VAHTI-hyvät käytännöt tukimateriaali

5.11.2021

**Tietotilinpäätös - malli**

Sisällysluettelo

[1 Johdanto 3](#_Toc80254503)

[SAATE 4](#_Toc80254504)

[JULKINEN TIIVISTELMÄ 7](#_Toc80254505)

[TIIVISTELMÄ JOHDOLLE 8](#_Toc80254506)

[1.1.1 JOHDANTO 9](#_Toc80254507)

[1.1.2 LAINSÄÄDÄNTÖ JA MUU OHJEISTUS 10](#_Toc80254508)

[1.1.3 TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN 11](#_Toc80254509)

[1.1.4 TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT 12](#_Toc80254510)

[1.1.5 REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN 13](#_Toc80254511)

[1.1.6 SEURANTA JA MITTARIT 14](#_Toc80254512)

[1.1.7 ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN 16](#_Toc80254513)

Tietotilinpäätös - malli

# Johdanto

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

Toivomme, että annat meille palautetta tästä materiaalista. Saatuamme useampia tai muuten keskeisiä parannus ja korjausehdotuksia, pyrimme julkaisemaan ne uudessa päivitetyssä versiossa mahdollisimman pikaisesti.

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

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

### SAATE

Tämä tietotilinpäätöksen mallipohja pohjautuu [Kuntaliiton laatimaan malliin](https://www.kuntaliitto.fi/osallistuminen-ja-vuorovaikutus/tietoyhteiskunta/tiedonhallinta) ja sitä on edelleen kehitetty Digi- ja väestötietoviraston Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) tietosuojan kehittämisen työryhmässä.

Mallipohja on laadittu tukeutuen tietosuojavaltuutetun ohjeeseen. Tietotilinpäätöksen lopullinen sisältö ja painotukset muotoutuvat aina toimiala- ja organisaatiokohtaisesti. Asiakirjan rakenteeseen ja sisältöön sekä laatimisprosessiin vaikuttaa, millainen merkitys tietotilinpäätökselle on organisaatiossa annettu.

**Tietotilinpäätöksen tarkoitus:** Osoitusvelvollisuuden toteennäyttäminen, organisaation tietojen käsittelyn kuvaus, sisäisen valvonnan työkalu, suunnittelun ja toiminnanohjauksen sekä raportoinnin ja johtamisen tuki. Tietotilinpäätöksellä voidaan lisätä luottamusta organisaation menettelytapoihin tietojen käsittelyssä.

 **Tietotilinpäätöksen laadinnan prosessi:** Määritellään tietotilinpäätöksen merkitys ja tavoitteet organisaatiolle sekä sisällön laajuus. Tunnistetaan tietotilinpäätöksen laadintaan osallistuvat tahot organisaatiossa. Koordinointivastuussa voi olla siihen nimetty työryhmä tai esim. tiedonhallinta-, tietosuoja- tai tietoturvaryhmä, joka huolehtii tietojen keräämisen organisoinnista ja sisällön tuottamisesta. Keskeistä on, että koko organisaatiota koskevan tiedon keruuprosessiin tarvitaan usean henkilön yhteistä panostusta.

**Aikataulutus:** Kerran vuodessa vuosikellon mukaan, muulloin pyydettäessä. Aikataulutuksessa voi hyödyntää [Tietosuojan vuosikello -mallia](https://dvv.fi/documents/16079645/17634906/DHK_Tietosuoja_vuosikello_0305_2021.pdf/39f390d7-0fd4-8b66-db8c-680547ec2de7/DHK_Tietosuoja_vuosikello_0305_2021.pdf?t=1620048667625)

**Ohje:** Malli on viitteellinen ja se sisältää seitsemän lukua, jotka alkavat yleisellä kuvauksella luvun aihepiiristä. Kunkin luvun lopussa on kysymyksiä, joiden avulla voi tarkemmin hahmotella tietotilinpäätöksen mukaan otettavia asioita. Tarkoitus ei ole vastata kaikkiin kysymyksiin vaan soveltaa niitä siten, että tietotilinpäätös vastaa oman organisaation tarpeisiin. Tietotilinpäätöksessä kannattaa hyödyntää mahdollisuuksien mukaan erilaisia havainnollistavia esitystapoja, kuten kaavioita ja kuvitusta.

