja yhdistellään osallistujien koulutustietoihin kolme sukupolvea taaksepäin. Aineistossa on yhteensä 2500 osallistujaa, minkä lisäksi aineistoon kuuluu heidän sukulaistensa henkilötietoja (koulutustiedot). Aineisto tallennetaan yhteiselle alustalle, ja tutkijat tallentavat sitä sekä työkoneille että omille henkilökohtaisille koneilleen analyysiä varten.

- Riskiarvioinnissa huomioitavia seikkoja:
  - Erityisten henkilötietoryhmien käsittely (seksuaalista suuntautumista koskevat tiedot, terveystiedot)
  - Aineiston tallentaminen ja jakaminen tutkimusryhmille?
  - Mahdolliset siirrot ETA-maiden ulkopuolelle?
  - Aineiston tallentaminen tutkijoiden omille koneille?
  - Toimenpiteitä riskin pienentämiseksi: tallennus- ja siirtotapojen huolellinen suunnittelu, tutkijoiden informointi aineiston käsittelystä

Esimerkkitapaus 4

- *Tutkimusprojektissa kerätään 385000 henkilön verinäytteet, joista analysoidaan henkilöiden genomitietoja. Verinäytteisiin yhdistetään tietoja rekisteröityjen elintavoista, koulutuksesta, verotettavista tuloista sekä edeltävien sukupolvien asuinpaikoista.*
- Riskiarvioinnissa huomioitavia seikkoja:
    - Tutkimuksessa käsitellään laajasti ja yhdistellen arkaluontoisia tietoja, joiden paljastuminen voisi aiheuttaa tutkittaville suurta taloudellista vahinkoa.

Esimerkkitapaus 5

- *Kansainvälisessä rokotetutkimuksessa kerätään yhteensä 40000 henkilön terveystietoja. Tutkimuksen alussa osallistujat täyttävät yksityiskohtaisen kyselyn, jossa kysytään yksityiskohtaisesti demografisia tietoja (mm. maa, sukupuoli, ikä, etninen ryhmä) sekä terveystietoja. Rokotteen antamisen jälkeen osallistujat täyttävät sähköistä oirepäiväkirjaa kaksi kuukautta. Tutkimuksen aikana osallistujilta otetaan kaksi verinäytettä, minkä lisäksi osallistujat itse ottavat itseltään viikoittain nenänäytteen, joka lähetetään tutkijoille. Lisäksi aineistoon yhdistetään rekisteritietoja osallistujien terveydestä. Aineistoa analysoidaan neljässä eri maassa.*
- Riskiarvioinnissa huomioitavia seikkoja:
  - Projektissa kerätään erittäin laajasti erityisiä henkilötietoja (terveystiedot, etninen ryhmä) sekä suoraan tutkittavalta että yhdistelemällä tietoja rekisteritietoihin.
  - Millaisia riskejä rekisteröidylle voi aiheutua, jos hänen tietonsa päätyvät tutkimusryhmän ulkopuolelle?
  - Tietoja tallennetaan paperilla (alkukysely, suostumuslomake) ja sähköisesti (alkukyselyn tallentaminen sähköiseen muotoon, oirekysely).
  - Toimenpiteitä riskin pienentämiseksi: tallennus-, jakamis- ja siirtotapojen huolellinen suunnittelu, tutkijoiden informointi aineiston käsittelystä

Esimerkkitapaus 6

- *Pitkittäistutkimuksessa seurataan saamelaislasten (30 perhettä) elämää kahdessa Suomen kunnassa, joissa on merkittävä saamelaisväestö. Lasten elämää tallennetaan videoimalla heitä päiväkodeissa, koulussa ja vapaa-ajalla. Aineisto sisältää sekä lasten että heidän opettajiensa ja vanhempiensa haastatteluita sekä asiakirja-aineistoja mm. heidän arvosanoistaan.*
- Riskiarvioinnissa huomioitavia seikkoja:
  - Erityisten henkilötietoryhmien käsittely (etnistä vähemmistöä koskevat tiedot, 30 perhettä isohko otos suhteessa ko. etniseen ryhmään)
  - Aineistojen turvallinen tallentaminen pitkittäistutkimuksen aikana?
  - Toimenpiteitä riskin pienentämiseksi: tallennus- ja siirtotapojen huolellinen suunnittelu, tutkijoiden informointi aineiston käsittelystä

Suppeasta riskiarviosta tietosuojariskien vaikutusten arviointiin (DPIA)

- Milloin vaikutusten arviointi on tehtävä?
    1. Suppea riskiarvion perusteella henkilötietojen käsittely aiheuttaa korkean riskin rekisteröidylle
    2. Tietosuoja-asetuksessa yksilöityjen käsittelytilanteiden johdosta
    3. Käsittelytoimenpide on lisätty tietosuojaviranomaisen luetteloon
    4. Kansallinen lainsäädäntö edellyttää tietosuojavaikutusten arviointia
- Kattava kuvaus: https://tietosuoja.fi/vaikutustenarviointi
- Hyvin tehty suppea tietosuojariskien arviointi nopeuttaa vaikutusten arvioinnin laatimista
- DPIA:n mallipohja on tutkimuksen tietosuojan sivuilla: https://www.tuni.fi/tutkimuksen-tietosuoja

Muu tietosuojadokumentaatio

Muista myös muu tietosuojadokumentaatio:

- Tietosuojailmoitus
- Vaikutustenarvio (tehtävä, jos riskiarvion mukaan korkea riski rekisteröidyille)
- Käsittelysopimukset (jos henkilötietoja käsitellään esim. tutkimusryhmän ulkopuolella)
- Yhteisrekisterinpitäjyyssopimus (jos useita rekisterinpitäjiä)

Kysyttävää?

Ota yhteyttä: researchdata@tuni.fi