

# GDPR:n osoitusvelvollisuuden toteuttaminen organisaatiossa

Mikko Nurmi

2019 Laurea

Laurea-ammattikorkeakoulu

## **GDPR:n osoitusvelvollisuuden toteuttaminen organisaatiossa**

Mikko Nurmi  
Tietojenkäsittely  
Opinnäytetyö  
Toukokuu, 2019

Mikko Nurmi

### GDPR:n osoitusvelvollisuuden toteuttaminen organisaatiossa

Vuosi	2019	Sivumäärä	43
-------	------	-----------	----

---

Nykypäivänä, alati kehittyvässä ja kansainvälistyvässä teknologiaympäristössämme yrityksen sitoutuminen henkilötietojen turvalliseen ja oikeaoppiseen käsittelyyn kasvaa jatkuvissa määrin. Samalla yrityksen tarve omata luotettava, toimintavarma sekä korkea tietoturvan taso korostuu entisestään. Ihmisten oikeusturvan sekä yksityisyyden suojan takia on merkittävää, että yrityksessä käsitellään rekisteröityjen tietoja tietosuoja kunnioittavalla tavalla. EU:n alueen tietosuojalainsäädäntö uudistui keväällä 2018, kun uusi henkilötietolaki astui voimaan sen jäsenvaltioissa. Asetuksen tarkoituksena on yhtenäistää tietosuoja Euroopan alueella rekisteröityjen oikeuksia noudattaen.

Opinnäytetyössä perehdytään yhteen asetuksen keskeisempään uudistukseen, joka on osoitusvelvollisuuden sisällyttäminen yrityksen tietoturvaan. Jatkossa rekisterinpitäjän on konkreettisesti pystyttävä osoittamaan mitä, missä ja miten se käsittelee henkilötietoja toiminnassaan. Työssä käsitellään tietosuoja-asetusta, tietoturvaa sekä kuvaillaan tietoturvadokumentaation luomista osoitusvelvollisuuden toteuttamiseksi. Tutkimusmenetelmänä käytettiin tutkimuksellisen kehittämistyön menetelmäperiaatteita.

Tutkimustyön pohjalta luotiin kehittämissuunnitelma kansainvälisiä tietoturvastandardeja hyödyntäen, jolla yritys voi dokumentoida sekä päivittää nykyiset tietosuojaikäytänteensä asetuksen vaatimalle tasolle. Opinnäytetyön viimeisessä osiossa kuvaillaan työpaikallani tehtyä tietoturvakartoitusta sekä siitä syntyviä toimenpiteitä. Työstä syntyneitä tuloksia hyödynnetään tulevaisuudessa työpaikallani tietoturvadokumentaation päivittämisessä.

Asiasanat: General Data Protection Regulation (GDPR), tietosuoja-asetus, tietoturvasuunnitelma, osoitusvelvollisuus

Mikko Nurmi

Implementing GDPR's accountability in an organization

Year	2019	Pages	43
------	------	-------	----

---

Nowadays, in our ever-evolving and internationalizing technology environment, companies' commitment to the safe and correct processing of personal data is growing constantly. At the same time, companies' need to have a reliable and high level of security is further emphasized. Due to the protection of human rights and the protection of privacy, it is important that a company deals with the data in a way that respects data protection. EU's legislation on data protection was reformed in the spring of 2018, when the new Personal Data Act entered into force in EU's member states. The purpose of the regulation is to unify data protection of data subjects registered in the European territory.

The thesis introduced one of the key reforms of the regulation, which is accountability of the data protection principles in a company. In the future, the data administrator must be able to demonstrate in concrete terms what, where and how personal data is handled. The thesis dealt with the general data protection regulation, security and describes the creation of security documentation for the implementation of the accountability. This thesis applied the principles of the developmental research.

Based on the research, a development plan was created using international data security standards, whereby a company can document and update its current data protection practices to the level required by the regulation. The final part of the thesis described the security survey held at the author's workplace and the operations that resulted from it. The results of the thesis will be used in updating the security documentation of the author's workplace in the future.

Keywords: General Data Protection Regulation (GDPR), data protection regulation, security plan, accountability

## Sisällys

1	Johdanto .....	6
2	Opinnäytetyön taustaa ja tavoitteet.....	7
2.1	Kehittämisiongelma .....	7
2.2	Aihealueen rajausta ja tavoitteet .....	7
2.3	Hyödyt .....	8
3	Tutkimusmenetelmät .....	8
4	Käsitteitä .....	11
5	GDPR.....	12
5.1	Henkilötietojen käsittelyn periaatteet.....	13
5.2	Tietosuojavastaava .....	14
5.3	Henkilötietojen tietoturvaloukkaus.....	15
5.4	Osoitusvelvollisuus.....	15
5.4.1	Seloste käsittelytoimista.....	16
5.4.2	Standardit ja sertifiointi .....	17
5.5	Tietosuojaperiaatteiden toteuttaminen .....	18
5.6	Sisäänrakennettu ja oletusarvoinen tietosuojaja.....	19
5.7	Riskiperusteinen lähestymistapa .....	19
6	Tietoturvallisuus.....	20
6.1	Ulkoistaminen .....	22
6.2	Riskien kartoitus .....	22
7	Tietoturvasuunnitelma .....	23
7.1	Tietoturvapoliittika .....	25
7.2	Tietoturvan hallintajärjestelmä ISMS .....	26
7.3	Hallinnollinen turvallisuus.....	28
7.4	Henkilöstöturvallisuus.....	29
7.5	Salassapitosopimus - NDA.....	30
7.6	Fyysinen turvallisuus .....	31
7.6.1	Turvallisuusvyöhykkeet .....	31
7.6.2	Laitteistoturvallisuus .....	33
7.7	Ohjelmistoturvallisuus .....	34
8	Case - yritys X.....	35
9	Yhteenveto .....	37
10	Oman oppimisen arviointi.....	38
	Lähteet .....	40
	Kuviot .....	42
	Taulukot .....	43

## 1 Johdanto

Nykypäivänä elämme verkkoysteiskunnassa, jossa tieto toimii digitaalisen talouden valuuttana. Kaikkialla maailmasta liikkuvista, kerätyistä sekä analysoiduista henkilötiedoista on tullut taloudellisesti merkittävä voimavara. Verkossa on runsaasti kanavia, joiden kautta käyttäjien tietoja on helposti kenen tahansa saatavilla ja juuri verkkoympäristössä tietosuojaan liittyvät puutteet koetaan ongelmallisina. Sosiaalisessa mediassa käyttäjät saattavat jakaa varomattomasti henkilökohtaisia tietojaan sekä informaatiota mielenkiinnon kohteistaan. Mitä enemmän näitä tietoja kerätään, sitä enemmän sitä on mahdollista yhdistellä. Saatua tietoa voidaan hyödyntää yksityisen henkilön tietojen selvittämiseen, yritysmaailmassa markkinoinnin kohdentamiseen ja kilpailevan yrityksen peittoamiseen. Väriin käsiin joutuneet tiedot saattavat olla vahingollisia tietojen kohteena olevalle henkilölle. Saatuja henkilötietoja voidaan käyttää väärin muun muassa henkilön nimissä ostoa tai myyntiä, identiteettivarkauksia sekä arkaluonteiset tiedot, esimerkiksi terveystiedot, mahdollistavat henkilöiden kiristämisen. Tietojen väärinkäytökset ovat myös vahingollisia niiden käsittelystä vastuussa olevan yrityksen toiminnalle. Väärinkäytöksistä saattaa koitua yritykselle maineen menetyksiä, taloudellisia seuraamuksia sekä asiakaskunnan siirtymistä kilpaileviin yrityksiin. Tietojen oikeaoppinen ja turvallinen käsittely onkin yrityksen liiketoiminnan jatkuvuuden kannalta merkittävä osa-alue.

EU:n alueen tietosuoja vaatimukset uudistuivat, kun sen jäsenvaltioissa keväällä 2018 sovellettavaksi tuli Euroopan unionin yleinen tietosuoja-asetus, paremmin tunnettu nimellä GDPR (General Data Protection Regulation). Asetus laadittiin vuonna 2016 ja se tuli täydentämään jo voimassa olevaa henkilötietolakia. Yksi asetuksen keskeisimmistä periaatteista on osoitusvelvollisuuden noudattaminen, jolla organisaation on pystyttävä käytännössä osoittamaan noudattavansa tietosuojalainsäädäntöä. Henkilötietolain aikaan riitti, että organisaatiossa oli tietoturva riittävän laadukkaalla tasolla sekä tietoturva-asetuksia noudatettiin. Osoitusvelvollisuuden avulla organisaatiolta saadaan suoraa näyttöä siitä, että se on aktiivisesti pyrkinyt tiedostamaan tietoturvaan liittyviä riskejä. Organisaation tietoturvaa pidetään riittävällä tasolla henkilötietojen suojaamiseksi väärinkäytöksiltä sekä niihin oikeudettomilta tahoilta.

Tässä opinnäytetyössä perehdytään osoitusvelvollisuuden vaateisiin ja tietoturvaan rekisterinpitäjän näkökulmasta. Tutkimustyöhön perustuen kuvaillaan yrityksen tietoturvasuunnitelmaan sisältyvät osa-alueet sekä ne toimenpiteet, joita hyödyntäen organisaatiossa voidaan päivittää tietoturvasuunnitelman vaatimalle tasolle. Tietoturvasuunnitelman toteuttaminen itsessään on laaja prosessi ja siihen tulisi osallistua mahdollisimman moni tahon organisaation sisältä. Näin saadaan otettua tietoturvasuunnitelman huomioon toimintatavat aina ruohonjuuritasolta yritysjohtoon saakka.

## 2 Opinnäytetyön taustaa ja tavoitteet

Tämän työn selkeää yhteyttä työelämään on rajattu ja työnantajani nimi on tarkoituksella jätetty mainitsematta työssäni. Tavoitteena on kehittää yleisesti toimintasuunnitelma, jolla organisaatio voi dokumentoida tietoturvakäytäntönsä. Työn tuloksia hyödynnetään kuitenkin työpaikallani sekä tulevaisuus näyttää opinnäytetyöni hyödyllisyyden työnantajalleni. Osastoni päätehtävänä on ylläpitää asiakasrekisteriä ja työpaikallani henkilötiedoiksi luokiteltavaa tietoa käsitellään päivittäin huomattavia määriä organisaation sisällä ja sidosryhmien välillä. Uuden tietosuoja-asetuksen vaikutuksesta rekisterinpitäjän velvoitteisiin on tiedotettu organisaatiossa kohtalaisesti sekä työyhteisössä on ollut epätietoisuutta, miten asetuksen voimaan tulo vaikuttaa heidän omaan päivittäiseen työskentelyynsä. Tiedotuksen puutteellisuus johtuu osin myös siitä, että kukaan ei vielä tarkkaan tiedä, kuinka asetusta sovelletaan käytännössä sekä käytännön esimerkkejä on vähäisesti. Henkilötietojen turvallinen käsittely on kuitenkin olennainen osa organisaation toimintaa ja työyhteisössä on perustettu tietosuoja-asetusta tutkiva työryhmä, johon kuuluu henkilöstöä eri osastoilta. Työryhmän tarkoituksena on ollut perehtyä tarkemmin tietosuoja-asetuksen tuomiin muutoksiin sekä sen vaatimuksiin tietoturvan saralla. Opinnäytetyössä perehdytään tietoturvallisuuteen sekä rekisterinpitäjän osoitusvelvollisuuden vaatimuksien toteuttamiseen, jota voidaan myöhemmin hyödyntää organisaation tietoturvan päivittämisessä. Yrityksessä on myös tehty kevään 2019 aikana tietoturvakartoitus, jonka raportti valmistui hiljattain. Raportin avulla saadaan yritykseen luotua tietoturva-politiikka, joka toimii pohjana tietoturvan päivittämisessä. Havaitut puutteet tullaan korjaamaan ja tietoturvan suhteen muuttuneet käytänteet kouluttamaan henkilöstölle.

### 2.1 Kehittämisiongelma

Aiheeseen liittyvään aineistoon perehtymisen ja tutkimustyön perusteella kuvaillaan suunnitelma yrityksen tietoturvan päivittämiseksi. Hyvin laadittu ja dokumentoitu tietoturvasuunnitelma on kuitenkin hankalaa täysin yksin toteuttaa, ja sen toteuttamiseksi organisaatiossa tulisi osallistua mahdollisimman paljon henkilöstöä eri osastoilta. Esimerkiksi itse tiedän missä ja miten henkilötietoja käsitellään omalla osastollani päivittäisessä työskentelyssä, mutta on lähes mahdotonta kartoittaa kaikkia muiden osastojen toimintatapoja ja varantoja, joissa henkilötietoja säilytetään.

### 2.2 Aihealueen rajaus ja tavoitteet

Opinnäytetyö keskittyy yhteen tietosuoja-asetuksen tuomaan keskeiseen muutokseen, joka on osoitusvelvollisuuden sisällyttäminen yrityksen tietoturvaan. Asetuksen kaikkien muutosten huomioiminen kasvattaisi työn laajuutta liian suureksi ja näin ongelmakohtiin perehtyminen jäisi heikoksi. Rajaamalla pois asetuksen muita velvoitteita saadaan määriteltyä kattava kokonaiskuva osoitusvelvollisuudesta. Opinnäytetyössä käsitellään kuitenkin lyhyesti muutamia asetuksen kohtia, kuten tietosuojavastaavan nimittämistä sekä henkilötietojen käsittelyn periaatteita. Tutkimustyön pohjalta kehitetään erinäisiä ohjeistuksia ja standardeja hyödyntäen

toimintasuunnitelma, jolla organisaatio voi dokumentoida ja päivittää omat tietoturvakäytänteet asetuksen vaatimalle tasolle.

Osoitusvelvollisuuden toteuttaminen on yksi uuden asetuksen tuomia keskeisimpiä muutoksia voimassa oleviin toimintaperiaatteisiin tietoturvassa. Jatkossa organisaatiolla on oltava kyky osoittaa noudattavansa asetusta henkilötietojen käsittelyn yhteydessä ja toteuttavansa käytännössä asetuksen asettamia tietosuojaperiaatteita. Henkilötietolain aikaan oli riittävä, että säännöksiä vain noudatettiin (Oikeusministeriö 2017, 14).

Jotta saavutetaan opinnäytetyön tavoitteet, tulee löytää vastaukset seuraaviin kysymyksiin:

- Mitä osoitusvelvollisuudella tarkoitetaan rekisterinpitäjän näkökulmasta?
- Kuinka oleellinen tekijä hyvä tietoturvallisuus on osana yrityksen liiketoimintaa?
- Kuinka päivittää yrityksen tietoturva asetuksen vaatimalle tasolle?
- Kuinka dokumentoida yrityksen tietoturvakäytänteet?

### 2.3 Hyödyt

Uuden tietosuoja-asetuksen vaikutuksien tutkiminen on ajankohtaista, ja henkilötietojen turvallinen käsittely on oleellinen osa organisaation liiketoimintaa sen elinvoiman sekä luotettavuuden kannalta. Asiakkaiden ja sidosryhmien luottamus organisaation menetelmiin tietosuojaan ja tietoturvan osalta on toimintaa vahvasti tukeva tekijä. Tietosuojaan ja tietoturvan huomioiminen, esimerkiksi verkkopalveluissa on laissa säädetyn velvollisuuden ohella myös oleellinen osa hyvää palvelua.

