# **Henkilötietojen suojaa koskeva vaikutustenarviointi (DPIA)**

Vaikutustenarvioinnin (DPIA = Data Processing Impact Assessment) tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn liittyviä riskejä rekisteröidyn oikeuksille ja vapauksille. Vaikutustenarviointi on osa tietosuojalainsäädännön vaatimusten noudattamista ja dokumentointia.

Tutustu ensin tietosuojavaltuutetun toimiston ohjeisiin:

* Käsittelyperusteet: <https://tietosuoja.fi/kasittelyperusteet>
* Vaikutusten arviointi: <https://tietosuoja.fi/vaikutustenarviointi>

Henkilötietojen käsittelytoimen / tutkimuksen nimi:

Kirjoita tekstiä napauttamalla tätä.

Yhteyshenkilö henkilötietojen käsittelyä koskevissa asioissa

Nimi: Kirjoita koko nimi napauttamalla tätä.

Sähköpostiosoite: Kirjoita sähköpostiosoite napauttamalla tätä.

Arvioinnin tekijä(t) (mikäli eri kuin yhteyshenkilö):

Nimi: Kirjoita koko nimi napauttamalla tätä.

Sähköpostiosoite: Kirjoita sähköpostiosoite napauttamalla tätä.

Päivämäärä: Kirjoita päivämäärä napauttamalla tätä.

Ohje lomakkeen täyttöön: Lomake on tarkoitettu täytettäväksi sähköisesti. Sarakkeet joustavat tekstin mukana, joten voit halutessasi lisätä suurenkin määrän tekstiä tai kuvia.

## Kuvaa henkilötietojen käsittely

|  |
| --- |
| Kuvaa henkilötietojen käsittelyn luonne: kuinka keräät, käytät, tallennat ja hävität/arkistoit henkilötiedot? Mistä tiedot kerätään? Jaetaanko tietoja muille osapuolille? Voit laatia myös tietovuokaavion (data flow diagram) selkeyttämään tietovirtojen kuvausta.  Kirjoita tekstiä napauttamalla tätä. |
| Kuvaa henkilötietojen käsittelyn laajuus: kuinka paljon henkilötietoja kerätään ja käytetään? Kuinka usein? Kuinka kauan henkilötietoja säilytetään? Kuinka monta yksilöä käsittely koskee ja mikä on tietojen maantieteellinen laajuus? Millaisia erityisiä henkilötietoryhmiä tai rikostuomioita koskevia henkilötietoja käsitellään? (Erityiset henkilötietoryhmät katso: <https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely>)  Kirjoita tekstiä napauttamalla tätä. |
| Käsittelyn toiminnallinen kuvaus: millaista käsittelyä tietoihin kohdistuu, esim. kerääminen, analysointi, muuttaminen, yhdistäminen, poistaminen, suorien tunnisteiden käsittely ja poistaminen jne. Mikä taho suorittaa kuvattua toimintaa?  Kirjoita tekstiä napauttamalla tätä. |
| Yksilöi käsittelyn resurssit: kirjaa tähän ketkä pääsevät henkilötietoihin käsiksi, mitä tietojärjestelmiä, sovelluksia, verkostoja, asiakirjoja ja tiedonsiirron kanavia käytetään.  Kirjoita tekstiä napauttamalla tätä. |

