Tampereen ammattikorkeakoulu

Tietosuojaperiaatteiden toteutumisen mittaaminen julkishallinnon organisaatiossa

Tiina Apponen-Palo

OPINNÄYTETYÖ
Toukokuu 2023

Tietojärjestelmäosaaminen, ylempi AMK
Tampereen ammattikorkeakoulu

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojärjestelmäosaamisen ylempi tutkinto-ohjelma

APPONEN-PALO, TIINA:
Tietosuojaperiaatteiden toteutumisen mittaaminen julkishallinnon organisaatiossa

Opinnäytetyö 74 sivua, joista liitteitä 1 sivu
Toukokuu 2023

EU:n yleisen tietosuoja-asetuksen (EU:n yleinen tietosuoja-asetus 2016/679) yksi vaatimus on nimittää tietosuojavastaava käsiteltäessä laajamittaisesti henkilötietoja. Tietosuojavastaavan tehtävään kuuluu johdolle raportointi, josta on kirjoitettu vain vähän alan kirjallisuudessa.

Opinnäytetyön tavoite oli selvittää EU:n yleisen tietosuoja-asetuksen tietosuojaperiaatteiden toteutumisen mittaamista. Opinnäytetyö oli case-tutkimus, jonka kehittämistehtävän tarkoituksena oli laatia kehittämissuunnitelma julkishallinnon organisaation toimeksiantajalle tietosuojaperiaatteiden toteutumisen mittaamiseksi ja raportoinnin kehittämiseksi.

Tutkimusmenetelmäksi valittiin laadullinen tutkimus. Tutkittavaa ilmiötä lähestyttiin teoreettisen aineistoanalyysin ja teemahaastattelun aineiston perusteella. Laadullisessa tutkimuksessa teoreettinen viitekehys muodostettiin EU:n yleisen tietosuoja-asetuksen, tietosuojaperiaatteiden vaatimusten ja alan kirjallisuuden sekä ISO/IEC-standardien ympärille. Teoreettinen viitekehys täydennettiin mittaamisen menetelmien ja raportoinnin kirjallisuudella. Laadullisen tutkimuksen empiirisenä osuutena toteutettiin eri asiantuntijoille teemahaastatteluja, joissa tutkittavaa ilmiötä lähestyttiin teemojen riskienhallinta, raportointi ja mittaaminen avulla.

Tutkimuksen tärkeimmät löydökset tietosuojaperiaatteiden toteutumisen mittaamiseksi ovat tietosuojan hallintajärjestelmän, tietosuojan vaikutustenarvioinnin ja tietosuojavaatimusten mittaaminen joko sidosryhmittäin tai projektien kautta. Keskeisin löydös raportoinnin kehittämiseksi on ESG-raportoinnin hyödyntäminen raportointirakenteen laatimisessa. Kehittämissuunnitelmassa esitetään eri vaihtoehtoja tietosuojaperiaatteiden toteutumisen mittaamiseksi ja raportoinnin kehittämiseksi.

Esitettyjen mittareiden käyttöönotosta on merkittävää hyötyä ajantasaisen raportoinnin kehittämiseksi johdon päätöksenteon tueksi ja periaatteiden mittaamiseksi. Esitettyjen menetelmien avulla raportointi tietosuojaperiaatteiden toteutumisesta viedään osaksi organisaation raportointisykliä, ja siten kehitetään johdon kokonaiskuvaa organisaation tilasta.

Asiasanat: tietosuoja-asetus, tietosuojaperiaatteet, raportointi, mittaaminen, ISO/IEC27701 -standardi

ABSTRACT

Tampere University of Applied Sciences
Master's Degree Programme in Information System Competence

APPONEN-PALO, TIINA:
Measuring the Implementation of Data Protection Principles in a Public Administration Organisation

Master´s thesis 74 pages, appendices one page
May 2023

The objective of this thesis was to gather information about how to measure the implementation of Data Protection Principles. The purpose of the thesis was to prepare a development plan for the client at the public administration organisation to measure the implementation of Data Protection Principles and to develop reporting.

This study was carried out as a case-study. The theoretical framework was supplemented with literature on measurement methods and reporting. The empirical part consists of a theme interview with six experts. The phenomenon was approached using the themes of risk management, reporting, and measurement. The data were analysed using qualitative content analysis.

The main founding in this study is the measuring of the Privacy Information Management System (PIMS), Data Protection Impact Assessment (DPIA) and/or Data Protection requirements by target groups or through projects. These results suggest using ESG reporting as a structure to develop the reporting.

In this study presented alternatives has significant benefit for the decision-making and to measure Data Protection Principles. With these presented methods, reporting on the Data Protection requirements and principles will be included as part of the organisation's reporting cycle. Thus, the management's overall picture of the organisation's state is developed.

Key words: data protection regulation, data protection principles, reporting, measure, ISO/IEC27701 -standard

SISÄLLYS

LYHENTEET JA TERMIT

eNPS	työntekijän nettosuositteluindeksi (eng. Employee Net Promoter Score)
ESG	ympäristö, yhteiskuntavastuu ja hyvä hallintotapa (eng. Environmental Social Governance), vastuullisuusraportointi
KPI	suorituskykymittari, suorituskykymittaristo (eng. Key Performance Indicator)
Kypsyystaso	lähtötaso (eng. maturity)
Mittari	täsmällisesti määritelty menetelmä, jonka avulla kuvataan tietyn menestystekijän suorituskykyä tai tunnuslukuja
Mittaristo	kokonaisuus, joka muodostuu mittauskohteen kannalta keskeisistä mittareista
Osoitusvelvollisuus	rekisterinpitäjä ja henkilötietojen käsittelijä osoittaa noudattavansa tietosuojalainsäädäntöä
PCI DSS	standardi maksukorttiostamisen tietoturvavaatimuksista (eng. Payment Card Industry Data Security Standard)
Rekisterinpitäjä	henkilö tai taho, joka määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot
Rekisteröity	henkilöä koskeva tieto, jonka tietoja tallennetaan rekisteriin
SLA	palvelutasosopimus (eng. Service Level Agreement)
Tietosuoja	lainsäädännöllinen menettely ohjata ja rajoittaa henkilötietojen käsittelyä
Tietoturva	tekninen menettely suojata henkilötietoja järjestelmässä
TSA-sopimus	yrityskauppaprosessissa myyjän ja ostajan välinen sopimus (eng. Transitional Services Agreement)
Tunnusluku	ks. mittari
VAHTI-työryhmä	julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

1 JOHDANTO

Menestyvää organisaatiota johdetaan strategian avulla. Organisaatio arvioi, seuraa ja mittaa asetettujen tavoitteiden saavuttamista, pyrkii jatkuvasti kehittämään toimintaympäristöä ja kilpailukykyä. Menestyvällä organisaatiolla on kyky ennakoida tulevaa ja vähentää jatkuvuuteen, operatiiviseen toimintaan, talouteen, henkilöstön viihtyvyyteen ja rekisteröidyn oikeuksiin kohdistuvia uhkakuvia ja todellisia riskejä. Onnistuakseen näissä tehtävissä organisaation johdon tulee saada ajantasaista tietoa toimintaan vaikuttavista tekijöistä päätöksentekoa varten.

EU:n yleistä tietosuoja-asetusta (jatkossa tietosuoja-asetus) on sovellettu henkilötietojen käsittelyn parissa vuodesta 2018 alkaen. Tietosuoja-asetus edellyttää, että organisaatio osoittaa noudattavansa tietosuojalainsäädöksiä käsiteltäessä henkilötietoja. Organisaation johdon tulee kyetä varmistumaan, että tarvittavat tietosuojaan liittyvät suojatoimenpiteet tuotetaan ja että rekisteröidyn oikeudet toteutuvat lainsäädösten mukaisesti.

Julkishallinnon organisaation tulee nimittää tietosuoja-asetuksen vaatimuksen mukaisesti tietosuojavastaava (EU:n yleinen tietosuoja-asetus 2016/679 artikla 37). Sosiaali- ja terveydenhuollon erityislainsäädäntö säätää tietosuojavastaavan nimittämisestä (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021).

Tietosuojavastaavan tehtäviä on määritelty tietosuoja-asetuksessa (EU:n yleinen tietosuoja-asetus 2016/679 artikla 39). Tehtäviin sisältyy raportointi johdolle. Raportoinnin sisältöä ja tapaa ei ole säädetty tietosuoja-asetuksessa, eikä määritelty ohjaavissa työryhmissä (Tietosuojatyöryhmä 2016, 17) tai tietosuojavastaavan tehtävää ohjaavissa kirjoissa (Andreasson ym. 2019).

Tietosuojavastaavan yleisimmät vaikeudet raportointityössä ovat toimialueen laajuus, raportointikohteiden määrittelemättömyys ja manuaalinen tiedonkeruu. Tämän opinnäytetyön tavoite on tutkia tietosuoja-asetuksen tietosuojaperiaattei-

den toteuttamisen mittaamista. Tulosten saavuttamiseksi havainnollistetaan tiedon mittaamisen perusteet ja selvitetään miten tietosuojaperiaatteiden toteutuminen on mitattavissa. Opinnäytetyön tutkimustulosten avulla on tarkoitus laatia kehittämissuunnitelma toimeksiantajalle tietosuojaperiaatteiden toteutumisen mittaamiseksi ja raportoinnin kehittämiseksi. Opinnäytetyö toteutetaan kehittämistehtävänä, jonka keskiössä on julkishallinnon organisaatio.

On toivottavaa, että tulokset tarjoavat tukea tietosuoja-asetuksen tietosuojaperiaatteiden toteuttamiseen ja hyödyttävät tiedon mittaamista ja raportointia. Lisäksi on toivottavaa, että asiantuntijan roolissa toimiva tietosuojavastaava, liiketoiminnan tai johdon edustaja voi soveltaa ja hyödyntää tutkimustuloksia oman toiminnan kehittämiseksi.

Opinnäytetyössä käytetään termiä organisaatio, joka käsittää julkishallinnon organisaation ja minkä tahansa muun organisaation toimia rekisterinpitäjänä tai henkilötietojen käsittelijänä tietosuoja-asetuksen vaatimusten toteuttamiseksi. Tässä opinnäytetyössä ei käsitellä rekisterinpitäjän ja henkilötietojen käsittelijän asemaa, vaatimuksia ja tehtäviä erillisinä tehtävinä vaan asiaa lähestytään kokonaisuutena termin ”organisaatio” kautta.

Opinnäytetyö koostuu kuudesta luvusta. Johdannon jälkeen toisessa luvussa esitetään tutkimusmenetelmä ja kolmannessa luvussa lähestytään teorian avulla tietosuojaa, riskienhallintaa ja standardeja. Neljännessä luvussa siirrytään teorian kautta mittaamiseen ja raportointiin ja viidennessä luvussa esitetään tutkimustulokset teoriasta ja teemahaastatteluaineistosta sekä kehittämissuunnitelma. Kuudes luku sisältää opinnäytetyön pohdintaosuuden.

2 CASE-TUTKIMUS

Opinnäytetyö on case-tutkimus. Case-tutkimuksella pyritään tavoittamaan tuloksia, joilla voidaan kehittää organisaation toimintaa. Case-tutkimusta hyödynnetään laatia kehittämissuunnitelma toimeksiantajalle tietosuojaperiaatteiden toteutumisen mittaamiseksi ja raportoinnin kehittämiseksi. Lähestymistavaksi valittiin case-tutkimus, koska opinnäytetyön tavoitteena on saavuttaa tuloksia, joiden avulla toimeksiantajan toimintaa voi kehittää.

Tutkittavaa kohdetta lähestytään laadullisin tutkimusmenetelmin. Tutkittavasta kohteesta eli periaatteiden mittaamisesta tunnistettiin vähän suomenkielistä lähdeaineistoa. Opinnäytetyön aihetta valittaessa tietosuojaperiaatteiden mittaamisesta ei tunnistettu aiempia tutkimuksia. Laadullisessa tutkimuksessa tutkimuksen tavoitteena on sellaisen ilmiön kuvaaminen ja ymmärtäminen (Saaranen-Kauppinen & Puusniekka 2009, 13), josta tiedetään vähän. Käyttämällä laadullisen tutkimuksen menetelmää saadaan syvempää merkitystä ja kokemusta ilmiöstä, joka on tutkittavana kohteena.

2.1 Tutkimusongelma, tutkimuskysymys ja tavoite

Koska julkishallinnon organisaatiossa käsitellään laajamittaisesti henkilötietoja, on sinne nimitettävä tietosuojavastaava. Sosiaali- ja terveydenhuollon toimialalla tietosuojavastaavan tehtävästä on säädetty vuodesta 2007 lähtien (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159 (kumottu) 20 §). Sosiaali- ja terveydenhuollon toimialalla tietosuojavastaavat ovat toimineet pitkään ja tietosuojavastaavan tehtävänkuvaan on ohjeistettu kuuluvan raportointi johdolle.

Tietosuojavastaavan tehtävästä kertovaa ja tietosuojan toteuttamista ohjaavaa kirjallisuutta on laajasti saatavilla. Kansallisestikin tunnetut tietokirjailijat ohjeistavat, että oleellisen ja ajankohtaisen tiedon saattamiseksi johdon tietoisuuteen tulisi raportoinnin olla tehokasta (Andreasson, Riikonen & Ylipartanen 2019, 186).

Tietosuojaperiaatteiden mittaamisesta ei ole aiempia tutkimuksia ja kirjallisuutta vain vähän. Aiempien tutkimusten puute ja toimeksiantajan halu kehittää organisaation toimintaa vahvistavat tutkimustarvetta ja sen ajankohtaisuutta.

Opinnäytetyön tutkimuksen laatija toimii tietosuojavastaavana sosiaali- ja terveydenhuollon erityislainsäädännön ja tietosuoja-asetuksen vaatimusten mukaisissa tehtävissä. Tehtävänkuvaan on kuulunut raportointi, mikä on toteutettu vaihtelevalla aikavälillä ja ollut aikaa vievää. Raportointi on viivästynyt ja siksi välittänyt vanhentunutta tietoa. Kerättyä tietoa on ollut runsaasti, mutta se on ollut vaikeasti hyödynnettävissä ja vertailtavissa. Kun on pyydetty tietoja organisaation osa-alueilta, tiedonkeruun ei aina ole katsottu kuuluvan työtehtävien piiriin, ohjeistus on koettu epäselväksi tai ymmärretty tarkoituksesta poikkeavalla tavalla. Joko aikataulutavoitteita tietojen keräämiseksi ei ole omaksuttu tai niissä ei ole kyetty pysymään, jolloin pyydettyjä tietoja ei ole saatu ajallaan. Yleisimmät vaikeudet raportointityössä ovat toimialueen laajuus, raportointikohteiden määrittelemättömyys ja manuaalinen tiedonkeruu.

Case-tutkimuksessa esitetään kaksi pääosaa, joita ovat teoreettinen ja empiirinen osa (Kananen 2013, 44). Opinnäytetyön teoreettisessa viitekehyksessä esitetään oleellinen tieto, mitä ilmiöstä tiedetään opinnäytetyötä tehdessä. Opinnäytetyöllä pyritään tuottamaan uutta tietoa. (Kananen 2017, 76.)

Tutkittava kohde – tietosuojaperiaatteiden toteutumisen mittaaminen – on epäselvä ilmiö. Laadullisen tutkimuksen menetelmällä lähestytään epäselvää ilmiötä muuttamalla tutkimusongelma kysymysten muotoon (Kananen 2013, 65). Tutkimuskysymykset ohjaavat aineistonkeruuta, ja laatimalla tutkimuskysymykset mahdollisimman aukottomaksi ja rajaavaksi voidaan saaduilla vastauksilla ratkaista tutkimusongelma. (Kananen 2013, 59, 62.) Kehittämistehtävän keskeisimmät tutkimuskysymykset ovat:

- Mitä kehitettävää olisi raportoinnissa, jotta raportointi tietosuojaperiaatteista toimisi osana päätöksentekoa?
- Miten tietosuojaperiaatteiden toteutumisen mittaamisella voidaan kehittää organisaation toimintaa?

Opinnäytetyössä havainnollistetaan tiedon mittaamisen perusteet ja esitetään miten mittaamista voi kohdentaa tietosuojaperiaatteiden toteutumiseen.

Mittaamalla tietosuojaperiaatteiden toteutumista tulosten pohjalta voidaan asettaa tavoitteita puutteiden korjaamiseksi. Raportoimalla tavoitteista ja puutteista johdolle muodostuu käsitys asia-alueen laajuudesta. Raportointityön yleisimpien vaikeuksien selvittämiseksi opinnäytetyön tavoite on tutkia tietosuoja-asetuksen tietosuojaperiaatteiden toteuttamisen mittaamista. Kehittämistehtävässä laaditaan kehittämissuunnitelma toimeksiantajalle tietosuojaperiaatteiden toteutumisen mittaamiseksi ja raportoinnin kehittämiseksi.

2.2 Tutkimusmenetelmä ja rajaus

Aiheen laajuuteen ja opinnäytetyön laatimiseen käytettävissä olevaan aikaan nähden aihe rajataan käsittelemään tietosuoja-asetuksen tietosuojaperiaatteita ja vaatimuksia sekä vaatimusten toteutumisen mittaamista organisaation yksikössä. Tarkastelun alle ei oteta rekisterinpitäjän ja henkilötietojen käsittelijän vastuita erillisinä tehtävinä, vaan asiaa lähestytään kokonaisuutena termin ”organisaatio” kautta.

Ilmaisumuotona käytetään termiä ”organisaatio”, joka käsittää julkishallinnon organisaation, minkä tahansa muun organisaation tai yksikön toimia rekisterinpitäjänä tai henkilötietojen käsittelijänä tietosuoja-asetuksen osoitusvelvollisuuden ja vaatimustenmukaisuuden toteuttamiseksi. Tietosuoja-asetuksen tieteelliselle tutkimukselle asettamia vaatimuksia ei myöskään huomioida tässä tarkastelussa. Tavoitteena ei myöskään ole käsitellä esitettyjen kehitystoimenpiteiden jalkauttamista toimeksiantajan toimintaan.

2.3 Toimeksiantaja

Opinnäytetyön toimeksiantaja on Kansaneläkelaitoksen Tietopalvelujen Kantapalvelut -yksikkö. Kela on itsenäinen julkisoikeudellinen laitos, jonka hallintoa ja

toimintaa valvovat eduskunnan valitsemat valtuutetut (laki Kansaneläkelaitoksesta (731/2001) 1 §). Kanta-palvelut -yksikölle on säädetty sosiaali- ja terveydenhuollon erityislainsäädännössä tehtävä tuottaa sosiaali- ja terveydenhuollon palvelujentuottajien lukuun valtakunnalliset tietojärjestelmäpalvelut (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021). Kansaneläkelaitoksen 8 000 työntekijästä noin 200 asiantuntijaa työskentelee Tietopalvelujen Kanta-palvelut -yksikössä.

Kansaneläkelaitos on julkaissut avoimilla internetsivuillaan organisaation strategian, joka muodostuu kolmesta eri tavoitteesta: luottamuksesta ja yhteistyön vahvistamisesta, asiakaskokemuksen kehittämisestä sekä tiedon liikkuvuudesta ja hyödyntämisestä. Kelan visio on ”Lähellä ihmistä. Hyvinvointia tiedolla, tuella ja yhteistyöllä”. (Kansaneläkelaitos 2022.)

2.4 Aineistonkeruu, luokittelu ja analysointi

Tutkimusaineistoa kerätään teoreettisen analyysin ja teemahaastattelujen avulla. Tutkimusmenetelmänä käytetään laadullista tutkimusta eli kvalitatiivista tapaustutkimusta. Ilmiö muutetaan tutkimusongelmaksi, jolloin ilmiön selvittämiseksi esitetään tutkimuskysymyksiä ja laadullisen tutkimuksen aineistonkeruumenetelmin avulla etsitään vastauksia. (Kananen 2017, 71.)

Kvalitatiivinen tutkimusmenetelmän aineistonkeruumenetelmä ja tulosten analysointi sopii kehittämistehtävän tutkimusongelman selvittämiseen, koska menetelmän avulla voidaan tunnistaa kohteita toimeksiantajan toiminnan kehittämiseksi. Laadullisen tutkimuksen yleisimpiä aineistonkeruumenetelmiä ovat haastattelu, teemahaastattelu, kysely, havainnointi ja tiedonkeruu erilaisista dokumenteista (Tuomi & Sarajärvi 2009, 71).

Opinnäytetyön teoreettisen viitekehyksen lisäksi aineistonkeruumenetelmäksi on valittu teemahaastattelu. Teemahaastattelun avulla kerätään informaatiota, jotta tutkittavasta kohteesta saadaan tietoa käytännön ja teorian tasolla. Teemahaastattelun tavoite on saada luotettavaa tietoa tutkimusongelman kannalta tärkeiltä alueilta. (Hirsjärvi & Hurme 2011, 42–43.)

Teemahaastattelun etuna on, että se ei sido tutkijaa kvalitatiivisen tai kvantitatiivisen menetelmän käyttöön eikä siinä ole ennakkoon määritelty haastattelukertojen määrää (Hirsjärvi & Hurme 2011, 42, 48).

Kun tutkittava ilmiö on epäselvä ja kompleksinen, teemahaastattelu sopii aineistonkeruumenetelmäksi. Hirsjärvi & Hurme (2011) esittää, että yksityiskohtaisten kysymysten sijaan haastattelu etenee tiettyjen keskeisten teemojen varassa ja haastateltavien näkemykset saadaan esiin (48).

Case-tutkimuksessa laadullisen tutkimuksen menetelmiä käytettäessä on aineiston laadulla ja sen syvällisyydellä enemmän merkitystä aineiston määrään nähden Teemahaastattelussa aineistoa kerätään niin kauan kuin se on tarpeen ilmiön selvittämiseksi. (Kananen 2017, 126–127.) Teemahaastattelu muodostuu usein eri haastattelukierroksista, koska haastattelukierroksilla karttuu ymmärrys tutkittavasta ilmiöstä ja ei voida olettaa, että ensimmäisellä haastattelukierroksella kaikki tarvittava tieto saataisiin kerättyä ilmiöstä, jota varsinaisesti ei tunneta tai ymmärretä (Kananen 2013, 96.)