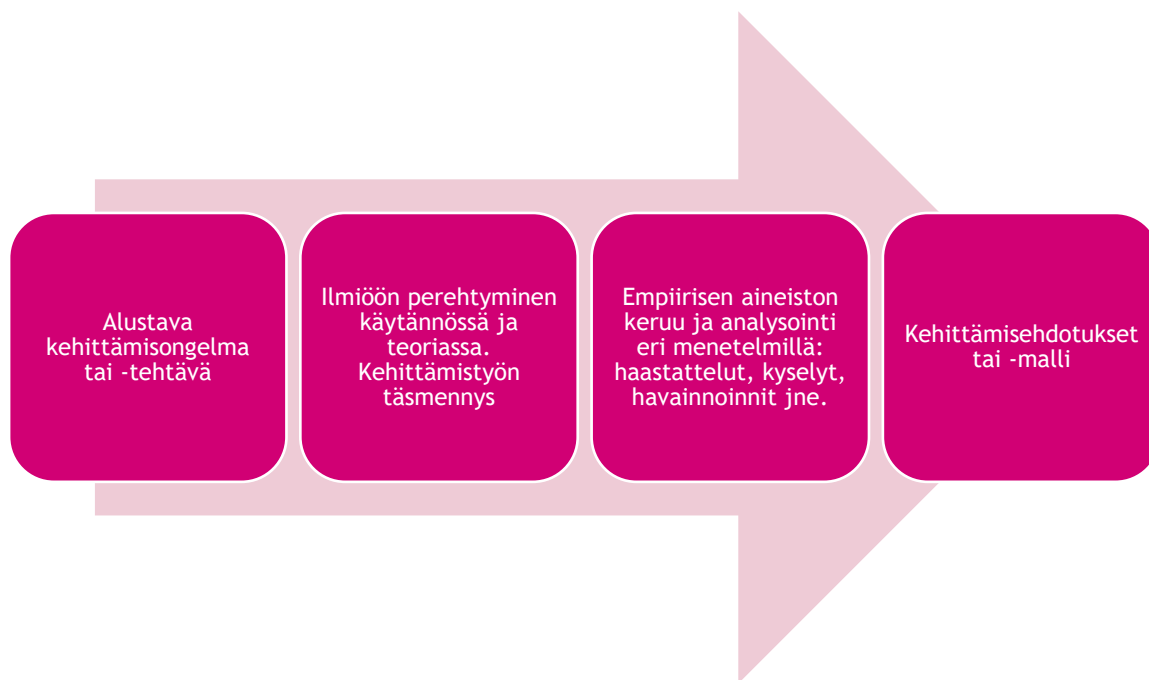
Kehittämistyön tuotoksesta sekä tietosuoja-asetuksen tutkimisesta hyötyy lähes kaikki organisaation työyhteisöön kuuluvat sekä sen sidosryhmät. Henkilötietoja käsitellään jatkossa entistä turvallisemmin, ja rekisteröity saa uuden tietosuoja-asetuksen asettamat hyödyt käyttöönsä. Työyhteisössä saadaan ohjeistusta ja yhtenäisyyttä työskentelymenetelmiin sekä perehdytystä uuden tietosuoja-asetuksen osalta.

## 3 Tutkimusmenetelmät

Opinnäytetyössä hyödynnettiin tutkimuksellisen kehittämistyön prosessin menetelmäperiaatteita, jonka etenemisen eri vaiheet on havainnollistettu kuviossa 1. Tutkimuksellinen kehittämistyö voi saada alkunsa erilaisista lähtökohdista, kuten organisaation kehittämistarpeista tai tarpeesta saada aikaan muutoksia. Tutkimukselliseen kehittämistyöhön kuuluu yleensä käytännön ongelmien ratkaisua sekä uusien ideoiden tai käytäntöjen tuottamista tai toteuttamista. Sen prosessin eri vaiheita hyödyntäen voidaan luoda organisaatioon käytännön parannuksia sekä ratkaisuja. Kehittämistyötä ei ohjaa ensi sijassa teoreettiset vaan käytännölliset



tavoitteet, joihin haetaan tukea teoriasta. Kaikenlainen kehittämistyö voidaan jäsentää yksinkertaiseksi muutostyön prosessiksi, jossa siihen kuuluu kehittämishaasteiden selvittäminen, niitä koskevien tavoitteiden asettaminen ja suunnitelma siitä miten tavoitteisiin voidaan päästä. Tämä muodostaa suunnitteluvaiheen, joka johtaa suunnitelman toteutusvaiheeseen ja lopuksi arviointivaiheeseen, jossa arvioidaan muutostyön onnistuminen (Ojasalo, Moilanen & Ritalahti 2014, 17-20).



Kuvio 1: Tapaustutkimuksen vaiheet

Tapaustutkimus on hyvin tyypillinen tutkimusstrategia ja sen lähtökohdat ovat tieteellisen tutkimuksen traditiossa. Tapaustutkimus soveltuu myös hyvin kehittämistyön lähestymistavaksi, kun tehtävänä on tuottaa kehittämisehdotuksia ja -ideoita. Tapaustutkimus tuottaa tietoa nykyajassa tapahtuvasta ilmiöstä sen todellisessa tilanteessa ja elinympäristössä. Tapaustutkimus vastaakin usein kysymyksiin ”miten?” ja ”miksi?”, ja kehittämistyössä on tarkoituksena tuottaa uutta tietoa kehittämisen tueksi. Usein tapaustutkimus liitetään erityisesti laadulliseen tutkimukseen ja menetelmiin, mutta siinä on myös mahdollista hyödyntää määrällisiä menetelmiä. Aineistot kerätään yleensä luonnollisissa tilanteissa, esimerkiksi havainnoinnilla tilanteita tai analysoimalla kirjallisia aineistoja (Ojasalo ym. 2014, 52-53, 55.)

Kehittämistyön tietoperusta perustuu hyvin paljolti aiheeseen liittyvään kirjallisuuteen sekä uuden tietosuojasetuksen tekstiin tulkitsemiseen. Tämä muodosti teoreettisen viitekehyksen työlle. Tietoturvasuunnitelman dokumentaation luomisessa hyödynnettiin myös kansainvälistä standardointijärjestö International Organization of Standardization (ISO) määrittelemiä tietoturvallisuuden menettelytapoihin liittyvää ISO/IEC 2700-standariperheen eri ohjeistuksia. Standardisarja ei sisällä pakollisia velvoitteita, vaan toimii ohjeistuksena sekä apuna organi-

saation toiminnan johtamisessa ja laadunvalvonnassa. Aiheen ajankohtaisuudesta johtuen tietoa löytyy verkosta myös paljon alan ammattilaisten julkaisuista, muun muassa oikeusministeriön sivustoa päivitetään säännöllisesti ja valtiohallinnon VAHTI työryhmä jakaa ohjeistusta aiheeseen liittyen.

Tutkimuksen pätevyyttä ja luotettavuutta voidaan tarkastella yleisesti kahdesta eri näkökulmasta, onko tutkimuksen aikana käytetyt mittaus- tai tutkimusmenetelmät valideja ja/tai reliaabeleja sekä ovatko tutkijan tutkimuksen tuloksista tehdyt päätelmät valideja ja/tai reliaabeleja? (Hiltunen, 2009).

Validiteetti eli pätevyys ilmaisee sen, miten hyvin tutkijan valitsema mittaus- tai tutkimusmenetelmä mittaa juuri tutkimuksessa tutkittavan ilmiön ominaisuutta. Mitataanko tutkimuksessa sitä, mitä siinä hyödynnetyn menetelmän avulla on ollut haluttu selvittää. Mikäli tutkimuksen validiteetti on puutteellinen tai se puuttuu kokonaan, niin tutkimuksen arvo kärsii. Tällöin tutkitaan lopulta aivan muuta asiaa kuin mitä alun perin on ollut tarkoitus selvittää ja koko tutkimus itsessään sekä sen empiiriset havainnot kohdistuvat sivuun siitä, mitkä olivat tutkimuksen alkuperäiset tavoitteet. Tutkimuksessa aineisto- ja sisältövaliditeetilla tarkoitetaan tutkimusaineiston pätevyyttä ja sitä, kuinka hyvin tämän aineiston analysointimenetelmä vastaa tutkimusaineistoa, kuinka hyvin koottu aineisto vastaa ulkopuolisia kriteereitä. Arvioijan on koko tutkimuksen aikana kyettävä arvioimaan tutkimusprosessia ja seuraamaan sen aikana johdettuja päätelmiä. Näin arvioija kykenee havaitsemaan, etteivät tutkimuksen tulokset perustu pelkästään tutkijan henkilökohtaiseen intuitioon, vaan tuloksille saadaan validiteettia. Siksi tutkijan on mahdollisimman hyvin kuvattava aineistonsa, tulkintansa sekä ratkaisu- ja tulkintatavat. Validiteetissa onkin juuri kyse siitä, onko tutkimus perustellusti tehty ja ovatko sen tulokset ja päätelmät päteviä ja ”oikeita” (Hiltunen, 2009).

Reliabiliteetti eli luotettavuus ilmaisee sen, miten luotettavasti ja toistettavasti tutkijan valitsema mittaus- tai tutkimusmenetelmä mittaa haluttua ilmiötä. Johtuuko tutkimustulos tai tutkimuksessa esitelty päätelmä vain sattumasta vai kyetäänkö samaan tulokseen pääsemään yhä uudelleen? Luotettava tutkimus on tehty siten, että se toistettuna alkuperäisen tutkimuksessa käytetyin menetelmien, se antaa saman tuloksen samoissa olosuhteissa. Periaatteessa tutkimusmenetelmä voi olla reliaabeli, vaikka se ei olisikaan validi. Tällöin tutkimuksessa käytettyjen menetelmien avulla voidaan päätyä hyödyllisiin tuloksiin, mutta valitut menetelmät eivät johda siihen lopputulokseen, mihin tutkimuksella tähdättiin. Mitä alhaisempi reliabiliteetti tutkimuksella on, sitä alhaisempi on myös tutkimuksen validiteetti (Hiltunen, 2009).

Työssäni käytetty tutkimusmenetelmä (tapaustutkimus) sopi hyvin tutkimusmenemäksi, sillä työpaikan henkilöstö ei ollut kovin tietoinen siitä, miten henkilötietoja käsitellään. Organisaatiossa oli siis selvästi tarvetta kyseiselle kehittämistyölle, jonka vuoksi käytetty tutkimusmenetelmä oli luontevin valinta.

Olen myös kuvaillut työssäni käytettyä tutkimusmenetelmää ja sen eri vaiheita monipuolisesti, ja käyttänyt monipuolisia, luotettavia ja ajankohtaisia lähteitä. Viittaamalla eri tietoturva-asiantuntijoiden lähteisiin saadaan tutkimustyölle luotettavuutta ja yhtenäisyyttä. Lisäksi olen koko opinnäytetyöni ajan työskennellyt päätoimisesti työpaikallani, jonka vuoksi olen päässyt näkemään itse suurimmat ongelmakohdat työpaikallani tietoturvaa koskien. Näihin ongelmakohtiin peilaten, olen pyrkinyt tekemään tutkimustyön parhaalla mahdollisella tavalla.

#### 4 Käsitteitä

Henkilötieto	Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettavissa olevaan luonnolliseen henkilöön. Henkilön tunnistaminen voi tapahtua suoraan tai epäsuorasti tunnistetietojen perusteella. Esimerkiksi yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.
Henkilötietojen käsittely	Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen. Henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä, luovuttamista yms.
Henkilötietojen käsittelijä	Ihminen tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tällä ei tarkoiteta rekisterinpitäjän alaisuudessa toimivia työntekijöitä vaan se saattaa olla esimerkiksi yritys, yksityinen elinkeinonharjoittaja, yhdistys tai muu palveluntarjoaja, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.
Rekisterinpitäjä	Henkilötietoja käsittelevä taho, kuten luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu henkilö, joka määrittelee henkilötietoihin liittyvien käsittelyiden tarkoitukset ja menetelmät.
Yhteisrekisterinpitäjä	Kun vähintään kaksi rekisterinpitäjää määrittelee yhdessä käsittelyn tarkoitukset ja käytänteet.

Tietosuoja	Henkilötietolain sekä erityislakien henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista rekisteröidyn yksityisyyden suojan ja oikeusturvan takaamiseksi. Tietosuojan tarkoituksena on ohjata rekisterinpitäjiä hyviin henkilötietojen käsittelykäytäntöihin sekä turvata henkilötietojen kohteen yksityiselämää, etuja ja oikeuksia.
Tietosuojavastaava	Rekisterinpitäjää avustava henkilö, jolla on erityistuntemusta tietosuojalainsäädännöstä sekä alan käytänteistä. Tietosuojavastaavan tehtävän on valvoa asetuksen noudattamista organisaatiossa.

(Tietosuojavaltuutetun toimisto 2018a.)

## 5 GDPR

EU:n alueen tietosuojalainsäädännön uudistaminen käynnistämisen alkoi vuonna 2012, kun tietosuojalainsäädäntö ei enää vastannut globaalin ja digitaalitalouden tarpeisiin. Uudistuksen tarkoituksena oli turvata henkilötietojen suoja samalla, kun parannettaisiin EU:n sisämarkkinoiden toimintaedellytyksiä. Tämän prosessin tuloksena syntyi EU:n yleinen tietosuoja-asetus GDPR (General Data Protection Regulation). Uusi tietosuoja-asetus on henkilötietojen käsittelyä koskeva yleissäädos, joka tuli voimaan 25.5.2016 ja sitä on sovellettu 25.5.2018 alkaen. Asetuksessa on kansallista liikkumavaraa, jonka käyttämisestä säädetään uudessa tietosuojalainlaissa. Suomen hallituksen esitys EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi annettiin eduskunnalle maaliskuussa 2018 ja eduskunta hyväksyi sen 13.11.2018. Tietosuojalain ohella henkilötietojen käsittelystä säädetään edelleen myös sektorikohtaisessa lainsäädännössä (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 1).

Uuden tietosuoja-asetuksen tullessa sovellettavaksi tuo se uusia velvoitteita rekisterinpitäjälle ja oikeuksia rekisteröidylle. Organisaation olisi siirtymäajan jälkeen tiedettävä, mitä, missä ja miten ne henkilötietoja käsittelevät sekä pystyttävä myös osoittamaan, että se on ottanut huomioon asetuksen vaatimukset toiminnassaan. Vaikka uusi henkilötietolaki rakentuu samalle pohjalle vuonna 1999 voimaan tulleen vanhan lain kanssa ja kyseisen lain pääperiaatteet säilyvät yleisessä tietosuoja-asetuksessa, niin organisaatiolla on oltava kyky osoittaa, että vanha lain pykälät oikeasti toteutetaan. Järvinen (2018). Vaikka henkilötietolain periaatteet säilyvät pääosin uudessa tietosuoja-asetuksessa ennallaan, niin niistä osaa on täsmennetty sekä asetus edellyttää aivan uudenlaista suhtautumista tietosuoja koskeviin kysymyksiin. Näistä merkittävimpiä muutoksia on juuri osoitusvelvollisuuden sisällyttäminen organisaation tietoturvaan. Osat asetuksen vaatimuksista on selvää sekä osassa haetaan vielä linjaa, koska ei ole vielä hirveästi käytännön esimerkkejä, miten asetusta sovelletaan siirtymäajan

päätyessä. Henkilötietojen käsittelyn yhteydessä rekisterinpitäjän on toiminnassaan huomioitava, että heidän menetelmätavat noudattavat uutta lainsäädäntöä sekä henkilötiedot ovat kulloisenkin riski tason huomioiden turvassa.

