

Tietosuojaa koskeva vaikutustenarviointi (DPIA)

**Tietosuojavaikutusten arvioinnin käsittelyvaiheet:**

|  |  |  |
| --- | --- | --- |
| Vaihe | Päivämäärä | Nimi |
| Luonnos laadittu | Syötä päivämäärä | Nimi |
| Tietosuojavastaavaa kuultu | Syötä päivämäärä | Nimi |
| Vaikutustenarviointi valmis | Syötä päivämäärä | Nimi |

Tutkimuksen nimi:

Tutkittavien lukumäärä: Tutkittavien lukumäärä (arvio)

Tutkimuksen suunniteltu kestoaika: alkaa pvm.— päättyy pvm.

Tutkimuksen vastuullinen johtaja: Vastuullinen johtaja

Yhteystiedot: Vastuullisen johtajan yhteystiedot

Tutkimusryhmä: Tutkimusryhmä tai tutkimusala

# Henkilötietojen käsittelyn yleiskuvaus

**Käsiteltävät henkilötietotyypit ja henkilötietojen lähteet**

Kuvaa, mitä henkilötietoja käsitellään, kenen henkilötietoja käsitellään (rekisteröityjen ryhmät), keneltä tai mistä henkilötiedot saadaan (henkilötietojen lähde) ja mihin tarkoituksiin henkilötietoja käsitellään (käyttötarkoitus) sekä kuhunkin käyttötarkoitukseen sovellettava käsittelyn oikeusperuste (käsittelyn lainmukaisuus).

Mitä henkilötietoja tutkimuksessa käsitellään?

|  |
| --- |
| Rekisteröidyltä eli tutkittavalta itseltään kerättävät henkilötiedot: |
|  |

|  |
| --- |
| Muista lähteistä kerättävät henkilötiedot: |
|  |

**Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely**

Erityisiin henkilötietoryhmiin kuuluvia ovat tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys, sekä geneettiset tai biometriset tiedot, joita käsitellään henkilön yksiselitteistä tunnistamista varten, tai terveyttä koskevat tiedot, taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot. Käsitelläänkö tutkimuksessa erityisiin henkilötietoryhmiin (arkaluontoisiin henkilötietoihin) kuuluvia tietoja tai rikostuomioita tai rikkomuksia koskevia tietoja?

|  |
| --- |
| Erityisiä henkilötietoryhmät tai rikostuomioita tai rikkomuksia koskevat tiedot: |
|  |

**Henkilötietojen käsittelyn toiminnallinen kuvaus**

Laadi kuvaus henkilötietojen käsittelyn luonteesta, laajuudesta, asiayhteydestä ja tarkoituksista. Huomioi henkilötietojen käsittelyn koko elinkaari henkilötietojen keräämisestä tietojen tuhoamiseen tai arkistointiin asti.

Kuvauksen tulisi sisältää tiedot siitä, miksi ja miten henkilötietoja on tarkoitus käsitellä. Kuvaa erityisesti, miten henkilötiedot kerätään, mihin henkilötietoaineistot tallennetaan, mitä tahoja henkilötietojen käsittelyyn osallistuu ja mikä kunkin tahon rooli ja vastuut ovat, miten aineistoa jaetaan mahdollisten muiden käsittelyyn osallistuvien tahojen kanssa ja mitä aineistolle tehdään tutkimushankkeen päätyttyä. Mikäli henkilötietojen käsittelystä on laadittu erillinen tietovirtakaavio tai käsittelytoimien seloste, voit viitata tässä kyseisiin asiakirjoihin.

|  |
| --- |
| Henkilötietojen käsittelyn toiminnallinen kuvaus |
|  |

# Tarpeellisuus ja oikeasuhteisuus

### Käyttötarkoitussidonnaisuus

Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Mihin nimenomaiseen käyttötarkoitukseen henkilötietoja kerätään ja mihin tietoja on myöhemmin mahdollisesti tarkoitus käyttää? Miten varmistutaan siitä, että henkilötietoja ei käsitellä muihin tarkoituksiin?

|  |
| --- |
| Käyttötarkoitussidonnaisuuden periaatteen toteuttaminen |
|  |

###

### Tietojen minimointi

Miten varmistutaan siitä, että tutkimuksen yhteydessä kerätään ja käsitellään ainoastaan käsittelyn tarkoituksen kannalta asianmukaisia ja olennaisia henkilötietoja, eikä ylimääräisiä tietoja kerätä?

|  |
| --- |
| Tietojen minimoinnin periaatteen toteuttaminen |
|  |

### Käsittelyn läpinäkyvyys ja informoinnin oikea-aikaisuus

Rekisteröidyille on oltava läpinäkyvää, miten heitä koskevia henkilötietoja kerätään ja käytetään. Henkilötietojen käsittelyyn liittyvät tiedot on toimitettava tiiviisti esitetyssä, läpinäkyvässä ja helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.