Teemahaastattelu nauhoitetaan, jotta teemahaastattelun aikana tutkija voi keskittyä haastateltavaan ja hänen tuottamaan aineistoon. Valitulla tallennusvälineellä nauhoitettu haastattelu litteroidaan analysointia varten (Kananen 2017, 104, 124.)

Aineiston litterointi tehdään karkealla tasolla, jolloin haastattelusta ei tuoda esille kaikkia ilmaisuja. Sanatarkka litterointi mahdollistaa aineiston käytön sellaisenaan sitaattina opinnäytetyössä. (Kananen 2013, 99, 100–101.) Sisällön analyysia varten teemahaastattelun aineisto koodataan sen läpikäynnin sujuvoittamiseksi. Koodaamisen avulla etsitään olennaista tietoa aineistosta ja pyritään selkeyttämään sitä tutkimuskysymysten ratkomiseksi. (Saaranen-Kauppinen, A. & Puusniekka, A. 2006.)

Koodaamisen jälkeen aineisto luokitellaan eli tiivistetään aihealueisiin, jotta aineistosta saadaan systemaattinen, looginen kokonaisuus ja muodostuu käsitys

tutkittavasta ilmiöstä. Aineiston luokittelu toteutetaan luokittelemalla asiakokonaisuuksia ja aineisto siirretään taulukkomuotoon. (Kananen 2013, 105.)

Kvalitatiivisessa tutkimuksessa aineiston analysointimenetelmä ei ole rajattu kuin kvantitatiivinen tutkimusmenetelmä (Kananen 2013, 134). Laadullisen tutkimuksen analyysin oikeellisuutta ja sopivuutta voi varmistaa dokumentoinnin avulla (Kananen 2013, 134).

3 TIETOSUOJA

Tietosuojan tehtävä on mahdollistaa tai rajoittaa yksilön henkilötietojen käsittelyä lainsäädännöllä tai sopimuksin. Tietosuojalainsäädäntö säätää ja sopimukset määräävät milloin ja miten henkilötiedon käsittely on sallittua. Tietoturvan tehtävä on turvata henkilötiedot teknisillä suojatoimenpiteillä.

Tietosuoja-asetusta on sovellettu kaikissa EU-maissa vuodesta 2018 lähtien (EU:n yleinen tietosuoja-asetus 2016/679 artikla 2). Tietosuoja-asetus on suoraan sovellettava kaikissa EU-maissa käsiteltäessä henkilötietoa tietosuoja-asetuksen kansallisen liikkumavaran puitteissa (Digi- ja väestötietovirasto 2021, 18).

Tietosuoja-asetus vahvistaa luonnollisten henkilöiden tietojen suojelua ja henkilötietojen vapaata liikkuvuutta EU:n alueella. Tietosuoja-asetuksella suojellaan luonnollisten henkilöiden oikeuksia ja vapauksia ja heidän oikeuttaan henkilötietojen suojaan. (EU:n yleinen tietosuoja-asetus 2016/679 artikla 1: 1–2.) Tietosuoja-asetus vahvistaa rekisteröidyn keinoja hallita henkilötietojensa käsittelyä (Tietosuojavaltuutetun toimisto n.d.).

Tietosuojavastaavan tehtävästä on säädetty tietosuoja-asetuksessa (EU:n yleinen tietosuoja-asetus 2016/679 artikla 37–39). Tietosuojavastaava auttaa varmistamaan henkilötietojen asianmukaisen käsittelyn organisaatiossa. Tietosuojavastaavan tehtävään kuuluu muun muassa auttaa organisaatiota tuottamaan palvelunsa siten, että henkilötietojen käsittely on läpinäkyvää ja lainmukaista, ja että rekisteröidyn tietoja käsitellään asianmukaisesti ja turvallisesti.

Tietosuojavastaavan tehtäviin kuuluu erilaisia vastuita, joiden tarkoituksena on varmistaa henkilötietojen asianmukainen käsittely organisaatiossa. Tietosuojavastaavan tehtävät ovat suoraan sovellettavia tietosuoja-asetuksen artiklan 39 mukaisesti:

- neuvoa ja kouluttaa organisaatiota tietosuojaan liittyvissä asioissa

- seurata, että organisaatio noudattaa tietosuoja-asetuksen vaatimuksia ja muita soveltuvia lakeja, säädöksiä ja menettelyjä mukaan lukien henkilöstön koulutus, tietosuojatietoisuuden lisääminen ja näihin liittyvät tarkastukset
- neuvoa ja valvoa tietosuojan vaikutustenarvioinnin laatimista
- toimia yhteyspisteenä tietosuojaan liittyvissä kysymyksissä viranomaiselle ja tehdä yhteistyötä viranomaisen kanssa (artikla 39).

Artikla 38 määrittelee tietosuojavastaavan roolin organisaation tietosuojaan liittyvissä asioissa. Tietosuojavastaavan on oltava pätevä ja riippumaton asiantuntija organisaation sisällä. Tietosuojavastaavan tulee olla erikoistuneita tietosuojaan ja valmiita tarjoamaan neuvoja organisaation sisäisissä tietosuojaan liittyvissä asioissa. Artiklassa 38 määritellään, että tietosuojavastaava raportoi suoraan organisaation johdolle. Tämä korostaa tietosuojavastaavan tärkeää roolia organisaation tietosuojaan liittyvissä asioissa ja varmistaa, että tietosuoja on huomioitu kaikilla organisaation tasoilla. (EU:n yleinen tietosuoja-asetus 2016/679 artikla 38.)

Tietosuojalainsäädäntö muodostuu useiden kansallisten lakien kokonaisuudesta, jota on päivitetty tai tullaan päivittämään vastaamaan tietosuoja-asetuksen (2016/679) vaatimuksia. Suomen perustuslaki (731/1999) 10 § säätää, että jokaisen yksityiselämä, kunnia ja kotirauha on turvattu ja että kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton (Suomen perustuslaki).

Tietosuojalaki (1050/2018) on henkilötietojen käsittelyä varten säädetty yleislaki, jota sovelletaan yhdessä tietosuoja-asetuksen kanssa (Eduskunta 2021). Julkishallinnossa henkilötietojen käsittely toteutetaan noudattamalla tietosuoja-asetuksen vaatimuksia, ja lisäksi viranomaisen toimintaa sääntelee muu lainsäädäntö kuten laki julkisen hallinnon tiedonhallinnasta (906/2019) (tiedonhallintalaki) ja laki viranomaisen toiminnan julkisuudesta (621/1999) (julkisuuslaki).

Julkishallinnon organisaatioiden eli viranomaisen tulee noudattaa toimintaansa ohjaavaa lainsäädäntöä ja tietosuojalainsäänteyä käsitellessään henkilötietoa. Julkishallinnon organisaatioiden toimintaa säädetään useilla eri laeilla ja säädöksillä, jotka tulee tunnistaa viranomaisen omassa toiminnassa.

Sosiaali- ja terveydenhuolloin toimintaa säädellään potilastiedon osalta sote-erityislainsäädännöllä muun muassa säätämällä potilasta koskevan tiedon olevan arkaluontoista ja salassa pidettävää (laki potilaan asemasta ja oikeuksista (785/1992) 13 §).

3.1 Tietosuojaperiaatteet

Tietosuoja-asetuksessa esitetään vaatimukset henkilötietojen käsittelyä koskevista periaatteista, jotka ovat suoraan sovellettavia (EU:n yleinen tietosuoja-asetus 2016/679 artikla 5). Organisaation tulee noudattaa tietosuojaperiaatteita koko henkilötietojen käsittelyn elinkaaren ajan (Tietosuojavaltuutetun toimisto. n.d.). Tietosuojaperiaatteet ovat

1. lainmukaisuus, asianmukaisuus ja läpinäkyvyys
2. käyttötarkoitussidonnaisuus
3. tietojen minimointi
4. täsmällisyys
5. säilytyksen rajoittaminen
6. eheys ja luottamuksellisuus (EU:n yleinen tietosuoja-asetus 2016/679 artikla 5).

Ensimmäinen periaate ”lainmukaisuus, asianmukaisuus ja läpinäkyvyys” tarkoittaa, että henkilötiedolle tulee olla käsittelyperuste, joka muodostuu lain, sopimuksen tai rekisteröidyn suostumuksen perusteella. Noudattamalla lainmukaisuutta henkilötietojen käsittelyssä saavutetaan vaatimus asianmukaisuudesta. Asianmukaisuuden vaatimus tarkoittaa, että henkilötietoja käsitellään asianmukaisesti ja kohtuullisesti käsittelyn tarkoitukseen nähden ja lisäksi henkilötietojen käsittelyn elinkaaresta viestitään ja informoidaan rekisteröityä selkeällä ja ymmärrettävällä tavalla. Läpinäkyvyys tarkoittaa, että henkilötietojen käsittelystä viestitään ja informoidaan selkeästi ja ymmärrettävästi ja informointi on helposti saatavilla. (Tietosuojavaltuutetun toimisto. n.d.)

Toisen periaatteen ”käyttötarkoitussidonnaisuus” -vaatimus toteutuu, kun henkilötietoja käsitellään kuten laissa, sopimuksessa tai rekisteröidyn suostumuksella

on sovittu ja sen mukaisesti. Käyttötarkoitussidonnaisuus on keskeisin periaate, joka yhdistää muut periaatteet, niiden vaatimusten toteuttamisen ja pitämisen ajantasaisena. Käyttötarkoitussidonnaisuus edellyttää perustetta henkilötietojen käsittelylle, henkilötietojen käsittelyä vain käyttötarkoituksen mukaisesti, organisatoristen ja teknisten suojatoimenpiteiden toteuttamista suhteessa käsiteltävään henkilötietoon ja ajantasaista läpinäkyvää informointia. (Tietosuojavaltuutetun toimisto. n.d.)

Tietojen minimointiperiaatteen vaatimus toteutuu, kun käsitellään asianmukaisia, olennaisia ja rajoitettuja eli välttämättömiä käyttötarkoituksen mukaisia henkilötietoja (Tietosuojavaltuutetun toimisto. n.d.).

”Täsmällisyys” –periaatteen vaatimus on, että käsitellään vain täsmällisiä henkilötietoja ja epätarkat tai virheelliset henkilötiedot oikaistaan tai poistetaan. Rekisterinpitäjällä tulee olla asianmukaiset menetelmät tietojen täsmällisyyden ja oikeellisuuden arvioimiseksi ja kyky reagoida rekisteröidyn esittämään pyyntöön oikaista epätarkka tai virheellinen tieto tai poistopyyntöön tarpeettomien tietojen osalta. (Tietosuojavaltuutetun toimisto. n.d.)

”Säilytyksen rajoittaminen” -periaatteen vaatimus toteutuu, kun henkilötietoja säilytetään vain käyttötarkoituksen ajan eli niin kauan kuin henkilötietojen säilyttämisestä on säädetty tai sovittu (Tietosuojavaltuutetun toimisto. n.d.).

Kuudennen periaatteen ”eheys ja luottamuksellisuus” -vaatimus toteutuu, kun järjestelmissä ja palveluissa varmistetaan henkilötietojen luottamuksellisuus, eheys ja saatavuus. Rekisterinpitäjän tulee arvioida organisatoristen ja teknisten suojatoimien riittävyyttä suhteessa olosuhteisiin ja rekisteröidyn oikeuksiin ja vapauksiin kohdistuviin tunnistettuihin riskeihin. Vaatimuksen toteutuminen edellyttää, että henkilötiedot suojataan koko käsittelyn elinkaaren ajan. Laadittuja suojatoimia on testattava säännöllisesti ja tehtävä tarvittavia parannuksia suojatoimien kehittämiseksi. (Tietosuojavaltuutetun toimisto. n.d.)

3.2 Osoitusvelvollisuus

Tietosuoja-asetuksen artiklassa 5 esitettyjen periaatteiden ja niiden vaatimusten noudattaminen tulee kyetä osoittamaan, mistä muodostuu osoitusvelvollisuus (EU:n yleinen tietosuoja-asetus 2016/679 artikla 5, kohta 2). Osoitusvelvollisuus tarkoittaa kykyä osoittamaan noudattavansa tietosuojalainsäädäntöä ja että tarpeelliset tekniset ja organisatoriset suojatoimenpiteet on toteutettu osoitusvelvollisuuden vaatimusten täyttämiseksi. Osoitusvelvollisuus tarkoittaa, että henkilötietojen käsittelyyn liittyvät suojatoimenpiteet ja prosessit on tehty ja dokumentoitu. Näistä toimista muodostuu dokumentointivelvollisuus. (Tietosuojavaltuutetun toimisto n.d.)

Osoitusvelvollisuus tulee huomioida, kun suunnitellaan henkilötietoja sisältävää rekisteriä. Tietosuojaperiaatteiden ja osoitusvelvollisuuden toteuttamisen tukena voi käyttää sertifikaatteja tai käytännesääntöjen käyttöön ottamista. (Tietosuojavaltuutetun toimisto n.d.) Käytännesääntö tukee organisaatiota tietosuoja-asetuksen ja osoitusvelvollisuuden noudattamisessa. Yksityisellä sektorilla käytännesääntöjen toteuttamista valvoo viranomaisen akkreditoima valvontaelin, joka Suomessa on tietosuojavaltuutetun toimisto. (Tietosuojavaltuutetun toimisto 2021).

Tietosuoja-asetuksen vaatimuksen mukaan tulee olla osoitettavissa, että henkilötietojen käsittely tapahtuu läpinäkyvästi, lainmukaisesti ja asianmukaisesti. Tietovarantoja, tietojohtamista, tietojenkäsittelyä ja tietoturvallisuutta voidaan tarkastella tilinpäätösluonteisesti, kun organisaation tulee arvioida tietosuoja-asetuksen vaikutuksia ja hahmottaa kokonaiskuva henkilötietojen käsittelyn nykytilasta. Osoitusvelvollisuuden hoitamiseksi voi hyödyntää tietotilinpäätöstä, joka mielletään organisaation johdolle suunnatuksi kokonaiskuvaksi henkilötietojen käsittelystä. (Andreasson ym. 2019, 185, 190–191.)

3.3 Riskienhallinta

Riskienhallinta on osa organisaation liiketoiminnan jatkuvuuden hallintaa ja tavoitteiden saavuttamista. Riskienhallinta kohdistuu organisaation eri toiminta-

alueisiin kuten strategiaan, liiketoimintaan, rahoitukseen, prosessien jatkuvuuden-, toipumisen- ja häiriönhallintaan. Riskienhallinnalla pyritään ennaltaehkäistä tunnistetun tai tunnistamattoman haitan tai uhan toteutumista sekä epävarmuuksien vaikutuksia organisaation toimintaan. Organisaatiolla tulisi olla ajantasainen, oikeasuhtainen ja riittävän kattava käsitys toimintaan vaikuttavista riskeistä, uhkista tai epävarmuuksista. Riskienhallinnalla määritellään selkeästi riskien alentamiseksi laadittavat hallintatoimenpiteiden vastuuhenkilöt, jotka seuraavat riskien muuttumista. Riskienhallinta ei ole vain päätöksentekijöiden seurannan väline vaan jokaisella työntekijällä on vastuu ja mahdollisuus tuoda esiin normaalista toiminnasta poikkeavia havaintoja tai riskejä niiden vaikutuksineen, jotta päätöksen tekijät saavat ajantasaista tietoa muutoksista. Riskienhallinta on osa ajantasaista johtamista, päätöksentekoa, toiminnan seurantaa ja suunnittelua. (Rousku, K. 2017. 11, 12.)

Riskienhallinta auttaa organisaatiota ennakoimaan uhkia ja myötävaikuttaa sen kykyyn saavuttaa liiketoiminnalliset tavoitteet ja kohdentamaan kehitystoimenpiteitä. Riskienhallinnalla organisaatiolle muodostuu ymmärrys riskeistä ja kyky saavuttaa liiketoiminnalliset tavoitteet. Riskienhallinnan avulla organisaatiolle muodostuu kyky tunnistaa ja hallita riskejä ja kustannuksia. Organisaatio voi kohdentaa kehitystoimenpiteet ja resurssit riskien alentamiseksi. (Rousku, K. 2017. 12.)

Tunnistettujen riskien madaltamiseksi kehitetään hallintatoimenpiteitä, joiden turvin riski pyritään poistamaan kokonaan tai madaltamaan riskitaso siedettäväksi. Organisaation johto voi tietoisella riskinotolla päättää hyväksyä riskin seurauksineen. Jotta riskienhallinnan tuottama lisäarvo saadaan esiin, hallintatoimenpiteiden kustannusten ja vaikutusten tulee olla mitattavissa. (Rousku, K. 2017. 13–14.)

Riskejä tulee hallita myös henkilötietojen käsittelyssä erityisesti tietosuojan vaikutustenarvioinnilla. Tietosuojan vaikutustenarvioinnin merkitys on arvioida suunniteltujen käsittelytoimien vaikutuksia ja mahdollisia riskejä ja vähentää hallintatoimenpitein riskien toteutumista rekisteröidylle (EU:n yleinen tietosuoja-asetus 2016/679 artikla 35). Tietosuoja-asetuksen vaatimusten mukaisessa riskiarvioin-

nissa näkökulma on arvioida henkilötietojen käsittelystä aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja rekisteröidyn oikeuksille ja vapauksille (Tietosuojavaltuutetun toimisto n.d.).

Tietosuoja-asetuksen vaatimusten mukaisesti tietosuojan vaikutustenarviointi tulee laatia, jos henkilötietojen käsittely sisältää esimerkiksi uutta teknologiaa, on laajamittaista tai kohdistuu erityiseen henkilötietoryhmään. Tietosuojan vaikutustenarvioinnilla arvioidaan henkilötietojen käsittelyn tarpeellisuutta, lainmukaisuutta, kuvataan henkilötietojen käsittelyn toimet, arvioidaan riskejä ja laaditaan hallintatoimenpiteitä riskien vähentämiseksi tai madaltamiseksi. Tietosuojan vaikutustenarvioinnin tavoite on riskilähtöisesti arvioida jäljelle jääneen riskin vaikutuksia rekisteröidylle ja organisaation toimintaan. Tavoite on tunnistaa riski ja arvioida onko riski hyväksyttävissä organisaation toiminnan olosuhteissa. (Tietosuojavaltuutetun toimisto n.d.)

Organisaation tulee tunnistaa jo suunnitteluvaiheessa, mitä mahdollista haittaa rekisteröidylle voi muodostua henkilötietojen käsittelystä (Tietosuojavaltuutetun toimisto n.d.). Tietosuojan vaikutustenarviointi ja sen uhkataulukko nähdään työkaluna, joka toimii välineenä uhkien tunnistamiseen (Tietosuojavaltuutetun toimisto 2021, 28).

Henkilötietojen käsittelyn ja rekisteröidyn oikeuksien riskienhallinta ei eroa muusta riskienhallintaprosessista. Kimmo Rousku kuvaa valtiovarainministeriön julkaisussa (2017, 18) ISO/IEC31000 -standardin riskienhallintaprosessin vaiheet: määrittele toimintaympäristö, tunnista riskit, tee riskianalyysi, arvioi riskien merkityksiä, käsittele riskit, seuraa ja katselmoi riskianalyysia.

Riskilähtöisen arvioinnin lisäksi viranomaista koskee hyvän hallinnon periaatteet ja julkisuutta koskevat säännökset. Viranomaiselle laissa säädettyjen tehtävien ja palvelujen tuottamisessa rekistereihin tallennettujen tietojen luottamuksellisuus korostuu niiden arkaluonteisuuden vuoksi. Riskienhallinta on osa tunnistaa ja ennaltaehkäistä luottamuksellisuutta horjuttavia tekijöitä organisaation sisällä ja ulkopuolella.

3.4 Standardit

Standardi on tukikehikko, jonka avulla organisaation toimintaa ja prosesseja voi ohjata ja sekä arvioida käyttöönotettujen menetelmien tehokkuutta. Standardin käyttö on vapaaehtoista organisaatioille ja niitä on laadittu laaja valikoima eri toimialoille. Organisaatio voi valita standardivalikoimasta toimintaansa parhaiten tukevan työvälineen. Standardit määrittelevät tuotteen, palvelun tai järjestelmän ominaisuuksiin liittyvät vaatimukset ja tukevat organisaation toimintaa suoriutua muun muassa lainsäädännön vaatimuksista. (Suomen standardisoimisliitto n.d.)

ISO (International Organization for Standardization) on kansainvälinen, riippumaton organisaatio, johon kuuluu 167 kansallista standardointielintä. Kansainvälisiä ISO-standardeja on käytetty vuodesta 1951, jolloin julkaistiin ensimmäinen ISO-standardi. Nykyään kansainvälisiä ISO-standardeja on 24 599. (International Organization for Standardization n.d.) Suomessa eurooppalaisen standardijärjestön (CEN) ja kansainvälisen ISO:n jäsenenä toimii SFS ry, joka edistää standardien laadintaa ja suomalaisten näkökulmien huomioimista standardityössä (Suomen standardisoimisliitto n.d.).

3.4.1 ISO/IEC27001

Tietoturvan toteuttamisen tueksi voi hankkia niin kutsutun tietoturvastandardi perheen. ISO/IEC 27001 -standardi on julkaistu vuonna 2005. Standardi tukee organisaatiota tarvittavien dokumenttien laadinnassa ja tietoturvan hallintajärjestelmän käyttöönotossa.

Tietoturvan hallintajärjestelmä ohjaa organisaatiota käyttämään, ylläpitämään, valvovaan, tarkistamaan ja parantamaan toimintaansa. Standardi esittää yksityiskohtaiset vaatimukset, miten tietoturvakontrollit jalkautetaan organisaation toimintaan. Tietoturvan hallintajärjestelmän avulla organisaatio voi varmistua muun muassa noudattavansa lakeja ja määräyksiä. (International Organization for Standardization n.d.)

