Saimaan ammattikorkeakoulu
Liiketalous Lappeenranta
Liiketalouden koulutusohjelma
Yritysten ja taloushallinnon juridiikka

Leila Turunen

Tietosuojavastaava Euroopan Unionin yleisen tietosuoja-asetuksen mukaan

Opinnäytetyö 2017

Tiivistelmä

Leila Turunen
Tietosuojavastaava Euroopan Unionin yleisen tietosuoja-asetuksen mukaan, 39 sivua, 1 liite
Saimaan ammattikorkeakoulu
Liiketalous Lappeenranta
Liiketalouden koulutusohjelma
Yritysten ja taloushallinnon juridiikka
Opinnäytetyö 2017
Ohjaajat: lehtori Timo Hynynen, Saimaan ammattikorkeakoulu

Tämän opinnäytetyön tavoitteena oli tutkia tietosuojavastaavan nimittämistä, asemaa ja tehtäviä yleisen tietosuoja-asetuksen mukaan. Opinnäytetyö perustui aiheen ajankohtaisuuteen. Yleistä tietosuoja-asetusta aletaan soveltaa 25. toukokuuta 2018.

Opinnäytetyön tutkimusmenetelmänä käytin lainopillista tutkimusmenetelmää. Teoriaosuuden oikeuslähteinä käytin Suomen henkilötietolakia, Euroopan Unionin yleistä tietosuoja-asetusta, WP29-tietosuojatyöryhmän ohjeistusta ja TATTI-työryhmän mietintöä sekä aiheeseen liittyvää kirjallisuutta ja internet-aineistoja. Empiirisessä osassa selvitin pienen tilitoimiston tarvetta nimittää tietosuojavastaava yritykseensä.

Tutkimuksen tuloksena syntyi tietosuojavastaavan huoneentaulu. Tarkoituksena oli saada aikaan selkeä huoneentaulu kaikkien sitä tarvitsevien käytettäväksi. Tutkimuksessa avattiin yleisen tietosuoja-asetuksen käsitteitä ja tietosuojavastaavaan liittyvien artikloiden sisältöä.

Asiasanat: tietosuojavastaava, tietosuoja, henkilötieto, rekisteröity, rekisterinpitäjä, yleinen tietosuoja-asetus

Abstract

Leila Turunen
Data Protection Officer in accordance with the General Data Protection Regulation of the European Union, 39 pages, 1 appendix
Saimaa University of Applied Sciences
Faculty of Business Administration Lappeenranta
Degree Programme in Business Administration
Specialisation in Business Law
Bachelor´s Thesis 2017
Instructor: Mr Timo Hynynen, Senior Lecturer

The objective of this thesis was to examine the designation, position and tasks of the data protection officer in accordance with the General Data Protection Regulation of the European Union. The thesis based on the relevance of the topic. The General Data Protection Regulation shall be applied from 25 May 2018.

The research method for the thesis was a juridical research method. The sources of the theoretical part were the Finnish Personal Data Act, the General Data Protection Regulation of the European Union, the Article 29 Data Protection Working Party's Guidelines and the TATTI Working Group Report. Also related literature and Internet materials were used. In the empirical part was searched the need for a small accounting firm to designate the data protection officer.

As a result of this thesis, the information sheet of the data protection officer was made. The aim was to make a simple information sheet, so anyone in need of one could use it. The study opened up the concepts of the General Data Protection Regulation and the content of articles related to the data protection officer.

