KATI TIKKA

EU:N TIETOSUOJA-ASETUKSEN MUKAISEN PROSESSIN KÄYNNISTÄMINEN YHTEISTYÖSSÄ YRITYS OY:N KANSSA

Liiketalouden koulutusohjelma
2019

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

EU:N TIETOSUOJA-ASETUKSEN MUKAISEN PROSESSIN KÄYNNISTÄMINEN YHTEISTYÖSSÄ YRITYS OY:N KANSSA

Tikka, Kati
Satakunnan ammattikorkeakoulu
Liiketalouden koulutusohjelma
Kesäkuu 2019
Ohjaaja: Saarikko, Simo
Sivumäärä: 65
Liitteitä: 2

Asiasanat: tietosuoja-asetus (GDPR), tietosuoja, henkilörekisteri, henkilötieto

---

Tämän opinnäytetyön tavoitteena oli selvittää Yritys Oy:n tietosuojan nykytila, miten EU:n tietosuoja-asetus vaikuttaa yrityksen toimintaan ja millä tavalla yrityksen tulee varautua tietosuoja-asetukseen, jotta yrityksen toiminta vastaa tietosuoja-asetuksessa määrättyjä toimenpiteitä. Opinnäytetyön tarkoituksena on EU:n tietosuoja-asetuksen mukaisen prosessin käynnistäminen yhteistyössä Yritys Oy:n kanssa.

Teoreettinen viitekehys nojaa EU:n yleiseen tietosuoja-asetukseen (2016/679), jota on sovellettu 25.5.2018 alkaen kaikissa EU:n jäsenvaltioissa sekä tietosuojalainsäädäntöön ja oikeusministeriön ohjeisiin.

Opinnäytetyö on tapaustutkimus ja sen empiirinen osuus koostuu kvantitatiivisesta kyselytutkimuksesta sekä kvalitatiivisestä haastattelusta. Tutkimusaineisto kerättiin puolistrukturoidun kyselylomakkeen sekä haastattelun avulla. Tietosuojakysely (Webropol) lähetettiin sähköpostilla valitulle kohdejoukolle (N = 127) ja vastausprosentti oli 55.

EU:n tietosuoja-asetukseen valmistautuminen oli hyvin aloitettu kohdeyrityksessä, mutta sen tietosuojakäytännöt ja osaamisen taso eivät kaikilta osin vastanneet tietosuoja-asetuksen mukaisia vaatimuksia. Kyselyn tuloksien perusteella yritykselle laadittiin tietosuojan kehittämissuunnitelma, joka sisälsi henkilöstön tietosuojakoulutus tarpeita. Kehitettävää yrityksellä on henkilötietojen käsittelyn toimintamallien ja ohjeiden laadinnassa, tiedon jalkauttamisessa ja henkilöstön kouluttamisessa sekä tietosuoja organisaation ja esimiesten tukemisessa toiminnan jatkuvuuden turvaamiseksi.

Lisäksi kehittämishaasteeksi nousee yrityksen tietosuojan dokumentaatio, suunnitelmallinen ja säännöllinen seuranta sekä valvonta, joita vaaditaan osoittamaan, että tietosuoja-asetusta on noudatettu.

STARTING A PROCESS UNDER THE EU DATA PROTECTION REGULATION IN COOPERATION WITH THE COMPANY

Tikka, Kati
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Business Administration
June 2019
Supervisor: Saarikko, Simo
Number of pages: 65
Appendices: 2

Keywords: General Data Protection Regulation (GDPR), data protection, personal register, personal data

---

The aim of this thesis is to find out the current state of enterprise data protection. How the General Data Protection Regulation (GDPR) affects the company's operations and how the company should be prepared to comply with the privacy regulation to ensure that the company is in compliance with the measures set out in the GDPR. The purpose of the thesis is to launch the GDPR process in cooperation with the company.

The theoretical framework relies on the EU Data Protection Regulation (2016/679) which has been applied since 25 May 2018 in all EU Member States as well as data protection legislation and the instructions of the Ministry of Justice.

The thesis is a case study and it's empirical part consist of a survey and an interview. The research material was collected using a semi-structured questionnaire and an interview. The privacy questionnaire was sent to the selected target population (N = 127) and the response rate was 55 %.

Preparing for an EU Data Protection Regulation was well launched in the target company but it's privacy practices and level of expertise did not fully meet the requirements of the Data Protection Regulation. Based on the results of the survey, a data protection development plan was developed for the company which included the needs of staff data protection training. The company being developed has been working on the development of policies and guidelines for the processing of personal data. The company to be developed has knowledge in the implementation and training of it's personnel as well as in the protection of the organization and it's superiors to ensure the continuity of operations.

In addition, the development challenge is the company's data protection documentation, systematic and regular monitoring, and the controls required to demonstrate compliance with the privacy policy.

SISÄLLYS

1 JOHDANTO

Tämä kehittämistyö käsittelee EU:n yleistä tietosuoja-asetusta (2016/679), jota on sovellettu 25.5.2018 alkaen kaikissa EU:n jäsenvaltioissa ja sen muutoksia toimeksiantajan näkökulmasta. Asetuksen velvoitteet koskevat kaikkia henkilötietoja käsitteleviä ja rekisterinpitäjiä EU:n alueella. Asetusta sovelletaan yksityisellä ja julkisella sektorilla kaikkeen henkilötietojen käsittelyyn. Uusi sääntely edellyttää, että henkilötietoja käsittelevä yritys pystyy osoittamaan noudattavansa tietosuoja-asetuksen sääntelyä. Asetuksella pyritään lisäämään henkilötietojen käsittelyn avoimuutta ja vahvistaa rekisteröidyn oikeutta valvoa omien henkilötietojen käsittelyä. (Oikeusministeriö 2017) Lisäksi 1.1.2019 voimaan astunutta Tietosuojalakia (1050/2018), joka täsmentää EU:n tietosuoja-asetusta.

Opinnäytetyön toimeksiantajana toimii Päijät-Hämeessä toimiva konserni, jossa työskentelee n. 300 työntekijää neljällä eri toimialalla. Toimeksiantajan pyynnöstä esittelen yrityksen tässä opinnäytetyössä Yritys Oy:na. Tämän opinnäytetyön tarkoituksena on EU:n tietosuoja-asetuksen mukaisen prosessin käynnistäminen yhteistyössä Yritys Oy:n kanssa. Opinnäytetyön tavoitteena on selvittää Yritys Oy:n tietosuojan nykytila, miten EU:n tietosuoja-asetus vaikuttaa yrityksen toimintaan ja millä tavalla yrityksen tulee varautua tietosuoja-asetukseen, jotta yrityksen toiminta vastaa tietosuoja-asetuksessa määrättyjä toimenpiteitä. Kyselyn tuloksien perusteella laaditaan yritykselle tietosuojan kehittämissuunnitelma, joka sisältää henkilöstön tietosuojakoulutus tarpeita.

Opinnäytetyö on tapaustutkimus ja sen empiirinen eli tutkimuksellinen osuus koostuu kvantitatiivisesta kyselytutkimuksesta sekä kvalitatiivisestä haastattelusta. Päätutkimusaineisto kerätään puolistrukturoidun kyselylomakkeen avulla, jossa on yhdistettynä monivalintakysymyksien lisäksi avoimia kysymyksiä. Opinnäytetyön teoriaosuus rajataan käsittelemään EU:n tietosuoja-asetusta (679/2016) yleisesti ja sen tuomia muutoksia Yritys Oy:n näkökulmasta.

2 KEHITTÄMISTYÖN LÄHTÖKOHDAT

Opinnäytetyön toimeksiantajana toimii Päijät-Hämeessä toimiva konserni, jossa työskentelee n. 300 työntekijää neljällä eri toimialalla. Aihe ja tutkimusongelmat nousivat työelämän tarpeesta ja ovat ajankohtaisia. Toimeksiantajan pyynnöstä esittelen yrityksen tässä opinnäytetyössä Yritys Oy:na. Yhtiöiden toimialoina ovat hotelli- ja ravintola palvelut, urheilu- ja vapaa-ajan palvelut, opetus sekä kiinteistö- ja huoltopalvelut. Opinnäytetyöntekijä oli yrityksessä henkilöstöhallinnon työharjoittelussa, jolloin osallistui myös tietosuojaryhmään ja ohjeiden sekä toimintamallien laadintaa yhtiöille. Tämän opinnäytetyön tarkoituksena on EU:n tietosuoja-asetuksen mukaisen prosessin käynnistäminen yhteistyössä Yritys Oy:n kanssa.

3 KEHITTÄMISTYÖN TAVOITE, TARKOITUS JA TEHTÄVÄT

EU:n yleisen tietosuoja-asetuksen 2016/679 soveltaminen astui voimaan 25.5.2018 alkaen. Uusi sääntely edellyttää, että henkilötietoja käsittelevä yritys pystyy osoittamaan noudattavansa tietosuoja-asetuksen sääntelyä. Siksi yrityksen on tärkeä muun muassa varmistaa, että henkilötietojen käsittelyä koskeva dokumentointi ja sisäinen ohjeistus ovat kunnossa. Uusi tietosuojalaki 2018/1050 astui voimaan 1.1.2019, jolla täydennetään sekä täsmennetään EU:n yleistä tietosuoja-asetusta ja sovelletaan sen kanssa rinnakkain. Uudessa tietosuojalaissa säädetään mm. valvontaviranomaisesta, joistakin henkilötietojen käsittelyyn liittyvistä erityistilanteista esim. sananvapauden ja henkilötietojen yhteensovittamisesta. Laki kumoaa nykyisen henkilötietolain sekä tietosuojalautakuntaa sekä tietosuojavaltuutettua koskevat lait. (Oikeusministeriö 2018.)

Yritys Oy:ssä käsitellään paljon erilaisia henkilötietoja, kuten asiakkaiden, opiskelijoiden, työntekijöiden ja yhteistyökumppaneiden nimiä ja/tai yhteystietoja.

Henkilötietoja käsitellään mm. asiakkuuksien ja myynnin hallintaa, liiketoimintaa, oppilaitostoimintaa, työntekoa ja laskutusta varten sekä erilaisia työsuhteen hallintaan liittyviä tarpeita varten. Yrityksen oman henkilöstön henkilötietojen lisäksi yrityksessä käsitellään henkilötietoja, jotka tulevat yritykselle mm. asiakasyrityksiltä ja yhteistyökumppaneilta, eivätkä suoraan rekisteröidyiltä itseltään. Yritys Oy toimii siten sekä rekisterinpitäjänä (oma henkilöstö) että henkilötietojen käsittelijänä (asiakasyritysten lukuun käsitellyt henkilötiedot) (EU:n tietosuoja-asetus 679/2016). Henkilötietoja säilytetään ja käsitellään myös ulkoisilla palvelimilla. Yritys ei siirrä henkilötietoja EU:n ulkopuolelle.

Valtiovarainministeriön (2016, 31) mukaan ”Tietosuojan nykytila-analyysi tarkoittaa organisaation henkilötietojen käsittelyn ja tietosuojakyvykkyyksien nykytilan arviointia suhteessa tietosuoja-asetuksen vaatimuksiin.” Oleellista on arvioida rekisteröityjen oikeuksien ja mahdollisten riskien toteutuminen, jonka avulla voidaan tunnistaa tietosuojan puutteet ja kehityskohteet sekä tarvittavat toimenpiteet. Niiden avulla yritys voi parantaa tietosuojan nykytilaa ja huolehtia sen toteutumisesta osana jokapäiväistä operatiivista toimintaa.

Opinnäytetyön aihe nousi työelämän tarpeesta ja toimeksiantajana on konserni, jossa tämän työn laatijana olin hr-asiantuntija työharjoittelussa kevään 2018. Aihe on juridinen, mutta liittyy myös esimiestyön aihealueeseen henkilöstöhallintoa koskien. Aihe on mielestäni kiinnostava ja tärkeä myös oman osaamisen näkökulmasta sekä ajankohtainen.

Tämän opinnäytetyön tarkoituksena on EU:n tietosuoja-asetuksen mukaisen prosessin käynnistäminen yhteistyössä yrityksen kanssa. Opinnäytetyön tavoitteena on selvittää Yritys Oy:n tietosuojan nykytila, miten EU:n tietosuoja-asetus ja tietosuojalaki vaikuttavat yrityksen toimintaan ja millä tavalla yrityksen tulee varautua tietosuoja-asetukseen, jotta yrityksen toiminta vastaa tietosuoja-asetuksessa määrättyjä toimenpiteitä. Kyselyn tuloksien perusteella laaditaan yritykselle tietosuojan kehittämissuunnitelma sekä selvitys henkilöstön tietosuojakoulutus tarpeista. Lisäksi yhteistyössä tietosuojaryhmän kanssa luodaan ohjeistusta, kuinka Yritys Oy:n käytännön arjen toimia tulee muuttaa, jotta yrityksen toimintaperiaatteet ja käytänteet vastaavat asetuksen tuomia muutoksia sekä velvoitteita.

Tällä opin näytetyöllä pyritään vastaamaan seuraaviin kysymyksiin:

- Millainen on Yritys Oy:n tietosuojan nykytilanne ja henkilöstön tietosuoja tiedon taso?
- Mitä muutoksia EU:n tietosuoja-asetus tuo Yritys Oy:n käytänteisiin, rekisterien pitämiseen ja henkilötietojen käsittelyyn?
- Miten näihin muutoksiin valmistaudutaan?

Opinnäytetyö on rajattu tarkastelemaan tietosuoja-asetuksen keskeisimpiä muutoksia ja olennaisimpia asioita Yritys Oy:n näkökulmasta. Opinnäytetyön laajuuden ulkopuolelle jäävät toimeksiantosopimuksien sisältö, fyysinen tietoturva sekä Yritys Oy:n käyttämien tietojärjestelmien tietoturva. Työssä käsitellään erityisesti henkilötiedon käsittelyyn liittyvää tietosuojaa.

Hallinnollista tietoturvaa on mm. ohjeistus ja käyttäjien antama sitoumus noudattaa annettuja ohjeita. Fyysiseen tietoturvaan kuuluvat henkilö-, käyttö-, tietoliikenne-, laitteisto-, ohjelmisto- ja tietoaineistoturvallisuudet. Fyysisessä tietoturvassa keskeistä on henkilöiden toiminta annettujen ohjeiden mukaisesti. (Valtiovarainministeriö 2013). Opinnäytetyön teoria osassa tarkastellaan EU:n tietosuoja-asetusta (2016/679) ja kerrotaan yleisesti mitkä ovat yrityksen vastuut ja velvollisuudet ja mitä muutoksia toimintatavoissa tai tietosuojassa pitäisi tehdä.

4 EU:N TIETOSUOJA-ASETUS

4.1 Yleistä tietosuoja-asetuksesta

Opinnäytetyössä keskitytään EU:n tietosuojauudistuksen sisältöön, EU:n yleiseen tietosuoja-asetukseen 2016/679 ja EU:n tietosuojadirektiiviin 2016/680 sekä Suomessa voimassa olevaan EU:n Tietosuojalakiin 2018/1050. Tietosuoja-asetukseen sisältyy mm. säännökset henkilötietojen käsittelyä koskevista periaatteista, käsittelyn laillisuudesta, rekisteröidyn suostumuksen edellytyksistä ja arkaluonteisten tietojen käsittelystä. Uudistus velvoittaa rekisterinpitäjiä tarkistamaan tietosuojakäytäntöjen lainmukaisuuden. (Andreasson, Koivisto & Ylipartanen 2016, 35.) Asetuksesta käytetään yleisesti lyhennettä GDPR, joka tulee englannin kielen sanoista General Data Protection Regulation (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 13).

EU:n tietosuoja-asetuksen määritelmän mukaan henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. (EU:n tietosuoja-asetus 679/2016, 4 luku 1 art.)

Tietosuoja-asetus määrittää, että henkilötietoja pitää käsitellä lainmukaisesti, läpinäkyvästi ja asianmukaisesti. Henkilötietojen käsittelylle pitää olla tietosuoja-asetuksen mukainen peruste ja henkilötietoja saa kerätä sekä käsitellä vain tämän perusteen vaatiman verran. Suurin tietosuoja-asetuksen tuoma muutos on osoitusvelvollisuus, joka siirtää todistustaakan henkilörekisterin ylläpitäjälle. Osoitusvelvollisuus edellyttää huomattavan määrän dokumentaatiota ja seurantaa. (EU:n tietosuoja-asetus 679/2016, 4 luku.) Kun yritys kerää asiakkaasta henkilötietoja eri rekistereihin, on yrityksen velvollisuus käsitellä henkilötietoja Suomen lain vaatimalla tavalla.

Opinnäytetyössä tutkitaan yksityiselle yritykselle tärkeitä tietossuojalain osia, jotka liittyvät asiakasrekistereiden keräämiseen, suojaamiseen, säilyttämiseen ja hävittämiseen. Lisäksi tarkastellaan, mitkä ovat yrityksen oikeudet ja velvollisuudet rekisterinpitäjänä huomioiden Euroopan unionin tietosuojauudistus. (EU:n tietosuoja-asetus 679/2016.)

Asiakkaita koskevan henkilötiedon lisäksi Yritys Oy käsittelee työntekijöitään koskevia henkilörekistereitä. Tällaiset rekisterit yleensä sisältävät työntekijöiden työsuhteeseen ja palkkaukseen liittyviä tietoja esim. työsopimus, yhteystietoja sekä sairaspoissaolo tietoja. Perustelu työntekijöistä kerättyyn henkilötietoon on oltava oleellista työsuhteen kannalta, kuten molempien osapuolten oikeuksien ja velvollisuuksien hoitaminen tai työnantajan tarjoamat etuudet. (EU:n tietosuoja-asetus 679/2016 88 art.; Tietosuojalaki 2018/1050; Tietosuojavaltuutetun www-sivut 2018.)

Tietosuojasuunnitelma voidaan laatia, kun ensin on arvioitu organisaation nykyiset henkilötietojen käsittely- ja tietosuojakäytänteet sekä tunnistettu organisaation tietosuojan tavoitetila huomioiden EU:n tietosuoja-asetuksen vaatimukset. Tietosuoja-asetuksen mukainen käytännönprosessi (Kuvio 1.) ja tarvittavien toimenpiteiden päävaiheet Valtiovarainministeriön (2016, 31) suosituksen mukaisesti ovat: johdon tahtotilan ilmaisu, ohjeistus ja koulutus, kehittäminen ja seuranta ja raportointi.

Johdon tahtotila	**Ohjeistus ja koulutus**	**Analyysit ja kehittäminen**	**Seuranta & raportointi**
- tietosuojan taso - tuki ja ohjaus - tavoitteet	- henkilöstö - luottamushenkilöt - yhteistyötahot - vapaaehtoiset	- prosessit - toiminta - järjestelmät	- tilinpäätös - auditoinnit - sertifikaatit - todistus

Kuvio 1. Tietosuoja-asetuksen prosessi (Valtiovarainministeriö 2016, 31).

Yksi ensimmäisistä ja tärkeimmistä toimenpiteistä tietosuojatyön onnistumiselle on organisaation johdon osallistuminen ja tuki tietosuojatyölle. Yrityksen johto omistaa tietosuojatoiminnan ja vastaa siitä, että tietosuoja toteutuu organisaatiossa osana

jokapäiväistä toimintaa tietosuojasääntelyn vaatimalla tavalla. Tarvittavien resurssien ohjaaminen on johdon vastuulla tietosuojan nykytilan arvioimiseksi, valtuuttaa sekä mahdollistaa sen pohjalta tunnistettujen kehitystoimenpiteiden toteuttaminen. Tietosuojan kehittämisen edistymisen raportointi ja projektin seuranta tulisi sisällyttää johdon strategiseen ohjaukseen. (Valtiovarainministeriö 2016, 31).

Valtiovarainministeriön (2016, 33) mukaan tietosuoja-asetuksen mukainen toiminta tulisi toteuttaa projektina, jonka päävaiheet ovat rekistereiden kartoitus, arviointi, dokumentointi ja ylläpidon sekä kehittämiskohteiden määrittely. Yrityksen olisi hyvä laatia myös seuraavat dokumentit; tietosuojaselosteet, seloste käsittelytoimista, henkilötietojen käsittely ohjeet, prosessikaaviot rekisteröityjen oikeuksista, sisäinen ja ulkoinen viestintä liittyen tietotilinpäätökseen, kuvaus tietosuojatyön suunnittelusta ja seurannasta sekä tietosuojavastaavan päiväkirja.

4.2 Tietosuoja-asetuksen keskeiset käsitteet

EU:n tietosuoja-asetuksessa (2016/679) on määritelty erilaisia käsitteitä, jotka ovat osittain samanlaisia, kuin Suomen henkilötietolaissa on säädetty, jonka puolestaan 1.1.2019 korvasi tietosuojalaki. Uudessa sääntelyssä käsitteitä on laajemmin määritelty sekä asetukseen on lisätty muutamia uusia käsitteitä. Tässä luvussa esitellään kehittämistyön keskeiset käsitteet, joita ovat henkilötieto, henkilötietojen käsittely, henkilötietojen käsittelijä, suostumus, rekisteri, rekisterinpitäjä ja rekisteröity.