Tietosuoja-asetuksen vaikutuksia arvioidessaan organisaation tulee hahmotella kokonaiskuva miten sen henkilötietojen käsittelyä toteutetaan eri toimissa. Henkilötietojen käsittelyn nykytilan arvioinnissa voidaan esimerkiksi kuvata, mitä henkilötietovarantoja organisaatiossa on, miten tietosuojaperiaatteita toteutetaan tällä hetkellä, toimintaan sisältyvät henkilötietovirrat, miten tietoturvaa huolehditaan ja pidetään yllä sekä miten toteutetaan henkilötietojen käsittelyn riskienhallintaa. Nykytilan kartoituksen voi toteuttaa esimerkiksi luomalla tietotilinpäätös organisaatiossa, joka on yrityksen sisäisen tarkastelun tuotoksena laadittu raportti tietojen käsittelyä koskevista keskeisistä asioista. Tätä dokumenttia voidaan jatkossa hyödyntää organisaation sisäiseen tietojohdantamiseen ja sen avulla on mahdollista tiedottaa organisaation sidosryhmille tietojen käsittelyyn liittyvistä periaatteista (Oikeusministeriö 2017, 11).

Tietosuoja-asetuksen tarkoituksena on lisätä Euroopan unionin alueella rekisterinpitäjien ja henkilötietojen käsittelijöiden työskentelyn avoimuutta ja läpinäkyvyyttä henkilötietojen käsittelyn yhteydessä. Lisäksi tavoitteena on vahvistaa rekisteröityjen mahdollisuuksia valvoa, kuinka heitä koskevia tietoja käsitellään organisaatiossa. Uusi asetus koskee kaikkia sen soveltamisalaan kuuluvia henkilötietoja käsitteleviä tahoja niin rekisterinpitäjiä kuin henkilötietojen käsittelijöitä. Näiden tahojen on käsittelymenetelmiä määritellessään ja itse käsittelyn yhteydessä toteutettava organisaatiossa asianmukaiset tekniset ja organisatoriset toimenpiteet asetuksen tietosuojaperiaatteiden noudattamista varten. Laajemmin avattuna tekniset ja organisatoriset toimenpiteet sisältävät suojatoimenpiteitä tietoturvallisuudessa kuten henkilöstön koulutusta, ohjeita ja määräyksiä henkilötietojen käsittelyyn, salassapitosopimuksia, tietojärjestelmien tietoturvaa, tietojen salausta, auditointeja, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmää, tietotilinpäätösprosessia ja sertifikaattien käyttöönottoa (Oikeusministeriö 2017, 9, 13.)

## 5.1 Henkilötietojen käsittelyn periaatteet

Asetus velvoittaa, että jatkossa henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (*lainmukaisuus, kohtuullisuus, läpinäkyvyys*). Lainmukaisuudella tarkoitetaan, että henkilötiedoilla on ensinäkin lain mukainen perustelu käsittelyyn. Tietosuoja-asetuksessa mainitut lainmukaiset käsittelyperusteet ovat suostumus, sopimuksen täytäntöönpano, rekisterinpitäjän lakisääteisen veloitteen noudattaminen, elintärkeiden etujen suojaaminen, yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen sekä oikeutettujen etujen toteuttaminen. Myös sopimukseen perustuva henkilötietojen käsittely on lainmukaista, vaikka sopimuksesta ei säädettäisi laissa. Asianmukaisuudella tarkoitetaan eräänlaista reiluuutta. Tämä tarkoittaa sitä, että

rekisterinpitäjät ottavat tietoja käsitellessään huomioon myös rekisteröidyn edut ja odotukset. Lisäksi tämä edellyttää myös sitä, että tietoja ei väärinkäytetä esimerkiksi keräämällä rekisteröidyistä salaa tietoja ja rekisteröity tietää käsittelyn luonteesta ja tarkoituksesta. Asiamukainen henkilötietojen käsittely liittyy myös käyttötarkoitussidonnaisuuden periaatteen rajoittamalla yhteen tarkoitukseen kerätyn tiedon hyödyntämistä toissijaiselle käytölle. Käyttötarkoitussidonnaisuus ei kuitenkaan kiellä käsittelemästä yhtä tarkoitusta varten kerättyä tietoa myös toiseen käyttötarkoitukseen, kunhan se ei ole alkuperäisen käyttötarkoituksen kanssa yhteensopimatonta. Läpinäkyvyyden periaate on merkittävä, koska itse tietojen käsittely ei tapahdu julkisesti eivätkä sen tuloksetkaan aina heti kosketa rekisteröityä välittömästi, jotta hän voisi reagoida käsittelyyn. Tällä periaatteella halutaan varmistaa, että rekisteröity saa tiedon siitä, miten heitä koskevia henkilötietoja kerätään, käytetään, säilytetään tai muutoin käsitellään. Jotta tämä olisi mahdollista, henkilötietojen käsittelyyn liittyvien tietojen pitää olla helposti saatavilla sekä selkeällä ja yksinkertaisella kielellä ilmaistu. Lisäksi on tiedotettava käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista. Rekisteröidyn ei tarvitsisi vaivalloisesti etsiä tietosuojaselostetta tai muita hänen kannaltaan tarpeellisia tietoja, vaan informaatio löytyy esimerkiksi samalta sivustolta, jonne rekisteröity antaa tietojansa (Korpisaari, 2018, 92.)

## 5.2 Tietosuojavastaava

Asetus velvoittaa rekisterinpitäjiä nimeämään tietosuojavastaavan, jonka tulee olla riippumattomassa asemassa organisaatiossa sekä hän raportoi suoraan rekisterinpitäjän tai käsittelijän ylimmälle johdolle. Tietosuojavastaavan nimittäminen kohdistuu erityisesti julkiselle sektorille ja hänet voidaan tarvittaessa nimetä myös useampaa viranomaista tai julkishallinnon elintä edustamaan. Jotta tietosuojavastaavan toimenkuva on tällöin hallittavissa, tulee ottaa huomioon kohteiden organisaatorakenteet ja niiden koot. Tietosuojavastaavan nimeäminen täytyy tehdä, mikäli organisaatiossa tietojenkäsittelyä suorittaa viranomaisen tai julkishallinnon elin tai sen ydintehtävät muodostuvat käsittelytoimista, jotka luonteeltaan vaativat rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Nimeäminen täytyy tehdä, myös silloin, kun käsittelytoimet kohdistuvat henkilötietojen erityisiin tietoryhmiin, rikostuomioihin tai rikoksia sisältäviä tietoja (Pietikäinen, 2016).

Tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa asetuksen vaatimusten täytäntöönpanosta ja sen soveltamisesta koko organisaatiossa. Hänen velvollisuutensa on vahvistaa asetuksen velvoitteen noudattamisesta sekä tuoda esiin siinä havaitsemiaan puutteita. Tietosuojavastaavan tehtävänä on antaa tietoja ja ohjeistusta tietosuoja sääntöjen mukaisista velvollisuuksista johdolle sekä henkilötietojen käsitteleville työntekijöille. Hän toimii myös rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä asioissa sekä tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa ja organisaation yhteyshenkilö heidän suun-

taansa. Tietosuojavastaava ei ole itse henkilökohtaisesti vastuussa tietosuojasäännösten noudattamisesta, vaan nämä vastuut kuuluvat rekisterinpitäjän sekä henkilötietojen käsittelijälle (Tietosuojavaltuutetun toimisto 2018b).

### 5.3 Henkilötietojen tietoturvaloukkaus

Yksi asetuksen uusista rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksista. Tietoturvaloukkauksen sattua on siitä ilmoitettava rekisteröidylle sekä valvontaviranomaiselle. Tämän ilmoituksen on tapahduttava 72 tunnin kuluessa siitä, kun loukkaus on havaittu. Ilmoituksessa tulee olla kuvaus siitä, mitä on tapahtunut, rekisteröityjen ryhmät ja lukumäärät, joita loukkaus koskettaa sekä niiden vaikutus kohteena olevalle. Kuvauksessa tulee olla myös kuvaus jatko toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa haittavaikutuksien lieventämiseksi (Pietikäinen, 2016).

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapausta, jonka seurauksena rekisteröidyn henkilötietoja tuhoutuu, katoaa, niitä luovutetaan tai muutetaan luvottomasti. Tietoturvaloukkaus tapahtuu aina, kun niihin pääsee käsiksi osapuoli, jolla ei ole niihin oikeutta. Rekisterinpitäjän on tällöin myös arvioitava, millainen riski tietoturvaloukkauksesta on aiheutunut sen kohteena olleelle henkilölle ja ryhdyttävä asianmukaisiin toimenpiteisiin vahinkojen minimoimiseksi (Tietosuojavaltuutetun toimisto 2018c).

### 5.4 Osoitusvelvollisuus

Osoitusvelvollisuus on yksi keskeinen periaate tietosuojasetuksessa. Yrityksen on jatkossa dokumentoitava nykyiset sekä muuttuvat käytänteet, jotta se pystyy tarvittaessa osoittamaan viranomaisille, että asetuksen velvollisuuksia noudatetaan. Tämän velvoitteen avulla rekisterinpitäjä tai henkilötietojen käsittelijä voi dokumentein osoittaa, että se on aktiivisesti pyrkinnyt tunnistamaan tietosuojaan liittyviä riskejä ja ottanut käyttöönsä tarvittavat toimenpiteet henkilötietojen suojaamiseksi. Mikäli henkilötietoja käsitellyt taho ei kykene käytännössä osoittamaan noudattavansa tietosuojasetuksen vaatimuksia, niin se voi aiheuttaa mainerisikin lisäksi myös hallinnollisia seuraamuksia. Koska yrityksen on jatkossa pystyttävä osoittamaan noudattavansa lakia, niin se edellyttää samalla uudenlaista suhtautumista tietosuoja koskeviin kysymyksiin. Tämä asetuksen kohta edellyttää yritykseltä henkilötietojen käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön dokumentointia sekä sen on toteutettava organisaatiossa tarvittavat tekniset ja organisatoriset toimenpiteet. Osoitusvelvollisuuden laajuuteen vaikuttaa muun muassa organisaation suuruus, henkilötietojen määrä ja se, minkälaisia henkilötietoja rekisterinpitäjä käsittelee toiminnassaan (Tietosuojavaltuutetun toimisto 2018b).

#### 5.4.1 Seloste käsittelytoimista

Asetuksen myötä rekisterinpitäjän ja tarvittaessa rekisterinpitäjän edustajan on velvollisuus laatia kirjallinen kuvaus sen toteuttamasta henkilötietojen käsittelystä, jota kutsutaan selosteeksi käsittelytoimista. Käsittelytoimia kuvaavan selosteen laatiminen edistää osoitusvelvollisuuden toteuttamista ja se on myös hyödyllinen työkalu henkilötietojen käsittelyn hahmottamiseen sekä analysoimiseen silloin kun velvollisuutta sen laatimiseen ei välttämättä ole. Selosteen tekeminen vaaditaan, jos organisaatiossa on yli 250 työntekijää. Seloste on myös toteutettava, mikäli henkilötietojen käsittely ei ole satunnaista, se aiheuttaa mahdollisen riskin rekisteröidyn oikeuksille tai käsiteltävät henkilötiedot koskevat erityisiä tietoryhmiä tai rikostuomioihin ja rikoksia sisältäviä henkilötietoja. Rekisterinpitäjän laatimassa selosteessa tulee kuvata vähintään seuraavat tiedot:

- Rekisterinpitäjän, mahdollisen yhteisrekisterinpitäjän, mahdollisen rekisterinpitäjän edustajan sekä tietosuojavastaavan nimet ja yhteystiedot.
- Laillinen käyttötarkoitus kaikille tiedoille, joita se ryhtyy toiminnassaan käsittelemään. Käyttötarkoitus on kuvattava riittävän yksityiskohtaisesti sekä se määrittelee lisäksi myös sen, mihin tarkoituksiin henkilötietoja saadaan jatkossa käyttää, mitä henkilötietoja on tarpeen kerätä ja kuinka pitkään niitä voidaan säilyttää organisaation tietovarannoissa. Selosteessa on myös hyvä kuvata mihin tietosuojasetuksen mukaiseen käsittelyperusteeseen tietojen käsittely perustuu.
- Kuvaus rekisteröityjen ryhmistä sekä henkilötietoryhmistä. Keitä rekisteröidyt ovat sekä minkälaisia tietoja heistä käsitellään.
- Vastaanottajaryhmät, joille henkilötietoja luovutetaan. Vastaanottajia voi olla luonnolliset henkilöt, oikeushenkilöt, viranomaiset sekä muita organisaation sidosryhmiä. Vastaanottajia ovat myös täysin ulkopuolisten rekisterinpitäjien lisäksi yhteisrekisterinpitäjät sekä henkilötietojen käsittelijät, joille henkilötiedot siirretään tai luovutetaan. Selosteessa ei kuitenkaan tarvitse mainita viranomaisia, joille luovutetaan henkilötietoja jäsenvaltion lainsäädäntöön perustuvan selvitystyön yhteydessä.
- Tietoryhmien suunnitellut poistamisen määräajat tai ne kriteerit, joilla tietojen säilyttämisaajat määritellään. Määrittelyn säilytysajan perusteella on pystyttävä arvioimaan, kuinka pitkään rekisteröityä koskevia henkilötietoja käsitellään. ”Henkilötietoja säilytetään niin kauan kuin on tarpeellista tiettyjen laillisten tarkoitusten saavuttamiseksi” ei ole riittävä ilmaisu säilytysaikoja määriteltäessä.



- Kuvaus teknisistä ja organisatorista turvatoimista. Selvitys siitä, millä tavoilla tiedot on suojattu organisaation ulkopuolisilta tahoilta, miten organisaation sisällä on rajoitettu käyttöoikeuksia henkilötietoihin ja millä tavalla näiden oikeuksien käyttöä seurataan

(Tietosuojavaltuutetun toimisto 2018d.)

Uusi asetus velvoittaa, että rekisterinpitäjien ja henkilötietojen käsittelijöiden on jatkossa pääsääntöisesti pidettävä yllä selostetta sen vastuulla olevista käsittelytoimista. Tämä seloste tulee olla dokumentoitu kirjalliseen muotoon ja pyydettyäessä kyettävä toimittamaan viranomaisille (Oikeusministeriö 2017, 14).

#### 5.4.2 Standardit ja sertifiointi

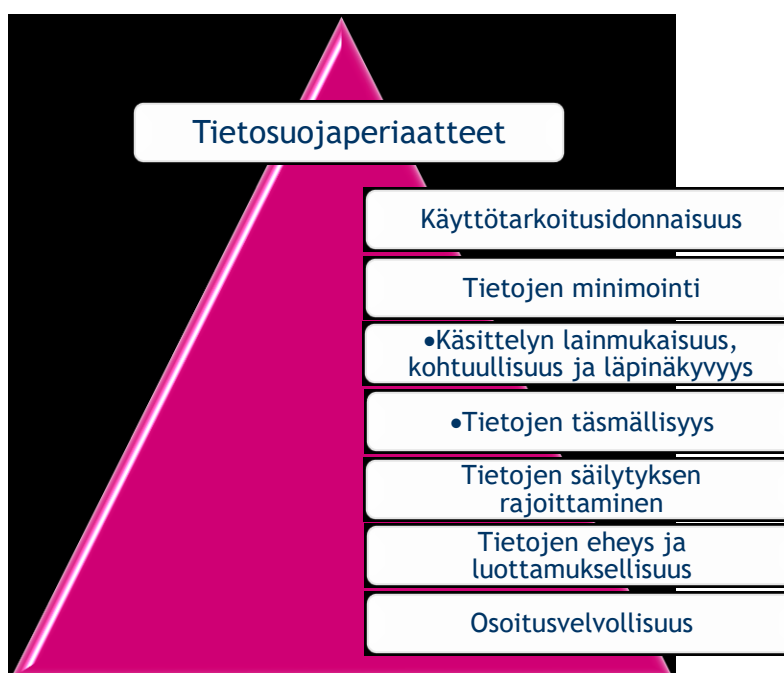
Yhtenä keinona osoitusvelvollisuuden toteuttamiseksi organisaatio voi sisällyttää toimintaansa asetuksen mukaisia tietosuojaa koskevia sertifikaatteja tai käytännesääntöjä, joiden avulla pystytään osoittamaan, että yrityksessä noudatetaan asetuksessa säädettyjä velvollisuuksia. Organisaatioille myönnettävien sertifikaattien hyötynä on myös, että se mahdollistaa rekisteröidyn kykenevän arvioimaan helposti tietosuojan tasoa yrityksen tuotteissa tai palveluissa. Alakohtaisilla käytännesäännöillä pystytään puolestaan helpottamaan asetuksen soveltamista käytäntöön, sillä niissä voidaan huomioida tietyillä aloilla suoritettavan käsittelyn erityispiirteet. Esimerkiksi erikokoisten organisaatioiden toimenpiteet sekä tarpeet henkilötietojen käsittelyn yhteydessä. Käytännesäännöt ja sertifiointit eroavatkin toisistaan siten, että sertifiointit ovat ulkopuolisten tahojen laatimia sekä hyväksymiä toimintatapoja, joita organisaatio voi vapaaehtoisesti sisällyttää omaan toimintaansa (Oikeusministeriö 2017, 14).