## Arvioi henkilötietojen käsittelyn tarpeellisuus ja oikeasuhtaisuus

|  |
| --- |
| Nimeä yksi tai useampi käsittelyn tietty, nimenomainen ja laillinen tarkoitus: käsittelytarkoitus voi olla esim. tieteellinen tutkimus. Mitä käsittelyllä on tarkoitus saavuttaa? Mikä on käsittelyn tavoitevaikutus rekisteröidyille? Mitä hyötyä henkilötietojen käsittelystä on rekisterinpitäjälle ja yleisesti?  Kirjoita tekstiä napauttamalla tätä. |
| Kuvaa henkilötietojen käsittelyn lainmukaisuus ja oikeasuhtaisuus: mikä on käsittelyn lainmukainen peruste? Esim. tutkittavan nimenomainen suostumus tai yleiseen etuun perustava tutkimus.  Kirjoita tekstiä napauttamalla tätä. |
| Kuinka varmistetaan, että tiedot ovat olennaisia, asianmukaisia ja rajoitettuja siihen, mikä on tarpeellista tietojenkäsittelyn tarkoitusten toteuttamista varten: kirjaa tähän kuinka ja missä on määritelty tarpeellisuus suhteessa käyttötarkoitukseen, esim. tutkimussuunnitelmassa. Kuinka varmistat henkilötietojen laadun ja minimointiperiaatteen noudattamisen? Eli kuinka huolehdit siitä, että tiedot ovat olennaisia, asianmukaisia ja rajoitettuja siihen, mikä on tarpeellista tietojenkäsittelyn tarkoitusten toteuttamista varten. Voitaisiinko tavoite saavuttaa jollakin muulla tavalla kuin käsittelemällä henkilötietoja suunnitellulla tavalla? Kuinka rajoitetaan suunnitellun käsittelyn laajentuminen?  Kirjoita tekstiä napauttamalla tätä. |
| Mikäli olet keräämässä tietoja myös suoraan tutkittavilta, kuvaa tutkittavien oikeuksia tutkimuksessa edistävät toimenpiteet: kirjaa, miten olet toteuttanut tutkittavien informoinnin henkilötietojen käsittelystä, esim. tiedote, tietosuojaseloste, keskustelu. Kuinka tutkittavan oikeus tarkastaa omia tietoja toteutetaan? Kirjaa myös, jos tarkastusoikeutta rajoitetaan tietosuoja-asetuksen 89 artiklan mukaisesti.  Kirjoita tekstiä napauttamalla tätä. |

## Kansainväliset tietojen siirrot

|  |
| --- |
| Onko tarkoitus siirtää/käsitellä henkilötietoja EU/ETA-alueen ulkopuolelle tai kv-järjestöille (esim. WHO)? Ota huomioon myös tiedon tallennuspaikka (esim. EU:n ulkopuolella sijaitseva palvelin, yhdysvaltalainen pilvipalvelun tarjoaja EU-alueella tai säännölliset etäyhteydet EU/ETA:n ulkopuolelta). Kirjaa osapuolet + valtiot, joihin tietoja siirretään, sekä tietosuoja-asetuksen V luvun mukainen siirtoperuste (esim. komission vastaavuuspäätös tai mallisopimuslausekkeet)  Kirjoita tekstiä napauttamalla tätä. |

## Tunnista ja arvioi riskit (katso ohje: <https://tietosuoja.fi/arvioi-riskit> )

Arvioi rekisteröidyille henkilötietojen käsittelystä aiheutuvia riskejä, niiden todennäköisyyttä ja vakavuutta, sekä laske riskiluku. Vaikutukset voivat olla esim. taloudellisia, fyysisiä (kuten terveyshaitta, väkivallan uhka), psyykkisiä (kuten ahdistus, stressi, mielipaha), mainehaitta, identiteettivarkauden uhka, lisävaiva, seuraukset työnantajan taholta tai lainmukaisten oikeuksien toteutumatta jääminen.

* Mitkä seikat voivat aiheuttaa riskejä tutkittavan yksityisyyden suojalle? Esim. käsitelläänkö arkaluonteisia henkilötietoja, geneettisiä tai rikoksia koskevia tietoja. Esimerkiksi lähtökohtana poliittinen/uskonnollinen vapaus, ammattiliittoon kuuluminen, terveystiedot, rikokset ja rikostuomiot jne. ovat erityisiä henkilötietoryhmiä koskevia ns. arkaluonteisia tietoja, joihin liittyy korkea riski rekisteröidyn oikeuksille ja vapauksille.
* Kuinka riskien alkuperä on otettu huomioon riskien hallinnassa?
* Kirjaa tähän riskienhallinnan tunnistamista, arviointia ja käsittelyä. Mitä riskejä on tunnistettu, esim. laiton pääsy tietoihin, asiaton muuttaminen, tietojen katoaminen jne.
* Millaisia ovat tutkittavien oikeuksiin ja vapauksiin kohdistuvat mahdolliset vaikutukset laittoman tietoihin pääsyn, tietojen asiattoman muuttamisen ja tietojen katoamisen osalta?
* Onko tietojen käsittelyllä seurauksia rekisteröityjen perusoikeuksiin tai muihin lainmukaisiin oikeuksiin?
* Tunnistatko uhkia, jotka voivat johtaa laittomaan pääsyyn tietoihin, asiattomaan muuttamiseen ja tietojen katoamiseen? Esim. tietomurto, tietojen huolimaton käsittely, vika tietojärjestelmässä