Henkilötieto

Henkilötietoja ovat kaikki tiedot, jolla voidaan tunnistaa ja yksilöidä henkilöitä, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötietoja ovat esimerkiksi nimi, puhelinnumero, sijaintitiedot, verkkotunnistetiedot ja isovanhempien perinnöllisiä sairauksia koskevat tiedot. (EU:n tietosuoja-asetus 679/2016, 1 luku 4 art.; Tietosuojavaltuutetun www-sivut 2018)

Henkilötietojen käsittely

Henkilötietojen käsittelyyn sisältyy kaikki henkilötietoihin kohdistuvat toimet tiedon koko elinkaaren ajalta aina suunnittelusta hävittämiseen asti. Henkilötietojen käsittelyä on mm. kaikki henkilötietojen automaattinen tai manuaalinen kerääminen, muokkaaminen, tallentaminen, järjestäminen, säilyttäminen tai hävittäminen. (EU:n tietosuoja-asetus 679/2016, 2 luku 4-6 art.; Tietosuojavaltuutetun www-sivut 2018; Valtiovarainministeriö 2016, 10.)

Henkilötietojen käsittelijä

Henkilötietojen käsittelijä on ihminen, virasto tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän puolesta. Henkilötietojen käsittelijä voi olla esimerkiksi toisen yrityksen markkinointia hoitava markkinointitoimisto, ulkoistettu palkkahallinto tai IT-palveluntarjoaja, jolla on pääsy rekisterinpitäjän henkilötietoihin. (EU:n tietosuoja-asetus 679/2016 1 luku 28-29 art.; Tietosuojavaltuutetun www-sivut 2018)

Rekisteri

Rekisterillä tässä työssä tarkoitetaan henkilötietoja sisältävää jäsenneltyä tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla tai manuaalisesti ja jonne on merkitty vähintään kahden henkilön tiedot. Se voi olla järjestetty Excel-taulukoksi, luetteloksi järjestelmässä, mappina tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot ovat saatavilla tietyin perustein esim. tiedot on voitu jakaa keskitetyin, hajautetuin, toiminnallisin tai maantieteellisin perustein. (EU:n tietosuoja-asetus 679/2016, 4 luku 6 art.)

Rekisterinpitäjä

Rekisterinpitäjä on ihminen, ryhmä tai organisaatio, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjä voi olla esimerkiksi jäsenistään tietoja keräävä yhdistys, potilastietoja käsittelevä sairaala, verkkokauppa tai sosiaalisen median palvelu. (EU:n tietosuoja-asetus 679/2016, 1 luku 4 art.)

Rekisteröity

Rekisteröidyllä tarkoitetaan rekisterissä oleva tunnistettava tai tunnistettavissa olevaa henkilöä, jonka tietoja käsitellään (EU:n tietosuoja-asetus 679/2016, 1 luku 4 art.; Hanninen ym. 2017, 20).

Suostumus

Rekisteröity voi esimerkiksi antaa kirjallisen tai suullisen suostumusta koskevan lausuman tai ilmaista suostumuksensa jollakin muulla selkeällä toimella, kuten rastittamalla ruudun internetsivustolla. Suostumus on voitava peruuttaa yhtä helposti kuin sen on voinut antaa. Jokaisen tiedon kohdalta on pystyttävä näyttämään, että sen keräämiseen on saatu rekisteröidyn henkilön suostumus tai jokin muu asetuksen edellytyksistä on täyttynyt. (EU:n tietosuoja-asetus 679/2016, 7 luku 8 art.; OpiTietosuojaa.fi www-sivut 2018; Tietosuojavaltuutetun www-sivut 2018.)

4.3 Tietosuojan nykytilanteen kartoittaminen

Organisaation henkilötietojen käsittely- ja tietosuojakäytänteiden nykytila-arvion ja -analyysin tekeminen kannattaa aloittaa kartoittamalla ja läpikäymällä yrityksen käytössä olevat henkilörekisterit ja millä perusteella niitä ylläpidetään sekä ketkä tietoja käsittelevät. Analyysin kohteena ovat mm. asiakastiedot, henkilöstöhallinnon tiedot, ulkoistukset, sopimukset sekä tietoturva. Kun organisaatio on kartoittanut henkilötietojen käsittelyn nykytilan, sen tulisi selvittää, mitä konkreettisia muutoksia ja toimenpiteitä tietosuoja-asetuksen sääntely sen suorittamalle henkilötietojen käsittelylle tarkoittaa. (Valtiovarainministeriö 2016b, 31-33).

Henkilörekistereiden kartoitusta varten on hyvä laatia dokumentti, jossa on kirjattuna henkilörekisterin nimi, käyttötarkoitus, tietojen tallennustapa ja -paikka, rekisterin vastuuhenkilö, pääkäyttäjä, käyttöoikeudet, miten rekisteri on suojattu, sopimuskumppanit, henkilötietoluokat, käsittelyperuste, säilytysaika, tietovirrat ja maantieteellinen sijainti. Nykytilan kartoituksen ja analysoinnin jälkeen yritykselle tulisi laatia riskiarvio, jossa kartoitetaan, tunnistetaan ja analysoidaan tunnistetut riskit. Analyysin jälkeen arvioidaan riskin merkitys toiminnalle ja rekisteröidyille henkilöille. Edellä tehtyjen vaiheiden jälkeen määritellään, miten riskiä käsitellään, kuka vastaa ja mitä toimenpiteitä tehdään määritellyn ajan puitteissa. (Valtiovarainministeriö 2016b, 31-33).

Kartoitusta varten organisaatiolta kerätään pohjatietoja erilaisin haastatteluin tai kyselylomakkein. Pohjatietojen perusteella organisaatiolle voidaan tehdä tietosuojan

vaikutusten arviointi, riskianalyysi tai laatia tietoturvapolitiikka ja –ohjeistus sekä tietoturvallisuuden kehittämissuunnitelma. (Valtiovarainministeriö 2016b, 31-33). Riskikartoitusten toteuttaminen ja dokumentointi ovat myös tapoja osoittaa, että yritys noudattaa asetuksen velvoitteita.

4.4 Tietosuojan hallintamalli

Tietosuojan hallintamallissa (Kuvio 2.) koostuu kymmenestä eri osa-alueesta, joista on tarkemmin säädetty EU:n tietosuoja-asetuksessa sekä kansallisessa tietosuojalaissa. Nämä osa-alueet kuvaavat tietosuojaan- ja tietoturvaan liittyviä kokonaisuuksia, joita organisaation tulisi huomioida kehittäessään omaa tietosuojanhallintaa.

Kuvio 2. Tietosuojan hallintamalli koostuu kymmenestä eri osa-alueesta (Digitaalinen Helsinki www-sivut 2019.)

Yksi osa tietosuojan hallintamallia on riskienkartoittaminen (kts. Kuvio 2.). Riskikartoituksessa tunnistetaan keskeisimmät puutteet ja heikkoudet. Riskianalyysin tarkoituksena on löytää sopivimmat hallintakeinot olennaisesti toimintaan kohdistuvien uhkien vähentämiseksi. Tärkeää on arvioida riskien merkitys, ja luoda tietyn riskitason

ylittäville uhille hallintatoimia. Näin voidaan kohdistaa resurssit merkityksellisiin suojaustoimiin ja säästää kustannuksissa. Riskianalyysi dokumentoidaan tietoturva- ja tiesuoja riskienkäsittelysuunnitelmaan. (Digitaalinen Helsinki www-sivut 2019.)

Rekisterinpitäjän velvollisuudet kasvavat sitä mukaan, mitä korkeampia riskejä henkilötietojen käsittelyyn liittyy. Jolloin on pystyttävä osoittamaan, että rekisterinpitäjä noudattaa tietosuoja-asetusta. Yksi työkalu riskien arviointiin on tietosuojaa koskeva vaikutustenarviointi (Kuvio 3.), jonka tarkoituksena on auttaa tunnistamaan, arvioimaan sekä hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Tietosuojan vaikutustenarvioinnin keskiössä tulee olla yksilö ja hänen oikeuksiinsa ja vapauksiinsa kohdistuvat uhat. Vaikutustenarviointi on pakollinen vain silloin, kun suunniteltu käsittely voi aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille. Vaikutustenarvioinnissa kuvataan henkilötietojen käsittelyä, arvioidaan käsittelyn tarpeellisuutta, oikeasuhteisuutta ja henkilötietojen käsittelystä aiheutuvia riskejä sekä tarvittavia toimenpiteitä, joilla riskeihin puututaan. Sen avulla rekisterinpitäjä voi noudattaa tietosuojalainsäädännön vaatimuksia. Henkilötietojen käsittely on suunniteltava ja dokumentoitava, koska työnantajille kertyy esimerkiksi henkilötietoja työntekijöistä mm. rekrytoinnin, työsopimuksen solmimisen ja kehityskeskustelujen yhteydessä. Lisäksi henkilötietoja tallentuu hr-järjestelmien ohella esimiesten, palkkahallinnon, työterveyden ja IT-tuen haltuun. Henkilötietojen käsittelyn tuoma vastuu on osa eri tehtävien hoitoon liittyvää toiminnallista vastuuta, joten työtehtävät ja vastuut on määriteltävä yrityksessä asianmukaisesti. (EU:n tietosuoja-asetus 679/2016, 2 art.; Tietosuojalaki 1050/2018; OpiTietosuojaa.fi www-sivut 2018; Tietosuojavaltuutetun www-sivut 2018)

Kuvio 3. Henkilötietojenkäsittelyn vaikutustenarviointi prosessi Tietosuojavaltuutetun toimiston mukaan (Tietosuojavaltuutetun www-sivut 2018).

Ennakkokuulemisella tarkoitetaan tilannetta, jossa rekisterinpitäjän on ennen henkilötietojen käsittelyn aloittamista kuultava tietosuojaviranomaista. Ennakkokuuleminen on toteutettava, kun vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin rekisteröidylle, eikä rekisterinpitäjä ole omilla toimenpiteillään saanut riskiä alhaisemmaksi. Esimerkiksi silloin, jos rekisteröity voisi joutua kärsimään huomattavista tai peruuttamattomista seurauksista, joita ei itse välttämättä pysty torjumaan, kuten laiton tietoihin pääsy, joka johtaisi rekisteröityjen henkeä uhkaavaan vaaraan, irtisanomiseen tai taloudelliseen uhkaan. Ennakkokuulemista ei voida toimittaa ennen kuin rekisterinpitäjä on tehnyt tietosuojaa koskevan vaikutustenarvioinnin. (EU:n tietosuoja-asetus 679/2016, 2 luku 32-34 art.; Tietosuojavaltuutetun www-sivut 2018)

Kehittämissuunnitelma

Riskien analysoinnin tuloksena saadaan priorisoitu lista kehittämiskohteista, jotka avataan ja pohditaan niille eri ratkaisuvaihtoehtoja. Ero vaiheiden aikana; projektisuunnitelma, johdon tahtotila, ohjeistus ja koulutus, nykytila-analyysi ja riskiarviossa esiin tulleiden asioiden pohjalta laaditaan kehittämissuunnitelma, jossa määritellään tarvittavat toimenpiteet, aikataulut ja vastuuhenkilöt. Tietosuojan käyttöönotto projekti on

jatkuva prosessi, jossa samat asiat toistuvat vuodesta toiseen. Vuosittain seurataan tietosuoja-asioita, kouluttaudutaan, analysoidaan, arvioidaan riskit, toteutetaan tarvittavat toimenpiteet ja tehdään tietotilinpäätös. Tietotilinpäätös antaa kokonaiskuvan yrityksen henkilötietojen käsittelyn ja tietosuojan nykytilasta. Sen avulla johto voi valvoa ja arvioida nykytilaa sekä ohjata resursseja sen kehittämiseen. (Tietosuojavaltuutetun www-sivut 2018; Valtiovarainministeriö 2016b, 31-33)

Tärkeää on huomioida, että lähes kaikki henkilötietoja käsittelevät prosessit ja rekisterit perustuvat myös tietojärjestelmiin, mobiilisovelluksiin tai pilvipalveluihin. Jonka vuoksi tietosuoja-asetuksen velvoitteet pitää toteuttaa myös näissä järjestelmissä sekä huomioitava myös nykytilan kartoituksessa. Tietosuoja-asetus edellyttää sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden ja tietoturvan toteuttamista järjestelmissä ja palveluissa sekä näiden kehitysprosesseissa. (Andreasson ym. 2016, 35-40.)

5 TIETOSUOJA-ASETUKSEN MUKAISET MUUTOKSET

Vuonna 2018 voimaan tullut lakimuutos tuo merkittäviä uudistuksia organisaatioilta vaadittaviin menettelyihin ja asettaa uusia suoria velvollisuuksia, joista olennaisimpia EU:n tietosuoja-asetuksen (2016/679) mukaan ovat: osoitusvelvollisuus**,** riskiperusteinen lähestymistapa**,** informointi ja seloste käsittelytoimista**,** rekisteröidyn oikeudet**,** rekisterin pitäjän ja henkilötietojen käsittelijän velvollisuudet**,** sopimukset henkilötietojen käsittelijöiden kanssa valvontaviranomaisen ja tietosuojavastaavan roolit. Tietosuojalaki täsmentää EU:n tietosuoja-asetusta (Oikeusministeriö 2018).

Osa EU:n tietosuoja-asetuksen velvoitteista kohdistuu vain osaan organisaatioista tai henkilötietojen käsittelytoimista. Esimerkiksi tietosuojavastaavan nimittäminen, tietosuojaa koskevan vaikutustenarvioinnin laatiminen, ennakkokuuleminen ja velvollisuus laatia seloste käsittelytoimista. Hyvä on dokumentoida, millä tavalla

organisaatiossa on päädytty edellä mainittujen velvoitteiden noudattamista tai noudattamatta jättämistä koskevaan ratkaisuun. (Tietosuojavaltuutetun www-sivut 2018.)

5.1 Henkilötietojen käsittely ja säilytys

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (Kuvio 4.). Henkilötietoja voi olla talletettuna esimerkiksi sähköisissä tiedostoissa, tietokannoissa, paperilla, kortistossa, mapeissa tai ääni- tai kuvatallenteella. (Tietosuojavaltuutetun www-sivut 2018.)

Tietosuojaperiaatteiden mukaan henkilötietoja on

• käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi

• käsiteltävä luottamuksellisesti ja turvallisesti

• kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten

• kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden

• päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä

• säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

Kuvio 4. Kuviossa on suoralainaus tietosuojavaltuutetun mukaan tietosuojaperiaatteiden mukaisesti kuvattuna, mitä henkilötiedoilla tarkoitetaan (Tietosuojavaltuutetun www-sivut 2018).

Uutena käsitteenä on määritelty henkilötietojen käsittelijä, jolla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Merkittävä uusi velvoite on, että tietosuoja-asetus velvoittaa rekisterinpitäjän solmimaan sopimuksen henkilötietojen käsittelystä rekisterinpitäjän ja henkilötietojen käsittelijän välillä. Kuitenkin henkilötietojen käsittelijän omalla vastuulla on aina noudattaa tietojen käsittelyssä tietosuoja-asetuksen vaatimuksia. (EU:n tietosuoja-asetus 679/2016, 1 luku 28-29 art.) Tietosuoja-asetuksen myötä myös vaitiolosopimuksesta

tulee standardi kaikilla aloilla, sillä lähes kaikilla työntekijöillä on pääsy johonkin henkilörekisteriin.

Tietosuoja-asetuksen yhteydessä henkilötietojen suojaikärajaksi määritettiin 16 vuotta, jota Suomen uusi Tietosuojalaki (2018/1050) täsmentää ja säätää, että lapsen ikäraja tietoyhteiskunnan palveluissa on 13 vuotta. Rekisterinpitäjän vastuulla on tarkistaa, että alle 13 vuotiaalla on vanhempien suostumus esimerkiksi henkilötietojen antamista edellyttävien palveluiden käyttämiseen tai sosiaaliseen mediaan. Tämä on tärkeää huomioida yrityksissä, joissa palveluiden käyttäjinä ovat myös alaikäiset esim. opiskelijat ja nuoremmat perheenjäsenet. Digitaalisesti henkilötietoja kerättäessä vanhemman suostumuksen saaminen on usein haasteellista, koska perhesuhteita on vaikea digitaalisesti selvittää sekä varmentaa. Moni yritys on saattanut tästä syystä tarjota palveluita vain yli 16- vuotiaille. Lisäksi on tärkeää huomioida, että yritys voi ostaa erilaisia palveluita alihankintana esimerkiksi mainostoimiston, tilitoimisto, henkilöstövuokraus yrityksen, sähköpostipalvelun tai analytiikkapalvelun tarjoajan kanssa, jolloin nämä tahot tekevät henkilötietojen käsittelyä yrityksen lukuun, silloin myös kyseinen alihankkija vastaa jatkossa suoraan sanktioiden uhalla asetuksen vaatimusten noudattamisesta. (EU:n tietosuoja-asetus 679/2016, 2 luku 8 art.; Oikeusministeriä 2018; Tietosuojalaki 1050/2018, 2:5 §; Tietosuojavaltuutetun www-sivut 2018)

Erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä. Tällaisista tiedoista ilmenee henkilön esim. henkilön etninen alkuperä, poliittisia mielipiteitä, uskonnollinen vakaumus, ammattiliiton jäsenyys tai terveyttä koskevia tietoja. (Tietosuojavaltuutetun www-sivut 2018)

5.2 Rekisterinpitäjän roolit ja vastuut

Osoitusvelvollisuus

Tietosuoja-asetus velvoittaa organisaatioita osoittamaan noudattavansa tietosuoja-asetusta esimerkiksi dokumentoimalla henkilötietojen käsittelyyn liittyvät prosessit ja muut käytännön tietosuojatoimenpiteet. Osoitusvelvollisuuden tarkoituksena on näyttää, miten rekisterinpitäjä kunnioittaa rekisteröityjen eli henkilötietojen käsittelyn

kohteena olevien tietosuojaa. Sen toteuttaminen lisää myös rekisterinpitäjän toimintaan kohdistuvaa luottamusta. Osoitusvelvollisuus merkitsee käytännössä sitä, että vain riittävällä ja asianmukaisella dokumentaatiolla voi osoittaa olevansa tilintekokykyinen ja katsoa toimivansa asetuksen mukaisesti. Tietosuojaperiaatteet, kuten lainmukaisuus, kohtuullisuus, läpinäkyvyys ja käyttötarkoitussidonnaisuus sekä tietojen minimointi ovat osoitusvelvollisuuden piirissä ja ne konkretisoidaan käytännön tasolle. Osoitusvelvollisuus edistää tietosuojatoimiensuunnitelmallisuutta ja läpinäkyvyyttä henkilötietojen käsittelyssä. Oleellinen osa tietosuojaa on kertoa esimerkiksi järjestelmän käyttäjille, mitä tietoa heistä on tallennettuna järjestelmään. Näistä kerrotaan henkilörekisteriselosteessa, jonka tulee olla järjestelmän käyttäjien saatavilla. Tietosuojaseloste on laajennettu rekisteriseloste, jossa lisäksi informoidaan rekisteröidyn oikeuksista. Samaan henkilörekisteriin kuuluvat erikseen pidetyt atk-rekisterit ja manuaaliset luettelot sekä kortistot, jos niitä käytetään saman tehtävän hoitamiseen. Lisäksi velvollisuutta toteutetaan käsittelytoimia koskevilla ohjeistuksilla sekä muilla henkilötietojen käsittelyyn liittyvien prosessien dokumentoinnilla. (EU:n tietosuoja asetus 679/2016, 3 art.; Tietosuojavaltuutetun www-sivut 2018)

Rekisterinpitäjällä on vastuu varmistaa ja osoittaa, että henkilötietojen käsittely noudattaa tietosuoja-asetusta. Käytännössä tämä tapahtuu laajalla käsittelyn dokumentaatiolla ja seurannalla, joita tarkistetaan säännöllisesti sekä tarpeen mukaan päivitetään. (EU:n tietosuoja-asetus 679/2016, 4 art.)

Vaikutustenarviointi ja ilmoitusvelvollisuus

Tietosuojaa koskevasta vaikutustenarvioinnista (Data Protection Impact Assessment, DPIA) säädetään tietosuoja-asetuksessa sekä siihen liittyvästä mahdollisesta valvontaviranomaisen ennakkokuulemisesta. Jos henkilötietojen käsittely tilanteeseen kohdistuu korkea riski on rekisterinpitäjän tehtävä tietosuojaa koskeva vaikutustenarviointi. Vaikutustenarviointi tulee tehdä esimerkiksi käsiteltäessä laajamittaisesti erityisiin henkilötietoryhmiin kuuluvia tietoja, joita ovat terveydentilatiedot tai rikostuomiota tai rikkomuksia koskevat tiedot. Tällöin on kyseessä riskiperusteinen ilmoitus velvollisuus. Lisäksi tietosuoja-asetus asettaa tarkennettuja vaatimuksia tietoturvaan sekä ilmoitusvelvollisuuden tietoturvaloukkaustilanteissa. (OpiTietosuojaa.fi www-sivut 2018)

Tietoturvaloukkauksista ilmoittaminen

Rekisterinpitäjän on varauduttava mahdollisiin tietoturvaloukkauksiin laatimalla toimintaohjeet tietoturvaloukkaustilanteita varten. Henkilötietojen tietoturvaloukkauksesta on tehtävä ilmoitus valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta. Tietoturvaloukkauksesta on ilmoitettava ilman aiheetonta viivytystä myös rekisteröidylle, mikäli loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietosuoja-asetuksen mukaan ilmoitus voidaan jättää tekemättä esimerkiksi silloin, jos loukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä tai jos tietoturvaloukkauksen kohteena olleet henkilötiedot ovat olleet salatussa muodossa eivätkä vaadittavat salausavaimet ole vaarantuneet. (EU:n tietosuoja-asetus 679/2016, 32-34 art.)