Tietoturvasuunnittelun jäsentämistä ja organisoimista varten on kehitetty kansainvälisiä ja kansallisia standardeja, joita yleisesti kutsutaan tietoturvastandardeiksi. Nämä ovat erityisen hyödyllisiä tietoturvasuunnittelun dokumentoinnissa ja tarjoavat selkeän sekä vertailukelpoisen rakenteen suunnittelussa muodostuneille dokumenteille. On kuitenkin tärkeää muistaa, että standardin noudattaminen ei yksin takaa riittävää tietoturvallisuutta vaan se ainoastaan määrittelee, mitä suunnittelutyöhön sisältyy ja missä muodossa tulokset esitetään. Standardit määrittelevät ne osa-alueet, jotka on huomioitava organisaation tietoturvallisuudessa, ylläpidossa sekä kehittämisessä. Standardit sisältävät suuntaviivat ja yleisperiaatteet tietoturvallisuuden hallintaan. Ne kuvaa, miten turvallisuuteen parantamiseen tähtäävät toimet käynnistetään ja toteutetaan sekä miten turvallisuushallintoa ylläpidetään ja kehitetään. Standardit eivät varsinaisesti anna valmiita määräyksiä, vaan toimivat yleisohjeena sekä ovat myös erittäin hyvä työvälineenä olemassa olevien tietoturvakäytäntöjen kattavuuden arviointiin. ISO:lla on työryhmiä, jotka laativat omaan alaansa liittyviä standardeja, jotka julkaistaan, kun vähintään 75% järjestön toimintaan osallistuvista kansallisista standardointielimistä on hyväksynyt standardiluonnoksen (Hakala, Vainio & Vuorinen 2006, 46-47, 50.)

Organisaatio voi halutessaan hakea todistusta tietoturvallisista toimintatavoistaan ja tätä toimenpidettä kutsutaan tietoturvallisuuden hallintajärjestelmän sertifiointiksi. ISO on määritellyt sertifiointissa vaadittavat kriteerit, jotka ovat kuvattuna ISO/IEC 27001 -standardissa. Virallisten ISO -standardien hankkiminen on maksullista, mutta silti suositeltavaa. Verkosta on saatavilla myös laadukkaita ilmaisia teoksia, joita organisaatio voi hyödyntää kattavan tietoturvadokumentin luomisessa. Tämänlaisia ohjeistuksia ja suosituksia tarjoaa muun muassa Valtiohallinnon VAHTI työryhmä, joka on julkaissut sivuillaan vapaasti luettavaksi tarkoitettua laadukasta materiaalia tietoturvallisuudesta. Mikäli yritys haluaa toteuttaa kattavan tietoturvadokumentin, voidaan se luoda esimerkiksi kirjaamalla ISO standardien pääkohdat tietoturvaperiaatteisiin ja -käytäntöihin. Vaikka tavoitteena ei olisi saada virallista sertifikaattia, niin on silti suositeltavaa tietoturvadokumenttia luodessa tutustua mahdollisimman useaan aiheeseen liittyvään dokumenttiin sekä ohjeistukseen. Hyödyllistä ohjeistusta sekä suosituksia ISO standardien lisäksi tarjoaa mm. edellä mainittu VAHTI, ISF (Information Security Forum) sekä Katakri. Katakri on viranomaisten auditointityökalu, jota voidaan hyödyntää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa.

### 5.5 Tietosuojaperiaatteiden toteuttaminen

Uudessa asetuksessa säädetään tietosuojaperiaatteista henkilötietojen käsittelyssä, jotka ohjaavat rekisterinpitäjää käsittelemään rekisteröidyn tietoja hänen oikeuksia ja vapauksia kunnioittavalla tavalla. Nämä periaatteet on esitetty kuviossa 2 ja ne vastaavat hyvin pitkälti periaatteita, jotka olivat voimassa henkilötietolain aikaan. Asetuksessa näistä tiettyjä kohtia on tarkennettu.



Kuvio 2. Tietosuojaperiaatteet

Jatkossa organisaation on huolehdittava, että näitä tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. On arvioitava, mitä periaatteet käytännössä tarkoittavat ja miten ne toteutuvat päivittäisessä toiminnassa. Periaatteiden noudattamisen osoittaminen vaatii jatkossa henkilötietojen käsittelyn aiempaa tarkempaa dokumentointia ja sen suunnittelua (Oikeusministeriö 2017, 12).

#### 5.6 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennettu tietosuojan periaate edellyttää, että yllä mainitut tietosuojaperiaatteet sisällytetään tehokkaasti henkilötietojen käsittelyä koskeviin toimiin niiden jokaisessa vaiheessa. Oletusarvoisen tietosuojan periaatteella tarkoitetaan, että rekisterinpitäjän tulee käsitellä vain kunkin henkilötietojen käsittelyn vaiheen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen käsittelyn laajuutta, määrää, säilytysaikaa sekä saatavilla oloa. Rekisterinpitäjän tulee toteuttaa ne toimenpiteet, jotka takaavat etenkin sen, ettei oletusarvoisesti tietoihin pääse käsiksi ulkopuolinen taho ilman niihin oikeutetun käsittelijän myötävaikutusta. Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden toteuttamiseksi organisaation tulee tunnistaa ja ottaa huomioon tietosuojaa koskevat kysymykset jo siinä vaiheessa, kun yrityksessä suunnitellaan henkilötietojen käsittelyä sisältäviä toimintoja tai kehitetään tietojärjestelmiä. Tietojärjestelmät tuleekin jatkossa jo lähtökohdaisesti rakentaa niin, että ne kykenevät noudattamaan asetuksen vaateita. Järjestelmän olisi kyettävä poistamaan tarpeettomia ja vanhentuneita tietoja sekä toteutettava muutenkin rekisteröityjen oikeuksia asetuksen edellyttämällä tavalla (Oikeusministeriö 2017, 13).

#### 5.7 Riskiperusteinen lähestymistapa

Asetuksessa on keskeisenä rekisterinpitäjän velvoitteiden määräytymisen osalta omaksuttu riskiperusteinen lähestymistapa, johon liittyy riskien arviointi ja ongelmien ennaltaehkäisy. Asetuksen velvoitteet ja asianmukaiset suojatoimet on suhteutettava henkilötietojen käsittelyssä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Tämän tarkoituksena välttää matalariskisen toiminnan ylisääntely ja kohdentamaan tarvittavat toimenpiteet henkilötietojen käsittelyssä siihen liittyvän riskin perusteella. Tietosuoja-asetuksen riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista (Oikeusministeriö 2017, 16).

Organisaation on toteutettava perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä, jotta kykenee toteuttamaan tietosuoja-asetuksen tavoittelemaa sisäänrakennettua ja oletusarvoista tietosuojaa ja muita asetuksessa säädettyjä velvollisuuksia. Asetuksessa riskeillä tarkoitetaan henkilötietojen käsittelyn yhteydessä rekisteröidylle mahdollisesti tapahtuvia fyysisiä tai aineellisia vahinkoja. Riskeillä tarkoitetaan myös mahdollisuutta aineettoon vahinkoihin, esimerkiksi silloin kun käsittely saattaa johtaa tietojen kohteena olevan

identiteettivarkauteen tai petokseen, taloudellisiin vahinkoihin, syrjintään tai pseudonymisoinnin (*henkilötietoja ei enää pystytä enää yhdistämään tiettyyn henkilöön ilman lisätietoja*) kumoutumiseen. Riski voi olla esimerkiksi korkeampi silloin, kun käsitellään erityisiä henkilötietoryhmiin kuuluvia tietoja tai heikossa asemassa olevien henkilötietoja (lapset, sairaat) tai arvioidaan rekisteröidyn henkilökohtaisia ominaisuuksia (analyysin muodostaminen). Myös korkean riskin kynnyks täytyy, kun käsitellään suuria määriä henkilötietoja tai käsittelytoimet koskevat suurta määrää rekisteröityjen tietoja (Oikeusministeriö 2017, 16).

Olenaisena osana sisäänrakennetun- ja oletusarvoisen tietosuojan käsitteisiin kuuluu myös määritellä henkilötietojen elinkaaren kulkua tietojen keräämisestä aina niiden poistoon saakka. Kuviossa 3 on havainnollistettu vaiheittain henkilötietojen elinkaari (Pietikäinen 2016).



Kuvio 3 - Henkilötietojen elinkaari

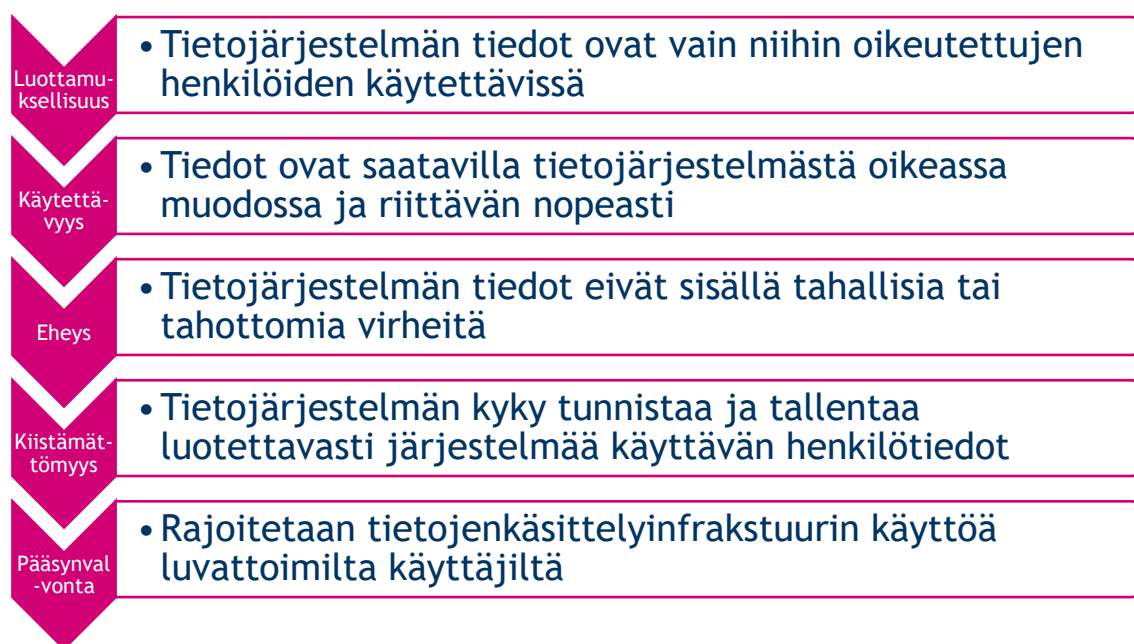
## 6 Tietoturvaluisuus

Tietosuoja on perustuslaillinen oikeutemme, joka takaa meille oikeuden elää elämäämme niin kuin tahdomme ilman kenenkään perusteetonta puuttumista siihen. Henkilötietolainsäädäntö osoittaa rekisterinpitäjälle ne rajat, joissa sillä on oikeus muun muassa käsitellä arkaluonteisia tietoja. Tietoturvalla halutaan määritellä tietosuojan näkökulmasta ne toimenpiteet, joilla saadaan turvattua sekä suojattua rekisteröidyn yksityisyys, edut ja oikeudet. Toisin sanoen tietoturvalla tarkoitetaan niitä toimenpiteitä, joilla taataan tietosuojan toteutus (Andreasson, Koivisto & Ylipartanen, 2013, 14).

Hieman laajemmin avattuna tietoturvaluudella halutaan suojata sekä varmistaa tietojen ja palveluiden, järjestelmien ja tietoliikenteeseen kohdistuvien riskien hallintaa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvaluuden tavoitteena on taata tietojen luottamuksellisuus, eheys ja käytettävyys laitteisto- ja ohjelmistovikojen sekä tahallisten, tarkoituksella tehtyjen tai tapaturmaisten tekojen ja tapahtumien aiheuttamilta uhilta ja vahingoilta. Tietoturvaluuden korkea taso ja laatu on yritykselle merkittävä sen asiakkaiden, toi-

minnan sekä julkisuuskuvan kannalta. Matala tietoturvallisuuden taso voi vaarantaa asiakkaiden ja yrityksen turvallisuuden sekä taloudelliset edut. Se saattaa myös aiheuttaa vahinkojen ja tiedon väärinkäytösten myötä lisätyötä ja -kustannuksia sekä heikentää yrityksen uskottavuutta (Valtiovarainministeriö, 2007, 7).

Valitettavan usein ajatellaan, että tietoturvallisuus on itsenäinen kehittämiskohde ja sen suunnittelu sekä kehittäminen tapahtuvat tietohallinnon ja it-ammattilaisten ehdoilla. Näkökulma turvallisuuteen jää kapeaksi ja lopputuloksena organisaatioon syntyy kaksi erilaista turvakulttuuria: erilliset käytännöt fyysisen turvallisuuden ja tietoturvallisuuden edistämiseksi. Kahden eri kulttuurin seurauksena rakennetaan todennäköisesti erillisiä järjestelmiä sekä käytänteitä huolehtimaan organisaation tietoturvallisuudesta. Lisäksi tehdään päällekkäisiä töitä ja osa ratkaisuista saattaa olla jopa ristiriidassa keskenään. Vaikka tietoturvallisuus on organisaation toiminnan sekä sen jatkuvuuden kannalta ensisijaisen tärkeä kehittämis- ja ylläpito-kohde, niin on myös hyvä huomioida, ettei se saa muodostua tärkeimmäksi tietojenkäsittelyä ja sitä kautta toimintaprosesseja ohjaavaksi toiminnoksi. Usein tietoturvallisuudesta vastaava taho haluaa luoda mahdollisimman kattavat ja jäykät turvallisuusmääritykset, jotka vaikeuttavat liikaa varsinaisen liiketoiminnan ydinprosessien hoitamista. Alan kirjallisuus ja eri organisaatioiden tuottamat tietoturvastandardit tarjoavat hieman toisistaan poikkeavia määritelmiä käsitteelle tietoturvallisuus. Laajennettu tiedon arvoon perustuvassa määritelmässä tietoturvallisuus koostuu viidestä osatekijästä, joita on avattu enemmän kuviossa 4. Nämä määritelmät lähtevät kuitenkin samasta perusajatuksesta, että yrityksen tärkein omaisuus on tieto, joka halutaan pitää organisaatiossa luotettavana, nopeasti, oikeassa muodossa ja ainoastaan oikeiden henkilöiden saatavilla (Hakala ym. 2006, 4-5, 14, 17.)



