



TIETOSUOJAVALTUUTETUN  
TOIMISTO

Tietosuojavaltuutetun toimisto

# **Tietosuojaan vaikutustenarvioinnin ohje**



## Muutoshistoria

Aika	Muutos
12/2021	Ohje julkaistu kommenttikierroksen jälkeen.



## Sisällys

### Tietosuojan vaikutustenarvioinnin ohje

Johdanto .....	5
Mikä on tietosuojan vaikutustenarviointi? .....	5
Miksi tietosuojan vaikutustenarviointi tehdään? .....	6
Miten tietosuojan vaikutustenarviointi tehdään? .....	6
Ohjeen rakenne .....	8
1. Kuvaus henkilötietojen käsittelystä (kontekstin hahmottaminen) .....	9
2. Tietosuojasääntelyn noudattamisen arviointi .....	10
2.1 Tietosuojaperiaatteiden noudattaminen .....	10
2.1.1 Lainmukaisuus (käsittelyperuste) ja kohtuullisuus .....	11
2.1.2 Läpinäkyvyys (rekisteröityjen informointi) .....	12
2.1.3 Käyttötarkoitussidonnaisuus .....	13
2.1.4 Tietojen minimointi ja säilytyksen rajoittaminen .....	14
2.1.5 Tietojen täsmällisyys .....	15
2.1.6 Henkilötietojen käsittelyn turvallisuus (luottamuksellisuus, eheys ja käytettävyys) .....	16
2.2 Henkilötietojen käsittelijät .....	17
2.3 Henkilötietojen siirrot ETA-alueen ulkopuolelle .....	18
2.4. Huolehdi rekisteröidyn oikeuksien toteuttamisesta .....	20
2.4.1 Rekisteröidyn oikeuksien toteuttaminen (TSA art. 12) .....	20
2.4.2 Oikeus saada pääsy tietoihin (TSA art. 15) .....	21
2.4.3 Oikeus tietojen oikaisemiseen (TSA art. 16) sekä ilmoitusvelvollisuus (TSA art. 19) .....	22
2.4.4 Oikeus tietojen poistamiseen (TSA art. 17) sekä ilmoitusvelvollisuus (TSA art. 19) .....	22
2.4.5 Oikeus käsittelyn rajoittamiseen (TSA art. 18) sekä ilmoitusvelvollisuus (TSA art. 19) .....	23
2.4.6 Oikeus siirtää tiedot järjestelmästä toiseen (TSA art. 20) .....	23
2.4.7 Oikeus vastustaa tietojen käsittelyä (TSA art. 21) .....	24
2.4.8 Automaattinen päätöksenteko (ml. profilointi) (TSA art. 22) .....	24
3 Riskien arviointi .....	26
3.1 Arvioi riskit rekisteröidyn näkökulmasta .....	26
3.2. Tunnista uhat .....	28
3.2.1 Uhkatalukko .....	28
3.2.2 Muita työkaluja ja näkökulmia uhkien tunnistamiseen .....	30
3.3. Arvioi vaikutuksien vakavuus rekisteröidyn näkökulmasta .....	31
3.4 Arvioi uhkien toteutumisen todennäköisyys .....	34



3.5 Määrittele ja toteuta lisäsuojatoimenpiteet uhkien todennäköisyyden ja vaikutusten vakavuuden madaltamiseksi hyväksyttävälle tasolle .....	35
3.6 Laadi uhkien todennäköisyyden ja vaikutusten vakavuuden arvioinnin yhteenveto.....	37
4 Tietosuojan vaikutustenarvioinnin hyväksyminen sekä mahdolliset korjaavat toimenpiteet .....	39
Muita tietosuojan vaikutustenarvioinnin ohjeita ja lähdeaineistoa:.....	40
Käsitteitä .....	41
Liitteet .....	45



## Johdanto

### Mikä on tietosuojan vaikutustenarviointi?

Tietosuojan vaikutustenarvioinnin tarkoituksena on tunnistaa ja vähentää henkilötietojen käsittelyyn liittyviä riskejä sekä tuottaa aineistoa, jolla tietosuojasääntelyn noudattaminen voidaan osoittaa. Vaikutustenarviointia voidaan käyttää jatkuvana apuna sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamisessa sekä riskien hallinnassa silloin, kun henkilötietojen käsittelyyn liittyy korkeita riskejä rekisteröidylle. Tämä ohje on laadittu yleisen tietosuoja-asetuksen (jatkossa TSA) 35 artiklassa sekä rikosasioiden tietosuojalain (jatkossa RTsL) 20 §:ssä tarkoitetun tietosuojan vaikutustenarvioinnin (jatkossa TVA) laatimisen tueksi. Jälkimmäisestä katso lisäksi liite II.

TSA 35 artiklan mukaan vaikutustenarviointi on tehtävä silloin, kun suunnitellaan henkilötietojen käsittelyä, joka todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. [Katso tietosuojavaltuutetun toimiston verkkosivuilta, milloin vaikutustenarviointi pitää tehdä<sup>1</sup>.](#)

Vaikutustenarvioinnin toteuttamistapaa ei ole määritetty TSA:ssa tarkemmin. TSA 35 artiklassa on lueteltu TVA:n vähimmäisisältö, jota on edelleen tarkennettu vaikutustenarviointia koskevassa ohjeessa<sup>2</sup>.

Jokaisen organisaation on varmistettava, että sen toiminnassa noudatetaan henkilötietojen käsittelyä koskevaa sääntelyä riippumatta siitä, onko käsittely korkeariskistä vai ei. TVA eroaa tässä lainmukaisuuden varmistamisesta. Se edellyttää tarkempaa riskien ja niitä koskevien suojatoimenpiteiden etukäteistä tunnistamista, erittelyä ja kuvaamista.

#### Tietosuojan vaikutustenarvioinnin ydinkysymykset

Miksi ja miten aiomme käsitellä henkilötietoja?

Mitä henkilötietoja aiomme käsitellä?

Miten suunnittelemamme henkilötietojen käsittely vaikuttaa rekisteröityihin, kun käsittely sujuu suunnitelmien mukaisesti?

Mikä suunnittelemassamme henkilötietojen käsittelyssä voi mennä pieleen?

Miten todennäköisesti jokin menee pieleen?

Miten voimme vähentää tätä todennäköisyyttä?

TVA on päivitettävä toimintaympäristön, lainsäädännön ja riskien muuttuessa, esimerkiksi silloin, kun otetaan käyttöön joitakin henkilötietojen käsittelyyn vaikuttavia tai siihen liittyviä toiminnallisuksia. Vaikutustenarvioinnin päivittämisen tarvetta on lisäksi suositeltavaa arvioida säännöllisesti, esimerkiksi kahden vuoden välein.

Vaikutustenarvioinnin tekemistä koskevia vaatimuksia sovelletaan myös ennen 25.5.2018 alkaneisiin, edelleen käynnissä oleviin käsittelytoimiin. Rekisterinpitäjän on siis tehtävä käynnissä olevan käsittelyn osalta vaikutustenarviointi silloin, kun siihen olisi velvoite muutoinkin tietosuojalainsäädännön mukaan. Vaikutustenarviointi voi koskea yksittäistä käsittelytoimea tai samankaltaisten käsittelytoimien kokonaisuutta.

<sup>1</sup> <https://tietosuoja.fi/vaikutustenarviointi>

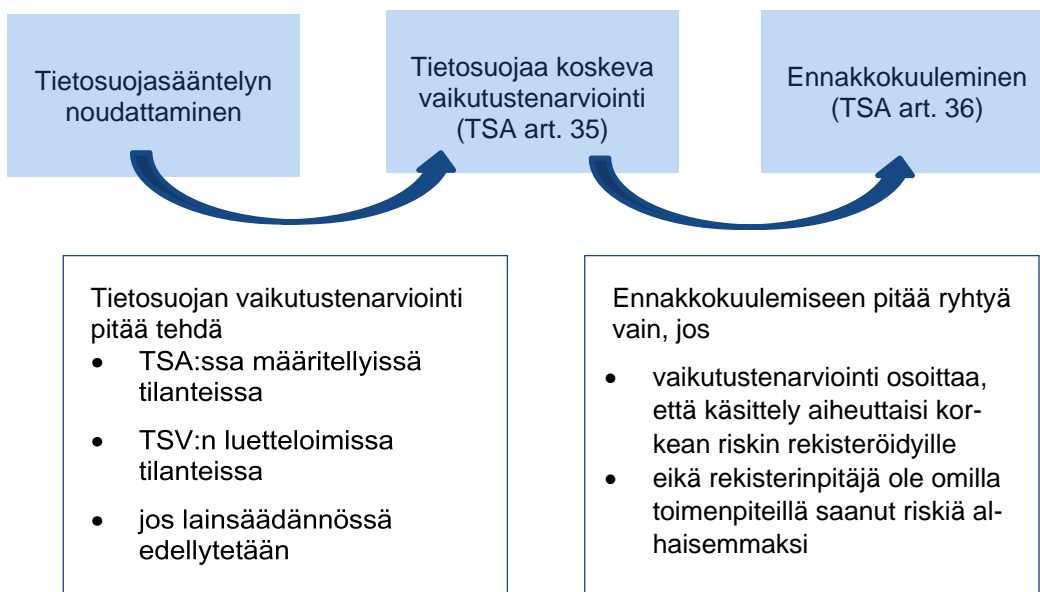
<sup>2</sup> Artikla 29 mukaisen tietosuojatyöryhmä WP29:n ohje WP 248 rev.01, liite II. Euroopan tietosuojaneuvosto (EDPB) hyväksyi ensimmäisessä täysistunnossaan artikla 29 mukaisen tietosuojatyöryhmän laatimat TSA:a koskevat ohjeet, ml. ohje WP 248 rev.01.

## Miksi tietosuojan vaikutustenarviointi tehdään?

Tietosuojan vaikutustenarvioinnin laatisesta voi olla organisaatiolle monia hyötyjä. Sen avulla voidaan havaita henkilötietojen käsittelyyn liittyvät uhat ja tunnistaa, mitä toimenpiteitä uhkien välttämiseksi on tarpeen tehdä ennen merkittävien taloudellisten sijoitusten tekemistä. Suunnitellun käsittelyn muuttaminen suunnitteluvaiheessa maksaa yleensä murto-osan myöhemmin aiheutuvista kustannuksista. Jos tietosuojavaikutuksia ei voida hyväksyä, voidaan koko suunnitelma jopa joutua peruuttamaan.

Tietosuojan vaikutustenarviointi voi tuoda myös maine-etuja. Rekisterinpitäjä voi kuulla rekisteröityjen mielipiteitä suunnitellusta käsittelystä ennen käsittelyn aloittamista, tai tietosuojan vaikutustenarviointi voidaan julkaista rekisteröityjen nähtävälle läpinäkyvyyden lisäämiseksi sekä käyttäjäkokemuksen parantamiseksi. Jos käsittelyyn liittyvä uhka konkretisoituu, tietosuojavaikutusten arviointia koskeva dokumentaatio voi auttaa osoittamaan, että rekisterinpitäjä yritti asianmukaisesti estää tapahtuman. Näin voidaan vähentää riskiä vahinkovastuusta, negatiivisesta julkisuudesta ja maineen menettämisestä.

Tietosuojan vaikutustenarvioinnin tekemättä jättäminen tilanteessa, jossa se tulisi tehdä, voi johtaa hallinnollisiin seuraamuksiin, mukaan lukien seuraamusmaksu tai käsittelykielto. Rekisterinpitäjiä kehoitetaan siksi dokumentoimaan, miksi TVA on jossain tilanteessa päätetty jättää tekemättä. Tämä on tärkeää erityisesti ns. harmaan alueen tilanteissa. Laatimalla vaikutustenarvioinnin tällaisissa tilanteissa, rekisterinpitäjä voi viestittää sidosryhmilleen suhtautuvansa vakavasti tietosuojaan liittyviin kysymyksiin.



*Kuva 1. Vaikutustenarvioinnin sijoittuminen henkilötietojen käsittelyä koskevien velvollisuuksien kokonaisuudessa. Kun käsittelyyn liittyy korkea riski rekisteröidyille, on tietosuojasääntelyn noudattamisen lisäksi laadittava tietosuojaa koskeva vaikutustenarviointi. Vaikutustenarviointia ei siis ole välttämätöntä tehdä kaikissa tilanteissa. Jos vaikutustenarvioinnissa määriteltyjen korjaavien toimenpiteiden toteuttamisen jälkeen jäännösriski on edelleen korkea, on pyydettävä tietosuojavaltuutetun ennakkokuulemistä.*

## Miten tietosuojan vaikutustenarviointi tehdään?



Rekisterinpitäjä on vastuussa TVA:n laatimisesta. Rekisterinpitäjän on yksilöitävä vaikutustenarvioinnin kohde. Lisäksi on suositeltavaa yksilöidä sen laatimiseen osallistuvat henkilöt (kuten rekisterinpitäjän edustajat, henkilötietojen käsittelijän edustajat, tietosuojavastaava, it-asiantuntijat, tietoturva-asiantuntijat, käytännön käsittelyyn perehtyneet henkilöt ja mahdolliset ulkopuoliset asiantuntijat). Rekisterinpitäjän pitää myös määritellä menettely, jolla havaitut riskit, mahdolliset toimenpideehdotukset niiden vähentämiseksi sekä mahdollinen jäännösriski hyväksytään.

Henkilötietojen käsittelijän on autettava rekisterinpitäjää TVA:n tekemisessä ja antaa rekisterinpitäjälle vaikutustenarvioinnin tekemiseksi tarpeelliset tiedot.

Rekisterinpitäjän on vaikutustenarviointia tehdessään pyydettävä neuvoja tietosuojavastaavalta, jos sellainen on nimitetty.

Suunnitelluista käsittelytoimista on suositeltavaa kuulla käsittelyn kohteena olevia henkilöitä tai näiden edustajia. Kuulemisessa pitää ottaa huomioon kaupallisista tai yleisestä edusta tai käsittelyn turvallisuudesta johtuvat intressit. Rekisteröityjen tai heidän edustajiensa kuulemisella voidaan saada lisätietoa suunnitellun henkilötietojen käsittelyn hyväksyttävyydestä ja mahdollisista väärinkäsityksistä.

Yksittäistä tietosuojaa koskevaa vaikutustenarviointia voidaan käyttää muiden käsittelytoimien arviointiin, joiden luonne, laajuus, asiayhteys, tarkoitus ja riskit ovat samankaltaisia. Vaikutustenarviointia ei siis tarvitse tehdä sellaisista suunnitelluista käsittelytoimista, joiden vaikutukset on jo arvioitu. Näin voi olla esimerkiksi, kun samankaltaista tekniikkaa on käytetty samantyyppisten tietojen keräämiseen samoja tarkoituksia varten.<sup>3</sup>

Kun valmistelet vaikutustenarvioinnin tekemistä, ota huomioon seuraavat seikat:

- 1) Määrittele vaikutustenarvioinnin kohde. Onko kyseessä tuote/ohjelmisto/järjestelmä/prosessi? IT-pohjainen tuote vai IT-pohjainen palvelu?
- 2) Määrittele roolit ja vastuut. Tunnista käsittelyyn osalliset ja heidän roolinsa ja vastuunsa: rekisterinpitäjä(t) ja henkilötietojen käsittelijä(t) sekä henkilötietojen vastaanottajat.
- 3) Selvitä vaikutustenarvioinnin kohteeseen soveltuva henkilötietojen suoja koskeva sääntely (EU:n yleisen tietosuojasetuksen ohella mm. toimialakohtainen sääntely).
- 4) Valitse osallistujat ja määrittele heidän roolinsa (juridinen ja tekninen osaaminen, käytännön henkilötietojen käsittelystä tietävät henkilöt, tietosuojavastaava). Mieti paras tapa arvioinnin toteuttamiseen (esim. työpajatyöskentely, katselmointi) ja huolehdi arvioinnin riittävästä resursoinnista. Henkilötietojen käsittelijän (esim. järjestelmätoimittaja) tulee avustaa rekisterinpitäjää tietosuojan vaikutustenarvioinnin tekemisessä. On suositeltavaa varata myös henkilötietojen käsittelyn kohteena oleville henkilöille tai heidän edustajilleen tilaisuus tulla kuulluksi.
- 5) Konsultoi mahdollista tietosuojavastaavaa tietosuojan vaikutustenarviointia tehdessäsi. Vastuu vaikutustenarvioinnin tekemisestä (ml. valitut suoja-toimenpiteet) sekä mahdolliseen ennakkokuulemismenettelyyn ryhtymisestä on kuitenkin rekisterinpitäjällä.