Tietosuoja-asetuksen artikla 32 sisältää vaatimuksen, joka edellyttää teknisiä toimenpiteitä henkilötietojen suojaamiseksi. Artiklassa annetaan esimerkkejä turvatoimista ja ohjaimista, tämä artikla ei kuitenkaan sisällä ohjeita siitä miten turvallisuustaso saavutettaisiin. Tietosuoja-asetuksen artikla 40 ohjaa hyödyntämään hyväksyttyjä käytännesääntöjä ja artikla 42 ohjaa sertifiointimekanismin hyödyntämistä osoittaakseen noudattavansa artiklan 32 kohtia 1 ja 2. (EU:n yleinen tietosuoja-asetus 2016/679 artikla 32, 40, 42.)

ISO/IEC 27001 -standardi sisältää vaatimuksen teknisten suojaustoimenpiteiden toteuttamisesta ja ohjaa tietoturvan hallintajärjestelmän suunnittelua, toteuttamista, ylläpitoa ja jatkuvaa parantamista. ISO/IEC 27001 -standardi esittää siis käytännöt suojata organisaation tietoa ja toimintaa mukaan lukien työntekijät, prosessit ja teknologia, ja auttaa suojaamaan ja hallitsemaan organisaation kaikkea tietoa riskienhallinnan avulla. ISO/IEC 27001 -standardin avulla suojataan kaikkea organisaation tietoa, ei pelkästään henkilötietoa, vähentämällä, seuraamalla ja tarkastelemalla riskejä ja ylläpitämällä jatkuvasti valmiutta muuttuviin tietoturvauhkiin. Standardia noudattamalla organisaatiolla on kyky osoittaa, että riittävät tekniset suojaustoimenpiteet on toteutettu tietosuoja-asetuksen vaatimusten noudattamiseksi.

Tietoturvan puuteanalyysi

ISO/IEC 27001 -standardin hankintaa suunnitellessa on mahdollista tehdä auditointia esivalmisteleva ja tukeva puuteanalyysi (eng. Gap Analysis). Puuteanalyysissa käydään tietoturvastandardin kohdat läpi, joka tuo lisäarvoa organisaation maturiteetista eli kypsyystasosta. Puuteanalyysissa käydään läpi organisaation turvallisuustaso ja pyritään tunnistamaan mahdollisia aukkoja toiminnassa.

ISO/IEC 27001 -standardin puuteanalyysi on arvio, joka suoritetaan auditoinnin vaiheiden 1 ja 2 välillä. Puuteanalyysin avulla pyritään tunnistaa organisaation turvallisuustasossa tai teknisissä suojaustoimenpiteissä heikkouksia tai puutteita. Puuteanalyysin avulla havaitut heikkoudet tai puutteet korjataan sovituin toimenpitein auditoinnin ensimmäisen vaiheen jälkeen. Puuteanalyysi tukee organisaatiota auditoinnin toiseen vaiheeseen valmistautumisessa ja etenemisessä sertifiointiprosessiin. (Eurofins 2018.)

3.4.2 ISO/IEC27701

Tietosuoja-asetus esittää vaatimukset ryhtyä tarvittaviin toimiin henkilötietojen ja yksityisyyden suojaamiseksi kaikessa henkilötietojen käsittelyssä henkilötiedon elinkaaren ajan (EU:n yleinen tietosuoja-asetus 2016/679 artikla 32). Tietosuoja-asetus ei kuitenkaan esitä konkreettisia tapoja ja ohjeita miten henkilötietoja tulisi suojata.

Tietoturvastandardiperheeseen on julkistettu laajennos, joka ohjaa henkilötietojen käsittelyn vaatimusten toteuttamista. ISO (International Organisation for Standardization) ja IEC (International Electrotechnical Commission) kehittivät ISO/IEC27701 -standardin eli tietosuojastandardin ohjaamaan henkilötietojen käsittelyä ja toimintaa esitettyjen vaatimusten täyttämiseksi. Tietosuojastandardi ISO/IEC27701 ohjaa toimialariippumattomasti julkisia ja yksityisiä organisaatioita ja voittoa tavoittelemattomia yhteisöjä. (International Organization for Standardization n.d.)

ISO/IEC27701 -standardin avulla organisaatio suunnittelee henkilötietojen hallintajärjestelmän (PIMS), jalkauttaa hallintajärjestelmän organisaation toimintaan, ylläpitää tietosuojan hallintaa ja kehittää jatkuvasti henkilötietojen käsittelyyn liittyvää toimintaa organisaation toimintaympäristössä. (Suomen standardisoimisliitto n.d.)

Tietosuojan hallintajärjestelmä ohjaa ja kehittää organisaation toimintaa, jonka avulla organisaatio voi arvioida tietosuoja-asetuksen noudattamista ja toiminnan oikeasuuntaisuutta. Tietosuojan hallintajärjestelmä sisältää vaatimuksia konkreettisin hallintatoimenpitein, joiden avulla organisaatio voi vahvistaa tietosuojan toteutumista toiminnassaan. Tietosuojan hallintajärjestelmä ohjaa organisaation toimintaa ja tietosuoja-asetuksen noudattamista hyvällä tasolla.

Tietosuojan puuteanalyysi

ISO/IEC27701 -standardin puuteanalyysin avulla organisaatio tunnistaa puutteet vaatimusten täyttämiseksi jo ennen auditointia. Puuteanalyysin käyttö edellyttää,

että organisaatiossa on käytössä ISO/IEC 27001 -standardin mukainen tietoturvan hallintajärjestelmä. Puuteanalyysin avulla tunnistetaan ja kohdennetaan osa-alueet, joita tulee kehittää, ja se sujuvoittaa priorisointia tietosuojastandardin vaatimusten täyttämiseksi. (IT Governance. n.d.)

Tietoturvastandardi ISO/IEC 27001 ja tietosuojastandardi ISO/IEC27701 sisältävät organisaation toiminnan ohjauksen ja suunniteltavan hallintajärjestelmän. Organisaation johdon tulee sitoutua sen jalkauttamiseen henkilökunnalle. Molemmat hallintajärjestelmät sisältävät vaatimukset seurata, mitata ja raportoida hallintajärjestelmän vaatimusten toteutumisesta.

3.4.3 Auditointi

Auditointi ja katselmointi on osa standardin käyttöönottoa ja organisaation toiminnan kehittämistä. Auditointi tai katselmointi on määräajoin tai tapauskohtaisesti tapahtuvaa valvontaa ja tarkastuksia. Riskienhallinta vaatii jatkuvaa seuraamista ja päivittämistä. (Rousku, K. 2017. 28.)

Auditointi ei ole aina sidoksissa standardin käyttöönottoon tai sen määräajan tapahtuvaan tarkastukseen. Sosiaali- ja terveydenhuollon erityislainsäädäntö säätää, että tietojärjestelmät voivat liittyä valtakunnallisen tietojärjestelmäpalvelun eli Kanta-palvelujen asiakkaaksi, kun järjestelmä on sertifioitu. Sertifiointi toteutuu onnistuneesti, kun tietojärjestelmän tuottaja esittää todistukset siitä, että järjestelmä täyttää olennaiset vaatimukset. (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021.) Toisin sanoen kyseessä on auditointiprosessi, jolla osoitetaan yleisimpien tietoturvavaatimusten noudattaminen.

Auditoinnin ja katselmoinnin avulla arvioidaan miten riskienhallinnan ja riskien käsittelyn tavoitteet ovat toteutuneet. Auditoinnin ja katselmoinnin tuloksen perusteella organisaatio voi käsitellä riskejä, joita ei ole tunnistettu aiemmin korkeiksi riskeiksi tai joilla voi olla vaikutusta organisaation operatiiviseen toimintaan tai liiketoimintaan. Auditoinnin avulla arvioidaan riskienhallinnan onnistumista.

Auditointeja ja tarkastuksia toteutetaan organisaation sisäisenä tai ulkoisena auditointina. Ulkoiseen auditointiin valitaan validoitu sertifiointielin. (Rousku, K. 2017. 28.)

Organisaatio saa ISO/IEC-sertifikaatin läpäistystä auditoinnista. Organisaatio jatkaa hallintatoimenpitein riskien alentamista ja puutteiden hallintaa seuraavaan auditointiin asti. Auditoinnin tarkoituksena voidaan pitää organisaation ymmärryksen ja tietouden lisäämistä organisaation nykytilasta ja toimintatavoista, prosessien ja toimintatapojen kehittämiskohteiden tunnistamista, puutteiden havainnointia ja tarvittavien hallintatoimenpiteiden käyttöönottoa. Auditoinnin tai puuteanalyysin tulos on merkittävä tiedonlähde kehityskohteiden tunnistamiseksi ja niiden priorisoimiseksi organisaation toiminnassa.

4 MITTAAMINEN JA RAPORTOINTI

Tietosuoja-asetus edellyttää toimenpiteitä rekisteröidyn oikeuksien toteuttamiseksi ja henkilötietojen suojaamiseksi. Tietosuoja-asetuksen vaatimusten toteuttamista ovat rekisteröidyn oikeus saada pääsy omiin tietoihin, oikeus tietojen oikaisemiseen ja poistamiseen, oikeus käsittelyn rajoittamiseen, oikeus siirtää tiedot järjestelmästä toiseen tai vastustamisoikeus (EU:n yleinen tietosuoja-asetus artikla 13–21) ja ilmoittaminen henkilötietojen tietoturvapoikkeamasta valvontaviranomaiselle sekä tarvittaessa rekisteröidylle (EU:n yleinen tietosuoja-asetus artikla 33–34). Nämä ovat tyypillisimpiä mittaamisen kohteita. Vaatimusten toteuttamisesta voidaan kerätä tietoa rekisteröityjen tietopyyntöjen määristä, henkilötietojen käsittelyn volyymista ja käsittelyn läpimenoajasta sekä rekisteröidyn oikeuksiin ja vapauksiin ja organisaation maineeseen ja luotettavuuteen vaikuttavista poikkeamista tai loukkauksista.

Valtiovarainministeriö on julkaissut suosituksia VAHTI-työryhmien toiminnan yhteydessä. VAHTI-työryhmien ohjeet ja suositukset ovat edelleen sovellettavissa organisaation toimintaan, vaikka lainsäädäntöä on muutettu yhteensopivaksi tietosuoja-asetuksen kanssa. Organisaation tuottamaa tietoturvatoimintoja ja riskienhallintaa tulee jokaisen organisaation arvioida oman toimintansa näkökulmasta toiminnan ylläpitämiseksi ja kehittämiseksi. VAHTI-työryhmien suositukset yhdessä lainsäädännön ja tietosuoja-asetuksen kanssa muodostavat tavoite- ja vähimmäistason tietoturvaratkaisujen määrittelemiseksi. Asettamalla turvallisuustasoon liittyviä tavoitteita ja kehittämiskohteita ja seuraamalla tuloksia määritellyillä mittareilla organisaatio voi johtaa tietoturvatoimintaa. Asetettujen tavoitteiden saavuttamista tulee tarkastella toiminnan jatkuvuuden, laadun, asiakaspalvelun, sidosryhmien, muutoksen hallinnan ja säädösten näkökulmasta. (Valtiovarainministeriö. 2006, 16.)

Menestyvä organisaatio toimii säädösten ja asetusten mukaisesti, arvioi kustannusten vaikutuksia, riskien suuruutta ja ennakoi muutosta. Tätä varten organisaation johto tarvitsee ajantasaista tietoa päätösten tekoa varten.

Mittareita on laajasti käytettävissä ja niitä on suunnattu taloudellisten, operatiivisten tai ei-rahallisten arvojen ja tunnuslukujen mittaamiseen. Moni organisaatio hyödyntää erilaisia mittareita myös arvioidakseen käytäntöjensä menestystä ja tunnistaakseen kehitettäviä osa-alueita, ja joiden avulla organisaation tietosuojakäytäntöjä voi kehittää. (Polonetsky & Tene 2022.)

Tietosuojakäytänteiden tehokkuuden ja vaikuttavuuden arviointi on muodostumassa monien organisaatioiden ytimeksi strategisissa arvoissa, sillä tietosuojan ja sen toteuttamisen sivuuttaminen voi aikaansaada tarpeettomia riskejä. Moni organisaatio voi saavuttaa tavoitteensa ottamalla käyttöön tietosuojamittarit. Mittareiden avulla voi varmistaa tietosuojalainsäädännön, määräysten ja standardien noudattamista, organisaation kykyä ylläpitää luottamusta asiakkaisiin ja vahvistaa organisaation tietosuojakäytänteiden tehokkuutta ja arvoa. (Polonetsky & Tene 2022.)

4.1 Mittaaminen

Mittaamisen haasteet tai vaikeudet muodostuvat pääpiirteittäin siitä, että organisaatiossa ei kerätä lukuja, joita voisi arvioida, vertailla ja mitata. Mittaaminen koetaan vaikeaksi erityisesti, jos tieto on tallennettu dokumentteihin laadullisessa muodossa tai jos ylläpitäminen ja päivittäminen on hankalaa ja aikaa vievää mittareiden suuren lukumäärän takia. Mittareita ja mittaristoja ei tule valita siten, että yksi mittari sopii kaikkeen organisaation toimintaan, vaan mittarit tulee valita organisaation tarpeisiin ja tavoitteisiin. Julkishallinnon organisaatioon valitut mittarit ja mittaristot eivät välttämättä sovi pienemmän yrityksen käyttöön.

Perinteisimmillään mittaamisessa on kyse jonkin suureen kuten painon tai pituuden mittaamisesta. Määrällisen luvun mittaaminen tapahtuu mittarilla, joka vaihtelee mitattavan kohteen mukaan. (Tietoarkisto n.d.)

Jos mitattava kohde on epäselvä kuten asia tai ilmiö, mittaaminen käynnistetään määrittelemällä ja käsitteellistämällä asia tai ilmiö, jota halutaan mitata; tunnistetaan, mikä on mittaamisen kohde. Suunniteltaessa mittaria – tai otettaessa käyt-

töön valmis mittari – tulee mittari kohdentaa asioihin, joita sen halutaan mittaavan. Mittarin tuottamiseksi tutkittava ilmiö on operationalisoitava. (Tietoarkisto n.d.)

Tutkittavan ilmiön operationalisointi tarkoittaa menetelmää, jolla pyritään määrittelemään abstrakti käsite, esimerkiksi ”onnellisuus”, ”tasa-arvo”, ”suvaitsevaisuus”. Kvantitatiivisen tutkimuksen toteuttamiseksi käsitteet tulee muuttaa analyyttisiksi, jotta niitä voidaan mitata. Arvioitaessa miten tuntemattomasta ilmiöstä voi kerätä tietoa mitattavaksi voidaan hyödyntää operationalisoinnin menetelmiä. (Tietoarkisto n.d.) Abstrakteista käsitteistä voidaan luoda mittareita, kun operationalisoinnissa käytetään neljää eri vaihetta ilmiön määrittelyyn:

1. käsitteen yleinen hahmottaminen ja määrittäminen
2. käsitteen osa-alueiden määritteleminen
3. siirtyminen teoreettisesta kielestä konkreettiseen arkikieleen ja indikaattoreihin
4. operationalisoinnin tarkka kuvaaminen (Tietoarkisto n.d.).

Ilmiöiden ja käsitteiden operationalisoinnin tuloksena voidaan siis muodostaa mittareita (Tietoarkisto n.d.).

Tiedon mittaamista varten mittari tulee suunnitella niin, että se pystyy täsmällisesti määrittelemään tietyn menestystekijän suorituskykyä eli tunnuslukuja. Mittaaminen suoritetaan tunnusluvuilla. Suorituskyky määrittää miten mitattava kohde on saavuttanut asetettuja tavoitteita. (Lönnqvist et al. 2006, 19, 29). Menestystekijä on organisaation keskeisin liiketoiminnan ja strategian mitattava asia. Organisaation menestystekijät muodostuvat mitattaessa suorituskykyä. Organisaation suorituskykyä voidaan mitata asiakkaiden, sidosryhmien ja viranomaisten tarpeiden näkökulmasta kuten myös yksittäisen työntekijän osaamisen ja tehokkuuden näkökulmasta tai työilmapiirin kokemuksesta. (Lönnqvist et al. 2006, 20, 21, 22).

Menestystekijöitä on kuvattu taloudellisina tai ei-taloudellisina kuten esimerkiksi myynnin kasvuna tai tuotteen läpimenoaikana. Kriittinen menestystekijä on esimerkiksi liiketoiminnan ydin, joka vaikuttaa kriittisesti organisaation toimintaan tai

suoritustasoon. Kriittinen menestystekijä edistää organisaation menestystä. Seuraamalla menestystekijöitä tunnistetaan syy-seuraussuhteita, jotka voivat esittää tietoa muun muassa onnistuneesta asiakaspalvelusta tai henkilöstön osaamisesta. Onnistunut asiakaspalvelu voi tehostaa myyntiä ja henkilöstön osaaminen voi edistää tehokasta toimintaa organisaatiossa. Seuraustekijät antavat siis tietoa liiketoiminnan tavoitteista ja tuloksista. (Lönnqvist et al. 2006, 22.)

Mittarin validiteetilla tarkoitetaan mittarin pysyvyyttä ja hyvyyttä eli mittarin kykyä mitata kattavasti ja tehokkaasti tarvittavia kohteita. Mittarin validiteetti on hyvä, kun se mittaa sitä, mitä sen on tarkoitus mitata. Mittarin validiteettiin voivat vaikuttaa monet tekijät kuten huonosti suunniteltu otanta tai huonosti ajoitettu mittaaminen tai jopa haastateltavan ja haastattelijan välinen henkilökemia. (Tietoarkisto n.d.)

Mittarin reliabiliteetilla tarkoitetaan tilannetta, jossa satunnaisvirheet tai olosuhteet eivät vaikuta mittariin eli mittari on johdonmukainen: se mittaa aina samaa asiaa. Reliabiliteetti suomennetaan ”luotettavuus”, ”käyttövarmuus”, ”toimintavarmuus”. (Tietoarkisto n.d.) Mittaristo tarkoittaa kokonaisuutta, joka muodostuu mittauskohteen kannalta keskeisistä mittareista. Mittaristo voidaan rakentaa systemaattisesti mittaristomallin tai mittariston viitekehyksen mukaan. (Lönnqvist et al. 2006, 29.)

Mittareita käytetään apuna tunnistamaan organisaation prioriteetit, korkeat riskialueet ja kohdentamaan rahoitusta ja resursseja (Tene & Culnan 2021, 4). Arvioitaessa menestystekijöitä, syyseuraussuhteita ja selvitettäessä lukuja, joita halutaan mitata, organisaation tulee ensin paneutua ilmiöihin ja selvittää ne ilmiöt, joista organisaatio haluaa tietoa. Organisaation on selvitettävä minkä tiedon keräämisestä ja mittaamisesta on hyötyä organisaation toiminnalle. Organisaatio tuntee itse parhaiten oman toiminta-alueensa ja kykenee päättämään mitkä ovat sen tarpeet. Nämä tunnistamalla organisaatio tietää mikä kerättävä tieto on merkityksellistä. Organisaatiot arvioivat ja mittaavat usein prosesseja ja läpimenoaikoja, mutta tämä ei mahdollista kaikkien kuten esimerkiksi laadullisten prosessien mittausta. Näissä tapauksissa prosesseille tulee muodostaa tunnusluvut jotain tiettyä ennalta sovittua tarkoitusta varten. (Laamanen 2001, 157–158.)

Aineettomaan pääomaan voidaan luokitella muun muassa henkilöstön osaaminen, yrityksen imago ja asiakassuhteet. Näiden osa-alueiden toimintoja ovat esimerkiksi koulutus tai työnkierto henkilöstön osaamisen lisäämiseksi, vierailut asiakkaan luona asiakassuhteen kehittämiseksi tai yhteiset kehityshankkeet. Nämä mittaamisen kohteet eivät ole fyysisesti havaittavissa, kuten tuotteiden määrä tai läpimenoaika, ja siksi ne ovat vaikeasti mitattavia. (Lönnqvist et al. 2006, 55.) Mittaaminen koetaan vaikeaksi, koska aineettomasta pääomasta ei ole kerätty lukuja tietojärjestelmiin samalla tavalla kuin taloudellisista tai ei-taloudellisista tiedoista.

Mittaaminen on vaikeaa myös siksi, että aineettoman pääoman määrittely on hankalaa saada täsmälliseksi (Lönnqvist et al. 2006, 55). Lönnqvist et al. (2006) mukaan aineeton pääoma on osa-alue tai toiminto, joita organisaatiossa tulee tuottaa palvelun tai tuotteen käytön lisäämiseksi, tuotteen hankkimiseksi tai arvon lisäämiseksi (55). Muita menestystekijöitä asiantuntijaorganisaatiossa ovat esimerkiksi tuotoksen laatu, ajanhallinta, henkilöstön tieto ja osaaminen tai yhteistyön laatu asiakkaan kanssa (Lönnqvist et al. 2006, 53).

Asiantuntijatyön ja aineettomaan pääoman lisääntyessä tiedon mittaaminen hankaloituu, sillä aiemmin käytössä olleet mittarit taloudellisista ja ei-taloudellisista tiedoista ovat olleet saatavilla tietojärjestelmistä. Aineettomalle pääomalle tulee suunnitella mittarit tarvittavan informaation keräämiseksi eli tiedonkeräysmenetelmä tulee suunnitella samassa yhteydessä kuin mittari suunnitellaan. Oikean käyttökelpoisen mittarin suunnittelu on vaikeaa ja edellyttää tuntemusta organisaation toiminnasta ja tavoitteista. (Lönnqvist et al. 2006, 69.)

Aineettoman pääoman tai muun tunnistamattoman ilmiön mittaaminen ei kuitenkaan ole mahdotonta, siksi ei pidäkään jättää organisaation toimintaa mittaamatta vain sen vuoksi, että se koetaan vaikeaksi. Tietojärjestelmät mahdollistavat usein taloudellisten ja muiden ei-fyysisten mittareiden tiedon keräämisen, mutta aineettomalle pääomalle tulee suunnitella ja laatia mittarit organisaation tarpeisiin pohjautuen. Siten suunnitellessa mittaria tulee huomioida mikä on mittaamisen kohde ja miten mitattavasta kohteesta saadaan tietoa (Lönnqvist et al. 2006, 73).