Kuvio 4: Tietoturvallisuuden osa-alueet

Tietoturvallisuuden koetaankin työyhteisössä usein olevan laaja ja vaikeasti hahmottava kokonaisuus, joka vain hankaloittaa ja hidastaa työntekoa. Kun tietoturvallisuus toteutetaan oikein, sen ei pitäisi vaikeuttaa käyttäjän toimintaa. Sen sijaan sen tulisi mahdollistaa ja tehostaa yrityksen liiketoimintaa, nykyisen ja uuden teknologian sekä palveluiden käyttämistä. Mikäli tietoturvallisuuden koetaan vain hankaloittavan yrityksen toimintaa, niin on syytä tarkistaa, onko yrityksen turvamekanismit toteutettu tarkoituksenmukaisesti ja suhteutettu uhkiin sekä riskeihin. Tietoturvallisuuden kehittäminen on osa yrityksen toimintaa siinä missä esimerkiksi liiketoiminnan kehittäminenkin.

### 6.1 Ulkoistaminen

Henkilötietojen käsittelyyn kuuluu riskejä, kuten kaikkeen inhimilliseen toimintaan. Niitä ei voi kokonaan poistaa, mutta niiden todennäköisyyttä voidaan pienentää sekä vaikutuksia lieventää. Niiden tapahtumiseen voi varautua siirtämällä vastuuta organisaation ulkopuolelle. Ulkoistamalla tietojenkäsittelytoimintoja niitä tuottaville palveluyrityksille on hyvä muistaa, että ulkoistettu riski on hoitamattomana yhtä vakava kuin se olisi omissa organisaatioissa. Jos riskejä siirretään oman organisaation ulkopuolelle, on yritysjohdon myös pystyttävä seuraamaan palveluntarjoajan toimintaan sekä otettava selvää sen tarjoaman turvallisuuden tasosta. (Hakala ym. 2006, 90).

Nykypäivänä organisaatioissa ulkopuolisia palveluntarjoajia otetaan ja integroidaan yhä enemmässä määrin mukaan toimintaan, niin yritysten on tiedostettava omien tietojensa kulku ulkoisten osapuolien keskuudessa sekä niihin kuuluvat riippuvuussuhteet. Mikäli yrityksen ulkoinen osapuoli ei suojaa riittävästi yrityksen tietoja tai omia tietojärjestelmiään, niin se tuottaa riskialttiutta. Ulkoiseen osapuoleen kohdistuvasta turvallisuushäiriöstä voi muodostua vakava rasite oman yrityksen toiminnalle, maineelle sekä brändin arvolle. Palveluntarjoajia kannattaa kehottaa ottamaan vähintään yrityksen omat tietoturvaperiaatteet käyttöönsä. On myös suositeltavaa suorittaa toimittajille auditointeja ja pyytää selvitys heidän omista tietoturvakäytännöistä toimintatapojen varmistamiseksi. Ulkoiset osapuolet eivät kuitenkaan ole pelkästään riskitekijöitä, vaan jotkin niistä voivat päin vastoin myös osaltaan vähentää riskejä ja auttaa yritystä saavuttamaan tärkeitä tietoturvariskien hallinnan tavoitteita. It-palveluntarjoajat voivat auttaa yrityksen tietoturvariskien infrastruktuuria tarjoamalla esimerkiksi turvallisuusarvioita ja -auditointeja sekä turvalaitteita, -ratkaisuja tai -palveluita (Keskuskauppa-kamari 2016, 11).

### 6.2 Riskien kartoitus

Riskien kartoitus on syytä aloittaa määrittelyllä siitä, mitä suojattavaa yrityksellä on, mitkä ovat sen toiminnalle tärkeitä suojattavia kohteita. Vasta tämän jälkeen on aika arvioida sitä, millaisia uhkia toiminnalle tärkeisiin asioihin kohdistuu. Tässä järjestyksessä toimittaessa on

yrityksen helppoa pitää tietoturvaluuustyö oman toimintansa näköisenä. Jos arviointi esimerkiksi aloitetaan uhista, niin on mahdollista, että suojautuminen ei ole suhteessa yrityksen toimintaa ja saattaa painottua väärin asioihin. Tavoiteltava yrityksen turvallisuuden taso määräytyy yrityksen näkemyksen mukaisesti. Yleensä organisaation sisällä on riittävä tieto siitä, mitä tarvitsee suojata ja millainen uhka siihen kohdistuu. Tämän jälkeen on helpompaa valita suojatut tavat. Niiden valikoimisessa ja laajuuden arvioinnissa voi olla suositeltavaa käyttää asiantuntijoita. Näin varmistetaan se, että organisaatiossa saavutetaan suojaa, joka mahdollisimman hyvin vastaa suojattavan arvon merkitystä yritykselle. Arvioitaessa suojattavia arvoja ei kannata pelkästään arvioida, minkä arvoinen jokin asia on taloudellisessa mielessä. On syytä huomioida myös, mitä arvon vahingoittuminen, väliaikainen toimintakyvyttömyys tai jopa tuhoutuminen aiheuttaisi yrityksen toiminnalle (Heljaste, Korkiamäki, Laukkala, Mustonen, Peltonen & Vesterinen 2008, 15).

Kuin muissakin tietoturva osa-alueiden kartoituksissa, niin riskejä arvioidessa on samalla tavalla suositeltavaa ottaa mahdollisimman paljon henkilöstöä. Vaikka samaa kohdetta arvioisi useampi työntekijä, saattavat he tuntea kohteen eri näkökulmasta. Näin saadaan ryhmätyöskentely menetelmällä mahdollisimman kattava tieto kohteen suojaustason tarpeista. On myös syytä käyttää riskien arvioinnissa useampia menetelmiä, koska yleensä yhtä menetelmää hyödyntämällä ei välttämättä löydy kaikkia uhkia. Löytyneistä riskeistä tulee tunnistaa tärkeimmät sekä priorisoida tärkeimmät kohteet, jotta nämä torjuttaisiin ensimmäisinä. Monessa tilanteessa on hyödyllistä pyrkiä arvioimaan tunnistettujen riskien suuruus sijoittamalla ne matriisiin, taulukkoon tai kaavioon, jossa on ylimpänä todennäköisimmät riskit ja alimpana epätodennäköisimmät. Tietosuoja-asetuksen lähtökohtana on, että riskejä tulisi arvioida niiden ihmisten näkökulmasta, joiden henkilötiedoista on kysymys. Millainen vahinko ihmiselle aiheutuu, jos heidän tietoihinsa ei enää ole pääsyä tai jos heidän yksityiset tietonsa päättyvät väärin käsiin tai julkisuuteen (Korpisaari 2018, 28).

Turvallisuusriskeihin liittyy kaksi puolta - uhkat ja haavoittuvuudet. Kun uhka kohtaa haavoittuvuuden tapahtuu tietoturvaloukkaus. Tietoturvaluuudessa riskit ovat aina olemassa, ne tulee tunnistaa ja pyrkiä ehkäisemään kehittämällä eri mekanismeja henkilötietojen suojaamiseksi. Näitä ovat erinäiset suoja- ja torjuntatoimenpiteet, jotka yrittävät estää mahdollisen hyökkäyksen tapahtumista ja torjua hyökkäyksen sen sattuessa. Haavoittuvuuksia korjataan siten, että hyökkääjä, joka läpäisee puolustuksen ei pääse tekemään vahinkoa organisaatiossa. (Axelord 2004, 11).

## 7 Tietoturvasuunnitelma

Ihmisillä, yrityksillä ja toimialoilla on usein hyvin vahvoja vallitsevia asenteita ja uskomuksia, jotka määrittävät niiden toimintaa ja jonka perusteella ne katsovat toimintaympäristöään. Usein yrityksissä esimerkiksi uskotaan, että yrityksen tuotteet ja palvelut ovat jo vuosia olleet riittävän hyvällä tasolla eikä ole tarvetta tehdä parannuksia jo voimassa oleviin jo totuttuihin

käytänteisiin. Ei välttämättä huomioida, että esimerkiksi vuosien saatossa henkilöstö on vaihtunut tai alati kehittyvä teknologia vaatii tietoturvallisuuden jatkuvaa perehdyttämistä, päivittämistä, seurantaa sekä ylläpitoa organisaatiossa (Lahtinen & Isoviita 2001, 21).

Uuden tietosuoja-asetuksen myötä organisaatioilla on ollut lähes pakko päivittää tietoturvasuutensa ajan tasalle, mutta se on myös saattanut lamaannuttaa toimintaa paikoittain sekä ollut haasteellista toteuttaa työyhteisössä. Organisaation hyvä tietoturvallisuus edellyttääkin pitkäjänteistä ja huolellista suunnittelua. Mitä laajemmin yrityksen henkilöstö osallistuu suunnitteluun, sitä parempia tuloksia sillä saavutetaan. Yrityksen kannattaa luoda erillinen dokumentti, joka sisältää tarkasti käytössä olevat tietoturvaratkaisut. Kyseisiä tietoja sisältävää dokumenttia kutsutaan nimellä tietoturvasuunnitelma, mutta nimi saattaa olla harhaanjohtava sillä dokumentti sisältää nykyisiä tietoturvan ylläpitämiseksi tehtyjä teknisiä ja hallinnollisia toimenpiteitä. Esimerkiksi valtiohallinnon työryhmä VAHTI käyttää nimitystä tietoturvakäytännöt ja -periaatteet. Tässä opinnäytetyössä on hyödynnetty ISO/IEC 27001 -sarjan dokumentointiohjeita, joita esitellään myöhemmin tietoturvasuunnitelman luvuissa. Huolella laadittu ja dokumentoitu tietoturvasuunnitelma voi toimia organisaation työntekijöiden ja sidosryhmien suorana ohjeena, kuinka yrityksessä tulee käsitellä henkilötietoja turvallisesti sekä oikeaoppisesti rekisteröidyn oikeuksia noudattaen. Samalla saadaan yhtenäisyyttä työskentelymenetelmiin sekä suoraa näyttöä siitä, että yrityksen johto on ottanut huomioon uuden tietosuoja-asetuksen vaateet toiminnassaan.

Yrityksen turvallisuusoppaassa muistutetaan vielä, että jokainen yritys on oman näköisensä ja siksi tietoturvallisuutta ei kannatta täysin kehittää muilta kopioituilla suunnitelmilla ja käytänteillä. Toki esimerkiksi standardeja sekä sertifikaatteja on syytä hyödyntää, mutta yrityksen tulee aina itse kantaa vastuu siitä, miten turvallisuutta kehitetään ja miten sitä tehdään yritykselle järkevällä tavalla (Heljaste ym. 2008, 12).

Tietoturvasuunnitelman toteuttaminen on mittava projekti, joka edellyttää kaikkien tietojärjestelmien sekä organisaation toimintojen kartoittamista. Uuden tai päivitettävän tietoturvasuunnitelman ja siihen liittyvän seurantajärjestelmän sekä ohjeistuksen luominen edellyttää projektin osittamista hallittaviin kokonaisuuksiin. Hyvä tietoturvasuunnittelu ottaa huomioon eri organisaatio tasoilla sekä tehtävissä toimivat henkilöt ja heidän tarpeensa. Tietoturvasuunnitelmaa ei pitäisi koskaan tehdä pelkästään tietohallinnon tai muun turvallisuudesta vastaavan elimen virkatyönä, koska heillä ei välttämättä ole riittävää kokonaisnäkemystä organisaatiosta ja sen eri toimintaprosesseista. Eri toimintojen riittävä huomiointi edellyttää siis niistä vastaavien ns. prosessin omistajien vahvaa osallistumista turvasuunnitteluun. Ruohonjuuritasolla työskentelevän henkilön mukaan ottaminen jo suunnitteluvaiheessa helpottaa myös turvallisuustiedon levittämistä organisaation jokaiselle tasolle. He voivat samalla toimia lieventämässä muutos vastarintaa, jota muutokset saattavat tuottaa työyhteisössä. Muutos vastarintaa saattaa syntyä esimerkiksi silloin, kun suunnittelu johtaa merkittäviin muutoksiin



turvallisuuskäytännöissä sekä vaikuttaa työntekijöiden rutiineihin. Suunnitelman valmistumisen jälkeen projektimuotoinen työskentely päättyy, mutta turvallisuuden ylläpito ja kehittäminen jatkuvat (Hakala ym. 2006, 18, 22.)

### 7.1 Tietoturvapoliittika

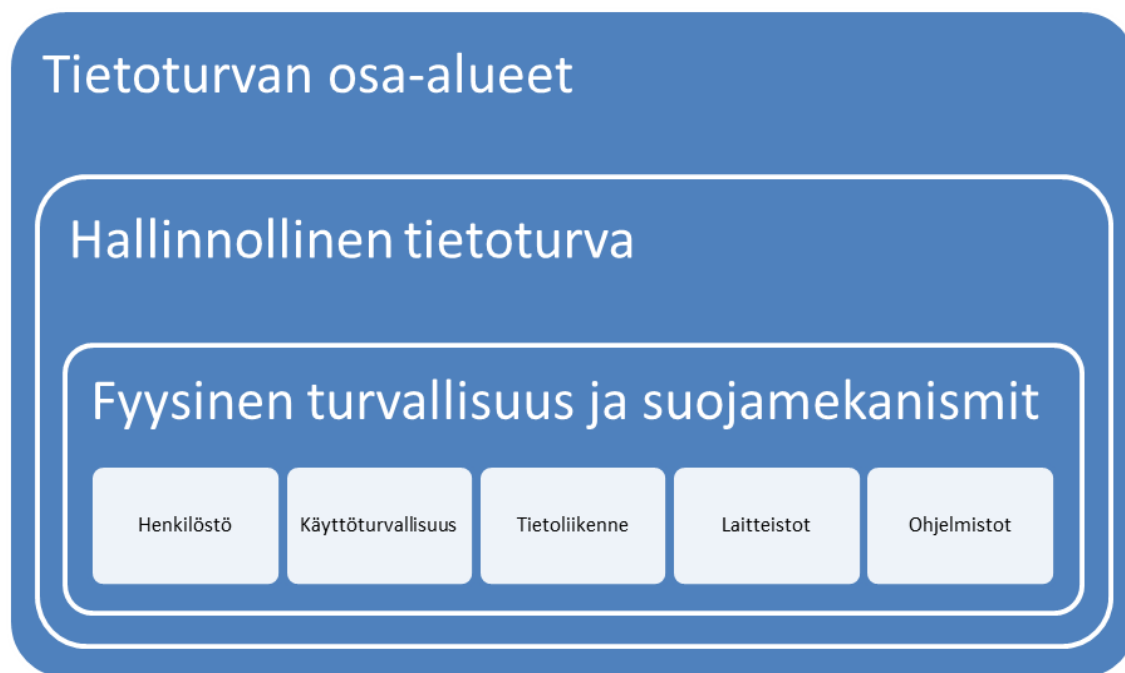
Tietoturvasuunnitelman yhtenä tavoitteena on luoda yritykselle toimiva tietoturvapoliittika (Information security policy), joka muodostaa suurimman osan organisaation turvallisuuden tasosta. Tämän huolella suunnittelu ja toteuttaminen luo hyvän pohjan tietoturvan tasolle yrityksessä ja sen vaiheet ovat välttämättömiä tietoturvallisuuden hallinnassa. Kehittäessä tietoturvallisuutta pitkäjänteisesti tulee organisaatiossa olla yritystä varten tehty ja johdon allekirjoittama tietoturvapoliittika, jossa määritellään turvallisuusasteet aina johdosta työntekijöihin saakka. Organisaation kaikkien tasojen johtajien on varmistettava, että heidän henkilöstönsä ymmärtävät turvallisuuspolitiikan käytänteet ja noudattava niitä jatkuvasti työssään (Vacca 2013, 60, 62.)