Sanktiot

Tietosuojalaki (2018/1050) säätää, että tietosuojavaltuutettu jatkaa valvontaviranomaisena ja kasvavien työtehtävien vuoksi tietosuojavaltuutetun toimistoon perustetaan kaksi apulaistietosuojavaltuutetun virkaa sekä perustetaan viisijäseninen asiantuntijalautakunta. Tietosuojavaltuutettu voi asettaa yritykselle, yhteisölle tai viranomaiselle uhkasakon tietojen luovuttamista koskevan määräyksensä tehostamiseksi. Säännösten rikkomisesta voidaan määrätä hallinnollinen seuraamusmaksu, joka voi olla lievemmissä rikkomuksissa enintään 10 miljoona euroa tai 2 % yrityksen kokonaisliikevaihdosta ja vakavammissa rikkeissä enintään 20 miljoona euroa tai 4 % yrityksen kokonaisliikevaihdosta. Seuraamusmaksu perustuu tietosuoja-asetukseen ja käytössä on myös lievempiä keinoja kuten huomautus. Seuraamusmaksua ei kuitenkaan tietosuojalain mukaan sovelleta julkisella sektorilla tapahtuvaan henkilötietojen käsittelyyn. (Oikeusministeriö 2018) Mahdollisia sanktioita rikkomustilanteissa voi vähentää organisaation aktiiviset panostukset tietoturvallisuuteen ja tietosuojan ylläpitoon. Tämän vuoksi on tärkeää, että organisaatiot panostavat tietoturvaan ja tietosuojaan alusta asti kaikessa kehitystyössä.

5.3 Tietosuojavastaava

Yrityksessä tulee olla nimettynä tietosuojavastaava, jos siellä käsitellään suurempia määriä arkaluonteisia henkilötietoja tai, kun yrityksen keskeisiin toimintoihin kuuluu rekisteröityjen henkilöiden järjestelmällinen seuranta. Tietosuoja-asetuksessa on säädettytietosuojavastaavan tehtävistä ja asemasta, jonka lisäksi ohjeistusta tietosuojavastaavista on antanut EU:n tietosuojatyö-ryhmä WP 29. Tietosuojavastaavan tehtäviin sisältyy organisaation tietojenkäsittelyyn liittyvien toimintatapojen seuranta ja huolehtia, että ne vastaavat asetuksessa tai muualla erityislainsäädännössä säädettyä. Tietosuojavastaava neuvoo ja auttaa organisaatiota tietosuojaperiaatteiden ja -vaatimusten toteuttamisessa sekä toimii yhteyshenkilönä sekä valvontaviranomaiseen, että rekisteröityihin. Tietosuojavastaava ei kuitenkaan vastaa organisaation henkilötietojen käsittelyn lainmukaisuudesta, vaan siitä on vastuussa yrityksen johto. (EU:n tietosuoja asetus 679/2016, 37-39 art.; Oikeusministeriö 2018)

Tietosuojavastaavan tehtävien hoidon selkeyttämiseksi ja toimenkuvan hallitsemiseksi on hyvä laatia tietosuojavastaavan tehtäväkuvaus. Sen avulla tietosuojavastaava voi määritellä, aikatauluttaa ja seurata toimenkuvaan kuuluvia rutiinitehtäviä sekä varata riittävästi aikaa jokapäiväiselle tietosuojatoiminnalle, kuten esimerkiksi erilaisten tietosuojaongelmien ratkaiseminen ja henkilöstön neuvontaa tietosuojakysymyksissä. (Valtiovarainministeriö 2016b, 33).

Tietosuojavastaavan ja tietosuojaryhmän tehtävänä on toimia johdon tukena, laatia ja jalkauttaa ohjeita, seurata ja tiedottaa henkilöstöä lainsäädännön muutoksista, varmistaa henkilöstön perehdytysprosessi, kouluttaa ja neuvoa henkilöstöä tietosuoja asioissa, henkilöstön tietosuoja- ja tietoturva osaamisen mittaaminen sekä henkilötietojen käsittelyn valvonta. Lisäksi tietosuojapoikkeamien raportointi yrityksen johdolle, tietotilinpäätöksen määrämuotoinen kokoaminen, vaikuttavuusarvioiden laatiminen (eng. PIA) sekä yhteydenpito valvontaviranomaisiin. (Tietosuojavastaavan www-sivut 2018; OpiTietosuojaa.fi www-sivut 2019)

5.4 Rekisteröidyn oikeudet

Suostumus

Yrityksen on jokaisen tiedon kohdalta pystyttävä näyttämään, että sen keräämiseen on saatu rekisteröidyn henkilön suostumus tai jokin muu asetuksen edellytyksistä on täyttynyt. Yrityksen rekrytoinnin osalta pääsääntöisesti on hankittava työnhakijan suostumus, mikäli työnantaja kerää tietoja muualta, kuin työnhakijalta itseltään. Lisäksi suostumuksen käsite on vahvassa roolissa työelämän tietosuojalain tarpeellisuusvaatimuksen kohdalla. Kyseisen lainkohdan mukaisesti henkilötietojen käsittelyn tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella. (EU:n tietosuoja asetus 679/2016, 6 art., 13-14 art.)

Rikoslaista poistetaan henkilörekisteririkos ja rikoslaissa säädetään rangaistavaksi esimerkiksi tilanne, jossa rekisterinpitäjän palveluksessa oleva henkilö luvatta tutkii henkilötietoja vastoin niiden käyttötarkoitusta. Kyse on tietosuojarikoksesta, josta tuomitaan sakkoa tai vankeutta enintään yksi vuosi. (Oikeusministeriö 2018)

Oikeus tulla unohdetuksi

Rekisteröidyillä on jo aiemmin ollut esimerkiksi tarkastus- ja korjausoikeus tietoihinsa, mutta jatkossa on mahdollisuus vaatia myös omien tietojen hävittämistä (right to be forgotten). Oikeutta tulla unohdetuksi ei sovelleta lakisääteisiin rekistereihin. Tietojen poistaminen ei ole mahdollista lakisääteisen tehtävän suorittamiseen liittyvän käsittelyn yhteydessä. (EU:n tietosuoja-asetus 679/2016, 13-14 art.)

Oikeus saada tietoa henkilötietojen käsittelystä

Rekisterinpitäjällä on informointivelvoite eli velvollisuus tiedottaa avoimesti henkilötietojen käsittelystä. Tietosuoja-asetus osin tarkentaa ja laajentaa henkilötietolaissa säädettyä, ja uusia viestittäviä asioita ovat henkilötietojen säilytysajan ja tietosuojavastaavan yhteystietojen ilmoittaminen. Henkilötietojen käsittelystä annetun

informaation pitäisi olla tiiviissä ja ymmärrettävässä muodossa sekä helposti saatavilla. (EU:n tietosuoja-asetus 679/2016, 13-14 art.)

Uusi tietosuojalaki säätää sananvapauden, tutkimuksen ja arkistoinnin turvaamiseksi poikkeuksia henkilötietojen käsittelyedellytyksiin esimerkiksi, kun kyse on sananvapaudenturvaamisesta juornalismissa tai tieteellisessä ja historiallisessa tutkimuksessa niiden tavoitteiden kannalta. Poikkeukset merkitsevät mm. sitä, että rekisteröidyllä ei näissä tapauksissa ole esimerkiksi oikeutta tarkastaa itseään koskevia tietoja, mutta edellyttää myös henkilötietojen käsittelijä laatii tietosuojaa koskevan vaikutustenarvioinnin tai sitoutuu noudattamaan erityisiä käytännesääntöjä. Tutkimusta ja tilastointia varten on mahdollista käsitellä mm. terveyttä, uskontoa, seksuaalista käyttäytymistä ja poliittisia näkemyksiä koskevia tietoja. (Oikeusministeriö 2018)

Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada pääsy omiin henkilötietoihinsa eli tarkastusoikeus. Joka tarkoittaa sitä, että rekisterinpitäjän on rekisteröidyn pyynnöstä ilmoitettava, käsitelläänkö häntä koskevia henkilötietoja vai ei sekä toimitettava nämä tiedot pyydettäessä henkilölle. Tietosuoja-asetuksessa ei aseteta määrämuotoa pyynnön tekemiselle, jolloin pyynnön voi tehdä muullakin tavoin kuin kirjallisesti ja omakätisesti allekirjoitettuna. Rekisterinpitäjä voi tarvittaessa pyytää rekisteröityä toimittamaan lisätietoja henkilöllisyyden vahvistamiseksi, jotta rekisteröidyn oikeus voidaan toteuttaa loukkaamatta muiden oikeuksia tai vapauksia. Tietosuoja-asetuksen mukaan rekisteröidyn pyyntöön tulisi vastata kuluvan kuukauden aikana. (EU:n tietosuoja-asetus 679/2016, 13 art.)

Oikeus tietojen oikaisemiseen

Tietosuoja- asetus säätää, että rekisteröidyllä on oikeus pyytää rekisterinpitäjää oikaisemaan häntä koskeva virheellinen henkilötieto tai pyytää täydentämään puutteelliset henkilötiedot. Oikeus tietojen oikaisemiseen vastaa nykysääntelyä ja voidaan toteuttaa jatkossa vastaavalla menettelyllä. Tietosuoja-asetuksessa ei oteta kantaa menettelyyn, jolla pyyntö on toteutettava, mutta siinä määritellään määräaika sille, missä

ajassa rekisterinpitäjän on käsiteltävä rekisteröidyn pyyntö. Viranomaisen toimenpiteistä tulee asianomaista informoida kuukauden kuluessa pyynnöstä, mutta käsiteltävä ilmanaiheetonta viivytystä. Tietyin edellytyksin määräaikaa on mahdollista jatkaa. (EU:n tietosuoja-asetus 679/2016, 13 art.)

Rekisteröidyn oikeus saada ilmoitus tietoturvaloukkauksesta

Rekisterinpitäjällä on velvollisuus ilmoittaa rekisteröidylle hänen henkilötietoihinsa kohdistuneesta tietoturvaloukkauksesta ja vastaavasti rekisteröidyllä on oikeus saada ilmoitus aiheutuneesta tietoturvaloukkauksesta. Tämä on tietosuoja-asetuksessa säädetty uusi oikeus. Oikeus saada ilmoitus esimerkiksi henkilötietojen vuotamisesta ulkopuolisille on tärkeä osa rekisteröidyn oikeuksia. (EU:n tietosuoja-asetus 679/2016, 13 art.)

Oikeus siirtää tiedot järjestelmästä toiseen

Tietosuoja-asetuksen mukaan henkilöllä on oikeus siirtää häntä koskevat tiedot toiselle rekisterinpitäjälle koneluettavassa muodossa, mikäli se on teknisesti mahdollista. Siirto-oikeutta ei kuitenkaan sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamisessa tai julkisen vallan käyttämisessä. (EU:n tietosuoja-asetus 679/2016, 20 art.)

5.5 Henkilöstön tietosuoja ohjeistukset ja kouluttaminen

Hyvä tietosuojan hallinta edellyttää henkilöstön ohjeistamista ja kouluttamista. On tärkeää, että työntekijöille annetaan selkeät ja tarkat tiedot siitä mitä heiltä odotetaan henkilötietojen suojaamisen osalta. Vastuualueiden, roolien ja raportointikanavien pitää olla mahdollisimman yksinkertaisia ja selkeitä ottaen huomioon yrityksen toimialat ja erityispiirteet. Selkeällä organisaatiokaavalla ja työnjaolla vältetään epäselvyyksiä, kuka arkipäivässä vastaa tietosuojaan liittyvistä asioista ja miten pitää toimia eri

tilanteissa. Moni työntekijä haluaa tehdä työnsä mahdollisimman hyvin ja laadukkaasti henkilötietojen suojausta toteuttaen, jota yritys tukee selkeillä sisäisillä kirjallisilla ohjeilla. (Elinkeinoelämän keskusliitto 2018; OpiTietosuojaa www-sivut 2018)

Henkilöstön kouluttamisessa korostuu myös viestinnän tärkeys. Jatkuvasti muuttuvassa työelämässä oikean tai uuden toimintatavan sisäistäminen on haasteellista, jos ei käytännössä tiedä, mistä on kyse ja asia ei tunnu järkevältä arjen työtehtävissä. Henkilökunnan koulutusta suunniteltaessa on hyvä huomioida, että koulutus kohdistetaan ja paketoidaan oikealla tavalla, jotta työntekijät voivat samaistua siihen. Koulutustilaisuus on tehokas tapa kouluttaa uusia asioita etenkin, kun otetaan uudet rutiinit ja toimintatavat käyttöön lain muutosten johdosta. Henkilöstöä voi opettaa ja ohjata monella eri tavalla yksittäisten asioiden osalta esimerkiksi uutiskirjeen tai blogikirjoituksen kautta, tiimipalaverissa tai kahdenkeskisissä keskusteluissa tilanteen ja tarpeen mukaan. Tietosuoja kouluttajien tulisi olla asiantuntijoita ja kokeneita omassa työssään. Koulutuksen aikana on hyvä käydä avointa keskustelut, jotka avaavat koulutuksen sisältöä sekä estävät mahdollisia väärinymmärryksiä. Koulutus olisi hyvä toteuttaa vuorovaikutteisena ja osallistujia osallistavana kokonaisuutena. Koulutuksessa olisi tärkeää käydä asioita läpi käytännön läheisesti, jolloin tieto on helpompi soveltaa myös omaan työhönsä. (Frisk 2005, 16, 29-31; Elinkeinoelämän keskusliitto 2018)

Vaikeinta on usein oppia vanhoista tavoista pois eli organisaatio tai henkilö jättämään vanhat tottumukset ja hyväksymään uusia toimintatapoja, mutta sinnikkyys palkitaan. Johdonmukaisella toimintatavalla sekä jatkuvan viestinnän ja koulutuksen kautta asia ei pääse unohtumaan. Tietosuojan seuranta ja parantaminen ovat yrityksessä jatkuva prosessi (Kuvio 5.), jonka kautta voidaan nopeallakin aikataululla reagoida mahdollisiin puutteisiin toimintatavoissa ja menettelyissä. (OpiTietosuojaa.fi www-sivut 2018.)

Kuvio 5. Tietosuojan seuranta ja parantaminen ovat yrityksessä jatkuva prosessi (Opi-Tietosuojaa.fi www-sivut 2018).

6 OPINNÄYTETYÖN MENETELMÄLLISET LÄHTÖKOHDAT

6.1 Käytettävät menetelmä

Tapaustutkimus on empiirinen, eli kokemusperäinen tutkimus ja vaatii empiirisiä tutkimusmenetelmiä. Tutkimusstrategiana tässä opinnäytetyössä on tapaustutkimus eli case-tutkimus, jossa tutkittava tapaus muodostaa jonkinlaisen kokonaisuuden. Tapaustutkimuksessa tutkitaan yksittäistä tapahtumaa, rajattua kokonaisuutta (esim. syksyllä 2018 yrityksessä x henkilöstön tietosuojakyse ly) tai yksilöä käyttämällä aineiston keruussa eri metodeja. Käytössä ovat yhtä hyvin kvantitatiiviset kuin kvalitatiivisetkin menetelmät ja tutkimus perustuu tutkimuskohteen havainnointiin ja mittaamiseen. Tapaustutkimuksessa tavoitteena on ilmiöiden kuvailu ja syvällisemmän ymmärryksen lisääminen huomioiden siihen liittyvät olosuhteet pyrkimättä kuitenkaan yleistettävään tietoon. Opinnäytetyöhön on valittu kaksi empiiristä tutkimusmenetelmää sillä perusteella, että ne tuottavat mahdollisimman paljon tutkimuskysymyksiin kohdennettua tietoa yrityksen tietosuojan nykytilanteesta. Käyttämällä samaan aikaan useampaa tutkimusmenetelmää, saadaan laajempia näkökulmia ja siten voidaan lisätä tutkimuksen reliabiliteettiä eli luotettavuutta. (Hirsjärvi, Remes & Sajavaara 2009, 134-135, 210-211; Kuisma 2018, 17-18; KvaliMOTV www-sivut 2018) Tässä tapaustutkimuksessa on tarpeen mukaan koottu sekä laadullista, että määrällistä tutkimusta sopivana kokonaisuutena niin, että tutkimusongelma saadaan ratkaistua.

Opinnäytetyön tutkimusmenetelminä käytetään kvalitatiivista kyselytutkimusta sekä laadullista haastattelua**.** Opinnäytetyössä käytetään puolistrukturoituakyselyä, jossa on monivalintakysymyksiä sekä avoimia kysymyksiä. Lisäksi tutkimuksessa käytetään avointen kysymysten osalta kvalitatiivista eli laadullista menetelmää. (Hirsjärvi ym. 2009, 180-181). Opinnäytetyön tekijä kokoaa kyselyn ja tietosuojavaltuutetun haastattelu vastauksista tunnistetut riskit ja niiden merkitykset, analysoi sekä laatii kehittämissuunnitelma ehdotuksen yritykselle.

Suurimmaksi osin monivalintakysymyksiin pohjautuva kyselylomake laaditaan Webropol- työkalulla, johon kohderyhmän jäsenet saavat kutsulinkin ja infon

sähköpostitse. Vastaukset käsitellään niin, ettei yksittäisiä vastaajia voida tunnistaa. Kyselylomakkeen kysymykset käsitellään yrityksen tietosuojaryhmässä ja kysely esitestataan ennen sen toteuttamista. (Hirsjärvi ym. 2009, 196-197). Tutkimusmenetelmä on tapaustutkimus ja tutkimuksen tarkoitus on kehittävä (Koppa www-sivut 2018).

Kyselylomake on kvantitatiiviselle tutkimukselle tyypillinen aineistonkeruu menetelmä, jolla saadaan kerättyä laaja otos ja kysymykset esitetään kaikille vastaajille samalla tavalla. Opinnäytetyön aineisto kerättiin strukturoiduilla kyselylomakkeilla (Liite 1.), joissa oli sekä monivalintakysymyksiä että avoimia kysymyksiä. Käytössä ei ollut valmista mittaria, joten tätä tutkimusta varten laadittiin uusi mittari. Lomakkeen kysymykset laadittiin EU:n tietosuoja-asetuksen pohjalta.

Kyselylomake on luotu pääsääntöisesti strukturoituja monivalintakysymyksiä käyttäen. Monivalintakysymyksen hyviä puolia ovat, että ne auttavat vastaajaa tunnistamaan kysyttävän asian nopeasti ja tuotettuja vastauksia on paljon helpompi käsitellä ja analysoida tietokoneella. (Hirsijärvi ym. 2009, 182–193.) Tarkemman informaation saamiseksi kyselyssä on myös avoimia kysymyksiä.

Lomakkeesta pyrittiin tekemään mahdollisimman selkeä ja helppo lukuinen, koska aihe on laaja ja käsitteet ovat monille vastaajista vielä vieraampia. Webropol- kysely laadittiin niin, että jokaiseen kysymykseen tuli vastata jotakin, että kyselyä pääsi jatkamaan eteenpäin. Näin kysely työkalu kannustaa vastaajaa vastamaan jokaiseen kysymykseen. Vaihtoehtokysymyksissä oli mahdollisuus valita useampi vastausvaihtoehto sekä mahdollisuus kommentoida vastausta avoimeen tilaan omin sanoin.

Kysely esitestattiin viidellä henkilöllä. Vastauksien ja tietosuojaryhmän vetäjän sekä hr- asiantuntijan kommenttien perusteella kyselyyn tehtiin pieniä parannuksia. Lomakkeen alussa kysytään vastaajien taustatiedoksi millä organisaation tasolla vastaaja toimii ja osasto, jolla hän työskentelee. Taustatietoja kyselyssä kysytään vain siltä osin, kun niillä on lisäarvoa toimeksiantajalle.

Ensimmäisessä osiossa kysytään henkilötietojen käsittelyyn liittyviä asioita. Yritys Oy:ssä käsitellään erilaisia henkilötietoja kuten esim. opiskelijoiden, asiakkaiden, yhteistyökumppaneiden ja oman henkilöstön tietoja. Tämän lisäksi on oleellista

kartoittaa millaisia henkilötietoja ja miten niitä organisaatiossa tarkalleen käsitellään sekä miten henkilötiedot Yritys Oy:ssä hankitaan, koska siitä ei ollut ihan selkeää tietoa.

Toisessa osiossa käsitellään organisaation hallussa olevia tietovarantoja ja tietojen säilyttämistä. Tietosuoja-asetuksen mukaan henkilötietojen käsittelyyn tarvitaan asianomaisen suostumus. Lisäksi kartoitettiin henkilörekisterien suojausta, onko rekisteriselosteet laadittu ja niiden tarkoituksen ymmärtämistä sekä onko henkilötietojen säilytysajatmääritelty ja henkilöstön tiedossa.

Kolmannessa osiossa keskitytään Yritys Oy:n tietojen käsittelyn menettelytapoihin ja periaatteisiin. Tässä osiossa kartoitetaan olemassa olevaa ohjeistusta asioista sekä miten henkilöstö ymmärtää tietosuojaan liittyvät käsitteet, toimintatavat ja vastuut sekä millainen on heidän lisätiedon tarpeet tietosuojaa ja tietoturvallisuutta koskevissa asioissa omassa työssään. Osiossa kartoitetaan tarkemmin myös rekisteröidyn oikeuksien toteutuminen tietosuoja-asetuksen mukaisesti sekä miten dokumentteja ja missä muodossa niitä käsitellään, säilytetään ja arkistoidaan Yritys Oy:ssä. Sähköpostia käytetään yrityksessä paljon ja sitä käytetään myös henkilötietojen käsittelyyn, jonka vuoksi kyselyssä kartoitettiin tarkemmin sähköpostin käyttöä henkilötietojen käsittelyssä.