Tiedonkulku ja viestintä on perustunut taulukoiden, kaavioiden ja indeksien esittämiseen. Helpon ja sujuvan viestin esittämiseen tarvitaan pisteitä, viivoja, kaavioita, symboleja, kuvia, sanoja, numeroita tai sävyjä. Dashboardeja ja mittareita parannetaan ja niitä päivitetään jatkuvasti. Projektinhallintaympäristössä jokaisella tiedon vastaanottajalla voi olla erilaisia vaatimuksia ja he voivat pyytää erilaisia tietoja projektin elinkaaren aikana. (Kerzner 2017, 11–13.)

Mittareita tulee päivittää, kun tavoitteet muuttuvat, mittari ei tuota tarvittavaa tietoa tai mittarin tuottama tieto havaitaan tarpeettomaksi. Kerätyn tiedon ja sen vertailtavuuden vuoksi mittareiden kehittämistä tai muuttamista on kuitenkin hyvä tehdä pienissä osioissa tietojen vertailtavuuden säilyttämiseksi. (Sampo Consulting 2021.)

4.2 Balanced Scorecard

Balanced Scorecard syntyi, kun kahdessatoista USA:ssa ja Kanadassa sijaitsevassa suuryrityksessä toteutettiin ja kehitettiin yritysten suoritusten mittausta. Tämän kehitysprojektin yhteydessä Kaplan ja Norton havaitsi, että yrityksissä ei mitattu aineetonta pääomaa. Kaplan ja Norton esitteli vuonna 1992 menestystekijämittariston eli Balanced Scorecardin, jolla kyettiin mittaamaan myös osaamista ja henkilöstön menestystekijöitä. Balanced Scorecard on siis kehittyneempi mittaristo, jolla taloudellisten tunnuslukujen lisäksi mitataan aineetonta pääomaa kuten osaamista, työntekijöiden motivaatiota, prosessien tehokkuutta, informaatioteknologian toimivuutta, asiakassuhteita ja -lojaaliutta, poliittista ja yhteiskunnallista hyväksyntää. (Malmi et al. 2006, 16–17.)

Balanced Scorecard eli tasapainotettu tuloskortti on alun perin suunniteltu taloudellisten, asiakas- ja sisäisten prosessien, oppimisen ja kasvun mittaamista varten. Organisaation strategisten tavoitteiden saavuttamista arvioidaan taloudellisen näkökulman avulla. Tällä myös määritellään tavoitteet, jotka pyritään saavuttamaan strategialla. Asiakasnäkökulmaa mitattaessa usein kerätään tunnuslukuja markkinaosuudesta, asiakastyytyväisyydestä, asiakaskannattavuudesta, asiakasuskollisuudesta tai uusien asiakkaiden lukumääristä. (Malmi et al. 2006, 26.)

Asiakasnäkökulmaa mittaaviin perusmittareihin kuuluu asiakaslupauksen mittari, jolla pyritään selvittämään mitä tuotetta tai palvelua asiakas tarvitsee asiakastyytyväisyyden ja asiakasuskollisuuden optimoimiseksi. Sisäiset prosessit mahdollistavat taloudellisen ja asiakasnäkökulman toteutumisen. Sisäisistä prosesseista voi olla hyödyllisempää arvioida innovointiprosessin tuotosta kuin toiminnassa olevan operatiivisen toiminnan tehostamista. Balanced Scorecard muokataan mittaamaan organisaation tiettyjä tarpeita ja tavoitteita. (Malmi et al. 2006, 26–27.)

Julkisella sektorilla mitataan enemmän palvelujen tai tuotteiden laatua ja saatavuutta, jotka ovat yhteiskunnan kiinnostuksen kohteita, kuin varsinaista taloudellista näkökulmaa. Balanced Scorecard muokataan julkisella sektorilla mittaamaan resursseja, vaikuttavuutta, prosesseja ja rakenteita sekä uudistumista ja työkykyä. (Malmi et al. 2006, 24.)

Organisaatioiden tarpeet määrittelevät mittarien näkökulmat. Kaplan ja Nortonin arvion mukaan organisaation käyttöön valitaan 20–25 mittaria, joista 8–10 mittaria on sisäisten prosessien näkökulmaa varten ja lopuille muille näkökulmille valitaan keskimäärin viisi mittaria. Mittarien määrät vaihtelevat aina riippuen organisaatiosta ja mitattavista kohteista. Usein käy myös niin, että organisaatiot vähentävät mittareiden määrää, jos on ilmennyt, että valittu mittari ei vastaa käyttötarvetta tai -tapaa. Jo neljä mittaria yhdelle tasapainotetulle tuloskortille voi olla riittävä valinta käyttötarkoituksesta riippuen. (Malmi et al. 2006, 31.)

Tasapainotetulla tuloskortilla arvioitavien ja mitattavien kohteiden tulee olla tasapainossa valittujen näkökulmien kesken. Tasapainoa suhteutetaan taloudellisten ja ei-taloudellisten mittauskohteiden välillä. Tavoitteena on muodostaa tasapaino, jolloin keskiössä ovat strategiset tavoitteet, joiden saavuttamista mukailevat ja tehostavat muut näkökulmat ja niiden mittarit. Tasapainoa haetaan lyhyen ja pitkän aikavälin tavoitteisiin ja niin ikään tasapainoa haetaan helppojen ja vaikeiden mittareiden välille. Tavoite on, että mittaria käytetään ja että sen suhteellisen helppo ja yksinkertainen käyttää. Siten on merkityksellistä saavuttaa tasapaino eri vaikeusasteisten mittareiden kesken. (Malmi et al. 2006, 32–33.)

4.3 Suorituskykymittari

KPI-mittaristot ovat organisaation toiminnalle keskeisiä mittareita ja niitä on usein käytössä organisaatiossa. KPI mittaa toimintaa tai suorituskykyä, mutta ei strategian onnistumista kuten Balanced Scorecard. (Malmi et al. 2006, 35.)

KPI-mittari (eng. Key Performance Indicator) on suorituskykymittari, joka kertoo miten tehokkaasti yritys voi saavuttaa liiketoiminnan kannalta keskeiset tavoitteet. KPI-mittarit voidaan asettaa organisaation ylä- ja alatasolle erityyppisesti. Organisaation ylätasolla voidaan arvioida yleistä liiketoiminnan suorituskykyä ja alatasolla mitata toimintoja esimerkiksi myynnin tai markkinoinnin parissa. KPI-mittarin tarkoitus on kertoa millä alueella organisaatio menestyy ja missä on kehitettävää. (Sampo Consulting 2021.)

Kun halutaan mitata yrityksen taloudellista menestystä suorituskykymittaria tarkemmalla tasolla, käytetään KRI-mittaria (Key Result Indicator). Se mittaa taloushallinnon alalta saatavia tunnuslukuja, jotka koskevat esimerkiksi tuottoa sijoitetulle pääomalle, myyntikatetta ja varaston kiertonopeutta. KPI-mittari nähdään operatiivisten tunnuslukujen mittarina, josta on yhteys KRI-mittariin. (Lightning Accounting n.d.)

4.4 Tietosuojamittari

Taloudellisten ja operatiivisten tunnuslukujen suorituskyvyn mittaamisen lisäksi tietosuojassa käytetään KPI-mittareita. Tietosuojamittarit (eng. Privacy KPI) ovat nousseet vaatimustenmukaisuuden ja osoitusvelvollisuuden toteuttamisen rinnalle. Niiden avulla kehitetään tietosuojan tasoa ja arvioidaan organisaation kypsyyttä esimerkiksi kehittämällä ja parantamalla asiakastyytyväisyyttä ja asiakasluottamusta tunnistamalla riskejä. Tietosuojamittareiden avulla kuten muillakin suorituskykymittareilla arvioidaan organisaation strategian toteutumista ja tavoitteiden saavuttamista ja arvioidaan tietosuojan toteuttamisen vaikutusta tulokseen. Samoin kuin muita suorituskykymittareita tietosuojamittaria käytetään bud-

jetin ja resurssien arviointiin ja turvaamiseen, suorituskyvyn mittaamiseen, kehityskohteiden tunnistamiseen ja vastuullisuuden ja luottamuksen lisäämiseen. (Polonetsky & Tene 2022.)

Tietosuojaan kohdistettujen suorituskykymittareiden avulla voidaan kerätä tietoa sisäisten ja ulkoisten asiakkaiden suhteesta ja luottamuksesta, kehitettävistä kohteista ja vahvistaa tietosuojalakien ja määräysten noudattamista organisaatiossa (Polonetsky & Tene 2022). Polonetsky & Tene esittää, että trendit ja mitattavat tiedot voi ryhmitellä kuuteen luokkaan niiden tyypittelyn perusteella:

Yksilön oikeudet

- Yksilön oikeuksiin kohdistetut mittarit mittaavat niiden rekisteröityjen prosentuaalista määrää, jotka ovat antaneet suostumuksen sähköpostimarkkinointiin ja luvan jakaa tietoa itsestään, keräävät rekisteröityjen pyyntöjä ja asiakastyytyväisyystilastoja, tietosuojaloukkaustapahtumia sekä mittaavat vaikutusten laajuutta. Näiden tietojen avulla voi mitata kuinka tehokkaasti tietosuojakäytänteet suojaavat asiakkaiden henkilötietoja ja missä määrin asiakkaat luottavat organisaatioon.

Koulutus ja tietoisuus

- Tämä mittaristo kokoaa yhteen henkilöstölle tarjottujen tietosuojakoulutusten määrän, koulutetun henkilöstön määrän ja henkilöstön sitoutuneisuutta tietosuojatyöhön. Kun henkilöstö on kiinnostunut ja sitoutunut noudattamaan tietosuojalainsäädäntöä ja yritykset voivat varmistaa lainmukaisuuden, organisaatio pystyy samalla ylläpitämään ja parantamaan imagoa, luotettavuutta ja yksilön suojaa. Mittariston avulla organisaatio voi tunnistaa kehitettäviä kohteita henkilöstön tietosuojaan liittyvässä osaamisessa tai tietoisuudessa, mitä voi hyödyntää seuraavan koulutuksen sisältöä laadittaessa

Kaupallisuus ja asiakkuudet

- Kaupalliset ja asiakkuusmittarit keräävät tietoa ja mittaavat asiakkaiden kanssa allekirjoitettujen tietojenkäsittelysopimusten määrää, ulkopuolisten toimittajien arvioita organisaation tietosuojakäytänteistä tai tietosuojasertifikaattien määrää. Mittarit keskittyvät asiakkaisiin ja organisaation sitoutumiseen sekä seuraavat tietosuojakäytänteiden kykyä tukea liiketoiminnallisia ja strategisia prioriteetteja, kun käyttöön otetaan uusia teknologioita.

Osoitusvelvollisuus

- Organisaatio osoittaa kykynsä noudattaa lakeja esimerkiksi laatimalla tietosuojan vaikutustenarvioinnit, seuraamalla tietosuojakonsultaation määrää eri projektien kesken ja pitämällä tietosuojakäytännöt, -menettelyt ja -ohjeistukset ajan tasalla samalla kun organisaatio parantaa kilpailu- ja maine-etuansa.

Tietosuojan valvonta

- Nämä mittarit mittaavat organisaation tietosuojaan liittyvien palvelujen tai tehtävien määriä. Mittarit keräävät määriä eri hallintajärjestelmistä, tietosuojan vaikutustenarvioinneista ja esimerkiksi lukuja tietosuojan usein kysytyt kysymykset -palvelusta. Näiden mittareiden tavoite on muuttaa tietosuojakäytänteet mitattavaksi käytännön tasolla.

Käytännöt ja linjaukset

- Organisaatio voi seurata vaatimustenmukaisuutta ja tietosuojalainsäädännön noudattamista samanaikaisesti kehittäessään ympäristö-, sosiaali- ja hallintoluokitustaan. Läpinäkyvyys lisää asiakkaiden ja sidosryhmien luottamusta siihen, että organisaatio käsittelee tietoja eettisesti ja samalla lisää tietoisuutta käytänteiden mahdollisista muutoksista.

4.5 Tietosuojamittareiden kohteet

Tietosuojaan liittyvät tehtävät – kuten kaikki toiminnot organisaatiossa – voi esimerkiksi viedä vuosikelloon tehtävinä ja tavoitteina ja arvioida vuosikellon avulla tehtävien edistymistä ja tavoitteiden saavuttamista. Johdon edustajat tai tietosuojavastaavat voivat käyttää mittareita edistämään vaatimustenmukaisuuden toteutumista liiketoiminnassa tunnistamalla riskejä ja tuomalla esiin puutteita, joita liiketoiminnan ratkaisuissa tulisi tunnistaa ennakoidusti. Mittareiden avulla voi asettaa lähtötason (eng. maturity, suom. kypsyystaso) ja arvioida ja vertailla organisaation tasoa lainsäädäntöön ja standardeihin tai kilpailijoiden kesken. Mittaamisen avulla liiketoiminnassa voi vähentää riskien toteutumista, vähentää toteutuvien riskien heikentävää vaikutusta luottamukseen ja organisaation imagoon. Tietosuojan kypsyystasoarviointi ja tason kehittäminen on keino organisoida ja yksinkertaistaa tietosuojan laajaa ympäristöä ja toimialaa sekä mitata käytänteiden ja määräysten mukaisia prosesseja ja suorituskykyä. (Tene & Culnan 2021, 4.)

The Future of Privacy Forum (FPF) on tutkinut tietosuojan suorituskykyyn ja tavoitteisiin liittyviä mittareita. FPF asetti työryhmän (Privacy Metrics Working Group) selvittämään osoitusvelvollisuuteen ja lainmukaisuuden todentamiseen liittyviä erilaisia mittareita, näiden tarkoituksia ja sidosryhmiä. Työryhmän raportissa annetaan selvitys yleisimmistä organisaatioissa käytettävistä mittareista, riskienhallinnasta ja suorituskyvyn mittaamisesta sekä työkaluista, joilla voi kerätä tietoja mittareiden kokoamista varten. (Tene & Culnan 2021, 3.)

Myös tietosuojamittareita valittaessa tulee tunnistaa tarpeet tiedon mittaamiselle, tavoitteet, mitatun tiedon hyödyntäminen jatkossa, resursointi ja organisaation kypsyystaso. Tietosuojamittarit voivat olla laadullisia tai kvantitatiivisia mittareita, joilla kerätään tietoa johtamiseen, seurantaan, suorituskyvyn mittaamiseen tai raportointiin. Tietosuojamittarit kohdennetaan vaatimustenmukaisuuden, operatiivisen tai liiketoiminnan osa-alueisiin tai esimerkiksi ulkoisten asiakkaiden tai kumppaneiden mittaamiseen. Jotta mittarit toimivat tehokkaasti ja niistä saa mahdollisimman suuren hyödyn, mittareita tulee arvioida niille asetettujen tavoitteiden perusteella. Määräysten noudattamiseksi vaatimustenmukaisuus sisältää mittaamista ja KPI-seurantaa, joiden avulla voidaan osoittaa erilaisten lakien ja määräysten noudattamista. (Tene & Culnan 2021, 3.)

Operatiivisessa mittaamisessa arvioidaan dokumentointia ja sisäisten tietosuojatehtävien suorituskyvyn parantamista. Tavoite on hallita organisaation riskejä ja edistää toimintoja asetettujen tavoitteiden saavuttamiseksi, joita ovat esimerkiksi tietosuojalainsäädösten mukaisesti toimiminen, määräysten ja laadittuja linjausten noudattaminen tai standardin vaatimusten ja menettelyjen mukaisesti toimiminen. Operatiivisessa mittaamisessa voidaan kerätä tunnuslukuja häiriöhallinnasta, niiden raportoinnista tai SLA-laskennasta (eng. Service Agreement Level, suom. palvelutasosopimus) muun riskienhallinnan yhteydessä. Operatiivisessa mittaamisessa voi kerätä tietoa kumppanin, toimittajan tai palveluntarjoajan kanssa toteutetusta tiedon jaosta ja kansainvälisestä tiedon siirrosta. Operatiivisessa mittaamisessa voi muodostaa mitattavia tunnuslukuja henkilöstön kouluttamisesta ja tietosuojatietoisuuden lisäämisestä. (Tene & Culnan 2021, 3–4.)

Asiakkuudessa keskitytään asiakkaiden sitouttamiseen ja liiketoiminnan jatkuvuuteen. Mittareiden avulla selvitetään ja arvioidaan miten organisaation läpinäkyvyys tietosuoja-asioissa edistää asiakkaiden luottamusta ja lisää asiakastyytyväisyyttä. Lisäksi asiakkuudessa voi mitata käyttäjien sitoutumista organisaation tuotteisiin ja arvioida miten sitoutumista voi edistää. Myös henkilötietojen käsittelijöiden tai kolmansien osapuolten palvelutasoa, tyytyväisyyttä ja virheettömyyttä voi mitata ja arvioida, kuten edellä operatiivisessa mittaamisessa on kuvattu. Mittaamisen avulla voi valvoa sopimushallintaa, sisäänrakennetun tietosuojan noudattamista ja toteuttamista, tiedon elinkaaren hallintaa, varmistua tietosuojan vaikutustenarviointien (DPIA, TIA) laatimisesta, henkilötietojen tietoturvaloukkausten selvittämisestä ja rekisteröidyn oikeuksien ja vapauksien toteuttamisesta. Liiketoiminnan mittareiden avulla voi seurata tietosuojakäytänteiden kykyä tukea liiketoiminnallisten strategisten prioriteettien saavuttamista, valvoa prosesseja ja myös ottaa käyttöön uusia tekniikoita. (Tene & Culnan 2021, 4.)

Organisaation ulkoiset mittarit voidaan asettaa mittaamaan organisaation tai tuotemerkin mainetta. Mittaamisen avulla haetaan etulyöntiasemaa ja kykyä erottua kilpailijoista. Saatujen tietojen perusteella organisaatio voi kehittää avoimuutta, läpinäkyvyyttä ja parhaita käytäntöjä. Ulkoiseen mittaamiseen sisältyy sidosryhmien kanssa käyty yhteistyö lainsäätäjien, tutkijoiden tai standarditoimielinten kanssa. Ulkoisella mittaamisella voi seurata poliittisten tavoitteiden kuten lainsäädäntö- ja sääntelyaloitteiden ja uusien säännösten ehdottamista ja noudattamista. (Tene & Culnan 2021, 4.)

Tietosuojan suorituskykymittareilla mitataan vaatimustenmukaisuutta osoittavia tietoja kuten rekisteröityjen tarkastuspyyntöjen ja tietosuojan vaikutustenarviointien määrää, joiden perusteella johto pääsee seuraamaan prosessien tehokkuutta. Kehittyneempi mittari näyttää prosessien läpimenoajat kuten rekisteröidyn tarkastuspyynnön vastaamiseen kuluneen ajan (Polonetsky & Tene 2022.) tai henkilötietojen tietoturvapoikkeaman selvittämiseen ja ilmoitusvelvollisuuden hoitamiseen kuluneen ajan.

Tene & Culnan esittää taulukossa 1 työryhmän The Future of Privacy Forum (FPF) laatiman menetelmän sidosryhmien kerätä tietoja tietosuojavaatimusten noudattamisesta ja raportointitietojen tarkoituksen (Tene & Culnan 2021, 4–5).

TAULUKKO 1. Mittarit ja niiden raportoinnin tarkoitus esitetty sidosryhmittäin (Mukaillen Tene & Culnan 2021, 5)

Sidosryhmät	Mittari	Raportointitietojen tarkoitus
Johtajat	• Kuvaus korkean luokan riskistä ja kypsyystasosta • Aineelliset vahingot	• Varmistaa myynnin ja tuen • Resurssien oikea kohdentaminen riskeihin • Raportti riskeistä ja niiden vaikutuksista tulokseen • Raportti kypsyydestä, tilasta ja edistymisestä
Johto	• Perusteellinen riskien arviointi • Arviointi riskiperusteisesta menettelytavasta ja vaikutuksesta • Tapahtumien (häiriöt) luvut ja trendit • Projektin toteutuksen edistyminen/kulut • Tulokset korkean tason suorituskyvystä	• Varmistaa sisäänosto/tuki ja valvonta • Riskien hyväksyminen/päätökset • Tapahtuman luokittelu ja priorisointi • Tehokkuuden ja kypsyystason hallinta • Varmistaa tuki tietojen keräämiseksi
Tietosuojatiimi	• Kokonaisriskien arviointi jaksoittain • Arviot ohjelman/projektin tilasta, tapahtumien (häiriöt) luvut ja trendit, kontrollien jalkautus, ulkoisten kumppaneiden mittarit sekä tapahtumien, toiminnallisuuksien ja suorituskyvyn mittarit • Tietosuojan vaikutusarviointi (DPIA, TIA), kumppaneiden arviointi	• Ongelman havaitseminen: tehokkuuden varmistaminen tai arviointi, puutteiden ja ongelmien seuranta kypsyystason arvioinnilla • Sidosryhmien informointi tiedottamalla/dashboard, vuorovaikutuksen edistäminen • Tiimin sitouttaminen tärkeimpiin tavoitteisiin • Sisäinen resurssien allokointi • Suorituskykyarviot
Liiketoiminta	• Projektin tai tuotteen riskit ja vaatimustenmukaisuus • Osoitusvelvollisuus/suorituskyky • Riskianalyysit • Edistyminen uusien vaatimusten täytäntöönpanossa/osoittaa tunnistetut ongelmat	• Kommunikointi markkinoinnin, HR:n, tuotteiden, suunnittelutiimien ja liikekumppaneiden kanssa varmistaakseen ongelman havaitseminen, vaatimustenmukaisuuden noudattaminen ja sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen • Liiketoimintayksiköiden vastuun varmistaminen johdettaessa tietosuojariskejä
Ulkoinen	• Tietosuojan vaikutustenarvioinnit PIA, TIA, DPIA • Sääntelyviranomaiset, itsesääntelyelimet ja/tai ulkopuoliset tarkastajat: vastuullisuuden kartoitus, rekisteri toiminnallisista aktiviteeteista kuten ROPA, PIA, DPIA, TIA, tiedottaminen tapahtumista/häiriöistä • Media ja kumppanit: vaatimustenmukaisuus liiketoiminnassa	• Asiakkaat: läpinäkyvyys ja luottamus, brändin erottuvuus • Sääntelyviranomaiset: vaatimustenmukaisuus, osoitusvelvollisuuden osoittaminen • Sijoittajat ja osakkeenomistajat: vaatimustenmukaisuus, osoitusvelvollisuuden osoittaminen ja käytäntöjen tehokkuus • Kumppanit: kommunikointi käytänteistä ja osoitusvelvollisuudesta • Media: brändin ja maineen ylläpitäminen
Sisäinen tarkastus ja riskienhallinta	• Pyynnön mukaan	• Vaatimustenmukaisuuden osoittaminen ja vahvistaminen sekä riskien, kustannusten ja kehittämisen seuranta

Työntekijät	• Koulutus ja tietoisuuden lisääminen • Riskianalyysit • Liiketoiminnan mahdollistaminen • Päivitykset käytänteiden ja jalkautuksen materiaaleihin	• Sujuva työskentely tietosuojatiimin kanssa • Koulutus ja tietoisuuden lisääminen • Myynnin tai suhteiden päälliköt: tietosuojakäytänteiden ja kontrollien jako asiakkaiden kanssa erottuvuuden mahdollistamiseksi • Työntekijän nettosuositteluindeksin (eNPS) kasvattaminen

Lisäksi Tene & Culnan esittää taulukossa 2 tietosuojaan ja vaatimustenmukaisuuden osoittamiseen liittyviä esimerkkejä mitattavista kohteista ja niiden mittareista. Tene & Culnan esittävät sidosryhmille kohteita, joista tietoja kerätään mitattavaksi kuten esimerkiksi rekisteröidyn oikeuksien ja vapauksien toteuttamisesta, henkilöstön koulutuksesta ja tietoisuuden lisäämisestä, vaatimustenmukaisuudesta tai käytänteiden toteuttamisesta (taulukko 2). Menetelmän avulla tietosuojavaatimusten mittaamisen kohteita laajennetaan sidosryhmille ja projekteihin.