<sup>3</sup> WP 248 rev.01, s. 8.



- 6) Kartoita ja hyödynnä jo olemassa oleva tietosuojaa/tietoturvaa koskeva materiaali (esim. henkilötietoinventaarit, tietovuokaaviot, 30 artiklan mukaiset selosteet käsittelytoimista jne.)
- 7) Huolehdi siitä, että on olemassa prosessi tietosuojan vaikutustenarvioinnin hyväksymiselle ja että vaikutustenarvioinnin myötä esiin mahdollisesti nousseet tarvittavat toimenpiteet aikataulutetaan ja vastuutetaan tietyille henkilöille. Varmistu myös siitä, että toimenpiteiden toteutumista seurataan konkreettisesti ja vaikutustenarviointia päivitetään tarvittaessa, vähintään jos henkilötietojen käsittelyyn liittyvät riskit muuttuvat.

## Ohjeen rakenne

Tässä ohjeessa TVA on jaettu neljään vaiheeseen. Ensin kuvataan vaikutustenarvioinnin kohde (luku 1). Tämän jälkeen arvioidaan, onko suunniteltu henkilötietojen käsittely henkilötietojen käsittelyä koskevan sääntelyn mukaista (luku 2). Tässä yhteydessä tarkastellaan henkilötietojen käsittelyn tarpeellisuutta ja oikeasuhteisuutta sekä tietosuojaperiaatteiden ja tietosuojaoikeuksien toteutumista. Lisäksi varmistetaan muun suunniteltua henkilötietojen käsittelyä koskevan lainsäädännön noudattaminen.

Tämän jälkeen arvioidaan henkilötietojen käsittelystä rekisteröidylle koituvat riskit. Se tehdään tunnistamalla uhat, niiden vakavuus sekä toteutumisen todennäköisyys (luku 3).

Lopuksi kuvataan, mitä toimenpiteitä TVA:n loppuunsaattaminen edellyttää (luku 4).

Ohjeen viimeisillä sivuilla on määritelty keskeisimmät ohjeessa käytetyt käsitteet sekä lyhenteet.

Tietosuojavaltuutetun toimisto on laatinut tämän ohjeen liitteeksi Excel-muodossa olevan kirjaamistyökalun, jota voi käyttää vaikutustenarvioinnin tekemisessä (liite I). Työkalu on yksinkertainen perusmalli, ja sen käyttö on vapaaehtoista. Organisaatioita kannustetaan muokkaamaan työkalua vastaamaan paremmin niiden omiin tarpeisiin.

Tätä ohjetta voi soveltuvin osin käyttää myös rikosasioiden tietosuojalain 20 §:ssä tarkoitetun vaikutustenarvioinnin tekemiseen. Liitteessä II annetaan tästä lisätietoja.





## 1 Kuvaus henkilötietojen käsittelystä (kontekstin hahmottaminen)

Vaikutustenarvioinnin ensimmäisessä vaiheessa yksilöidään ja rajataan arvioinnin kohde ja muodostetaan yleiskuva henkilötietojen käsittelystä. Lähtökohtana voi olla suunnitelma tai kuvaus siitä, mitä henkilötietojen käsittelyllä tavoitellaan, jolloin käsittelyn toteuttamistapa ja suojoitoimenpiteiden yksityiskohdat täydentyvät vaikutustenarvioinnin edetessä. Tällöin vaikutustenarvioinnin vaiheita voidaan joutua toistamaan siten, että päästään riittävän yksityiskohtaiselle tasolle. Kuvauksesta tulisi ilmetä henkilötietojen käsittelyn luonne, laajuus, asiayhteys sekä tarkoitukset.

Tietovuokaavion laatiminen auttaa hahmottamaan tietojen liikkumista. Mahdollinen kaavio on suositeltavaa liittää tietosuojan vaikutustenarviointiin. Kaaviota voi hyödyntää myös jäljempänä uhkien tunnistamista koskevassa osiossa (ks. luku 3.2).

Kun laadit kuvausta henkilötietojen käsittelystä, määrittele seuraavat seikat:

- **Henkilötietojen käsittelyn tarkoitus ja tavoite:** Missä yhteydessä henkilötietoja käsitellään? Mitkä rekisteröityjen oikeudet ja vapaudet käsittelyyn liittyvät? Mitä käsittelyllä halutaan saada aikaiseksi ja miksi henkilötietoja tarvitaan näiden tarkoitusten toteuttamiseen?
- **Henkilöt, joiden tietoja käsittely koskee (rekisteröidyt):** Keiden henkilöiden tietoja käsitellään? Mikä on rekisterinpitäjän suhde/yhteys rekisteröityihin? Käsitelläänkö rekisterinpitäjään nähden heikommassa asemassa olevien henkilöiden tietoja (esim. ikääntyneet, lapset, työntekijät, potilaat)? Voivatko alaikäisiä koskevat tiedot tulla käsittelyn kohteeksi? Huomioi eri rekisteröityjen ryhmät (esim. työntekijät ja asiakkaat). Kuinka paljon rekisteröityjä on? Minkälaisen maantieteellisen alueen käsittely kokonaisuudessaan kattaa?
- **Roolit ja vastuut:** Yksilöi rekisterinpitäjä(t) eli ne tahot, joilla on valta ja vastuu määrätä henkilötietojen käsittelyn tarkoituksista ja keinoista. Pohdi, tuleeko kyseeseen yhteisrekisterinpitäjyys (ks. artikla 26). Yksilöi myös käsittelyyn liittyvät henkilötietojen käsittelijä(t).
- **Henkilötiedot:** Mitä henkilötietotyyppisiä käsitellään? Käsitelläänkö erityisiä henkilötietoryhmiä, rikostuomioita ja rikkomuksia koskevia tietoja tai henkilötunnuksia? Huomioi myös tekniset tiedot, jotka luetaan henkilötiedoiksi (arvioi esim. lokitiedot, verkkotunnistetiedot).
- **Käsiteltävien henkilötietojen määrä:** Kuinka suuria määriä henkilötietoja käsitellään? Huomioi erilaiset henkilötietoryhmät.
- **Käsiteltävien tietojen maantieteellinen laajuus:** Missä maissa tietoja käsitellään? Käsitelläänkö tietoja näiden maiden ulkopuolella?
- **Henkilötietojen elinkaari:** Mistä tiedot kerätään tai hankitaan (tietolähteet)? Kuinka kauan tietoja säilytetään (henkilötietojen säilytysajat ja niiden määräytymisen perusteet)? Kenelle tietoja luovutetaan (tietojen vastaanottajat)?
- **Tekninen toteutus:** Mitä tietoteknisiä resursseja ja toiminnallisuuksia suunniteltu käsittely edellyttää? Onko vaihtoehtoisia toteutustapoja arvioitu tietosuojan ja tietoturvan näkökulmasta? Huomioi henkilötietojen elinkaaren hahmottamisessa myös rajapinnat, käyttöliittymät, palvelimet, konesalit, käyttäjäryhmät sekä käyttövaltuudet ym.



## 2 Tietosuojasääntelyn noudattamisen arviointi

Ennen henkilötietojen käsittelyyn liittyvien riskien arvioimista on varmistuttava henkilötietojen käsittelyä koskevan lainsäädännön noudattamisesta. Tässä vaiheessa kuvataan, millä tavalla TSA:sta sekä muusta toimintaan sovellettavasta henkilötietojen käsittelyä koskevasta lainsäädännöstä johdettavat vaatimukset toteutetaan. Huomaa, että tässä ohjeessa ei avata toimialakohtaisesta sääntelystä tulevia velvoitteita.

Tämän jakson mukainen arvio tietosuojaperiaatteiden ja rekisteröidyn oikeuksien noudattamisesta on tarpeen tehdä aina, kun henkilötietoja käsitellään riippumatta siitä, liittyykö käsittelyyn myös velvollisuus vaikutustenarvioinnin tekemisestä.

### 2.1 Tietosuojaperiaatteiden noudattaminen

#### 2.1.1 Yleinen arvio suunnitellun käsittelyn tarpeellisuudesta ja oikeasuhteisuudesta

Tietosuojan vaikutustenarvioinnissa tulee olla arvio siitä, että suunniteltu henkilötietojen käsittely on tarpeellista ja oikeasuhtaista käsittelyn laillisten tarkoitusten saavuttamiseksi ts. käsittely vastaa tehokkaasti tähän tarpeeseen ja se puuttuu vähiten rekisteröidyn yksityisyyteen ja henkilötietojen suojaan. Henkilötietoja olisi käsiteltävä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoilla.

Arvioi suunnitellun käsittelyn tarpeellisuutta ja oikeasuhteisuutta. Pohdi ainakin seuraavia kysymyksiä:

- Miksi käsittelytoimet ovat tehokas keino organisaatiollesi esimerkiksi sille osoitetun tehtävän tai sopimuksen täyttämiseksi taikka sen tarjoaman palvelun toteuttamiseksi?
- Onko olemassa muita, henkilötietojen suojaan vähemmän puuttuvia keinoja saman tavoitteen saavuttamiseksi?
- Miksi käsittelyn laajuutta tai keinoja voidaan pitää oikeasuhtaisena kyseisen tehtävän/tarkoituksen saavuttamiseksi? Vertaa käsittelyn etuja sen potentiaalisesti aiheuttamiin riskeihin rekisteröidyille. On mahdollista, että lähtökohtaisesti tarpeelliselta vaikuttavaan henkilötietojen käsittelyyn liittyvät riskit ovat niin korkeita, ettei käsittelyä voida pitää oikeasuhtaisena.

Kun vaikutustenarviointia päivitetään, on hyvä tarkistaa, onko toteutetulla henkilötietojen käsittelyllä saavutettu sille asetetut tavoitteet siten, että käsittelytoimia voidaan edelleenkin pitää tarpeellisina ja oikeasuhteisina.

Jos suunniteltu käsittely ei ole tarpeellista ja oikeasuhteista, ei käsittelyä voida toteuttaa sellaisenaan. Tällöin myöskään vaikutustenarvioinnin jatkaminen ei ole tarpeen, ellei suunnitelmaa muuteta.

#### 2.1.2 Tietosuojaperiaatteiden noudattaminen

Jotta tietosuojaperiaatteiden noudattamista voidaan kattavasti arvioida, on selvítettävä tietosuojan vaikutustenarvioinnin kohteena olevaan käsittelyyn soveltuva tietosuojalainsäädäntö. Toimialakohtainen lainsäädäntö on otettava huomioon kautta linjan. Tietosuojaperiaatteet on voitu ottaa



huomioon jo henkilötietojen käsittelyä koskevaa lainsäädäntöä valmisteltaessa. Esimerkiksi käsittelyperusteesta, käsiteltävistä henkilötiedoista sekä tietojen käyttötarkoituksista ja luovutusperusteista on voitu säätää laissa.

**Soveltuva sääntely:** Määrittele vaikutustenarvioinnin kohteeseen soveltuva sääntely: TSA, tietosuojalaki ja mahdollinen henkilötietojen käsittelyä koskeva muu lainsäädäntö. Ota huomioon myös mahdolliset TSA 40 artiklan mukaiset käytännesäännöt ja 42 artiklan mukaiset sertifiointit, jos sellaiset tulevat tapauksessa sovellettaviksi.

[Tietosuojaperiaatteet](#)<sup>4</sup> ilmenevät tietosuojasetuksen 5 artiklasta. Periaatteita on kuusi, ja niiden mukaan henkilötietoja on:

- [käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi](#)<sup>5</sup>
- [kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten](#)<sup>6</sup>
- [kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden](#)<sup>7</sup>
- [päivitettävä aina tarvittaessa: epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä](#)<sup>8</sup>
- [säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten](#)<sup>9</sup>
- [käsiteltävä luottamuksellisesti ja turvallisesti](#)<sup>10</sup>.

### 2.1.3 Lainmukaisuus (käsittelyperuste) ja kohtuullisuus

Jotta henkilötietoja voidaan käsitellä, on käsittelylle oltava lainmukainen peruste. Käsittelyperusteista säädetään TSA:n 6 artiklassa ja sitä täydentävässä tietosuojalain 4 §:ssä, sekä erityisiin henkilötietoryhmiin kuuluvien tietojen osalta TSA:n 9 artiklassa ja tietosuojalain 6 §:ssä. Lisäksi rikostuomioita tai rikkomuksia koskevien tietojen käsittelystä säädetään TSA:n 10 artiklassa, ja henkilötunnuksen käsittelystä tietosuojalain 29 §:ssä. Vastaavasti rikosasioiden tietosuojasäännösten perusteella tehtävässä vaikutustenarvioinnissa käsittelyn tulee perustua kansalliseen RTsL:n ja/tai sitä yksityiskohtaisempaan viranomaista koskevaan erityislakiin (esim. laki henkilötietojen käsittelystä poliisitoimessa 616/2019).

#### [Lisätietoa käsittelyperusteista](#)<sup>11</sup>

Jos toimialakohtaisessa lainsäädännössä säädetään henkilötietojen käsittelystä, on tätä sääntelyä noudatettava.

<sup>4</sup> <https://tietosuoja.fi/tietosuojaperiaatteet>

<sup>5</sup> <https://tietosuoja.fi/lainmukaisuus-asianmukaisuus-lapinakyvyys>

<sup>6</sup> <https://tietosuoja.fi/kayttotarkoitussidonnaisuus>

<sup>7</sup> <https://tietosuoja.fi/tietojen-minimointi>

<sup>8</sup> <https://tietosuoja.fi/tietojen-tasmallisyys>

<sup>9</sup> <https://tietosuoja.fi/sailytyksen-rajoittaminen>

<sup>10</sup> <https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus>

<sup>11</sup> <https://tietosuoja.fi/kasittelyperusteet>



Jos käsittelyn osapuolet on tunnistettu yhteisrekisterinpitäjiksi, on varmistettava, että niiden välinen vastuunjako on vahvistettu, ja järjestelyn keskeiset osat ovat rekisteröidyn saatavilla TSA:n 26 artiklan mukaisesti.

Kun arvioit käsittelyperusteen olemassaoloa sekä käsittelyn lainmukaisuutta ja kohtuullisuutta, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Mikä on henkilötietojen käsittelyperuste tai -perusteet?
- Jos kyseessä on oikeutettu etu, onko käsittelyperusteeseen liittyvät mahdolliset harkinta- ja dokumentointivelvoitteet huomioitu (esim. oikeutetun edun tasapainotesti)?
- Jos käsittely perustuu suostumukseen, onko suostumus vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu?
- Onko suostumuksen peruuttaminen tehty yhtä helpoksi kuin sen antaminen?
- Jos kyseessä ovat erityiset henkilötietoryhmät (9 artikla), mikä on soveltuva poikkeusperuste niiden käsittelylle? (9 artiklan 2 kohta, tietosuojalain 6 §)
- Jos käsitellään rikostuomioita ja rikkomuksia ja niihin liittyviä turvaamistoimia koskevia tietoja, täytyvätkö niiden käsittelyn edellytykset (10 artikla, tietosuojalain 7 §)?
- Jos käsitellään henkilötunnuksia, täytyvätkö henkilötunnusten käsittelyn edellytykset (tietosuojalain 29 §)?
- Sovelletaanko toimintaan sellaista erityislainsäädäntöä, jossa säädetään henkilötietojen käsittelystä? Jos kyllä, miten tämän lainsäädännön noudattaminen on varmistettu?
- Millä tavalla käsittely vastaa rekisteröityjen perusteltuja odotuksia?

