VAHTI-hyvät käytännöt tukimateriaali 16.8.2021

16.8.2021

**Tietosuoja - vaikutustenarviointi**

Kommenttiversio

Sisällysluettelo

[1 Johdanto 2](#_Toc80860525)

Tietosuoja - vaikutustenarviointi

# Johdanto

Tämä tukimateriaali on laadittu julkisen hallinnon organisaatioille turvallisen työskentelyn ja toiminnan edistämisesi. Tukimateriaalit pohjautuvat julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) asiantuntijaryhmien kokoamiin riskienhallinnan, toiminnan jatkuvuuden ja valmiuden, tietoturvallisuuden ja tietosuojan hyviin käytäntöihin. Hyvien käytäntöjen mukaisesti toimimalla edistämme samalla kyberturvallisuuden toteutumista.

Toivomme, että annat meille palautetta tästä materiaalista. Saatuamme parannus ja korjausehdotuksia 30.9.2021 mennessä, julkaisemme sen jälkeen tästä päivitetyn version lokakuussa 2021.

[Linkki palautekyselyyn.](https://response.questback.com/dvv/digiturvahyvatkaytannotpalaute)

Jokainen organisaatio ja asiantuntija vastaa siitä, että tukimateriaali sovitetaan tarkemmin organisaation omaan toimialaan ja sitä koskevaan lainsäädäntöön.

Tämän tukimateriaalin tuottamisesta on vastannut VAHTI tietosuojan kehittäminen työryhmän asiantuntijat.

# Tietosuojan vaikutustenarviointi

## Henkilötietojen käsittelyn kuvaus

* + **Käsittelyn asiayhteys**

*Kirjaa tähän, mihin tarkoitukseen/mitä varten henkilötietoja käsitellään*

* + **Käsittelyn laajuus**

*Kirjaa tähän käsiteltävän tiedon määrä, alueellinen kattavuus ja käsittelyn laajuus. Käsitelläänkö tietoja EU:n ulkopuolisissa maissa?*

* + **Käsittelyn toiminnallinen kuvaus**

*Kirjaa tähän millaista käsittelyä tietoon kohdistuu esim. kerääminen, analysointi, muuttaminen, yhdistäminen, säilytysajan määrittäminen, poistaminen jne.*

* + **Käsittelyn resurssien yksilöinti**

*Kirjaa tähän ketkä ihmiset pääsevät tietoon käsiksi, mitä tietojärjestelmiä, sovelluksia, verkostoja, asiakirjoja ja tiedonsiirron kanavia käytetään.*

## Käsittelyn oikeasuhteisuutta ja tarpeellisuutta edistävät toimenpiteet

* + **Nimeä yksi tai useampi käsittelyn tietty, nimenomainen ja laillinen tarkoitus**

*Käyttötarkoitus voi olla esim. henkilöstöhallinto, opiskelijahallinto, rekrytointi, taloushallinto, jne. Tee käyttötarkoituksesta myös hieman tarkennettu kuvaus*

* + **Nimeä käsittelyn lainmukaisuuden peruste**

*Nimeä tietosuoja-asetuksen art. 6 mukainen käsittelyperuste: suostumus, sopimuksen toimeenpano, rekisterinpitäjän lakisääteinen tehtävä (mikä), rekisteröidyn elintärkeä etu, rekisterinpitäjän yleistä etua koskeva tehtävä tai julkisen vallan käyttäminen (tarkenne tietosuojalain 4 §:stä, rekisterinpitäjän oikeutettu etu (mikä)*

* + **Kuinka on huolehdittu siitä, 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, missä ja miten on määritelty se, että juuri näitä henkilötietoja tarvitaan tässä käyttötarkoituksessa*

* + **Kuinka käsiteltävien henkilötietojen elinkaaren aikana on huolehdittu siitä, että tiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen** **tietojenkäsittelyn tarkoitusten toteuttamista varten**

*Esim. tunnisteellisten henkilötietojen muuttaminen pseudonyymiksi, anonyymiksi /hävittäminen heti kun tietoja ei enää tarvita. Anonymisoitu tieto ei ole enää henkilötieto.*

## Rekisteröityjen oikeuksia edistävät toimenpiteet

* + **Rekisteröidylle annetut tiedot**

*Kirjaa tähän miten on toteutettu rekisteröityjen informointi henkilötietojen käsittelystä, esim. tiedote, tietosuojaseloste, verkkosivut, keskustelu.*

* + **Kuinka rekisteröidyn oikeus tarkastaa tiedot toteutetaan**?