TAULUKKO 2. Mitattavat kohteet ja niille asetettavat mittarit kategorioittain (Mukaillen Tene & Culnan 2021, 6–9)

Mittareiden kategoriat	Mitattavat kohteet	Mittarit
Rekisteröidyn oikeudet	• Rekisteröidyn pyynnöt tarkastaa, oikaista tai poistaa omat tietonsa • Pyyntöjen ja valitusten käsittely	Määrä vastaanotetuista pyynnöistä • Käynnissä • Suljettu • Käsittelyn kesto • % tyytyväinen ja % tyytyväinen toimitukseen vaaditussa ajassa • Pyynnöt tyypin tai SLA-aikojen mukaan
	Tietosuojapoikkeamat ja -loukkaukset	• Tapausten lukumäärä tyypin/riskin vakavuuden/liiketoimintayksikön mukaan • Asiakkaiden määrä, joihin poikkeama tai loukkaus vaikuttaa • % tapauksista tyypin mukaan tai SLA-aikojen mukaan • % tapauksista, joissa perimmäinen syy on tunnistettu ja korjaavat toimenpiteet toteutettu • # ja % valvontaviranomaiselle ilmoitetuista tapauksista ja rekisteröidylle • # ja % määrä tapahtumista, jotka ilmoitettu 72 h sisällä raportoiduista tapauksista • Keskimääräinen aika tapauksen tunnistamiseen (tunnistamiskyvyn mittari) • Keskimääräinen aika ratkaista tunnistettu tapaus (prosessin tehokkuuden mittari)

	Tietosuojaan liittyvät valitukset	kuten edellä
	Yleiset tietosuojaan liittyvät kyselyt	kuten edellä
	Suostumus	• Suostumus evästeiden käyttöön, evästeiden kieltäminen • Suostumus tietojen käsittelyyn • Suostumus tietojen jakamiseen • Suostumus sähköpostimarkkinointiin
Koulutus ja tietoisuuden lisääminen	Tietosuojaan liittyvät koulutukset ja tietoisuuden lisääminen	• Tarjottujen koulutusten määrä • Koulutetun henkilöstön määrä • Koulutuksiin osallistuneiden määrä • % kohdennetusta henkilöstöstä suorittanut koulutuksen ajallaan • Osallistujat (henkilöittäin) • % työntekijöistä, jotka läpäisevät testin koulutuksen lopussa • # suoritettujen sertifikaattien/todistusten määrä • # laadittujen ja katsottujen lisämateriaalien määrä (esim. uutiskirjeet, uutisointi sähköpostitse, uutiset, valkoiset paperit, web-sivut, vierailijoiden määrä verkkosivustolla, sisäiset pelikirjat)
	Prosesseihin ja ohjeisiin liittyvät tietosuojan usein kysytyt kysymykset	• Työntekijöiden sitoutuminen
Kaupallisuus ja asiakkuudet	Tietosuojan vaikutustenarviointi (DPIA, TIA, PIA) Turvallisuus ja tietojen suojaus	• Neuvoteltu asiakas • Suljettu asiakas • Neuvoteltu myyjä tai kumppani • Suljettu myyjä tai kumppani • Seuranta oleellisesti muuttuneista ehdoista, jotka poikkeavat standardoidusta tavasta • Aikaikkuna tapahtuman päättämiseen
	Kumppaneiden ja toimittajien arvostelu	• Toimittajan tietosuojan vaikutustenarvioinnit, riskiarvioinnit (# käynnissä, # valmis, # kesken, # suunniteltu, # tulokset) • Toimittajan kontrollit (# valmis, # käynnissä, # suunniteltu, havainnot) • Jokaisen toimittajan PCI DSS-arvioinnit ja tila • Toimittajan vaatimustenmukaisuuden noudattamiseen liittyvät ongelmat (# vakavuus, tila suhteessa tavoiteltuun sulkemispäivään jne.)
	RFI (Request for Information) RFP (Request for proposal)	• Vaatimustenmukaisuuden todistukset • Valmistumisen aikataulu • Standardoitujen RFI/RFP saatavilla olevien UKK määrä
	Yritysjärjestelyt/Divestointi/TSA-sopimus/Yhteishankkeet	• Neuvoteltu/suljettu • Tunnistettujen korjaavien toimenpiteiden määrä
	Toimitusketju	• # tietojen jakamista koskevista sopimuksista • % sopimukset, joissa on tietosuojalauseke

Vaatimustenmukaisuus	Käytännöt, menettelyt, ilmoitukset (kuluttajat, työntekijät)	• # inventointi • Ajantasaisuus • Viimeisin päivitys/tarkistuspäivä
	Tietosuojan vaikutustenarvioinnit (PIA, DPIA)	• Korkean riskin tietojen käsittelytoimien lukumäärä, jotka edellyttävät DPIA:n laatimista (% kokonaismäärästä/% alkuseulonnasta) • Määrä laadituista ja hyväksytyistä DPIA- ja PIA-arvioista • Läpimenoaika vs. SLA
	Tietosuojan vaikutustenarviointi henkilötietojen siirrosta EU:n ja ETA-alueen ulkopuolelle (TIA)	• Määrä tietojen siirtojen vaikutustenarvioinneista (Schrems II jälkeen) • Määrä kumppaneiden ja toimittajien kyselyistä
	Seloste käsittelytoimista	• Seloste käsittelytoimista määrä • #- ja % eri sovelluksista selosteessa käsittelytoimista • Määrä valmistuneet selosteet käsittelytoimista
	Projektien tai tuotteiden konsultointi	• Määrä neuvotelluista toimista markkinoinnissa • Määrä neuvotelluista toimista HR:ssä • Konsultoinnin määrä uusien liiketoimintamallien tai teknologiaratkaisujen parissa (esim. pilvipalvelu) • Monialaisten projektien määrä
	Sääntely	• Määrä säätelyjen tiedusteluista (tyyppi, avattu, suljettu)
	Liiketoiminta ja sen toiminnot	Liiketoimintayksikköä kohden: • Määrä nimetyistä tietosuoja-asiantuntijoista / lähettiläistä (K/E) • Liiketoimintayksikön tietosuojan käytännöt käytössä ja dokumentoitu? (K/E) • #- ja % vaatimustenmukaisuuden täyttävistä sovelluksista, jotka käsittelevät henkilötietoja • Edistymisen tila (liikennevalot tai % valmis) alkutasoon nähden (BAU) tai % muutoksia on toteutettu sääntelyn täytäntöönpanotoimissa • Vaatimustenmukaisuuden tilan seuranta- ja tarkastustoimet (ajallaan, myöhässä)
Tietosuojan kilpailijat (hub & spoke järjestely) ja kolmasosapuoli	Tietosuojatoiminnot tuotanto- ja kehitystiimeissä	• Henkilötietojen hallintajärjestelmien lukumäärä (PIMS) • Määrä DPIA:n konsultoinneista • Määrä menettelysääntöjen tuesta • Määrä yksikön/osaston henkilötietojen poiminnoista ja käyttöarvostelut • Monialaisten tietosuojaprojektien määrä • Tuettujen DSR määrä • Määrä tarjotuista tietosuojakoulutuksista yksiköittäin/osastoittain • Tietosuojaan liittyvien usein kysyttyjen kysymysten lukumäärä ja viestintä tietoisuuden lisäämiseksi (yksikkö/osasto/roolikohtainen)

Käytännöt	Lainsäädäntötyö Sijoittajien luokittelu Ympäristö, yhteiskuntavastuu ja hyvä hallintotapa (ESG)	• Laskujen valvonta • Uusien lakien seuranta • Arvostelujen läpikäynti ja tila • Luokituslaitosten tulokset

Markkinoista ja toiminta-alueista riippumatta tunnistetaan hyötyjä mittaamisen käynnistämiseksi ja samoin tunnistetaan mittaamisen käynnistämiseen liittyvät vaikeudet. Mittaamisen hyödyt painottuvat kustannustehokkuuden arvioinnin lisäksi kykyyn tunnistaa organisaation lähtötaso, johon perustuen voi tehdä sisäistä ja ulkoista toimintaa parantavia toimia liiketoiminnan tai työntekijöiden viihtyvyyden lisäämiseksi. Mittaamisen haasteet muodostuvat muun muassa organisaation toiminnasta, jos organisaatiossa ei ole täysin selvää mitä mitataan ja miksi mitataan. Haasteita muodostuu manuaalisesta työskentelystä ja resurssien kuluttamisesta manuaalisessa tiedon keruussa, jos laitteet ja järjestelmät eivät tue automaattista tiedon keruuta tai tiedon visualisointia raportointia varten. Organisaation tahtotila, strategiset tavoitteet ja käytettävissä olevat resurssit tulisi tunnistaa, jotta tavoitteita saavutettaisiin.

4.6 Ympäristö, yhteiskuntavastuu ja hyvä hallintotapa

Mittareiden suunnitteluun ja käyttöönottoon julkishallinnon organisaatio voi hakea mallia myös yritysmaailmasta. Yritysvastuusta ja vastuullisesta sijoittamisesta käytetään termiä ESG - Environmental Social Governance eli ympäristö, yhteiskuntavastuu ja hyvä hallintotapa liiketoiminnassa. ESG-raportointi mahdollistaa läpinäkyvyyden yrityksen riskienhallintaan, vastuullisiin toimiin, vastuulliseen sijoittamiseen ympäristön, yhteiskuntavastuun ja sosiaalisen vastuun parissa liike- ja yritystoiminnassa. ESG-mittareista laaditun vastuullisuusraporttien perusteella sijoittaja voi valikoida sijoituskohteita niiden riskienhallinnan perusteella, jossa on otettu tehokkaasti huomioon riskit ympäristöön, ihmisoikeuksiin, työoloihin ja liiketoiminnan etiikkaan liittyen. (Nordea. 2023.)

ESG-vastuullisuusarvioinnin yrityksen liiketoiminnasta tekee ulkopuolinen tarkastaja. ESG-raportointi tuo esiin yrityksen ympäristöön, yhteiskuntaan ja hyvään hallintoon liittyviä tuloksia kuten riskienhallinta, etiikka, ihmisoikeudet, tietosuoja,

turvallisuus, taksonomia. ESG-raportointi tehostaa suurten kansallisten ja kansainvälisten yritysten raportointia.

Julkishallinnon organisaatioiden läpinäkyvyys palvelun tuottamisen, tarjonnan ja turvallisuuden osoittamisessa on tärkeä osa julkishallinnon toimintaa, jossa ensisijainen mittaamisen kohde on yhteiskunnalle tuotetut palvelut ja tuotteet. ESG-raportoinnin avulla myös julkishallinnon organisaatiot voivat lisätä läpinäkyvyyttä ja tuoda vastuullisuuttaan esille niin ympäristö-, yhteiskunta kuin hyvään hallintoon liittyvissä asioissa.

Useiden julkishallinnon organisaatioiden kanssa Suomessa toimiva CGI on laatinut ESG-raportin, jonka mukaan tietoturvan, tietosuojan ja liiketoiminnan osa-alueita on mitattu laajasti (CGI 2022, 1). CGI:n ESG-raportissa esitetään prosesseja, joista tietoja on kerätty mitattavaksi.

CGI:n sisäisissä prosesseissa kerätään tietoja kuukausitason kokouksista, joissa muun muassa turvallisuuden arviointiryhmä käy läpi strategian alueet liiketoimintayksiköiden ja johdon kanssa. Kuukausitason kokouksissa käydään läpi projektien tila, kuluneen jakson tärkeimmät kohokohdat ja avaintulokset. CGI:n raportin mukaan turvallisuuden arviointiryhmän toimet mahdollistavat jatkuvan arviointi- ja tarkistusprosessin, jolla organisaatio varmistaa ylimmän johdon tietoisuuden kokonaistilanteesta ja johdon sitoutuneisuuden ja ohjauksen. (CGI 2023, 113.)

CGI:n raportin mukaan maailmanlaajuisen turvallisuusohjelman avulla seurataan ja valvotaan yrityksen toimintaa. Maailmanlaajuiseen turvallisuusohjelmaan sisältyy kyberturvallisuus, yleinen ohjaus, strateginen ohjaus ja riskien vähentäminen. Raportointi tapahtuu kvartaaleittain, jossa turvallisuusohjelmasta esitetään päivitykset kriittisistä ja erittäin vakavista tapahtumista, joilla voi olla vaikutuksia aineellisiksi vahingoiksi sekä selvitykset meneillään olevista korjaavista toimenpiteistä tai hallintatoimenpiteistä. Turvallisuusohjelman ja jatkuvan raportoinnin hyödyt ovat jatkuvan tietoisuuden varmistaminen, jolloin ylin johto saa oikea-aikaista tieto kohteista, joissa tarvitaan turvallisuuden investointeja ensisijaisesti. (CGI 2023, 113.)

ESG-raportointi on laaja tapa tarkastella organisaation tilaa ja raportoida. Onnistunut raportointi tarvitsee hyvin suunnitellut ja harkitut mittarit, joita käytetään kaikilla organisaation tasoilla sen toiminnassa. ESG-mittarit kohdennetaan yhteen tai kaikkiin osa-alueisiin. Vastuullisuusraportoinnin laajuuden vuoksi raportointi laajennetaan usein vaiheittain organisaation eri toiminta-alueisiin.

Suomessa Neste on kohdentanut mittaamisen turvallisuuteen. Johto ja henkilöstö on painottanut mittaamisessa työturvallisuutta. Työturvallisuustulosten tavoitteet mittaavat vastuullisuutta ja operatiivisen toiminnan sujuvuutta. Asetetut ilmastotavoitteet ovat uusimpana mittauskohteena. (Niemi 2021a.) Terveystalo on valikoinut sosiaalisen (Social) vastuun ESG-mittareista. Tietojen mittaamisessa on tunnistettu, että mittaaminen voi olla hankalaa, jos alalla ei ole vakiintuneita käytäntöjä, tiedot eivät ole vertailtavissa ja mittareita tulkitsee esimerkiksi toimialueen ulkopuolinen. Terveystalo mittaa myös digitaalista jalanjälkeä toimiakseen suunnannäyttäjänä ja parantaa digitalisaatiolla terveydenhuoltoalan tuottavuutta. (Niemi 2021b.)

ESG-raportointia suunnataan pörssiyhtiöiden parista myös pk-yrityksille. Pienyritysten toimintaan sopivat mitattaviksi kaikki ESG-raportoinnin osa-alueet. Ympäristökohteissa mitattaisiin muun muassa toiminnan sertifiointia tai ympäristöjärjestelmän rakentamista. Sosiaalisessa vastuussa mitattaisiin työntekijöiden tasa-arvoisuutta, työntekijöiden vaikuttamismahdollisuutta ja turvallisuutta, vastuullista hankintojen edistämistä ja vastuullisuutta asiakassuhteissa. Hyvästä hallintotavasta mitattaisiin muun muassa toimintaa kriisin aikana ja kriisiviestinnän hallintaa, eettisyyttä hankintasuhteissa ja korruption vastaista toimintaa. Pienyritys voi keskittyä parantamaan yhtä osa-aluetta kerrallaan saadakseen konkreettisia tuloksia ja näyttöjä aikaan. (Ekokompassi. n.d.)

Vastuullisuus on noussut yritysten kriittiseksi menestystekijäksi mikä luo pohjaa parempaan liiketoimintaan. Säätely ja raportointivaatimukset ovat lisääntyneet ja proaktiivisia toimia vastuullisuustoimenpiteiden toteuttamiseksi odotetaan yrityksiltä. Muuttuneen markkinamaailman vaatimukset ovat mahdollistaneet sen, että esimerkiksi ilmastoasioihin asetettuja raameja ylitetään yrityspuolella. (Ilkka 2022.)

4.7 Raportointi

Mittaamalla ja arvioimalla tunnistettuja puutteita tai muutosta voidaan ennustaa organisaation toimintakykyyn tai tuottavuuteen vaikuttavia tekijöitä. Mittareiden tarkoitus ei ole tarjota lisää informaatiota vaan tuottaa tietoa oikeaan aikaan substanssin edustajalle tai johdolle kustannustehokkaan toimintatavan saavuttamiseksi. Jos raportteja ei tuoteta, organisaatio ei saa tietoa muutoksista. Jos taas informaatiota on liikaa, raporttien sisältö saattaa olla merkityksetön tavoitteiden saavuttamisessa. Ongelma raportoinnissa on, että ne esittävät lukuja ja arvoja menneessä muodossa. Raportoinnin ongelmaa voi ratkaista mittaamalla tietoja ja lukuarvoja, jotta voidaan ennustaa muutosta ja tulevaisuuden tapahtumia.

Raporttien laadinnan tavoitteena tulee olla, että raporttien sisältö on kohdennettu oikealle kohderyhmälle. Raporttien tulee olla helposti luettavissa ja tulkittavissa niin että ne kertovat tehokkuuden tai toimintakyvyn muutoksista käyttävät sopivaa julkaisumuotoa kustannustehokkaalla tavalla. (Sousa 2017).

Raportit, jotka eivät vastaa varsinaiseen tarpeeseen, heikentävät tehokasta ja luotettavaa raportointia ja aiheuttavat virheellisiä päätöksiä. Myös asiantuntijatiimi saattaa päätyä tuottamaan raportteja, jotka eivät ole hyödynnettävissä päätöksenteossa, jos mittaria ei ole määritelty ja arvioitu tarpeen mukaisesti. (Kerzner 2017, 11.)

Mittareista saatavilla tiedoilla raportoidaan eri sidosryhmille. Raportointi tietosuojasta edellyttää yhteenvetojen esittämistä kirjallisesti ja suullisesti. Keskeinen tehtävä on muuttaa mitattua tietoa narratiiviin, jotta eri sidosryhmät kuten johtoryhmä, riskienhallintaryhmä, liiketoiminta, operatiiviset ryhmät ja asiakkaat (kumppani, toimittaja, palveluntuottaja, asiakas) saavat tarvitsemansa tiedon. (Kerzner 2017, 260–261.)

Yksinkertaisimmillaan raportointi on visuaalisesti esitetty taulukko, dashboard tai tiedote. Mittareista kerätty tieto raportoidaan kohderyhmälle sopivaksi. Yksinkertaisin dashboard on raportointi liikennevalojen väreillä. Tällöin raportointiin on koottu kriittisimmät toimintaan vaikuttavat tekijät. (Kerzner 2017, 260–261.)

Punainen valo

- ongelma vaikuttaa ajankäyttöön, kustannuksiin tai laatuun. Johdon tai sidosryhmien edustajien toimenpiteitä tai päätöksiä voidaan tarvita.

Keltainen valo

- mahdollinen ongelma voi muodostua, jos tilannetta ei seurata tai valvota. Johdon tai sidosryhmien edustajat informoidaan tilanteesta. Johdon tai sidosryhmien edustajien toimenpiteitä ei välttämättä tarvita.

Vihreä valo

- tehtävät tai tavoitteiden saavuttaminen etenee suunnitellusti. Johdon tai sidosryhmien edustajien toimenpiteitä ei tarvita. (Kerzner 2017, 260–261.)

On suositeltavaa, että liikennevalon värejä käytetään raportoitaessa johdon edustajille. Liikennevalojen värit selventävät kriittisyyden tilan projektin tai resurssien tilasta. Punainen väri projektiin liittyvissä riskeissä tarkoittaa esimerkiksi joidenkin riskien eskaloitumista ja riskien alentamista hallintatoimenpiteillä. Keltainen väri tarkoittaa esimerkiksi joidenkin riskien tunnistamista ja riskien hallintatoimenpiteiden käynnistämistä tai laatimista. Vihreä valo tarkoittaa esimerkiksi, ettei riskejä ole. (Kerzner 2017, 260–261.)

Kuvatessa projektin resursseihin liittyviä riskejä punainen väri tarkoittaisi esimerkiksi puutteita henkilöstön osaamisessa, joita tarvitaan projektin toteuttamiseen. Keltainen väri tarkoittaisi esimerkiksi tarvittavassa osaamisessa olevan tunnistettuja riskiä, mutta osaamisen puutteella ei ole merkittävää vaikutusta projektin onnistumiseen. Vihreä väri tarkoittaisi esimerkiksi tarvittavan osaamisen ja pätevyyden olevan käytettävissä projektin toteuttamiseen. (Kerzner 2017, 260–261.)