### 2.1.2 Läpinäkyvyys (rekisteröityjen informointi)

Rekisterinpitäjän on kerrottava rekisteröidyille henkilötietojen käsittelystä selkeästi ja ymmärrettävästi. Tästä yleisestä informoinnista on joitakin poikkeuksia (ks. TSA art. 13.4 ja tietosuojalaki 33 §)

Informoinnin tarkemmat vaatimukset riippuvat osittain siitä, kerätäänkö tietoja henkilöltä itseltään vai muualta. Informoinnin tarkempia vaatimuksia ovat:

- [tietosisältö](#)<sup>12</sup>
- [esittämistapaa koskevat vaatimukset](#)<sup>13</sup>
- [jakelua ja toimittamistapaa koskevat vaatimukset](#)<sup>14</sup>
- [ajankohtaa koskevat vaatimukset](#)<sup>15</sup>

Kun arvioit näiden vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Miten ja missä yhteydessä rekisteröidyille kerrotaan henkilötietojen käsittelystä? Missä vaiheessa palvelupolkua käsittelystä kerrotaan?
- Saako rekisteröity kattavasti tietoa käsittelystä, jotta hän voi varmistaa henkilötietojensa tehokkaan suojan?
- Mistä tiedot löytyvät? Ovatko ne helposti rekisteröidyn saatavilla?

<sup>12</sup> <https://tietosuoja.fi/documents/6927448/8214536/Informointivelvoitteen+edellytt%C3%A4m%C3%A4t+tiedot/419957bd-fd5a-4090-9c64-cf4769b10570/Informointivelvoitteen+edellytt%C3%A4m%C3%A4t+tiedot.pdf>

<sup>13</sup> <https://tietosuoja.fi/rekisteroidyn-informointi>

<sup>14</sup> <https://tietosuoja.fi/oikeus-saada-tietoa-kasittelysta>

<sup>15</sup> <https://tietosuoja.fi/oikeus-saada-tietoa-kasittelysta>



- Onko rekisteröidylle tarjottu tieto ymmärrettävää kohdeyleisön näkökulmasta (esim. lapset)?
- Esitetäänkö tiedot ymmärrettävästi? Onko tietojen esittämistavassa hyödynnetty kerroksellisuutta tai muuta tapaa, jolla luettavuutta voidaan helpottaa?
- Miten informaation ajantasaisuudesta huolehditaan?
- Jos rekisteröityjä ei informoida tai informointia lykätään, miten tämä perustellaan?

### 2.1.3 Käyttötarkoitussidonnaisuus

#### Käyttötarkoituksen yksilöinti etukäteen

Henkilötietojen käsittelyn tarkoitus tai tarkoitukset on suunniteltava ja määritettävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tiettyssä, nimenomaisessa ja laillisessa tarkoituksessa. Tämä edellyttää käyttötarkoitusten yksilöintiä ja perustelemista. Tiettyä tarkoitusta varten kerätyt henkilötietoja ei saa käsitellä tarkoituksiin, jotka eivät ole yhteensopivia alkuperäisen käyttötarkoituksen kanssa.

Käyttötarkoitus vaikuttaa muihin periaatteisiin, jotka kohdistuvat käsiteltäviin tietoihin. Näitä periaatteita ovat esimerkiksi tietojen minimointi, säilytysaikojen rajoittaminen, tietojen täsmällisyys sekä myöhemmän käsittelyn yhteensopivuus. Tästä syystä henkilötietojen käsittelyn tarkoitukset on etukäteen yksilöitävä. Tarkoitusten tulee olla yksilöityjä, nimenomaisia ja laillisia.

Rekisterinpitäjä kuvaa käsittelyn tavoitteet oman toimintansa kannalta. Hyvin yleisluontoinen kuvaus käsittelytarkoituksesta ei ole riittävä, vaan käsittelytarkoitus on määriteltävä riittävän täsmällisesti, jotta käyttötarkoituksen yksilöinnin ja nimenomaisuuden vaatimus täyttyy. Rekisteröidyn on pystyttävä muodostamaan määrittelyn perusteella riittävän täsmällinen käsitys siitä, mihin henkilötietoja aiotaan käyttää.

#### Myöhemmän käsittelyn yhteensopivuus

Käyttötarkoitus sitoo myöhempiä käsittelyä siten, että sen tulee olla yhteensopivaa alkuperäisen käyttötarkoituksen kanssa. Muun käsittelyn yhteensopivuuden arvioinnista säädetään TSA 6 artiklan 4 kohdassa. Henkilötietojen käsittely tilastoinnin, tieteellisen tutkimuksen ja yleisen edun mukaisesti arkistointitarkoituksiin on yhteensopivaa, jos noudatetaan asianmukaisia suojatoimia. Lisäksi rekisteröidyn suostumus tai erityislainsäädäntö voivat oikeuttaa käsittelyn muuhun tarkoitukseen.

[Lisätietoa käyttötarkoitussidonnaisuudesta tietosuojavaltuutetun toimiston verkkosivuilla](https://tietosuoja.fi/kayttotarkoitussidonnaisuudesta-tietosuojavaltuutetun-toimiston-verkkosivuilla)<sup>16</sup>.

Kun arvioit tämän periaatteen noudattamista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Mitkä ovat henkilötietojen käsittelyn tarkoitukset? Kuvaa suunnitellun käsittelyn tavoitteita rekisterinpitäjän toiminnan kannalta.
- Mihin käsittelyllä pyritään?
- Ovatko käyttötarkoitukset lainmukaisia ja selkeästi yksilöityjä?
- Miten käsittelytarkoitukset on dokumentoitu?

<sup>16</sup> <https://tietosuoja.fi/kayttotarkoitussidonnaisuus>



- Miten varmistetaan siitä, että käsittely pysyy käyttötarkoituksen tai -tarkoitusten mukaisena?
- Onko tietojen käsittelyä muihin tarkoituksiin rajattu teknisin ja/tai organisatorisin keinoin (esim. tietojen salaaminen, hajautus, ohjeistukset, sopimusvelvoitteet)? Kuvaile, millä tavalla.
- Millä perusteella mahdollista jatkokäsittelyä voidaan pitää yhteensopivana alkuperäisen käsittelytarkoituksen kanssa?
- Onko käsittelyn tarkoitus rekisteröidylle riittävän ennalta-arvattavaa ottaen huomioon rekisteröidyn oikeudet odotukset sekä käsittelystä annettava informaatio?

#### 2.1.4 Tietojen minimointi ja säilytyksen rajoittaminen

Tiedon minimoinnilla tarkoitetaan rekisteröidyistä kerättävien ja käsiteltävien tietojen määrän minimointia<sup>17</sup>. Henkilötietoja saa käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta. Sen arvioimiseksi, mitkä tiedot katsotaan asianmukaisiksi ja olennaisiksi, on selkeästi tunnistettava se syy, miksi kyseisiä henkilötietoja tarvitaan. Jos käsittelyn tarkoitus, esimerkiksi palvelun toteuttaminen, on mahdollista tehdä siten, että tiettyjä tietoja ei käsitellä, ei henkilötietojen käsittely niiltä osin ole tarpeellista eikä henkilötietoja tule silloin käsitellä. Henkilötietoja ei saa kerätä tai käsitellä laajemmin kuin on tarpeellista käyttötarkoituksen kannalta. Kerättävien ja käsiteltävien tietojen tarpeellisuus tulee myös perustella.

[Lisätietoa tietojen minimoinnista](#)<sup>18</sup>.

Kun arvioit näiden vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

Minimointivaatimus henkilötietojen käsittelyssä:

- Mihin tarkoituksiin tietoja kerätään?
- Onko käsittelyn tarkoitus mahdollista toteuttaa ilman näitä tietoja?
- Kuvaako kerätty tieto sitä ominaisuutta, jota on tarkoitus arvioida?
- Miten on huolehdittu siitä, että tietoja ei kerätä "varmuuden vuoksi"?
- Onko kerättävien ja säilytettävien tietojen tarpeellisuus perusteltu?
- Onko mahdollista käyttää pseudonymisointia? Jos on, säilytetäänkö yhdistämisen mahdollistavat lisätiedot erikseen?

Minimointivaatimus tietojärjestelmien suunnittelussa:

- Onko lomakkeissa käytössä vapaakenttiä? Onko niiden käyttäminen välttämätöntä? Onko vapaa-kenttien täyttäminen ohjeistettu siten, ettei niihin täytetä tarpeettomia tietoja?
- Onko vapaaehtoiset ja pakolliset tietokentät merkitty riittävällä tavalla? Ovatko vapaaehtoiset tietokentät välttämättömiä käsittelyn tavoitteen kannalta?
- Miten on varmistettu, että henkilötietojen käsittelystä ei synny/jää tarpeettomia kopioita?
- Miten on varmistettu, että järjestelmä ei kerää tarpeettomia tietoja? Syntykö väliaikaisia tiedostoja – jos syntyy, onko pääsy niihin rajattu ja huolehditaanko niiden poistamisesta?
- Miten on varmistettu, että henkilötietojen pääsy- ja käyttöoikeudet ovat rajoitettavissa?
- Miten käyttöoikeuksia hallitaan henkilöiden vaihtuessa?
- Onko henkilötietojen pääsy- ja käyttöoikeudet rajoitettu minimiin?

<sup>17</sup> Yleisen tietosuojasetuksen 5 artiklan 1 kohdan c alakohta. Lisätietoja EDPB:n Guidelines 4/2019 on article 25 Data Protection by Design and by Default s. 19-20.

<sup>18</sup> <https://tietosuoja.fi/tietojen-minimointi>



Henkilötietoja saa säilyttää vain niin kauan kuin ne ovat tarpeen henkilötietojen käyttötarkoitusta varten. Säilytyksen rajoittaminen on yhteydessä tietojen minimoinnin periaatteeseen: henkilötietojen käsittely tulee minimoida myös ajallisesti. TSA:ssa ei ole määritelty tarkkoja henkilötietojen säilytysaikoja. Henkilötietojen säilytysaikaan voi vaikuttaa myös muu soveltuva lainsäädäntö. Lainsäädännöstä voi seurata erilaisia kanneajoja, jotka on otettava huomioon säilytysaikoja määriteltäessä. Lainsäädännössä on myös voitu asettaa tietyille tiedoille vähimmäis- tai enimmäissäilytysajat sekä vaatimus siitä, että tiedot tulee poistaa tietyn ajan kuluessa.

Rekisterinpitäjän on arvioitava henkilötietojen tarpeellisuutta suhteessa kysymyksessä olevaan käyttötarkoitukseen. Ellei tarkkaa päättymisaikaa ole mahdollista määritellä, käsittelyn kesto on syytä ilmaista muulla myöhemmin seurattavissa olevalla tavalla. Henkilötietojen säilytysajat on syytä dokumentoida, jotta säilytyksen rajoittamista koskevan periaatteen noudattaminen voidaan osoittaa.

Kun henkilötietoja ei enää tarvita, ne tulee poistaa tai muuttaa pysyvästi sellaiseen muotoon, ettei niistä voi enää tunnistaa yksittäistä henkilöä.

Lue lisää [säilytyksen rajoittamisesta](#)<sup>19</sup> ja [aineiston hävittämisestä](#)<sup>20</sup>.

Kun arvioit näiden vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Mihin tarkoituksiin tietoja käsitellään ja miten kauan niiden käsittely on tarpeellista näihin tarkoituksiin?
- Onko tietojen säilytysajat rajoitettu minimiin?
- Tarkastellaanko tarpeellisuutta säännöllisesti ja poistetaanko mahdolliset tarpeettomat tiedot?
- Soveltuuko käsiteltäviin tietoihin lainsäädäntöä, joka vaatii tai ohjaa säilyttämään tietoja tietyn ajan?
- Mistä ajankohdasta tietojen säilytysaika alkaa kulua ja koska se päättyy?
- Koskeeko eri tietoja tai tietoryhmiä eri säilytysajat?
- Voidaanko eri osien säilytyskaudet erottaa toisistaan?
- Miten tiedot poistetaan?
- Miten henkilötietojen poistaminen käytännössä toteutetaan: kuka poistaa, miten ja milloin?
- Onko mahdollista ottaa käyttöön automaattinen tietojen hävittäminen säilytysajan päättyessä, vai toteutetaanko poistaminen manuaalisesti?
- Miten hävittäminen toteutetaan varmuuskopioiden ja lokitietojen osalta?
- Miten säilytysaikojen ja poistamisprosessien noudattamista seurataan?
- Ovatko henkilötiedot anonymisoitavissa (edes käsittelyn loppuvaiheessa)?
- Jos henkilötiedot poistamisen sijaan anonymisoidaan, miten varmistetaan, että anonymisointi toteutetaan TSA:n edellyttämällä tavalla?
- Miten huolehditaan siitä, ettei henkilöitä voida enää uudelleen tunnistaa tiedoista?

### 2.1.5 Tietojen täsmällisyys

Käsiteltävien henkilötietojen pitää olla käyttötarkoituksen kannalta täsmällisiä. Tiedot on päivitettävä tarvittaessa. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava viipymättä.

<sup>19</sup> <https://tietosuoja.fi/sailytyksen-rajoittaminen>

<sup>20</sup> <https://tietosuoja.fi/aineiston-havittaminen-anonymisointi-tai-arkistointi-tutkimuksen-paattyessa>



Lue lisää [tietojen täsmällisyydestä](#)<sup>21</sup>.

Kun arvioit täsmällisyyteen liittyvien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Ovatko tiedot luonteeltaan staattisia vai edellyttävätkö ne päivittämistä?
- Miten varmistetaan, että käsitellyt henkilötiedot ovat täsmällisiä, ajan tasalla ja paikkansa pitäviä?
- Miten varmistetaan, että epätarkat ja virheelliset tiedot poistetaan tai oikaistaan viipymättä?
- Miten tietoja päivitetään? Kuinka ajantasaisuutta valvotaan?
- Kuinka usein tietojen paikkansa pitävyyttä arvioidaan? Esimerkiksi säännöllisesti, tarvittaessa, jne.
- Miten rekisteröity voi vaikuttaa tietojen täsmällisyyteen ja päivittää tietoja tarvittaessa?
- Miten varmistetaan kolmannelta osapuolelta vastaanotetun tiedon täsmällisyys?
- Miten varmistetaan, että kerätyt tiedot koskevat oikeaa henkilöä?

### 2.1.6 Henkilötietojen käsittelyn turvallisuus (luottamuksellisuus, eheys ja käytettävyys)

Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseksi.

Luottamuksellisuudella tarkoitetaan sitä, että henkilötietojen tulisi olla ainoastaan sellaisten henkilöiden saatavilla, joilla on työtehtäviensä edellyttämä tarve ja oikeus saada pääsy tietoihin. Henkilötiedot on suojattava niin, että niitä ei pääse katselemaan tai muuten käsittelemään luvottomasti. Henkilötietojen luottamuksellisuuden loukkaukset voivat aiheuttaa yksilöille erilaisia haittoja ja vahinkoja kuten henkistä kärsimystä, jos terveydentilatiedot päätyvät sivullisten saataville, tai taloudellista vahinkoa, jos vuotaneita henkilötietoja käytetään oikeudettomasti identiteettivarkauden tekoon. Tämän välttämiseksi henkilötietojen käsittely on suunniteltava siten, että tiedot on suojattu luvottomalta pääsylvä ja oikeudettomalta käytöltä niin tietojen käsittelyn, siirron kuin säilytyksenkin aikana.

Eheys tarkoittaa tietojen muuttumattomuutta niitä käsiteltäessä, siirrettäessä ja säilytettäessä. Henkilötietoja on siis suojeltava siltä, että ne tahallisesti tai vahingossa kadotetaan, tuhotaan tai niitä muokataan oikeudettomasti. Puutteet henkilötietojen eheydessä voivat vaikuttaa henkilöihin, jos heitä koskevat päätökset tehdään virheellisten tai oikeudettomasti muutettujen tietojen perusteella. Näiltä osin henkilötietojen eheys linkittyy henkilötietojen täsmällisyyden periaatteeseen (ks. luku 2.1.5).