**[Mallipohja – Tietotilinpäätös on organisaatiokohtainen asiakirja, joka muotoutuu kunkin organisaation omien tarpeiden mukaan. Tässä esitetty rakenne ja sisältö ovat vain viitteellisiä.]**

**[Organisaatio] TIETOTILINPÄÄTÖS vuosi [xxxx]**

***Pituus****:*

***Aikataulutus****: kerran vuodessa vuosikellon mukaan, muulloin pyydettäessä*

***Tarkoitus****: Osoitusvelvollisuuden toteennäyttäminen, organisaation tietojen käsittelyn kuvaus, sisäisen valvonnan työkalu, suunnittelun ja toiminnanohjauksen sekä raportoinnin ja johtamisen tuki.*

***Rajaukset****:*

**Päiväys ja laatija:**

**Allekirjoitukset tai muu hyväksyntä:**

SISÄLLYSLUETTELO

[1 Johdanto 3](#_Toc80254583)

[SAATE 4](#_Toc80254584)

[JULKINEN TIIVISTELMÄ 7](#_Toc80254585)

[TIIVISTELMÄ JOHDOLLE 8](#_Toc80254586)

[1.1.1 JOHDANTO 9](#_Toc80254587)

[1.1.2 LAINSÄÄDÄNTÖ JA MUU OHJEISTUS 10](#_Toc80254588)

[1.1.3 TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN 11](#_Toc80254589)

[1.1.4 TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT 12](#_Toc80254590)

[1.1.5 REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN 13](#_Toc80254591)

[1.1.6 SEURANTA JA MITTARIT 14](#_Toc80254592)

[1.1.7 ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN 16](#_Toc80254593)

### JULKINEN TIIVISTELMÄ

Kirjoita tiivistelmä, kun olet saanut tietotilinpäätöksen valmiiksi. Kerro tiivistelmässä keskeisistä tietosuojaan, tietoturvaan, riskienhallintaan ja yleiseen tiedonhallintaan liittyvistä havainnoista ja vuoden aikana tapahtuneista tärkeimmistä tapahtumista esimerkiksi tietojärjestelmähankinnoista ja kehittämisprojekteista. Jos tekoälyä käytetään organisaatiossa merkittävissä määrin, kerro sen hyödyntämisestä. Tiivistä myös kehittämistarpeet tulevalla vuodelle.

### TIIVISTELMÄ JOHDOLLE

Kirjoita myös oma, erillinen tiivistelmä johdolle keskeisistä havainnoista, ja mittareista ja ehdotuksista toimenpiteiksi. Johdon tulee saada tästä tiivistelmästä kokonaiskuva henkilötietojen käsittelyn nykytilasta ja kehittämistarpeista. Huomioi, että johdon tiivistelmä saattaa sisältää salassa pidettävää tietoa. Jos johdon tiivistelmä sisältää salassa pidettävää tietoa, voi/kannattaa tiivistelmä laatia erillisenä asiakirjana, jolloin tietotilinpäätöstä voidaan käsitellä täysin julkisena asiakirjana.

### JOHDANTO

Tietotilinpäätös tarjoaa ajantasaisen **tilannekuvan** organisaation henkilötietojen käsittelyn nykytilasta sekä arvion tietosuojan toteutumisesta. Tietotilinpäätöksessä kartoitetaan henkilötietojen käsittelyyn liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä. Tavoitteena on tukea tietosuojatyön tekemistä ja lisätä tekemisen vaikuttavuutta. Tietotilinpäätös toimii myös yhtenä **osoitusvelvollisuuden** osoittamisen välineenä **ja sisäisen ja ulkoisen valvonnan raporttina**. Osoitusvelvollisuuteen kuuluu mm. se, että organisaation **sopimuksissa ja alihankinnoissa** on huomioitu tietosuojan ja -turvan vaatimukset. Lisäksi rekisterinpitäjä tulee huomioida rekisteröidyn henkilötietojen käsittelyyn kohdistuvat **riskit.** Rekisterinpitäjän tulee huolehtia siitä, että henkilöstöllä ja ulkopuolisilla henkilötietojen käsittelijöillä on tarvittava **ohjeistus ja osaaminen**.

Rekisterinpitäjän tulee myös **seurata, raportoida ja valvoa** tietosuojaan ja -turvaan liittyviä asioita ja huolehtia siitä, että tietosuojaan koskeva sääntely toteutuu organisaatiossa. Osoitusvelvollisuuteen kuuluu myös **sisäänrakennetun tietosuojan** vaatimus, millä tarkoitetaan sitä, että tietosuojaperiaatteet toteutuvat kaikissa käsittelyn vaiheissa. Tietosuojaperiaatteet (5 art.) ovat 1. lainmukaisuuden, kohtuullisen ja läpinäkyvyyden periaate, 2. käyttötarkoitussidonnaisuuden periaate, 3. tietojen minimoinnin periaate 4. täsmällisyyden periaate, 5. säilytyksen rajoittamisen periaate ja 6. eheyden ja luottamuksellisuuden periaate.

Tietotilinpäätöksellä voidaan lisätä luottamusta siihen, että organisaatiossa noudatetaan edellä mainittuja tietosuojaperiaatteita ja käsitellään henkilötietoja sen mukaisesti. Hyvin hoidetulla tietosuojatyöllä vaikutetaan organisaation tehokkuuteen ja kilpailukykyyn. Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista.

Avainsanat: kokonaiskuva, osoitusvelvollisuus, sisäinen ja ulkoinen raportointi, sopimus, alihankinta, riskit, ohjeistus, osaaminen, valvonta, sisäänrakennettu tietosuoja

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin tarvittavilta osin]*

*[Kuvaa tietotilinpäätöksen tarkoitus, tavoitteet ja kohderyhmät. Keskitytäänkö tietosuojaan ja tietoturvaan vai laajemmin tiedonhallinnan kokonaisuuteen? Onko tietotilinpäätös osa strategiatyötä ja kehittämistyötä? Kerro, miten ja milloin tietotilinpäätös julkaistaan ja kuka työstä vastaa. Kerro lisäksi, miten tietotilinpäätöksen tiedot on koottu. Kerro keskeisistä tietosuojaan, tietoturvaan, riskienhallintaan ja yleiseen tiedonhallintaan liittyvistä vuoden aikana tapahtuneista tärkeimmistä tapahtumista, esimerkiksi tietojärjestelmähankinnoista ja kehittämisprojekteista. Sisältääkö tietotilinpäätös rajoituksia, onko siinä erikseen julkinen ja salassa pidettävä osio? Suositus on, että tietotilinpäätös olisi pääosin julkinen, mutta esimerkiksi tietoturvallisuuteen liittyvät asiat voivat olla salassa pidettäviä.]*

### LAINSÄÄDÄNTÖ JA MUU OHJEISTUS

Julkishallinnon organisaatiot noudattavat **Suomen ja EU:n lainsäädäntöä**. Organisaatioita ohjaavat mm. hallintolaki, julkisuuslaki, tietosuoja-asetus, tietosuojalaki, tiedonhallintalaki, arkistolaki sekä lukuiset muut yleis- ja erityislait. Lisäksi **rahoittajat** (projektit, hankkeet) antavat omia ohjeistuksia henkilötietojen käsittelystä, säilyttämisestä ja arkistoinnista. Organisaatio voi toimia myös käsittelijänä toisen rekisterinpitäjän lukuun. Sen lisäksi organisaatioilla on omia **käytännesääntöjä ja ohjeistuksia** sekä **kansallisia tai kansainvälisiä sertifikaatteja**. Organisaatioissa on myös omavalvontaa, sisäisiä tarkastuksia ja auditointeja. Tässä luvussa tehtävänä käydään läpi lainsäädännöllistä ja omien ohjeistuksiin ja politiikkoihin liittyviä taustoja tietojenkäsittelyn osalta. Toisaalta tiedon laatuun ja käytettävyyteen liittyvät tekijät tulisi myös huomioida tietotilinpäätöksessä. Sosiaali- ja terveyspalvelujen tuottajien on laadittava tietosuojan ja tietoturvan omavalvontasuunnitelma, jonka malli saattaa olla hyödynnettävissä tietototilinpäätöksessä. Tässä luvussa vastataan tietosuojaperiaatteiden kysymyksiin koskien tietojenkäsittelyn lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä.

Avainsanat: lainsäädäntö, kansallinen, EU, rahoittajat, käytännesäännöt, ohjeistukset, politiikat, sertifikaatit, omavalvontasuunnitelma

*[Käy läpi keskeinen lainsäädäntö, ohjeistukset, toimintapolitiikat, strategiat, sertifioinnit, sisäiset tarkastukset ja auditoinnit. Ota huomioon myös mahdolliset rahoittajien ohjeistukset.]*

### TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

Tietosuoja-asetuksen (artikla 24) mukaan rekisterinpitäjä on vastuussa siitä, että se toteuttaatarvittavat **tekniset ja organisatoriset toimenpiteet**, joilla osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän on huomioitava henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudelta vaihtelevat riskit ja suhteuttava toimenpiteet näiden mukaisesti. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutuksia, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tila- ja käytönvalvontaa, pääsynhallinta, päivitysten ja muutosten hallintaa, fyysistä turvallisuutta, henkilöstöturvallisuutta, toimittajien ja sopimusten hallintaa, tietoturvallisuuden hallintaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, käytännesääntöjen sekä sertifikaattien käyttöä. Tässä kappaleessa annetaan kuva siitä, miten tiedon eheys, saatavuus ja luottamuksellisuus taataan sekä myös tiedon läpinäkyvyys (5 art.).

Avainsanat: tekniset ja organisatoriset toimenpiteet

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin tarvittavilta osin]*

 *[Kuvaus toimintaympäristöstä, miten tietoturva ja -tietosuoja on organisoitu ja millainen on tietosuojan ja -turvan hallintamalli ja/tai kehittämismalli, esim. kuka vastaa mistäkin asiasta, miten tietohallinto on järjestetty, hoidetaanko omana työnä, onko ulkoistettu. Onko seloste käsittelytoimista (30 art.) tehty ja tarvittaessa saatavilla. Huomioi myös tietosuojavastaavan rooli ja käytetäänkö esim. vuosikelloa. Kerro miten henkilökunnan koulutukset ja perehdytykset hoidetaan sekä laaditut toimintapolitiikat ja muut ohjeistukset sekä omalle että ulkopuolisille henkilötietojen käsittelijöille ja kuka näiden ajantasaisuudesta vastaa. Kuvaa myös, miten on toteutettu muut tekniset ja organisatoriset toimenpiteet (riskianalyysit, vaikutustenarvioinnit, ennakkokuulemiset, omavalvontasuunnitelma, jatkuvuuden hallinta, päivitysten ja muutosten hallinta, henkilötietojen tietoturvapoikkeamiin varautuminen, työntekijöiden turvallisuusselvitykset, salassapitosopimukset, tila- ja käytönvalvonta, etäyhteydet, kryptaus, pseudonymisointi.) IT-sopimuskumppanit, miten sovellusten ja tietokoneiden ym. hankinta, käyttöönotto, kehittäminen ja ylläpito on toteutettu?*  *Miten tietosuoja- ja tietoturvariskit huomioidaan hankinnoissa ja palveluostoissa?* *Miten on hoidettu valvonta ja sisäinen tarkastus? Onko olemassa laatustandardeja, käytännesääntöjä, auditointeja tai sertifiointeja. Vastaa kysymykseen siitä, miten huolehditaan tietojen laadusta ja saatavuudesta. Ota huomioon myös erilaiset tutkimusluvat, niiden käsittely ja organisaation ohjeistus rekisteröityjen oikeuksien toteuttamisesta.]*

### TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT

Tiedonhallintalaki edellyttää, että tiedonhallintayksikön tulee ylläpitää sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia, joka sisältää tiedot mm. toimintaprosesseista, tietovarannoista, tietoaineistoista, arkistoinnista, tietojärjestelmistä ja tietoturvallisuustoimenipiteistä. Tämä tapahtuu esimerkiksi kokonaisarkkitehtuurin, tietojärjestelmäarkkitehtuurin, tietovarantokuvausten, asiakirjajulkisuuskuvauksen, tiedonohjaussuunnitelmien ja erilaisten prosessikuvausten avulla. Tiedonhallintamallia ylläpidetään palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi.

Tarkoituksena on selventää sitä, miten tietoa hallintaa sen koko **elinkaaren** ajan, tiedon vireille tulosta hävittämiseen tai arkistointiin saakka. Lisäksi kuvaukset toimivat ja toteuttavat julkisuusperiaatetta sekä toimivat omien tietojen pyyntöön liittyvinä apuvälineitä. Tiedonohjaussuunnitelmilla voidaan todentaa esimerkiksi sitä, että tietojen säilytysajat on määritelty asianmukaisesti ja että niiden hävittäminen on suunnitelmallista. Tietovarantoja ja tietojenkäsittelyä saatetaan hoitaa myös organisaation ulkopuolella, esim. palkanlaskenta. Organisaatiolla on olemassa ohjeistus ja sopimukset näihin ulkoisiin tietojenkäsittelytilanteisiin. Organisaatio voi myös käsitellä tietoja käyttäen omia palvelinsalejaan tai ulkoisista pilvipalveluista.

Organisaatio voi johtaa tiedolla ja hyödyntää omaa tietopääomaansa vain, jos johdolla on tarpeeksi tietoa muun muassa omasta toiminnasta, toimintaympäristöstään, prosessien toimivuudesta, henkilökunnan osaamisesta, tietovirroista ja tietovarannoista. Tässä luvussa kuvataan muun muassa sitä, miten organisaatio toteuttaa tietosuojaperiaatteina tietojen minimointia, käyttötarkoitussidonnaisuutta ja säilytyksen rajoittamista ja tiedon läpinäkyvyyttä.

Avainsanat: tiedonhallintamalli, kuvaukset, kokonaisarkkitehtuuri, tietovarannot, tiedonohjaussuunnitelmat, prosessikuvaukset, tiedon elinkaari

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin tarvittavilta osin]*

 *[Kuvaus tiedonhallintayksikön vastuiden, tiedonhallintamallin ja muutosvaikutusten arviointiprosessin organisoimisesta. Kerro mitä keskeisiä tietovarantoja ja tietojärjestelmiä on olemassa? Onko henkilötiedoille/rekistereille merkitty käyttötarkoitukset. Miten on huolehdittu tiedon elinkaaren hallinnasta mukaan lukien säilytysajat, hävittäminen ja arkistointi. Kerro tilanne koskien kokonaisarkkitehtuurikuvauksia, asiakirjajulkisuuskuvausta, tiedonohjaussuunnitelmia, arkistonmuodostussuunnitelmia, prosessikuvauksia, tietovirtakuvauksia, tietojärjestelmäkuvauksia ym. Onko ulkopuolisia henkilötietojen käsittelijöitä ja tietovarantoja, käytetäänkö pilvipalveluita. Onko tehty tarvittavat sopimukset ja ohjeistukset henkilötietojen käsittelijöiden kanssa. Miten organisaatiossa on huolehdittu tiedonsaannista ja tietojen luovuttamista, onko olemassa sähköisen asioinnin kanavia, rajapintoja, katseluyhteyksiä. Hyödynnetäänkö tietoa, onko olemassa avointa dataa, mitä julkaistaan ja mistä löytyy, onko tehty tiedolla johtamisen määrityksiä]*

### REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN

Jokaisella on oikeus henkilötietojensa suojaan. Tietosuoja on perusoikeus, jonka tarkoituksena on turvata **rekisteröidyn oikeuksien ja vapauksien** toteutuminen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Rekisterinpitäjän velvollisuus on huolehtia rekisteröidyn oikeuksien toteutumisesta. Näitä ovat muun muassa rekisteröidyn oikeus saada tietoa henkilötietojen käsittelystä, oikeus saada pääsy tietoihin ja oikeus oikaista virheellisiä tietoja. Lisäksi rekisteröidyillä on oikeus tietyillä rajauksilla saada tieto sosiaali- ja terveydenhuollon käyttö ja -luovutustiedoista. Rekisterinpitäjän tulee **informoida** rekisteröityjä henkilötietojen käytöstä avoimesti ja selkeästi. Rekisterinpitäjän tulee myös varautua mahdollisiin henkilötietojen tietoturvaloukkauksiin ja harjoitella niihin varautumista käytännössä. **Henkilötietojen tietoturvaloukkauksia** ovat mm., että tiedot lähetetty väärälle vastaanottajalle, suojaamaton tiedonsiirtoväline on hävinnyt esim. USB-tikku, haittaohjelmatartunta, kyberhyökkäys ja hakkerointi. Rekisterinpitäjän tulee tilastoida henkilötietojen tietoturvaloukkaukset ja ilmoittaa niistä tietosuojavaltuutetun toimistolle ja tietyn edellytyksin myös rekisteröidyille. Henkilötietojen käsittelijöillä on velvollisuus puolestaan ilmoittaa henkilötietojen tietoturvaloukkauksista rekisterinpitäjälle. Tässä luvussa kuvataan tietosuojaperiaatteina erityisesti läpinäkyvyyttä ja kohtuullisuutta.

Avainsanat: rekisteröityjen oikeudet, informointi, henkilötietojen tietoturvaloukkaukset

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin]*

[*Kuvaa, miten organisaatiossa on hoidettu rekisteröityjen informointi, onko esim. tietosuojaselosteita muita informoinnin menetelmiä käytössä ja miten rekisteröidyn oikeudet toteutuvat organisaatiossa käytännössä. Kerro myös mistä tietosuojaselosteet ja muu informointimateriaali löytyvät. Kuvaa myös tietopyyntö-virheenkorjaus ja lokitietojen pyyntöön liittyvät prosessit sekä henkilötietojen tietoturvaloukkausprosessit ja mistä näihin liittyvät mahdolliset lomakkeet löytyvät. Ota huomioon myös tutkimuslupien käsittely ja rekisteröityjen oikeudet erilaisissa tutkimuksissa. Kerro myös henkilötietojen tietoturvaloukkausten harjoittelusta ja mahdollisista muista harjoituksista.]*

### SEURANTA JA MITTARIT

Organisaatiolla on velvoitteita kuvata erilaisilla mittareilla toimintaansa. Osa mittaristosta palvelee organisaation omaa tarvetta ja osa mittareita ovat sellaisia, joita joudutaan raportoimaan muualla. Ilman mittareita on vaikea tietää, miten organisaatio on kehittynyt ja mitä osa-alueita tulee vielä kehittää. Alla on kuvattu yleisimpiä tiedonhallintaan, tietosuojaan, tietoturvaan ja riskienhallintaan liittyviä mittareita. Organisaatio valitsee omien tarpeidensa mukaan käytettävät mittarit ja voi myös seurata muita asioita, mitkä koetaan tarpeelliseksi ja omaa toimintaa kuvaavaksi. Tarvittaessa mittareiden toteumat voi jaotella organisaation toiminnan kannalta tarkoituksenmukaisesti, kuten esim. kunnassa toimialakohtaisesti (omiin sarakkeisiin sote/ muut toimialat). Mittarit on ryhmitelty kuuteen eri osioon. Näitä ovat tietohallinto, riskien arviointi ja tarkastukset, tietovarannot, asianhallinta, osaaminen ja ohjeistus sekä rekisteröidyn oikeudet.

 Voit myös kuvata sidosryhmäyhteistyötä alueellisissa ja kansallisissa tietosuoja- ja tietoturvaryhmissä.

[*Voit hyödyntää alla olevia tunnuslukuja, poistaa omalle organisaatiolle tarpeettomat mittarit tai lisätä oman organisaatiosi kannalta uusia merkityksellisiä tunnuslukuja.]*

|  |  |  |  |
| --- | --- | --- | --- |
| **Tunnusluku** | **Mittari** | **Toteuma 2020** | **Toteuma 2019** |
| **Tietohallinto** |  |  |  |
| Työasemat | lkm |  |  |
| Käyttäjien (AD-tunnuksia) | lkm |  |  |
| Käyttötukipyynnöt  | lkm |  |  |
| Matkapuhelimia  | lkm |  |  |
| Kannettavat tietokoneet  | lkm |  |  |
| IT-palvelut, tietohallinto | htv |  |  |
| IT-ulkoiset sopimuskumppanit | lkm |  |  |
| Tietosuoja-tietoturva hlöstö | htv |  |  |
| Tietojärjestelmien kehittämisbudjetti | euroa |  |  |
| Käynnissä olevat projektit, joissa IT-osuus | lkm |  |  |
| **Riskien arviointi ja tarkastukset** |  |  |  |
| Tehdyt riskianalyysit, (sis. esim. HaiPro) | lkm |  |  |
| Tehdyt vaikutustenarvioinnit | lkm |  |  |
| Tehdyt ennakkokuulemiset | lkm |  |  |
| Tehdyt turvallisuusselvitykset | lkm |  |  |
| Tehdyt tarkastukset | lkm |  |  |
| Tehdyt auditoinnit, sisäiset | lkm |  |  |
| Tehdyt auditoinnit, ulkoiset | lkm |  |  |
| Sertifikaatit | lkm |  |  |
| Omavalvontasuunnitelma | lkm |  |  |
| **Tietovarannot** |  |  |  |
| Kokonaisarkkitehtuurikuvaus valmiusaste | % |  |  |
| Prosessikuvaukset valmiusaste | % |  |  |
| Tiedonohjaussuunnitelmat valmiusaste | % |  |  |
| Tietovirtojen kuvaukset valmiusaste | % |  |  |
| Tietovarannot | lkm |  |  |
| Tietojärjestelmät | lkm |  |  |
| Pilvipalvelut | lkm |  |  |
| Rajapinnat | lkm |  |  |
| Katseluyhteydet | lkm |  |  |
| Sähköisen asioinnin kanavat | lkm |  |  |
| Avattua dataa | lkm |  |  |
| **Osaaminen ja ohjeistus** |  |  |  |
| Henkilöstön koulutukset | % |  |  |
| Luottamushenkilöiden koulutukset | % |  |  |
| Henkilöstön osaamiskartoitukset | % |  |  |
| Seloste käsittelytoimista (30 art.) valmiusaste | % |  |  |
| Ohjeiden ajantasaisuus | % |  |  |
| Ohjeiden päivittämissykli | lkm |  |  |
| **Asianhallinta** |  |  |  |
| Asiarekisteriin rekisteröidyt asiat | lkm |  |  |
| Tieto- ja asiakirjapyynnöt (Julkisuuslaki) | lkm |  |  |
| Aineistojen digitointi | lkm |  |  |
| Analogiset arkistoaineistot | hm |  |  |
| **Rekisteröidyn oikeudet** |  |  |  |
| Tietosuojaselosteet ja muu informointi valmiusaste | % |  |  |
| Henkilötietojen tietoturvaloukkaukset | lkm |  |  |
| Henkilötietojen tietoturvaloukkaukset ilmoitukset/ TSV | lkm |  |  |
| Henkilötietojen tietoturvaloukkaukset ilmoitukset/ rekisteröidyille | lkm |  |  |
| Henkilötietojen tietoturvaloukkausharjoitukset | lkm |  |  |
| Tehdyt tarkastuspyynnöt | lkm |  |  |
| Tehdyt poistopyynnöt | lkm |  |  |
| Tehdyt korjauspyynnöt | lkm |  |  |
| Käyttö- ja luovutuslokipyynnöt | lkm |  |  |
| Esille tulleet tietosuojarikkomukset  | lkm |  |  |
| Epäillyt tietosuojarikkomukset | lkm |  |  |
| Palveluestohyökkäykset | lkm |  |  |
| Virushavainnot | lkm |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN

Organisaation tulee arvioida tietosuojan ja -turvan tilanne toimintapolitiikan, mittareiden, kokonaisarkkitehtuuri ja muiden kuvausten avulla sekä mahdollisten asiakkaiden ja henkilöstön palautteiden näkökulmasta ja verrata kehitystä aiempiin vuosiin. Henkilöstön osaamisen sekä käsittelytoimien, tietovirtojen ja toimintaprosessien arviointi ja kehittäminen ovat keskiössä. Organisaation johto voi johtaa tiedolla vain, jos sillä on riittävä ymmärrys omasta toiminnasta ja toimintaympäristöstään. Tavoitteena on päästä kohti tiedon hyödyntämistä. Tarkoituksena on tuoda esille myös keskeiset kehittämistavoitteet. Samalla on myös arvioitava asetettujen kehittämistavoitteiden toteutumista.

[*Täydennä oman organisaatiosi kannalta vastaamalla alla oleviin kysymyksiin]*

*[Kuvaa organisaation nykytilanne, tunnistetut kehittämistarpeet ja toteutetut kehittämistoimenpiteet. Arvioi tehtyjen kehittämistavoitteiden toteutumista ja tee suositukset tarvittaviksi kehittämistoimiksi. Mieti henkilökunnan osaamistarpeet, millaista koulutusta, ohjeistusta, prosessien kehittämistä tarvitaan. Miten tekoälyä ja tietoa hyödynnetään, onko olemassa avointa dataa, mitä julkaistaan ja mistä löytyy, onko tehty tiedolla johtamisen määrityksiä. Kuvaa kokonaisarvio mm. asiakastyytyväisyydestä, henkilökunnan tyytyväisyydestä ja erilaisten tiedonhallintaa liittyvien prosessin toimivuudesta.]*