*Kirjaa tähän miten rekisteröity voi tarkastaa itseään koskevat tiedot esim. lomake, yhteyshenkilö, tietosuojavastaava. Kirjaa myös, jos tarkastusoikeutta rajoitetaan tietosuojalain mukaisesti. Varmista pyynnön esittäjän henkilöllisyys.*

* + **Jos rekisteröidyllä on oikeus siirtää tiedot järjestelmästä toiseen, kuinka tämä toteutetaan**?

*Oikeutta sovelletaan, kun käsittely toteutetaan automaattisesti ja käsittely perustuu suostumukseen tai sopimukseen ja rekisteröity on itse toimittanut tiedot rekisterinpitäjälle. Ei sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten. Jos käsittelyperuste on yleinen etu, niin tähän voi kirjata, että oikeutta siirtää tiedot toiseen järjestelmään ei sovelleta. Jos oikeus tulee sovellettavaksi, kerro miten rekisteröity voi oikeuttaan käyttää esim. ottamalla yhteyttä rekisterinpitäjään.*

* + **Kuinka rekisteröidyn oikeus oikaista/poistaa tiedot toteutetaan**?

*Tätä oikeutta sovelletaan, kun käsittelyn perusteena on suostumus, sopimuksen toimeenpano, rekisteröidyn elintärkeä etu tai rekisterinpitäjän oikeutettu etu. Ei sovelleta, jos käsittelyn perusteena on rekisterinpitäjän lakisääteinen tai yleisen edun mukainen tehtävä. Jos oikeus tulee sovellettavaksi, kerro miten reksiteröity voi oikeuttaan käyttää esim. ottamalla yhteyttä rekisterinpitäjään.*

* + **Kuinka rekisteröidyn oikeus vastustaa tai rajoittaa käsittelyä toteutetaan**?

*Kerro minne rekisteröity voi ottaa yhteyttä, jos esim. kiistää henkilötietojen paikkansapitävyyden ja haluaa vastustaa tai rajoittaa sillä perusteella tietojensa käsittelyä.*

* + **Rekisteröidyn oikeus vastustaa suoramarkkinointia***Rekisteröidyllä on oikeus vastustaa tietojensa käyttämistä suoramarkkinointitarkoituksiin. Oikeus koskee vain käsittelyä, joka perustuu yleistä etua koskevan tehtävän suorittamiseen, julkisen vallan käyttöön tai rekisterinpitäjän lakisääteiseen tehtävään.*
	+ **Rekisteröidyn oikeus olla joutumatta automaattisen päätöksenteon kohteeksi***Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin ja jolla on häntä koskevia oikeusvaikutuksia.*
	+ **Käytetäänkö tehtävässä/tietojärjestelmän käytössä henkilötietojen käsittelijöitä ja miten toiminta on ohjeistettu?**

*Henkilötietojen käsittelijöitä ovat ne, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun tai joilla on pääsy rekisterinpitäjän henkilötietoihin esim. alihankkijat, konsultit tai tietojärjestelmätoimittajan edustajat vikatilanteiden selvittelyssä tai helpdesk -toiminnoissa. Henkilötietojen käsittelijöitä eivät ole rekisterinpitäjän henkilökuntaan kuuluvat henkilöt. Kerro onko tehty tietosuojasopimus ja sisältääkö sopimus ohjeet henkilötietojen käsittelystä.*

* + **Yksilöi kansainväliset tietojen käsittelyt ja siirrot sekä niihin liittyvät suojatoimet**

*Kerro käsitelläänkö tai siirretäänkö tietoja EU:n ja ETA:n ulkopuolelle ja jos siirretään, niin yksilöi käytetyt suojatoimet, esim. riittävän tietosuojan tason, EU:n hyväksymien mallilausekkeiden, yritystä sitovien sääntöjen tai rekisteröidyn suostumuksen perusteella. Kerro lisäksi, käsitelläänkö tai onko tarkoitus siirtää tietoja pilvipalveluun.*

## Kuinka hallitaan rekisteröidyn oikeuksiin ja vapauksiin kohdistuvia riskejä

* + **Riskien alkuperä, luonne, erityisluonne ja vakavuus**

*Kirjaa tähän, mitkä seikat voivat aiheuttaa riskejä rekisteröidyn yksityisyyden suojalle esim. käsitelläänkö arkaluonteisia henkilötietoja, geneettisiä tietoja, tehdäänkö profilointia tai pisteytyksiä, poiketaanko rekisteröityjen informoinnista ja miksi. Esim. Lähtökohtana poliittinen/uskonnollinen vapaus, ammattiliittoon kuuluminen, terveystiedot, rikokset ja rikostuomiot jne. ovat erityisiä henkilötietoryhmiä koskevia ns. arkaluonteiset 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.*