Keywords: data protection officer, data protection, personal data, data subject, controller, General Data Protection Regulation

Sisällys

Lyhenteet ja käsitteet

EU	Euroopan unioni
EY	Euroopan yhteisö
GDPR	EU:n yleinen tietosuoja-asetus
Henkilötieto	Kaikkia tunnistettavaan tai tunnistettavissa olevaan luonnolliseen henkilöön koskeva tieto.
Henkilötietojen käsittelijä	Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.
Henkilötietojen käsittely	Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti.
Rekisterinpitäjä	Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
Rekisteröity	Luonnollinen henkilö, jonka henkilötietoja käsitellään.
Profilointi	Henkilötietojen automaattinen käsittely, jossa arvioidaan kyseisen henkilön henkilökohtaisia ominaisuuksia henkilön tietoja käyttäen.
Tietosuoja	Yksityisyyden suojaaminen henkilötietoja käsiteltäessä.
Tietosuojavaltuutettu	Valvontaviranomainen, joka valvoo henkilötietojen rekisteröintiä, käyttöä ja luovutusta.
Tietosuojavastaava	Tietosuoja-asetuksen määrittelemä rooli, jonka henkilötietojen käsittelijä tai rekisterinpitäjä nimeävät organisaatioon asiantuntijaksi.
Tietotilinpäätös	Tietotilinpäätös on organisaation laatima vapaaehtoinen raportti, joka antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta.
TATTI-työryhmä	Oikeusministeriön nimittämä EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmä
Vaikutuksenarviointi	Suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointi tietosuojaan ja yksilön vapauksiin.

WP29-tietosuojatyöryhmä	EU:n tietosuojavaltuutetuista koostuva riippumaton, neuvoa antava elin.

1 Johdanto

Tässä opinnäytetyössä tutkitaan Euroopan unionin yleistä tietosuoja-asetusta tietosuojavastaavan näkökulmasta. Aihe on valittu ajankohtaisuutensa vuoksi ja kiinnostus aiheeseen on omakohtainen. Ajankohtaiseksi aiheen tekee se, että Euroopan unionin tietosuoja-asetusta aletaan soveltaa Suomessa ja muissa EU:n jäsenvaltioissa 25.5.2018 alkaen. Tietosuoja-asetuksen mukaan tietosuojavastaava on nimettävä, jos tietojenkäsittelyä suorittaa viranomainen tai julkisen alan toimielin ja yrityksien, jotka käsittelevät henkilötietoja systemaattisesti ja laaja-alaisesti. Tietosuojavastaavan asema, nimittäminen ja tehtävät ovat varsinkin pienille ja keskisuurille yrityksille uusia asioita ja on tärkeää tietää, mitä heidän tulee ottaa huomioon tietosuoja-vastaavaa nimittäessään ja mitä tietosuojavastaavan toimenkuvaan kuuluu. Asetuksessa on myös määritelty, mitkä tehtävät tietosuojavastaavalla täytyy olla. Näiden tehtävien lisäksi tiesuojavastaavalla voi olla myös muita erikseen määriteltyjä tehtäviä.

1.1 Tavoitteet

Opinnäytetyön tavoitteena on löytää vastaus kysymykseen: Mikä on tietosuojavastaavan asema yleisen tietosuoja-asetuksen mukaan? Tarkoitus on myös selvittää, mitä organisaatioiden johdon tulee ottaa huomioon tietosuojavastaava nimitettäessä ja millaisia muutoksia se aiheuttaa yrityksille. Yleistä tietosuoja-asetusta ja sen artikloita tutkin tietosuojavastaavan näkökulmasta ja lisäksi selvitän, mitä konkreettista yritysten tulee ottaa huomioon siirtymäaikana, ennen kuin asetus tulee voimaan toukokuussa 2018. Tavoitteena on myös laatia selkeä ja konkreettinen huoneentaulu tietosuojavastaavalle hänen tehtävistään ja vastuistaan. Opinnäytetyössä tutustun myös yhden pienen yrityksen rekistereihin ja selvitän, onko niiden perusteella kyseisen yrityksen nimettävä tietosuojavastaava yleisen tietosuoja-asetuksen mukaan.

1.2 Rajaukset

Tutkimuksessa keskityn pelkästään tietosuojavastaavan näkökulmaan. Rajauksen avulla haluan konkreettista tietoa tietosuojavastaavan tehtävistä ja vastuista, jotta yritykset voisivat hyödyntää näitä tietoja käytännössä. Yksittäisen osakokonaisuuden eli tietosuojavastaavan aseman tutkiminen tässä opinnäytetyössä on

ajankohtaisuutensa vuoksi hyvin looginen valinta. Ulkopuolelle jätän yleisen tietosuoja-asetuksen tutkimisen ja rekisterinpitäjän oikeuksien ja velvollisuuksien sekä rekisteröidyn oikeuksien tutkimisen. Nämä aiheet rajaan ulkopuolelle, koska näitä on jo tutkittu jonkin verran aikaisemmissa tutkimuksissa ja tietosuojavastaavan rooli tulee olemaan merkittävä hyvinkin monissa yrityksissä.

Primääriaineistona tutkimuksessa käytän lainopillisia oikeuslähteitä. Oikeuslähteisiin luetaan etenkin lait, säädökset ja niiden valmisteluaineisto, oikeustapaukset ja oikeuskirjallisuus. Edellä mainitut lähteet voidaan jakaa niiden velvoittavuuden mukaan kolmeen ryhmään: vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin. (Husa, Mutanen & Pohjolainen, 2008, 32–33.) Lainsäädännön jatkohankkeissa keskityn lähinnä TATTI-työryhmän mietintöön, jossa työryhmä on antanut esityksen kansallisen lainsäädännön muuttamiseksi.

2 Tutkimusmenetelmä

Opinnäytetyön tutkimuksessa käytän lainopillista tutkimusmenetelmää, joka perustuu lakeihin ja säädöksiin. Lainopillisen tutkimuksen tehtävänä on vastata tutkimuskysymykseen voimassa olevan oikeusjärjestyksen mukaan. Keskeistä on myös tulkita voimassa olevaan oikeusjärjestykseen kuuluvia sääntöjä ja niiden sisältöä. Lainoppi eli oikeusdogmatiikka perustuu voimassa oleviin oikeuslähteisiin. Lainopillisessa tutkimuksessa oikeuslähteitä tulee käyttää etusija- ja käyttöjärjestyssääntöjen osoittamassa järjestyksessä. (Husa, Mutanen & Pohjolainen 2008, 20.)

Luku perustuu kokonaisuudessaan Antti Kolehmaisen (2005) artikkeliin *Tutkimusongelma ja metodi lainopillisessa työssä*. Kolehmaisen mukaan lainopin tarkoituksena on tuottaa voimassa olevaa oikeutta koskevia perusteltuja tulkinta-, punninta- ja systematisointikannanottoja eli lyhyesti sanottuna, mitä oikeus oikein on. Näissä kannanotoissa keskityn siihen, mikä on voimassa olevan oikeuden tietyn hetkinen sisältö vallitsevan lainopin mukaisesti. Huomiota kiinnitän siihen, miten oikeus on tosiallisesti toteutunut ja miten se tulee tulevaisuudessa todennäköisesti toteutumaan. Tutkimusongelman tulee olla yhteiskunnallisesti tärkeä tai muuten sitä ei ole järkevää ruveta tutkimaan.

Lainopillisessa tutkimuksessa tutkimuskysymys on tutkimuksen tärkein elementti. Tutkimuskysymyksen tulee olla tutkimuksen punainen lanka, jota noudatetaan koko tutkimuksen ajan. Tutkimuskysymys voi olla säännösten tulkintaa tai systematisointia, joilla haen tietoa oikeusjärjestyksen sisällöstä. Hyvin aseteltu kysymys auttaa pitämään tutkimuksen kasassa ja ehkäisee liiallista rönsyilyä. Kun tutkimuksessa on vain yksi oleellinen kysymys, on mahdollista keskittyä vain yhteen oleelliseen asiaan. Mikäli kysymyksiä on useampia, niiden täytyy olla sidoksissa toisiinsa, jotta vältyn liian irrationaalisista tutkimuksen kohteista. Oma kontribuutio voi näkyä esimerkiksi onnistuneena systematisoimisena.

Kolehmaisen mukaan tutkimusmenetelmän eli metodin on oltava sellainen, että sen avulla saadaan selville jotain merkittävää ja mielenkiintoista. Lainopillisessa kirjoittamisessa on tärkeää dokumentoida tutkimusaineisto ja tutkijalta vaaditaan huolellisuutta lähdeaineistojen lainaamisessa. Tutkiessaan aihetta on kirjoittajan oltava objektiivinen, looginen ja noudatettava rehellisyyden periaatetta. Tutkija ei voi esittää totena sitä, mikä on epätosi ja pätemätön.

Oikeuslähteet jaan myös ns. ”aarniolaisen” ajattelun mukaisesti vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin. Vahvasti velvoittavia ovat kansallisen oikeuden normistot (Suomen perustuslaki, perusoikeudet, lait sekä lakien nojalla annetut alemman tasoiset normit) ja tavanomainen oikeus sekä kansallisen oikeuden ulkopuoliset normisto, joita ovat eurooppaoikeuden sitovat osat.

Heikosti velvoittavia oikeuslähteitä ovat lainvalmisteluaineisto ja tuomioistuinratkaisut, joilla on ennakkotapausarvoa. Sallittuja oikeuslähteitä ovat esimerkiksi lainoppi, vertailevat argumentit, yleiset oikeusperiaatteet, eettiset ja moraaliset perusteet sekä käytännölliset argumentit. Eurooppalainen oikeus vaikuttaa nykyisin entistä enemmän suomalaiseen laintulkintaan, koska eurooppaoikeudella on etusija kansalliseen lainsäädäntöön nähden.

Oikeuslähteinä tässä opinnäytetyössä käytän myös lainvalmisteluun kuuluvia perusselvityksiä, kuten komiteamietintöjä, oikeusministeriön lainvalmisteluosaston julkaisuja, ministeriöiden ja erilaisten työryhmien raportteja ja asiantuntijaselvityk-

siä. Eduskunnan ja valtioneuvoston asiakirjat, kuten valiokuntien mietinnöt ja hallitukset esitykset ovat edellisiä merkityksellisempiä. Nämä asiakirjat ja mietinnöt ovat sitä merkityksellisempiä mitä lähempänä ne ovat lopullista lainvalmistelua.

Lainopillisessa tutkimuksessa järjestystä luon systematisoinnilla. Tällöin oikeusnormit esitän jäsentyneenä jonkin valitun perusteen mukaisesti. Lainopillisissa opinnäytetöissä systematisointi liittyy käytännössä opinnäytetyön rakenteeseen. Tässä työssä ensiksi käsittelen yleiset asiat, jonka jälkeen paneudun yksityiskohtaiseen ja tarkkaan tietoon. Tarkoituksena on myös, että tutkielma etenee loogisesti ja etenemisjärjestys palvelee lukijaa. Työ on järkevää jäsentää sisällöllisin perustein, eikä pelkästään lakipykälien mukaan, koska tällöin saan lukijaystävällisemmän kokonaisuuden.

Tässä opinnäytetyössä käytän oikeuslähteitä, joista henkilötietolaki ja Euroopan unionin yleinen tietosuoja-asetus kuuluvat vahvasti velvoittaviin oikeuslähteisiin. Vahvasti velvoittaviin oikeuslähteisiin liittyy virkavirhesanktio, mikäli näitä oikeuslähteitä jätetään soveltamatta ensisijaisesti ratkaisuja tehtäessä. Velvoittavissa oikeuslähteissä tekstin sisältö on kuitenkin hyvin monimutkaisesti ja epäselvästi ilmaistu, joten niiden lisäksi joutuu käyttämään myös heikosti velvoittavia oikeuslähteitä. Heikosti velvoittavissa oikeuslähteissä on selitetty lainsäätäjien tarkoitus ja avattu lakitekstiä ymmärrettävään muotoon.

Tässä tutkimuksessa heikosti velvoittavia oikeuslähteitä ovat WP29-tietosuojatyöryhmän ohjeet yleisen tietosuoja-asetuksen soveltamisesta käytäntöön ja EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Näistä heikosti velvoittavista oikeuslähteistä poikkeaminen ei aiheuta virkavirhesanktioita, mutta niiden huomioimatta jättämien tulee perustella päätöksenteossa. Lisäksi käytän sallittuja oikeuslähteitä, joita ovat muun muassa tietosuojavaltuutetun toimiston ohjeet ja Andreasson, Riikonen ja Ylipartasen kirjoittamat kirjat *Tietosuojavastaavan käsikirja* (2014) ja *Osaava tietosuojavastaava* (2017).

Oikeuslähteiden käytön systematisoinnissa käsittelen ensin EU:n yleisen tietosuoja-asetuksen artikloita, jotka ovat tässä opinnäytetyössä yleisiä asioita. Tä-

män jälkeen siirryn käsittelemään yksityiskohtaisempia tietoja. Näihin yksityiskohtaisiin tietolähteisiin kuuluvat tässä opinnäytetyössä WP29-tietosuojatyöryhmän ohjeet ja TATTI-työryhmän mietintö.

3 Lainsäädäntö

Tässä luvussa käsittelen lainsäädäntöä, joka liittyy tietosuojavastaavan asemaan yleisen tietosuoja-asetuksen näkökulmasta ja sen laatimisprosessia sekä sen tulkintoja. Lisäksi selvitän, mitä Suomessa on tehty yleisen tietosuoja-asetuksen voimaan saattamiseksi. Lähemmin tarkasteltavaa lainsäädäntöä ovat henkilötietolaki, Euroopan unionin yleinen tietosuoja-asetus, WP29-tietosuojatyöryhmän ohjeet ja TATTI-työryhmän mietintö.

3.1 Henkilötietolaki

Tällä hetkellä Suomessa tietosuojan yleissääntely perustuu henkilötietolakiin (523/1999). Tämän lisäksi henkilötietojen käsittelyä sääntelevät lukuisat kansalliset erityislait. (Andreasson, Koivisto & Ylipartanen 2014, 17.) Henkilötietolailla saatettiin voimassa ollut tietosuojan yleislainsäädäntö vastaamaan EU:n henkilötietodirektiiviä ja muita kansainvälisiä velvoitteita (Andreasson ym. 2016).

Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista (Henkilötietolaki 523/1999). Mikäli jollain erityislailla on säädetty samasta yksityiskohdasta ja asiasta kuin henkilötietolaissa, niin henkilötietolaki väistyy toissijaisuutensa perusteella.

Henkilötietolain 2 §:ssä määritellään lain soveltamisesta, ja sen mukaan lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Myös muuhun henkilötietojen käsittelyyn sovelletaan tätä lakia silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. Henkilötietolaki ei koske henkilötietojen käsittelyä, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiinsa.

Koska Euroopan unionin tietosuoja-asetus on pakottavaa lainsäädäntöä, ei kansallinen lainsäädäntö voi olla ristiriidassa sen kanssa. Ristiriitaisuuksien poistamiseksi Suomen lainsäädäntöä joudutaan tarkistamaan asetuksen mukaiseksi. Yhtenä mahdollisuutena on uuden lainsäädännön laatiminen, jossa otetaan huomioon muutokset nykyiseen lainsäädäntöön. *Tietosuojauudistuksen valmistelu on jaettu kahdelle eri oikeusministeriön työryhmälle: toinen käsittelee tietosuojadirektiivin ja toinen tietosuoja-asetuksen vaikutuksia lainsäädäntöön* (Eduskunta 2017).

Aikaisemmin tietosuojavastaava on pitänyt nimetä sosiaali- ja terveysalalle. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (9.2.2007/159) määrittelee 6. luvun 20 §:n 5 momentissa tietosuojavastaavasta seuraavaa: *Lisäksi jokaisella palvelujen antajalla ja Kansaneläkelaitoksessa on oltava seuranta ja valvontatehtävää varten tietosuojavastaava (28.3.2014/250).* EU:n tietosuoja-asetus velvoittaa nyt julkista hallintoa ja muitakin yrityksiä, tietyin ehdoin, nimeämään tietosuojavastaavan.

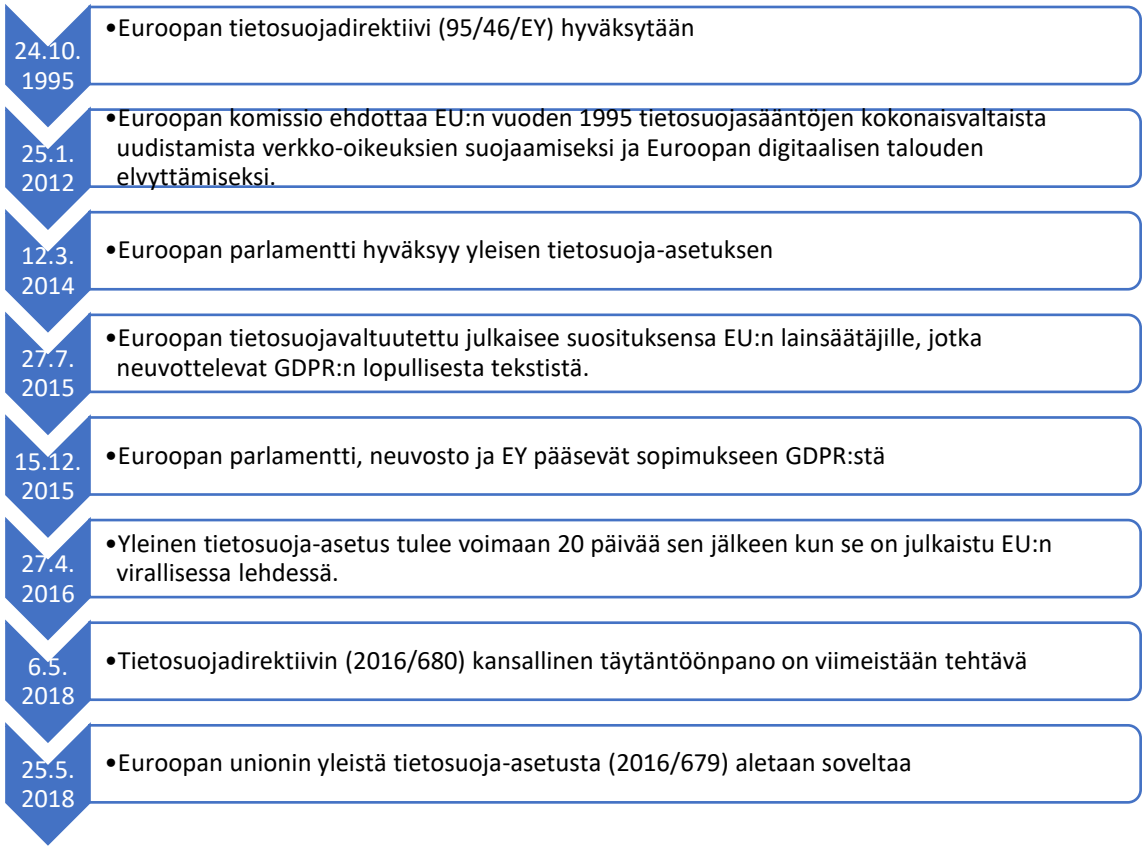
3.2 Euroopan unionin yleinen tietosuoja-asetus

Euroopan parlamentti ja neuvosto antoivat keväällä 2016 asetuksen luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta eli Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679). Yleinen tietosuoja-asetus tulee 25.5.2018 lähtien suoraan sovellettavaksi kaikissa EU:n jäsenmaissa.

Tietosuojadirektiivi korvaa vuonna 2008 annetun puitepäätöksen rikosasioissa tehtävissä sekä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta. Yleinen tietosuoja-asetus korvaa vuoden 1995 henkilötietodirektiivin 95/46/EY ja sen kansalliseksi täytäntöön panemiseksi annetun henkilötietolain (523/1999) säännökset niiltä osin kuin henkilötietojen käsittely kuuluu asetuksen soveltamisalaan. (Eduskunta 2017.)