Tällä asiakirjalla johto osoittaa sitoutumisensa tietoturvallisuuteen sekä velvoittaa yrityksen muita työntekijöitä osallistumaan tietoturvallisuuden ylläpitoon. Tietoturvapoliittikalla saadaan tarvittavaa tukea työntekijöiden toimintaan tietoturvallisuuteen liittyen. Asiakirja voi olla vaikka vaan yhden sivun mittainen, mutta se luo organisaatiolle toiminnan oikeutuksen. Johdon sitoutuminen tietoturvallisuuteen on aina merkittävää. Jos esimerkiksi yrityksen toimitusjohtaja vähättelee ja laiminlyö tietoturvallisuutta, niin tällä on heikentävä vaikutus muiden työntekijöiden toimintaan tietoturvallisuuden osalta (Heljaste ym. 2008, 12).

Tietoturvapoliittika muodostuu organisaation johdon hyväksymistä käytännöistä ja ohjeista, joiden avulla haluttu tietoturvallisuuden taso saavutetaan. Se laaditaan yleisellä tasolla kuvaamaan, mikä on organisaation eri liiketoimintaprosessien edellyttämä tietojen turvaamisaste, millä menetelmillä haluttuun turva tasoon voidaan päästä ja miten tietoturvallisuutta ylläpidetään ja kehitetään. Tietoturvasuunnitelman laatimisesta vastaavat organisaation turvallisuudesta huolehtiviin elimiin kuuluvat henkilöt yhdessä tietohallinnon, tietojenkäsittelyn ja tietotekniikan ammattilaisten kanssa. Suunnitelma pyritään yleensä laatimaan keskipitkälle aikavälille (2-5 vuotta) sekä sen lähtökohtina ovat pidempiaikaisen tietoturvapoliittikan asettamat suuntaviivat ja reunaehdot. Organisaation toimintaprosesseissa sekä uuden teknologian käyttöönotossa tapahtuvat muutokset edellyttävät tietoturvasuunnitelman jatkuvaa päivittämistä ja suunnitelmaa onkin syytä tarkistaa vähintään vuosittain. On myös suositeltavaa tarkistaa tietoturvasuunnitelmaa aina, kun organisaation tietojärjestelmissä tai työmenetelmissä tapahtuu olennaisia muutoksia (Hakala ym. 2006, 7,9.)

Hallinnon on pidettävä huolta, että tietoturvasuunnittelu on tietohallintatavan mukaista perustuen selvityksiin ja arvioihin organisaation hallussa olevista asiakirjoista sekä niihin tallennet-

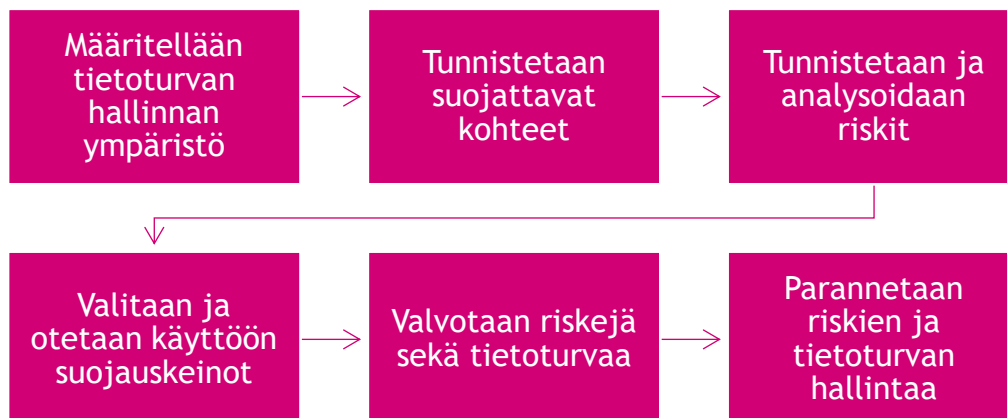
tujen tietojen merkityksestä. Suunnittelussa on otettava myös huomioon vaatimus hyvän julkisuus- ja salassapitorakenteen toteuttamisesta tietojärjestelmissä (Ohje tietoturval- lisuudesta 2010, 8). Tietoturvallisuuden kokonaisuus halutaan usein pilkkoa helpommin käsiteltä- viin osiin, joiden avulla myös pystytään dokumentoimaan tarvittavat toimenpiteet tietoturval- lisuuden osalta.



Kuvio 5: Tietoturvallisuuden kokonaisuus

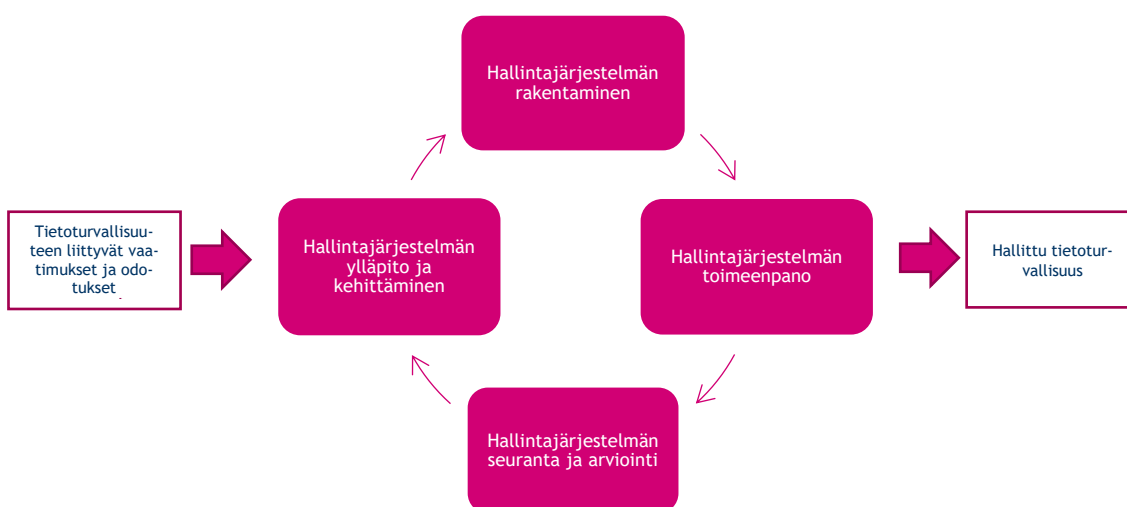
## 7.2 Tietoturvan hallintajärjestelmä ISMS

Yritysjohdon tietoturvatyön organisoimiseksi sekä avuksi kannattaa organisaatiossa luoda erilinen tietoturvan johtamis- ja hallintajärjestelmä ISMS (*Information Security Management System*). Tietoturvallisuuden hallinta perustuu hallinnon tietoturvallisuudelle asettamiin vaatimuksiin sekä riskien tunnistamisesta lähtevään tietoturvallisuuden jatkuvaan kehittämiseen. Hallintajärjestelmän kulun vaiheet on havainnollistettu kuviossa 6, jonka suunnitteleminen ja käyttöönotto kannattaa aloittaa tavoitteiden määrittelyllä. Onnistuneeseen tietoturvaan yrityksessä päästään tiedostamalla ensin se, mitä pitää suojata. Nämä voivat olla esimerkiksi IT-järjestelmiä tai fyysisiä dokumentteja ja määrittelyn tavoitteena on tunnistaa yrityksen kannalta tärkeimmät turvattavat asiat. Kun suojattavat kohteet on dokumentoitu, niin ne pitää vielä luokitella kriittisyyden mukaan, jotta liiketoiminnan kannalta tärkeimmät kohteet turva- taan aikajärjestyksessä (Hakala ym. 2006, 106).



Kuvio 6: Tietoturvan johtamis- ja hallintajärjestelmän kulun vaiheet

Järjestelmän tulisi kattaa kaikki tietoturvan johtamisessa, hallinnoimisessa ja valvonnassa tarvittavat menettelyt ja toimenpiteet. Hallintajärjestelmä ei ole vain yksittäinen dokumentti, vaan tietoturvallisuuden hallinta ja johtaminen nähdään prosessina, jossa tietoturvallisuuden hallintajärjestelmää kehitetään jatkuvasti vastaamaan organisaation toiminnan ja toimintaympäristön muutosten aiheuttamiin turvallisuustarpeisiin. Prosessiajattelun lähtökohtana on PDCA (Plan-Do-Check-Act) -prosessimallin sisältämät tehtävät voidaan jakaa neljään osaa, jonka soveltamista tietoturvallisuuden hallintajärjestelmään on kuvattu kuviossa 7. Suunnitteluvaiheessa (Plan) prosessi käynnistetään ja tehdään liiketoimintavaikutus - ja riskianalyysit sekä muodostetaan näiden pohjalta jatkuvuusstrategia. Toteutusvaiheessa (Do) suunnitellut ratkaisut toteutetaan ja aloitetaan koulutus henkilöstölle. Tarkistusvaiheessa (Check) prosessin tilasta tuotetaan tietoa valvonnan, testauksen, katselmointien ja auditointien sekä raportoinnin avulla. Kehitysvaiheessa (Act) ratkaisuja parannetaan kerättyjen tietojen perusteella. Kehittämisykli vaatii aktiivista toimintaa ja sen tarkoituksena on johtaa toiminnan jatkuvaan parantamiseen (Hakala ym. 2006, 106; VAHTI 3/2007, 38-39.)



Kuvio 7: PDCA-mallin soveltaminen tietoturvallisuuden hallintajärjestelmässä

### 7.3 Hallinnollinen turvallisuus

Yrityksen tietoturvalliset toimintatavat tarvitsevat johtamista sekä kehittämistä siinä, missä muutkin yleiset liiketoiminnan prosessit. ”Hallinnollisella turvallisuudella pyritään varmistamaan tietoturvan kehittäminen ja johtaminen” (Hakala 2006, 10). On tärkeää sisällyttää tietoturvalliset toimintatavat päivittäisiin prosesseihin, jolloin pidetään huolta siitä, että tietoturva huomioidaan päivittäisessä työskentelyssä niin työntekijöiden kuin yritysjohtajien tasolla. Hallinnollisella tietoturvalla määritellään menettelytavat muiden tietoturvan osa-alueiden ohjaamiseen sekä kehittämiseen ja tietoturvan johtamista pidetäänkin yleisesti hyvin laajana käsitteenä. Yrityksen johdon ei välttämättä silti tarvitse tehdä kuin se tärkein eli varmistaa, että yleiset toimintatavat ovat lainsäädännöllisesti oikein. Tavoitteena on varmistaa, että kaikki tietoturvan osa-alueet ovat tarpeeksi hyvällä tasolla sekä sen näkyvimpiä tuotoksia ovatkin henkilöstön organisointi, yleiset linjaukset, ohjeistukset sekä erilaiset dokumentit, kuten tietoturvapoliittikka. Tärkeimmät hallinnollisessa turvallisuudessa huomioitavat ja dokumentoitavat asiat on esitelty taulukko 1:ssä.

Aihe	Kuvaus
Nykytilan kartoitus	Tunnistetaan tietoturvan nykyinen taso, kehityskohteet ja lainsäädännön vaikutukset toimintaan
Riskienhallinta	Sisäisten ja ulkoisten riskien kartoitus ja analysointi
Yritysjohtajan osallistuminen	Sitoutuminen tietoturvatyöhön ja tarvittavien resurssien osoittaminen
Tietoturvapoliittikka	Laaditaan yrityksen toimintaa ohjaava tietoturvapoliittikka
Vastuualueet, organisointi ja viestintä	Nimetään erityisesti tietoturvasta vastaavat henkilöt. Sovitaan viestintä- ja raportointi käytännöistä
Tietoturvaohjelman laatiminen	Laaditaan tarpeeksi kattavan ohjeistuksen ja koulutuksen tarjoaminen työntekijöille. Päämääränä on tietoturvatietouden lisääminen ja ohjeiden kehittäminen
Sopimukset	Tietoturva-asioista mainitseminen henkilöstöön, asiakkaisiin tai ulkoistukseen liittyvissä sopimuksissa
Suunnitelmat	Jatkuvuus-, toipumis- ja tietoturvan kehittämissuunnitelmien laatiminen ja ylläpito

Taulukko 1: Hallinnollisen turvallisuuden dokumentaatio (ISO/IEC 27001:fi 2006, 32-34; ISF 2007, 15-23)

#### 7.4 Henkilöstöturvallisuus

Henkilöstöturvallisuudella määritellään ne toimet, joilla sekä varmistetaan yrityksen tietojärjestelmien käyttäjien turvallinen toiminta tietojen käsittelyssä sekä mahdollisesti rajataan heidän mahdollisuuksiaan käyttää organisaation tietoja tai tietojärjestelmiä (Hakala ym. 2006, 11).

Internetin uutispalstoilla on tänä päivänä luettavissa useasti erilaisia tietoturvaluutisia. Aiheet vaihtelevat tietomurtotapauksista haittaohjelmien leviämiseen verkossa. Yrityksiin kohdistuvista tietoturvahyökkäyksissä yhteinen tekijä on lähes aina ihmisen rooli. Nykyaikaiset käyttöjärjestelmät ovat niin kehittyneitä, että niihin harvemmin pääsee käsiksi suoraan taho, jolla ei ole käyttöoikeuksia järjestelmään. Yrityksissä työskentelee usein sellaisia henkilöitä, joiden tietoturvaton työskentelytavat helpottavat näiden tahojen toimintaa. Tämänlainen henkilö voi olla esimerkiksi tietojärjestelmän pääkäyttäjä tai ylimmän johdon työntekijä, joita yhdistää pääsy kriittisiin tietoihin, kuten henkilötietoihin tai palvelinhuoneisiin. Tehokkaimmista suojaohjelmat tai palomuurit eivät aina pysty estämään työntekijän tekemää tahallista tai tahatonta virhettä henkilötietojen käsittelyn yhteydessä. Inhimillisten virheiden avulla oikeudettomat tahot pystyvät tuottamaan yritykselle huomattavaa vahinkoa sekä liikeloudellisia seuraamuksia. Mikäli yrityksen työntekijä esimerkiksi avaa haittaohjelmalla varustetun sähköpostitiedoston, voi se samalla antaa ulkopuoliselle taholle mahdollisuuden päästä käsiksi yrityksen asiakkaiden henkilötietoihin tai muuten muihin salassa pidettäviin tiedostoihin (Laaksonen & Nevasalo 2006, 139-140.)