Vaikka tietojen käytettävyyttä ei erikseen mainita tietosuojaperiaatteiden yhteydessä, on sekin otettu huomioon TSA:ssa eri yhteyksissä. Rekisterinpitäjän on varmistettava, että henkilötiedot ovat käytettävissä silloin, kun niitä tarvitaan. Henkilötietoja on siis suojeltava siltä, että jokin vahingossa tai tahallisesti, tilapäisesti tai pysyvästi estää henkilötietojen käytön suunniteltuun tarkoitukseen. Tällaiset tilanteet voivat vaikuttaa myös asianomaisiin henkilöihin siten, ettei esimerkiksi kyseinen palvelu ja siihen liittyvä oikeus tai vapaus ole käytettävissä (esim. palkanmaksu ei onnistu

<sup>21</sup> <https://tietosuoja.fi/tietojen-tasmallisyys>





eikä työ sopimuksen mukaisia korvauksia työsuorituksista voida maksaa tai tilisiirrot eivät onnistu eikä niihin perustuva vaihdanta toimi).

Tietosuojasetuksessa ei ole määritelty tarkasti sitä, millaisia teknisiä ja organisatorisia toimenpiteitä rekisterinpitäjien ja henkilötietojen käsittelijöiden tulee kulloinkin toteuttaa. Toimenpiteiden voidaan ymmärtää kattavan laajasti kaikki tavat ja keinot, jotka rekisterinpitäjä voi toteuttaa käsittelyn yhteydessä. Asianmukaisuudella tarkoitetaan sitä, että nämä keinot ovat toimivia ja riittävän tehokkaita. Tekninen tai organisatorinen toimenpide kattaa laajasti erilaiset toimet teknisten ratkaisujen käytöstä työntekijöiden kouluttamiseen.

Oikeudettomien muutosten välttämiseksi tietojärjestelmä on suunniteltava siten, että vain oikeutetut käyttäjät voivat muuttaa tietoja ja tällaisetkin muutokset lokitetaan mahdollista jälkeenpäin tapahtuvaa selvittämistä varten. Lokitiedot ovat yksi keino toteuttaa käytönvalvontaa ja edesauttaa mahdollisten poikkeamisten havaitsemista ja niihin puuttumista. Käytettävyyttä ja eheyttä voidaan tukea esimerkiksi huolehtimalla asianmukaisesta varmuuskopioinnista.

Rekisterinpitäjiltä edellytetään teknologisen kehityksen seuraamista ja teknisten sekä organisatoristen suoja-toimenpiteiden päivittämistä tarpeen mukaan niiden tehokkuuden takaamiseksi.

Lisätietoja tietosuojaperiaatteiden huomioonottamisesta eri teknisissä ja organisatorisissa toimenpiteissä on esitetty [ohjeessa 04/2019 oletusarvoisesta ja sisäänrakennetusta tietosuojasta<sup>22</sup>](#).

Arvioidessasi näiden periaatteiden toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Minkälaisia henkilötietojen **luottamuksellisuutta** edistäviä toimenpiteitä organisaatiossa on jo käytössä ja missä määrin niihin voidaan tukeutua arvioitavassa käsittelyssä?
- Minkälaisia henkilötietojen **eheyttä** edistäviä toimenpiteitä organisaatiossa on jo käytössä ja missä määrin niihin voidaan tukeutua arvioitavassa käsittelyssä?
- Minkälaisia henkilötietojen **käytettävyyttä** edistäviä toimenpiteitä organisaatiossa on jo käytössä ja missä määrin niihin voidaan tukeutua arvioitavassa käsittelyssä?
- Onko organisaatiossa käytössä menettelytapa, jolla henkilötietoihin ja niihin käsittely- ja siirtojärjestelmiin liittyviä turvallisuusuhkia tunnistetaan ja analysoidaan säännöllisesti?
- Onko organisaatiolla kyky havainnoida mahdollisia henkilötietojen turvallisuuteen kohdistuvia tietoturvaloukkauksia?
- Onko tietoturvaloukkauksiin reagoimiseen olemassa prosessi ja menettelytavat (ml. loukkausten ilmoituskanava ja riskiarviointi koskien ilmoitusvelvollisuutta tietosuojaviranomaiselle/rekisteröidylle)?
- Miten henkilötietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaavien toimenpiteiden asianmukaisuus ja riittävyys varmistetaan myös tulevaisuudessa?

## 2.2 Henkilötietojen käsittelijät

**Henkilötietojen käsittelijä** toimii rekisterinpitäjän ohjeiden mukaisesti sen puolesta tai sen lukuun.

<sup>22</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_201904\\_dataprotection\\_by\\_design\\_and\\_by\\_default\\_v2.0\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf)



**Rekisterinpitäjä** määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet niin, että käsittely täyttää TSA:n vaatimukset.

Huomaa, että henkilötietojen käsittelijällä ei tarkoiteta rekisterinpitäjän alaisuudessa toimivia työntekijöitä, jotka käsittelevät henkilötietoja osana työtehtäviään. Lisätietoja rekisterinpitäjän ja henkilötietojen käsittelijän roolien määrittämisestä ja velvollisuuksista löydät [Euroopan tietosuojaneuvoston ohjeistuksesta](#)<sup>23</sup>.

Tietosuojasetuksessa säädetään suoria velvoitteita henkilötietojen käsittelijöille. Henkilötietojen käsittelijän on avustettava ja neuvottava rekisterinpitäjää tiettyjen tietosuojasetuksessa määriteltyjen velvoitteiden noudattamisessa. Näitä velvoitteita ovat muun muassa tietosuoja koskevat vaikutustenarvioinnit, ilmoitukset henkilötietojen tietoturvaloukkauksista ja auditointeihin osallistuminen.

Henkilötietojen käsittelijän on lisäksi toteutettava riittävät suojatoimet sekä asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi. Rekisterinpitäjän velvollisuutena on osoittaa, että tietosuojaperiaatteet toteutuvat tehokkaasti myös niiltä osin, kun henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun.

Lue lisää [henkilötietojen käsittelijöiden velvollisuuksista](#)<sup>24</sup>.

Kun arvioit henkilötietojen käsittelijän käyttöön liittyvien vaatimusten täyttymistä, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Onko käsittelyssä mukana henkilötietojen käsittelijöitä? Tunnista käsittelijät.
- Täyttävätkö käytetyt henkilötietojen käsittelijät niille asetetut kriteerit (TSA art.28.1)? Miten tämä varmistetaan?
- Onko henkilötietojen käsittelystä laadittu sopimus, joka täyttää tietosuojasetuksen 28 artiklan vaatimukset?
- Onko henkilötietojen käsittelijöille annettu muut tarpeelliset dokumentoidut ohjeet? Miten ohjeiden toimitustavasta ja muutoksista on sovittu osapuolten kesken?

### 2.3 Henkilötietojen siirrot ETA-alueen ulkopuolelle

Henkilötietoja saa TSA:n nojalla siirtää Euroopan talousalueen (ETA:n) ulkopuolelle tai kansainvälisille järjestöille vain TSA:n V luvussa määritellyin edellytyksin. V luvun säännösten tarkoituksena on varmistaa, että tietosuojan taso säilyy olennaisilta osin samanlaisena kuin ETA-alueella, kun henkilötietoja siirretään kolmanteen maahan tai kansainväliselle organisaatiolle.

Huomioi myös henkilötietojen käsittelijöiden (esimerkiksi pilvipalveluiden tarjoajien) osalta, missä henkilötiedot fyysisesti sijaitsevat. Esimerkiksi palveluntarjoajana toimivan henkilötietojen käsittelijän pääsy etäyhteydellä henkilötietoihin ETA:n ulkopuolelta katsotaan henkilötietojen siirroksi ETA-alueen ulkopuolelle.

<sup>23</sup> [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor\\_fi](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_fi)

<sup>24</sup> <https://tietosuoja.fi/henkilotietojen-kasittelijat>



Jos komissio on tehnyt kyseisestä maasta tai kansainvälisestä järjestöstä tietosuojan riittävyttä koskevan päätöksen<sup>25</sup>, voit siirtää henkilötietoja samoin edellytyksin kuin ETA-alueen sisällä, eikä erillistä siirtoerustetta edellytetä. Huomaa kuitenkin, että komission päätös voi olla rajattu ainoastaan tiettyyn kolmannen maan alueeseen tai yhteen tai useampaan tiettyyn sektoriin (esim. Kanadaa koskeva päätös koskee ainoastaan kaupallisia organisaatioita). Lisäksi kolmansissa maissa ja kansainvälisissä organisaatioissa tapahtuva kehitys voi aiheuttaa muutoksia päätöksiin. Mikäli henkilötietoja siirretään kolmansiin maihin tai kansainväliselle organisaatiolle eikä komissio ole tehnyt tietosuojan riittävyttä koskevaa päätöstä kyseisestä maasta tai kansainvälisestä organisaatiosta, varmista soveltuva siirtoeruste tietosuoja-asetuksen V luvusta (esim. komission hyväksymät va-kiolausekkeet).

Lisätietoja eri [siirtoerusteista](#)<sup>26</sup> sekä [TSA:n 49 artiklassa säädetyistä poikkeuksista, jotka soveltuvat vain viime kädessä erikseen määritellyissä erityistilanteissa](#)<sup>27</sup>.

Kun kansainväliset henkilötietojen siirrot ja niihin käytettävä(t) siirtoeruste(et) on identifioitu, tietoja siirtävien rekisterinpitäjien ja henkilötietojen käsittelijöiden on tarkistettava tapauskohtaisesti, taa-taanko siirrettäville henkilötiedoille kolmannen maan lainsäädännössä ja/tai käytännössä sellainen henkilötietojen suojan taso, joka vastaa olennaisilta osin ETA-alueen tasoa. Arvioinnissa on otet-tava huomioon siirron tapauskohtaiset olosuhteet, kyseessä olevan kolmannen maan lainsäädäntö sekä käytössä oleva siirtoeruste. Arviointi on osoitusvelvollisuuden myötä dokumentoitava huolel-lisesti. Jos käytettyyn siirtoerusteeseen sisältyvät suojoimet eivät ole riittäviä, niitä voidaan tie-tyissä tilanteissa täydentää teknisillä, organisatorisilla tai sopimus pohjaisilla suojoimilla. Jos käy-tetty siirtoeruste ei riitä takaamaan olennaisilta osin samaa tietosuojan tasoa eikä myöskään so-veltuvia täydentäviä suojoimia löydy riittävän tietosuojan tason takaamiseksi, ei siirtoa tule tehdä.

[Lisätietoja siirtoerusteista täydentävistä suojoimista ja niihin liittyvästä arvioinnista](#)<sup>28</sup>.

Henkilötietojen siirtoja kolmansiin maihin tai kansainvälisille järjestöille voi tapahtua myös toimival-taisten viranomaisten, esimerkiksi Puolustusvoimien, poliisin, tuomioistuimen, Tullin, Rajavartiolaito-ksen ja Rikosseuraamuslaitoksen suorittaessa henkilötietojen käsittelystä rikosasioissa ja kansal-lisen turvallisuuden ylläpitämisen yhteydessä annetun lain (rikosasioiden tietosuojalaki, 1054/2018) 1 §:n mukaisia tehtäviä. Näihin siirtoihin sovelletaan rikosasioiden tietosuojalain 7 luvun säännök-siä, jotka poikkeavat tietosuoja-asetuksen henkilötietojen siirtoa koskevista artikloista.

Kun arviot henkilötietojen kolmansiin maihin siirtämisen lainmukaisuutta, voit hyödyntää seuraavia esimerkikisymyksiä:

<sup>25</sup> Ajantasainen listaus [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_fi](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_fi). Rikosasioiden tietosuojadirektiivin (2016/680; LED) 36 artiklassa tarkoitet-tuja komission vastaavuuspäätöksiä ei ole vielä annettu lukuun ottamatta Iso-Britanniaa koskevaa vastaa-vuus päätöstä (loppuvuosi 2021) ja siten rikosasioiden tietosuoja säännösten soveltamisalalla on kolmansiin maihin siirrossa käytettävä muita RTsL:n siirtoinstrumentteja.

<sup>26</sup> <https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle>

<sup>27</sup> <https://tietosuoja.fi/erityistilanteita-koskevat-poikkeukset>

<sup>28</sup> [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measu-res-supplement-transfer\\_en](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measu-res-supplement-transfer_en), katso myös [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_recommen-dations\\_202002\\_europeanessentialguaranteessurveillance\\_fi.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommen-dations_202002_europeanessentialguaranteessurveillance_fi.pdf)



- Siirretäänkö henkilötietoja EU:n / ETA:n ulkopuolelle tai kansainväliselle organisaatiolle? Jos siirretään, mihin maihin ja/tai mille organisaatioille?
- Onko komissio tehnyt tietosuojan riittävyttä koskevan päätöksen (art. 45) ko. maasta tai kansainvälisestä organisaatiosta?
- Jos ei, mitä suojatoimia henkilötietojen siirroissa ETA:n ulkopuolelle käytetään (art. 46)?
- Riittääkö käytetty siirtomekanismi takaamaan olennaisilta osin saman tietosuojan tason kuin ETA-alueella tekemäsi tapauskohtaisen arvioinnin pohjalta? Jos ei, mitä täydentäviä suojatoimia on otettu käyttöön ja miksi?

## 2.4. Huolehdi rekisteröidyn oikeuksien toteuttamisesta

Rekisterinpitäjän on helpotettava rekisteröidyn tietosuojaoikeuksien käyttämistä sekä tarvittaessa toteutettava tietosuojaoikeudet rekisteröidyn pyynnön mukaisesti.

Tietosuojaoikeuksilla tarkoitetaan yleisen tietosuoja-asetuksen III luvun mukaisia rekisteröidyn oikeuksia. Rekisteröidyllä on oikeus

- [saada tietoa henkilötietojensa käsittelystä<sup>29</sup> \(ks. jakso 2.1.2\)](#)
- [saada pääsy tietoihin<sup>30</sup>](#)
- [oikaista tietoja<sup>31</sup>](#)
- [poistaa tiedot ja tulla unohdetuksi<sup>32</sup>](#)
- [rajoittaa tietojen käsittelyä<sup>33</sup>](#)
- [siirtää tiedot järjestelmästä toiseen<sup>34</sup>](#)
- [vastustaa tietojen käsittelyä<sup>35</sup>](#)
- [olla joutumatta automaattisen päätöksenteon kohteeksi<sup>36</sup>.](#)

Se, mitä oikeuksia rekisteröity voi kulloinkin käyttää, riippuu siitä, millä perusteella kyseessä olevia henkilötietoja käsitellään. Tietosuojavaltuutetun toimiston verkkosivuilla on [taulukko siitä, millä tavalla käsittelyperuste vaikuttaa käytettävissä oleviin oikeuksiin<sup>37</sup>](#).

Määrittele käsittelyperusteen mukaisesti, mitkä tietosuojaoikeudet liittyvät kyseessä olevaan käsittelyyn. Kuvaa, millä tavalla oikeudet otetaan huomioon henkilötietojen käsittelyssä sekä miten oikeuksia koskevat pyynnöt käsitellään ja toteutetaan.

### 2.4.1 Rekisteröidyn oikeuksien toteuttaminen (TSA art. 12)

TSA 12 artiklassa määritellään, millä tavalla tietosuojaoikeuksia koskevat pyynnöt on käsiteltävä. Rekisterinpitäjän on varmistettava, että nämä vaatimukset pyyntöjen käsittelystä toteutuvat.

<sup>29</sup> <https://tietosuoja.fi/oikeus-saada-tietoa-kasittelysta>

<sup>30</sup> <https://tietosuoja.fi/oikeus-saada-paasy-tietoihin>

<sup>31</sup> <https://tietosuoja.fi/oikeus-oikaista-tietoja>

<sup>32</sup> <https://tietosuoja.fi/oikeus-poistaa-tiedot>

<sup>33</sup> <https://tietosuoja.fi/oikeus-rajoittaa-kasittelya>

<sup>34</sup> <https://tietosuoja.fi/oikeus-siirtaa-tiedot>

<sup>35</sup> <https://tietosuoja.fi/oikeus-vastustaa-kasittelya>

<sup>36</sup> <https://tietosuoja.fi/oikeus-olla-joutumatta-automaattisen-paatoksenteon-kohteeksi>

<sup>37</sup> <https://tietosuoja.fi/rekisteroidyn-oikeudet-eri-tilanteissa>



Lue lisää [oikeuksien toteuttamisesta](#)<sup>38</sup>.