Tietosuojan valvontaa ja seurantaa kartoitetaan kyselyn neljännessä osassa. Kyselyyn sisällytettiin kysymyksiä myös tietoturvallisuuteen liittyen Yritys Oy:n tietotarpeet huomioiden tietosuoja-asetuksen mukaisesti, vaikka tämä opinnäytetyö on rajattu käsittelemään vain tietosuojaa. Tämä osio antaa myös tietoa, miten tietosuoja- ja tietoturvallisuus on yrityksessä ymmärretty, millaista ohjeistusta ja valvontaa on ja mitä pitäisi vielä kehittää tai parantaa, jotta toiminta on tietosuoja-asetuksen säätämällä tasolla. Kyselylomakkeen lopussa kartoitetaan avoimella kysymyksellä henkilöstön tarpeita ja toiveita tietosuoja koulutuksen sisältöön sekä toteuttamistapoihin.

6.2 Opinnäytetyön aineiston keruumenetelmät

Puolistrukturoitu kysely

Empiirinen eli tutkimuksellinen osuus tehdään puolistrukturoidunkyselyn avulla, jolla kartoitetaan Yritys Oy:n henkilörekistereiden määrä ja niiden nykytila. Kysely toteutetaan käyttäen verkkoselain-pohjaista Webropol-työkalua. Aineistoa käsittelee ainoastaan tutkija, jolle yrityksen Webropol-työkalun pääkäyttäjä on luonut tunnukset opinnäytetyön toteuttamista varten. Kyselyn tiedot säilytetään Webropol-työkalussa.

Opinnäytetyössä käsitellään kyselyn vastaajien henkilötietoja lainmukaisesti, asianmukaisesti ja vastaajan kannalta läpinäkyvästi. Heitä informoidaan tietosuoja-asetuksen edellyttämällä tavalla henkilötietojen käsittelystä kirjallisesti ennen kyselyyn vastaamista ja vastaamalla kyselyyn vastaaja antaa suostumuksensa antamiensa tietojen käsittelyyn. (Tietoarkisto www-sivut 2018)

Tietosuoja-asetuksesta ja tietosuoja kyselystä informoitiin koko henkilöstöä Yritys Oy:n intrassa. Tietosuoja kyselyyn laaditaan erillinen info vastaajille, joka lähetettiin kyselyn yhteydessä vastaajille sähköpostiin. Lisäksi vastauslomakkeen alussa vielä käytiin läpi vastaamiseen liittyviä tärkeitä pääkohtia. Näin varmistettiin, että vastaaja saa riittävästi tietoa tietosuoja kyselystä, sen tavoitteista sekä vastaajan oikeuksista tietosuoja-asetuksen mukaisesti.

Haastattelu

Nykytilan kysely kartoituksen jälkeen vielä haastateltiin Yritys Oy:n tietosuojavastaava, että opinnäytetyöhön saadaan mahdollisimman tuorein tieto organisaation tietosuojan nykytilasta. Tuloksien perusteella laaditaan yritykselle kehittämisehdotuksia, jotta yrityksen toiminta vastaisi tietosuoja-asetuksessa määrättyjä toimenpiteitä.

6.3 Vastaajien valinta

Kohderyhmä koostui yhteensä 127 vastaajasta, jotka oli ennalta valittu Yritys Oy:n tietosuojaryhmän sekä hr-asiantuntijan toimesta. Henkilöiden valinta perustui siihen, että heidän tiedettiin varmasti olevan tekemisissä yrityksen henkilörekistereiden kanssa. Ennakkovalinnan suoritti Yritys Oy:n tietosuojaryhmä sekä hr-asiantuntija, ja sen osuus ei ollut osa tätä opinnäytetyötä. Tutkimuksessa kysely lähetettiin sähköpostitse Webropol-työkalun kautta yrityksen valituille vastaajille, jotka työssään käsittelevät henkilötietoja. Näin saatiin mahdollisimman kattavan sekä todellinen kuva yrityksen henkilötietietojen käsittelyn ja säilyttämisen nykytilasta sekä henkilöstön tietosuoja tiedon tasosta.

Tutkimus oli luonteeltaan kvantitatiivinen. Tutkimusaineisto kerättiin puolistrukturoidulla kyselylomakkeella. Tietosuojakysely lähetettiin sähköpostilla valitulle kohdejoukolle (N = 127). Kyselyyn vastaamisaika oli ensin kaksi viikkoa, ja sitä pidennettiin viikolla ja muistutettiin vastaajia kyselyyn vastaamisesta sähköposti muistutuksella sekä yrityksen Intran sivuilla. Kohdejoukkona olivat yrityksen henkilöstö, jotka työssään käsittelevät henkilötietoja tai rekistereitä. Vastattuja lomakkeita palautui yhteensä 70 kappaletta, vastausprosentti oli näin ollen 55 %.

Tietosuojavastaavan haastattelu

Kyselyn lisäksi haastateltiin Yritys Oy:n tietosuojavastaavaa, koska yrityksen tietosuojaryhmän henkilöissä oli opinnäytetyön aikana henkilövaihdoksia. Haastattelun tavoitteena oli vielä tarkentaa Yritys Oy:n tietosuojan nykytilaa.

6.4 Kehittämistyön aineistoin analysointi

Kysely laadittiin, toimitettiin vastaajille sekä analysoitiin yrityksen Webropol- ohjelmaa käyttäen. Tämän jälkeen tutkijana tein johtopäätöksiä vertaamalla keräämääni aineistoa teoriaan, aikaisempiin tutkimuksiin ja omiin kokemuksiini. Avoimien

kysymysten ja haastattelun vastaukset analysoitiin sisällön erittelyllä, jolla Tuomen ja Sarajärven (2006, 107.) mukaan tarkoitetaan dokumenttien analyysia, jossa kuvataan laadullisesti esimerkiksi tekstin sisältöä. Sisällön erittelyssä tiedot voidaan kerätä sanallisessa muodossa, sanallisina ilmaisuina tai sitten määrällisessä muodossa, luokiteltuina ja tilastoituina. Johtopäätökset tullaan kertomaan opinnäytetyön johtopäätökset ja pohdinta kappaleessa. Tuloksien esittämisessä hyödynnetään grafiikkaa, prosentteja sekä perustunnuslukuja.

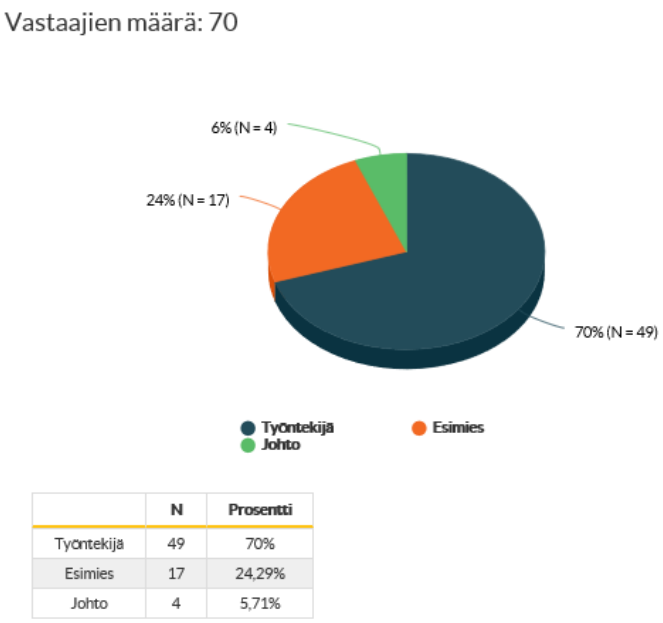
6.5 Tulosten luotettavuus

Opinnäytetyötä tarkastellaan reliabiliteetti ja validiteetti huomioiden, sekä miten hyvin tuloksia voidaan hyödyntää toimeksiantajan näkökulmasta sekä yleisesti. Puolistrukturoitukysely tutkimusmenetelmällä voidaan saada luotettavia vastauksia asetettuihin tutkimusongelmiin. Kyselyn huolellinen laadinta, esitestaus, oikea kysymysten asettelu ja sisällöllinen kattavuus sekä vastaajien informointi parantavat opinnäytetyön luotettavuutta. Mittausvirheiden mahdollisuus pienenee, kun analysoinnissa käytetään Wepropol- työkalua, jolla myös kysely laaditaan. Lisäksi kyselyyn vastaa valittu kohdejoukko, jonka otanta on riittävän suuri. (KAMK www-sivut 2018)

7 TUTKIMUSTULOKSET

7.1 Tietosuoja kysely Yritys Oy:n henkilöstölle

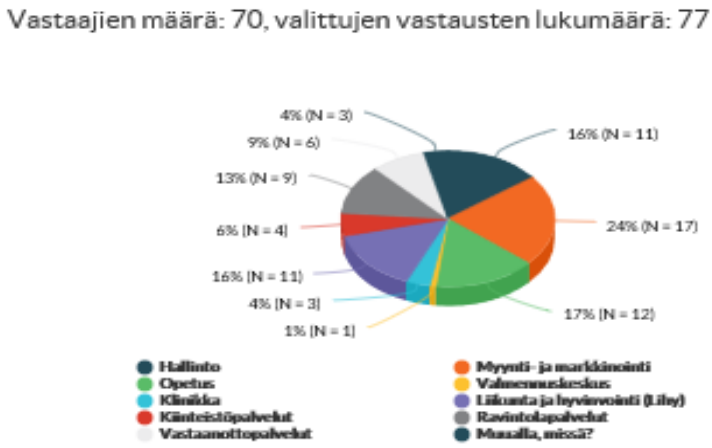
Tietosuojakysely lähetettiin sähköpostilla valitulle kohdejoukolle (N = 127). Kohdejoukkona olivat yrityksen henkilöstö, jotka työssään käsittelevät henkilötietoja tai rekistereitä. Vastattuja lomakkeita palautui yhteensä 70 kappaletta, vastausprosentti oli näin ollen 55 % (Kuvio 6.). Kaikista vastaajista työntekijöitä oli 49 hlö (70 %), esimiehiä 17 hlö (24,29 %) ja johtoa 4 (6 %).



	N	Prosentti
Työntekijä	49	70%
Esimies	17	24,29%
Johto	4	5,71%

Kuvio 6. Tietosuoja kyselyyn vastasi yhteensä 70 henkilöä (N = 127).

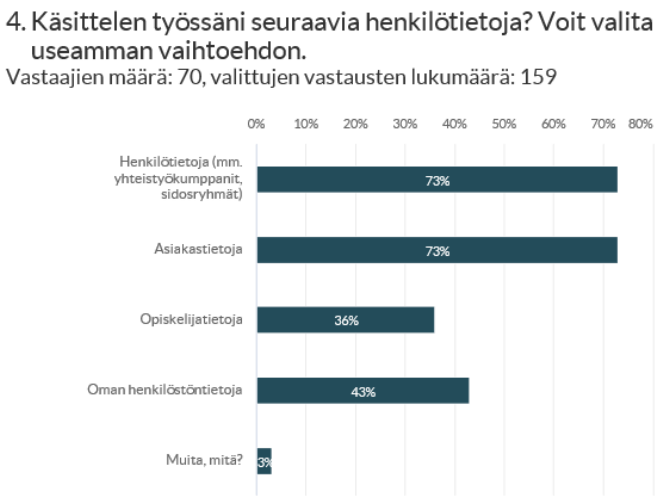
Tässä opinnäytetyössä käsitellään vain yleisesti kysymystä 3., missä käsiteltiin vastaajan osastoa, jossa hän työskentelee (Kuvio 7.). Kysymykseen vastasi 70 vastaajaa, joista 7 henkilöä työskenteli useammalle osastolle yhtiöissä. Jokaiselta osastolta oli ainakin yksi vastaaja vastannut kyselyyn, mutta eniten vastaajia oli myynti- ja markkinointi osastolta 17 kpl, opetuksesta 12 kpl sekä hallinnosta 11 vastaajaa ja ravintolapalveluista yhteensä 12 vastaajaa.



Kuvio 7. Kuviossa kuvataan vastaajien osastoja, joilla he työskentelevät (N = 70).

7.1.1 Henkilötietojen käsittely

Kyselyn vastaajista työssään henkilötietoja käsittelee (Kuvio 8.) lähes kaikki. Eniten he käsittelevät yhteistyökumppaneiden, asiakkaiden sekä sidosryhmien henkilötietoja (N = 51, 73 %). Opiskelijoiden henkilötietoja vastaajista käsitteli 36 % ja oman henkilökunnan tietoja 43 %. Lisäksi muita tietoja kysymykseen vastasi muutama vastaaja (3 %) ja he kertoivat käsittelevänsä kameravalvontaa tai asiakkaiden tai oman henkilöstön terveystietoja.



Kuvio 8. Kuviossa kuvataan vastaajien vastuksia millaisia henkilötietoja he käsittelevät työssään ja vastausvaihtoehdoista voi valita useamman.

Seuraavaksi kyselyssä tarkennettiin vielä millaisia henkilötietoja vastaajat käsittelevät työssään. Kuviossa 9. kuvataan tarkemmin, millaisia henkilötietoja 70 vastaajaa yrityksessä käsittelee. Yhteensä vastaajat vastasivat kysymykseen 628 kpl annetuista vaihtoehdoista. Eniten työssään he käsittelevät henkilötiedoista puhelinnumeroita (98,57 %), sähköpostiosoitteita (98,57 %), nimi tietoja (97,14 %), osoitteita (91,43 %), henkilötunnuksia (N = 40, 54,14 %), sopimustietoja (N = 33, 47,14 %) ja tilinumeroita (N = 32, 45,71 %).

Arkaluontoisia henkilötietoja henkilötunnuksen lisäksi, joita vastaajat työssään käsittelevät olivat mm. terveystiedot (N = 23, 32,86 %), alle 16 vuotiaan tiedot (N = 24, 34,29 %), sairauspoissaolo tiedot (N = 24, 34,29 %), palkkatiedot (N = 14, 20 %), videokuva (N = 8, 11,43 %).

	N	Prosentti
Nimi	68	97,14%
Osoite	64	91,43%
Puhelinnumero	69	98,57%
Sähköposti	69	98,57%
Henkilötunnus	40	57,14%
Terveystiedot	23	32,86%
Valokuva	19	27,14%
Alle 16-vuotiaan tietoja	24	34,29%
Osakerekisteri tietoja	5	7,14%
Videokuva	8	11,43%
Tilinumero	32	45,71%
Matkakulut	16	22,86%
Työhakemus	15	21,43%
Sairauspoissaolotietoja	24	34,29%
Opintotietoja	15	21,43%
Sopimustietoja	33	47,14%
Sosiaalisenmedian tietoja	14	20%
Kehityskeskustelu tietoja	14	20%
Työsuhdetietoja	18	25,71%
Työsopimus	18	25,71%
Palkkatiedot	14	20%
Verokortti	10	14,29%
HOIKS	5	7,14%
HOKS	10	14,29%
Muu, mikä?	1	1,43%

Avoimeen tekstikenttään annetut vastaukset

Piilota

Vastausvaihtoehdot	Teksti
Muu, mikä?	verkkolaskutietoja/Y-tunnus

Kuvio 9. Kuviossa vastaajien vastaukset millaisia henkilötietoja he tarkemmin työssään käsittelevät.

Kyselyssä kysyttiin vastaajilta, millaisia tietojärjestelmiä he työssään käyttävät Yritys Oy:n toiveesta, vaikka tässä opinnäytetyössä ei keskitytä tietoturvallisuuden asioihin tarkemmin, mutta se on tärkeä osa yrityksen tietosuojan hallintaa.

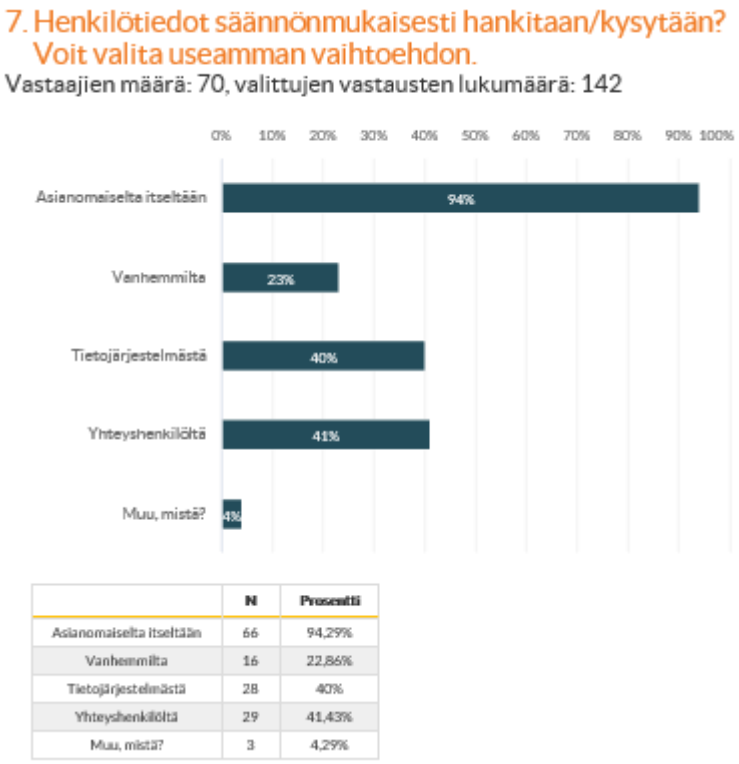
	N	Prosentti
VERP	51	72,86%
MaraPlan	17	24,29%
Liksa	3	4,29%
CRM	1	1,43%
Lanka	1	1,43%
Lasso	2	2,86%
HHP	9	12,86%
Centre	1	1,43%
Digital Bookers	7	10%
Lyyti	15	21,43%
Primus	5	7,14%
Mehiläisen järjestelmä mm. TyökykyKompassi	13	18,57%
Verifone	2	2,86%
File Maker Pro	4	5,71%
Oma Excel- taulukko/Word-tiedosto	42	60%
Kameravalvonta	7	10%
Avainkortit	11	15,71%
Sähköpostilistat	40	57,14%
KELA	4	5,71%
Vakuutusyhtiöt	4	5,71%
Muita, mikä?	13	18,57%

Kuvio 10. Kuviossa kuvataan Yritys Oy:n käytössä olevia järjestelmiä sekä sovelluksia, ja kysymyksellä kartoitettiin, kuinka moni vastaajista työssään käsittelee kyseisiä järjestelmiä, joissa henkilötietoja.

Edellä olevassa kuviossa 10. kuvataan tarkemmin yrityksen käytössä olevia järjestelmiä, joita henkilöstö käyttää työssään. Kolme eniten käytössä olevaa olivat VERP toimintajärjestelmä, jota käyttää 51 vastaajista, omia Excel/Word- taulukkoja käyttää 42 vastaajista sekä tallennettuja sähköpostilistoja myös käyttää 42 vastaajista. Lisäksi vastaajat käyttävät seuraavia järjestelmiä, joita ei ollut vastausvaihtoehdoissa, kuten Wilma, Webpropol, HEEROS, Abloy avainhallinta, Vita: laboratoriopalvelut, FirstBeat: hyvinvointianalyysi, Ergopro, postiviidakko uutistyökalu, kuvapankki, palomuuri, palvelemien käyttäjätiedot, GolfBox, ERS- hankkeen henkilötietolomakkeet sekä paperinen henkilötietolomake, jota ei ole sähköisesti saatavilla.

Seuraavassa kysymyksessä kartoitettiin, mistä vastaaja pääsääntöisesti saa henkilötiedot, joita työssään käsittelee (Kuvio 11.). Vastausvaihtoehtoja pystyi valitsemaan useamman, mutta keskiarvo vastaajien kohdalla oli kaksi eri vaihtoehtoa. 66 (94 %) vastaajista kertoi saavansa henkilötiedot suoraan asianomaiselta. 29 (41 %) vastaajista kertoo, että tiedot saadaan yhteyshenkilöltä ja 28 (40 %) vastaajaa yrityksen tietojärjestelmistä. Vastaajista 16 (23 %) ilmoitti saavansa tietoja myös vanhemmilta. Lisäksi

kolme vastaajista vastasi saavansa henkilötietoja kollegoilta, työntekijöiltä, omistajilta sekä opintopolusta.



	N	Prosentti
Asianomaiselta itseltään	66	94,29%
Vanhemmilta	16	22,86%
Tietojärjestelmästä	28	40%
Yhteyshenkilöltä	29	41,43%
Muu, mistä?	3	4,29%

Kuvio 11. Kuvion kysymyksessä kartoitettiin mistä vastaaja pääsääntöisesti saa henkilötiedot, joita hän työssään käsittelee.

7.1.2 Organisaation hallussa olevat tietovarannot ja tietojen säilyttäminen

Kysymyksellä kartoitettiin henkilöstöltä tietoja organisaation hallussa olevista tietovarannoista ja tietojen säilyttämisestä (Kuvio 12.). Vastausvaihtoehtoina olivat samaa mieltä, erimieltä tai en osaa sanoa. 42 (60 %) vastaajista vastasi, että asianomaisilta pyydetään suostumus hänen henkilötietojensa käyttämiseen, mutta 11 (15,71 %) vastaajista oli eri mieltä ja 17 (24,29 %) heistä ei osannut sanoa miten yrityksen käytäntö on. Kirjallinen suostumus dokumentoidaan 26 vastaajan mukaan, mutta 17 vastaajista oli eri mieltä ja suurin osa 27 heistä ei osannut sanoa, mikä on yrityksen käytäntö. Myös suurimmalle osalle vastaajista 38 (54,29 %) oli epäselvää, onko yrityksen käytössä olevat henkilörekisterit suojattuja ja henkilötietojen käsittely on turvattu. Kolme vastaajista oli eri mieltä ja suojauksesta samaa mieltä vastaajista oli 29 (41,43 %) hlö.