Johdon edustajille ja liiketoiminnalle voi raportoida Balanced Scorecardin avulla esittämällä strategian ja liiketoiminnan tavoitteiden saavuttamista. Organisaation sisäistä raportointia voi hoitaa esimerkiksi arvioimalla vuosikelloon asetettujen tehtävien toteutumista. Sisäisiin raportteihin on suositeltavaa ottaa käyttöön kevyempi raportointimenetelmiä. Joissakin käytettävissä olevissa ohjelmissa on oletuksena dashboard, joka visualisoi kerätyt tiedot selkeään esitysmuotoon. Hankkimalla lisenssin Microsoft Power BI -ohjelmistoon kerätyn tiedon visualisointi on sujuvaa ja vähentää raportin laatimisessa manuaalista työskentelyä. Edellä esitetyt raportointimenetelmät mahdollistavat raportoinnin kuukausittain,

kvartaaleittain tai kolmannesvuosittain. Kerran vuodessa laadittava tietotilinpäätös on kattava raportointi sidosryhmille.

Raportoinnin merkitys kasvaa yritysmaailman ottaessa laajemmin käyttöön ESG-raportoinnin ja yksityisen sektorin asiakkaat edellyttävät tietojen saantia yrityksen vastuullisuudesta. Tässä luvussa kuvatut menetelmät antavat rakennetta ja suuntaviivoja tuottaa tietoa johdon päätöksentekoa varten. Jos on havaittavissa, että raportointi ei ole sujuvaa tai oikea-aikaista, riskiperusteisella tarkastelulla yksinkertaisinta on järjestää tarvittavat resurssit asian korjaamiseksi.

5 KEHITTÄMISTEHTÄVÄN TULOKSET

Tässä opinnäytetyössä on käytetty teoreettista viitekehystä tutkimuskysymysten selvittämiseen. Teoria on toiminut tukena tuottaa tietoa tutkittavasta kohteesta, ja opinnäytetyössä on esitelty tutkittavaan aiheeseen liittyvää kirjallisuutta, joka kytkeytyy tutkimusongelman selvittämiseen (Eskola & Suoranta 2000, 80).

Opinnäytetyön kehittämistehtävän lähestymistavaksi valittiin case-tutkimus, koska opinnäytetyön tavoitteena on saavuttaa tuloksia, joiden avulla voidaan kehittää organisaation toimintaa. Tietosuojaperiaatteiden toteutumisen mittaamisesta tunnistettiin vain vähän kirjallisuutta, josta syystä laadullinen tutkimusmenetelmä valittiin epäselvän ja kompleksisen ilmiön selvittämiseksi. (Saaranen-Kauppinen & Puusniekka 2009, 13). Laadullisessa tutkimuksessa käytetään teemahaastatteluja, joiden avulla voidaan kerätä tietoa alaan perehtyneiltä asiantuntijoilta ja saada heidän näkemys esiin (Kananen 2013, 76). Teemahaastatteluista voidaan kerätä tietoja, jota ei olisi saatavilla kirjallisuudesta.

5.1 Henkilötietojen ja haastatteluaineiston käsittely

Asiantuntijat valittiin teemahaastatteluun työnkuvan, työkokemuksen tai aseman perusteella. Asiantuntijat pyydettiin laadullisen tutkimuksen teemahaastatteluun sähköpostitse. Teemahaastatteluun lupautui kuusi asiantuntijaa, joista kolme oli organisaation sisältä ja kolme organisaation ulkopuolelta.

Teemahaastattelujen aineiston keruu sisälsi henkilötietojen käsittelyä. Tietosuoja-asetuksen vaatimusten ja korkeakoulun tieteellisten tutkimusten ohjeiden noudattamiseksi teemahaastatteluun osallistuville annettiin informointi henkilötietojen käsittelystä ja heiltä pyydettiin suostumus käsitellä henkilötietoja tutkimuksen ajan. Suostumuksen perusteella haastattelutilaisuudet nauhoitettiin ja litteroitiin alustavasti Teams-sovelluksessa. Haastateltavan käytettävissä olevan ajan mukaan haastattelukierroksia järjestettiin yhdestä kolmeen kertaan. Haastatteluaineistoa kertyi yhteensä 8 h 10 min.

Aineisto litteroitiin karkealla tasolla ja anonymisoitiin. Aineisto koodattiin ja luokiteltiin analysointia varten. Luokiteltu aineisto tiivistettiin tyypittelyn avulla ja vietiin taulukkomuotoon. Tyypittelyn avulla aineistosta saatiin muodostettua kokonaisuus ja kyettiin muodostaa käsitys tutkittavasta ilmiöstä. Aineisto tallennettiin Tampereen ammattikorkeakoulun ohjeistuksen mukaisesti tutkimusaineiston käsittelystä vastaavan tutkijan henkilökohtaiselle tietokoneelle, josta henkilötiedot hävitettiin tutkimuksen päätyttyä.

5.2 Teemahaastattelun tulokset

Teemahaastatteluissa riskienhallinnan, raportoinnin ja mittaamisen teemojen avulla lähestyttiin tutkittavaa ilmiötä. Teemahaastattelun tutkimuskysymykset esitetään liitteessä 1.

Riskienhallinta

Riskienhallinnan teemassa haastateltavilta kysyttiin miten riskienhallintaan liittyvällä mittaamisella voisi kehittää organisaation toimintaa ja että mitä kehitettävää riskienhallinnassa olisi, jotta riskienhallinta toimisi osana päätöksentekoa (liite 1).

Riskienhallinnan teemasta löydettiin hyödyllisiä kehityskohteita. Teemahaastattelun aineistosta tunnistettiin, että johdon tarve on saada ajantasaisista tietoa riskeistä ja että johdolle tulisi esittää riskien merkittävyyttä ja laajuutta päätöksenteon tueksi. Riskienhallintaa kehittämällä ennakoitavuus päätöksenteossa kehittyy.

Teemahaastatteluissa tuotiin esille, että ajantasaiselle riskien käsittelylle ja muutosten arvioinnille on tarve organisaation toiminnan kehittämisessä ja liiketoiminnan jatkuvuuden varmistamisessa. Ilmeni, että tarve lisäresursoinnista tulisi perustella tulevien muutosten pohjalta, eikä menneisiin tapahtumiin tai resurssitarpeisiin perustuen.

Vastaajien keskuudessa nähtiin tarpeelliseksi kehittää riskienhallintaa riskiperusteisesti, jolloin perustelut lisäresursoinnista nojautuisivat tulevaan muutokseen.

Haastateltavat pitivät tärkeänä, että muutokset tunnistetaan hyvissä ajoin ja esitetään mahdolliset vaikutukset palvelun elinkaaren ajan loppukäyttäjälle asti. Huomioimalla muutosten vaikutukset palvelun tai tuotteen elinkaareen ajan, läpinäkyvyys rahoittajille ja loppukäyttäjille lisääntyy. Riskienhallinta nähtiin tärkeäksi tueksi perustella resurssitarpeita organisaation sisällä, rahoittajille ja loppukäyttäjille. Kohdistettaessa resursointi kehityskohteisiin tai merkittävien hallintatoimenpiteiden priorisointiin organisaation toimintaa voidaan kehittää, jolloin myös tuotteiden ja palvelujen laatu paranee.

Aineistosta nousi esiin, että organisaation toimintaa tulee tarkastella riskilähtöisellä ajattelutavalla rekisteröidyn oikeuksiin nähden, ja että riskiarviointia tulee kehittää tietosuojan näkökulmasta. Arvioitaessa liiketoimintaan vaikuttavia riskejä nähdään mahdolliseksi, että rekisteröidyn oikeuksiin ja vapauksiin vaikuttavat riskit voivat jäädä arvioimatta tai tunnistamatta, niillä on realisoituessaan kuitenkin merkittäviä vaikutuksia liiketoiminnan jatkuvuuteen ja imagoon.

Aineistosta ilmeni, että sopimuskumppaneiden valvontaa ja riskienhallintaa tulisi kehittää. Tunnistettiin, että organisaation kyky valvoa sopimusten noudattamista heikkenee sopimuskumppaneiden määrän laajentuessa. Haastatteluissa tuotiin esiin riskienhallinnan kehittämisen näkökulmasta, että organisaatiolla tulisi olla näkyvyys sopimuskumppaneiden ja palveluntuottajien käytöntöihin noudattaa sopimusten sisältöjä.

Vastaajien keskuudessa tuotiin esiin riskienhallinnan haasteet päivittäisessä työskentelyssä, johon voi olla vaikea saada näkyvyys suuressa organisaatiossa. Päivittäisessä työskentelyssä voi tapahtua riskejä, joita on vaikea havaita isossa mittakaavassa ja joiden pienistä haitoista voi muodostua tarpeettomia organisaation toimintaan vaikuttavia suuria riskejä. Haastatteluissa tuotiin esiin organisaation sisäisten ohjeiden ja linjausten noudattamisen tärkeys päivittäisessä työskentelyssä. Niiden mukaisesti toimittaessa voidaan välttää niin sanottuja tarpeettomia riskejä. Niitä voi syntyä, jos henkilöstö ei tunnista tai jättää noudattamatta organisaation sisäisiä ohjeita. Haastateltavat korostivat jokaisen vastuuta perehtyä sisäisiin tietosuojaan liittyviin ohjeisiin ja toimia niiden mukaisesti. Lisäämällä tietosuojan näkyvyyttä jokapäiväisessä työskentelyssä ja muistuttamalla toimintatavoista ja ohjeista riskien realisoituminen vähentyy.

Riskienhallinta tulisi viedä osaksi kaikkia organisaation toimia. Haastatteluissa tuotiin esiin, että raportoitaessa riskienhallinnan muutoksista ja vaikutuksista kannattaisi hyödyntää myös data-analyytikkoja erilaisten trendien tunnistamiseksi. Data-analyytikot hallitsevat analysoinnin, havainnoinnin ja ennakoinnin. Tällaista resurssin hyödyntämistä käytetään vähän tietosuojan saralla päinvastoin kuin finanssialalla. Haastatteluissa suositeltiin myös raportointia riskienhallinnasta liikennevaloin asiantuntijan kerättyä taustadatan ja tuotua siitä esiin merkittävimmät muutokset. Näin toimittaessa uskottiin myös raportoinnin kehittyvän. Riskienhallinnan teeman aineiston perusteella voidaan esittää, että läpinäkyvällä riskienhallinnalla organisaatio saa toimintaansa vaikuttavista tekijöistä kokonaiskuvan.

Raportointi

Raportoinnin teemassa haastateltavilta kysyttiin mitä kehitettävää olisi raportoinnissa, jotta raportointi toimisi osana päätöksentekoa, ja mitä hyötyä raportoinnista on organisaation johdon edustajille. Lisäksi kysyttiin mitä raportoinnissa tulisi huomioida, jotta raportointi toimisi osana päätöksentekoa (liite 1).

Raportoinnin teemasta nousi esiin käytännön kohteita organisaation raportointimenettelyjen kehittämiseksi. Seuraavan jakson kehityskohteista tai ongelmista tulisi raportoida ennakoidusti. Ennustettavuuden avulla voidaan tuoda esiin resursointitarpeita, ja että liiketoimintaan vaikuttavat riskit tulisi tunnistaa ennakoivasti. Raportointia tulisi kehittää esimerkiksi hyödyntämällä tekoälyn puolueetonta analysointia trendeistä. Haastatteluissa ilmeni, että työskentelyä sujuvoitetaan, kun hyödynnetään kerättyä tietoa eri raportointitapoihin ja -sykleihin.

Raportointia tulisi kehittää ulkoisten tekijöiden muutosten ja tilannekuvan esittämiseen, joka nähtiin tärkeänä resursoinnin kannalta. Organisaation toimintaan vaikuttavat lainsäädännön muutokset tai EU-komission ohjeistukset voivat vaikuttaa resurssitarpeisiin, jotta uusia toiminnallisuuksia saadaan toteutettua määräajassa. Lainmuutoksen toteuttamisesta voi nousta uusia tehtäviä, joista tulisi raportoida aiemmin kuin vuotuisen raportoinnin yhteydessä.

Tuloksissa tuotiin esiin havainnoinnin ja raportoinnin yhteydessä annettavan yhteenvedon merkitystä. Raportoitaessa tunnuslukujen tai lukumäärien nousua, tilasto ei välttämättä kerro organisaation toiminnassa huonontuneesta laadusta. Muutoksia sisäisissä prosesseissa voi tapahtua, kun henkilöstö sisäistää paremmin ohjeita paremmin. Raportoitaessa tunnuslukuja niitä tulee tarkastella eri näkökulmista.

Myös haastateltavat suosittelivat raportointia toteutettavaksi liikennevaloin tai tilannekuvana. Liikennevalot toimivat tiiviinä ja selkeänä esitysmuotona ja tilannekuva lisää ymmärrystä raportoivasta kohteesta.

Muutokset ja havaitut riskit tulee nostaa myös tietosuojan raportoinnissa esiin. Johdon tulee ymmärtää, että tietosuojaan liittyvät riskit ovat aina uhka imagolle. Tavoitteiden saavuttamista tulee seurata tekemisen kautta yhtä lailla kuin budjetin kautta ja niitä tulee seurata eri näkökulmista. Budjetista raportoimisen tulee olla läpinäkyvää. Konkreettisten vaikutusten esiin tuominen lisää johdon ja rahoittajien käsitystä kokonaisuudesta.

Haastateltavat pitivät tärkeänä, että johto pystyy raportoimaan ulospäin sidosryhmille, sijoittajille ja asiakkaille. Sen vuoksi on tärkeää prosessoida raportointimenetelmät niin, että tuotetaan raportteja erilaisia tarpeita varten ajantasaisina.

Mittaaminen

Mittaamisen teemassa haastateltavilta kysyttiin miten riskienhallintaan liittyvällä mittaamisella voisi kehittää organisaation toimintaa ja että mitä kehitettävää tietosuojaperiaatteiden mittaamisessa olisi, jotta mittaamisesta saatava tieto toimisi osana päätöksentekoa. Haastateltavilta muun muassa kysyttiin millainen kyky organisaatiolla tulisi olla mitata ja osoittaa noudattavansa tietosuoja-asetusta ja että miten periaatteet voi viedä mitattavalle tasolle (liite 1).

Mittaamisen teemassa haastateltavat toivat esiin kohteita, joista on hyötyä erityisesti raportoinnin kehittämisessä. Haastateltavat viittasivat kuluihin ja kustannuksiin, joita aiheutuu rahoittajille ja asiakkaille. Kerätyn ja mitatun lähdedatan pohjalta kustannuksia voi perustella kokonaiskuvan hahmottamiseksi rahoittajille. Li-

säksi mittaaminen ja raportointi tekee organisaation tekemisestä uskottavaa. Mittaaminen ja raportointi antaa todisteita periaatteiden noudattamisesta organisaatiossa. Mittaaminen ja läpinäkyvä raportointi erottaa organisaatioiden joukosta sellaiset, jotka todella noudattavat periaatteita.

Haastatteluissa tuotiin esiin myös, että toteutumista mittaamalla voi vaikuttaa palvelun ja tuotteen laatuun ja siten myös varsinaiseen toimintaan ja kustannuksiin organisaatiossa. Mittaamalla palvelun ja tuotteen laatua saadaan myös kustannusvaikutukset esiin.

Keräämällä dataa ja mittaamalla suoritetta saadaan yksinkertaisin signaali johdolle joko resurssien riittävyydestä tai uhkien muodostumisesta riskeiksi. Haastateltavien keskuudessa paljon toivottu ajantasainen ennakoiva raportointi onnistuu mittaamalla tietoa ja esittämällä lisäresurssien tai riskien vaikutuksia kustannuksiin. Kun tunnistetaan trendi, päätöksenteko kohdentuu tulevaan muutokseen ja tällöin resursointi on oikeasuuntaista. Katsottiin, että muutostrendin mittaaminen on merkityksellisempää kuin jo tapahtuneen raportointi.

Haastatteluissa arvioitiin, miten periaatetasoa voidaan mitata. Tietosuojaperiaatteiden toteutumisen seuraamista voidaan edistää, kun asetetaan jokaiselle periaatteelle oma mittari ja kun niitä kehitetään jatkuvasti organisaation toimintaan sopivaksi. Tietosuojastandardi avaa periaatteiden vaatimukset käytännön tasolle, jolloin standardin vaatimuksia noudatettaessa organisaatio voi varmistua noudattavansa periaatteiden toteuttamista. Haastatteluissa suositeltiin hyödynnettäväksi tietosuojastandardia, koska se esittää vaatimukset konkreettisella tasolla.

Eräs haastateltava tähdensi, että osa tietosuoja-asetuksen tietosuojaperiaatteista on jo konkreettisella tasolla kuten henkilötietojen minimoinnin periaate. Muutoin tietosuojaperiaatteet tunnistettiin väljiksi, joiden konkretisointi tunnistettiin haasteelliseksi.

Tietosuojastandardin tietotosuojan hallintajärjestelmä vuorostaan tunnistettiin konkreettisemmaksi työvälineeksi arvioimaan tietosuojaperiaatteiden toteutu-

mista, sillä standardi itsessään esittää vaatimuksia, jotka ovat konkreettisella tasolla. Kun vaatimukset ovat konkreettisella tasolla, niiden toteutuminen on mitattavissa ja arvioitavissa.

Jotta voidaan mitata periaatteen toteutumista, on kullekin periaatteelle määriteltävä vaatimukset eli määriteltävä mitä mikin periaate tarkoittaa käytännössä. Näin toimittaessa voidaan seurata ja mitata yksittäisen projektin suoriutumista esimerkiksi kontrolli- tai tarkistuslistojen avulla. Periaatteen käsite tulee siis avata ja tehdä siitä konkreettinen. Tällöin käytännössä voidaan seurata toteutusta.

Kun käytännön toteutusta seurataan, raportille voidaan tuottaa tietoa esimerkiksi liikennevaloin volyymeista ja lisätä näkyvyyttä tietosuojaperiaatteiden toteutumisesta. Samassa yhteydessä saadaan kerättyä tietoa periaatteiden toteutumisesta yksittäisissä projekteissa.

Sisäisillä prosesseilla saadaan varmistettua, että projekti on varmuudella noudattanut periaatteita ja määriteltyjä vaatimuksia. Eli toisin sanoen yksittäisen projektin valvonta osoittaa projektin noudattavan vaatimuksia käytännössä. Esimerkiksi tarkistuslistan avulla saadaan todenmukaista raportointia projektin vaatimusten noudattamisesta.

Vain kohdentamalla mittaaminen varsinaiseen toteutukseen saadaan todisteita organisaation sisäisten toimintojen vaatimusten noudattamisesta. Ellei todenneta organisaation kykyä noudattaa periaatteita toiminnassaan, on suhtautuminen siihen kriittistä. Jotta organisaatio voi lisätä uskottavuuttaan, tulee mitata varsinaista toteutusta.

Periaatteiden toteutumisen mittaamiseen on muitakin keinoja. Kun kartoitetaan organisaation nykytilaa tekemällä kyselytutkimuksia kehittäjien ja henkilöstön parissa, saadaan kartutettua ymmärrystä organisaation nykytilasta henkilöstön kokemuksen kautta. On johdonmukaista selvittää henkilöstön kokemuksia periaatteiden toteuttamisesta omassa työtehtävässä tai projektissa tietosuojatietoisuuden tunnistamiseksi. Haastatteluissa todettiin, että kun periaatteet kuuluvat osana jokapäiväiseen työskentelyyn se lisää organisaation uskottavuutta.

5.3 Teoria-aineiston keskeiset löydökset

Teoreettisen aineiston avulla tunnistettiin hyötyjä ISO/IEC27701 -standardin käyttöönotosta ja tunnistettiin menettelyjä lähestyä epäselvää ilmiötä määrittelyn ja operationalisoinnin keinoin. Määrittelyn ja operationalisoinnin kautta epäselvä ilmiö tai asia voidaan muuntaa konkreettiseksi. Tunnistettiin myös mittareita tietosuojavaatimusten toteutumisen mittaamiseksi eri sidosryhmien toimesta. Lisäksi löydettiin mittareita, joita hyödyntämällä tietosuojavaatimusten noudattamista eri puolilla organisaation toimintaa voidaan konkretisoida ja kerätä todisteita osoitusvelvollisuuden toteuttamisesta. Läpikäydystä lähdemateriaalista ei käynyt ilmi keinoa periaatetason toteutumisen mittaamiseen.

Teoria-aineistossa on esitelty tietosuojan vaikutustenarviointi, joka on henkilötietojen käsittelystä aiheutuvien uhkien ja riskien hallinnassa keskeinen työväline. Sillä arvioidaan tapauskohtaisesti käsittelytoimen vaikutukset rekisteröidyn oikeuksiin ja vapauksiin nähden. Tunnistettuja uhkia ja niistä aiheutuvia riskejä vähennetään hallintatoimenpitein. Tietosuojan vaikutustenarvioinnilla tunnistettujen uhkien ja riskiarviointien käsittely saattaa kuitenkin jäädä irralliseksi muusta organisaation riskienhallinnasta.

Tietosuojan vaikutustenarvioinnilla arvioitujen uhkien ja riskien läpinäkyvyyttä on suositeltavaa kehittää viemällä arvioitujen riskien ja niiden hallintatoimenpiteiden seuranta osaksi organisaation muuta riskienhallintajärjestelmää. Tietosuoja-asetuksen riskilähtöinen ajattelutapa rekisteröidyn oikeuksien toteutumisesta eroaa muista hallittavien riskien näkökulmista. Henkilötietojen käsittelyyn, tietoturvaan ja liiketoimintaan vaikuttavien riskien hallinta on tarpeen lähentää keskenään, jotta voidaan saada kokonaiskuva organisaation tilasta.