Miten tutkittavalle kerrotaan henkilötietojen käsittelystä? Miten henkilötietojen käsittelyä koskeva informaatio annetaan? Milloin informaatio annetaan?

|  |
| --- |
| Informoinnin toteutustapa |
|  |

### Suostumuksenhallinta, jos käsittelyperusteena on suostumus

Mikäli tutkittavalta pyydetään suostumus henkilötietojen käsittelyyn, miten suostumusten hallinta on järjestetty? Miten suostumus annetaan, miten suostumustietoja säilytetään ja miten suostumus on mahdollista peruuttaa?

|  |
| --- |
| Suostumuksenhallinnan kuvaus, jos käsittelyn oikeusperusteena on suostumus |
|  |

### Säilytyksen rajoittaminen ja pseudonymisointi tai anonymisointi

Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Rekisterinpitäjän on asetettava määräajat henkilötietojen poistoa tai niiden säilyttämisen tarpeellisuuden määräaikaistarkastelua varten, jotta voidaan varmistaa, ettei henkilötietoja säilytetä pidempään kuin on tarpeen.

Miten henkilötietojen säilytysaika tai sen määräytymisen peruste on määritetty? Miten mahdollinen jatkokäyttö on huomioitu säilytysaikaa määritettäessä? Miten ja missä vaiheessa henkilötietojen pseudonymisointi tai anonymisointi toteutetaan?

|  |
| --- |
| Säilytyksen rajoittaminen ja pseudonymisointi tai anonymisointi |
|  |

### Rekisteröidyn oikeudet ja oikeuksista poikkeaminen

Henkilötietojen käsittelyn oikeusperusteesta riippuen rekisteröidyllä voi olla oikeus saada pääsy henkilötietoihinsa, oikaista tietoja, oikeus saada tiedot poistetuksi (oikeus tulla unohdetuksi), rajoittaa tietojen käsittelyä ja vastustaa henkilötietojen käsittelyä.

Kuvaa rekisteröidyn oikeuksien käyttämistä koskeva prosessi. Kenelle rekisteröity voi toimittaa pyyntönsä? Miten varmistutaan siitä, että rekisteröidyn pyytämät tiedot ovat toimitettavissa rekisteröidylle tai muu pyyntö toteutettavissa, ja miten rekisteröityjen pyynnöt ja vastaukset dokumentoidaan ja arkistoidaan?

|  |
| --- |
| Rekisteröidyn oikeuksien käyttämistä koskeva prosessi |
|  |

Tietosuojalainsäädäntö mahdollistaa rekisteröidyn oikeuksista poikkeamisen tietyissä tilanteissa. Poiketaanko käsittelyssä rekisteröidyn oikeuksista?

|  |  |
| --- | --- |
| Oikeus, josta poiketaan | Poikkeamisen peruste |
|  |  |

### Eheys, luottamuksellisuus ja saatavuus

Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.

Kuvaa menettelyt, mukaan lukien tietoturvaratkaisut, joilla henkilötietojen eheys ja luottamuksellisuus varmistetaan käsittelyprosessin eri vaiheissa käsittelyn elinkaaren aikana.

|  |
| --- |
| Eheys ja luottamuksellisuus käsittelyn elinkaaren aikana |
|  |

### Henkilötietojen siirrot ja vastaanottajat

**Yhteisrekisterinpitäjät**

Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Mikäli henkilötietojen käsittelyyn osallistuu useampia osapuolia yhteisrekisterinpitäjinä, kirjaa yhteisrekisterinpitäjinä toimivat osapuolet yhteystietoineen, kunkin osapuolen rooli henkilötietojen käsittelyssä sekä mahdollisen tietosuojavastaavan yhteystiedot.

|  |
| --- |
| Yhteisrekisterinpitäjät |
|  |

**Henkilötietojen käsittelijät (alihankkijat)**

Henkilötietojen käsittelijällä tarkoitetaan tahoa, joka käsittelee henkilötietoja rekisterinpitäjän puolesta ja lukuun.