|  |  |  |  |
| --- | --- | --- | --- |
| Kuvaa rekisteröityjen oikeuksiin ja vapauksiin kohdentuvat riskit ja uhat, sekä mahdollinen rekisteröidyille aiheutuva haitta | **Todennäköisyys**  1=vähäinen, 2=mahdollinen, 3=todennäköinen | **Vakavuus**  1=vähäinen, 2=merkittävä, 3=vakava | **Riskiluku** (todennäköisyys x vakavuus)  1-3=matala, 4=keskitaso,  6-9=vakava |
| 1. Kirjoita tekstiä napauttamalla tätä. | Kirjoita todennäköisyys. | Kirjoita vakavuus. | Kirjoita riskiluku. |
| 2. Kirjoita tekstiä napauttamalla tätä (ei pakollinen). | Kirjoita todennäköisyys. | Kirjoita vakavuus. | Kirjoita riskiluku. |
| 3. Kirjoita tekstiä napauttamalla tätä (ei pakollinen). | Kirjoita todennäköisyys. | Kirjoita vakavuus. | Kirjoita riskiluku. |
| 4. Kirjoita tekstiä napauttamalla tätä (ei pakollinen). | Kirjoita todennäköisyys. | Kirjoita vakavuus. | Kirjoita riskiluku. |

## Tunnista riskiä vähentävät organisatoriset tai tekniset toimenpiteet

**Kirjaa tähän toimenpiteet, joilla riskeihin puututaan:** esim. säännöllinen ja jatkuva arviointi, aikataulut ja valvontavastuut, suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja, tietojärjestelmien suojaus, manuaalisen aineiston suojaus, tietojen pseudonymisointi, tietojen anonymisointi/hävittäminen, koodiavaimen suojaus ja säilytys, sopimukset, suojatoimet, koulutukset, salassapitositoumukset, käsittelijöiden rajaaminen.

|  |  |  |  |
| --- | --- | --- | --- |
| **Riski** | **Toimenpide riskin vähentämiseksi** | **Vaikutus riskiin**  1 = poistettu 2 = vähennetty 3 = hyväksytty | **Jäännösriskit**  1 = matala 2 = keskitaso 3 = korkea |
| Kirjoita riskin numero. | Kirjoita tekstiä napauttamalla tätä. | Kirjoita vaikutus riskiin. | Kirjoita riskin taso. |
| Kirjoita riskin numero. | Kirjoita tekstiä napauttamalla tätä. | Kirjoita vaikutus riskiin. | Kirjoita riskin taso. |
| Kirjoita riskin numero. | Kirjoita tekstiä napauttamalla tätä. | Kirjoita vaikutus riskiin. | Kirjoita riskin taso. |
| Kirjoita riskin numero. | Kirjoita tekstiä napauttamalla tätä. | Kirjoita vaikutus riskiin. | Kirjoita riskin taso. |

## Tietosuojavastaavan kommentti

Yhteyshenkilö henkilötietojen käsittelyä koskevissa asioissa

Nimi: Kirjoita yhteyshenkilön nimi napauttamalla tätä.

Sähköpostiosoite: Kirjoita sähköpostiosoite napauttamalla tätä.

Päivämäärä: Kirjoita päivämäärä napauttamalla tätä.

|  |
| --- |
| Rekisteripitäjän/organisaation tietosuojavastaavan kommentti:  Kirjoita tekstiä napauttamalla tätä. |