Yhdeksäntoista vastaajista oli samaa mieltä, että käytössä olevista henkilörekistereistä on laadittu rekisteriseloste, mutta ylipuolet 44 vastaajista ei osannut sanoa ja seitsemän heistä oli eri mieltä. Henkilöstöltä kysyttiin, onko henkilötietojen- ja rekistereiden säilytysajat määritelty yrityksessä. 49 (70 %) vastaajista ei osannut sanoa ja seitsemän heistä oli eri mieltä, vain 14 (20 %) oli samaa mieltä.

Rekisteriselosteet ovat jokaisen saatavilla väittämään 39 vastaajista ei osannut sanoa, 16 heistä oli eri mieltä ja 15 vastaajista kertoi olevansa tietoisia asiasta. Yrityksen rekisteriselosteisiin intrassa oli vastaajista perehtynyt 26 henkilöä ja 29 vastaajista oli eri mieltä sekä 15 vastaajaa ei osannut sanoa.

	Samaa mieltä	Eri mieltä	En osaa sanoa	Yhteensä	Keskiarvo	Mediaani
Asianomaiselta pyydetään suostumus hänen henkilötietojensa käyttämiseen	42	11	17	70	1,64	1
	60%	15,71%	24,29%			
Kirjallinen suostumus dokumentoidaan	26	17	27	70	2,01	2
	37,14%	24,29%	38,57%			
Käytössä olevat henkilörekisterit on suojattu ja henkilötietojen käsittely on turvattu	29	3	38	70	2,13	3
	41,43%	4,28%	54,29%			
Käyttämistäni henkilörekistereistä on laadittu rekisteriseloste	19	7	44	70	2,36	3
	27,14%	10%	62,86%			
Henkilötietojen- ja rekisterien säilytysajat on määritelty	14	7	49	70	2,5	3
	20%	10%	70%			
Rekisteriselosteet ovat jokaisen saatavilla	15	16	39	70	2,34	3
	21,43%	22,86%	55,71%			
Olen perehtynyt yrityksemme rekisteriselosteisiin intrassa	26	29	15	70	1,84	2
	37,14%	41,43%	21,43%			
Yhteensä	**171**	**90**	**229**	**490**	**2,12**	**2**

Kuvio 12. Kuviossa kuvataan vastaukset organisaation hallussa olevista tietovarannoista ja tietojen säilyttämisestä (N = 70).

Avoimena kysymyksenä kyselyssä kysyttiin: ” Mihin/kenelle henkilötietoja työssäsi voidaan luovuttaa tai tallentaa? (esim. järjestelmiin, yhteistyökumppaneille, kollegoille, asiakkaille, omiin tiedostoihin? jne.).” Kysymykseen vastasi kaikki 68

vastaajaa jotakin, mutta 3 vastausta ei antanut selkeää vastausta kysymykseen. Vastauksien yhteenvedossa ei lähdetä erottelemaan eri järjestelmiä elleivät ne eroa aiemmin kyselyssä olleiden vastauksien tiedoista.

Vastaukset voidaan luokitella seuraaviin ryhmiin:
Suluissa on kuvattuna vastaajien määrä luokittelu ryhmittäin.

Ei luovuteta ulkopuolisille (10)
Kollegoille ja talon sisällä (29)
Yrityksen tietojärjestelmiin (48)
Omiin tiedostoihin (Excel, Word, e-mail) (24)
Asiakkaille (4)
Esimiehille, johdolle (2)
Osakkeenomistajille (1)
Yhteistyökumppaneille ja alihankkijoille (20)
Viranomaistahoille (mm. KELA, Verotoimisto, vakuutusyhtiöt, opetushallitus, poliisi) (9)
Sisäiseen markkinointiin (4)
Arkistoon (1)

7.1.3 Tietojen käsittelyn menettelytavat ja periaatteet yrityksessä

Kyselyn väittämissä tietojen käsittelymenettelytavoista ja periaatteista yrityksessä kartoitettiin mm. onko yrityksessä tietosuoja-asetuksen vaatimia kirjallisia ohjeistuksia, onko ohjeistukset henkilöstön saatavilla ja onko tietosuoja asioista ollut koulutusta ja riittävästi tietoa saatavilla. Lisäksi onko henkilöstölle selkeä omat vastuut tietosuojaan liittyen.

Väittämät vastauksineen on kuvattu tarkemmin kuviossa 13. Lyhyesti yhteenvetona vastauksista voidaan kertoa, että kirjallisia ohjeita tai niiden olemassa olosta on vain muutamalla vastaajalla tietoa. Lisäksi vastaajista 51 (72,86 %) on eri mieltä, että olisi

saanut tietosuoja ja tietoturvaa koskevista ohjeista koulutusta ja riittävästi tietoa työpaikalla. Suurin osa vastaajista vastaa tietävänsä oman vastuunsa tietosuoja asioissa ja ymmärtää henkilötietoja- ja reksitereitä käyttäessä vaitiolo- ja salassapitovelvollisuuden velvoitteet.

	Samaa mieltä	Eri mieltä	En osaa sanoa	Yhteensä	Keskiarvo	Mediaani
Käytössäni olevista henkilörekistereistä on laadittu kirjalliset kuvaukset (rekisterien tietovirta)	13	13	44	70	2,44	3
	18,57%	18,57%	62,86%			
Olen analysoinut, mitä tietoturva- ja tietosuojariskejä käyttämieni henkilötietojen käsittelyyn liittyy (riskinarviointi)	21	29	20	70	1,99	2
	30%	41,43%	28,57%			
Henkilötiedon korjaamiseen liittyvästä menettelystä on kirjallinen ohjeistus	6	19	45	70	2,56	3
	8,57%	27,14%	64,29%			
Rekisteröidyn kielto-oikeuden toteuttamisesta on kirjallinen ohjeistus	3	15	52	70	2,7	3
	4,28%	21,43%	74,29%			
Henkilötietojen turvaloukkaus tilanteiden varalle on kirjallinen ohjeistus (Henkilötietojen luottamuksellisuus on vaarantunut)	3	16	51	70	2,69	3
	4,28%	22,86%	72,86%			
Henkilötietojen käsittelystä on laadittu tietosuojaa ja tietoturvaa koskevat ohjeet	12	10	48	70	2,51	3
	17,14%	14,29%	68,57%			
Tietosuojaa ja tietoturvallisuutta koskevat ohjeet ovat henkilöstön saatavilla	15	9	46	70	2,44	3
	21,43%	12,86%	65,71%			
Olen saanut tietosuojaa ja tietoturvaa koskevista ohjeista koulutusta ja riittävästi tietoa	5	51	14	70	2,13	2
	7,14%	72,86%	20%			
Ymmärrän oman vastuuni/roolini tietosuojaan ja tietoturvaan liittyen	50	7	13	70	1,47	1
	71,43%	10%	18,57%			
Henkilötietoja ja -rekistereitä käyttäessäni ymmärrän oman vastuuni vaitiolo- ja salassapitovelvollisuudesta	61	2	7	70	1,23	1
	87,14%	2,86%	10%			
Yhteensä	**189**	**171**	**340**	**700**	**2,22**	**2**

Kuvio 13. Vastaajien näkemys tietojen käsittelyssä noudatettavista menettelytavoista ja periaatteista yrityksessä (N = 70).

Seuraavaksi kyselyssä kartoitettiin rekisteröidyn (=henkilö, jonka tiedoista kyse) oikeuksien toteutumista (Kuvio 14.). Yrityksessä on toteutettavissa rekisteröidyn omien tietojensa tarkistamisoikeus 33 (47,14 %) vastaajan mukaan, kolme oli eri mieltä ja loput 34 (48,57 %) ei osannut sanoa. Samoin luvuin vastaajat vastasivat väitteeseen:

”Rekisteröidyn omien tietojen oikaiseminen ja poistaminen on toteutettavissa yrityksessämme.” Lisäksi 28 (40 %) vastaajista oli sitä mieltä, että rekisteröidyllä on oikeus rajoittaa omien tietojensa käsittelyä yrityksessä, neljä vastaajista oli eri mieltä ja suurin osa 38 (54,29 %) ei osannut sanoa.

	Samaa mieltä	Eri mieltä	En osaa sanoa	Yhteensä	Keskiarvo	Mediaani
Rekisteröidyn omien tietojen tarkastamisoikeus on toteutettavissa yrityksessämme	33	3	34	70	2,01	2
	47,14%	4,29%	48,57%			
Rekisteröidyn omien tietojen oikaiseminen ja poistaminen on toteutettavissa yrityksessämme	33	3	34	70	2,01	2
	47,14%	4,29%	48,57%			
Rekisteröidyllä on oikeus rajoittaa omien tietojen käsittelyä yrityksessämme	28	4	38	70	2,14	3
	40%	5,71%	54,29%			
Rekisteröidyllä on oikeus siirtää tiedot järjestelmästä toiseen yrityksessämme	10	8	52	70	2,6	3
	14,28%	11,43%	74,29%			
Yhteensä	**104**	**18**	**158**	**280**	**2,19**	**3**

Kuvio 14. Kuviossa vastaajien vastukset miten rekisteröidyn (= henkilö, jonka tiedoista kyse) oikeudet toteutuvat käytännössä (N = 70).

Dokumenttien käsittely, säilytys ja arkistointi väittämät ja niiden vastukset ovat tarkemmin kuvattuna kuviossa 15. Selkeästi vastauksista erottui väittämä, että käytössä on paperisia asiakirjoja, joissa on henkilötietoja. Samaa mieltä oli 50 vastaajaa, 19 heistä oli eri mieltä ja vain yksi ei osannut sanoa. Vastaajista 34 tietää, miten tietosuoja huomioiden asiakirjat säilytetään, arkistoidaan ja hävitetään yrityksessä. Neljätoista vastaajista oli eri mieltä ja 22 ei osannut sanoa. Henkilötietoja sisältävät asiakirjat tulee säilyttää aina lukitussa paikassa 33 vastaajan mielestä, 32 heistä oli eri mieltä asiasta ja viisi ei osannut sanoa.

	Samaa mieltä	Eri mieltä	En osaa sanoa	Yhteensä	Keskiarvo	Mediaani
Käytössäni on paperisia asiakirjoja, joissa on henkilötietoja	50	19	1	70	1,3	1
	71,43%	27,14%	1,43%			
Henkilörekisteriin liittyvien paperisten asiakirjojen käsittelyyn on olemassa kirjallinen ohjeistus	11	18	41	70	2,43	3
	15,72%	25,71%	58,57%			
Tiedän, miten tietosuoja huomioiden asiakirjoja säilytään, arkistoidaan ja hävitetään yrityksessämme	34	14	22	70	1,83	2
	48,57%	20%	31,43%			
Lukitsen työhuoneeni ja suljen näyttöpäätteen lyhyidenkin poissaolojen ajaksi	43	27	0	70	1,39	1
	61,43%	38,57%	0%			
Säilytän henkilötietoja sisältävät asiakirjat aina lukitussa paikassa	33	32	5	70	1,6	2
	47,14%	45,72%	7,14%			
Henkilötietoja sisältävät tilat ja järjestelmät on valvottu/lukittu myös työajan jälkeen	48	7	15	70	1,53	1
	68,57%	10%	21,43%			
Asiakirjojen säilytys- ja arkistointitilat ja -kaapit ovat riittävän turvallisia sekä palo- ja murtosuojattuja	8	25	37	70	2,41	3
	11,43%	35,71%	52,86%			
Yhteensä	**227**	**142**	**121**	**490**	**1,78**	**2**

Kuvio 15. Kuviossa kuvataan dokumenttien käsittelyyn, säilytykseen ja arkistointiin liittyvät vastaukset (N = 70).

Avoimen kysymyksenä kyselyssä kysyttiin, miten vastaaja työssään huomioi, ettei ulkopuoliset henkilöt pääse näkemään käsittelyssä olevia henkilötietoja. Esimerkiksi asiakirjoja, sähköposteja ym. Vastaukseen vastasi kaikki 70 vastaajaa, joista neljä vastaajista jätti kuitenkin vastaamatta kysymykseen ja kaksi vastasi ei mitenkään.

Vastaukset luokiteltiin seuraaviin ryhmiin:

Henkilötietojen käsittely vain digitaalisessa muodossa (3)
Koneen lukitseminen poissa ollessa (29)
Henkilökohtaisten salasanojen käyttö (25)
Salasanojen vaihto 3 kk:n välein (3)
PC:n suojaus sovellus käytössä kaikissa koneissa (2)

Ei säilytä tietoja, mitä ei tarvita (4)
Työhuoneen oven sulkeminen/lukitseminen (24)
Säilytetään vain asiakkaalta saatu tieto (1)
Henkilötietoja sisältävät paperit säilytetään lukollisessa kaapissa (13)
Näyttöruutu niin ettei ulkopuolinen pysty näkemään siihen (4)
Tietokoneen ruudun sulkeminen asiakkaan läsnä ollessa (1)
Yleinen varovaisuus (4)
Paperien kääntäminen, jos joku tulee työtilaan (7)

Kehitysehdotus vastaajalta oli saada näytönsuoja kannettavaan, ettei ulkopuoliset näe näytölle, kun työskentelee julkisissa kulkuneuvoissa ja toinen vastaaja kertoi puolestaan, että julkisilla paikoilla ei käsitele henkilötietoja. Huomiona useammassa vastauksessa tuli esille, että lähes kaikilla on sama avain työhuoneisiin ja useampi henkilö työskentelee samassa huoneessa eli avokonttori tyylisesti. (5)

Kuviossa 16. kuvataan tarkemmin vastaajien vastauksia sähköpostin käytöstä ja tietojen käsittelystä. Suurin osa vastaajista kertoo käyttävänsä sähköpostia henkilötietojen siirtämiseen ja suurimmalla osalla ei osannut sanoa onko sähköpostin tietosuojan riittävyys varmistettu henkilötietojen siirtämisiin. Suurin osa vastaajista koki tarpeelliseksi, että työpaikalla olisi kirjalliset ohjeet henkilötietojen käsittelystä sähköpostitse.

	Samaa mieltä	Eri mieltä	En osaa sanoa	Yhteensä	Keskiarvo	Mediaani
Käytän työssäni sähköpostia henkilötietojen siirtämiseen	52	16	2	70	1,29	1
	74,28%	22,86%	2,86%			
Pystyn jälkikäteen osoittamaan kenelle olen sähköpostilla henkilötietoja lähettänyt	63	2	5	70	1,17	1
	90%	2,86%	7,14%			
Käytän työssäni sähköpostia henkilötietojen tallentamiseen	24	42	4	70	1,71	2
	34,29%	60%	5,71%			
Sähköpostin tietosuoja riittävyys on varmistettu henkilötietojen siirtämiseen	10	5	55	70	2,64	3
	14,29%	7,14%	78,57%			
Koen tarpeelliseksi, että työpaikallani olisi henkilötietojen käsittelystä sähköpostitse kirjalliset ohjeet	58	4	8	70	1,29	1
	82,86%	5,71%	11,43%			
Yhteensä	**207**	**69**	**74**	**350**	**1,62**	**1**

Kuvio 16. Kuviossa kuvataan sähköpostin käyttöä ja tietojen käsittelyä vastaajien näkökulmasta (N = 70).

7.1.4 Tietosuojan valvonta ja seuranta

Tässä osiossa käsitellään tietoturvallisuuteen liittyviä asioita, joita kartoitettiin Yritys Oy:n toiveesta samassa kyselyssä, vaikka tietoturva asioita oli tästä opinnäytetyöstä rajattu pois. Tietosuojan valvonta ja seuranta (Kuvio 17.) painottuu paljon järjestelmiin, joissa henkilötietojen käsittelyä, siirtoa, tallennusta sekä valvonta tapahtuu. Tietosuoja asetus edellyttää yrityksiä noudattamaan siinä säädettyjä toimenpiteitä, jonka vuoksi toimeksiantaja saa tästä kyselyn osiosta paljon tärkeää dataa tietoturvan osalta nykytilanteesta sekä toimintansa kehittämisen lainsäädäntö huomioiden.

Nostan tähän opinnäytetyöhön muutaman kohdan tietosuojan valvonnasta ja seurannasta. Vastaajista suurin osa 51 (72,86 %) ei osaa sanoa ja 11 (15,71 %) vastaajaa on eri mieltä, valvotaanko työpaikalla säännöllisesti henkilötietojen käyttöä ja käsittelyn lainmukaisuutta. Vastaajista 31 (44,29 %) oli samaa mieltä, että käyttämissään henkilötietorekistereissä käyttöoikeudet on rajattu vain työtehtävissä tarvittaviin tietoihin. Kahdeksan (11,43 %) vastaajaa oli asiasta eri mieltä ja 31 (44,29 %) vastaajista ei

osannut sanoa miten asia on. Vain 13 (18,57 %) vastaajan mielestä työpaikalla on määritelty henkilötietojen käsittelyyn liittyvät tehtävät, vastuualueet ja vastuuhenkilöt. Yhdeksäntoista (27,14 %) vastaajista oli erimieltä ja 38 (54,29 %) ei osannut vastata väittämään. Kyselyn mukaan 48 (68,57 %) vastaajista ei tiennyt onko työpaikalla nimetty tietosuojavastaava.

	Samaa mieltä	Eri mieltä	En osaa sanoa	Yhteensä	Keskiarvo	Mediaani
Työpaikallani henkilötietoja sisältävät tiedostot ovat riittävästi suojattu	14	12	44	70	2,43	3
	20%	17,14%	62,86%			
Henkilötietoja pääsee käsittelemään vain henkilöt, joilla on oikeus tietoon	28	8	34	70	2,09	2
	40%	11,43%	48,57%			
Työpaikallani henkilötietojen käyttöä ja käsittelyn lainmukaisuutta valvotaan säännöllisesti	8	11	51	70	2,61	3
	11,43%	15,71%	72,86%			
Käyttämistäni henkilörekisteri tiedoista tehdään varmuuskopiointi	9	10	51	70	2,6	3
	12,86%	14,28%	72,86%			
Tiedän missä varmuuskopioitu tieto säilytetään ja kenen toimesta	7	22	41	70	2,49	3
	10%	31,43%	58,57%			
Pääsy käyttämiini tietojärjestelmiin edellyttää henkilökohtaista käyttäjätunnusta ja salasanaa	59	6	5	70	1,23	1
	84,29%	8,57%	7,14%			
Salasanan vaihtoa vaaditaan säännöllisesti	42	20	8	70	1,51	1
	60%	28,57%	11,43%			
Jälkikäteen on mahdollista todeta, kuka on katsonut, lisännyt tai poistanut tietoa järjestelmistä	17	14	39	70	2,31	3
	24,29%	20%	55,71%			
Käyttämissäni henkilötietorekistereissä käyttöoikeudet on rajattu vain työtehtävissä tarvittaviin tietoihin	31	8	31	70	2	2
	44,28%	11,43%	44,29%			
Työpaikallani on määritelty henkilötietojen käsittelyyn liittyvät tehtävät, vastuualueet ja vastuuhenkilöt	13	19	38	70	2,36	3
	18,57%	27,14%	54,29%			
Työpaikallani on nimetty tietosuojavastaava	5	17	48	70	2,61	3
	7,14%	24,29%	68,57%			
Työnantaja on ohjeistanut henkilöstön työsuhteen päättyessä palauttamaan kaikki käytössä olleet laitteet välittömästi työnantajalle	51	2	17	70	1,51	1
	72,86%	2,86%	24,28%			
Yhteensä	**284**	**149**	**407**	**840**	**2,15**	**2**

Kuvio 17. Yrityksen tietosuojan seurantaa ja valvontaa koskevat vastaukset ovat tarkemmin kuvattuna oheisessa kuviossa (N = 70).

7.1.5 Tietosuoja asioiden koulutus henkilöstölle

Tietosuoja asioiden koulutuksesta kysyttiin vastaajilta avoimella kysymyksellä seuraavasti: ” Tietosuoja asioista on suunnitteilla henkilöstölle koulutusta. Millaisilla menetelmillä mieluiten opiskelisit asioita? Esimerkiksi lukemalla tietoa Intrasta, tulostettava tietopaketti vai koulutustilaisuus.” Kaikki 70 vastaajaa vastasi kysymykseen.

Eniten vastauksia tuli koulutustilaisuuden ja tulostettavan tietopaketin puolesta yhteensä 38 kpl, joista kuusi vastaajista ehdotti pienryhmässä osasto kohtaista koulutusta ja neljä koulutusta henkilöstöpäivien yhteydessä. Keskustelevan koulutustilaisuuden puolesta oli 18 vastaajaa ja tulostettava tietopaketti Intraan riittäisi kahdeksalle vastaajista. Seitsemän vastaajista oli sitä mieltä, että heille riittäisi yleinen tieto asiasta Intraan luettavaksi. Yksi vastaaja oli sitä mieltä, että sähköposti ohjeet ovat riittävät, ja puolestaan toisen vastaajan mielestä olisi hyvä olla kaikille tietosuoja testi asioiden osaamisen varmistamiseksi. Lisäksi kolme vastaajista ei osannut sanoa mitään.

