Opinnäytetyö (AMK)

Tietojenkäsittely

2018

Aino Lähde

TIETOSUOJA-ASETUKSEEN VALMISTAUTUMINEN OHJELMISTOALAN YRITYKSESSÄ

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2018 | 25 sivua

Aino Lähde

TIETOSUOJA-ASETUKSEEN VALMISTAUTUMINEN OHJELMISTOALAN YRITYKSESSÄ

Opinnäytetyö tehtiin osana toimeksiantajan valmistautumista EU:n tietosuoja-asetukseen. Kaikki henkilötietoa käsittelevät yritykset joutuvat noudattamaan uuden tietosuoja-asetuksen määrittelemiä lakeja kahden vuoden siirtymäajan päättymiseen mennessä 25.5.2018. Opinnäytetyö keskittyy tietosuoja-asetuksen läpikäyntiin ja henkilötiedon käsittelyprosessien kartoitustöiden esittelyyn. Kartoitustyö on laaja ja monivaiheinen prosessi ja sen keskeisimmät vaiheet on tehty ja dokumentoitu osana opinnäytetyötä. Opinnäytetyön tarkoituksena oli kehittää toimeksiantajan henkilötiedon käsittelyprosessit sekä yleiset tietoturvakäytännöt vastaamaan tietosuoja-asetuksen asettamia kriteereitä. Opinnäytetyö sisältää salassapitosopimuksen alaista tietoa, joka on poistettu julkaistusta versiosta.

Opinnäytetyö on toteutettu tutustumalla teoriaosuudessa EU:n tietosuoja-asetuksen keskeisimpiin kohtiin toimeksiantajaa ajatellen. Opinnäytetyön soveltavaan osuuteen sisältyy toimeksiantajan henkilötietoprosessien kartoitus, sekä hallinnollisten ja teknisten tietoturvatoimien esittely. Kartoitustyön apuna on hyödynnetty malliesimerkkeinä toisten organisaatioiden julkaisemia tietotilinpäätöksiä sekä julkaistuja tietosuoja- ja tietoturvaoppaita. Tutkimusmenetelmä on tapaustutkimus ja tutkimuksen tarkoitus kehittävä.

Tavoitteena opinnäytetyölle oli saattaa toimeksiantaja lähemmäs tietosuoja-asetuksen mukaista yritystoimintaa. Opinnäytetyön tuloksena saavutettiin dokumentaatio toimeksiantajan henkilötiedon käsittelystä ja tietoturvatoimenpiteistä sekä poikkeamatilanteessa toimimisesta. Dokumentaatio toimii myös perehdytysmateriaalina. Laadittua dokumentaatiota käytettiin myös materiaalina henkilökunnan koulutukseen koskien tietosuoja-asetusta. Tavoitteena ollut työkokemus ja tietouden lisääminen ajankohtaisesta tietosuojaan liittyvästä aiheesta myös toteutui.

Ennen kaikkea opinnäytetyö auttoi toimeksiantajaa pääsemään lähemmäs kohti tietosuoja-asetuksen vaatimien direktiivien noudattamista. Opinnäytetyön tutkimustulos hyödyntää myös muita yrityksiä toimimalla apuvälineenä samankaltaisten toimenpiteiden toteuttamisessa.

ASIASANAT:

henkilörekisteri, henkilötieto, tietosuoja, tietotilinpäätös, tietoturvallisuus, yleinen tietosuoja-asetus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information technology

2018 | 25 pages

Aino Lähde

PREPARING FOR THE GENERAL DATA PROTECTION REGULATION IN A SOFTWARE COMPANY

The purpose of this thesis was to present a software company's preparation for the EU General Data Protection Regulation (GDPR). Every company handling personal data registers is obligated to follow the laws set by the regulation at the end of the transition time which ends on 25th May 2018. The thesis is focused around GDPR and presents the project of mapping out the personal data registers and their handling procedures. Mapping out the personal registers consists of different stages which are implemented and documented as a part of this thesis. The aim of this thesis was to develop the commissioning company's personal data register's handling processes to meet the requirements set by the new regulation. This thesis includes classified information which is censored from the published version.

The theoretical part of the thesis includes becoming familiar with and writing down the most important points of the GDPR for the commissioning company. In the practical part, the commissioning company's processes of personal data handling are mapped out and the company’s information security policies are presented. The data balance sheets and information security guides of other organizations have worked as a model examples when executing the personal data mapping and updating the commissioning company's security measures. This thesis was a case study and the aim was to improve already existing methods in the commissioning company.

The goal for this thesis was to help the commissioning company act according to the regulation. The result of this thesis was the documented procedures of personal data handling and information security guides including the guide for working in an incident situation. These documents work as an introduction material for the staff. They also worked as a part of a training material when the company's personnel familiarized themselves with GDPR. The thesis’s writer was also able to gain work experience and to increase knowledge concerning a current information security topic.

Most of all, the thesis helped the commissioning company to familiarize with and work in accordance GDPR and its directives. The thesis' results work also as a guide to other companies encountering the similar actions to these of the commissioning company.

KEYWORDS:

Personal data register, personal data, data balance sheet, data protection, information security, general data protection regulation

SISÄLTÖ

SANASTO

EU-maat	Euroopan Unioniin kuuluvien jäsenmaidensa muodostama taloudellinen ja poliittinen liitto, jonka alueella tuotteet, palvelut, henkilöt ja raha liikkuvat vapaasti ilman tulleja ja muita esteitä (Tulli 2018).
ETA-maat	Euroopan talousalue, joka muodostuu EU:n jäsenmaiden lisäksi vapaakauppaliittoon kuuluvista maista lukuun ottamatta Sveitsiä (Tulli 2018).
GDPR	General Data Protection Regulation. EU:n tietosuoja-asetus, joka mittavasti uudistaa henkilötiedon käsittelyä alkaen 25.5.2018 (Järvinen & Rousku 2017a, 19).
Henkilötieto	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (Tietosuojavaltuutetun toimisto 2013).
Henkilörekisteri	Henkilötietoa sisältävä tietojoukko, joka on järjestetty automaattista tietojenkäsittelyä apuna käyttäen tai muulla tavoin toteutettu kortisto, josta henkilötieto voidaan löytää helposti (Tietosuojavaltuutetun toimisto 2013).
Pilvipalvelu	Palvelimien eli tietokoneiden verkosto. Esimerkiksi pilvipalvelun tarjoaman yrityksen ylläpitämällä palvelimella sijaitseva tallennustila, jota voi ostaa omaan käyttöönsä. Pilveen tallennettuun tietoon pääsee käsiksi internetin kautta tietokoneella tai mobiililaitteella. (Kangasniemi & Lintulahti 2017.)
Rekisterinpitäjä	Määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot, voi olla esim. julkinen viranomainen, luonnollinen henkilö tai virasto (Ohjelmistoyrittäjät ry 2016a).
Rekisteröity	Henkilö, jota koskeva tieto on käsittelyn kohteena (Ohjelmistoyrittäjät ry 2016a).
Tietotilinpäätös	Luo kokonaiskuvan yrityksen tietojenkäsittelyn nykytilasta ja tiedonhallinnan tehokkuudesta. Raportoidaan tietojen käsittelyä koskevat keskeiset asiat. (Andreasson ym. 2014a, 117.)

1 JOHDANTO

Opinnäytetyön tavoitteena on auttaa toimeksiantajaa valmistautumaan EU:n tietosuoja-asetukseen. Jokaisen henkilötietoa käsittelevän organisaation tulee noudattaa tietosuoja-asetusta 25.5.2018 mennessä. Siihen liittyviä toimia opinnäytetyössä ovat toimeksiantajayrityksen henkilötiedon käsittelytapojen kartoitus ja tietoturvaan keskittyvien prosessien dokumentointi. Tavoitteena on myös dokumentoida ja esittää toimeksiantajan syyt henkilötiedon keräämiselle sekä täsmentää henkilötiedon käsittelyn prosesseja. Tarkoitus on, että toimeksiantaja pystyy todistamaan rekistereissä esiintyville noudattavansa tietosuoja-asetusta. Opinnäytetyön tekijän tavoitteena on myös saada työkokemusta ajankohtaisesta aiheesta.

Opinnäytetyö on toteutettu toimeksiantona ohjelmistoalan yritykselle. Se esittelee EU:n tietosuoja-asetuksen mukaisia henkilötiedon käsittelyyn liittyviä kartoitustoimenpiteitä. Toimeksiantaja muiden henkilörekisterin ylläpitäjien tavoin on velvollinen toimimaan tietosuoja-asetuksen mukaisesti. Opinnäytetyö on toteutettu tiiviissä yhteistyössä toimeksiantajan kanssa, jotta työstä saadaan eheä kokonaisuus ja sen tuloksista on hyötyä toimeksiantajalle. Työssä esitellyt toimenpiteet ovat erittäin tärkeitä, koska ne auttavat hahmottamaan henkilötietorekisterien ylläpitämistä ja niiden oikeaoppista käsittelyä. Opinnäytetyö sisältää tietosuoja- ja tietoturvatoimenpiteiden kuvauksia, jotka ovat toimeksiantajan pyynnöstä poistettu julkaistusta verisosta.

Digitalisaatio on asettanut yrityksille haasteita käsitellä henkilötietoa turvallisesti. Opinnäytetyö esittelee toimeksiantajan prosessit henkilötiedon turvalliseen käsittelyyn ja dokumentaatio toimii täten koosteena yritykselle itselleen heille toteutetuista toimista sekä esimerkkinä tavoista, joilla yritys yleisesti voi varmistaa ylläpitämiensä henkilörekisterien tietosuoja-asetuksenmukaiset käsittelytavat.

Tietosuoja-asetus edellyttää lukuisia toimenpiteitä henkilötietoja käsittelevältä yritykseltä. Opinnäytetyö sisältää tarkastelun tietosuoja-asetuksen tuomien keskeisimmistä uudistuksista ja kuvauksen toimenpiteistä, jotka ovat osa henkilötiedon kartoitusprosessia ja tietoturvatoimenpiteitä toimeksiantajayrityksessä. Opinnäytetyön osana toteutettiin toimia, jotka visualisoivat esimerkiksi henkilötiedon kartoitustoimenpiteitä. Opinnäytetyön loppuun on koottu johtopäätökset työn tuloksista.

Teoriaosuus esittelee EU:n tietosuoja-asetuksen keskeisimpiä kohtia ja tutkii niitä keinoja, joilla toimeksiantaja pystyy todistamaan noudattavansa tietosuoja-asetusta. Soveltava osuus esittelee toimeksiantajalle toteutetun tietotilinpäätöksen sekä hallinnollisen ja teknisen tietoturvan suunnittelun. Soveltavassa osuudessa esiintyy myös opinnäytetyön aikana tehtyjä kuvioita, jotka liittyvät toteutettuihin dokumentaatioihin. Tällaisia kuvioita ovat esimerkiksi henkilötiedon käsittelyä kuvaava prosessikaavio ja vuosikello.

Tutkintoon sisältyvien kurssien ja työharjoittelun kautta saatujen kokemusten pohjalta opinnäytetyön aihe valikoitui helposti. Opitut taidot ja sen kautta kerätty itsevarmuus rohkaisi valitsemaan aiheen, jota toimeksiantaja ehdotti. Yhdessä toimeksiantajan kanssa suunniteltu aihe motivoi ryhtymään opinnäytetyön parissa työskentelyyn, sillä siitä on hyötyä sekä yritykselle, että opiskelijalle itselleen.

2 EU:N TIETOSUOJA-ASETUS

Henkilötiedot ja niistä koostuvien rekisterien käsittelyn vaatimat toimenpiteet uudistuvat. EU:n uusi tietosuoja-asetus eli GDPR (General Data Protection Regulation) uudistaa ja päivittää henkilötiedon käsittelyä. EU:ssa vuonna 1995 säädetty henkilötietodirektiivi toimii kansalaisten perusoikeuksiin kuuluvan tehokkaan tietosuojan takaajana (Tietosuojavaltuutetun toimisto 2016). Henkilötietodirektiivin korvaa uusi tietosuoja-asetus.

Tietojenkäsittely on edennyt valtavin harppauksin vuodesta 1995, jonka vuoksi sääntöjen ja ohjeistusten uusiminen on ollut välttämätöntä. Jokaisen kansalaisen tietoja löytyy tavalla tai toisella sähköisistä henkilörekistereistä, jonka vuoksi niiden turvallinen ja oikeaoppinen käsittely on ensiarvoisen tärkeää. 25.5.2016 Euroopan unioni aloitti kahden vuoden mittaisen siirtymävaiheen helpottaen uuteen tietosuoja-asetukseen valmistautumista. Jokainen yritys, joka käsittelee henkilötietoa, on velvollinen osoittamaan, että se noudattaa tietosuoja-asetusta viimeistään 25.5.2018 mennessä. Henkilötietoa voidaan hyödyntää rikollisisin tarkoitusperin esimerkiksi erilaisten ostotapahtumien tekoon, joka tekee siitä alttiin tietoturvahyökkäyksille. Tästä syystä yritysten on suhtauduttava erinomaisella tarkkuudella käsittelemäänsä henkilötietoon. (Järvinen & Rousku 2017a, 19.)

Yrityksen siirtyessä noudattamaan uutta tietosuoja-asetusta sen kannattaa ensimmäisenä määritellä syyt henkilötiedon käsittelylle. Henkilötiedon käsittelyprosessin hahmottamisesta on hyvä lähteä liikkeelle. Miksi tietoa kerätään, miten sitä kerätään ja minne se tallentuu? (Andreasson ym. 2014b, 16.) GDPR on kokonaisuus, johon tutustuminen kannattaa aloittaa peruskäsitteistä. Kokonaiskuvan hahmottaminen auttaa pääsemään alkuun ja lisäämään ymmärrystä siitä, miksi uusi asetus on päätetty ottaa käyttöön. Henkilötietojen ollessa yksi yrityksen arkaluontoisimmista tietokokonaisuuksista, vaatii se ehdottomasti turvallista käsittelyä ja asiantuntevaa osaamista.

Arkaluonteisuutensa ja kallisarvoisuutensa takia henkilötiedon käsittelyn turvaamiseksi luodun tietosuoja-asetuksen määrittelemät rangaistukset sääntöjen rikkomisesta ovat myös tuntuvat. Asetuksen mukaisten säädösten rikkomisesta yritys saattaa joutua maksamaan jopa 20 miljoonaa euroa tai 4% maailmanlaajuisesta liikevaihdosta (Saarelainen 2016). Niin henkilötiedon käsittelyyn kuin sitä suojaamaan luotuun tietosuoja-asetukseen tulee suhtautua vakavasti, sillä niiden laiminlyömisestä määrättävät maksuvaatimukset ovat mittavia puhumattakaan maineen kärsimisestä.

2.1 Rekisterinpitäjä ja henkilötiedon käsittelijä

Rekisterinpitäjä voi olla esimerkiksi yritys, joka nimenomaisesti mainitussa roolissaan on määritellyt henkilötiedon käsittelyn tarkoitukset tai keinot. Rekisterinpitäjän toimeksiannosta henkilötiedon käsittelijä voi olla esimerkiksi luonnollinen henkilö, viranomainen tai virasto. (Ohjelmistoyrittäjät ry 2016b.) Ero rekisterinpitäjään ja henkilötiedon käsittelijään voidaan käsittää esimerkiksi siten, että Yritys A:n palveluksessa työskentelevä myyjä ylläpitää ja käsittelee yrityksen asiakastietoja toimenkuvansa puolesta. Tällöin myyjä on henkilötiedon käsittelijä, mutta työskennellessään Yritys A:lle, asiakasrekisterit ovat yrityksen hallussa, jolloin Yritys A on rekisterinpitäjä.

Vastuu henkilötiedon asetuksenmukaisesta käsittelystä kuuluu rekisterinpitäjälle. Se voi tarkoittaa esimerkiksi perehdytyksen ja kouluttamisen järjestämistä henkilötiedon käsittelijöille. Rekisteröidyille tiedottaminen kuuluu myös rekisterinpitäjän vastuulle. (Hyppönen 2017a.) Tietosuoja-asetuksen siirtymäajan aikana monet yrityksistä ovat esimerkiksi informoineet rekistereissään esiintyviä asiakkaitaan asetuksen mukana tuomista muutoksista ja uudistuksista. Jatkossa ilmoitusvelvollisuus esimerkiksi tietojen vuotamisesta rekisterissä esiintyville henkilöille kuuluu myös rekisterinpitäjälle.

2.2 Perustelu henkilötiedon käsittelylle

Tietosuoja-asetuksen myötä perustelu henkilötiedon käsittelylle muuttuu. Kerätään henkilötietoa sitten asiakas-, markkinointi- tai kampanjarekisteriperustein, tulee sen täyttää jokin asetuksen määrittelemistä kuudesta perusteesta. Suostumus, sopimus, laki, rekisteröidyn suojaaminen, julkinen tehtävä tai oikeutettu etu määrittelevät lainmukaiset perusteet henkilötiedon käsittelylle. (Pynnä 2016a.)

Verkkokaupan asiakkaille on helposti osoitettavissa sähköpostiosoitteiden tallentamisen syyt, kun tilausta koskeva informaatio lähetetään sitä kautta asiakkaalle. Kotiosoitteen rekisteröiminen on tarpeellista, mikäli asiakas haluaa tilauksensa lähetettävän tämän kotiin tai kotia lähimpään noutopisteeseen. Tietosuoja-asetuksen vaatima osoitusvelvollisuus yrityksessä on yksinkertaisemmin toteutettavissa, kun jokaisen kerätyn henkilötiedon voidaan osoittaa olevan olennainen liiketoiminnan kannalta. Tällaisissa tapauksissa edellä mainituista perusteista ainakin suostumus toteutuu, mikäli verkkokauppa varmistaa sen asiakkailtaan asiakkaaksi rekisteröinnin tai ostotapahtuman yhteydessä.

Asiakkaita koskevan henkilötiedon lisäksi yritys käsittelee työntekijöitään koskevia henkilörekistereitä. Tällaiset rekisterit yleensä sisältävät työntekijöiden palkkaukseen liittyviä tietoja, yhteystietoja sekä mahdollisesti sairaslomaan oikeuttavia asiakirjoja. Perustelu työntekijöistä kerättyyn henkilötietoon on oltava oleellista työsuhteen kannalta, kuten molempien osapuolten oikeuksien ja velvollisuuksien hoitaminen tai työnantajan tarjoamat etuudet (Tietosuojavaltuutetun toimisto 2017a).

2.3 Osoitusvelvollisuus

Erilaiset ohjeistukset sekä prosessikuvaukset voivat toimia rekisterinpitäjän apuna täyttää tietosuoja-asetuksen määrittelemä osoitusvelvollisuus. Organisaatiolta on löydyttävä dokumentaatio, jonka avulla se pystyy osoittamaan toteuttavansa asetuksenmukaiset vaatimukset. (Tarhonen 2018.) Yrityksen on suhtauduttava käsittelemäänsä henkilötietoon läpinäkyvästi ja tarkan salassapidon ohella pystyttävä osoittamaan henkilötiedon kohteelle mitä tietoa kerätään ja miksi. Henkilölle tiedottamisen on oltava selkeää hänen antaessaan suostumuksensa tietojensa käsittelylle. Tietojensa luovuttavalle henkilölle tulee olla selvää, miksi kyseistä informaatiota tarvitaan sen lisäksi, että yritys takaa tiedon turvallisen käsittelyn. Pelkkä lain noudattaminen passiivisesti ei riitä, vaan yrityksen on pystyttävä todistamaan, että tietosuojasäännökset huomioidaan (Hyppönen 2017b).

Osoitusvelvollisuuden täyttyminen voi myös muilla tavoin hyödyttää organisaation toimintaa, sillä sen toteutumista varten laaditut dokumentaatiot arkistoivat tehtyjä toimenpiteitä. Mikäli jotkin käsittelytavat kaipaavat päivittämistä, on sellaisen toimenpiteen tarpeellisuuden huomaaminen helpompaa esimerkiksi prosessikuvausten avulla. Asetuksen määrittelemät toimenpiteet ja niiden toteuttamiseen koulutettu henkilökunta jouhevasti toimiessaan selkeyttää organisaation liiketoimintaprosesseja ja auttaa hahmottelemaan kokonaiskuvaa varsinkin henkilötiedonkäsittelyprosesseista.

2.4 Rekisteröidyn oikeudet

Yrityksen on tärkeää ilmoittaa asiakkaalle henkilötiedon keräämisen syyt. Asiakkaan luottamus yritystä kohtaan kasvaa, kun asiakkaalta pyydetään suostumusta tietojensa luovuttamiseen sekä täsmennetään, miksi tietoja tarvitaan. Suostumus takaa myös oikeuden tulla unohdetuksi ja oikeuden tietojen siirtoon, jotka sisältyvät tietosuoja-asetuksen määrittelemiin uudistuksiin. Jokaisessa tapauksessa yritys ei kuitenkaan vaadi

tietojensa luovuttavalta taholta suostumusta, mikäli jokin muu tietosuoja-asetuksen määrittelemistä perusteluista tiedon käsittelylle täyttyy. (Pynnä 2018.) GDPR tarkentaa yksilön oikeuksia olla tietoinen luovuttamansa henkilötiedon tarkoitusperistä.

Jotta rekisteröidyn oikeudet otettaisiin huomioon, tulee yrityksen harjoittaa mahdollisimman läpinäkyvää toimintaa henkilötietojen käsittelyprosesseissaan. Yrityksen kannattaa panostaa selkeyteen, jotta rekisterissä esiintyville henkilöille voidaan vaivattomasti osoittaa tiedon käsittelyn syyt sekä mahdollistaa toimenpiteet tietojen poistamiseen tai siirtoon henkilön pyynnöstä. Henkilötiedon käsittelyprosessit on syytä suunnitella huolella esimerkiksi tietotilinpäätöksen tekoa apuna käyttäen, jotta toimintaperiaatteet tiedon käsittelyn takana selkeytyvät ja tulevat kirjattua ylös koko henkilökunnan saataville sekä esimerkiksi rajattuna versiona julkiseksi dokumentaatioksi yrityksen toiminnasta (Andreasson ym. 2014c, 117–119).

Suostumus henkilötiedon käsittelyyn on syytä pyytää rekisterissä esiintyvältä tiedon luovuttamisen vaiheessa. Henkilöä voidaan pyytää esimerkiksi lukemaan yrityksen tietosuojaseloste rekisteröintivaiheessa, jolla varmistetaan henkilön suostumus tietojensa luovuttamiseen ja niiden käsittelyyn. Tietosuojaseloste saattaa esimerkiksi sisältää tietoa rekisterinpitäjästä, perustelut henkilötiedon käsittelylle, rekisteröidyn oikeudet yrityksen asiakkaana tai tietoa evästeistä ja niiden tarkoitusperistä (verkkokauppa.com, 2018).

Rekisteristä poistuminen tai tietojensa sellaisesta poistaminen on luotu helpommaksi tietosuoja-asetuksen myötä. Tietosuoja-asetus määrittelee yksilön oikeuden tulla unohdetuksi. Henkilö voi myös pyytää tietojensa oikaisemista. (Tietosuojavaltuutetun toimisto 2017c, 25.) Oikeus tulla unohdetuksi ei kuitenkaan koske esimerkiksi viranomaisen ylläpitämiä rekistereitä, kuten rikosrekisteriä.

GDPR parantaa monella tapaa yksilön oikeuksia ja tuo asiakkaan lähemmäs yritystä. Syyt henkilötiedon käsittelylle on perusteltava, joka helpottaa kerätyn tiedon hahmottamista yrityksissä sekä luo luottamusta asiakkaan ja yrityksen välillä. Tieto myös siitä, että henkilötieto voidaan poistaa tai siirtää toisen palvelun käyttöön, osaltaan vähentää henkilön epävarmuutta ja kasvattaa luottamusta tietojensa luovuttamiselle.

2.5 Sisäänrakennettu ja oletusarvoinen tietosuoja

Rekisterinpitäjän on varmistettava käsiteltävän henkilötiedon toteuttaminen tietosuojaperiaatteiden mukaisesti. Käsittelyprosessin on siis tapahduttava lainmukaisesti,

kohtuullisesti ja läpinäkyvästi. Käsiteltävät tiedot on minimoitava ja osoitettava, että niiden tarpeellisuus yritystoiminnan kannalta toteutuu. Tiedon sisältö tulee olla eheää ja luottamuksellista osoitusvelvollisuuden myös täyttyessä. Tietosuojaperiaatteiden toteutuminen on edellytys sisäänrakennetulle tietosuojalle. (Tietosuojavaltuutetun toimisto 2017c, 13.) Tietosuoja tulee ottaa huomioon jo suunnitteluvaiheessa, jotta esimerkiksi sovelluksessa on huomioitu sen turvallisuus alun alkaen, sisäänrakennetusti. Sovellus, joka tavalla tai toisella sisältää henkilötietoa, on syytä suunnitella vaadittavat turvatoimenpiteet huomioon ottaen.

Vain tarpeelliseksi osoitettujen tietojen kerääminen tulisi olla tietosuoja-asetuksen mukaan oletusarvoista. Kerättävän tiedon käsittelyoikeus tulee oletusarvoisesti olla rajattu vain niille henkilöille, joiden toimenkuvaan rekisterin ylläpito tai muu käsittely kuuluu. (Hyppönen, 2017c.) Yrityksen tulisi siis esimerkiksi varmistaa, tarvitaanko asiakkailta yritystoiminnan jatkuvuuden edellyttämiseksi yhteystietoja, jotka sisältävät asiakkaan nimen ja sähköpostiosoitteen. Tämän jälkeen asiakasrekisterin käsittelyoikeus tulisi olla rajattu vain esimerkiksi myyjien käyttöön, jotka toimenkuvansa puolesta vastaavat asiakkaisiin liittyvästä yhteydenpidosta.

Oletusarvoisesti tietosuojan tulisi toteutua kaikissa palveluissa, joissa henkilötietoa käsitellään. Henkilötiedon koko elinkaaren ajan on varmistettava, että sitä koskevat käsittelytavat ovat tietosuoja-asetuksen mukaiset. (Hyppönen, 2017d.) Yrityksen on siis varmistettava kaikkien toimenpiteiden ja niitä toteuttavien ohjelmien tietosuojan tila sekä tietysti henkilötietoa käsittelevien toimihenkilöinen riittävä taitotaso turvallisen tietojenkäsittelyn toteutumiseksi.

2.6 Kansainvälisyys

Mikäli yritys toimii ulkomailla, helpottuu sen yhteistyö valvontaviranomaisen kanssa. Valvontaviranomaiseen ei tarvitse olla yhteydessä jokaisessa EU:n jäsenvaltiossa, jossa yrityksellä on toimintaa, vaan ainoastaan yhdessä. GDPR esittelee uuden, ”yhden luukun” periaatteen (one-stop-shop), joka mahdollistaa tämän rekisterinpitäjälle tai henkilötiedon käsittelijälle. (Tietosuojavaltuutetun toimisto 2017d, 29.) Suomalainen yritys voi esimerkiksi asioida ainoastaan kotimaisen, päätoimintapaikan mukaan määräytyvän valvontaviranomaisen kanssa, vaikka liiketoiminta ulottuisikin Suomen lisäksi esimerkiksi Viroon, Ruotsiin ja Saksaan.

Yritys saattaa myös olla tilanteessa, jossa sen käsittelemiä henkilötietoja siirtyy EU- ja ETA-maiden ulkopuolelle. Tällaisessa tilanteessa esimerkiksi pilvipalvelun tarjoajan on noudatettava tiettyjä ennalta määrättyjä vaatimuksia, jotka sisältyvät tietosuoja-asetukseen. Mikäli yritys siis hyödyntää esimerkiksi yhdysvaltalaista pilvipalvelua, on kyseisen palveluntarjoajan oltava sitoutunut noudattamaan EU:n tietosuoja-asetusta. (Pöyry, 2017.) Henkilötietojen siirtyminen pilvipalvelun tarjoajan sijainnin johdosta EU:n ulkopuolelle vaatii yritykseltä tarkkaa selvitystyötä, muttei ole mahdoton yhdistelmä tietosuoja-asetuksesta huolimatta. Osa kansainvälisesti toimivista yrityksistä on ilmoittanut sitoutuvansa tietosuoja-asetuksen noudattamiseen, jotta heidän asiakassuhteensa säilyvät ajantasaisten tietosuojaperiaatteiden mukaisesti.

3 TIETOSUOJA-ASETUKSEN VAATIMAT TOIMENPITEET

Tietosuoja-asetukseen valmistautumisesta ja sen vaatimista varautumis- ja perehdytystoimenpiteistä on julkaistu vaihtelevasti erilaisia ohjeita ja koulutuksia. Toisaalta materiaalia on tarjolla paljon, mutta henkilötietorekisterin ylläpitäjän tulee olla kriittinen siinä, kuka tai mikä tarjoaa juuri kyseiselle liiketoiminnalle soveltuvaa apua. Jokaisen yrityksen toimintatavat ovat yksilölliset ja henkilötiedon käsittelyn menettelytavat poikkeavat paljon toisistaan. Yrityksen koko ja henkilökunnan sekä asiakkaiden määrä vaikuttavat toimenpiteiden toteuttamiseen ja tärkeysjärjestyksen laatimiseen.

Tekemistä tietosuoja-asetuksen kanssa voi olla paljon, mutta toteutettujen toimenpiteiden hyödyt ovat yritykselle itselleen usein yllättävän suuret. Henkilötiedon käsittelytoimenpiteiden tarkastelu ja dokumentointi niiden täsmällisyyden varmistamiseksi auttaa antamaan yritykselle kuvan tietojenkäsittelyn tilasta. Kartoitustyötä tehdessään yritykselle saattaa selvitä joidenkin tietojen olevan tarpeettomia tai tietojen käsittelyn turvallisuuteen tulee panostaa enemmän. Tiedon käsittelyyn liittyvät toimenpiteet paranevat turvallisuuden, mutta myös käytännöllisyyden nimissä, kun ylimääräinen ja tarpeettomaksi todettu tieto on poistettu ja jäljelle jäänyt oleellinen tieto on turvattu ja sen käsittelytoimenpiteet selkeytetty. (F-Secure 2018.)

Monelle aiheesta julkaistusta ohjeesta on yhteistä kehotus priorisoida toimenpiteitä kullekin yritykselle sopivaksi. Organisaatiolle olisikin helpompaa lähteä liikkeelle luomalla muistilista toteutettavista toimenpiteistä ja niiden merkitseminen tärkeysjärjestykseen. Tällä tavoin kriittisimmät toimenpiteet tulee varmasti toteutettua määräaikaan mennessä ja hyville, muttei niin oleellisille toimenpiteille jää aikaa asetuksen voimaanastumisen loppupuolelle.

3.1 Tietoturva takaa tietosuojan

Tietoturvatoimenpiteet on oltava yrityksessä ajan tasalla ja toimivat, jotta tietosuoja toteutuu. Osoitusvelvollisuuden täyttyminen, tietotilinpäätös ja monet muut toimenpiteet tietosuoja-asetuksen mukaisesti tehtyinä eivät vielä aseta yritystä täyteen valmiuteen, jos virustorjunta ei toimi jokaisella päätelaitteella tai henkilökunnan tietosuojaosaaminen

on puutteellista. (Hyppönen 2017e.) Tietoturvaan on syytä panostaa aina, mutta viimeistään henkilötietoa sisältäviä rekistereitä käsitellessä yrityksen turvallisuustason on oltava tietyt ehdot täyttävää.

Tieto on osa yrityksen tärkeintä varallisuutta sekä erityisesti asiakkaiden luottamus tietojensa turvalliseen käsittelyyn asettavat tietoturvan toteutumisen tehtävälistan kärkeen. Erilaisia keinoja tiedon turvaamiseen tulee tarkastella sen pohjalta missä muodossa tietoa yrityksessä säilytetään. Mikäli henkilötietorekisteri on esimerkiksi fyysinen kansio, joka sisältää paperilla salassa pidettävää tietoa, tulee kansion säilytyspaikka olla turvattuna. Lukittu arkistokaappi, jonka saa auki vain kansiota toimenkuvansa puolesta käsittelevä työntekijä, takaa jo kyseisen kansion suojaamisen kiitettävästi.

Kun yritystoiminta digitalisoituu muun maailman mukana, tuo se toisenlaisia haasteita tiedon turvaamiseksi. Jos tieto on useammassa sähköisessä kohteessa samanaikaisesti, on tiedon säilyminen turvattu toisaalla ensisijaisen tallennuskohteen esimerkiksi tuhoutuessa. Kannettava tietokone voi rikkoutua, mutta tieto saattaa säilyä pilvessä tai verkkolevyllä. Tiedon säilymisen kannalta tämä on ihanteellista, mutta asettaa aivan toisenlaiset mittasuhteet tietoturvalle, kuin mitä lukollinen arkistokaappi kansiolliselle papereita. Jokainen tietokone, jolla tietoa käsitellään, on suojattava ainakin virustorjuntaohjelmalla, kovalevyn kryptauksella sekä palomuurilla (Valtiovarainministeriö 2013). Käytettävien ohjelmistojen päivitykset ovat oltava ajantasaiset sekä käyttäjäprofiilit on suojattava vahvoilla salasanoilla. Yrityksen on varmistettava käyttämänsä pilvipalvelun tietosuojaperiaatteet ja luotettava siihen, että ulkoiselta taholta ostettu digitaalinen tallennustila on tietyn turvallisuustason täyttävää. Oleellista on myös varmistaa näitä työkaluja käyttävien työntekijöiden tietoturvaperiaatteiden hallitseminen. (Järvinen & Rousku 2017c, 103–104, 137–140, 155.)

Tapauksissa, joissa yrityksen liiketoiminta keskittyy lähes tai täysin digitaalisten palveluiden tuottamiseen, tulee sen tiedostaa ja varmistaa käyttämiensä työkalujen luotettavuus. Internet ei tunne valtion rajoja, tiedon konkretisoiminen on haastavampaa ja yrityksen tuottaman ja omistaman tiedon kokonaisuuden hahmottaminen monimutkaisempaa. Jokaisen yrityksen tulisikin kantaa vastuu käsittelemänsä tiedon turvaamisesta parhain mahdollisin keinoin. (Järvinen & Rousku 2017d, 12, 24–25.)

3.2 Henkilörekisterien kartoitus

Tietosuoja-asetus määrittelee henkilörekisteriksi kaikki sähköisessä muodossa olevat henkilötiedot sekä esimerkiksi joukon henkilötietoa sisältäviä papereita, jos ne on lajiteltu aakkosjärjestykseen (Rihti 2016). Yrityksellä on yleensä hallussaan vähintään henkilökuntaansa koskeva rekisteri, mutta monesti myös yrityksen asiakkaista ylläpidetään tunnistettavissa olevaa tietoa. Henkilörekisterien kartoitusta on siis lähdettävä tarkastelemaan ainakin kahdesta eri näkökulmasta. Millaista henkilökuntaa koskevaa tietoa yritys rekisteröi sekä millainen rekisterijärjestelmä yrityksellä on asiakkaistaan.

Henkilötiedon kartoitustyössä on tärkeää selvittää sen tarpeellisuus ja siihen liittyvät käsittelyprosessit. Lista henkilötiedon käsittelijöistä ja heidän käsittelyprosesseistaan auttaa luomaan kokonaiskuvaa yrityksen henkilötietoarkkitehtuurista. Henkilötiedon käsittelyprosessien hahmottaminen vaatii siis tallennusprosessien havainnollistamisen lisäksi myös tutustumista toimihenkilöihin, joilla on pääsyoikeus kyseessä olevien rekisterien hallinnoimiseen. On tärkeää määritellä, miksi kyseisillä toimihenkilöillä on käsittelyoikeus henkilötietorekistereihin. Erilaisten henkilötietorekisterien käsittely osana toimihenkilön työnkuvaa vaatii hahmottamista, jota voi lähestyä haastattelemalla kyseisiä työntekijöitä. Työntekijän toimenkuvan kannalta henkilötietojen käsittelyn on oltava tarpeellista. Näin varmistetaan, että henkilötietorekistereitä käsitellään ainoastaan välttämättömissä tilanteissa. (Tietosuojavaltuutetun toimisto 2014.)

Kun yrityksen ylläpitämät henkilötietorekisterit on listattu ja tiedetään mitä kerätään, miksi ja kuka tai ketkä rekistereitä pääsääntöisesti työnkuvansa puolesta käsittelevät, on rekisterien kuvaaminen esimerkiksi prosessikaavion muodossa helppoa. Haastattelujen pohjalta lähtötilanne saadaan käsitetyksi, josta onkin loogista lähteä suunnittelemaan mahdollisia tietosuoja-asetuksen tuomia muutoksia.

3.3 Henkilökunnan perehdytys

Tietosuoja-asetuksen noudattamista helpottavat ohjeistukset, kuten tietotilinpäätös, toimivat osana henkilökunnan perehdytystä. Henkilötiedon käsittelymenetelmiä kartoittavat dokumentit osoitusvelvollisuuden täyttymisen lisäksi tukevat henkilökunnan tietouden lisäämistä, jos kyseisiin dokumentaatioihin tutustuminen on osa perehdytystä tai koulutusta. Muita perehdytystä tukevia dokumentteja voivat olla esimerkiksi tietoturva- ja

tietosuojaopas henkilöstölle, salassapitosopimus ja sen kuittauksen edellyttäminen, yrityksen sisäisestä tietoverkosta, intranetistä löytyvät yleiset ohjeet lajiteltuina teemoittain sekä linkkejä ulkoisten tahojen, kuten viranomaisten laatimiin ohjeisiin.

Tietosuoja-asetuksen tuodessa uusia vaatimuksia turvallisen tietojenkäsittelyn toteutumiseksi, tulee perehdytyksen ajankohtainen sisältö varmistaa. Koulutuksen pitäjänä tulisikin olla henkilö tai henkilöitä, jotka ovat tutustuneet uuteen tietosuoja-asetukseen ja osaavat soveltaa sen määrittelemiä toimenpiteitä juuri kyseiseen organisaatioon. Osoitusvelvollisuuden täyttymiseksi koulutuksen pitämisestä tulisi saada kirjallinen merkintä, joka tallentaa koulutuksen ajankohdan, sisällön pääpiirteissään ja niiden henkilöiden kuittauksen, jotka koulutukseen tai perehdytykseen osallistuivat. Henkilörekisterejä käsittelevien toimihenkilöiden perehdytys asetuksenmukaisuuteen on avainasemassa muuta henkilökuntaa unohtamatta. Esimerkiksi työharjoitteluun osallistuvalle henkilölle yrityksen toimintaperiaatteisiin ja varsinkin tietosuojatoimenpiteisiin perehdyttäminen on erittäin tärkeää salassapitosopimusta unohtamatta. Tietosuojaa vahvasti tukevien salassapitosopimusten allekirjoitus tulisi aina olla ensimmäisten allekirjoitettavien sopimusten listalla työsuhteen solmimisen yhteydessä. (OpiTietosuojaa.fi 2018.)

Uusi tietosuoja-asetus tuo yritykselle ajankohtaiseksi henkilökuntansa perehdyttämisen, mutta digitalisaation kiihtyvän muutos- ja uudistusvauhdin mukana erilaiset ohjeet ja säädökset elävät jatkuvasti näiden muutosten mukana. Organisaation olisikin hyvä ottaa viimeistään GDPR:n myötä käyttöönsä säännöllisten koulutusten järjestäminen ja uusien työntekijöiden ja harjoittelijoiden perehdyttäminen osaksi rutiinitoimenpiteitä.

4 HALLINNOLLINEN JA TEKNINEN TIETOTURVA

Teoksessa Työpaikan tietoturvaopas, Järvinen ja Rousku (2017e, 54–55) toteavat työpaikan tietoturvallisuuden olevan osa organisaation kokonaisturvallisuutta. Oppaassa myös painotetaan turvallisen työympäristön luomista henkilöstölle, yrityksen asiakkaille ja muille sidosryhmille varmistamalla kiinteistön turvallisuus ja varautuminen mahdollisiin poikkeamatilanteisiin.

Uuden tietosuoja-asetuksen myötä toimeksiantaja ryhtyi päivittämään sekä hallinnollista, että teknistä tietoturvaansa. Yksi keskeisimmistä tavoitteista oli dokumentoida ylläpidetyt toimenpiteet sekä tietoturvan, että yleisen turvallisuuden osalta. Opinnäytetyön tarkoituksena oli luoda ja avustaa yhteistyössä tapausyrityksen toimihenkilöiden kanssa koulutuksia ja ohjeita, jotka perehdyttävät koko henkilökunnan toimimaan laadittujen ohjeiden mukaisesti, sekä olemaan tietoisia toimenpiteistä, joita mahdollisen poikkeamatilanteen tapahtuessa tulee suorittaa. Hallinnollisen ja teknisen tietoturvan kehittämiseen sisältyi jatkuvuussuunnitelman ja tietoturvaohjeen tuottaminen. (Lähde 2018a.)

Tietoturvan toteutumisen tueksi luodut dokumentaatiot tuotiin myös osaksi perehdytys- ja koulutusmateriaaleja, jotka olisivat jokaisen työntekijän ja työharjoittelijan saatavilla jatkuvasti. Ohjeiden lisäksi toimeksiantaja ylläpitää työntekijöiden sisäisen kommunikointipalvelun yhteydessä kanavaa, jonne tietoturva- ja tietosuoja-aiheiset kysymykset voi esittää milloin tahansa. Näillä toimenpiteillä toimeksiantaja mahdollistaa jokaiselle työntekijälle pysyä viimeisimpien tietoturvaa koskevien päivitysten ja ohjeiden tasalla, mutta myös helpon tavan kysyä tai informoida poikkeamatilanteista tai niiden epäilyistä.

4.1 Tietotilinpäätös

Yksi tietosuoja-asetukseen valmistautumista helpottava menetelmä on tietotilinpäätöksen laatiminen. Sen avulla yritys voi kuvata toimintaperiaatteensa, tietojen käsittelyn ulkoistamiseen liittyvät käytännöt, tietoturva- ja jatkuvuussuunnitelmansa sekä muita tietojenkäsittelyä koskevaa ohjeistusta. (Andreasson ym. 2014d, 118–119.)

Tietotilinpäätöksestä toimeksiantajalle pyrittiin tekemään dokumentaatio, josta selviää yrityksen keskeisimmät henkilötiedon käsittelytoimenpiteet sekä perustelu henkilötiedon käsittelylle. Toistaiseksi tietotilinpäätöksessä keskityttiin tietosuoja-asetuksen vaatiman

osoitusvelvollisuuden täyttymisen toteutumiseen, mutta kyseistä asiakirjaa on helppo laajentaa ja rakentaa siitä tulevaisuudessa huomattavasti organisaation kaikkia toimintaprosesseja paremmin kuvaava dokumentaatio. Tietotilinpäätöksestä voidaan julkaista useampi eri versio ja sitä voidaan sekä laajentaa, että supistaa käyttötarkoituksesta riippuen (Andreasson ym. 2014e, 119). Trafin (2017) tietotilinpäätökset vuosilta 2015 ja 2016 on julkaistu heidän kotisivuillaan. Näistä julkaistuista tietotilinpäätöksistä saa apua oman versionsa tekemiseen. Väestörekisterikeskus (2018) on julkaissut myös verkossa kuluneiden vuosien tietotilinpäätöksiään. Molempien organisaatioiden tietotilinpäätöksistä pystyy ainakin päättelemään yhteistyön ja ajankulun olleen mittavia dokumentaatioita luodessa, sillä ne kattavat erittäin kokonaisvaltaisesti koko organisaation tietojenkäsittelyn.

Toimeksiantajalle toteutetuista toimenpiteistä tietosuoja-asetukseen valmistautumiseen liittyen, tietotilinpäätös muodostui koko prosessia kantavaksi operaatioksi. Tietotilinpäätöksen tekeminen eteni esimerkkejä ja ohjeita noudattaen, jonka jälkeen luotiin yritykselle niiden perusteella oma versio. Tietotilinpäätöksen laajentuessa ja täsmentyessä toimeksiantajalle heräsi tarve myös muille dokumenteille ja perehdytysmateriaaleille. Nämä dokumentaatiot olivat esimerkiksi jatkuvuussuunnitelma sekä muut varotoimenpiteet poikkeamatilanteita varten.

Opinnäytetyön aikana tietosuoja-asetukseen valmistautumisen kulmakivenä pidettiin osoitusvelvollisuuden täyttymistä. Toimeksiantajalle oli tärkeää, että tietoturvan takaamiseksi tehdyt toimenpiteet olisivat dokumentoitu, jotta niiden ylläpitäminen ja henkilötiedon asianmukainen käsittelyprosessi voidaan osoittaa olevan asetuksenmukainen. Huolellisuus prosessien kuvaamisessa on tärkeää, jotta esimerkiksi henkilötiedon käsittelyn kohteena olevalle asiakkaalle voidaan pyydettäessä kuvata henkilötiedon käsittelyprosessi.

4.1.1 Tietotilinpäätöksen laatiminen

Tietosuojavaltuutetun toimiston julkaisemassa sähköisessä Laadi tietotilinpäätös – ohjeessa on kysymykset, joihin vastaamalla tietotilinpäätöksen runkoa on helppo lähteä hahmottelemaan:

1. Mitä tietovarantoja organisaation hallussa on?
2. Mikä on organisaation hallussa olevien tietojen laatu ja käytettävyys?

3. Mitä menettelytapoja ja periaatteita tietojen käsittelyssä noudatetaan?
4. Miten tiedot on suojattu?
5. Miten tietojen käyttöä valvotaan?
6. Miten rekisteröityjen oikeudet tietojen käsittelyssä toteutetaan?

(Laadi tietotilinpäätös, Tietosuojavaltuutetun toimisto 2012, 6.)

Toimeksiantajalle tuotetun tietotilinpäätöksen runko hahmottui pitkälti yllämainittujen kysymysten pohjalta. Kysymykset esitettiin niille toimihenkilöille, jotka vastaavat henkilötiedon käsittelyn ylläpidosta ja joilla on pääsy- ja muokkausoikeus valtaosiin ylläpidetyistä rekistereistä. Henkilötiedon käsittelyn jakautuessa useille eri toimihenkilöille, oli heidän haastatteleminen ja heiltä saatu apu tärkeä osa tietotilinpäätöksen laatimista. Haastattelujen pohjalta luotiin taulukot henkilötietorekistereistä sekä henkilötiedon käsittely dokumentti. (Lähde 2018b, Lähde2018c.)

Ensin hahmoteltiin kaikki henkilötieto, jota toimeksiantaja käsittelee. Kaiken henkilötiedon tarpeellisuus kyseenalaistettiin ja pohdittiin erityisesti sitä, onko yrityksen hallussa sellaista henkilötietoa, joka ei ole oleellista. Oli tärkeä pohtia pitääkö tieto enää paikkaansa ja voidaanko sitä vielä jossain tilanteessa tarvita. Henkilötietoa koskevat menettelytavat ja periaatteet olivat toimeksiantajalle hyvin selkeitä eikä niitä varten vaadittu erityisiä muutoksia asetuksen noudattamiseksi. Tietojen suojaaminen kuitenkin asetti haasteita tallennustilan ulkoistamisesta johtuen. Esimerkiksi virtuaalipalvelimen ylläpitämältä yritykseltä piti varmistaa, sitoutuuko se noudattamaan tietosuoja-asetusta. Tietojen valvominen oli yrityksessä jo ennen kartoitustyötä hyvin hoidettu, mutta tietotilinpäätöksen osaksi kuului näiden käytäntöjen dokumentointi.

Osoitusvelvollisuuden täyttymisen ollessa tietotilinpäätöksen keskiössä, oli erittäin oleellista pohtia rekisteröityjen oikeuksia tietojen käsittelyssä. Tietotilinpäätöksessä on tarkoitus vastata johdonmukaisesti siihen, mitä tietoa käsitellään, miksi sitä käsitellään ja mitkä ovat rekisteröidyn oikeudet. Näitä kysymyksiä selvennettiin tietotilinpäätökseen, jonka pohjalta on myös helppo luoda esimerkiksi tietosuojaseloste, joka tulisi rekisteröityjen luettavaksi.

4.1.2 Tietotilinpäätöksen hyödyt

Yritys hyötyy tietotilinpäätöksestä moninkertaisesti. Henkilörekisterien kartoittamisen lisäksi niiden käsittelyprosessit tulee kirjattua ylös ja näin ollen hahmoteltua selkeästi.

Tiedon suojaamisen ja turvallisen käsittelyn oletuksena voidaan pitää tietoisuutta yrityksen prosesseista siihen liittyen. Jotta organisaatio voi taata henkilötiedon turvallisen ja sen arvoa kunnioittavan käsittelyn, täytyy se pystyä todistamaan. Selvennystä vaativissa tilanteissa tietotilinpäätöksen kuuluisi toimia vastauksia antavana dokumenttina tiedon käsittelyyn liittyen.

Henkilötiedon käsittelyprosessien muuttuessa toimenpiteisiin on vaivattomampaa ryhtyä, kun olemassa olevat prosessit on jo kirjattu ylös. Muutostarve prosesseille on myös helpompaa huomata, kun niistä on laadittu selkeä dokumentaatio. Joidenkin prosessien ollessa epäselviä, voidaan niitä tarkastella ja selventää tutkimalla tietotilinpäätöstä.

Tietojen asetuksenmukaiset käsittelyprosessit on kirjattu yksien kansien sisään, joka osaltaan toteuttaa tietosuoja-asetuksen edellyttämän osoitusvelvollisuuden täyttymisen. Tietotilinpäätöksestä hyödytään, kun sen ajantasaisuus varmistetaan laatimalla säännöllinen tarkistusväli sen läpikäynnille.

5 LOPUKSI

Opinnäytetyön tavoitteena oli kartoittaa toimeksiantajayrityksen henkilötiedon käsittelytapoja, tallentaa ja kirjata ylös sen tietoturvaan keskitettyjä prosesseja sekä ennen kaikkea valmistautua EU:n uuteen tietosuoja-asetukseen. Tehdyn kartoitustyön ja valmistautumisen tavoitteena pidettiin myös yrityksen valmiustasoa osoitusvelvollisuuden täyttymiseksi sekä opinnäytetyön tekijän osaamisen kartuttamista ajankohtaisesta aiheesta.

EU:n tietosuoja-asetus on uusi, ja se koskee jokaista henkilötietorekistereitä käsittelevää organisaatiota. Tästä syystä aiheesta on julkaistu paljon erilaista materiaalia, jonka pohjalta toimeksiantajallekin oli mahdollista toteuttaa tietosuoja-asetuksen vaatimia toimenpiteitä. Ohjeita hyödyntäen toimeksiantajalle pystyttiin toteuttamaan henkilötiedon käsittelyprosessit kartoittava dokumentaatio, jonka avulla selkeytettiin toimintaprosesseja sekä varmistettiin henkilötiedon käsittelyä koskevien toimenpiteiden asetuksenmukaisuus. Opinnäytetyön menetelminä voidaan siis pitää aiheesta julkaistun materiaalin läpikäymistä ja sen pohjalta toteutettujen dokumentaatioiden, ohjeistusten sekä koulutusten järjestämistä.

Päätuloksina opinnäytetyölle voidaan pitää toimeksiantajayrityksen parempaa valmiutta toimia asetuksenmukaisesti ja osoittaa liiketoimintansa olevan ns. GDPR-valmis. Opinnäytetyön tekijänä sain ansaittua työkokemusta erittäin ajankohtaisesta aiheesta, joka edesauttaa ICT-alalle työllistymistä opintojen päätyttyä.

Uusi EU-direktiivi asettaa haasteita ja joissain määrin myös aiheuttaa hämmennystä. Ohjeita ja koulutuksia ollessa paljon tarjolla, täytyy niihin perehtyä ja olla tarkkana siitä, millainen ohjeistus koskee omaa yritystoimintaa sekä millainen toimenpiteitä koskeva tärkeysjärjestys tulisi toimenpiteiden toteuttamiselle asettaa. Organisointikyvyn, kriittisen tiedonlukutaidon ja uuden asiakokonaisuuden sisäistäminen ovat taitoja, joiden omaksumisessa onnistuin.

Tietotilinpäätös ja yrityksen tietoturvamenetelmien kartoitustyöt vaativat koko yrityksen henkilökunnan panostusta, mutta erityisesti hallinnollisessa asemassa olevien toimihenkilöiden valveutuneisuutta. Tietosuoja-asetukseen perehtymisessä onnistuttiin, mutta keväälle 2018 jäi vielä tekemistä. GDPR on uusi asetus, jonka soveltamista suoraan lakiin ei ole vielä tehty. Tästä syystä yrityksen todellista valmiustasoa voidaan kokea

testattavan vasta sitten, kun tietosuoja-asetukseen liittyvät ensimmäiset esimerkkitapaukset tulevat julki.

Olen toteuttanut opinnäytetyön sisältämät toimenpiteet yhteistyössä toimeksiantajan edustamien toimihenkilöiden kanssa. Opinnäytetyö oli osa työharjoittelua, joten toimenpiteet on toteutettu toimestani ensimmäistä kertaa. Yhteistyön ja tarkkuuden ansiosta monet opinnäytetyössä esiintyvät kartoitustyöt on toteutettu siten, että niistä on varmasti hyötyä yritykselle.

Toimeksiantajalle toteutettu työ, jonka tarkoituksena on varmistaa yrityksen valmius uuden tietosuoja-asetuksen vaatimien toimenpiteiden noudattamiseksi, voisi mahdollisesti toimia tulevaisuudessa kehikkona asiakkaille toteutetuista auditoinneista, jotka mittaisivat yrityksen tietoturvatasoa. Mikäli toimeksiantaja ei lähde toteuttamaan uutena palveluna asiakkaille tietoturvakartoituksia, voidaan opinnäytetyön osana tehtyjä toimenpiteitä kuitenkin hyödyntää ja soveltaa muulla tavalla. Vastaisuudessa hallinnollisten ja teknisten tietoturvametodien päivittäminen on ainakin jouhevampaa aikaisemmin luotujen dokumentaatioiden ansiosta. Esimerkiksi tietotilinpäätöksen päivittäminen on helpompaa nyt, kun kyseinen dokumentaatio on luotu.

Opinnäytetyö antoi erinomaista työkokemusta todellisen yrityksen toimintatavoista uuden direktiivin asettamien säädösten tutkimisessa ja niiden mukaan toimimisessa. Paras mahdollinen tapa valmentautua työelämään on toteuttaa sellainen projekti opinnäytetyönä, joka vahvistaa osaamista ja itsevarmuutta alan ammattilaisena.

LÄHTEET

Andreasson, A.; Koivisto, J. & Ylipartanen, A. 2014a, b, c, d, e. Tietosuojavastaavan käsikirja 2. Helsinki: Tietosanoma Oy.

EUGDPR.org. Julkaisuajankohta ei tiedossa. Viitattu 2.3.2018. https://www.eugdpr.org/key-changes.html

Pöyry, K. 2017. GDPR ja tietosuoja globaalissa julkisen pilven ympäristössä. Viitattu 19.3.2018. https://gapps.fi/fi/blog/gdpr-ja-tietosuoja-globaalissa-julkisen-pilven-ymparistossa/

Jakso 2. Kohti tietosuoja-asetusta, vieraana Eija Warma. F-Secure 2018. Viitattu 14.3.2018. https://soundcloud.com/f-secure/kyberykset-jakso-2

Hyppönen, J. 2017. EU:n tietosuoja-asetus ja sen vaikutukset. Viitattu 21.2.2018a, 2.3.2018b, 7.3.2018c, 12.3.2018d, e. https://www.fordione.fi/blogi/98-eu-n-tietosuoja-asetus-ja-sen-vaikutukset

Järvinen, P. & Rousku, K. 2017a, b, c, d, e. Työpaikan tietoturvaopas. Helsinki: Alma Talent.

Laadi tietotilinpäätös. 2012. Viitattu 1.3.2018. Sähköinen opas saatavilla osoitteesta http://tietosuoja.fi/fi/index/materiaalia/oppaat.html

Lähde. A. 2018. Hallinnollisen ja teknisen tietoturvan toteutus. Toimeksiantajayrityksen intranet. Viitattu 30.4.2018.

Lähde. A. 2018. Taulukot henkilörekistereistä. Toimeksiantajayrityksen intranet. Viitattu 30.4.2018.

Lähde. A. 2018. Henkilötiedon käsittely. Toimeksiantajayrityksen intranet. Viitattu 30.4.2018.

Kysymyksiä ja vastauksia tietosuojauudistuksesta 2016. Viitattu 15.2.2018. http://www.tietosuoja.fi Etusivu > EU:n Tietosuojauudistus > Kysymyksiä ja vastauksia

Kangasniemi & Lintulahti 2017. Mikä on pilvipalvelu? Viitattu 17.4.2018. https://yksityisille.hub.elisa.fi/mika-on-pilvipalvelu/

Miten valmistautua EU:n tietosuoja-asetukseen? 2017b, c, d, e. Viitattu 15.2.2018. Sähköinen opas saatavilla osoitteesta http://tietosuoja.fi/fi/index/euntietosuojauudistus.html

Ohjelmistoyrittäjät ry 2016. Viitattu 5.3.2018b ja 13.3.2018a. http://www.gdpr.fi/ > Sanasto.

OpiTietosuojaa.fi 2018. Viitattu 16.3.2018. https://opitietosuojaa.fi Etusivu > Työkalupakki > Perehdyttäminen

Pynnä, P. 2016. Tietosuoja-asetus for dummies – 10 askeleen ohjelma. Viitattu 5.3.2018. https://www.asml.fi/blogi/tietosuoja-asetus-10-pointtia/

Pynnä, P. 2018. Puretaan myyttejä – GDPR ja suostumus. Viitattu 5.3.2018. https://www.asml.fi/blogi/gdpr-eu-tietoosuoja-asetus-suostumus/

Päätelaitteiden hallinta 2013. Viitattu 12.4.2018. https://www.vahtiohje.fi Vahti-ohjeet > 2013 > Päätelaitteiden tietoturvaohje > Päätelaitteiden hallinta

Saarelainen A. Tällainen on tietosuoja-asetus – jopa 20 miljoonan sakot uhkaavat rikkojia. Tivi. Viitattu 16.3.2018. https://www.tivi.fi/Kaikki_uutiset/tallainen-on-tietosuoja-asetus-jopa-20-miljoonan-sakot-uhkaavat-rikkojia-6606546

Tarhonen L. 2018. Työttömäksi kolmessa kuukaudessa – tietosuoja-asiantuntijan tavoite ennen toukokuuta 2018. Viitattu 15.3.2018. https://www.asml.fi/blogi/gdpr-eu-tietosuoja-asetus/

Rihti 2016. Tiesitkö, että EU:n uusi tietosuoja-asetus tulee vaikuttamaan kaikkiin yrityksiin Suomessa? Viitattu 12.4.2018. https://www.telia.fi/yrityksille/artikkelit/artikkeli/tietosuoja-asetus-vaikuttaa-kaikkiin

Tietosuojavaltuutetun toimisto 2017a. Viitattu 5.3.2018. http://www.tietosuoja.fi Etusivu > Usein kysyttyä > Työelämä

Tietosuojavaltuutetun toimisto. 2013. Viitattu 5.3.2018. http://www.tietosuoja.fi Etusivu > Tietosuoja-aiheista sanastoa

Tietosuojavaltuutetun toimisto 2014. Viitattu 8.4.2018. http://www.tietosuoja.fi Etusivu > Rekisterinpitäjälle > Käyttötarkoituksen määrittely ja käsittelyn suunnittelu

Tietoturvan hallintajärjestelmä. Tietojesiturvaksi.fi. Viitattu 19.3.2018. https://tietojesiturvaksi.fi Etusivu > Tietoturvasuunnitelman laatiminen > Tietoturvan hallintajärjestelmä

Tietoturvapoikkeamatilanteiden hallinta 2017. Viitattu 12.3.2018. Sähköinen opas saatavilla osoitteesta https://www.vahtiohje.fi/web/guest/home;jsessionid=42F3089C10830C2AD01587242FA672CCB4B3417A354469FDA9746C42E8FA815CF6AB77B2358FA7312372B3

Trafi. 2017. Viitattu 20.3.2018. https://www.trafi.fi Etusivu > Tietopalvelut > Tietotilinpäätös

Tulli. 2018. Viitattu 16.3.2018. http://tulli.fi Tietoa tullista > Tullin toiminta > Tullialueet > EU-, Eta, Efta- ja Schengen-maat

Verkkokauppa.com. 2018. Viitattu 22.3.2018. https://www.verkkokauppa.com Etusivu > Ohjeita > Tietosuojaseloste

Väestörekisterikeskus 2018. Viitattu 20.3.2018. http://vrk.fi Tietoa Väestörekisterikeskuksesta > Tietotilinpäätös