Kun arvioit tätä koskevien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Onko olemassa prosessi rekisteröityjen pyyntöjen tunnistamiseksi ja käsittelemiseksi?
- Miten varmistetaan, että TSA:ssa asetettuja pyyntöön vastaamisen määräaikoja noudatetaan?
- Onko henkilökunta koulutettu tunnistamaan rekisteröidyn pyynnöt?
- Onko olemassa vastuuhenkilö rekisteröidyn oikeuksien toteuttamiselle?
- Miten varmistetaan se, että pyynnöt käsitellään oikea-aikaisesti?
- Miten rekisteröityjä avustetaan tietosuojaoikeuksien käytössä?
- Jos rekisteröityä pyydetään täsmentämään pyyntöään, miten varmistutaan siitä, ettei se hankaloita hänen oikeuksiensa toteuttamista?
- Miten rekisteröidyn henkilöllisyys varmistetaan? Onko olemassa menettelyt epäselvien tilanteiden varalta? Miten varmistetaan, ettei tietoja toimiteta väärälle henkilölle?
- Millä kielellä palvelua tarjotaan? Toteutetaanko rekisteröidyn oikeuksia näillä kielillä?
- Onko olemassa lomake tai muu yhteydenottoväylä rekisteröidyn oikeuksien toteuttamiselle? Onko se helposti rekisteröityjen löydettävissä?
- Miten on huolehdittu siitä, että rekisteröidyn oikeuksien toteuttamista koskevat ohjeet ovat helposti rekisteröityjen saatavilla?
- Miten on huolehdittu rekisteröidyn pyyntöjen toteuttamisen dokumentoinnista?
- Missä muodossa tiedot annetaan? Esimerkiksi ääninauha, video, kirjallinen dokumentti jne.
- Miten on varmistuttu siitä, että tiedot toimitetaan rekisteröidylle tietoturvallisesti?

#### 2.4.2 Oikeus saada pääsy tietoihin (TSA art. 15)

Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsittelee tämä häntä koskevia henkilötietoja sekä oikeus saada jäljennös käsiteltävistä tiedoista. Lisäksi rekisteröidylle on annettava informaatiota henkilötietojen käsittelystä. Näin rekisteröidyllä on mahdollisuus arvioida ja varmistaa käsittelyn lainmukaisuus.

Lue lisää [oikeudesta saada pääsy tietoihin](#)<sup>39</sup>.

Kun arvioit tätä oikeutta koskevien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Onko rekisteröidylle mahdollista tarjota pääsy omiin tietoihinsa sähköisen asiointipalvelun kautta?
- Onko tunnistettu tietosuojasetuksesta tai tietosuojalaista tulevia rajoitusperusteita, jotka vaikuttavat siihen, mitä tietoja rekisteröidylle annetaan?
- Saadaanko kaikki rekisteröityä koskevat tiedot koottua eri lähteistä TSA 12 artiklan mukaisissa määräajoissa?
- Saadaanko tuotettua helposti jäljennös rekisteröidyn tiedoista?
- Jos rekisteröity pyytää tiedot sähköisesti, onko olemassa mahdollisuus toimittaa ne sähköisessä muodossa?

<sup>38</sup> <https://tietosuoja.fi/rekisteroidyn-oikeudet>

<sup>39</sup> <https://tietosuoja.fi/oikeus-saada-paasy-tietoihin>



### 2.4.3 Oikeus tietojen oikaisemiseen (TSA art. 16) sekä ilmoitusvelvollisuus (TSA art. 19)

Rekisteröidyillä on oikeus tulla arvioiduksi oikeiden ja täsmällisten tietojen perusteella. Jos tiedot ovat virheellisiä tai puutteellisia, on tiedot oikaistava.

Rekisterinpitäjän on mahdollisuuksien mukaan ilmoitettava henkilötietojen oikaisemisesta jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää.

Lue lisää [oikeudesta tietojen oikaisemiseen](#)<sup>40</sup>.

Kun arvioit tätä oikeutta koskevien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Voidaanko rekisteröidylle tarjota mahdollisuus oikaista itseään koskevia tietoja sähköisen asiointipalvelun kautta?
- Onko olemassa menettelyä erilaisten oikaisupyyntöjen toteuttamiseen?
- Jos oikaisun sisällöstä ei päästä yksimielisyyteen, onko mahdollista lisätä rekisteröidyn näkemys virheelliseksi väitettyjen tietojen yhteyteen?
- Ovatko tietojen vastaanottajat selvitettävissä?

### 2.4.4 Oikeus tietojen poistamiseen (TSA art. 17) sekä ilmoitusvelvollisuus (TSA art. 19)

Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjä poistamaan itseään koskevat tiedot ilman aiheetonta viivytystä.

Rekisterinpitäjän on mahdollisuuksien mukaan ilmoitettava henkilötietojen poistamisesta jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää.

Jos rekisterinpitäjä on julkistanut henkilötiedot ja se on velvollinen poistamaan tiedot rekisteröidyn pyynnöstä, sen on toteutettava kohtuulliset toimenpiteet ilmoittaakseen henkilötietoja käsitteleville rekisterinpitäjille, että rekisteröity on pyytänyt näitä poistamaan henkilötietoihin liittyvät linkit tai henkilötietojen jäljennökset tai kopiot.

Lue lisää [oikeudesta tietojen poistamiseen](#)<sup>41</sup>.

Kun arvioit tätä oikeutta koskevien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Voidaanko rekisteröidylle tarjota mahdollisuus poistaa itseään koskevat tiedot sähköisen asiointipalvelun kautta?
- Miten poisto-oikeuden soveltuvuuden tapauskohtainen arviointi toteutetaan?
- Miten poistoprosessi toimii, jos rekisteröity on perunut suostumuksensa tietojen käsittelyyn?

<sup>40</sup> <https://tietosuoja.fi/oikeus-oikaista-tietoja>

<sup>41</sup> <https://tietosuoja.fi/oikeus-poistaa-tiedot>



- Miten poistoprosessissa on huomioitu se, jos rekisteröity on vastustanut tietojensa käsittelyä suoramarkkinointitarkoituksia varten?
- Miten tietojen poistaminen käytännössä toteutetaan (manuaalinen/automatisoitu poisto, varmuuskopiot jne.)?
- Missä ajassa tiedot konkreettisesti poistuvat (katumusajat, profiilin palautukset jne.)?
- Onko poistolle esteitä? (lakisääteiset säilytysajat jne.)

#### 2.4.5 Oikeus käsittelyn rajoittamiseen (TSA art. 18) sekä ilmoitusvelvollisuus (TSA art. 19)

Rekisteröity voi tietyissä tilanteissa pyytää rekisterinpitäjää rajoittamaan väliaikaisesti itseään koskevien henkilötietojen käsittelyä. Tällöin rajoituksen alaisia henkilötietoja saa säilyttämisen lisäksi käsitellä vain rekisteröidyn suostumuksella, oikeudellisen vaateen laatumiseksi, esittämiseksi tai puolustamiseksi, toisen luonnollisen henkilön tai oikeushenkilön oikeuksien suojaamiseksi tai tärkeää unionin tai jäsenvaltion yleistä etua koskevista syistä.

Rekisterinpitäjän on mahdollisuuksien mukaan ilmoitettava henkilötietojen käsittelyn rajoittamisesta jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää.

Lue lisää [oikeudesta käsittelyn rajoittamiseen](#)<sup>42</sup>.

Kun arvioit tätä oikeutta koskevien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Miten rajoittamisoikeuden soveltuvuuden tapauskohtainen arviointi toteutetaan?
- Miten toteutetun rajoittamisen poistosta informoidaan rekisteröityä?
- Miten rajoittaminen käytännössä toteutetaan kunkin tietojärjestelmän tai käsittelytoiminnon tasolla?
- Onko tunnistettu perusteita kieltäytyä toteuttamasta rajoittamisoikeutta?

#### 2.4.6 Oikeus siirtää tiedot järjestelmästä toiseen (TSA art. 20)

Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjälle toimittamansa henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä halutessaan siirtää kyseiset tiedot toiselle rekisterinpitäjälle.

Lue lisää [oikeudesta siirtää tiedot järjestelmästä toiseen](#)<sup>43</sup>.

Kun arvioit tätä oikeutta koskevien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Soveltuuko siirto-oikeus arvioitavana olevaan käsittelyyn ja mitä tietoja se koskee?
- Miten siirto-oikeus toteutetaan käytännössä? Onko se teknisesti mahdollista?
- Pystytäänkö tarvittaessa vastaanottamaan rekisteröidyn siirto-oikeuden perusteella siirtämiä tietoja?

<sup>42</sup> <https://tietosuoja.fi/oikeus-rajoittaa-kasittelya>

<sup>43</sup> <https://tietosuoja.fi/oikeus-siirtaa-tiedot>



### 2.4.7 Oikeus vastustaa tietojen käsittelyä (TSA art. 21)

Rekisteröidyllä on tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan.

Lue lisää [oikeudesta vastustaa tietojen käsittelyä](#)<sup>44</sup>.

Kun arvioit tätä oikeutta koskevien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Soveltuuko vastustamisoikeus arvioitavana olevaan käsittelyyn? Mitä tietoja vastustamisoikeus koskee?
- Onko vastustamisoikeuteen liittyvät kysymykset käsitelty mahdollisessa oikeutetun edun analyysissä?
- Miten vastustamisoikeus toteutetaan käytännössä?

### 2.4.8 Automaattinen päätöksenteko (ml. profilointi) (TSA art. 22)

Rekisteröidyllä on pääsääntöisesti oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Tähän pääsääntöön on kuitenkin poikkeuksia.

Lue lisää [profiloinnista ja automaattisesta päätöksenteosta](#)<sup>45</sup>.

Kun arvioit tätä oikeutta koskevien vaatimusten toteutumista, voit hyödyntää seuraavia esimerkkikysymyksiä:

- Sisältyykö henkilötietojen käsittelyyn automaattista päätöksentekoa, jolla on rekisteröityä koskevia oikeusvaikutuksia tai joka vaikuttaa rekisteröityyn vastaavalla tavalla merkittävästi? Jos kyllä, mihin tämä perustuu?
- Käytetäänkö erityisiin henkilötietoryhmiin kuuluvia tietoja? Millä perusteella tämä on mahdollista?
- Jos peruste on a) välttämättömyys sopimuksen tekemistä tai täytäntöönpanoa varten tai b) rekisteröidyn nimenomainen suostumus, ovatko käytössä olevat suojatoimet riittäviä?
- Mitä suojatoimia on käytössä?
- Miten tietosuojaperiaatteet on huomioitu? Erityisesti käyttötarkoitussidonnaisuus, minimointi, kohtuullisuus.
- Miten rekisteröity voi vaatia ihmisen osallistumista päätöksentekoon?
- Miten tietosuojaoikeuksien toteuttamisesta on huolehdittu? Miten oikeus saada tiedot oikaistua ja poistettua toteutetaan sekä päätöksenteon / profiloinnin pohjana oleviin tietoihin, että luotuihin profiileihin?
- Miten ja milloin rekisteröidyn oikeuksista informoidaan? Missä vaiheessa palvelupolkua informaatio annetaan?
- Miten korostetusta informointivelvollisuudesta on huolehdittu?
- Miten rekisteröidyn mahdollisuus saada pääsy relevantteihin tietoihin algoritmista varmistetaan? Mitä tietoja rekisteröidylle annetaan?

<sup>44</sup> <https://tietosuoja.fi/oikeus-vastustaa-kasittelya>

<sup>45</sup> <https://tietosuoja.fi/oikeus-olla-joutumatta-automaattisen-paatoksenteon-kohteeksi>





- Miten rekisteröidylle kerrotaan profiilin luomisessa / päätöksenteossa käytetyt tietotyypit tai tiedot?
- Miten rekisteröidylle kuvataan segmentit, joihin hänet on sijoitettu?



### 3 Riskien arviointi

Kun on kuvattu, millä tavalla henkilötietojen käsittelyn lainmukaisuudesta on varmistuttu, on arvioitava henkilötietojen käsittelyyn liittyvät riskit.

Riskien arviointi kattaa uhkien ja niiden toteutumisen vaikutusten tunnistamisen sekä vaikutusten vakavuuden ja uhan todennäköisyyden arvioinnin.

#### 3.1 Arvioi riskit rekisteröidyn näkökulmasta

Rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyvät riskit rekisteröidyn näkökulmasta. Tällöin rekisterinpitäjä arvioi, mitä rekisteröidyn vapauksia ja oikeuksia henkilötietojen käsittelyssä toteutunut uhka voi vaarantaa ja millä tavalla sekä mitä vaikutuksia rekisteröidylle voi tästä aiheutua.

Riskien arviointi on jatkuvaa toimintaa: toimenpiteiden riittävyttä suhteessa käsittelyyn liittyvään riskiin on arvioitava jatkuvasti ja päivitettävä tarvittaessa. Rekisterinpitäjällä on myös osoitusvelvollisuus riskiperusteisen lähestymistavan noudattamisesta.

#### Riski

Tässä ohjeessa ”riskillä” tarkoitetaan skenaariota, joka kuvaa tapahtumaa ja sen seurauksia rekisteröidylle sekä arviota seurausten vakavuudesta ja todennäköisyydestä<sup>46</sup>. Yleisen tietosuoja-asetuksen mukaisella tietosuojaa koskevalla vaikutustenarvioinnilla pyritään tunnistamaan ja hallitsemaan näitä riskejä.

Riski			
Uhka	Uhan vaikutukset rekisteröidyille	Vaikutusten vakavuus rekisteröidyille	Uhan todennäköisyys

Kuva 2. Riski muodostuu neljästä osatekijästä: uhka, uhan vaikutukset rekisteröidyille, vaikutusten vakavuus rekisteröidyille sekä uhan todennäköisyys.

#### Uhka

Uhallä tarkoitetaan henkilötietojen käsittelyn puutetta, heikkoutta tai haavoittuvuutta tai käsittelyyn liittyvää tapahtumaa, joka vaikuttaa haitallisesti tietosuojaoperaatioihin tai tietosuoja-oikeuksiin, ja jolla voi olla haitallisia vaikutuksia muihin rekisteröidyn oikeuksiin ja vapauksiin.

Riskien arvioinnissa tunnistetaan uhat sekä arvioidaan niiden vaikutukset rekisteröidyn oikeuksiin ja vapauksiin.

<sup>46</sup> Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski” s.7

Uhkien tunnistamisessa on huomioitava sekä sisäiset että ulkoiset lähteet. Uhat voivat syntyä niin tahallisesta kuin tuottamuksellisestakin toiminnasta.

Esimerkkejä uhista:

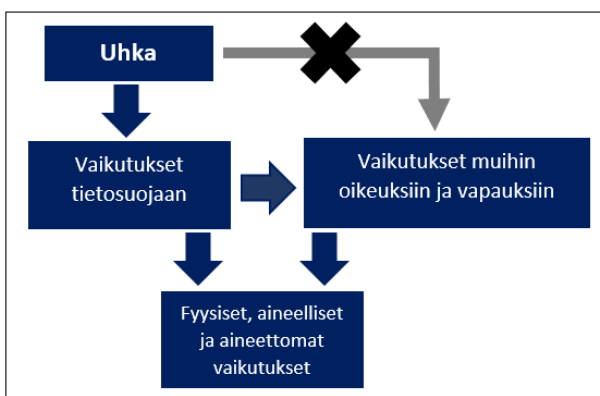
- tiedon luovuttaminen väärälle henkilölle
- kyberhyökkäys, joka johtaa tietojärjestelmän käyttökatkoon
- tietomurto
- tulipalo konesalissa
- rekisteröidyn pyynnön ohjautuminen väärään paikkaan

### Vaikutukset

TSA:n 35 artiklan viittaus oikeuksiin ja vapauksiin koskee ensisijaisesti oikeutta tietosuojaan ja oikeutta yksityisyyteen, mutta käsittää myös muita perusoikeuksia<sup>47</sup>, kuten sananvapauden, ajatuk-senvapauden, liikkumisvapauden, syrjintäkiellon, oikeuden vapauteen tai omantunnon ja uskonnon vapauden. Uhan vaikutukset voivat olla fyysisiä, aineellisia tai aineettomia<sup>48</sup>.