Seuraavaksi esimerkkinä suoria lainauksia vastaajien vastauksista kysymykseen:

> *Ehdottomasti koulutustilaisuus, jossa kerrottaisiin kokonaisvaltaisesti tietosuoja uudistuksesta ja sen jälkeen tarkemmin, mitä se tarkoittaa meidän yrityksessä ja omassa työnkuvassa. Tällä hetkellä omat tiedot pohjautuvat vain kuulopuheisiin, ja siihen mitä uutisissa/netissä on kerrottu asiasta.*
>
> *Hyvä kysymys tämäkin.*
>
> *Koulutustilaisuus, muuten osallistuminen tai riittävä asiaan perehtyminen taitaa jäädä vajaaksi. Yksiköittäin toteutettuna (kun kaikki osallistuu) saadaan työtehtäväkohtaisesti käytyä käytänteet läpi + pystytään kehittämään toimintaa/käytänteitä ja sopimaan miten jatkossa toimivat.*
>
> *Koulutus tilaisuus, jonka jälkeen tietopaketti on tulostettavissa Intrasta.*

Tulostettava tietopaketti, koska kaikki henkilökunnan jäsenet eivät käytä tietotekniikkaa. Koulutustilaisuus, jos käsiteltävä materiaali on kovin laaja esimerkiksi osana esimiespalaveria.

Sekä että – tulostettava tietopaketti + koulutustilaisuus. Live koulutus ehdoton, koska siellä syntyy keskustelua ja saa saman tien vastauksia.

7.2 Yritys Oy:n tietosuojavastaavan haastattelun yhteenveto

Tässä kappaleessa kuvataan Yritys Oy:n tietosuojavastaavan (2018) haastattelun vastaukset, niin kuin hän kysymyksiin (Liite 2.) vastasi. Vastauksia ei ole muokattu opinnäytetyöntekijän toimesta.

Yritys Oy:n tietosuojavastaavan mukaan johdolla ei ole erityisen hyvää kuvaa yrityksen tietosuojan tilasta. Käytännön tietosuojasta huolehtiminen on jätetty pitkälti tietosuojaryhmän vastuulle ja johto on tietosuojavastaavan kanssa keskustellut ainoastaan joistakin yksittäisistä tietosuoja asioista. Mitään ongelmia ei ole toistaiseksi ollut, joten tietosuojavastaava uskoo, että johtokin olettaa asioiden olevan ihan hyvällä mallilla.

Tietosuojavastaava kertoo, että Yritys Oy:ssä käytännön tietosuoja-asioita hoitaa pääasiassa tietosuojavastaava ja tietosuojaryhmän jäsenet. Tietosuojavastaava ja tietosuojaryhmäläiset tekevät tietosuoja-asioita muiden töidensä ohessa, joten tietosuoja-asioihin käytettävä aika on hyvin vähäistä. Ennen EU:n tietosuoja-asetuksen voimaantuloa oli ”tietosuojaprojekti”, jolloin ajankäyttö tietosuoja-asioihin oli huomattavasti suurempaa. Tarvittaessa eli esim. ongelmatilanteissa tietosuojavastaavalla olisi mahdollisuus käyttää työajastaan suurempi osa asian hoitamiseen. Loppukädessä vastuu tietosuojasta kuuluu kuitenkin yrityksen johdolle.

Tietosuojavaltuutetun työtehtäviin Yritys Oy:ssä kuuluu tarpeen mukaan avustaa henkilöstöä tietosuojaan liittyvissä asioissa sekä toimia kontaktihenkilönä asiakkaiden suuntaan, jos heillä on tietosuojaan liittyvää kysyttää/valitettavaa. Tietosuojavastaava

osallistuu myös esim. dokumenttien laadintaan yhdessä tietosuojaryhmän kanssa. Tarkemmin tietosuojavastaavan roolia ei ole yrityksessä kuitenkaan määritelty.

Haastateltavan mukaan tietosuoja-asetuksen mukainen rekisterinpitäjän osoitusvelvollisuus on pyritty huomioimaan laatimalla erilaisia dokumentteja. Tärkein laadittu dokumentti on Yritys Oy:n tietosuojapolitiikka, joka on organisaation sisäinen dokumentti tietosuojakäytännöistä. Ainoa kaikille Yritys Oy:n asiakkaille suunnattu dokumentti on tietosuojaseloste, joka löytyy yrityksen verkkosivuilta. Lisäksi omistaja-asiakkaille on toimitettu dokumentti henkilötietojen käsittelystä omistajapalvelusta. Henkilöstön Intranettiin on kasattu paljon eri henkilörekistereiden rekisteriselosteita ja lisäksi tietosuojaryhmällä on joitakin dokumentteja, joita ei ole julkaistu missään. Dokumentteja päivitetään aina tarpeen vaatiessa. Esimerkiksi tällä hetkellä yrityksessä ollaan ottamassa käyttöön uutta mobiilisovellusta, joten tietosuojaselosteeseen ollaan tekemässä päivitystä tähän liittyen.

Erillisiä ohjeita henkilöstölle tietosuojavastaavan mukaan on laadittu seuraavista aiheista:

i. Toiminta tietoturvaloukkauksissa
ii. Puhtaan pöydän periaate, eli ohje paperidokumenttien käsittelystä
iii. Ohje sähköpostin turvallisesta käytöstä
iv. Ohje tietojenkäsittelystä teknisillä laitteilla. Sisältää ohjeistusta esim. tietokoneen lukitsemisesta ja tietojen käsittelystä matkustaessa.

Hän kertoo myös, että ohjeistus on kaiken yrityksen henkilöstön saatavilla Intranet-sivustolla. Valitettavasti Intranetin seuraaminen on henkilöstöllä vielä varsin vähäistä, mutta sen roolia virallisena tiedotuskanavana on pyritty yrityksessä kasvattamaan.

Tietosuojavastaavan mukaan kunnollista tietosuoja asioiden jalkautusta henkilöstölle ei ole tehty, vaan tietosuoja-asioihin tutustuminen on jäänyt pitkälti työntekijöiden omalle vastuulle. Intranet on yrityksen henkilöstön virallinen paikka tiedotukselle ja ohjeistuksien jakamiselle, mutta toistaiseksi sen käyttö tai edes tietoisuus sen sisällöstä on liian vähäistä. Sama ongelma koskee toki tietosuojan lisäksi montaa muutakin asiaa.

Haastateltava kertoo, että yrityksessä paperidokumenttien säilytyksestä ja arkistoinnista on laadittu ohje, mutta tietosuojavastaavan arvion mukaan paperisia dokumentteja käsitellään ja arkistoidaan edelleen liikaa. Uuden toiminnanohjausjärjestelmän myötä paperisten dokumenttien käsittely on vähentynyt, mutta on edelleen liiallista. Tällöin on riski, että yritykselle muodostuu rekistereitä, joista kukaan ei ole kunnolla tietoinen. Lisäksi arkistointi tapahtuu lukituissa varastoissa, joihin pääsy on vain asianmukaisilla henkilöillä. Yrityksestä löytyy tuhottaville dokumenteille omat lukitut roskalaatikot, joihin henkilötietoja sisältävät dokumentit pitäisi hävitettäessä laittaa.

Tietosuojavastaava toteaa, että turvallisesta henkilötietojen käsittelystä sähköposteissa on laadittu erillinen ohje, mutta ohjeen noudattaminen on jäänyt pitkälti henkilöstön omalle vastuulle. Tietoturvaloukkausten varalle on laadittu ohje/prosessi. Suurimpana ongelmana tässä on, että kaikki työntekijät eivät välttämättä tunnista tietoturvaloukkausta, jolloin ne saattavat jäädä raportoimatta. Tunnistettuja tietoturvaloukkauksia ei ole kuitenkaan ollut.

Yrityksessä on tietosuojaryhmä, joka koostuu tietosuojavastaavan lisäksi viidestä henkilöstä. Tietosuojaryhmällä ei ole tällä hetkellä säännöllisiä kokoontumisia vaan niitä järjestetään aina tarpeen mukaan. Tietosuojavastaavan mukaan keskimäärin näitä on järjestetty noin kerran kuukaudessa. Tietosuojaryhmän tehtävänä on toimia tietosuojavastaavan tukena ja toimia omissa osastoissaan asiantuntijana/tukena tietosuoja asioissa.

Tietojohtaminen Yritys Oy:ssä on vastaajan mukaan vielä aika lapsen kengissä. Kaikki osastot ja johto hyödyntävät jollakin tavalla esim. business intelligence -raportointia, mutta kaikkea hyötyä ei tästä vielä saada irti. Yrityksellä on reilu 1,5 vuotta ollut käytössä uusi toiminnanohjausjärjestelmä, jossa on paljon dataa. Ongelmana on ollut toistaiseksi, että tieto ei ole ollut tarpeeksi luotettavaa, jonka vuoksi sitä ei ole päästy hyödyntämään tavoitteiden mukaisesti. Tietosuojavastaava kertoo, että yksi oleellisimmista tiedosta, joita johto haluaa hyödyntää, on yrityksen asiakastiedot. Asiakasdataa ei ole kuitenkaan vielä pystytty kunnolla hyödyntämään sen puutteellisuuden vuoksi. Tietosuojavaltuutettu korostaa, että viime aikoina asiakastietojen korjaamiseksi on tehty johdon halusta/tarpeesta kuitenkin paljon töitä. Asiakastiedot liittyvät tietysti suoraan tietosuojaan ja se on täytynyt ottaa tässä työssä huomioon.

Haastateltava kertoo, että yrityksessä ei vielä ole tehty mitään varsinaista riskien arviointia. Riskien arviointia varten on luotu lomake ja riskienhallinnan periaatteita on käsitelty osana tietosuojapolitiikkaa. Lisäksi riskinhallinnasta on oma dokumentti, jota ei ole vielä julkaistu missään. Tietosuojakäytäntöjen noudattamista valvoo pääasiassa yrityksen esimiehet, mutta mitään varsinaista käytäntöä tietosuoja asioiden valvomiseen ei ole luotu. Myös tietosuojavastaava ja tietosuojaryhmäläiset antavat tarvittaessa palautetta, jos havaitsevat, että sovittuja käytäntöjä ei noudateta. Hän kertoo, että koko henkilöstöä koskevia tietosuoja asioita tiedotetaan Intranetin välityksellä. Osastot saattavat tiedottaa asioista sisäisesti esim. sähköpostin välityksellä ja palavereissa. Esimiesten vastuulla on seurata, että työntekijät käsittelevät henkilötietoja asianmukaisesti. Mitään varsinaisia mittauksia tai selvityksiä ei yrityksessä ole kuitenkaan tehty.

Haastattelussa tietosuojavastaava kertoo, että henkilöstölle ei ole ainakaan toistaiseksi järjestetty koulutusta tietosuojaasioissa. Mikäli koulutusta järjestettäisiin, niin sen pitäisi tehdä osastoittain, koska eri osastot käsittelevät henkilötietoja hyvin eri tavalla. Koulutuksen tarpeellisuus vaihtelee myös suuresti osastoittain ja kaikille se ei välttämättä ole edes tarpeellista.

Tietosuojavastaavan mukaan, yrityksen tietosuojaan liittyvä dokumentaatio on kohtuullisen hyvällä mallilla, mutta esimerkiksi henkilöstön tietoisuudessa tietosuoja asioista on vielä paljon kehitettävää. Ja hän pohtii, että tietosuoja asioihin ei ole kevään 2018 jälkeen ollut tarpeeksi suurta panostusta, ja ne ovat yrityksessä jääneet muiden asioiden ”jalkoihin”. Positiivista tietosuojavastaavan mielestä on, että mitään tietosuojaan liittyviä suurempia ongelmia ei ole vielä ollut, mutta mahdollisiin tuleviin ongelmiin tulisi valmistautua vielä paremmin. Erilasia ongelmia varten olisi oltava valmiiksi luodut toimintamallit. Tietotilinpäätöstä ei yrityksessä ole ainakaan vielä toistaiseksi tehty, eikä sitä ole varsinaisesti suunniteltukaan.

Kolme tärkeintä asiaa, jotka tietosuojavastaavan mielestä tulisi seuraavaksi tietosuojan näkökulmasta toteuttaa on henkilöstön osaaminen/tietoisuus tietosuoja asioissa. Sopimustilanne henkilötietojen käsittelyyn osallistuvien kumppanien kanssa, kaikista kumppaneista ei edelleenkään ole kukaan oikein kartalla ja joitakin sopimuksia puuttuu edelleen sekä tietosuojavastaavan ja tietosuojaryhmän osaamisen kehittäminen,

Tietosuojavastaavan tulisi myös olla asiantuntija tietosuoja asioissa, joten osaamista tietosuojaasioissa tulisi kehittää ja päivittää jatkuvasti. (Yritys Oy:n tietosuojavastaava 2018)

7.3 Tulosten yhteenveto ja johtopäätökset

Yritys Oy:n tietosuoja kartoituksen perusteella asioita organisaatiossa on lähdetty työstämään keväällä 2018 tietosuojaryhmän vetämänä. Tietosuojavaltuutettu yritykseen valittiin toukokuussa 2018. Tämän opinnäytetyön tavoitteena oli selvittää Yritys Oy:n tietosuojan nykytila, miten EU:n tietosuoja-asetus vaikuttaa yrityksen toimintaan ja millä tavalla yrityksen tulee varautua tietosuoja-asetukseen, jotta yrityksen toiminta vastaa tietosuoja-asetuksessa määrättyjä säädöksiä. Tuloksien mukaan yrityksen johdolla ei ole kovin hyvää kuvaa yrityksen tietosuojan tilasta.

Kuten aiemmin teoria osuudessa todettiin, että yksi ensimmäisistä ja tärkeimmistä toimenpiteistä tietosuojatyön onnistumiselle on organisaation johdon osallistuminen ja tuki tietosuojatyölle. Yrityksen johto omistaa tietosuojatoiminnan ja vastaa siitä, että tietosuoja toteutuu organisaatiossa osana jokapäiväistä toimintaa riittävin resurssein tietosuojasääntelyn vaatimalla tavalla. Johdon vastuulla on kehitystoimenpiteiden toteuttaminen sekä seuranta. (Valtiovarainministeriö 2016, 31). Tärkeää olisi yrityksessä resursoida aikaa riittävästi tietosuojaorganisaation vastuuhenkilöille, jotka tekevät nyt tietisuoja työtä oman työnsä ohella. Johdon tulee muistaa, että he viimekädessä vastaavat tietosuoja asioista. Tietosuojavastaavalle ja tietosuojatryhmän jäsenille tulee myös auki kirjoittaa tehtävänkuvat sekä vastuut ja suunnitella säännölliset palaverit vuosikellon mukaisesti.

Taustatietoina kyselyssä pyrittiin kysymään vain yrityksen kannalta oleellisia asioita, jotta saadaan käsitys, onko kyselyyn vastaajia kaikilta organisaation tasoilta, eri toimialoilta sekä eri osastoilla mahdollisimman oikeellisen tiedon saamiseksi.

Kyselyssä kartoitettiin, millaisia henkilötietoja henkilöstö työssään käsittelee sekä tarkemmin eriteltynä mitä henkilötietoja ja millä tavoin. On tärkeä huomioida erilaiset henkilötiedot esim. asiakastiedot, alaikäisten opiskelijoiden tiedot tai oman henkilöstön tiedot. Yrityksen tulee kartoittaa mitkä tiedot ovat yrityksen näkökulmasta oleellisia tietoja, ja kenellä on oikeudet käsitellä henkilötietoja sekä, onko henkilötietojen käsittely yrityksessä rajattua. Lisäksi oleellista on auki kirjoittaa yrityksen toimintamallit, nimetä rekistereitä käyttävät henkilöt ja tarkentaa mitä henkilötietoja heillä on oikeus käsitellä. Tärkeää on jalkauttaa myös tiedot henkilöstölle sekä miten eri henkilötietoja käsitellään ja mitkä ovat rekisterinkäyttäjän vastuut ja velvollisuudet.

Yritys Oy:ssä on käytössä erilaisia järjestelmiä, jonka vuoksi oli tarpeellista kartoittaa mitä järjestelmiä ja millaisia omia tiedostoja henkilötietojen käsittelyyn henkilöstö käyttää. Henkilörekistereiden kartoitusta varten on yrityksessä hyvä laatia dokumentti, jossa on kirjattuna henkilörekisterin nimi, käyttötarkoitus, tietojen tallennustapa ja -paikka, rekisterin vastuuhenkilö, pääkäyttäjä, käyttöoikeudet, miten rekisteri on suojattu, sopimuskumppanit, henkilötietoluokat, käsittelyperuste, säilytysaika, tietovirrat ja maantieteellinen sijainti (Valtiovarainministeriö 2016b, 31-33).

Organisaation hallussa olevat tietovarannot

Tuloksien mukaan 42 vastaajista vastasi, että asianomaisilta pyydetään suostumus hänen henkilötietojensa käyttämiseen, mutta 11 vastaajista oli eri mieltä ja 17 heistä ei osannut sanoa miten yrityksen käytäntö on. Epätietoisuutta tuloksien mukaan oli kirjallinen suostumuksen dokumentoinnista, joka 26 vastaajan mukaan yrityksessä dokumentoidaan, mutta 17 vastaajista oli eri mieltä ja suurin osa 27 vastaajista ei osannut sanoa, mikä on yrityksen käytäntö. Myös suurimmalle osalle vastaajista 38 oli epäselvää, onko yrityksen käytössä olevat henkilörekisterit suojattuja ja henkilötietojen käsittely on turvattu.

Tietojen käsittelyssä noudatettavat menettelytavat ja periaatteet

Yrityksen käytössä olevista henkilörekistereistä on tietosuojavaltuutetun mukaan laadittu rekisteriselosteet ja ne ovat kaikkien saatavilla yrityksen intrassa, mutta ylipuolet (44) vastaajista ei osannut sanoa ja seitsemän heistä oli eri mieltä, että rekisteriselosteet on henkilörekistereistä yrityksessä laadittu. Henkilöstöltä kysyttiin, onko henkilötietojen- ja rekistereiden säilytysajat määritelty yrityksessä. 49 eli 70 % vastaajista ei osannut sanoa ja seitsemän heistä oli eri mieltä, vain 14 vastaajista oli samaa mieltä, että säilytysajat on määritelty.

Rekisteriselosteet ovat jokaisen saatavilla väittämään 39 vastaajista ei osannut sanoa, 16 heistä oli eri mieltä ja 15 vastaajista kertoi olevansa tietoisia asiasta. Tämän jälkeen vastaajat vastasivat kysymykseen, kuinka moni heistä on perehtynyt yrityksen rekisteriselosteisiin intrassa. Vastaajista 26 henkilöä kuitenkin kertoi perehtyneensä rekisteriselosteisiin ja 29 vastaajista puolestaan eivät olleet perehtyneet sekä 15 vastaajaa ei osannut sanoa olivatko perehtyneet yrityksen rekisteriselosteisiin. Tuloksista voidaan todeta, että henkilöstölle ei ole vielä keskeiset käsitteet hallussa, jonka vuoksi vastaukset ovat hieman ristiriidassa toisiinsa. Tärkeää on avata henkilöstölle yrityksessä käytettävät keskeiset käsitteet, joita ohjeissa ja toimintamalleissa käytetään. On oleellista, että henkilöstö ymmärtää mistä puhutaan. Keskeisiä käsitteitä tässä opinnäytetyössä olivat henkilötieto, henkilötietojen käsittely, henkilötietojen käsittelijä, suostumus, rekisteri, rekisterinpitäjä ja rekisteröity. Tämän vuoksi olisikin erittäin tärkeää kouluttaa henkilöstöä ensin tietosuojan keskeisiin käsitteisiin ja sen jälkeen vasta jalkauttaa yrityksen toimintamallit sekä ohjeet käytäntöön.

Tuloksien mukaan henkilötietoja käsittelee moni työntekijä, ja eniten vastaajat kertoivat käsittelevänsä työssään nimiä ja yhteystietoja. Lisäksi 40 vastaajista käsittelee työssään henkilötunnuksia, jotka luetaan arkaluonteiseksi tiedoksi. Myöskin yrityksessä alle 16-vuotiaiden henkilötietoja käsittelee 24 vastaajista, joka erityisesti tulisi huomioida ohjeistuksissa ja järjestelmissä. Tietosuojalain (1050/2018) mukaan rekisterinpitäjän vastuulla on tarkistaa, että alle 13 vuotiaalla on vanhempien suostumus esimerkiksi henkilötietojen antamista edellyttävien palveluiden käyttämiseen tai sosiaaliseen mediaan. Henkilötietoja käsittelevän henkilöstön tulee myös erottaa arkaluonteiset henkilötiedot ja millaisia velvollisuuksia niiden käsittelyyn liittyy.

Tietosuoja-asetuksessa säädetään, että henkilötietoja pitää käsitellä lainmukaisesti, asianmukaisesti, läpinäkyvästi sekä käsittelylle pitää olla tietosuoja-asetuksen mukainen peruste. Henkilötietoja saa kerätä ja käsitellä vain tämän perusteen vaatiman verran, jonka vuoksi Yritys Oy:n on hyvä kiinnittää huomioita näiden asioiden tarkentamiseen ja ohjeistuksen laatimiseen henkilöstölle sekä huomioida lain mukainen toiminta myös työntekijöiden omien tiedostojen ja sähköpostin käyttämisessä henkilötietojen käsittelyssä ja tallentamisessa sekä yrityksen tietojärjestelmissä.