* + **Rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat mahdolliset vaikutukset laittoman tietoihin pääsyn, tietojen asiattoman muuttamisen ja tietojen katoamisen osalta**

*esim. salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys, mainehaitta, sosiaalinen vahinko, identiteettivarkaus*

* + **Uhat, jotka voivat johtaa laittomaan pääsyyn tietoihin, asiattomaan muuttamiseen ja tietojen katoamiseen**

*Esim. tietomurto, tietojen huolimaton käsittely, vika tietojärjestelmässä*

* + **Riskien ja uhkien todennäköisyys ja vakavuus**

Esim. luokittelu: Todennäköisyys: 1. epätodennäköinen, 2. mahdollinen, 3. todennäköinen, 4. lähes varma ja Vakavuus: 1. vähäinen, 2. kohtalainen, 3. merkittävä, 4. kriittinen. Voit koostaa riskit esim. taulukkoon.

* + **Riskien käsittelyyn suunnitellut toimenpiteet**
	+ **seuraavan sivun taulukko**

|  |  |  |  |
| --- | --- | --- | --- |
| **Riskien tunnistaminen** | **Riskianalyysi** | **Riskin merkityksen arviointi** | **Riskin käsittely** |
| **Riskin tunniste** | **Riskin kuvaus** | **Todennäköisyys (1-4)** | **Vaikutus (1-4)** | **Riskin merkittävyys(T x V)** | **Toimenpiteiden kuvaus** | **Seuraukset rekisteröidylle** | **Tavoite-aikataulu** |
|
| **1** | Esim. henkilötietoja käytetään muuhun tarkoitukseen kuin niitä on kerätty, kuten sijaintitietoja käytetään työajan seurantaan. | **1** | **Epätodennäköinen** | **4** | **Vakava** | **4** | **Rajattu riski** |   | esim. mainehaitta, identiteettivarkaus, seuraukset työnantajan taholta. |   |
| **2** |   | **2** | **Mahdollinen** | **3** | **Merkittävä** | **6** | **Rajattu riski** |   |   |   |
| **3** |   | **3** | **Todennäköinen** | **2** | **Kohtalainen** | **6** | **Huomioitava riski** |   |   |   |
| **4** |   | **4** | **Lähes varma** | **1** | **Vähäinen** | **4** | **Huomioitava riski** |   |   |   |
| **5** |   |  | **Ei arvioitu** |  | **Ei arvioitu** |  | **Kriittinen riski** |   |   |   |
| **6** |   |  | **Ei arvioitu** |  | **Ei arvioitu** |  | **Huomioitava riski** |   |   |   |
| **7** |   |  | **Ei arvioitu** |  | **Ei arvioitu** |  | **Huomioitava riski** |   |   |   |
| **8** |   |  | **Ei arvioitu** |  | **Ei arvioitu** |  | **Huomioitava riski** |   |   |   |

* + **Mahdollinen ennakkokuulemismenettely tai tarve sille**

*Rekisterinpitäjän on ennen henkilötietojen käsittelyä kuultava valvontaviranomaista (Suomessa tietosuojavaltuutetun toimisto), jos tietosuojaa koskeva vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin, jos rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi.*

**5. Kuvaa sidosryhmien ottaminen mukaan**

* **Tietosuojavastaavan rooli**

*Tietosuoja-arviota tehtäessä on pyydettävä neuvoja tietosuojavastaavalta. Kirjaa tähän, miten ja milloin tietosuojavastaavalta on kysytty neuvoja ja onko ne otettu huomioon. Kirjaa myös se, jos tietosuojavastaavan antamaa ohjeistusta ei ole huomioitu ja miksi.*

**6. Suunnitellut toimenpiteet riskeihin puuttumiseksi**

* + **Toimenpiteet, joilla riskeihin puututaan**

*Esim. säännöllinen ja jatkuva arviointi, aikataulut ja valvontavastuut*

**Suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja***Esim. tieto- järjestelmien suojaus, manuaalisen aineiston suojaus, tietojen pseudonymisointi, tietojen anonymisointi/hävittäminen, koodiavaimen suojaus ja säilytys, sopimukset, suojatoimet, koulutukset, salassapitositoumukset, käsittelijöiden rajaaminen*

* + **Riskienarvioinnin lisätoimenpiteet**
	Hyväksyjä:
	Päivämäärä:
	+ **Jäännösriskit**
	Hyväksyjä:
	Päivämäärä: