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



[Nimi]

TIETOTILINPÄÄTÖS VUODELTA [XXXX]

[Päiväys ja laatija]

[allekirjoitukset tai muu hyväksyntä]

*[Raportin varsinaisesta tekstiosuudesta löytyy arviointia ja pohdintaa kuhunkin lukuun.]*

*[Taustaksi kannattaa perehtyä EU:n tietosuoja-asetuksen 5. artiklaan]*

*[Tietotilinpäätösmalli on rakennelma tai kehikko, joka on syntynyt tietosuojavaltuutetun ohjeeseen pohjautuen sekä tietotilinpäätösdokumentteja ja haastatteluja hyödyntäen. Kuitenkin niin, että kyseessä on prosessinkuvauksen tuloksena syntynyt dokumentti, jonka sisältö muotoutuu vasta organisaation käytännössä. Sellaisenaan se ei esitä yhtä totuutta, vaan kuten jo tietosuojavaltuutetun ohjeistuksessa mainitaan, niin tietotilinpäätös on aina toimiala sekä organisaatio kohtainen. Tietotilinpäätökselle organisaatiossa annettu merkitys vaikuttaa dokumentin rakenteeseen sekä sisältöön - epäilemättä myös prosessiin ja toimijoihin. Työ on tehty osana Tampereen yliopiston hallintotieteiden kurssia Konsultoiva asiantuntijatyö organisaatiossa keväällä 2018.]*

***[Pituus****: noin 15-20 sivua.*

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

***Tarkoitus****: Osoitusvelvollisuuden toteennäyttäminen, luottamuksen osoittamista sidosryhmiin nähden, johdon työväline tai sisäisen valvonnan työkalu. Vaikuttaa rakenteeseen, minkä takia myös edellä esitetty rakenne on viitteellinen.*

***Prosessi:*** *Yleensä tietosuojavastaava kerää tiedot osastoittain, mutta muitakin ratkaisuja voi olla. Kyseessä on yhden tietyn hetken tilanne. Tieto tuotetaan yleensä prosessin kautta, joka kehittyy kokemuksen myötä.*

***Painotukset****: Organisaatio ja toimialakohtaiset merkitykset.]*

[1 TIETOTILINPÄÄTÖKSEN TARKOITUS [XX] KUNNASSA 1](#_Toc521178006)

[2 TIETOTURVALLISUUDEN JA -SUOJAN TOTEUTTAMINEN ORGANISAATIOSSA 2](#_Toc521178007)

[3 TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT 4](#_Toc521178008)

[4 TIETOJENKÄSITTELYYN VAIKUTTAVA LAINSÄÄDÄNTÖ JA MUU OHJEISTUS 6](#_Toc521178009)

[5 REKISTERÖIDYN OIKEUDET JA NIIDEN TOTEUTUMINEN 7](#_Toc521178010)

[6 SEURANTA JA MITTAAMINEN 8](#_Toc521178011)

[7 ARVIOINTI JA KEHITTÄMINEN 9](#_Toc521178012)

[LÄHTEET 10](#_Toc521178013)

## 1 TIETOTILINPÄÄTÖKSEN TARKOITUS [XX] KUNNASSA

Tämän luvun tehtävänä on toimia tietotilinpäätöksen johdantona. Tekstistä olisi hyvä käydä ilmi tietotilinpäätöksen merkitys organisaatiossa ja kenelle se on varsinaisesti kohdennettu. Tämä kertoo luonnollisesti myös raportin sisällön painotuksista. Onko tietotilinpäätös osa strategiatyötä? Tietotilinpäätös voi olla osoitusvelvollisuuden osoittamisen väline, sisäisen ja ulkoisen valvonnan raportti, luottamuksen osoitusta rekisteröityjen ja sidosryhmien suuntaan, johdon työväline tai niitä kaikkia yhdessä. Raportin tässä vaiheessa tuntuisi luontevalta myös selvittää onko käsillä oleva dokumentti tiivistelmä tai onko erikseen rakennettu julkinen ja salainen versio. Näillä seikoilla on luonnollisesti vaikutusta myös sisältöön.

Johdannossa voidaan esimerkiksi kuvata, miten tietotilinpäätöksen tiedot on kerätty. Myös tietosuojaan ja laajemmin tiedonhallintaan liittyvien keskeisten käsitteiden kuten osoitusvelvollisuuden avaaminen saattaa olla erityisesti sidosryhmänäkökulman kannalta perusteltua. Tietosuojaperiaatteista lainmukaisuuden ilmeneminen organisaatiossa voisi olla hyvä esittää jo tässä alussa kuntalain, hallintolain, julkisuuslain ja EU:n yleisen tietosuoja-asetuksen kautta yleisesti.

Lopuksi voisi olla paikallaan tiivistelmän tekeminen käsitellyistä asioista, mikä sisältäisi myös katsauksen tärkeimpiin tapahtumiin. Varsinkin, jos organisaatiossa on ollut laajempi tietoturvapoikkeama (tietovuoto).

## 2 TIETOTURVALLISUUDEN JA -SUOJAN TOTEUTTAMINEN ORGANISAATIOSSA

Tämä luvun tehtävänä on selvittää tietoturvan ja tietosuojan organisoinnin toteuttamisen menetelmiä organisaatiossa. Tietosuoja- ja tietoturvatyön organisointi ja sitä myöten myös tietosuojavastaavan rooli on merkittävä tekijä myös tietoturvan kannalta. Rekisterinpitäjä on tietosuoja-asetuksen (artikla 24) mukaan vastuussa siitä, että se toteuttaatarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutusta, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tilivalvontaa ja käytönvalvontaa, tietojen salausta, tietojen anonymisointia tai pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, käyttövalvontaa, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, tietotilinpäätösprosessia, käytännesääntöjen sekä sertifikaattien käyttöä. (Kuntaliiton yleiskirja 14/2017) Näiden ohella tällä kohdin voisi miettiä etenkin tietojen saatavuuden, eheyden (oikeellisuus ja ristiriidattomuus) ja luottamuksellisuus sisältöä.

Ennen kaikkea pitäisi muistaa, ettei tietosuojaa ole olemassa ilman tietoturvaa. Tietosuojatyön organisoinnin kannalta työhön mukaan kannattaa ottaa yksiköitä, jotka käsittelevät henkilötietoja tai jotka huolehtivat järjestelmien tai sovellusten hankinnasta, käyttöönotosta, kehityksestä tai ylläpidosta. (VAHTI-raportti 2016, 20) Tietoturvallisuuden toteuttamiseksi voidaan organisaatiossa käyttää hyväksi hallintamalleja esim. ISO/IEC 27001 ja niihin liittyviä auditointeja. EU:n tietosuoja-asetus velvoittaa siihen, että henkilötietojen tietosuojasta on huolehdittava koko niiden elinkaaren ajan. Joka tapauksessa kunkin organisaation on itse suhteutettava tietoturva omaan kokoonsa ja toimintaansa nähden ylimitoittamatta sitä.

Tietosuoja-asetuksessa omaksutun riskiperusteisen lähestymistavan mukaan asetuksessa vaaditut konkreettiset toimenpiteet suhteutetaan henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. VAHTI-raportti (2016, 24-26) on tiivistänyt tietosuojan kannalta tärkeimpiä osa-alueita, joista voisi tarvittavin määrin mainita myös tietotilinpäätöksessä. Näitä ovat jatkuvuus ja riskienhallinta, riskianalyysi, turva-arkkitehtuuri, tietojärjestelmien hankinta, kehitys ja ylläpito, pääsynhallinta, omaisuuden ja tiedon hallinta, päivitysten ja muutosten hallinta, fyysinen turvallisuus, henkilöstöturvallisuus, toimittajien ja sopimusten hallinta, toiminnan jatkuvuuden hallinta, käsittelyn valvonta ja seuranta sekä tietoturvallisuuden hallinta. Lisäksi kannattaa huomioida laatustandardit ja auditoinnit sekä sidosryhmien kanssa tehdyt sopimukset. Erityisen tärkeää raportointia tietotilinpäätöksessä olisi myös tietoturvapoikkeamien käsittely, niiden määrät ja merkitys sekä siihen liittyvä ilmoitusvelvollisuus. (kts. esim. VAHTI-raportti 2017)

Tietotilinpäätöksessä voidaan myös kertoa tehdyistä tietosuojaan ja yksilön vapauksiin suunniteltujen henkilötietojen käsittelytoimien vaikutustenarvioinnista (PIA/DPIA) sekä ennakkokuulemisista (artikla 35 ja 36) (kts. esim. VAHTI-raportti 2016,13, Tietosuojavaltuutetun toimisto: vaikutustenarviointi 2018, Tietosuojatyöryhmä WP29 2017).

Tietosuojaperiaatteina voidaan tässä kohdin peilata erityisesti tiedon eheyttä ja luottamuksellisuutta (Tietosuojaperiaatteet artikla 5).

## **3 TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT**

Tämän luvun tehtävänä on toimia organisaation tiedonhallinnan, tietovarantojen sekä niihin liittyvien tietovirtojen kokonaistilan kuvauksen tiivistelmänä. Tässä voi huomioida oman tarpeen ja käyttötarkoituksen mukaan seuraavia seikkoja: kokonaisarkkitehtuuri (JHS 179), tietohallintolaki kokonaisuuden hallinnassa (tiedonhallinta ja tiedon elinkaari), tietojärjestelmäarkkitehtuuri, tietovarannot.

Tietovirtojen (viranomaiset, yksityiset, muut) tulisi vastata kysymyksiin keneltä ja kenelle.



Yllä on yksinkertaistettu kuva tietovirroista (VAHTI-raportti 2016, 32)

Tiedonhallinta (tiedolla johtaminen) ja tietojen luovutusten periaatteet olisi myös hyvä olla kuvattuna. Toimintatapojen dokumentointi voi sisältää kokonaisarkkitehtuuriperiaatteet (henkilötietojen käsittelyn osalta), tiedonohjaussuunnitelmat, sekä ICT-hankintojen tietosuojavaatimukset ja sopimusmallit, tietovirtakaaviot, henkilötietojen hallinta ja kulku, henkilötietoja sisältävät tietojärjestelmät.

Olennaista on kertoa tiedonhallinnan organisoinnista ja erityisesti tiedonohjaussuunnitelmien hyödyntämisestä osana tiedonhallintaa ja tietosuojan toteuttamista. Tiedonohjaussuunnitelmilla voidaan todentaa esimerkiksi sitä, että tietojen säilytysajat on määritelty asianmukaisesti ja että niiden ajanmukainen hävittäminen on suunnitelmallista.

Tietosuojaperiaatteina tällä osin voi peilata tietojen minimointia, käyttötarkoitussidonnaisuutta sekä tietojen säilytyksen rajoittamista. (Tietosuojaperiaatteet artikla 5)

4 TIETOJENKÄSITTELYYN VAIKUTTAVA LAINSÄÄDÄNTÖ JA MUU OHJEISTUS

Tässä luvussa tehtävänä on käydä läpi lainsäädännöllistä taustaa tietojenkäsittelyn osalta. Käytännesäännöt ja sertifioinnit sekä auditoinnit ovat myös osa tähän liittyvää ohjeistusta. Näitä on voitu käsitellä myös esimerkkimallin luvussa 2. Yleisiä tietosuojaperiaatteita EU:n tietosuoja-asetuksen (5. ja 6. artikla) mukaisesti voidaan tässä avata enemmänkin käytäntöön.

Laaditut tietosuojaselosteet ja niiden ajantasaisuus ovat myös tärkeitä seikkoja tietotilinpäätösraportoinnissa. Näihin kuuluvat erilaiset toimintapolitiikat, tietoturva- ja tietosuojapolitiikat, ohjeet ja henkilöstön koulutukset, perehdytykset sekä seloste henkilötietojen käsittelytoimista (30. artikla). Toisaalta tiedon laatuun ja käytettävyyteen liittyvät tekijät tulisi myös huomioida dokumentissa.

Tietosuojaperiaatteina tässä kohdin voi peilata lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä (Tietosuojaperiaatteet artikla 5).

5 REKISTERÖIDYN OIKEUDET JA NIIDEN TOTEUTUMINEN

Tällä kohdin tulisi miettiä etenkin tietosuojaperiaatteista läpinäkyvyyttä ja

tietojen täsmällisyyttä. Tietosuojapoikkeamista ja niihin varautumista voitaisiin tarvittaessa selventää henkilötietojen käsittelyn näkökulmasta. Lisäksi voisi olla hyvä ottaa esille tarkistusoikeudet sekä virheenkorjauspyyntöjen lukumäärät. Tietosuojaselosteiden ajantasaisuus on myös osa rekisteröityjen oikeuksien toteutumista. (artiklat 13 ja 14)

Luottamuksen osoittamisen pohjalta avattuna voisi vielä olla EU:n yleisen tietosuoja-asetuksen artikloiden sisältöjä oman organisaation kannalta katsottuna. Näin kyseeseen tulisivat ainakin seuraavat rekisteröidyn oikeuksia käsittelevät artiklat: rekisteröidyn oikeus saada pääsy tietoihin (artikla 15), oikeus tietojen oikaisemiseen (artikla 16), oikeus siirtää tiedot järjestelmästä toiseen (artikla 20) sekä tietoturvaloukkauksesta ilmoittaminen (artikla 33).

Viime kädessä on kyse siitä, mitä halutaan kertoa lukijalle. Silti tulee ennen kaikkea muistaa, että tietotilinpäätös on usein muutakin kuin vain henkilötietojen suojaamisen väline.

Tietosuojaperiaatteina tässä kohdin voi peilata erityisesti läpinäkyvyyttä ja kohtuullisuutta (Tietosuojaperiaatteet artikla 5).

6 SEURANTA JA MITTAAMINEN

Tämän luvun tehtävänä on koota yhteen organisaation tietosuojatyöhön liittyvät keskeiset seurannan menetelmät. Tärkeää on olla tietoinen organisaation tietosuojan nykytilasta, sillä se on merkittävää rekisterinpitäjän osoitusvelvollisuuden toteuttamisen kannalta. Siten säännöllisen raportoinnin tulisi sisältää tärkeimmät tietosuojaan ja henkilötietojen käsittelyyn liittyvät tekijät. Tällaisia ovat tietosuojamittarit sekä niiden käyttö raportointikauden aikana, tietosuojan kehityshankkeet ja niiden tilanne, havaitut puutteet ja tarpeet. Lisäksi merkittävimmät tietoturvaloukkaukset, joilla on tietosuojavaikutuksia, tehdyt riski- ja vaikutustenarvioinnit sekä niiden merkittävimmät löydökset hallintakeinoineen sekä rekisteröityjen oikeuksiin ja yhteistyöhön valvontaviranomaisten kanssa liittyvät tarpeelliset tiedot on hyvä olla osa raportointia. (Tietosuojayhteishanke työpaja 2017a)

Sosiaali- ja terveyspalvelujen tuottajien on laadittava tietosuojan ja tietoturvan omavalvontasuunnitelma, jonka malli saattaa olla hyödynnettävissä tietototilinpäätöksessä.

Omaan organisaatioon sopivat mittaristot ja tunnusluvut sekä niiden vertailu jatkuvuuden näkökulmasta lisää tämän luvun painoarvoa. IT-ympäristön dokumentointi kattaa puolestaan käyttövaltuudet ja pääsynhallinnan, auditoinnit, lokitarkastukset, tietosuoja- ja tietoturvaryhmät ja niiden kokoontumiset salassapitosopimukset. Koulutukset ja ohjeistukset (verkkokoulutukset ja muut koulutukset) voidaan esitellä myös tässä.

VAHTI-raporteista on saatavissa lisätietoa lokituksista ja tietoturvapoikkeamista:

Lokitietojen tarkastuspyynnöt ja lokitukset (VAHTI-raportti 2006)

Tietoturvapoikkeamien hallinta (VAHTI-raportti 2017)

Tämän työn liitteessä 2 on myös lisätietoa tunnusluvuista ja mittaristoista.

Raportointijärjestelmästä kokonaisuudessaan voisi tehdä yhteenvedon.

7 ARVIOINTI JA KEHITTÄMINEN

Tämän luvun tehtävänä on arvioida organisaation tietosuojan tilannetta sekä tuoda esille tietosuojaan liittyvät keskeiset kehittämistavoitteet. Tähän voidaan pyrkiä esimerkiksi kokonaisarkkitehtuurikuvauksella, jonka avulla voidaan tehdä organisaation kokonaiskehittämistä. Silti se ei korvaa muita kehittämisen menetelmiä. Toisaalta henkilökunnan tarpeita voidaan kuunnella koulutuksen, ohjeistuksen sekä prosessien tuntemisen lisäämiseksi. Miten organisaation tietosuojaosaamista lisätään?

Tässä osiossa voidaan arvioida tehtyjä kehittämistoimenpiteitä ja asettaa uusia. Miten organisaatio vastaa EU:n tietosuoja-asetuksen tuomiin haasteisiin? Onko luotu uusia prosesseja ja toimintatapoja, joilla pyritään näyttämään toteen asetuksen noudattaminen? Miten projekti ja sitä myöten prosessit ovat edenneet?

Politiikat ja ohjelmat sekä niiden mukanaan tuoma arvioinnin ja kehittämisen näkökulma on myös hyvä huomioida.

LÄHTEET