Tietosuojaan koskevan vaikutustenarvioinnin kannalta relevantteja vaikutuksia ovat sellaiset, jotka johtuvat henkilötietojen käsittelyn yhteydessä toteutuneesta uhasta. Nämä vaikutukset huomioi-daan laajasti. Muihin oikeuksiin ja vapauksiin kohdistuvat vaikutukset jäävät vaikutustenarvioinnin ulkopuolelle silloin, kun ne ovat seurausta sellaisten uhkien toteutumisesta, jotka eivät liity henkilö-tietojen käsittelyyn.

Yleisen tietosuoja-asetuksen tavoitteena on suojata henkilöiden perusoikeuksia ja -vapauksia, eri-tysisesti heidän oikeuttaan henkilötietojen suojaan. Esimerkiksi henkilötietojen luottamuksellisuuden menettämisestä aiheutuvat vaikutukset kohdistuvat henkilötietojen suojaan ja tietosuojaoikeuksiin. Lisäksi vaikutukset voivat kohdistua muihin henkilön perusoikeuksiin ja -vapauksiin, kuten tiedolli-seen itsemääräämisoikeuteen, yhdenvertaisuuteen tai liikkumisvapauteen. Se, mitä muita oikeuk-sia ja vapauksia henkilötietojen käsittely voi vaarantaa, riippuu käsittelyn luonteesta.



Kuva 3. TVA:ssa arvioitavat vaikutukset. Vaikutukset rekisteröidyille voidaan jakaa fyysisiin, aineellisiin ja aineettomiin. TVA:ssa arvioitavat vaikutukset kohdistuvat ensisijaisesti yksilön tietosuojaan. TVA:ssa ei arvioida vaikutuksia, jotka kohdistuvat vain muihin oikeuksiin ja vapauksiin ilman yhteyttä henkilötietojen käsittelyyn. Yksityisyyden suojaan ja

<sup>47</sup> Tietosuojatyöryhmä WP29:n lausunto 14/EN WP 218, TSA johdanto-osa 75

<sup>48</sup> Ks. TSA johdanto-osa 75.



*henkilötietojen käsittelyyn kohdistuvat vaikutukset voivat kuitenkin heijastua, ja usein heijastuvatkin, myös muihin henkilön oikeuksiin ja vapauksiin. Tällaiset vaikutukset arvioidaan TVA:ssa.*

## Vakavuus ja todennäköisyys

Kun henkilötietojen käsittelystä aiheutuvat uhat ja niiden vaikutukset rekisteröidyn oikeuksille ja vapauksille on tunnistettu, on arvioitava vaikutusten vakavuutta sekä uhkien toteutumisen todennäköisyyttä. Tämän kokonaisarvion perusteella valitaan toteutettavaksi tarkoituksenmukaiset suoja-toimet, joilla riskin tasoa pyritään alentamaan hyväksyttävälle tasolle. Riskejä on usein mahdotonta eliminoida kokonaan.

### 3.2. Tunnista uhat

Henkilötietojen käsittelyyn liittyvien riskien arviointi käynnistetään kartoittamalla henkilötietojen käsittelyyn kohdistuvat uhat. Sen jälkeen arvioidaan uhan toteutumisen mahdollisia vaikutuksia, niiden vakavuutta sekä uhan toteutumisen todennäköisyyttä.

#### 3.2.1 Uhkataulukko

Uhkien tunnistamisen välineenä voidaan käyttää Excel-työkalussa kuvattua uhkataulukkoa. Taulukkoon on listattu henkilötietojen käsittelyn elinkaaren mahdolliset eri vaiheet sekä ohjeen alussa esitellyt tietosuojaperiaatteet. Käsittelyn turvallisuus -periaatteen (TSA art. 5.1.f) osalta tarkastellaan erikseen käsittelyn luottamuksellisuutta, eheyttä ja käytettävyyttä. Taulukon avulla pyritään edistämään uhkien tunnistamisen systemaattisuutta ja auttamaan konkreettisten arvioitavaan käsittelyyn liittyvien uhkien tunnistamisessa.

Taulukko täytetään mahdollisimman konkreettisella tasolla. Jokaiseen kohtaan ei välttämättä voida tunnistaa uhkaa. Toisaalta uhkia voi löytyä yksittäisiin kohtiin useita. Jotkut uhat voivat koskea useita tietosuojaperiaatteita tai käsittelyn vaiheita. Tällöin on tärkeää varmistaa, että uhka tulee kirjatuksi vähintään yhteen taulukon kohtaan.

Seuraavan sivun esimerkissä pyritään osoittamaan, millä tarkkuudella uhat on tarkoituksenmukaista tunnistaa ja kuvata.

#### **Esimerkki 1**

Erilaisten uhkien tunnistaminen ns. ilmiantojärjestelmässä.

Kun uhkia arvioidaan rekisteröityjen näkökulmasta, on arvioinnissa yksilöitävä, keitä henkilöitä tai henkilörooleja koskevia tietoja tulee käsiteltäväksi tällaisessa tarkoituksessa. Roolien tunnistamisen avulla voidaan yksilöidä henkilön oikeudet ja vapaudet kyseisessä käsittelyssä. Tyypilliset henkilöroolit ovat ilmoittaja ja ilmoituksen kohde, jos ilmoitus on henkilön yksilöivä. Ilmoittaja kannustetaan tekemään ilmoitusta, ja yksi keino tähän on lupaus ilmoitusten nimettömästä käsittelystä. Tällöin ilmoittajaan kohdistuva uhka liittyy nimettömyyden murtumiseen ja siitä aiheutuviin vaikutuksiin oikeuksiin ja vapauksiin (ilmaisuusvapaus) sekä yksilöllisiin aineellisiin, fyysisiin ja henkisiin vaikutuksiin.

Toinen henkilörooli on ilmoituksen kohde, jonka osalta uhkina voidaan tunnistaa nimettömyyden aiheuttava tietolähteen epämääräisyys ja tunnistamattomuus (täsmällisyys). Kun tietoja kerätään muualta kuin henkilöltä itseltään uhka voi kohdistua läpinäkyvyyden periaatteeseen ja rekisteröidyn oikeuksiin. Kolmanneksi väärinkäytösepäilyä koskevat tiedot voivat päätyä sivullisille ja lopulta kyse on tällaisten ilmoitusten säilyttämisaikasta ja säilyttämisaikaisesta suojauksesta ja luotettavasta hävittämisestä. Ilmoituksen kohteen



muiden oikeuksien voidaan katsoa liittyvän syyttömyysolettamaan ja oikeudenmukaiseen oikeudenkäyntiin liittyviin seikkoihin, kuten oikeuteen perehtyä näyttöön ja tulla kuulluksi.

### Esimerkki 2

Täytetty uhkatalukko, joka kuvaa kuvitteellisessa tietojärjestelmää koskevassa vaikutustenarvioinnissa tunnistettuja uhkia. Kysymyksessä on kuvitteellinen tietojärjestelmä, joka on käytössä suuressa kuvitteellisessa yrityksessä, jossa käsitellään suuria määriä erityisiin henkilötietoryhmiin kuuluvia tietoja sekä hyödynnetään uutta teknologiaa.

	Lainmukaisuus ja kohtuullisuus	Läpinäkyvyys	Käyttötarkoitussidonnaisuus	Tietojen minimointi ja säilytysaikojen rajoittaminen	Täsmällisyys	Eheys	Luottamuksellisuus	Käytettävyys
<b>Kerääminen</b>		Rekisteröidylle annettava informaatio unohdetaan päivittää, eivätkä rekisteröidyt ole tietoisia siitä, että heitä koskevia tietoja saadaan myös lähteestä X.						
<b>Tallentaminen</b>							Salasanat tallennetaan järjestelmään salaamattomasti.	
<b>Yhdistäminen</b>					Työntekijä kerää rekisteröidyn henkilötietoja myös lähteestä, jonka oikeellisuudesta ei voida varmistua.			
<b>Käyttö ja muokkaaminen</b>			Työntekijä käyttää henkilötietoja toiseen tarkoitukseen kuin mihin tiedot on alun perin tarkoitettu.			Käyttöoikeuksien päivittämisen epäonnistumisen vuoksi henkilötietoja pääsee oikeudettomasti muokkaamaan organisaation sisällä kuka tahansa.		
<b>Luovutus ja saataville asettaminen</b>							Henkilötietoja tallennetaan vahingossa paikkaan X, jossa se on saatavilla myös organisaatiolle B.	
<b>Siirtäminen 3.maihin ja muut siirtotilanteet</b>	Henkilötietoja tallennetaan ohjeistuksen vastaisesti ETA:n ulkopuolella sijaitsevaan pilvipalveluun, joka merkitsee tietojen siirtoa kolmanteen							



	maahan ilman yleisen tietosuoja-asetuksen mukaisia suoja-keinoja							
<b>Säilyttäminen</b>	Työntekijä unohtaa poistaa henkilötiedot poistamiselle määritellyn suunnitelman mukaisesti.				Järjestelmän toimintahäiriön vuoksi rekisteröidyt eivät voi päivittää henkilötietojaan itse.			Henkilötiedot unohtetaan varmuuskopioida.
<b>Hävittäminen</b>				Työntekijä poistaa henkilötietoja, joita ei olisi saanut poistaa.				

### 3.2.2 Muita työkaluja ja näkökulmia uhkien tunnistamiseen

Alla annetaan esimerkkejä työkaluista uhkien tunnistamiseksi tehokkaasti. Listaus ei ole tyhjentävä tai pakottava. Työkalut valitaan kulloinkin kysymyksessä olevan käsittelyn luonteen ja kontekstin mukaan.

#### Organisaation asiantuntemus

Kun vaikutustenviannon laatimiseen osallistuu paitsi tietosuojan, myös tietoturvan, riskienhallinnan sekä käytännön toiminnan asiantuntijoita, voidaan mahdolliset uhat tunnistaa kattavasti eri näkökulmista.

#### Olemassa olevat visualisoinnit

Esimerkiksi tietovuo- tai työkuukavaavioista tai muista vastaavista visuaalisista kuvauksista on hyötyä mahdollisten uhkien tunnistamisessa. Hyödyntämällä kuvausta kaikista henkilötietojen käsittelyvaiheista, välineistä, tietovirroista jne., voidaan konkreettisesti havaita uhkille alttiit kohdat.

#### Uhkien aiheuttajien ja lähteiden tunnistaminen

Uhkien tunnistamista edesauttaa erilaisten uhkien aiheuttajien hahmottaminen. Uhan aiheuttajilla tarkoitetaan toimijoita tai käytäntöjä, joiden toimenpiteet tai toiminnot voivat johtaa uhan toteutumiseen.

Uhan aiheuttajia voi olla sekä organisaation sisäisiä että sen ulkopuolelta tulevia. Uhat voivat aiheutua ihmisten toiminnasta tai ei-inhimillisistä syistä.

Kun on kysymys automatisoidusta käsittelystä, voidaan katsoa, että myös automaattisen käsittelyn tietovälineet, laitteet ja ohjelmistot voivat aiheuttaa uhkia (esim. laiterikko sellaisenaan). Myös itseään koskevien tietojen käsittelyyn osallistuvat asiakkaat ja heidän päätelaitteensa sekä heidän käyttämänsä ohjelmistot voivat olla uhan aiheuttajia. Perinteisiä uhan aiheuttajia ovat sivulliset tai ulkopuoliset tahot, kuten hakkerit.



Uhan aiheuttaja	Esimerkit
<b>Sisäiset</b>	Työntekijät, IT-päälliköt, harjoittelijat, johtajat rekisterinpitäjän edustajina
<b>Ulkoiset</b>	Henkilötietojen vastaanottajat, valtuutetut kolmannet osapuolet, palveluntarjoajat, hakkerit, vierailijat, entiset työntekijät, kilpailijat, asiakkaat, huoltohenkilöstö, rikolliset, rikollisliigat, terroristijärjestöt
<b>Ei-inhimilliset</b>	Haittakoodi tuntemattomasta lähteestä (virukset, haittaohjelmat yms.), vesi (putkistot yms.), helposti syttyvät, syövyttävät tai räjähtävät materiaalit, luonnonkatastrofit, epidemiat, eläimet

Taulukko 1. Yleisimpiä uhan aiheuttajia<sup>49</sup>

### Henkilötietojen käsittelyyn käytettävät välineet

Uhkien tunnistamiseksi on suositeltavaa kartoittaa myös henkilötietojen käsittelyyn käytettäviin välineisiin liittyvät uhat.

Varsinkin ns. tietoturvariskien osalta, jotka kohdistuvat esimerkiksi käsittelyn laitteisiin, siirtokanaviin ja ohjelmistoihin, on hyödyllistä käydä läpi liitteenä olevan uhkatalukon luottamuksellisuuden, eheyden ja käytettävyyden uhkatapahtumat suunniteltuihin käsittelytoimiin kytkettyjen laitteiden, tiedonsiirron ja ohjelmistojen (ns. *supporting assets*) näkökulmasta. Tässä apuna voidaan käyttää esimerkiksi tietovirtakaaviota.

Resurssit	Esimerkit
<b>Järjestelmät</b>	Laitteisto ja elektroniset tietovälineet (tietokoneet, kovalevyt, USB-asema); ohjelmistot (käyttöjärjestelmät, tietokannat, viestiminen, sovellukset); tietoliikenneyhteydet (kaapelit, WiFi, kuituoptiikka)
<b>Organisaatiot</b>	Ihmiset, asiakirjat (tulosteet, kopiot, käsin kirjoitetut), asiakirjojen siirtokanavat (mm. sähköposti)

Taulukko 2. Esimerkkejä henkilötietojen käsittelyyn käytettävistä välineistä<sup>50</sup>

### Henkilötietojen elinkaari

Eräs tapa tunnistaa uhat on lähestyä henkilötietojen käsittelytoimintoja aikajärjestyksessä henkilötietojen elinkaaren mukaisesti. Tällöin voidaan paikantaa kussakin elinkaaren vaiheessa henkilötietojen käsittelyssä mahdollisesti toteutuvat uhat. Jaksossa 3.2.1. esitelty uhkatalukkotyökalu ilmentää henkilötietojen elinkaaren perustuvaa lähestymistapaa uhkien tunnistamisessa.

### 3.3. Arvioi vaikutusten vakavuus rekisteröidyn näkökulmasta

Kun rekisteröityihin kohdistuvat uhat on tunnistettu, on arvioitava näiden uhkien vaikutusten vakavuus. Arvioinnissa on otettava huomioon uhista välittömästi rekisteröidyn tietosuojalle aiheutuvien vaikutusten lisäksi myös vaikutukset rekisteröityjen muille perusoikeuksille ja -vapauksille. Näihin henkilötietojen käsittelyyn liittyviä oikeuksia ja vapauksia voivat tilanteesta riippuen olla esim. kotirauha, luottamuksellisen viestinnän suoja, liikkumisvapaus, sananvapaus ja yhdenvertaisuus.

<sup>49</sup> CNIL: Privacy Impact Assessment (PIA) Knowledge Bases (February 2018 edition), <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>, s.3

<sup>50</sup> CNIL: Privacy Impact Assessment (PIA) Knowledge Bases (February 2018 edition), <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> s.2



Vakavuuden arvioinnissa tulee ottaa huomioon tyypillisimmät fyysiset, aineelliset ja aineettomat vahingot.