Asiakkaita koskevan henkilötiedon lisäksi Yritys Oy käsittelee työntekijöitään koskevia henkilörekistereitä. Perustelu työntekijöistä kerättyyn henkilötietoon on oltava oleellista työsuhteen kannalta, kuten molempien osapuolten oikeuksien ja velvollisuuksien hoitaminen tai työnantajan tarjoamat etuudet (Tietosuojavaltuutetun www-sivut 2018). Oman henkilöstön työsuhde- ja työsopimuksia käsittelee vastaajista 18 henkilöä sekä palkkatietoja 14 henkilöä. Lisäksi arkaluonteisia tietoja, kuten oman henkilöstön sairauspoissaolotietoja käsittelee 24 henkilöä. Yrityksessä tulisi olla kirjalliset toimintaohjeet sekä kirjattuna henkilöt, jotka tietoja saa käsitellä, jotta asetuksen velvoitteet varmasti tulee huomioitua.

Yritys Oy:llä on useita yhteistyökumppaneita ja yritys voi ostaa erilaisia palveluita alihankintana, kuten aiemmin teoriaosuudessa tuotiin esille esimerkiksi mainostoimiston, tilitoimiston, henkilöstövuokraus yrityksen, sähköpostipalveluiden tai analytiikkapalveluiden tarjoajan kanssa. Tällöin nämä tahot tekevät henkilötietojen käsittelyä yrityksen lukuun, silloin myös kyseinen alihankkija vastaa jatkossa suoraan sanktioiden uhalla asetuksen vaatimusten noudattamisesta (EU:n tietosuoja-asetus 679/2016, 2 luku 8 art.; Oikeusministeriö 2018; Tietosuojavaltuutetun toimiston www-sivut 2018).

Rekisteröidyn oikeuksien toteutuminen

Yhtiön sisällä toimii neljä eri toimialaa, jonka vuoksi eri työssä tarvitaan erilaisia henkilötietoja ja järjestelmiä. Lisäksi kyselyssä selvitettiin mistä henkilöstö hankkii/kysyy

henkilötietoja. Yrityksessä tulee varmistaa, että suostumukset henkilötietojen käsittelyyn on kerätty lainsäädännön mukaisesti.

Merkittävä uusi velvoite on, että tietosuoja-asetus velvoittaa rekisterinpitäjän solmimaan sopimuksen henkilötietojen käsittelystä rekisterinpitäjän ja henkilötietojen käsittelijän välillä. Kuitenkin henkilötietojen käsittelijän omalla vastuulla on aina noudattaa tietojen käsittelyssä tietosuoja-asetuksen vaatimuksia. Tietosuoja-asetuksen myötä myös vaitiolosopimus tulisi olla kaikilla aloilla, koska lähes kaikilla työntekijöillä on pääsy johonkin henkilörekisteriin, kuten Yritys Oy:n tuloksista voimme todeta. (EU:n tietosuoja-asetus 679/2016, 1 luku 28-29 art.)

Dokumenttien käsittely, säilytys ja arkistointi

Tuloksien perusteella dokumenttien käsittely, säilytys ja arkistointi ohjeistukset olivat monelle vastaajista epäselviä ja mistä he tietoa työpaikalla löytävät. Hyvä on miettiä, miten yrityksessä viestitään koko kokonaisuus selkeästi henkilöstölle, asiakkaille, yhteistyökumppaneille sekä sidosryhmille.

Tietosuoja-asetuksen (679/2016) mukaan henkilötietojen käsittely on suunniteltava ja dokumentoitava, koska työnantajille kertyy esimerkiksi henkilötietoja asiakkaista ja omasta henkilöstöstä. Henkilötietojen käsittelyn tuoma vastuu on osa eri tehtävien hoitoon liittyvää toiminnallista vastuuta, joten työtehtävät ja vastuut on määriteltävä yrityksessä asianmukaisesti. Yritys Oy:ssä tulisi myös huolehtia tietosuojan päivitystöistä säännöllisesti, että kaikki tiedot ovat ajan tasalla sekä lain mukaisia mm. ohjeet, toimintamallit, tietosuojaselosteet, salassapitosopimukset, suostumus dokumentit, alihankinta – ja yhteistyökumppanien sopimukset, oppilaiden henkilötietoihin liittyvät lomakkeet ja tietosuojasopimukset jne. Lisäksi tuloksien mukaan useilla työntekijöillä oli käytössään yrityksen järjestelmien lisäksi omia Word- ja Excel tiedostoja sekä sähköpostissa tallennettuna henkilötietoja. Suositeltavaa olisi kartoittaa täyttyykö niiden käyttämisessä asetuksen mukaiset säädökset ja millaisia riskejä niiden käytöstä yritykselle voi koitua ja olisiko mahdollista siirtyä kokonaan turvatun järjestelmän käyttöön.

Lisäksi tietosuoja-asetuksen myötä yrityksen tulee varmistua, että tietojärjestelmät sekä nykyiset henkilötietojen käsittelyn prosessit taipuvat asetuksen muutoksiin mm. rekisteröityjen oikeuksien suhteen (Oikeusministeriö 2017, 23).

Sähköposti ja tietojen käsittely

Tietojen käsittely tulisi toteuttaa niin, ettei ulkopuoliset henkilöt pääse näkemään henkilöstön käsittelyssä olevia henkilötietoja (Tietosuojavaltuutetun www-sivut 2018). Kyselyn vastauksista tuli esille, että sähköpostia ei pysty lähettämään salattuna, mutta sitä käytetään henkilötietojen siirtämiseen. Sähköpostin salasanat vaihdetaan 3 kk:n välein ja jokaisella on henkilökohtaiset tunnukset käytössään. Henkilöstö toivoi ohjeistusta henkilötietojen käsittelystä sähköpostilla, johon tietosuojan näkökulmasta olisi myös hyvä työnantajan ottaa kantaa.

Valvonta ja seuranta

Tietosuojavastaavan haastattelun mukaan yritykselle ei ole laadittu tietotilinpäätöstä, eikä se ole ollut johdon tavoitteena. Tietotilinpäätös antaa kokonaiskuvan yrityksen henkilötietojen käsittelyn ja tietosuojan nykytilasta, ja sen avulla johto voi valvoa ja arvioida nykytilaa sekä ohjata resursseja sen kehittämiseen (Tietosuojavaltuutetun www-sivut 2018; Valtiovarainministeriö 2016b, 31-33).

Tärkeänä näkisin, että yrityksessä olisi nimettynä myös johdosta henkilö, joka vie asiaa aktiivisesti organisaatiossa eteenpäin yhdessä tietosuojaorganisaation kanssa antaen valtuuksia toteuttaa tietosuoja työtä. Yritykseen tulisi laatia tietosuojan hallinnan vuosikello, joka ohjaa säännölliseen toimintaan ja seurantaan. Tietosuojaorganisaation tulisi huolehtia, että ehdotetut muutokset toteutetaan ja tietosuoja-asetusta noudatetaan sekä henkilöstöä koulutetaan säännöllisesti. Lisäksi myös tulevaisuudessa uusien järjestelmien ja mahdollisten lakimuutosten jälkeen.

Yrityksessä tulisi nykytilan kartoituksen ja analysoinnin jälkeen laatia riskiarvio, jossa kartoitetaan, tunnistetaan ja analysoidaan tunnistetut riskit. Analyysin jälkeen

arvioidaan riskin merkitys toiminnalle ja rekisteröidyille henkilöille. Niiden jälkeen yrityksessä tulisi määritellä, miten riskiä käsitellään, kuka vastaa ja mitä toimenpiteitä tehdään määritellyn ajan puitteissa. (Valtiovarainministeriö 2016b, 31-33).

Yrityksen toimenpiteiden laajuus ja laatu ovat riippuvaisia organisaatiossa käsiteltävistä henkilötiedoista ja mitä riskejä niiden käsittelyyn liittyy sekä minkälaiset nykyiset käytännöt yrityksessä on käytössä. Yritys Oy:n tulisi olla tietoinen EU:n tietosuoja-asetuksen vaikutuksista organisaation eri toimintoihin (Oikeusministeriö 2017, 16).

Kyselyn ja haastattelun perusteella ilmeni myös arkisia riskejä, joihin tietosuojan parantamiseksi tulisi kiinnittää yrityksessä huomiota, kuten henkilötietojen lähettäminen ja tallentaminen sähköpostiin, omiin Excel - ja Word tiedostoihin, paperisten dokumenttien käyttö, papereiden jättäminen pöydälle sekä paperien säilyttäminen näkyvillä, julkisilla paikolla työskentely ja huoneen lukitsematta jättäminen. Lisäksi riskejä syntyy esimerkiksi, kun tulostetaan työpaikan yhteiseen tulostimeen, paperisten nimilistojen tai työvuorolistojen näkyvillä oleminen, tiedostojen säilyttäminen suojaamattomina muistitikuilla, suojaamattomat tiedostot tietokoneen työpöydällä, rajaamattomat käyttäjä oikeudet rekistereihin, ryhmätunnuksien käyttö tai etätyöskentely. Oleellista on pohtia, mitä tietoja eri henkilöt tarvitsevat työssään ja millaisia katselu- ja muokkaus oikeuksia järjestelmiin sekä onko rekisteriin kerättävien tietojen tarpeellisuus kartoitettu yrityksessä.

Tuloksien mukaan riskiksi nousee henkilöstön ja esimiesten tietämättömyys tietosuoja-asetuksen mukaisesta henkilötietojen käsittelyyn liittyvistä asioista, mistä he löytävät työnantajat ohjeistukset ja ovatko he ymmärtäneet omat vastuunsa ja velvollisuutensa henkilötietojen käsittelyn suhteen toimiakseen säädösten mukaisesti. Kyselyssä tuli myös esille, että vastaajista suurin osa eivät tienneet kuka on yrityksen tietosuojavastaava ja keneltä he saavat tukea tietosuoja asioissa.

Tietosuojavastaava toi haastattelussa puolestaan esille, että henkilöstö käyttää yrityksen Intraa, johon yrityksen tietosuoja ohjeistukset ja rekisteriselosteet on tallennettu. Tärkeää olisi jalkauttaa tiedot henkilöstölle riittävällä laajuudella ja useammalla eri kerralla esim. koulutuksen kautta ja varmistaa tiedon riittävä taso esimerkiksi tietosuoja testillä, joka pitäisi suorittaa hyväksytysti sovitussa aikataulussa.

Tietosuojavastaavan haastattelussa korostuu, että esimiesten rooli tietosuoja-asetuksen toteutuksen ja seurannan osalta on merkittävä. Esimiesten tulee toimia esimerkkinä tietosuoja-asioissa ja ohjeistaa alaisiaan toimimaan oikein mm. millaisia oikeuksia ja velvollisuuksia työntekijöillä on henkilötietojen käsittelyyn liittyen sekä kuinka näitä seurataan. Yritys Oy:n esimiesten tulisi tuntea tietosuoja-asetuksen mukaiset henkilötietojen käsittelyn yleisperiaatteet, käsittelyn laillisuusperusteet, rekisterinpitäjän velvollisuudet ja rekisteröidyn oikeudet sekä yrityksen toimintamallit ja käytännöt. Esimiehiä tulisi kouluttaa sekä laatia työkaluja käsittelyn seuraamiseksi.

Henkilöstön koulutus

Teoria osiossa tuli esille, että koulutuksen aikana on hyvä käydä avointa keskustelua, joka avaa koulutuksen sisältöä sekä estää mahdollisia väärinymmärryksiä. Koulutus olisi hyvä toteuttaa vuorovaikutteisena ja osallistujia osallistavana kokonaisuutena. Lisäksi koulutuksessa olisi tärkeää käydä asioita läpi käytännön läheisesti, jolloin tieto on helpompi soveltaa myös omaan työhönsä. (Frisk 2005, 16, 29-31; Elinkeinoelämän keskusliitto 2018)

Kyselyn ja haastattelun yhteenvetona voidaan todeta, että henkilöstö ja tietosuojaryhmä tarvitsee vielä tietosuoja- ja tietoturva asioista koulutusta sekä selkeitä toimintamalleja sekä ohjeita käytännöntyö huomioiden. Vastausten mukaan eniten he toivoivat koulutustilaisuutta, jossa avointa keskustelua sekä infopakettia Intraan. Osa vastaajista sekä tietosuojavastaava vielä toivoivat, että koulutustilaisuudet toteutettaisiin osastoittain erilaiset työtehtävät huomioiden.

7.4 Kehittämissuunnitelma

Tietosuojasuunnitelma voidaan laatia, kun ensin on arvioitu organisaation nykyiset henkilötietojen käsittely- ja tietosuojakäytänteet sekä tunnistettu organisaation

tietosuojan tavoitetila huomioiden EU:n tietosuoja-asetuksen vaatimukset (Valtiovarainministeriön 2016, 31).

Tietosuojatyön organisointiin liittyy olennaisesti yrityksen johdon vastuu ja velvoitteet. Nykytilan kartoituksen jälkeen yrityksen johdon tulisi yhteistyössä tietosuojaorganisaation kanssa järjestää rekisterihallinto, laatia kirjallinen tietosuojapolitiikka, periaatteet ja ohjeet sekä mahdollistaa riittävät resurssit tietosuojavastaavan ja tietosuojaryhmän tehtävien tekemiseen. Myös heidän työtehtävät ja asemat tulisi määritellä sekä perehdytystä ja koulutusta tietosuoja asioihin.

Yritys Oy:n olisi hyvä laatia seuraavat dokumentit tietosuojaselosteiden lisäksi; seloste käsittelytoimista, henkilötietojen käsittely ohjeet, prosessikaaviot rekisteröityjen oikeuksista, sisäinen ja ulkoinen viestintä liittyen tietotilinpäätökseen, kuvaus tietosuojatyön suunnittelusta ja seurannasta, tietosuojavastaavan päiväkirja sekä vuosikello. Edellä mainittujen lisäksi Yritys Oy:n henkilörekistereiden kartoitusta varten yrityksen on hyvä laatia dokumentti, jossa on kirjattuna henkilörekisterin nimi, käyttötarkoitus, tietojen tallennustapa ja -paikka, rekisterin vastuuhenkilö, pääkäyttäjä, käyttöoikeudet, miten rekisteri on suojattu, sopimuskumppanit, henkilötietoluokat, käsittelyperuste, säilytysaika, tietovirrat ja maantieteellinen sijainti. (Valtiovarainministeriö 2016b, 31-33).

Nykytilan kartoituksen ja analysoinnin jälkeen yritykselle tulisi laatia riskiarvio esimerkiksi, kuten aiemmin luvussa 4. kohdassa 4.4. on esitetty. Riskinarvio sisältää riskien tunnistamisen ja luokittelun, riskianalyysit, jonka jälkeen arvioidaan riskin merkitys toiminnalle ja rekisteröidyille henkilöille sekä laaditaan toimintaohjeet riskien toteutuessa. Johdon vastuulla on myös laatia tietosuojarikkomusten varalle seuraamuskäytännöt sekä tietosuojattavan jätteen hävitysprosessin järjestäminen. Tärkeää on laatia yritykselle omavalvontasuunnitelma sekä tietotilinpäätös. Henkilöstön kouluttaminen sekä tiedon jalkauttamisen mahdollistaminen ovat osa tietosuojan hallintaa.

Yhteenvetona tuloksien mukaan kehitettävää yrityksellä on henkilötietojen käsittelyn toimintamallien ja ohjeiden laadinnassa, tiedon jalkauttamisessa ja henkilöstön kouluttamisessa sekä tietosuoja organisaation ja esimiesten tukemisessa toiminnan jatkuvuuden turvaamiseksi. Lisäksi kehittämishaasteeksi nousee yrityksen tietosuojan

dokumentaatio, suunnitelmallinen ja säännöllinen seuranta sekä valvonta, joita vaaditaan osoittamaan, että tietosuoja-asetusta on noudatettu.

8 POHDINTA

Yrityksen nykytilanne on nyt kyselyn ja tietosuojavastaavan haastattelun avulla kartoitettu, tietosuojavastaava ja tietosuojaryhmä on valittu yritykseen sen toimesta ja he ovat tehneet työtä asioiden eteenpäin viemiseksi rekisteriselosteita ja ohjeistusta laatien. Kyselyn ja haastattelun avulla saatiin melko todenmukainen kuva Yritys Oy:n tietosuojan nykytilasta, henkilöstön tietosuojaosaamisen tasosta sekä mahdollisista puutteista ja kehittämistarpeista.

Mielestäni Webropol- kysely oli toimiva aineistonkeruumenetelmä ja onnistuin laatimaan hyvin informatiivisen kyselylomakkeen tietosuoja-asetuksen vaateet sekä yrityksen tarpeet huomioiden, jonka tietoja vielä päivitettiin tietosuojavastaavan haastattelulla. Aihe on laaja, jonka vuoksi pyrin rajaamaan siitä tietoturvaan liittyvät asiat pois, vaikka ne ovatkin tärkeä osa tietosuojan hallintaa. Toisaalta kuitenkin kyselylomakkeessa kartoitettiin myös tietoturva asioita toimeksiantajan pyynnöstä, jotta he pystyvät hyödyntämään kyselyn vastauksia itsenäisesti niiltä osin. Opinnäytetyön haasteina on tutkijan luotettavuus ja objektiivisuus, joihin olen pyrkinyt vastaamaan kuvaamalla opinnäytetyön toteuttamisen mahdollisimman läpinäkyvästi ja perustamalla tehdyt tulkinnat vain kerättyyn aineistoon.

Mielestäni tärkeää tietosuojan hallinnan toteuttamisessa yritykselle on suunnitelmallinen ja ennakoiva ote. Tietosuoja-asetus sekä tietosuojalain säädäntö huomioiden luoda yritykselle prosessit ja toimintamallit osana tietosuojan hallintamallia. Hyvä on pohtia asioita myös yrityksen rekistereiden, henkilöstön käytännön työn, ja henkilötietojen käsittelyn tarpeellisuus ja osoitusvelvollisuus huomioiden. Esimerkiksi, miten yrityksessä reagoidaan asiakkailta ym. tuleviin pyyntöihin saada nähdä heistä kerätyt tiedot. On hyvä huolehtia, että henkilöstö on koulutettu ja kaikki sujuu saumattomasti sovittujen toimintamallien mukaan.

Opinnäytetyön tuloksia ei voida yleistää, koska ne koskevat vain toimeksiantaja yritystä. Mutta opinnäytetyön teoriaosuutta sekä työn tuloksia voidaan soveltaa muidenkin yritysten henkilötietojen käsittelyä ja nykytilaa kartoittaessa sekä aloittaessa tietosuojan hallinnan prosessin luomista yritykseen.

Yksi tietosuoja-asetuksen oleellisimmista muutoksista on osoitusvelvollisuus, joka siirtää todistusvastuun henkilörekisterin ylläpitäjälle. Kuten opinnäytetyön teoria osuudessa tuli esille osoitusvelvollisuus edellyttää yritykseltä huomattavan määrän dokumentaatiota ja seurantaa. Tämän työelämälähtöisen opinnäytetyön tuloksissa korostui, että selkeät toimintamallit ja dokumentointi osoitusvelvollisuuden toteuttamiseksi tulee olla selkeä henkilöstölle, jotka käsittelevät jossakin muodossa henkilötietoja. Tärkeää olisi myös dokumentoida turhaltakin tuntuvat asiat, jotta jokainen turvaa oman selustansa henkilötietoja käsiteltäessä niin monella eri tavalla ja varmistetaan lainsäädännön mukainen toiminta.

Mielestäni hyvä olisi herätellä yrityksen henkilökunnan tietosuojatietoisuutta sekä aktivoitumista asian suhteen ja samalla myös omaa vastuuta esimerkiksi Intran käyttämiseen. Tärkeää on, että yrityksen johto sitoutuu asiaan toimien esimerkkinä henkilöstölle, jolloin työntekijät ymmärtävät, kuinka tärkeästä asiasta on kyse ja miten siihen yrityksessä tulee suhtautua. Selkeyttää mitkä ovat yrityksen toimintamallit ja käytännöt, ja miten ne vaikuttavat henkilöstön työhön käytännössä. Lisäksi mistä he saavat koulutusta, tarpeen mukaan apua ja löytävät ohjeita.

Havaitut puutteet johtuivat pääasiassa tietämättömyydestä sekä johdon sitoutumattomuudesta tietosuojan hallinnan kehittämiseen, joten toimenpiteissä korostuu oikea resurssointi, johdon tuki, ohjeet ja koulutus. Opinnäytetyöllä saatiin mielestäni hyvin vastauksia asetettuihin tutkimuskysymyksiin, ja selkeitä tuloksia sekä kehittämissuunnitelma toimeksiantajan tietosuoja työn tueksi. Opinnäytetyöprosessin aikana syntyneet kehittämisehdotukset on tarkemmin käsitelty tulosten yhteenveto ja kehittämissuunnitelma osiossa. Opinnäytetyön avulla ei pystytä tietosuoja-asetuksen mukaisen toiminnan toteutumista ratkaista, vaan tietosuojatyö jatkuu toimeksiantajan toimesta yrityksessä. Opinnäytetyö antaa kuitenkin hyvät valmiudet jatkamaan tietosuojatyötä sisältäen konkreettisen kehittämissuunnitelman sekä toimii itsessään yhtenä dokumenttina yritykselle asetuksen osoitusvelvollisuuden osoittamiseksi.

Tämän opinnäytetyön tekeminen on ollut opettavainen ja melko työläs prosessi opinnäytetyöntekijälle. Opinnäytetyöprosessin alustava aikataulu oli toukokuusta 2018 joulukuun 2019 loppuun. Opinnäytetyöntekijän omantyön ohessa toteutettuna opinnäytetyö kuitenkin valmistui vasta kesäkuussa 2019. Oma osaaminen ja tietotaito on monelta osin karttunut opinnäytetyötä tehdessä. Haasteellisena koin sen, että toimeksiantaja yrityksen kanssa yhteystyötä oli lähinnä prosessin alussa ja opinnäytetyön toteuttaminen oli oikeastaan kokonaan opinnäytetyöntekijän vastuulla, vaikka tarve kartoitukselle nousi toimeksiantajalta. Opinnäytetyön tarkoituksena on EU:n tietosuoja-asetuksen mukaisen prosessin käynnistäminen yhteistyössä toimeksiantaja yrityksen kanssa, joka toteutui hyvin prosessin alussa, kun olin osallisena tietosuojaryhmään työharjoitteluni aikana yrityksessä. Vähäinen yhteistyö yrityksen osalta vaikutti siihen, ettei opinnäytetyön tarkoituksen ollut käytännössä mahdollista toteutua tavoitteen mukaisesti ja luonnollisesti myös on vaikuttanut opinnäytetyön aikataulun pitkittymiseen. Toivon kuitenkin, että toimeksiantaja kokee tämän kartoituksen, teoriaosuuden tiedot sekä tulokset hyödyllisiksi, ja pystyisi myös niitä käytännössä hyödyntämään yrityksen tietosuojan hallintamallin toteuttamisessa ja kehittämisessä.

Jatkotutkimusaiheena voisi olla toimeksiantajayrityksessä esimerkiksi tietosuojakyselyn uusinta samalle kohdejoukolle, kun yrityksen tietosuoja asioita on saatu kehitettyä eteenpäin ja yrityksen henkilöstö koulutettua. Tietosuojakyselyä voi käyttää työkaluna yrityksen tietosuojan toteutumisen, kehittymisen sekä henkilöstön osaamisen seurannassa.

LÄHTEET

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2016. Tietosuojakäsikirja johdolle. 3. painos. Tallinna: Tietosanoma Oy.

Digitaalinen Helsinki www-sivut 2019. Viitattu 25.1.19. https://digi.hel.fi/kehmet/menetelmalaari/tietosuojan-vaikutustenarviointi/

Elinkeinoelämän keskusliitto 2018. Tietopaketti yrityksille: EU:n yleinen tietosuoja-asetus ja tietosuojalaki. Viitattu 10.9.2018. https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/

Euroopan komissio www-sivut 2018. EU:n tietosuojasääntöjen uudistus. Viitattu 10.9.2018. https://ec.europa.eu

Euroopan parlamentin ja neuvoston asetus (EU) 2016. EU:n yleinen tietosuoja-asetus. A27.4.2016/679.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680. EU:n tietosuojadirektiivi. D27.4.2016.

Frisk, T. 2005. Koulutuksen arviointi kouluttajan ja henkilöstön kehittäjän työssä. Hyvinkää: Educa-instituutti Oy.

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely. EU-tietosuoja-asetuksen vaatimukset. Vantaa: Kauppakamari.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. Helsinki: Tammi.

Hänninen A. 2018. VAHTI-seminaari 12.3.2018. Riskienhallinta tietosuoja-asetuksessa. Tietosuojavaltuutetuntoimisto. Viitattu 5.1.2019. https://vm.fi/documents/10623/7190948/VAHTI-seminaari_tietosuoja_ja_riskienhallinta_Anna_Hänninen_1203_2018.pdf/bdcb295c-e4d5-4a4e-aada-2f7426868e54/VAHTI-seminaari_tietosuoja_ja_riskienhallinta_Anna_Hänninen_1203_2018.pdf

KAMK www-sivut 2018. Viitattu 11.9.2018. https://www.kamk.fi/fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Luotettavuus

Keinänen, A. & Väätänen, U. 2016. Empiirinen oikeustutkimus - mitä ja milloin? Teoksessa Miettinen, T. (toim.) Oikeustieteellinen opinnäyte - artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edita Publishing Oy, 246-271.

Koppa www-sivut 2018. Viitattu 11.9.2018. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/tapaustutkimus

Kuisma P. 2018. Luento materiaali - Laadullinen tutkimus. Satakunnan ammattikorkeakoulu.

Oikeusministeriö 2018. Uusi tietosuojalaki voimaan vuoden 2019 alusta. Oikeusministeriön julkaisu 12/2018. Viitattu 4.1.2019. https://oikeusministerio.fi/artikkeli/-/asset_publisher/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta

Oikeusministeriö 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön julkaisu 4/2017. Helsinki 2017. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79316/OMSO_04_2017_OM_TSV_EU_tietosuoja.pdf?sequence=1&isAllowed=y

OpiTietosuojaa.fi www-sivut 2018. EU:n tietosuoja-asetus. Viitattu 8.9.2018. https://opitietosuojaa.fi/index.php/fi/oikeus/lait/eu-n-tietosuoja-asetus

Tietoarkisto www-sivut 2018. Aineistonhallinnan käsikirja. Viitattu 10.9.2018. http://www.fsd.uta.fi/aineistonhallinta/fi/tutkittavien-informointi.html

Tietosuojalaki 5.12.2018/1050. www.finlex.fi

Tietosuojavaltuutetun www-sivut 2018. Näin laadit tietosuoja-asetuksen edellyttämän selosteen käsittelytoimista. Viitattu 9.9.2018. http://www.tietosuoja.fi

Tietosuojavaltuutetun www-sivut 2018. Viitattu 9.9.2018. www.tietosuoja.fi

Tuomi, J. & Sarajärvi, A. 2006. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö. Tammi.

Valtiovarainministeriö 2013. Sovelluskehityksen tietoturvaohje. VAHTI 1/2013, Valtiovarainministeriö. Juvenes Print – Suomen Yliopistopaino Oy, 2013. Viitattu 13.11.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=03c32520-f3f8-4621-b0d4-ec4ca8edafb3&groupId=10128&groupId=10229

Valtiovarainministeriö 2016. EU-tietosuojan kokonaisuudistus. VAHTI-raportti–1/2016. Viitattu 13.11.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128

Yritys Oy:n tietosuojavastaavan haastattelu 2018.

LIITE 1

YRITYS OY:N YHTIÖIDEN HENKILÖREKISTEREIDEN TIETOSUOJAN NYKYTILAN KARTOITUS

Kyselyn tarkoituksena on luoda Yritys Oy:n yhtiöille toimivat tietosuojakäytänteet. Tietosuoja- asetuksen (EU 679/2016) mukaan henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen perusteella esimerkiksi nimi, henkilötunnus, osoite, puhelinnumero tai verkkotunnistetieto.

Henkilörekisteri on mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Tietomassa voi olla keskitetty, hajautettu tai jaettu eri perustein. Esimerkiksi jäsenrekisteri ja käyttäjärekisteri ovat henkilörekistereitä.

Rekisterinpitäjänä Yritys Oy:n yhtiöissä on työnantaja, joka yksin tai yhdessä henkilöstön kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Henkilötietojen käsittelijä on Yritys Oy:n yhtiöiden työntekijä tai työnantajan edustaja, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Tämän kyselyn toteuttaa tradenomi, amk opiskelija Kati Tikka Satakunnan ammattikorkeakoulusta osana opinnäytetyötä. Opinnäytetyön toimeksiantajana toimii Yritys Oy. Kyselyyn vastaaminen kestää n. 15 minuuttia ja vastaukset käsitellään luottamuksellisesti. Vastaustanne arvostetaan kovasti, koska niiden avulla saamme tärkeää tietoa tämän hetken tietosuojan tilanteesta yrityksessä ja tietoa jatkokehittämistarpeista tietosuojan parantamiseksi. Kiitos jo etukäteen!

Vastaamalla tähän kyselyyn annan suostumukseni, että vastauksiani voidaan hyödyntää Yritys Oy:n tietosuoja-asetuksen mukaisen toiminnan kartoittamiseen ja kehittämiseen sekä osana opiskelijan opinnäytetyötä. Kyselyn vastaukset käsitellään luottamuksellisesti ja vastaajia ei voida yhteenvedosta tunnistaa.

Vastaa seuraaviin kysymyksiin valitsemalla oikea vaihtoehto ja tarvittaessa täydennä vastaustasi kirjoittamalla siihen varattuun tilaan.

1. Taustatiedot *

- ◯ Työntekijä
- ◯ Esimies
- ◯ Johto

2. Yritys *

Muu, mikä? _____

3. Osasto, jossa työskentelen *

- ☐ Hallinto
- ☐ Liikunta ja hyvinvointi (Lihy)
- ☐ Myynti- ja markkinointi
- ☐ Kiinteistöpalvelut
- ☐ Opetus
- ☐ Ravintolapalvelut
- ☐ Valmennuskeskus
- ☐ Vastaanottopalvelut
- ☐ Klinikka
- ☐ Muualla, missä? _____

Vastaa seuraaviin kysymyksiin valitsemalla oikea vaihtoehto ja tarvittaessa täydennä vastaustasi kirjoittamalla siihen varattuun tilaan.

4. Käsittelen työssäni seuraavia henkilötietoja? Voit valita useamman vaihtoehdon. *

- ☐ Henkilötietoja (mm. yhteistyökumppanit, sidosryhmät)
- ☐ Asiakastietoja
- ☐ Opiskelijatietoja
- ☐ Oman henkilöstöntietoja
- ☐ Muita, mitä? _____

5. Mitä henkilötietoja käsittelet työssäsi? Voit valita useamman vaihtoehdon *

- ☐ Nimi
- ☐ Osoite
- ☐ Puhelinnumero
- ☐ Sähköposti
- ☐ Henkilötunnus
- ☐ Terveystiedot
- ☐ Valokuva
- ☐ Alle 16-vuotiaan tietoja
- ☐ Osakerekisteri tietoja
- ☐ Videokuva
- ☐ Tilinumero
- ☐ Matkakulut
- ☐ Työhakemus
- ☐ Sairauspoissaolotietoja
- ☐ Opintotietoja
- ☐ Sopimustietoja
- ☐ Sosiaalisenmedian tietoja
- ☐ Kehityskeskustelu tietoja
- ☐ Työsuhdetietoja
- ☐ Työsopimus
- ☐ Palkkatiedot
- ☐ Verokortti
- ☐ HOIKS
- ☐ HOKS
- ☐ Muu, mikä? _____

Vastaa seuraaviin kysymyksiin valitsemalla oikea vaihtoehto ja tarvittaessa täydennä vastaustasi kirjoittamalla siihen varattuun tilaan.

6. Mitä järjestelmiä käytät käsitellessäsi henkilötietoja? Voit valita useamman vaihtoehdon. *

- ☐ VERP
- ☐ MaraPlan
- ☐ Liksa
- ☐ CRM
- ☐ Lanka
- ☐ Lasso
- ☐ HHP
- ☐ Centre
- ☐ Digital Bookers
- ☐ Lyyti
- ☐ Primus
- ☐ Mehiläisen järjestelmä mm. TyökykyKompassi
- ☐ Verifone
- ☐ File Maker Pro
- ☐ Oma Excel- taulukko/Word-tiedosto
- ☐ Kameravalvonta
- ☐ Avainkortit
- ☐ Sähköpostilistat
- ☐ KELA
- ☐ Vakuutusyhtiöt
- ☐ Muita, mikä? _____

7. Henkilötiedot säännönmukaisesti hankitaan/kysytään? Voit valita useamman vaihtoehdon. *

- ☐ Asianomaiselta itseltään
- ☐ Vanhemmilta
- ☐ Tietojärjestelmästä
- ☐ Yhteyshenkilöltä
- ☐ Muu, mistä? _____

Valitse seuraavista vastausvaihtoehdoista mielestäsi parhaiten sopiva vaihtoehto.

8. Organisaation hallussa olevat tietovarannot. *

	Samaa mieltä	Eri mieltä	En osaa sanoa
Asianomaiselta pyydetään suostumus hänen henkilötietojensa käyttämiseen	○	○	○
Kirjallinen suostumus dokumentoidaan	○	○	○
Käytössä olevat henkilörekisterit on suojattu ja henkilötietojen käsittely ón turvattu	○	○	○
Käyttämistäni henkilörekistereistä on laadittu rekisteriseloste	○	○	○
Henkilötietojen- ja rekisterien säilytysajat on määritelty	○	○	○
Rekisteriselosteet ovat jokaisen saatavilla	○	○	○
Olen perehtynyt yrityksemme rekisteriselosteisiin Intrassa	○	○	○

9. Mihin/kenelle henkilötietoja työssäsi voidaan luovuttaa tai tallentaa? (esim. järjestelmiin, yhteistyökumppaneille, kollegoille, asiakkaille, omiin tiedostoihin? jne.) Kirjoita vastauksesi omin sanoin alla olevaan tilaan. *

_____
_____
_____
_____
_____
_____
_____

Vastaa seuraaviin kysymyksiin valitsemalla parhaiten sopiva vastausvaihtoehto.

10. Tietojen käsittelyssä noudatettavat menettelytavat ja periaattee *

	Samaa mieltä	Eri mieltä	En osaa sanoa
Käytössäni olevista henkilörekistereistä on laadittu kirjalliset kuvaukset (rekisterien tietovirta)	○	○	○
Olen analysoinut, mitä tietoturva- ja tietosuojariskejä käyttämieni henkilötietojen käsittelyyn liittyy (riskinarviointi)	○	○	○
Henkilötiedon korjaamiseen liittyvästä menettelystä on kirjallinen ohjeistus	○	○	○
Rekisteröidyn kielto-oikeuden toteuttamisesta on kirjallinen ohjeistus	○	○	○
Henkilötietojen turvaloukkaus tilanteiden varalle on kirjallinen ohjeistus (Henkilötietojen luottamuksellisuus on vaarantunut)	○	○	○
Henkilötietojen käsittelystä on laadittu tietosuojaa ja tietoturvaa koskevat ohjeet	○	○	○
Tietosuojaa ja tietoturvallisuutta koskevat ohjeet ovat henkilöstön saatavilla	○	○	○
Olen saanut tietosuojaa ja tietoturvaa koskevista ohjeista koulutusta ja riittävästi tietoa	○	○	○
Ymmärrän oman vastuuni/roolini tietosuojaan ja tietoturvaan liittyen	○	○	○
Henkilötietoja ja -rekistereitä käyttäessäni ymmärrän oman vastuuni vaitiolo- ja salassapitovelvollisuudesta	○	○	○

Vastaa seuraaviin kysymyksiin valitsemalla parhaiten sopiva vastausvaihtoehto ja tarvittaessa täydennä vastaustasi kirjoittamalla siihen varattuun tilaan.

11. Rekisteröidyn (= henkilö jonka tiedoista kyse) oikeuksien toteutuminen *

	Samaa mieltä	Eri mieltä	En osaa sanoa
Rekisteröidyn omien tietojen tarkastamisoikeus on toteutettavissa yrityksessämme	○	○	○
Rekisteröidyn omien tietojen oikaiseminen ja poistaminen on toteutettavissa yrityksessämme	○	○	○
Rekisteröidyllä on oikeus rajoittaa omien tietojen käsittelyä yrityksessämme	○	○	○
Rekisteröidyllä on oikeus siirtää tiedot järjestelmästä toiseen yrityksessämme	○	○	○

12. Dokumenttien käsittely, säilytys ja arkistointi *

	Samaa mieltä	Eri mieltä	En osaa sanoa
Käytössäni on paperisia asiakirjoja, joissa on henkilötietoja	○	○	○
Henkilörekisteriin liittyvien paperisten asiakirjojen käsittelyyn on olemassa kirjallinen ohjeistus	○	○	○
Tiedän, miten tietosuoja huomioiden asiakirjoja säilytään, arkistoidaan ja hävittetään yrityksessämme	○	○	○
Lukitsen työhuoneeni ja suljen näyttöpäätteen lyhyidenkin poissaolojen ajaksi	○	○	○
Säilytän henkilötietoja sisältävät asiakirjat aina lukitussa paikassa	○	○	○
Henkilötietoja sisältävät tilat ja järjestelmät on valvottu/lukittu myös työajan jälkeen	○	○	○
Asiakirjojen säilytys- ja arkistointitilat ja- kaapit ovat riittävän turvallisia sekä palo- ja murtosuojattuja	○	○	○

13. Miten työssäsi huomioit, ettei ulkopuoliset henkilöt pääse näkemään käsittelemiäsi henkilötietoja? esim. asiakirjat, sähköpostit ym. Kirjoita vastauksesi omin sanoin alla olevaan tilaan. *

Vastaa seuraaviin kysymyksiin valitsemalla parhaiten sopiva vastausvaihtoehto.

14. Sähköposti ja tietojen käsittely *

	Samaa mieltä	Eri mieltä	En osaa sanoa
Käytän työssäni sähköpostia henkilötietojen siirtämiseen	○	○	○
Pystyn jälkikäteen osoittamaan kenelle olen sähköpostilla henkilötietoja lähettänyt	○	○	○
Käytän työssäni sähköpostia henkilötietojen tallentamiseen	○	○	○
Sähköpostin tietosuoja riittävyys on varmistettu henkilötietojen siirtämiseen	○	○	○
Koen tarpeelliseksi, että työpaikallani olisi henkilötietojen käsittelystä sähköpostitse kirjalliset ohjeet	○	○	○

15. Yrityksen tietosuojan valvonta ja seuranta *

	Samaa mieltä	Eri mieltä	En osaa sanoa
Työpaikallani henkilötietoja sisältävät tiedostot ovat riittävästi suojattu	○	○	○
Henkilötietoja pääsee käsittelemään vain henkilöt, joilla on oikeus tietoon	○	○	○
Työpaikallani henkilötietojen käyttöä ja käsittelyn lainmukaisuutta valvotaan säännöllisesti	○	○	○
Käyttämistäni henkilörekisteri tiedoista tehdään varmuuskopionti	○	○	○
Tiedän missä varmuuskopioitu tieto säilytetään ja kenen toimesta	○	○	○
Pääsy käyttämiini tietojärjestelmiin edellyttää henkilökohtaista käyttäjätunnusta ja salasanaa	○	○	○
Salasanan vaihtoa vaaditaan säännöllisesti	○	○	○
Jälkikäteen on mahdollista todeta, kuka on katsonut, lisännyt tai poistanut tietoa järjestelmistä	○	○	○
Käyttämissäni henkilötietorekistereissä käyttöoikeudet on rajattu vain työtehtävissä tarvittaviin tietoihin	○	○	○
Työpaikallani on määritelty henkilötietojen käsittelyyn liittyvät tehtävät, vastuualueet ja vastuuhenkilöt	○	○	○
Työpaikallani on nimetty tietosuojavastaava	○	○	○
Työnantaja on ohjeistanut henkilöstön työsuhteen päättyessä palauttamaan kaikki käytössä olleet laitteet välittömästi työnantajalle	○	○	○

16. Tietosuoja asioista on suunnitteilla henkilöstölle koulutusta. Millaisilla menetelmillä mieluiten opiskelisit asioita? Esimerkiksi lukemalla tietoa Intrasta, tulostettava tietopaketti, koulutustilaisuus.
Kirjoita alla olevaan tilaan vastauksesi perusteluineen. *

LIITE 2

Tietosuojavastaavan haastattelu:

1. Mikä on yhtiöiden johdon näkemys organisaation tietosuojasta?
2. Onko yrityksen tietosuojan osalta vastuut ja resurssit selkeät? Kerrothan tarkemmin, miten käytännössä toteutettu.
3. Mitkä tietosuojavaltuutetun työtehtävät ovat yhtiöissä?
4. Miten tietosuoja-asetuksen mukainen rekisterinpitäjän osoitusvelvollisuus on huomioitu yrityksessä?
5. Millaisia dokumentteja tietosuojaan liittyen yritykselle on nyt laadittuna?
6. Kuinka usein dokumentteja päivitetään?
7. Mistä kaikista asioista on laadittu erillinen ohje tietosuojaan liittyen?
8. Onko ohjeistus henkilöstön saatavilla?
9. Miten ohjeet on jalkautettu henkilöstölle?
10. Miten tietosuoja-asetuksen mukainen dokumenttien säilytys ja arkistointi on huomioitu yrityksessänne?
11. Kuinka tietosuoja on huomioitu sähköpostin käytössä?
12. Miten mahdollisten tietoturvaloukkausten varalta on varauduttu?
13. Onko yrityksessänne tietosuojaryhmä ja kuinka usein se kokoontuu?
14. Mitkä ovat tietosuojaryhmän tehtävät yrityksessänne?
15. Miten tietojohtaminen on toteutettu yrityksessä?
16. Onko yrityksessä tehty tietosuojariskien arviointia ja analysointia?
17. Jos on tehty riskin arviointia, mitä se tarkalleen on sisältänyt ja miten se on dokumentoitu?
18. Miten yrityksessänne valvotaan ja seurataan tietosuoja asioita?
19. Miten henkilöstöä tiedotetaan tietosuoja-asioista?
20. Miten mittaatte ja seuraatte henkilöstön tietosuoja-asetuksen mukaista toimintaa?
21. Onko ollut henkilöstölle koulutusta tietosuoja-asioista ja mitä se on tarkalleen sisältänyt?
22. Miten henkilöstön tietosuoja koulutus on käytännössä toteutettu ja montako tuntia ollut kestoltaan?
23. Miten arvioisit missä vaiheessa tietosuojan nykytila on tällä hetkellä yrityksessänne?
24. Mitkä ovat kolme tärkeintä tietosuoja asiaa, joita tulisi seuraavaksi yrityksessänne kehittää?
25. Onko yritykselle laadittu tietotilinpäätös?