Henkilötietojen tietoturvalisen käsittelyn tärkeyttä ei siis pidä väheksyä ja siksi on tärkeää saada henkilöstö ymmärtämään tietoturvan merkitys koko organisaation toiminnalle. Henkilöstölle tulee ohjeistaa tietojen turvallista käsittelyä ICT-työvälineiden käytön yhteydessä (tietokone, tabletti, älypuhelin), palveluissa (sähköposti, internet, sosiaalinen media) sekä työtehtävissä. Esimerkiksi miten ja minne tietoja tallennetaan, luovutetaan, lähetetään sähköpostilla tai hävitetään. Mikäli työntekijä käsittelee työtehtävissään salassa pidettäviä tietoja, niin tulee hänelle olla selvitetty tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt. Koska työnteko tapahtuu yhä useammin organisaation ulkopuolella, tulee tietoturvalisesta työskentelystä ohjeistaa niin työpaikalla, työmatkalla, kotona sekä missä muualla työntekijä suorittaaakin työtehtäviään. Ohjeistusta laatiessa on hyvä kartoittaa kunkin työntekijän tietoturvalisuuden vaatimuksien taso hänen työtehtäviinsä perustuen. On kuitenkin syytä muistaa, että kaikki työntekijöitä koskevat kuitenkin yhtenäiset työskentelytavat tietoturvalisuuteen liittyen. Pitämällä säännöllisesti tietoturvakoulutuksia sekä jakamalla ohjeistusta tietoturvasta voidaan parantaa henkilöstön tietoturvalisuutta ja tämä on oleellinen osa-alue ylläpitää henkilöstön ammattitaitoa henkilötietojen käsittelyssä. Turvalisuusdokumentaatiolla saadaan yhtenäisyyttä työskentelymenetelmiin sekä sillä pyritään ehkäisemään,



Aihe	Kuvaus
Roolit ja vastuut	Henkilöstölle on selkeästi määriteltävä omat vastualueensa ja varahenkilökäytännöt. Pyritään välttämään tietoturvan kannalta vaarallisia työyhdistelmiä
Tietoturvapoliittikka	Tietoturvapoliittikan hyväksyminen ja sen mukainen toimiminen ovat olennainen osa henkilöstön tietoturvallista työskentelyä.
Työsuhteen alkaminen ja päättymisen	Kuvataan ne toimenpiteet, jotka on tehtävä aina, kun yritykseen tulee uusi työntekijä tai joku eroaa tehtävästään
Tietoturvakoulutus	Ilman kunnollista koulutusta ei voida olettaa, että henkilöstö osaa työskennellä tietoturvallisesti. Dokumentoidaan työntekijöiden tietoturvatietouden lisäämiseksi tehdyt toimet
Ulkoistaminen	Tietoturva-asioista huolehtiminen on oleellista myös ulkoistamisessa. Kirjataan ne toimenpiteet, joilla varmistetaan muualta hankitun palvelun tietoturvan taso

Taulukko 2. Henkilöstöturvallisuuden dokumentaatio (ISO/IEC 27001:fi 2006, 36; ISF 2007, 16-17)

## 7.6 Fyysinen turvallisuus

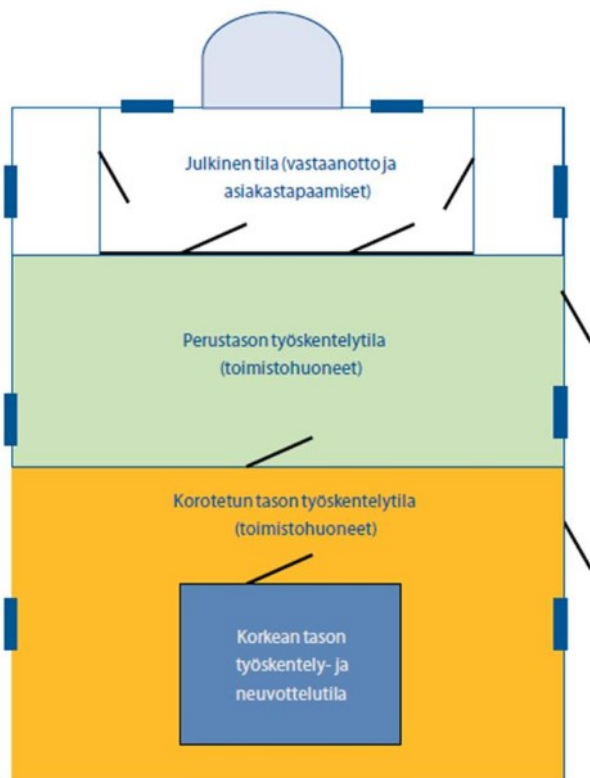
Yrityksen toimitilojen sekä niissä sijaitsevien laitteiden suojaamista tietoturvallisuudessa kutsutaan yleisesti nimellä fyysinen turvallisuus. Esimerkiksi mikäli tärkeitä tietoja sisältävää palvelinta ei ole fyysisesti turvattu, niin sen eheyttä, luottamuksellisuutta ja saatavuutta ei voida varmistaa. Tämänlaisia uhkia voi olla toimitiloissa sattuvat tuli-, vesi- tai sähkövahingot, jotka saattavat vaurioittaa tai tuhota tietokoneita sekä varmuuskopioita. Fyysisten turvatoimien tarkoituksena on myös estää sekä ehkäistä luvaton taho tunkeutumasta salaa tai väkisin yrityksen tiloihin, joissa käsitellään salassa pidettävää tietoa. Fyysisessä tietoturvassa kokonaisvaltainen suojaaminen on tehokkaampaa, kuin pelkkään tiettyyn toimialueeseen kohdistetut suojoimenpiteet. Esimerkiksi palvelinhuoneen turvan tasoon vaikuttaa myös sen ympärillä olevien muiden toimitilojen turvallisuus. Kun työntekijöiden päivittäinen työympäristö saadaan suojattua, voidaan keskittyä myös muihin osa-alueisiin tietoturvan suunnittelussa ja kehittämisessä. (Laaksonen ym. 2006, 125-127.)

### 7.6.1 Turvallisuusvyöhykkeet

Olellainen osa tietoturvallisuuden kokonaishallintaa on yrityksessä saavuttaa sellainen turvallinen työympäristö, joka vastaa keskeisiltä osiltaan tunnistettuihin uhkiin. Organisaation toimitilat voidaan rajata turvallisuusvyöhykkeisiin, joiden ulkokuoriin ja niiden kulkuaukkojen turvallisuuteen kohdistuu erityisiä vaatimuksia. Vyöhykemäärittelyyn vaikuttavat olennaisesti

riskianalyysin pohjalta tehdyt uhka-arviot ja salassa pidettävän tiedon suojaustason vaatimukset. Määrittelyyn vaikuttaa myös, että käsitelläänkö vyöhykkeillä tietoa sähköisesti, paperein vai suullisesti. Tulee arvioida minkä suojaustason tietoja milläkin vyöhykkeellä käsitellään ja säilytetään sekä miten kunkin työskentelypisteen sijoittaminen täyttää sille asetetut tietosuoja-vaatimukset. Organisaation tulee luokitella tekemänsä riskiarvioinnin perusteella hallinnsaan olevat alueet ja niissä sijaitsevat alueet ja toimitilat. Luokittelun perusteella voidaan laatia vyöhykekartta, johon merkitään alueet ja toimitilat sekä niissä käsiteltävän ja/tai säilytettävän tiedon suojaustason vaatimukset. Kuviossa 8 on luotu perusajatus esimerkki vyöhykekartan mallinnuksesta (Pietikäinen 2013).

Turvallisuusvyöhykkeet voidaan erottaa toisistaan esimerkiksi väritunnuksin. Värikoodit voidaan myös halutessaan merkitä henkilökortteihin, jolloin ne osoittavat kulkuoikeuden eri turvallisuusvyöhykkeille. Työntekijöiden sekä ulkopuolisten vierailijoiden kulkua sekä liikkumista turvallisuusvyöhykkeiden toimitiloissa voidaan seurata ja rajata teknisin keinoin. Tämä kulunvalvonnaksi kutsuttu aihealue on osa suurempaa kokonaisuutta, kulunhallintaa. Kulunhallinnan tehtävänä on johtaa, kehittää ja ylläpitää valvonnassa käytettyjä menetelmiä sekä toimintatapoja. Esimerkiksi yrityksen työntekijän kulkuoikeuksia päätetään kulunhallinnassa, mutta kulunvalvonta sisältää keinot, joilla työntekijän liikkumista toimitiloissa rajoitetaan (Pietikäinen 2013).



Kuvio 8. Turvallisuusvyöhykkeiden mallinnuskartta



Esimerkiksi julkisten asiakirjojen käsittely ei vaadi käsittely-ympäristöltään erityisiä turvallisuustoimia sekä tämä pätee myös tilaan, missä säilytetään ja käsitellään satunnaisesti heikoimman suojaustason tietoja. Tässä käsitteellä ”tila” tarkoitetaan joko yksittäistä huonetta tai niistä muodostuvaa kokonaisuutta ja tilojen lukituksen pitäisi olla toteutettu niin, ettei alueelle pääse oikeudettomia tahoja. Lukitusta onkin keskeisimpiä vyöhykejaon mahdollistavia tekijöitä ja se toimii yhtenä kulunvalvonnan elementtinä yrityksessä. Turvallisuusvyöhykkeelle saapuvan henkilön tunnistamista edellytetään perustasolta lähtien sekä korkeimpien tasojen vyöhykkeille ei tule olla pääsyä ilman siihen myönnettyä oikeutta ja sähköistä kulunvalvontaa. Korkeammilla turvallisuus tasoilla henkilön liikkumista on suositeltavaa valvoa loki-kirjauksilla. Mikäli jokin vaatimuksista jää täyttymättä, voidaan puute korvata esimerkiksi varustamalla ympäröivä alue kameravalvonnalla, muilla ilmaisimilla tai muilla korvaavilla järjestelyillä. Tämä ehkäisee osaltaan myös luvaton tunkeutumista ja näin itse toimitiloihin kohdistuu vähemmän suojausvaatimuksia. Korvaavilla menettelyillä voidaan lisäksi joissakin tapauksissa saavuttaa huomattavia kustannussäästöjä. Toimitilavyöhykkeitä määrittäessä on myös syytä pohtia toimitilan suojaustason tarvetta muutenkin kuin riski- ja uhka-arvioiden pohjalta. Voiko salassa pidettävän tiedon käsittelyä siirtää vain tietyille alueille? Voidaanko muokkaamalla työprosesseja vähentää tai poistaa kokonaan joidenkin turvallisuusvaatimusten tarvetta? Vaatimusten toteuttamiseksi on usein löydettävissä vaihtoehtoisia ratkaisumalleja (Pietikäinen 2013).

#### 7.6.2 Laitteistoturvallisuus

Yrityksen teknisten laitteiden suojaamista kutsutaan laitteistoturvallisuudeksi. Henkilöstön perehdyttäminen tärkeiden kohteiden, kuten kannettavien tietokoneiden, palvelimien, tulos-timien sekä matkapuhelimien laitteistopolitiikkaan on sekä muihin yleisiin ohjeisiin on merkittävää tietoturvan kannalta. Useasti ei välttämättä tiedetä, että esimerkiksi hajonneen tietokoneen kovalevyn sisältö saattaa olla luettavissa, vaikka kone itsessään ei olisi toimiva. Tärkeimmät fyysisessä tietoturvassa huomioitavat ja dokumentoitavat asiat on esitelty taulukossa 3.

Aihe	Kuvaus
Turva-alueiden määrittely	Jaetaan toimitilojen alueet tärkeyden mukaan erilaisiin turva-alueisiin
Suojaaminen	Otetaan käyttöön ja kirjataan eri alueiden suojaustoimenpiteet, kuten kulunvalvonta, murtohälyttimet tai paloturvallisuuteen vaikuttavat tekijät
Kouluttaminen	Huolehditaan henkilöstön osaamisesta fyysisen tietoturvan suojaamisessa. Laaditaan ohjeita erilaisten laitteiden ja tapahtumien hallintaan.
Riskitekijät	Mikäli IT-tiloissa on riskitekijöitä, kuten vesipisteitä, on ne otettava huomioon tietoturvallisuuden näkökulmasta.

Taulukko 3. Laitteistoturvallisuuden dokumentaatio (ISO/IEC 27001:fi 2006, 36; ISF 2007, 16-17)

### 7.7 Ohjelmistoturvallisuus

Alati kehittyvässä ja kansainvälistyvässä ympäristössämme yrityksen sitoutuminen tietoteknologiaan kasvaa jatkuvissa määrin, jolloin samalla yrityksen riippuvuus tietotekniikan luotettavuudesta, toimintavarmuudesta sekä jatkuvasta käytettävyydestä korostuu entisestään.

Tietojärjestelmissä käytettävien ohjelmistojen ja lisenssien hallintaa kutsutaan nimensä mukaisesti ohjelmistoturvallisuudeksi. Olennaista ohjelmistoturvallisuuden kannalta on ohjelmien ja järjestelmien luvattoman käyttämisen estäminen. Yleisimpiä tapoja toteuttaa tämä suojaustoimenpide on varmasti käyttäjän todentaminen henkilökohtaisen tunnistautumisen tai salasanan avulla. Yksinkertaiset ja tietyn tyyppiset salasanat ovat kuitenkin helposti murrettavissa ja yrityksen tietoturvaohjeistukseen kannattaakin lisätä kohta, jossa kerrotaan turvallisten ja monimutkaisten tunnuksien luomisesta. Käyttäjän on myös hyvä tietää mitkä ohjelmistot ovat turvallisia sekä mitä niistä hänen on lupa asentaa ja käyttää tietokoneillaan. Huonosti toteutetut sekä heikot ohjelmat ovat haitaksi yrityksen tietoturvalle, koska luvattoman käytön estäminen oikeaoppisilla salasanoilla ei ole avuksi, jos käyttäjä pystyy ohittamaan todennusmekanismit. Turvallinen ohjelmisto myös mahdollistaa loki- ja tapahtumatietojen kirjaamisen muistiin. Esimerkiksi näin voidaan selvittää, että kuka käyttäjä on ollut kirjautuneena järjestelmään tiettyinä ajankohtana tai miltä laitteelta kyseinen kirjautuminen on tehty. Nämä tiedot saattavat olla erityisen hyödyllisiä ongelmatilanteiden selvittämisessä (Pietikäinen 2016).

Lisenssien hallinta ei välttämättä kuulosta tärkeältä tietoturvallisuuden kannalta, mutta tämän osa-alueen laiminlyönti voi silti johtaa vakaviin tietoturvaloukkauksiin. Esimerkiksi virus-torjuntaohjelmiston lisenssin käyttöoikeudesta luopuminen voi samalla lopettaa itse ohjelman toimimisen ja päästää asiaan kuulumattoman tahon murtautumaan organisaation salassa pidettäviin tietoihin. Tärkeimmät ohjelmistoturvallisuudessa huomioitavat ja dokumentoitavat asiat on esitelty taulukossa 4.

Aihe	Kuvaus
Inventaario	Kirjataan yrityksessä käytössä olevat ohjelmistot sekä niiden versiot ja lisenssit. Jokaiselle ohjelmistolle olisi hyvä merkitä myös vastuhenkilö
Ohjelmistopolitiikka	Listataan yrityksessä sallitut ohjelmistot
Ohjelmistodokumentaatio	Dokumentoidaan ohjelmiston ominaisuuksien, resurssien, käyttöoikeuksien sekä -ohjeet. Myös ohjelmistoihin tehdyt muutokset olisivat suositeltavaa dokumentoida
Haittaohjelmilta suojautuminen	Kuvataan toimenpiteet, joilla yritys suojautuu esimerkiksi viruksilta. Henkilöstöä on ohjeistettava kirjallisesti / suullisesti ohjelmistojen turvallisesta käytöstä, päivityksien asentamisesta sekä esimerkiksi arkaluontoisten tietojen salaamisesta
Järjestelmien kuvaukset	Esimerkiksi palvelinympäristön tietoturvan lisäämiseksi tehdyt asetusmuutokset on dokumentoitava ja ohjeistettava ylläpitäjälle
Varmuuskopiointi	Varmuuskopiointikäytännöt ja niiden ohjeistukset on dokumentoitava ja tarpeen mukaan julkaistava myös henkilöstölle
Sopimukset	Dokumentoidaan mahdolliset ohjelmistoihin liittyvät tukisopimukset ja niihin liittyvät avunpyyntöperiaatteet

Taulukko 4. Ohjelmistoturvallisuuden dokumentaatio (ISO/IEC 27001:fi 2006, 29-31, 48-62; ISF 2007, 16-17)

## 8 Case - yritys X

Työpaikallani tehtiin keväällä 2019 yhteistyössä ulkopuolisen toimijan kanssa tietoturvakartoitus, jolla selvitettiin organisaation tietoturvallisuuden eri osa-alueiden nykytila. Kartoitus tehtiin haastatteleamalla yritysjohtoa, eri osastojen työntekijöitä ja myös ulkopuolisia sidos-

ryhmiä, kuten palvelumme tarjoajaa. Haastattelulla selvitettiin nykyiset käytänteet ja toiminnallisuudet tietoturvasa. Kartoituksen osa-alueet ovat havainnollistettu kuviossa 9. Kartoituksen perusteella syntyneessä dokumentissa kuvataan, miten yrityksen toimintaympäristössä on toteutettu tietoturvan hallintomenetelmiä sen eri osa-alueilla ja mahdollistaa kehityskohteiden tunnistamisen. Dokumentissa eri osa-alueiden turvallisuuden taso oli havainnollistettu ”liikennevalo” -menetelmällä, jossa kehitystarpeet priorisoidaan joko vihreän, keltaisen tai punaisen valon saaneina.