Teoreettisen aineiston merkittävä löydös on ISO/IEC27701 -standardi ja sen edellyttämä tietosuojan hallintajärjestelmän käyttöönotto. Tietosuojan hallintajärjestelmä ohjaa organisaation toimintaa, ja koska hallintajärjestelmä edellyttää seurantaa, mittaamista ja jatkuvaa arviointia, tietosuojavaatimusten toteuttamisen mittaaminen kehittyy standardin käyttöönoton myötä. Standardin suunnittelu organisaation toimintaan sopivaksi ja käyttöönotto lisää kustannuksia hetkelli-

sesti, ja lisäksi hallintajärjestelmän jalkauttaminen kuluttaa resursseja, mutta tietosuojan hallintajärjestelmä itsessään tuo ratkaisun tietosuojaperiaatteiden ja vaatimusten toteuttamiseen ja mittaamiseen.

Kun valitaan menetelmiä raportoinnin kehittämiseksi, on hyvä harkita myös tasapainotetun tuloskortin käyttöönottoa. Organisaation strategisten tavoitteiden saavuttamista arvioidaan muun muassa taloudellisesta näkökulmasta, jolloin kustannusvaikutuksia ja tehokkuutta voidaan mitata tasapainotetulla tuloskortilla. Sekä tietosuojavaatimusten että tietosuojaperiaatteiden toteuttamista tulee arvioida kustannusvaikutuksena, jolloin tietosuojasäännöstelyn toteutumista ja henkilötietojen tietoturvapoikkeamien aiheuttamia kuluja samoin kuin asiakkaiden luottamusta ja kustannushyötysuhdetta tulisi arvioida ja mitata tuloskortin näkökulmasta johdon ja sidosryhmien kanssa. Tasapainotetun tuloskortin käyttö on tosin vaikeaa ilman, että organisaatiossa käynnistetään kerätä tietoja tietosuojavaatimusten toteutumisesta eri sidosryhmittäin.

Merkittävä löydös teoreettisesta aineistosta on Tene & Culnan:in esittämät taulukot (taulukko 1–2), joiden avulla määritellään sidosryhmien vastuualueet tietosuojavaatimusten toteutumisen mittaamiseksi. Mukaillen Tene & Culnan:in esittämien sidosryhmien vastuualueita sekä mittaamisen ja raportoinnin kohteita, organisaation kyky kerätä todisteita tietosuojavaatimusten ja myöhemmässä vaiheessa tietosuojaperiaatteiden toteutumisesta kehittyy merkittävästi. Mukaillen Tene & Culnan -menetelmää, tunnistetaan mittaamisen kohteet ja saadaan todisteita tietosuojavaatimusten toteuttamisesta organisaation toiminnassa.

Jos organisaatio ei havittele toimintansa luottamuksen ja uskottavuuden todentamiseksi sertifikaattia tai ISO/IEC27701 -standardin käyttöönotto ei hyödytä organisaatiota henkilöstö- ja liiketoiminnan koon takia, mittaamista ja raportointia voi kehittää kustannustehokkaasti mukaillen Tene & Culnan -menetelmää. Yhtä lailla tietosuojan vaikutustenarviointi -työvälineen kehittäminen on kustannustehokas tapa kerätä tietoa tietosuojaperiaatteiden toteutumisesta riskienhallinnan näkökulmasta.

Sopivan mittaus- tai raportointitavan löytämiseksi on tärkeää vertailla eri menetelmiä. ESG-raportointi ja tietotilinpäätös ovat jälkikäteen tapahtuvaa raportointia.

Nämä raportointimenetelmät eivät sovi kehittämään ajantasaista raportointia toiminnan muutoksista ja niiden vaikutuksista. ESG-raportointi kuitenkin tuo rakenteen, jossa tiedon keruu ja mittaaminen on osa päivittäistä toimintaa. ESG-raportointi on laaja raportointimenetelmä, joka edellyttää mittaamisen olevan osa organisaation kaikkia rakenteita.

ESG-raportointi on kasvava trendi, sitä pyytävät sekä rahoittajat että loppukäyttäjät. ESG-raportointi lisää läpinäkyvyyttä rahoittajille ja loppukäyttäjille asti ja vahvistaa organisaation toiminnan uskottavuutta. ESG-raportointi voi olla työläs jalkauttaa osaksi kaikkia organisaation toiminnan alueita, mistä syystä raportointimalli usein otetaan käyttöön vaiheittain.

5.4 Teemahaastattelun keskeiset löydökset

Riskienhallinnan teemasta merkittävin löydös on, että riskienhallinnan menetelmiä käyttäen johdon ymmärrys organisaation toiminnasta vahvistuu, toiminnan hallinta ja sen ohjaus kehittyvät, ennakoiminen helpottuu ja läpinäkyvyys lisääntyy. Kehittämällä riskienhallintaa kehittyy uhkien tunnistaminen ja riskien hallintatoimenpiteiden laadinta, ennakointi muutoksista kehittyy ja tavoitteiden saavuttaminen paranee. Kun henkilöstö on vahvemmin mukana riskienhallinnassa, se kehittyy tunnistamaan uhkia, laatimaan hallintatoimenpiteitä ja raportoimaan oikeaaikaisesti muutoksista. Ajantasainen riskienhallinta tukee johtamista ja päätöksentekoa.

ISO/IEC27701-tietosuojastandardin käyttöönotto on merkittävä lisä organisaation tietosuojan kehittämiseksi. Sertifiointi vahvistaa organisaation luotettavuutta. Standardin käyttöönottoon liittyy puuteanalyysin laadinta, minkä tuloksen perusteella määritellään organisaation kypsyystaso. Tunnistetuille kehityskohteille ja puutteille laaditaan suunnitelma, mikä sujuvoittaa auditointiin siirtymistä. Kypsyystason arviointi luo hyvät edellytykset mittaamisen käynnistämiselle ja siten toiminnan kehittymisen seurannalle. Tietosuojastandardi edellyttää tietosuojan hallintajärjestelmän laatimista. Vaatimus on seurata, mitata ja raportoida. Vaatimuksen täyttäminen tukee mittaamisen käynnistämistä sisäisissä toiminnoissa eli raportoinnin kehittämistä.

Raportoinnin teemasta merkittävimpinä löydöksenä tunnistettiin tarve lisätä ennustettavuutta, lisätä johdon ymmärrystä kokonaistilasta ja lisätä läpinäkyvyyttä. Läpinäkyvyyden lisääminen rahoittajille ja loppukäyttäjille tunnistettiin tarpeelliseksi.

Jos organisaation raportointi on heikkoa ja jälkikäteen tapahtuvaa, saa organisaation sisäinen ja ulospäin suuntautuva raportointi ryhtiliikkeen, kun hyödynnetään vastuullisuusraportoinnin kehikkoa. Vastuullisuusraportointi sisältää tiedon keruun riskienhallinnasta ja tietosuojasta. Näitä tietoja voi hyödyntää selvittäessä muitakin raportoitavia kohteita esimerkiksi rekisteröidyn oikeuksia. Oikea-aikainen raportointi edellyttää useilta organisaation toiminta-alueilta ymmärrystä ja sisäistämistä raportoinnin merkityksestä. Jos raportointi jää irralliseksi, käyttämättömäksi elementiksi organisaatiossa, se ei luo lisäarvoa organisaatiolle eikä vahvista uskottavuutta organisaation toiminnasta.

Erityistä huomiota tulisi kiinnittää organisaation kykyyn raportoida rahoittajille, jotka tekevät valintoja sijoituskohteista. Myös loppukäyttäjien kokemusta organisaation luotettavuudesta ja uskottavuudesta tulee vahvistaa. Heidän tarpeisiinsa vastaaminen tulee huomioida, sillä loppukäyttäjät hyödyntävät palveluja ja edellyttävät vastuullisen toiminnan osoittamista. ESG-raportoinnin hyödyntäminen kehittää läpinäkyvyyttä, vahvistaa uskottavuutta ja sujuvoittaa kustannusvaikutusten hahmottamista organisaation eri toiminta-alueilla.

Mittaamisen teemassa keskeisin löydös on, että periaate määritellään ja viedään käytännön tasolle projekteihin. Mittaaminen tulee viedä osaksi projektin tehtäviä. Tällöin periaatteiden noudattamisesta voidaan kerätä todisteita. Henkilöstön osaamista ei tule sivuuttaa ja siksi tulee tutkia miten henkilöstö noudattaa periaatteita työssään. Määrittelemällä mitä periaatteet tarkoittavat kullakin toiminta-alueella, tiedon kerääminen ja mittaaminen on mahdollista. Mittareiden merkitys ei ole esittää pelkästään kustannusvaikutuksia. Organisaatio voi todentaa noudattavansa periaatteita mittaamalla ja raportoimalla siitä.

5.5 Kehittämissuunnitelma

Tässä kehittämissuunnitelmassa esitetään eri vaihtoehtoja tietosuojaperiaatteiden toteutumisen mittaamiseksi. Näistä vaihtoehdoista toimeksiantaja voi valita organisaatiolleen tai yksikölleen sopivan välineen tai menetelmän mittaamisen ja raportoinnin kehittämiseksi.

5.5.1 Aineettoman pääoman mittaaminen

Mitattaessa aineetonta pääomaa mittaaminen tulee kohdentaa henkilöstön osaamiseen. Mitatessa henkilöstön osaamista voidaan selvittää henkilöstön kokemusta toteuttaa tietosuojaperiaatteita osana arkista työtä tai projekteja. Seuraamalla ja mittaamalla henkilöstön osaamista voidaan tunnistaa tarpeet kohdennetulle koulutukselle tai ohjeistukselle. Henkilöstön suorituskykyä arvioidaan esimerkiksi suorituskykyarviointien, kehityskeskusteluiden tai kyselyjen avulla. Aineetonta pääomaa mitataan laajemmin tasapainotetulla tuloskortilla.

5.5.2 Tietosuojan vaikutustenarviointi

Tietosuojan vaikutustenarvioinnin tavoite on saavuttaa tila, jossa varmistutaan, että käsittelytoimi noudattaa ja toteuttaa tietosuojaperiaatteita sekä rekisteröidyn oikeuksia ja vapauksia. Tietosuojan vaikutustenarvioinnin sisällöstä arvioidaan tietosuojaperiaatteiden toteutumista.

Tietosuojan vaikutustenarvioinnin yhteydessä voidaan kerätä tietoja tietosuojaperiaatteiden toteutumisesta, joka esitetään taulukossa 3. Vaikutustenarvioinnin riskitaulukkoa voidaan muokata lisäämällä siihen sarakkeen, jossa havaittu riski määritellään yhteen kuudesta tietosuojaperiaatteista.

Tehtävä edellyttää jonkin verran manuaalista työtä, koska havaittu riski ja sille määritelty tietosuojaperiaate tulee siirtää arvioinnin jälkeen organisaation riskienhallintajärjestelmään. Näin saavutetaan kokonaiskuvan hallinta ja nähdään tarkemmin mitkä riskit vaikuttavat tietosuojaperiaatteiden toteutumiseen, kyetään

priorisoimaan ja hallitsemaan korjaavia toimenpiteitä kokonaisuutena ja tunnistamaan aukkoja tai puutteita tietosuojaperiaatteiden toteuttamisessa.

TAULUKKO 3. Tietosuojan vaikutustenarvioinnin riskiarviointitaulukkoon on lisätty sarake Tietosuojaperiaate luokittelulla 1–6. Mukaillen tietosuojavaltuutetun toimiston julkaisua (Tietosuojavaltuutetun toimisto n.d.)

Uhan kuvaus	Uhan vaikutukset	Vakavuus	Todennäköisyys	Riskiluku	Suojatoimenpide	Uusi vakavuus	Uusi todennäköisyys	Uusi riskiluku	Tietosuojaperiaate
Esimerkki 1									1
Esimerkki 2									2
Esimerkki 3									3
Esimerkki 4									4
Esimerkki 5									5
Esimerkki 6									6
Esimerkki 7									
Esimerkki 8									

Viemällä tietosuojan vaikutustenarvioinnilla havaitut korkeat riskit ja tietosuojaperiaatteet osaksi organisaation riskienhallintajärjestelmää, organisaation kyky viestiä muutoksista ja vaikutuksista kehittyy. Tällöin raportointi ei ole irrallista muusta organisaation raportoinnista ja saavutetaan läpinäkyvyyttä.

5.5.3 Tietosuojan hallintajärjestelmä

Tietosuojastandardin tietosuojan hallintajärjestelmä sisältää ohjeet tietosuojaperiaatteiden noudattamiseen. Standardissa on avattu tietosuoja-asetuksen periaatteet ja vaatimukset käytännön tasolla. Tietosuojan hallintajärjestelmä ohjaa toimintaa ja se on työväline, jonka avulla organisaatio kehittää tietosuojalainsäädännön mukaisuutta koko organisaation tasolla ja jalkauttaa vaatimukset organisaatioon.

Tietosuojastandardin tietosuojahallintajärjestelmän käyttöönottoon voi sisällyttää puuteanalyysin, jonka avulla arvioidaan ja tunnistetaan kehityskohteita tai puutteita organisaation toiminnoissa. Puuteanalyysin perusteella laaditaan alustava

toimenpidesuunnitelma puutteiden korjaamiseksi ja sen avulla voidaan seurata ja mitata kehitystä.

Tietosuoja hallintajärjestelmä edellyttää, että organisaatio mittaa, seuraa ja raportoi tietosuojavaatimusten toteuttamista. Organisaatio laatii alustavat mittarit vaatimusten toteuttamisesta. Mittaaminen kohdistetaan usein jo olemassa olevien prosessien läpimenoon ja suorituskykyyn, joita ovat esimerkiksi rekisteröidyn oikeuksien ja vapauksien toteuttaminen määräajassa, henkilötietojen tietoturvaloukkausten lukumäärä ja vakavuusluokka tai tietosuojan vaikutustenarvioinnin suorituskyky, läpimenoaika ja volyymi. Tietosuojahallintajärjestelmän kehittyessä ja laajentuessa organisaatiossa voidaan ottaa käyttöön lisää mittareita.

Tietosuojastandardin käyttöönotto tukee parhaiten toiminta-alueeltaan laajan ja henkilöstömäärältään suurikokoisen julkishallinnon organisaation lainmukaista toimintaa. Standardi kehittää koko organisaation turvallisuuden tilaa, sisäänrakennetun ja oletusarvoisen tietosuojan noudattamista, ja tukee mittaamista ja raportointia.

5.5.4 Tietosuojavaatimusten mittarit

Perinteisimpien kohteiden, joita ovat rekisteröidyn oikeuksiin liittyvät prosessit, läpimenoajat ja suorituskyky, lisäksi on suositeltavaa laajentaa mittaamiskohteiden määrää. Tietosuojavaatimusten mittaaminen tulee nähdä osana laajempaa kokonaisuutta, jossa mittaaminen viedään osaksi ylimmän ja keskijohdon toimintoja, liiketoimintaa ja henkilöstöä sekä sisäistä tarkastusta ja riskienhallintaa. Lisäksi on tärkeää, että mittarien käyttö sisällytetään osaksi projektityöskentelyä.

Aiemmin esitetyssä mukaelmassa Tene & Culnan:in esittämästä taulukosta (taulukko 1–2) on hyödynnettäviä osa-alueita mittaamisen kohteiden suunnitteluun. Taulukossa 1 on esitetty sidosryhmille mittarit ja raportoinnin tarkoitukset. Kun sidosryhmä kerää tietoja tietosuojavaatimusten toteuttamisesta esimerkiksi kuukausittaisten raporttien laatiminen sujuvoituu. Taulukon 2 esittämät tehtävät liike-

toiminnan, tietosuojatiimin, henkilöstön ja riskienhallinnan alueilla kehittävät mittaamista ja raportointia. Ehdotettujen sidosryhmien kerätessä tietoja tietosuojavaatimuksista tuotetaan ajantasaista tietoa johdolle (kuvio 1).

Tietosuojavaatimusten mittaamisen käynnistäminen edellyttää jokaiselta sidosryhmältä arvioinnin siitä mitä tietoja sidosryhmän tulee tuottaa. Tietosuojavaatimusten mittaamisen toimiessa osana organisaation kaikkia toimintoja saavutetaan parempi näkyvyys organisaation tilasta.

Tietosuojaperiaatteiden toteutuksen tulee toimia osana kaikkea työskentelyä, jotta sisäänrakennetun ja oletusarvoisen tietosuojan vaatimusta noudatetaan. Henkilöstölle suunnatuilla kyselyillä selvitetään tietosuojaperiaatteiden toteutumista. On tähdellistä kerätä tietoa henkilöstön kokemuksesta siitä miten tietosuojaperiaatteita noudatetaan arkisessa työssä. Lisäksi henkilöstön osaamisen kartoitus tietosuojaperiaatteiden toteuttamisesta antaa tietoa liiketoimintaan vaikuttavista riskeistä, tai palvelun tai tuotteen laatuun vaikuttavista tekijöistä.

Myös on tärkeää seurata ulkoisten kumppaneiden tietosuojavaatimusten toteuttamista, jotta organisaatio voi varmistua tietosuojavaatimusten ja käytänteiden noudattamisesta sopimuskauden ajan. Sopimusten seuranta tulee viedä osaksi sopimustenhallintaa. Organisaatio on vastuussa henkilötietojen käsittelijöistä ja alihankkijoista näiden käsitellessä henkilötietoja rekisterinpitäjän lukuun annettujen ohjeiden mukaisesti.

Organisaation seuratessa ulkoisten kumppaneiden tai henkilötietojen käsittelijöiden toimia aktiivisesti organisaatio osoittaa tietosuojaperiaatteiden ja sopimuskäytänteiden noudattamisen vakavuuden kaikissa käsittelytoimen vaiheissa koko sopimuskauden ajan. Organisaatio voi seurata sopimuskumppaneiden noudattavan tietosuojaperiaatteita pyytämällä näitä esittämään hyväksytysti laaditun tietosuojan vaikutustenarvioinnin. Aktiivista seurantaa voi tehdä pistokokein, kyselyinä tai tarkastustoimilla.

KUVIO 1. Kuvio esittää sidosryhmät tietosuojavaatimusten mittaamiseksi

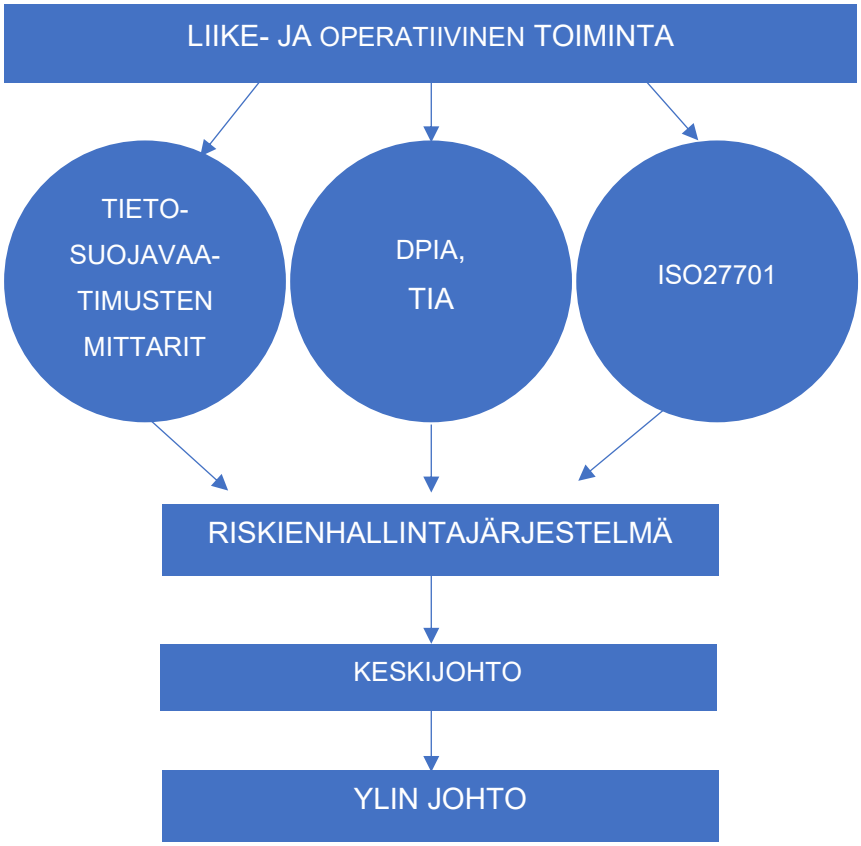
5.5.5 Raportointi

Käynnistämällä mittaaminen sidosryhmittäin kehitetään raportointia organisaation toiminnoista. Liike- ja operatiivisen toiminnan tulee mitata suorituskykyä, jotta ne voivat varmistua asetettujen tavoitteiden saavuttamisesta tietosuojan hallintajärjestelmän, tietosuojalainsäädännön, määräysten tai linjausten parissa. Tunnuslukujen esittäminen häiriöhallinnasta ja SLA-laskennasta edistää organisaation kokonaiskuvan riskienhallintaa. Henkilöstön tietosuojatietoisuuden lisääminen ja koulutus on osa osoitusvelvollisuuden varmistamista.

Tietosuojatiimi tai tietosuojavastaava arvioi tietosuojan vaikutustenarvioinnista tunnistettujen korkeiden riskien ja hallintatoimenpiteiden vaikutuksia käsittelytoimen lainmukaisuuteen ja tarvittaessa esittää suosituksen käsittelytoimen siirrosta

tietosuojavaltuutetun ennakkokuulemista varten. Tietosuojan vaikutustenarviointien yhteydessä tietosuojatiimi arvioi tietosuojaperiaatteisiin kohdistuvat riskit ja vie havainnot riskienhallintajärjestelmään. Tietosuojatiimi seuraa vaatimustenmukaisuuden toteutumista organisaatiossa ja siirtää kaikki havaitut puutteet tietosuojaperiaatteiden ja tietosuojavaatimusten noudattamisessa, rekisteröidyn oikeuksien toteuttamisessa tai tietoisuuden lisäämisessä riskienhallintajärjestelmään organisaation kokonaiskuvan ylläpitämiseksi.

Riskienhallinnan raportointia kehitetään tuottamalla riskienhallintajärjestelmä, jonka avulla tunnistetaan organisaation tuotteiden tai palvelujen toimintaan vaikuttavat riskit, niiden vaikuttavuus ja merkittävyys. Kuviossa 2 esitetään liike- ja operatiiviselle toiminnalle kohteet, joista kerätä tietoja riskienhallintajärjestelmään.