Esimerkkejä vaikutuksista muihin oikeuksiin ja vapauksiin:

- rekisteröity ei pääse verkkopankkiin pidentyneen huoltokatkon vuoksi, eikä pysty suorittamaan maksuja ajallaan
- potilastietojen päätyminen avoimeen verkkoon aiheuttaa henkistä kärsimystä ja mahdollistaa tietojen väärinkäytön
- potilastietojen käytettävyys on estynyt, mikä johtaa terveyden tai hengen vaarantumiseen
- rekisteröity ei pääse puhelutallennetietoihin, minkä vuoksi hän ei pysty selvittämään sopimusoikeudellisia vastuitaan
- turvakiellon alaisten tietojen luottamuksellisuuden menettäminen aiheuttaa uhan henkilön turvallisuudelle
- käyttäjätunnusten ja salasanojen levittäminen johtaa luottamuksellisen viestinnän suojan menettämiseen ja / tai identiteetin oikeudettomaan käyttöön

Vakavuuden arvioinnissa tulee ottaa huomioon myös henkilötietojen luonne, kuten tietojen arkaluonteisuus, salassa pidettävyys tai se, onko kyse TSA:n 9 artiklassa tarkoitetuista erityisiin henkilötietoryhmiin kuuluvista tiedoista tai 10 artiklassa tarkoitetuista rikostuomioita tai rikkomuksia koskevista tiedoista. Lisäksi vakavuutta voi lisätä käsittelyn kohteena olevien henkilöiden erityinen haavoittuvuus, kuten alaikäisen tai muuten heikommassa asemassa olevan henkilön tietoja käsitellessä. Koska henkilötietoja ja erilaisia henkilötunnisteita (henkilötunnus, luottokorttitiedot, käyttäjätunnukset/salasanat) voidaan käyttää erilaisten rikosten välineinä esim. tietomurroissa, identiteettivarkauksissa ja niihin liittyvissä rikoksissa, on myös kiinnitettävä huomiota siihen, miten helposti tietoja voidaan väärinkäyttää.

Rekisteröidyille aiheutuvien vaikutusten vakavuusarvioinnissa voidaan käyttää apuna seuraavaa neliportaista taulukkoa<sup>51</sup>:

	Yleinen kuvaus vaikutuksista	Esimerkkejä yksilöllisistä vaikutuksista
1. VÄHÄINEN VAKAVUUS	Rekisteröidyille ei aiheudu seuraamuksia tai he saattavat kohdata muutaman ongelman, joista he selviytyvät helposti.	<p>Fyysiset vaikutukset:</p> <ul style="list-style-type: none"><li>• Hetkellinen päänsärky</li></ul> <p>Aineelliset vaikutukset:</p> <ul style="list-style-type: none"><li>• Ajanhukka asian selvittämisessä,</li><li>• Roskapostin vastaanottaminen</li><li>• Verkkosivuilla julkaistun tiedon uudelleenkäyttö kohdennettua markkinointia varten<sup>52</sup></li></ul> <p>Henkiset vaikutukset:</p> <ul style="list-style-type: none"><li>• Yksityisyyden loukkaamisen tunne ilman oikeaa tai objektiivista harmia</li></ul>

<sup>51</sup> CNIL: Privacy Impact Assessment (PIA) Knowledge Bases (February 2018 edition), <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> s.4-5

<sup>52</sup> Katso myös EDPB Guidelines 8/2020 on the targeting of social media users.





		<ul style="list-style-type: none"><li>Tietojen kontrollin menettämisen pelko</li></ul>
2. KOHTALAINEN VAKAVUUS	Rekisteröidyt saattavat kohdata merkittäviä vaikutuksia, joista he selviytyvät joistakin vaikeuksista huolimatta.	<p>Fyysiset vaikutukset:</p> <ul style="list-style-type: none"><li>Vähäiset fyysiset vaivat</li><li>Hoidon saamatta jääminen lievään vaaan, joka siitä syystä muuttuu vakavammaksi.</li></ul> <p>Aineelliset vaikutukset:</p> <ul style="list-style-type: none"><li>Odottamattomat tai ylimääräiset maksut kuten virheellisesti annetut sakot tai oikeudenkäyntikulut</li><li>Pääsyn estyminen hallinnollisiin tai kaupallisiin palveluihin</li><li>Kulujen nousu (esim. nousseet vakuutusmaksut)</li><li>Mukavuuksien menettäminen (esim. vapaa-ajan, ostoksien tai loman menettäminen, käyttäjätunnuksen lakkauttaminen)</li></ul> <p>Henkiset vaikutukset:</p> <ul style="list-style-type: none"><li>Vähäiset, mutta objektiiviset psykologiset haitat (kunnianloukkaus, mainehaitat)</li><li>Suhdeongelmat henkilökohtaisiin tai ammatillisiin tuttaviiin (esim. huonontunut maine, tunnustuksen menettäminen)</li><li>Uhkailu yhteisöpalveluissa</li><li>Tunne yksityisyyden loukkaamisesta ilman peruuttamatonta haittaa</li></ul>
3. MERKITÄVÄ VAKAVUUS	Rekisteröidyt saattavat kohdata merkittäviä ongelmia, joista heidän tulisi selviytyä, vaikkakin todellisten ja merkittävien vaikeuksien kautta.	<p>Fyysiset vaikutukset:</p> <ul style="list-style-type: none"><li>vakava fyysinen haitta, josta aiheutuu pitkäaikaista harmia (esim. terveyden heikentyminen puuttuvan hoidon johdosta),</li><li>fyysisen koskemattomuuden loukkaus</li></ul> <p>Aineelliset vaikutukset:</p> <ul style="list-style-type: none"><li>Taloudelliset tappiot, joita ei korvata, kun tietoja on käytetty oikeudettomasti</li><li>Ei-tilapäiset taloudelliset vaikeudet (pakotettu lainanotto),</li><li>Kielto pankkitilin saamiseen</li></ul>



		<ul style="list-style-type: none"><li>• Ainutkertaisen mahdollisuuden menettäminen opinto- tai harjoittelupaikkaan tai työpaikkaan</li><li>• Asunnon tai työpaikan menettäminen</li><li>• Ulkomaille jumiin jääminen</li></ul> <p>Henkiset vaikutukset:</p> <ul style="list-style-type: none"><li>• Vakava psykologinen haitta (esim. masennus tai fobian kehittyminen)</li><li>• Tunne perusoikeuksien tai yksityisyyden loukkaamisesta peruuttamattomalla tavalla</li><li>• Nettikiusaaminen ja häirintä</li><li>• Kiristämisen uhriksi joutuminen</li></ul>
<b>4. KRIITTINEN VAKAVUUS</b>	Rekisteröidyt saattavat kohdata merkittäviä ja jopa pysyviä vaikutuksia, joista he eivät välttämättä selviydy.	<p>Fyysiset vaikutukset:</p> <ul style="list-style-type: none"><li>• Pitkäaikainen tai pysyvä fyysinen vaiva</li><li>• Kuolema (esim. murha, itsemurha tai kuolemaan johtava onnettomuus)</li><li>• Pysyvä haitta fyysiseen koskemattomuuteen puuttumisesta</li></ul> <p>Aineelliset vaikutukset:</p> <ul style="list-style-type: none"><li>• Huomattava velkaantuminen</li><li>• Työkyvyttömyys</li><li>• Todistusaineiston häviäminen oikeudenkäynnissä</li><li>• Pääsyn esto elintärkeään infrastruktuuriin (vesi, sähkö)</li></ul> <p>Henkiset vaikutukset:</p> <ul style="list-style-type: none"><li>• Pitkäaikainen tai pysyvä psykologinen haitta</li><li>• Perhesiteiden katkeaminen</li><li>• Rikosoikeudellinen rangaistus</li><li>• Hallinnollisen aseman muuttuminen tai oikeudellisen autonomian menettäminen (esim. edunvalvonta)</li></ul>

### 3.4 Arvioi uhkien toteutumisen todennäköisyys

Mahdollisten uhkien tunnistamisen jälkeen on arvioitava, miten todennäköisesti tunnistetut uhat toteutuvat.

Todennäköisyyttä voidaan arvioida tunnistamalla mahdolliset tietosuojaan vaikuttavat heikkoudet ja haavoittuvuudet sekä uhan aiheuttajat ja niiden kyvyt ja halukkuus hyödyntää olemassa olevia heikkouksia tai haavoittuvuuksia.



Käytännössä todennäköisyyden arvioinnissa ei useinkaan lähdetä tyhjästä, vaan organisaatiossa on jo käytössä erilaisia uhan todennäköisyyttä vähentäviä tietosuoja-asetuksen edellyttämiä teknisiä ja organisatorisia suojatoimia. Tällöin uhan todennäköisyys arvioidaan käytettävissä olevat suojatoimenpiteet huomioiden. Voit ottaa huomioon tietojen turvallisuus -periaatteen noudattamisen arvioinnin yhteydessä tunnistamasi tekijät (jakso 3.1.6 Henkilötietojen käsittely turvallisuus).

Arvioinnin taustana voidaan käyttää vastaavan uhan ilmenemistä historiallisesti esimerkiksi, jos käytettävissä on tilastotietoa uhan ilmenemisen yleisyydestä.

### Esimerkki 3

Ulkopuolinen (uhan aiheuttaja) voi pyytämällä saada oikeudettomasti tietoja (uhkatapahtuma), eikä käytössä ole kontrollikeinoja, joilla tällainen luovutus estettäisiin. Tällöin on todennäköistä, että uhan aiheuttaja kykenee toteuttamaan uhan.

Uhan todennäköisyyden arvioinnissa voidaan käyttää apuna seuraavaa asteikkoa:

EPÄTODENNÄKÖINEN	Vaikuttaa erittäin epätodennäköiseltä, että tunnistettu uhka toteutuu kyseessä olevassa tilanteessa (esim. paperisten dokumenttien varastaminen lukitusta kulunvalvonnalla suojatusta huoneesta tai tietokantaan pääsy avoimen verkon kautta on mahdollista, mutta edellyttää vahvaa tunnistautumista).
MAHDOLLINEN	Vaikuttaa epätodennäköiseltä, että tunnistettu uhka toteutuisi (esim. paperisten dokumenttien varastaminen lukitusta huoneesta tai tietokantaan pääsy avoimen verkon kautta on mahdollista, mutta salasana on heikko).
TODENNÄKÖINEN	Vaikuttaa todennäköiseltä, että tunnistettu uhka toteutuu (esim. paperisten dokumenttien varastaminen toimistosta, jonne ei pääse ilman ilmoittautumista vastaanotolla tai tietokanta on täysin auki avoimeen verkkoon, mutta tietokanta ei ole löydettävissä hakukoneilla).
LÄHES VARMA	Vaikuttaa erittäin todennäköiseltä, että tunnistettu uhka toteutuu (esim. paperisten dokumenttien varkaus julkisesta aulasta tai tietokanta täysin auki avoimeen verkkoon ja se löytyy hakukoneella.)

### 3.5 Määrittele ja toteuta lisäsuojatoimenpiteet uhkien todennäköisyyden ja vaikutusten vakavuuden madaltamiseksi hyväksyttävälle tasolle

Kun henkilötietojen käsittelyssä toteutettavat suojatoimet on alustavasti suunniteltu, on arvioitava niiden asianmukaisuutta ja oikeasuhteisuutta suhteessa tunnistettuihin uhkiin.



Suojaustoimenpiteiden soveltuvuuden kannalta on olennaista arvioida, miten suojaustoimenpiteet vaikuttavat uhkiin. Vähentääkö toimenpide uhan todennäköisyyttä vai vakavuutta? Vaikuttaako se molempiin? Esimerkiksi tietovälineen sisältämien tietojen salaaminen ei sinänsä vaikuta tietovälineen häviämisen todennäköisyyteen, mutta se vaikuttaa todennäköisyyteen, jolla tietovälineen mahdollinen ulkopuolinen haltija kykenee hyödyntämään tietoja tai aiheuttamaan niiden avulla haittaa tai vahinkoa.

Asianmukaisuuden ja oikeasuhtaisuuden arvioinnissa on otettava huomioon käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten lisäksi uusin tekniikka ja suojaustoimenpiteiden toteuttamiskustannukset.

Rekisterinpitäjiltä edellytetään teknologisen kehityksen seuraamista ja teknisten sekä organisatoristen suojaustoimenpiteiden päivittämistä tarpeen mukaan niiden tehokkuuden takaamiseksi. Toteuttamiskustannusten osalta rekisterinpitäjältä ei edellytetä käsittelyyn liittyvään riskiin nähden suhteettoman suurta taloudellista panostusta suojaustoimenpiteisiin tilanteissa, joissa edullisempia ja tehokkaita suojaustoimenpiteitä on tarjolla. Toisaalta, vaikka uhan todennäköisyyttä ei ole arvioitu korkeaksi, mutta sen vaikutus rekisteröidyn oikeuksille ja vapauksille on vakava, voi olla asianmukaista ja oikeasuhteista ottaa käyttöön suojaustoimenpiteitä, jotka eivät olisi perusteltuja yksinomaan taloudellisesti arvioiden. Virheellisesti alakanttiin arvioitu riski ei ole peruste suojaustoimenpiteiden laiminlyömiselle.

Uhkien arviointi on jatkuvaa toimintaa, eli suojaustoimenpiteiden asianmukaisuutta ja oikeasuhtaisuutta suhteessa käsittelyyn liittyviin riskeihin on arvioitava jatkuvasti ja päivitettävä tarvittaessa.

Mikäli suojaustoimenpiteiden asianmukaisuuden ja oikeasuhtaisuuden arvioinnissa päädytään siihen, että uhan todennäköisyyttä tai vakavuutta ei voida hyväksyä, on toteutettava tarvittavat lisätoimenpiteet tämän jäännösriskin madaltamiseksi hyväksyttävälle tasolle. Suojaustoimenpiteet voivat olla uhkiin varautuvia, niitä ennalta estäviä, rajoittavia, havainnoivia tai toteutuneita uhkia tai niihin johdaneita syitä korjaavia.

Lisäsuojaustoimenpiteitä valitessa tulee huomioida, että TSA:n nimenomaisesti edellyttämät vaatimukset muodostavat minimistandardin, jota tulee noudattaa kaikissa tapauksissa. Näin ollen lisäsuojaustoimenpide ei voi olla toimenpide, jonka yleinen tietosuojasetus edellyttää toteutettavaksi joka tapauksessa. Esimerkiksi käsittelyprosessissa tulee jo tietojen minimointivaatimuksen (TSA art. 5.1.c sekä jakso 3.1.4) noudattamiseksi varmistaa, ettei käsittelyssä synny tarpeettomia kopioita henkilötiedoista. Valittujen toimenpiteiden on lisäksi oltava säädösten mukaisia (esim. säädetyt säilyttämisaajat).

#### **Esimerkki 4**

Alla olevaan taulukkoon on poimittu joitakin ylempänä esimerkissä 1 havainnollistettuja uhkia, niihin kohdistettavia lisäsuojaustoimenpiteitä sekä näiden toimenpiteiden vaikutuksia.