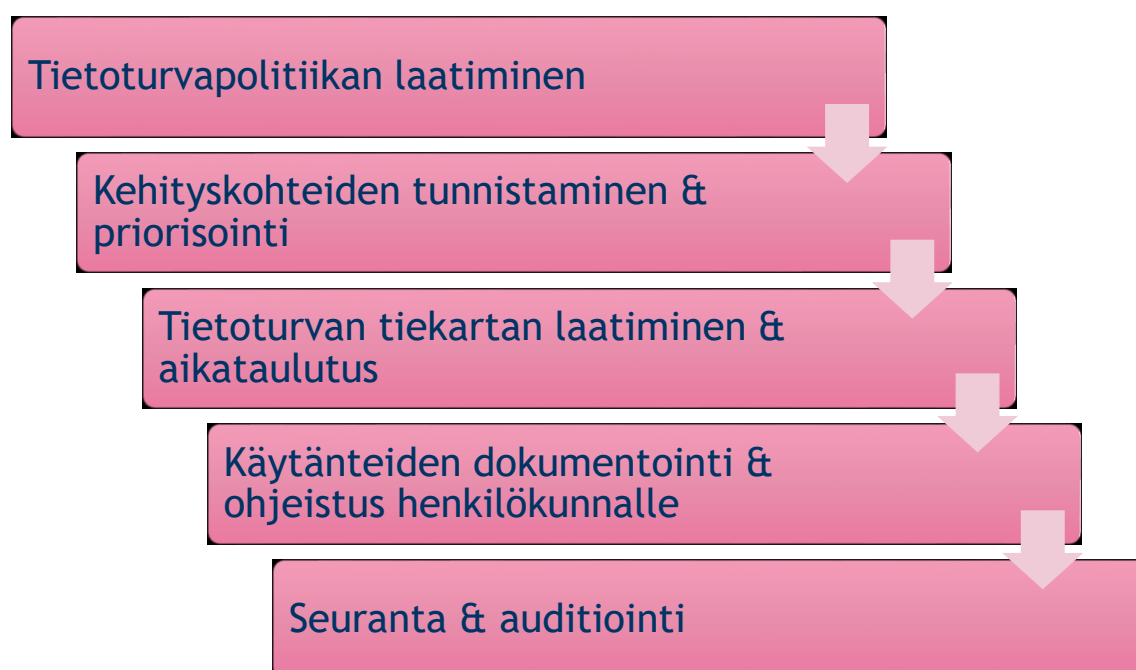
Kuvio 9: Tietoturvakartoituksen osa-alueet

Tietoturvakartoituksen pohjalta työpaikallani lähdetään kehittämään organisaation tietoturvaa, jonka prosessin vaiheet on alustavasti kuvattu kuviossa 10. Kesän 2019 aikana organisaatiossa on tavoitteena luoda yrityksen johdon kanssa yhdessä laadittu tietoturvapoliittikka, joka luo perustan yrityksen tietoturvasuunnitelmalle. Vastuu yrityksen toimivuudesta on ylimmällä johdolla ja johdolla on oltava kyky arvioida yrityksen kehittyminen sekä tietoturvaedellytykset. Tietoturvapoliittikan avulla saadaan luotua ohjeistusta ja käytänteitä, kuinka yrityksessä noudatetaan tietoturvaluutta jatkossa. Näitä voivat olla esimerkiksi salasankäytänteet, mobiililaitteiden käyttö, arkaluonteisen tiedon käsittely työpaikan ulkopuolella jne.

Tunnistetut kehityskohteet priorisoidaan sekä luodaan tietoturvan tiekartta, jossa kuvataan aikataulus havaittujen puutteiden korjaamiseksi. Kartoituksessa havaittiin myös puutteita GDPR:n osoitusvelvollisuuden noudattamisessa, jotka korjataan parantamalla yrityksen dokumentaatiota tietoturvaan liittyen.

Tietoturvapoliitiikan avulla syntyneet käytänteet dokumentoidaan ja laaditaan ohjeet ja säännöt henkilökunnalle. Päivitetyt käytänteet tullaan perehdyttämään henkilöstölle tietoturvakoulutuksilla, joissa käydään läpi organisaation tietoturvakäytänteet. Ohjeet asetetaan koko henkilöstön saatavilla sekä helposti sisäistettävissä. Tietoturvaohjeistus huomioidaan myös uuden työntekijän perehdytyksessä.

Jatkossa yrityksen tietoturvakäytänteitä päivitetään säännöllisesti tekemällä sisäisiä auditointeja sekä tarvittaessa myös mahdollisesti hyödynnetään ulkopuolisia tahoja. Tietoturva tullaan huomiomaan aina muutoksien (esim. tekniset muutokset, uudet järjestelmät) yhteydessä sekä dokumentit päivitetään.



Kuvio 10: Tietoturvan kehittäminen - yritys X

## 9 Yhteenveto

Uuden tietosuojasetuksen astuessa voimaan keväällä 2018 herätti se paljon keskustelua sekä viestimissä on ollut uutisointia sen tuottamasta päänvaivasta yrityksille. Huomattava osa aihetta käsittelevistä julkisista keskusteluista vaikutti paniikin lietsomiselta, ja uudistuksen alkuperäinen tarkoitus jäi pimentoon. Etenkin monia tahoja huolestuttaa EU:n tietosuojasetuksen noudattamisesta säädetyt sanktiot, jotka voivat nousta yrityksen koosta riippuen jopa 20 miljoonaan euroon tai neljään prosenttiin yrityksen liikevaihdosta. Sanktioitakin suurempa huolenaiheena on saattanut olla yrityksen maineelle tapahtuva kolaus. Julkisuuteen päätyneet vakavat tietosuojapuutteet ovat vahingollisia yrityksen taloudelle ja saattavat johtaa osakekurssin laskuun pörssissä. Tässä on hyvä huomioida se seikka, mikäli yritys täyttää EU:n tietosuojavaatimukset, niin tekee se yrityksestä luotettavamman kumppanin sekä houkuttelee

sijoittajia. Asetuksen tavoitteena ei ole vaikeuttaa yrityksen toimintaan vaan päinvastoin selkeyttää sekä yhtenäistää käytänteitä EU:n alueella.

Asetusta edeltänyt henkilötietodirektiivi oli tullut voimaan 1995, jolloin henkilötietojen käsittelyn tekninen toimintaympäristö ja tietojärjestelmissä käsiteltävät asiat olivat hyvin toiseltaiselta. Lisäksi henkilötietodirektiivi oli saatettu voimaan jokaisessa jäsenvaltiossa kansallisella lailla, minkä johdosta yritysten käsittelytehtäviin liittyvät velvollisuudet saattoivat erota toisistaan merkittävästi. Esimerkiksi tilanteet, joissa rekisterinpitäjällä on ilmoitusvelvollisuus paikalliselle tietosuojaviranomaiselle, vaihtelivat suuresti jäsenvaltioiden välillä, minkä vuoksi henkilötietojen liittyvien säännösten noudattaminen monikansallisissa yrityksissä oli monimutkaista, kallista ja haastavaa (Korpisaari, 2018).

On ensiarvoisen tärkeää, että yritys ottaa tietoturvallisuuden riittävällä vakavuudella sekä sisällyttää tietoturvaoperaatioita päivittäiseen toimintaansa. Tietoturvan laiminlyöminen voi johtaa vakaviin seurauksiin ja pahimmassa tapauksessa jopa liiketoiminnan lakkautumiseen. On ylimmän johdon vastuulla, että yrityksessä valitsee hyvät käytänteet sekä tietoturvaa ylläpidetään ja kehitetään. Johdon tulee luoda yhdessä joko sisäisten tai ulkoisten tietosuoja-asiantuntijoiden kanssa tietoturvapoliittikka, joka toimii perustana yrityksen tietoturvassa ja määrittelee käytänteet. Sovituilla toimenpiteillä pystytään luomaan tiekartta, jolla haluttu tietoturvallisuuden taso saavutetaan organisaatiossa. Henkilöstön käyttäytyminen toimii merkittävässä roolissa sekä työntekijöiden ohjeistus, kouluttaminen ja ylläpito on syytä priorisoida tietosuojan suhteen ensisijalle. Tietoturvadokumentaatiolla saadaan poikkeustilanteen sattuessa suoraa näyttöä viranomaisille siitä, että yritys on ottanut huomioon tietosuoja-asetuksen vaateet toiminnassaan. Näin saadaan tilanteesta riippuen vastuuta siirrettyä tai lievennettyä mahdollisia sanktioita.

Huolella suunnitellusta, toteutetusta ja ylläpidetystä tietoturvasta hyötyy kaikki osapuolet organisaatiossa. Yrityksen liiketoiminta ei kärsi tietoturvan laiminlyömisestä, sidosryhmät pystyvät luottamaan yrityksen kykyyn noudattaa lainsäädäntöä, työntekijät saavat yhtenäisyyttä ja ammattitaitoa työskentelyyn sekä ennen kaikkea yrityksen asiakkaat saavat turvaa omien tietojensa käsittelyyn. Lopuksi on vielä syytä muistaa, että tietoteknologian kehittyessä on yrityksellä oltava kyky pysyä ajan hermoilla sekä auditoida säännöllisesti tietoturvaoperaatioiden kattavuus. Mahdolliset muutokset tulee aina ohjeistaa henkilöstölle, jotta toiminta pysyy hyviä käytänteitä noudattaen asiallisena.

## 10 Oman oppimisen arviointi

Vaikka jo ennen kevättä 2018 liikkui paljon keskustelua uuden tietosuoja-asetuksen vaikutuksista tietosuojaan, niin en itse ollut aiheeseen tutustunut ja omat tottumukseni tietoturvassa olivat hyvin paljon yleisten käytänteiden varassa. Opinnäytetyön aihetta määritellessä en ollut varma osaamisestani sekä näin työn tuloksien laadusta. Olen kuitenkin tyytyväinen, että

aloin tutkimaan tietosuojasetusta ja tietoturvan kehittämistä. Työn aikana tietoturvaisuuden tutustuminen on laajentanut osaamistani ja parantanut suhtautumistani tietoturvaan.

Opittu tieto lisää ammattitaitoani ja työn tuloksia pystytään hyödyntämään työpaikallani. Vaikka työssä itsessään ei laajemmin kerrota sen yhteyttä työelämään, niin opinnäytetyön tekemisen myötä olen päässyt työpaikallani mukaan työryhmään, jonka tavoitteena on kehittää yrityksen tietoturvaa sekä päivittää organisaatioon tietoturvapoliittika asetuksen vaatimalle tasolle. Tähän työryhmään mukaan pääseminen kehittää ammattitaitoani entisestään ja on jatkossa hyödyksi työelämässäni.

Lähteet

Painetut

Miten valmistautua EU:n tietosuojasetukseen? 2017. Helsinki: Oikeusministeriö.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät - Uudenlaista osaamista liiketoimintaan. 3., uudistettu painos. Helsinki: Sanoma Pro Oy.

Heljaste, J., Korkiamäki, J., Laukkala, H., Mustonen, J., Peltonen, J. & Vesterinen, P. 2008. Yrityksen turvallisuusopas. Kauppakamari.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Vacca, J. 2013. Managing Information Security. Elsevier Science & Technology books.

Warren, A. 2004. Outsourcing Information Security. Artech House.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Tietosanomama Oy.

Valtiovarainministeriö. 2007. Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Helsinki: Edita Prima Oy.

Korpisaari P., Pitkänen O. & Warma-Lehtinen E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent Oy.

Laaksonen M. & Nevasalo T. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing Oy.

Lahtinen, J. & Isoviita, A. 2001. Asiakaspalvelun ja markkinoinnin perusteet. Avaintulos oy.

Information technology. Security techniques. Information Security management systems. ISO/IEC 27001. 2017.



## Sähköiset

Pietikäinen, S. 2013. Vahtiohje. Turvallisuusvyöhykkeet. Viitattu 20.2.2019  
<https://www.vahtiohje.fi/web/guest/turvallisuusvyohykkeet>

Pietikäinen, S. 2016. Vahtiohje. Rekisterinpitäjän velvollisuudet. Viitattu 13.9.2018  
<https://www.vahtiohje.fi/web/guest/rekisterinpitajan-velvollisuudet>

Tietosuojavaltuutetun toimisto. Organisaatiot. 2018a. Viitattu 4.6.2019  
<https://tietosuoja.fi/organisaatiot>

Tietosuojavaltuutetun toimisto. Osoita noudattavasi tietosuojasäädöksiä 2018b. Viitattu 12.9.2018  
<https://tietosuoja.fi/osoitusvelvollisuus>

Tietosuojavaltuutetun toimisto. Tietoturvaloukkaukset. 2018c. Viitattu 12.9.2018  
<https://tietosuoja.fi/tietoturvaloukkaukset>

Tietosuojavaltuutetun toimisto. Seloste käsittelytoimista. 2018d. Viitattu 11.2.2019  
<https://tietosuoja.fi/rekisterinpitajan-seloste-kasittelytoimista>

Laakso, M. Tietoturvasuunnitelma. Fyysinen turvallisuus- Viitattu 5.2.2019  
<https://tietojesiturvaksi.fi/tietoturvasuunnitelma/fyysinen-tietoturva>

Tietosuojavaltuutetun toimisto. Laadi tietotilin päätös. 2012. Viitattu 10.9.2018  
<https://tietosuoja.fi/documents/6927448/10594424/Laadi+tietotilin%C3%A4%C3%A4t%C3%B6s.pdf/4925bd9e-d07d-82fc-3f2d-71c5955310a0/Laadi+tietotilin%C3%A4%C3%A4t%C3%B6s.pdf.pdf>

Koivunen E. 2011. Tietoturvallisuuden perustason toteuttaminen. Viitattu 17.1.2019  
<https://www.vahtiohje.fi/web/guest/600>

Valtiojohdon tietoturvallisuuden johtoryhmä. Ohje tietoturvallisuudesta. 2010. Viitattu 12.2.2019  
[https://www.vahtiohje.fi/c/document\\_library/get\\_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229](https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229)

Keskuskaupakamari 2016. Tietoturvaopas yrityksille. ICC Cyber security guide for business Viitattu 19.4.2019  
<https://kauppakamari.fi/wp-content/uploads/2016/11/tietoturvaopas-yrityksille.pdf>

---

## Kuviot

Kuvio 1: Tapaustutkimuksen vaiheet .....	9
Kuvio 2: Tietosuojaperiaatteet .....	18
Kuvio 3: Henkilötietojen elinkaari .....	20
Kuvio 4: Tietoturvallisuuden osa-alueet .....	21
Kuvio 5: Tietoturvallisuuden kokonaisuus .....	26
Kuvio 6: Tietoturvan johtamis- ja hallintajärjestelmän kulun vaiheet.....	27
Kuvio 7: PDCA-mallin soveltaminen tietoturvallisuuden hallintajärjestelmässä .....	27
Kuvio 8: Turvallisuusvyöhykkeiden mallinnuskartta .....	32
Kuvio 9: Tietoturvakartoituksen osa-alueet.....	36
Kuvio 10: Tietoturvan kehittäminen - yritys X.....	37

---

## Taulukot

Taulukko 1: Hallinnollisen turvallisuuden dokumentaatio .....	28
Taulukko 2: Henkilöstöturvallisuuden dokumentaatio .....	31
Taulukko 3: Laitteistoturvallisuuden dokumentaatio.....	34
Taulukko 4: Ohjelmistoturvallisuuden dokumentaatio .....	35