Mikäli henkilötietojen käsittelyyn osallistuu käsittelijän asemassa toimivia tahoja (kuten kysely- analyysi- tai litterointipalveluiden tarjoajia), kirjaa käsittelijänä toimivat tahot yhteystietoineen, kunkin tahon rooli henkilötietojen käsittelyssä sekä mahdollisen tietosuojavastaavan yhteystiedot.

|  |
| --- |
| Henkilötietojen käsittelijät |
|  |

**Muut mahdolliset käsittelyyn osallistuvat tahot tai tietojen vastaanottajat**

Luovutetaanko henkilötietoja muille tahoille, tai onko muilla tahoilla pääsy henkilötietoihin?

|  |
| --- |
| Muut käsittelyyn osallistuvat tahot tai tietojen vastaanottajat |
|  |

**Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle**

Henkilötietojen siirto Euroopan talousalueen ulkopuolelle voidaan toteuttaa ainoastaan tietosuoja-asetuksen säännöksissä vahvistettuja edellytyksiä noudattaen.

Mikäli henkilötietoja siirretään Euroopan talousalueen ulkopuolelle, mihin henkilötietoja siirretään ja mitä EU:n tietosuoja-asetuksen mukaisia suojatoimia siirtoon sovelletaan?

|  |  |  |  |
| --- | --- | --- | --- |
| Henkilötietotyyppi | Vastaanottaja | Sijainti | Suojatoimi |
|  |  |  |  |

# Käsittelyn riskit

### Henkilötietojen käsittelyyn liittyvien riskien tunnistaminen <https://tietosuoja.fi/vaikutustenarviointi>

Pohdi, millaisia riskejä rekisteröidylle eli tutkittavalle voi aiheutua erityisesti i) henkilötietojen luvattomasta luovutuksesta tai pääsystä henkilötietoihin, ii) henkilötietojen vahingossa tapahtuvasta tai luvattomasta tuhoamisesta tai muuttamisesta tai iii) henkilötietojen häviämisestä tai muuttumisesta. Miten vakava seuraus on rekisteröidyn kannalta, mikäli riski toteutuu, ja kuinka todennäköistä riskin toteutuminen on?

Riskejä voivat olla esimerkiksi:

* pseudonymisoinnin kumoutuminen tai henkilötietojen valvontakyvyn menettäminen
* identiteettivarkauden tai petoksen kohteeksi joutuminen, taloudellinen menetys
* sosiaalinen vahinko, kuten maineen menetys tai
* henkeen tai terveyteen kohdistuva uhka (erit. erityisten henkilötietoryhmien kohdalla)

Pohdi toimenpiteitä, joilla rekisteröidylle aiheutuvaa riskiä voidaan pienentää. Voit miettiä esimerkiksi:

* Miten aineiston käyttöoikeudet rajataan niin, että pääsy henkilötietoaineistoon on vain niillä henkilöillä, joilla on tutkimukseen perustuva tarve käsitellä henkilötietoja?
* Missä henkilötietoja säilytetään? Miten säilytyksen tietoturvasta on huolehdittu niin, että henkilötietojen luottamuksellisuus ja eheys varmistetaan?
* Miten henkilötietoja siirretään tietoturvallisesti tutkimuksen eri vaiheissa?

### Luvaton luovutus tai pääsy tietoihin

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Riski | Todennäköisyys | Vakavuus  | Toimenpide | Jäännösriski[[1]](#footnote-1)  |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |

### Henkilötietojen tuhoaminen tai muuttaminen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Riski | Todennäköisyys | Vakavuus  | Toimenpide | Jäännösriski  |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |

### Henkilötietojen häviäminen tai muuttuminen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Riski | Todennäköisyys | Vakavuus  | Toimenpide | Jäännösriski  |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |
|  | Valitse kohde. | Valitse kohde. |  | Valitse kohde. |

### Tietosuojavastaavan kommentit

Nimi dpo@tuni.fi

Päivämäärä

|  |
| --- |
| Tietosuojavastaavan kommentit: |

#

# Yhteenveto

Suunnitellut toimenpiteet ovat riittäviä käsittelyyn liittyvien riskien poistamiseksi tai vähentämiseksi niin, että rekisteröidyn oikeuksille ja vapauksille ei todennäköisesti aiheudu käsittelystä korkeaa riskiä (tietosuojavaikutusten arvioinnin laatija täyttää):

[ ]  Kyllä

[ ]  Ei

Mikäli käsittelyyn liittyvää riskejä ei saada suunnitelluilla toimenpiteillä pienennettyä tai mikäli toimenpiteitä riskien pienentämiseksi ei ole toteutettavissa, valvontaviranomaiselle (tietosuojavaltuutettu) on toimitettava ennakkokuulemispyyntö ennen käsittelyn aloittamista. Yliopiston tietosuojavastaava avustaa ennakkokuulemismenettelyssä.

|  |
| --- |
| Tampereen yliopiston tietosuojavastaavaSähköposti: dpo@tuni.fi |

1. Jäännösriskillä tarkoitetaan tutkittavalle aiheutuvaa riskiä sen jälkeen, kun suojatoimenpiteet on toteutettu. [↑](#footnote-ref-1)