KUVIO 2. Kuvio esittää rakenteen liike- ja operatiiviselle toiminnalle tietojen keräämiseksi riskienhallintajärjestelmää ja raportointia varten keskijohdolle ja ylimmälle johdolle

Riskienhallintajärjestelmään viedään kaikki havainnot toimintaan vaikuttavista riskeistä mukaan lukien tietosuojan vaikutustenarvioinnilla, tietosuojavaatimusten mittareilla ja tietosuojan hallintajärjestelmän käytössä havaitut rekisteröidyn oikeuksien ja vapauksien toteuttamiseen vaikuttavat riskit.

Liike- ja operatiivisten toimintojen kerätessä tietoja riskienhallintajärjestelmään organisaatio tunnistaa riskien vaikutuksia tehokkaammin. Kerätessä tiedot riskienhallintajärjestelmään tunnistetaan riskejä, jotka voivat vaikuttaa liike- ja operatiivisiin toimintoihin. Hallintatoimenpiteiden avulla vähennetään ja estetään riskejä tapahtumasta ja saavutetaan näkyvyys riskien hallintatoimenpiteiden toteuttamisesta. Riskienhallintajärjestelmän avulla riskien seuranta on tehokasta ja läpinäkyvää riskienhallinnan asiantuntijoiden kesken. Riskienhallintajärjestelmän avulla merkittävät ja vakavat riskit raportoidaan keskijohdolle ja ylimmälle johdolle.

Ulkoisten kumppaneiden sopimuskäytänteiden ja lainmukaisuuden noudattamista tulee raportoida. Sopimuskäytänteiden ja lainmukaisuuden seuranta ja raportointi ovat tärkeitä, koska seurannan avulla voidaan varmistua kumppanin noudattavan tietosuojavaatimuksia, yleisiä käytänteitä ja lainmukaisuutta käsiteltäessä henkilötietoja. Seurannan ja raportoinnin avulla varmistutaan liiketoimien turvallisuudesta ja vähennetään riskien muodostumista liiketoiminnalle. Taulukossa 1 esitetään, että ulkoisen kumppanin esittäessä hyväksytty tietosuojan vaikutustenarviointi vahvistetaan luottamusta ja läpinäkyvyyttä tilaajan ja toimittajan välillä. Sopimuskäytänteiden seurantaa voi tehdä esimerkiksi pistokokein ja tuloksista raportoidaan keskijohdolle ja ylimmälle johdolle.

6 POHDINTA

Periaatetason mittaamisesta on hyötyä organisaation toiminnan kehittämisessä ja sillä varmistetaan tietosuoja-asetuksen tietosuojaperiaatteiden toteutuminen. Periaatteiden ja minkä tahansa organisaation sisäisen toiminnon mittaaminen, seuranta ja arviointi tarkentaa käsitystä kokonaisuudesta. Tässä opinnäytetyössä on esitetty tietosuojavaatimusten mittaamista eri sidosryhmissä, mikä tuo oletusarvoisen ja sisäänrakennetun tietosuojan toteuttamisen ja kokonaiskuvanhallinnan lähemmäksi sidosryhmien edustajia.

Tietosuojavastaavan tehtävä on raportoida organisaation johdolle tietosuojaan liittyvistä asioista, kuten henkilötietojen käsittelystä, riskeistä ja tietosuojaan liittyvistä käytännöistä. Vaatimus korostaa tietosuojavastaavan tärkeää roolia organisaation tietosuoja-asioiden koordinoinnissa, ja että tietosuoja otetaan huomioon kaikilla organisaation tasoilla. Raportointitehtävässä tavoite on varmistua, että organisaation ylimmällä johdolla on ajantasainen tieto tietosuoja-asioista ja mahdollisuus tarvittaessa tehdä päätöksiä tietosuojaan liittyvissä kysymyksissä. Kun sidosryhmät käynnistävät tietosuojavaatimusten mittaamisen, tietosuojavastaava voi varmistua, että tietosuoja on huomioitu kaikilla organisaation tasoilla.

Tietosuoja-asetus ohjaa jokaista organisaatiota riskilähtöiseen ajattelutapaan ja laatimaan suojatoimenpiteet käsittelytoimeen soveltuvaksi. Samoin tulee toimia, kun suunnitellaan tietosuojaperiaatteiden mittaamista ja kun kohdennetaan mittaamisen menetelmiä organisaation toimintaan sopiviksi. Mittaamalla tietosuojaperiaatteita organisaatio kykenee todistamaan osoitusvelvollisuuden toteutumista tarkemmalla tasolla. Mittaaminen kehittää raportointia ja luottamusta rahoittajien ja loppukäyttäjien suuntaan.

Tietosuojaperiaatteiden toteutumisen mittaamiseen tasapainotettu tuloskortti tuottaa tietoa sidosryhmille tietosuojavaatimusten noudattamisesta, ja se tuottaa laajan ja tasapainotetun näkymän säädösten noudattamisen vaikutuksista eri näkökulmista. Tasapainotetun tuloskortin jalostaminen tietosuojavaatimusten mittaamiseen ja johdon ja sidosryhmien käyttöön edellyttää tässä opinnäytetyössä

esitettyjen sidosryhmien ja mittaamisen kohteiden käynnistämistä organisaation sisäisissä toiminnoissa.

Tietosuojaperiaatteiden toteutumisen mittaamisen tueksi Tene & Culnan -menetelmää pidetään tämän opinnäytetyön merkittävänä löydöksenä. Tämän menetelmän avulla perustellaan eri sidosryhmiltä kerättävien tietojen tärkeys. Menetelmä tukee tietosuoja-asetuksen vaatimusten toteuttamista eri sidosryhmissä. On huomioitava, että Tene & Culnan -menetelmä ei välttämättä toimi sellaisenaan vaan sisältöä on muokattava toimeksiantajan toimintoihin sopivaksi. Teemahaastattelujen tulosten huomattavin löydös on, että mitatakseen periaatteita ne tulee määritellä ja viedä käytännön tasolle projekteihin. Vain periaatteiden toteutumista mittaamalla organisaatio voi todentaa noudattavansa niitä.

Opinnäytetyön tavoitteet saavutettiin. Laadullisen tutkimuksen menetelmin on tunnistettu miten periaatetasoa voi mitata. Kehittämissuunnitelmassa on esitetty vaihtoehtoja, joiden käyttöönotolla organisaation toimintaa voidaan kehittää. Vaihtoehdot ovat hyödynnettävissä erikokoisissa organisaatioissa ja toimialoilla, sillä esitettyjä työvälineitä on ilmaisesta maksulliseen. Työpanoksena ilmaisen mallin kehittäminen on vähäistä verrattuna kansainvälisen ISO/IEC-standardin käyttöönottoon, mikä vaatii suurta työpanosta. Tässä opinnäytetyössä esitettyjen tietosuojavaatimusten mittarien hyödyntäminen edellyttää keskisuurta työpanosta.

Ratkaisu tietosuojaperiaatteiden toteutumisen mittaamiseksi on tietosuojan hallintajärjestelmän, tietosuojan vaikutustenarvioinnin tai tietosuojavaatimusten mittaaminen joko sidosryhmittäin tai projektien kautta. Keskeisin löydös raportoinnin kehittämiseksi on ESG-raportoinnin hyödyntäminen raportointirakenteen laatimisessa.

Esitettyjen mittareiden käyttöönotosta on merkittävää hyötyä ajantasaisen raportoinnin kehittämiseksi johdon päätöksenteon tueksi. Esitettyjen menetelmien avulla raportointi tietosuojavaatimusten toteutumisesta viedään osaksi organisaation raportointisykliä, ja siten kehitetään johdon kokonaiskuvaa organisaation tilasta. Kun eri sidosryhmät mittaavat organisaation tietosuojaan liittyviä vaati-

muksia, tietosuojavastaava voi varmistua, että tietosuoja on otettu huomioon kaikilla organisaation tasoilla. Tämä auttaa varmistamaan, että organisaatio noudattaa tietosuoja-asetuksen vaatimuksia ja muita sovellettavia lakeja.

Kustannusvaikutusten selvittämiseksi ja tavoitteiden saavuttamiseksi tasapainotetun tuloskortin hyödyntämistä tietosuoja-asetuksen tietosuojaperiaatteiden ja tietosuojavaatimusten toteuttamisen näkökulmasta voidaan esittää tämän tutkimuksen jatkokehitysaiheeksi.

Arvioidessani opinnäytetyötä ja sen tavoitteiden saavuttamista näen, että olen esittänyt uusia ratkaisuja aiemmin vain vähän tutkitusta aiheesta. Mielestäni olen tutkijana ansiokkaasti saavuttanut kehittämistehtävän tavoitteet.

LÄHTEET

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Helsinki: Tietosanoma Oy.

Asetus 2016/679/EU. EU:n yleinen tietosuoja-asetus. 4.5.2016. Viitattu 4.12.2021. http://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504

CGI. 2023. Building a more sustainable and inclusive world. Environmental, Social and Governance Report. Verkkosivu. Viitattu 13.2.2023. https://www.cgi.com/sites/default/files/2023-02/cgi-2022-esg-report.pdf

Digi- ja väestötietovirasto. 2021. Digiturvallisuuden hallinta. Viitattu 8.1.2022. https://dvv.fi/documents/16079645/0/VHK_Digiturvallisuuden_hallinta_0112_2021.pdf/7f96c738-76ba-f853-b85b-d1596ac54167/VHK_Digiturvallisuuden_hallinta_0112_2021.pdf?t=1638360381233

Eduskunta. 2021. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Julkaistu 3.11.2021. Viitattu 8.1.2022. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx

Ekokompassi. n.d. ESG yritysvastuun veturina – miksi myös pk-yrityksen kannattaa asettaa tavoitteet ja mittarit? Verkkosivu. Viitattu 13.2.2023. https://ekokompassi.fi/esg-yritysvastuun-veturina-miksi-myos-pk-yrityksen-kannattaa-asettaa-tavoitteet-ja-mittarit/

Eskola, J. & Suoranta, J. 2000. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

Eurofins. 2018. GAP-analyysi ja esisertifiointi auttavat ISO 27001 -sertifiointiin valmistautumisessa. 11.1.2018. Verkkosivu. Viitattu 13.2.2023. https://www.eurofins.fi/expertservices/ajankohtaista/uutiset/201801-gap-analyysi-ja-esisertifiointi-iso-27001-sertifioinnissa/

Hirsjärvi, S. & Hurme, H. 2011. Tutkimushaastattelu – teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

Ilkka, H. 2022. Aikaansa seuraavien hallitusten vastuullisuusosaamisen täytyy olla laajaa ja syvällistä. EY Nordics Regional Assurance Managing Partner. 11.4.2022. Verkkosivu. Viitattu 13.2.2023. https://www.ey.com/fi_fi/board-matters/laaja-ja-syvallinen-vastuullisuusosaaminen-tarpeen-hallituksissa

International Organization for Standardization. n.d. Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines. Verkkosivu. Viitattu 19.3.2022. https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

International Organization for Standardization. n.d. ISO/IEC 27001:2005 Information technology - Security techniques - Information security management

systems - Requirements. Verkkosivu. Viitattu 5.12.2022. https://www.iso.org/standard/42103.html

IT Governance. n.d. ISO 27701 Gap Analysis Tool. Verkkosivu. Viitattu 13.2.2023. https://www.itgovernance.co.uk/shop/product/iso-27701-gap-analysis-tool

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Tampere: Suomen Yliopistopaino Juvenes Print Oy.

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Tampere: Suomen Yliopistopaino Oy Juvenes Print Oy.

Kansaneläkelaitos. 5.1.2022. Strategia. Verkkosivu. Viitattu 28.5.2022. http://www.kela.fi/strategia

Kerzner, H. 2017. Project Management Metrics, KPIs, and Dashboards: A Guide to Measuring and Monitoring Project Management. Vaatii käyttöoikeuden. Viitattu 8.2.2023. https://ebookcentral.proquest.com/lib/tampere/detail.action?pq-origsite=primo&docID=5015537

Key Performance Indicators (KPI) – ne eivät ole mitä luulet. 2023. Lightning Accounting. Verkkosivu. Viitattu 8.2.2023. https://lightningaccounting.fi/strategi-nen-taloushallinto/key-performance-indicators/

Laamanen, K. 2001. Johda liiketoimintaa prosessien verkkona - Ideasta käytäntöön. Laatukeskus. Helsinki.

Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906. Viitattu 8.1.2022. http://www.finlex.fi/fi/laki/alkup/2019/20190906

Laki Kansaneläkelaitoksesta 17.8.2001/731. Viitattu 26.5.2022. http://www.finlex.fi/fi/laki/ajantasa/2001/20010731

Laki potilaan asemasta ja oikeuksista 17.8.1992/785. Viitattu 8.1.2022. https://finlex.fi/fi/laki/ajantasa/1992/19920785

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 27.8.2021/784. Viitattu 13.2.2023. https://www.finlex.fi/fi/laki/alkup/2021/20210784

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (kumottu) 9.2.2007/159. Viitattu 28.5.2022. http://www.finlex.fi/fi/laki/ajantasa/kumotut/2007/20070159

Laki viranomaisen toiminnan julkisuudesta 21.5.1999/621. Viitattu 8.1.2022. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Lönnqvist, A., Kujansivu, P., Antikainen R. 2006. Suorituskyvyn mittaaminen – tunnusluvut asiantuntijaorganisaation johtamisvälineenä. 2. painos. Edita Publishing Oy. Helsinki: Oy Nord Print Ab. 2006.

Malmi, T., Peltola, J., Toivanen, J. 2006. Balanced Scorecard – Rakenna ja sovella tehokkaasti. 5. uudistettu painos. Talentum Media Oy. Jyväskylä: Gummerus Kirjapaino Oy. 2006.

Mikä on KPI ja mitä sillä voi mitata? 2021. Sampo Consulting. Verkkosivu. Viitattu 3.2.2023. https://sampoconsulting.com/mika-on-kpi/

Niemi, T. 2021a. Millaisia ESG-mittareita Neste käyttää johdon palkitsemisessa? Mandatum Life. 21.10.2021. Verkkosivu. Viitattu 13.2.2023. https://www.mandatumlife.fi/life-magazine/2021/millaisia-esg-mittareita-porssiyrityksissa-kaytetaan-johdon-palkitsemissa/

Niemi, T. 2021b. Terveystalo on ottanut vastuullisuusmittarit osaksi johdon palkitsemista. Mandatum Life. 18.10.2021. Verkkosivu. Viitattu 13.2.2023. https://www.mandatumlife.fi/life-magazine/2021/terveystalon-vastuullisuusmittareiden-joukossa-on--digitaalinen-jalanjalki/

Nordea. 2023. Vastuullinen sijoittaminen ja ESG-sijoittaminen. Verkkosivu. Viitattu 13.2.2023. https://www.nordea.fi/henkiloasiakkaat/palvelumme/saastaminen-sijoittaminen/vastuullinen-sijoittaminen.html

Polonetsky, J., Tene, O. 2022. Measuring privacy programs: The role of metrics. IAPP. Verkkosivu. Viitattu 13.2.2023. https://iapp.org/news/a/measuring-privacy-programs-the-role-of-metrics/

Rousku, K. 2017. Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. Helsinki. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

Saaranen-Kauppinen, A. & Puusniekka A. 2009. KvaliMOTV - Menetelmäopetuksen tietovaranto. Toinen vedos. Tampere: Yhteiskuntatieteellinen tietoarkisto Tampereen yliopisto. Viitattu 19.11.2021. https://www.fsd.tuni.fi/fi/tietoarkisto/julkaisut/kvalimotv.pdf

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Verkkosivu. Viitattu 9.12.2022. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_2_1.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Verkkosivu. Viitattu 9.12.2022. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_2_2.html

Sousa, D. 2017. Project Management Metrics, KPI's and Dashboards. LinkedIn. Verkkosivu. Vaatii käyttöoikeuden. Viitattu 3.2.2023. https://www.linkedin.com/pulse/project-management-metrics-kpis-dashboards-diamantino-de-sousa-mba/

Suomen perustuslaki 11.6.1999/731. Viitattu 8.1.2022. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Suomen Standardisoimisliitto SFS. 2015. Eurooppalainen opas standardeista ja sääntelystä. SFS-opas 14. Viitattu 16.1.2022. https://sfs.fi/wp-content/uploads/2020/11/SFS-OPAS_14_web.pdf

Suomen standardisoimisliitto SFS. n.d. ISO/IEC 27000 Tietoturvallisuuden standardisarja. Verkkosivu. Viitattu 5.12.2022. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

Suomen Standardisoimisliitto SFS. n.d. Mitä standardi tarkoittaa? Verkkosivu. Viitattu 18.3.2022. https://sfs.fi/standardeista/mika-on-standardi/

Suomen Standardisoimisliitto SFS. n.d. SFS ry. Verkkosivu. Viitattu 5.12.2022. https://sfs.fi/sfs-ry/

Tene, O., Culnan, M. 2021. Privacy Metrics Report. The Future of Privacy Forum. Verkkosivu. Viitattu 13.2.2023. https://fpf.org/wp-content/uploads/2022/03/FPF-PrivacyMetricsReport-R9-Digital.pdf

Tietoarkisto n.d. Kvantitatiivisen tutkimuksen verkkokäsikirja. Mittaaminen. Verkkosivu. Viitattu 7.1.2023. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/mittaaminen/mittaaminen/

Tietosuojalaki 5.12.2018/1050. Viitattu 8.1.2022. https://finlex.fi/fi/laki/ajantasa/2018/20181050

Tietosuojatyöryhmä. 2016. Tietosuojavastaavia koskevat ohjeet. Julkaistu 13.12.2016. Päivitetty 5.4.2017. Viitattu 28.5.2022. http://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf/3aad84e5-bb59-4e64-bdaf-adc1e5f2d719/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf?t=1527059636000

Tietosuojavaltuutetun toimisto. n.d. Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi. Verkkosivu. Viitattu 2.12.2022. https://tietosuoja.fi/arvioi-riskit

Tietosuojavaltuutetun toimisto. n.d. Käyttötarkoitussidonnaisuus. Verkkosivu. Viitattu 5.12.2022. https://tietosuoja.fi/kayttotarkoitussidonnaisuus

Tietosuojavaltuutetun toimisto. n.d. Lainmukaisuus, asianmukaisuus ja läpinäkyvyys. Verkkosivu. Viitattu 5.12.2022. https://tietosuoja.fi/lainmukaisuus-asianmukaisuus-lapinakyvyys

Tietosuojavaltuutetun toimisto. n.d. Luottamuksellisuus ja turvallisuus. Verkkosivu. Viitattu 5.12.2022. https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus

Tietosuojavaltuutetun toimisto. n.d. Osoita noudattavasi tietosuojasäännöksiä. Verkkosivu. Viitattu 5.12.2022. https://tietosuoja.fi/osoitusvelvollisuus

Tietosuojavaltuutetun toimisto. n.d. Säilytyksen rajoittaminen. Verkkosivu. Viitattu 5.12.2022. https://tietosuoja.fi/sailytyksen-rajoittaminen

Tietosuojavaltuutetun toimisto. n.d. Tietojen minimointi. Verkkosivu. Viitattu 5.12.2022. https://tietosuoja.fi/tietojen-minimointi

Tietosuojavaltuutetun toimisto. n.d. Tietojen täsmällisyys. Verkkosivu. Viitattu 5.12.2022. https://tietosuoja.fi/tietojen-tasmallisyys

Tietosuojavaltuutetun toimisto. n.d. Usein kysyttyä EU:n tietosuoja-asetuksesta. Verkkosivu. Viitattu 4.12.2021. https://tietosuoja.fi/gdpr

Tietosuojavaltuutetun toimisto. n.d. Vaikutustenarviointi. Verkkosivu. Viitattu 2.12.2022. https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto. n.d. Vaikutustenarviointi. Verkkosivu. Viitattu 3.3.2023. Tietosuojan vaikutustenarvioinnin työkalu (.xlsx-tiedosto). https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto. 2021. Tietosuojan vaikutustenarvioinnin ohje. Julkaistu 12/2021. Viitattu 2.12.2022. https://tietosuoja.fi/documents/6927448/66036250/TVA+ohje.pdf/ff0b6e1b-5b89-e85e-a2e5-6c4bd4c0ccfc/TVA+ohje.pdf?t=1639729535787

Tietosuojavaltuutetun toimisto. 2021. Tietosuojavaltuutetun toimisto julkaisi käytännesääntöjen valvontaelinten akkreditointikriteeristön. Julkaistu 9.2.2021. Verkkosivu. Viitattu 5.12.2022. https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-julkaisi-kaytannesaantojen-valvontaelinten-akkreditointikriteeriston

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. 8., uudistettu laitos. Helsinki: Kustannusosakeyhtiö Tammi.

LIITE

Liite 1. Teemahaastattelun kysymykset

Riskienhallinta	Miten riskienhallintaan liittyvällä mittaamisella voisi kehittää organisaation toimintaa?
	Mitä kehitettävää olisi riskienhallinnassa, jotta riskienhallinta toimisi osana päätöksen tekoa?
Raportointi	Mitä kehitettävää olisi raportoinnissa, jotta raportointi toimisi osana päätöksen tekoa?
	Mitä hyötyä raportoinnista on organisaation johdon edustajille?
	Mitä tulisi huomioida raportoinnissa, jotta raportointi toimisi osana päätöksen tekoa?
Mittaaminen	Miten periaatteet voi viedä mitattavalle tasolle?
	Millaista hyötyä periaatteiden mittaamisesta on organisaatiolle?
	Mitä kehitettävää tietosuojaperiaatteiden mittaamisessa olisi, jotta mittaamisesta saatava tieto toimisi osana päätöksen tekoa?
	Millainen kyky organisaatiolla tulisi olla mitata ja osoittaa noudattavansa tietosuoja-asetusta?
	Mitä tavoitteita tietosuojaperiaatteiden mittaamiselle voisi asettaa?
	Mitä välineitä mittaamiseen olisi käytettävissä organisaatiossa tai suositellaan käytettävän?
	Millainen mittari toimii osana päätöksen tekoa?