	Toimenpide	Vaikutus
<b>Lainmukaisuus ja kohtuullisuus</b>	Automatisoidaan henkilötietojen poistaminen.	On epätodennäköisempää, että tietojen poistaminen unohtuu ja tietoja säilytetään liian kauan ilman perustetta.
<b>Läpinäkyvyys ja rekisteröidyn oikeudet</b>	Tehdään rekisteröidylle annettavan informaation päivittämisestä säännöllisesti toistuva tehtävä. Määritetään informaation päivittämiselle vastuuhenkilöt.	On epätodennäköisempää, että rekisteröidyn saama tieto on vanhentunutta tai puutteellista.
<b>Käyttötarkoitussi-donnaisuus</b>	Järjestetään henkilöstölle koulutusta, jossa käsitellään henkilötietojen sallittuja käyttötarkoituksia.	On epätodennäköisempää, että henkilötietoja käsitellään käyttötarkoituksen vastaisesti.
<b>Tietojen minimointi ja säilytyksen rajoittaminen</b>	Pseudonymisoidaan käsiteltävät tiedot.	Esimerkiksi mahdollisen tietomurron sattuessa vaikutusten vakavuus on pienempi.
<b>Täsmällisyys</b>	Järjestetään rekisteröidyille mahdollisuus päivittää tietojaan itse tai päivittää tiedot automaattisesti luotettava lähteestä.	On epätodennäköisempää, että käsiteltävät henkilötiedot ovat virheellisiä tai vanhentuneita.
<b>Eheys, luottamuksellisuus ja käytettävyys</b>	Luodaan henkilöstölle ohjeistus henkilötietojen luovutus- ja tietopyyntöihin vastaamisesta.	On epätodennäköisempää, että henkilötietoja luovutetaan vahingossa oikeudettomasti organisaation ulkopuolelle.
	Lisätään järjestelmään ominaisuus, joka estää käyttäjää poistamasta tiettyjä tietoja.	On epätodennäköisempää, että tarpeellisia henkilötietoja poistetaan vahingossa tai tahallisesti.
	Automatisoidaan varmuuskopioiden luominen.	On epätodennäköisempää, että varmuuskopiointi unohtuu ja henkilötiedot menetetään lopullisesti.

### 3.6 Laadi uhkien todennäköisyyden ja vaikutusten vakavuuden arvioinnin yhteenveto

Sijoita jokainen uhka sille määritellyn vakavuuden ja todennäköisyyden perustella seuraavalla sivulla olevan taulukon mukaisesti.

Lopputuloksena syntyvään taulukkoon on sijoitettu jokainen tunnistettu uhka sen vaikutusten vakavuuden ja todennäköisyyden mukaisesti. Taulukko näyttää kunkin tunnistetun riskin tason.

Kun riski sijoittuu punaisella merkittyyn tasoon, on riskin taso erittäin korkea. Oranssilla merkityissä kohdissa riski on korkea. Riskin taso pienenee asteittain, ja tummimmalla vihreällä merkityssä kohdassa riskin taso on vähäinen.

Kun riski sijoittuu punaisella tai oranssilla merkittyyn tasoon, on ennakkokuulemiseen syytä ryhtyä.



V A K A V U U S	4. Kriittinen				
	3. Merkittävä				
	2. Kohtalainen				
	1. Vähäinen				
		1. Epätodennäköinen	2. Mahdollinen	3. Todennäköinen	4. Lähes varma

TODENNÄKÖISYYS



## 4 Tietosuojan vaikutustenarvioinnin hyväksyminen sekä mahdolliset korjaavat toimenpiteet

Kun edellä kuvatut vaiheet on suoritettu, rekisterinpitäjä hyväksyy tietosuojan vaikutustenarvioinnin, siinä tunnistetut riskit ja riskitasot, sekä valitut korjaavat toimenpiteet. Jokaisessa organisaatiossa on tarpeen määritellä menettely, jonka mukaisesti hyväksyntä tapahtuu. Johdon käyttöön voidaan esimerkiksi laatia yhteenveto, josta käy ilmi vaikutustenarvioinnin lopputulos tarpeellisine perusteluineen.

Tietosuojan vaikutustenarvioinnin julkaiseminen on suositeltavaa, mutta ei pakollista. Vaihtoehtoisesti vaikutustenarvioinnin voi julkaista osittain, ettei jaettavassa materiaalissa paljasteta esimerkiksi liikesalaisuuksia tai käsitellyn tietoturvaa vaarantavia seikkoja.

Ainakin seuraavat seikat pitää dokumentoida ennen kuin vaikutustenarviointi hyväksytään:

- Mitä lisäsuojatoimenpiteitä aiotaan ottaa käyttöön? Millä aikataululla? Kuka toteuttaa?
- Onko riskit saatu poistettua kokonaan tai madallettua hyväksyttävälle tasolle? Vai hyväksytäänkö riskit sellaisenaan?
- Lopullinen jäännösriski lisäsuojatoimenpiteiden jälkeen
- Onko aihetta pyytää tietosuojaviranomaiselta ennakkokuulemistä?

### Ennakkokuuleminen

Kaikkia riskejä ei ole aina mahdollista eliminoida kokonaan. Joidenkin riskien voidaan katsoa olevan hyväksyttäviä ottaen huomioon käytössä olevat suojatoimenpiteet ja käsittelystä koituvat hyödyt. Jos riski jää lisätoimenpiteiden toteuttamisesta huolimatta korkeaksi, tulee tietosuojaviranomaiselta pyytää ennakkokuulemistä ennen käsittelyyn ryhtymistä. Vastuu ennakkokuulemismenettelyyn ryhtymisestä on rekisterinpitäjällä.

Ennakkokuulemistä pitää pyytää esimerkiksi, jos rekisteröidyt voivat joutua kärsimään huomattavista tai jopa peruuttamattomista seurauksista, joita he eivät välttämättä pysty torjumaan (esim. laitton tietoihin pääsy, joka johtaa rekisteröityjen henkeä uhkaavaan vaaraan, irtisanomiseen tai taloudelliseen uhkaan) ja/tai joissa riskin ilmeneminen näyttää selvältä (esim. kun ei pystytä vähentämään niiden henkilöiden lukumäärää, joilla on pääsy tietoihin tietojen jakamis-, käyttö- tai levitystapojen vuoksi tai kun tiedossa olevaa haavoittuvuutta ei pystytä korjaamaan).<sup>53</sup>

Tietosuojavaltuutettu antaa tarvittaessa ennakkokuulemispyynnön johdosta rekisterinpitäjälle tai käsittelijälle kirjalliset ohjeet niistä toimenpiteistä, joihin on ryhdyttävä riskin alentamiseksi. Tietosuojavaltuutetun kirjalliset ohjeet rajautuvat vaikutustenarvioinnin kohteen sekä siinä tunnistettujen korkeiden jäännösriskien mukaisesti. Tarvittaessa tietosuojavaltuutettu voi ennakkokuulemisen yhteydessä käyttää myös sille tietosuoja-asetuksessa annettuja toimivaltuuksia, kuten varoitusta. Rekisterinpitäjän ja käsittelijän on syytä toteuttaa ohjeen mukaiset lisätoimenpiteet riskien madaltamiseksi ennen henkilötietojen käsittelyn aloittamista.

[Lue lisää ennakkokuulemisesta<sup>54</sup>.](#)

<sup>53</sup> WP 248 rev.01 s. 22.

<sup>54</sup> <https://tietosuoja.fi/ennakkokuuleminen>



## Muita tietosuojan vaikutustenarvioinnin ohjeita ja lähdeaineis- toa:

- Tietosuojatyöryhmän (WP 29) ohje 4.10.2017 wp 248 rev.01
- EDPB guidelines 4/2019 (v.2.0) on Data Protection by Design and by Default
- EDPS Accountability on the ground Part II: Data Protection Impact Assessment & Prior Consultation (v.1.3 July 2019)
- CNIL Privacy Impact Assessment (PIA) 2.2018
  - Methodology, Template and Knowledge bases
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems (v.2, 13.9.2018)
- SFS-ISO/IEC 29134:2018 Ohjeita tietosuojavaikutusten arviointiin





## Käsitteitä

### Anonymisointi

Anonymisointi tarkoittaa henkilötietojen käsittelyä niin, että henkilöä ei enää voida tunnistaa niistä. Tunnistamisen täytyy estyä peruuttamattomasti ja siten, että rekisterinpitäjä tai muu ulkopuolinen taho ei voi enää hallussaan olevilla tiedoilla muuttaa tietoja takaisin tunnistettaviksi. Anonymisoituja tietoja ei enää katsota henkilötiedoiksi. Niihin ei sovelleta tietosuojasäännöksiä.

### Ennakkokuuleminen

Ennakkokuulemisella tarkoitetaan tilannetta, jossa rekisterinpitäjän on ennen henkilötietojen käsittelyn aloittamista kuultava tietosuojaviranomaista. Ennakkokuuleminen on toteutettava, kun vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin rekisteröidyille, eikä rekisterinpitäjä ole omilla toimenpiteillään saanut riskiä alhaisemmaksi.

### Erityiset henkilötietoryhmät

Niin sanottuihin erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä. Tällaisista tiedoista ilmenee henkilön rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveyttä koskevia tietoja, seksuaalinen suuntautuminen tai käyttäytyminen tai geneettisiä tietoja ja biometrisia tietoja henkilön tunnistamista varten.

### EU:n yleinen tietosuoja-asetus (TSA, GDPR)

Henkilötietojen käsittelyä sääntelevä asetusta, jonka soveltaminen aloitettiin kaikissa EU-maissa 25.5.2018.

### Euroopan tietosuojaneuvosto (EDPB)

Euroopan tietosuojaneuvosto on riippumaton EU:n elin, joka vastaa tietosuojasääntöjen yhdenmukaisesta soveltamisesta kaikkialla Euroopan unionissa ja edistää EU:n tietosuojaviranomaisten välistä yhteistyötä. Euroopan tietosuojaneuvosto koostuu kansallisten tietosuojaviranomaisten (ml. tietosuojavaltuutetun toimiston) ja Euroopan tietosuojavaltuutetun (EDPS) edustajista.

### (Henkilö)rekisteri

Rekisterillä tarkoitetaan mitä tahansa jäsenneiltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

Huomaa, että aiemmasta henkilötietolaista poiketen tietosuoja-asetus soveltuu automaattiseen henkilötietojen käsittelyyn riippumatta siitä, muodostuuko tiedoista rekisteri. Se, muodostuuko käsittelyssä rekisteri tai rekisterin osa, on olennaista vain silloin, kun kyse on manuaalisesta käsittelystä.

### Henkilötieto

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Henkilötietoja voi olla talletettuna esimerkiksi sähköisissä tiedostoissa, tietokannoissa, paperilla, kortistossa, mapeissa tai ääni- tai kuvatallenteella.

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, psykisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

### Henkilötietoja koskeva tietoturvaloukkaus

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvottomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.



### **Henkilötietojen käsittelijä**

Henkilötietojen käsittelijäksi kutsutaan rekisterinpitäjältä ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun rekisterinpitäjän ohjeiden mukaisesti.

### **Henkilötietojen käsittely**

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.

### **Jäännösriski**

Suojatoimenpiteiden toteuttamisen jälkeen jäljelle jäävä riski, jota ei voida tai ei haluta poistaa. Lopullinen arvio riskistä suojatoimenpiteiden käyttöönoton jälkeen.

### **Kolmas maa**

Euroopan talousalueen (ETA) ulkopuolinen maa. ETA-alueeseen kuuluvat EU-maiden lisäksi Islanti, Liechtenstein ja Norja.

### **Osoitusvelvollisuus**

Osoitusvelvollisuus tarkoittaa sitä, että rekisterinpitäjän ja käsittelijän on pystyttävä käytännössä näyttämään, että tietosuojasetusta noudatetaan. Osoitusvelvollisuus voidaan toteuttaa esimerkiksi dokumentoimalla.

### **Profilointi**

Profilointi tarkoittaa henkilötietojen automaattista käsittelyä, jossa arvioidaan ihmisen henkilökohtaisia ominaisuuksia. Profiloinnilla tarkoitetaan erityisesti työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin liittyvien piirteiden analysointia tai ennakointia.

### **Pseudonymisointi**

Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Tällaiset lisätiedot täytyy säilyttää huolellisesti erillään henkilötiedoista. Pseudonymisoidut tiedot ovat yhä henkilötietoja, ja niiden käsittelyssä on sovellettava tietosuojasäännöksiä.

### **Rekisterinpitäjä**

Rekisterinpitäjäksi kutsutaan henkilöä, yritystä, viranomaista tai yhteisöä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

### **Rekisteröity**

Rekisteröity on henkilö, jota henkilötieto koskee (ks. myös **Henkilötieto**).

### **Rikosasioiden tietosuojadirektiivi, ja -laki (RTsL)**

Henkilötietojen käsittelystä rikosasioissa säädetään 1.1.2019 voimaan tulleessa rikosasioiden tietosuojalain. Lakia sovelletaan poliisin, syyttäjien, tuomioistuinten, Rikosseuraamuslaitoksen, Tullin, rajavalvontaviranomaisten ja muiden toimivaltaisten viranomaisten käsitellessä henkilötietoja rikosasiassa.



Rikosasioiden tietosuojalailla on pantu täytäntöön rikosasioiden tietosuojadirektiivi. EU:n direktiivin tavoitteena on nykyaikaistaa sääntelyä, helpottaa tietojen vapaata liikkuvuutta EU-maiden poliisi- ja oikeusviranomaisten välillä sekä varmistaa henkilötietojen suoja rikosasioita käsiteltäessä.

### **Riski**

Riskillä tarkoitetaan skenaariota, joka kuvaa tapahtumaa ja sen seurauksia rekisteröidylle sekä arviota seurausten vakavuudesta ja tapahtuman todennäköisyydestä.

### **Riskienhallinta**

Koordinoitu toiminta, jolla ohjataan ja valvotaan organisaatiota riskien osalta.

### **Seloste käsittelytoimista**

Seloste käsittelytoimista on kirjallinen kuvaus organisaation tekemästä henkilötietojen käsittelystä. Seloste on organisaation sisäinen asiakirja. Se toimii apuvälineenä henkilötietojen käsittelyn hahmottamiseen, ja sen tarkoituksena on osaltaan osoittaa, että henkilötietoja käsitellään tietosuojalainsäädännön mukaisesti.

### **Sisäänrakennettu ja oletusarvoinen tietosuoja**

Sisäänrakennetulla tietosuojalla tarkoitetaan sitä, että tietosuojaperiaatteet sisään rakennetaan rekisterinpitäjille tarjottaviin työkaluihin, tuotteisiin, sovelluksiin tai palveluihin. Oletusarvoisella tietosuojalla tarkoitetaan sitä, että työkalut, tuotteet, sovellukset tai palvelut takaavat oletusarvoisesti, että käsittely rajoittuu vain käsittelyn tarkoituksen kannalta tarpeellisiin henkilötietoihin.

### **Suostumus**

Suostumus on yksi mahdollinen oikeusperuste henkilötietojen käsittelylle. Suostumus antaa rekisteröidylle mahdollisuuden valvoa henkilötietojensa käsittelyä ja vaikuttaa henkilötietojen käsittelyyn peruuttamalla suostumuksen. Suostumuksen edellytyksistä säädetään yleisen tietosuoja-asetuksen 7 artiklassa.

### **Tietosuojalaki**

EU:n yleistä tietosuoja-asetusta täsmentävä kansallinen yleislaki, joka tuli voimaan 1.1.2019.

### **Tietosuojan vaikutustenarviointi (TVA)**

Tietosuojan vaikutustenarvioinnin tarkoituksena on tunnistaa ja vähentää henkilötietojen käsittelyyn liittyviä riskejä sekä tuottaa aineistoa, jolla tietosuojasääntelyn noudattaminen voidaan osoittaa.

### **Tietosuojavastaava**

Tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa. Tietosuoja-asetus sisältää edellytyksiä, joiden täytyttyä tietosuojavastaavan nimittäminen on organisaatiolle pakollista.

### **Tietoturva**

Tietoturva on yksi tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät. Tietoturva tarkoittaa muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyyden sekä rekisteröidyn oikeuksien toteutuminen.

### **Vastaanottaja**

Vastaanottajilla tarkoitetaan tietosuoja-asetuksessa kaikkia niitä tahoja (luonnolliset henkilöt tai oikeushenkilöt, viranomaiset, virastot tai muut elimet), joille henkilötietoja siirretään tai luovutetaan.



### **Yhteisrekisterinpitäjät**

Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä.

### **WP29**

Tietosuojadirektiivin 29 artiklan mukainen työryhmä WP 29 oli riippumaton EU:n työryhmä, joka käsittelee yksilöiden suojelua henkilötietojen käsittelyssä koskevia kysymyksiä yleisen tietosuoja-asetuksen soveltamisajan alkamiseen asti. (ks. Euroopan tietosuojaneuvosto (EDPB))



## Liitteet

**LIITE I** Excel-työkalu

**LIITE II** Tietosuojan vaikutustenarviointi rikosasioiden tietosuojalain mukaan