EU:n tietosuojalainsäädännön uudistaminen on varsinaisesti lähtenyt liikkeelle vuonna 2012, jolloin todettiin, että EU:n tiesuojalainsäädäntö oli jäänyt jälkeen kehityksestä. Uudistuksen tavoitteena oli turvata henkilötietojen suoja perusoikeutena ja digitaalitalouden kehitys. (Eduskunta 2017.)

Viimeisten vuosikymmenien aikana teknologia on kehittynyt ja muuttanut elämää niin nopeasti ja sellaisilla tavoilla, joita ei kukaan olisi voinut kuvitellakaan parikymmentä vuotta sitten. Tämän vuoksi tietosuojasäännöksiä oli tarpeen uudistaa ja muuttaa nykyistä teknologian aikakautta vastaavaksi. Kuvassa 1 on mukailtu aikajana Euroopan tietosuojavaltuutetun julkaisemasta EU:n yleisen tietosuoja-asetuksen (GDPR) kehityksestä.



Kuva 1. EU:n yleisen tietosuoja-asetuksen kehitys

Vaikka kyseessä on kansallisesti suoraan sovellettava asetus, se jättää jäsenvaltiolle direktiivinomaista kansallista liikkumavaraa. Tätä liikkumavaraa on erityisesti julkisella sektorilla mutta jossain määrin myös yksityisellä sektorilla. Asetuksen puitteissa on mahdollista antaa kansallista lainsäädäntöä, jolla tarkennetaan asetuksen säännöksiä. Lisäksi kansallisella lainsäädännöllä on jossain määrin mahdollista myös poiketa asetuksen velvoitteista. Alustavan arvion mukaan useassa sadassa kansallisessa säädöksessä on nykyisin säännöksiä henkilötietojen

käsittelystä. Nämä eri ministeriöiden hallinnonaloille kuuluvat säännökset on saatettava tietosuoja-asetuksen mukaisiksi asetuksen mahdollistaman kansallisen liikkumavaran puitteissa. (Oikeusministeriö, OM1/41/2016.)

3.3 TATTI-työryhmä

Yleisen tietosuoja-asetuksen voimaan tulon seurauksena Oikeusministeriö asetti 17.2.2016 TATTI-työryhmän selvittämään Euroopan unionin yleisen tietosuoja-asetuksen edellyttämien kansallisten lainsäädäntö-toimenpiteiden tarvetta ja valmistelemaan yleisen tietosuoja-asetuksen edellyttämiä muutoksia henkilötietojen käsittelystä annettuun yleiseen kansalliseen lainsäädäntöön sekä koordinoimaan asiasta annetun erityislainsäädännön tarkistamiseksi tarpeellista lainvalmistelutyötä. Työryhmän toimikaudeksi määriteltiin 17.2.2016–16.2.2018. (Oikeusministeriö, OM1/41/2016.)

Työryhmä sai mietintönsä valmiiksi kesäkuussa 2017 ja on luovuttanut sen oikeusministerille hallituksen esitystä varten. TATTI-työryhmä jatkaa kuitenkin vielä työskentelyään erityislakien säännösten parissa ja mahdollisesti esittää tarvittavia muutoksia kyseisiin lakeihin henkilötietojen käsittelyyn liittyen. Syksyllä oikeusministeriö järjesti lausuntokierroksen työryhmän mietinnön pohjalta. Tämän jälkeen hallitus antaa esityksensä eduskunnalle mahdollisesta uudesta tietosuojalaista.

Hallituksen oli tarkoitus antaa asiasta esitys eduskunnalle syksyn 2017 aikana. Tiedustellessani sähköpostitse oikeusministeriöltä lainvalmistelun tämän hetkisestä tilanteesta sain oikeusministeriön viestintäyksiköltä vastauksen, jossa kerrottiin, että hallituksen esitys tämänhetkisen arvion mukaan voitaisiin todennäköisesti antaa alkuvuodesta 2018. (Oikeusministeriön viestintäosasto 2017.)

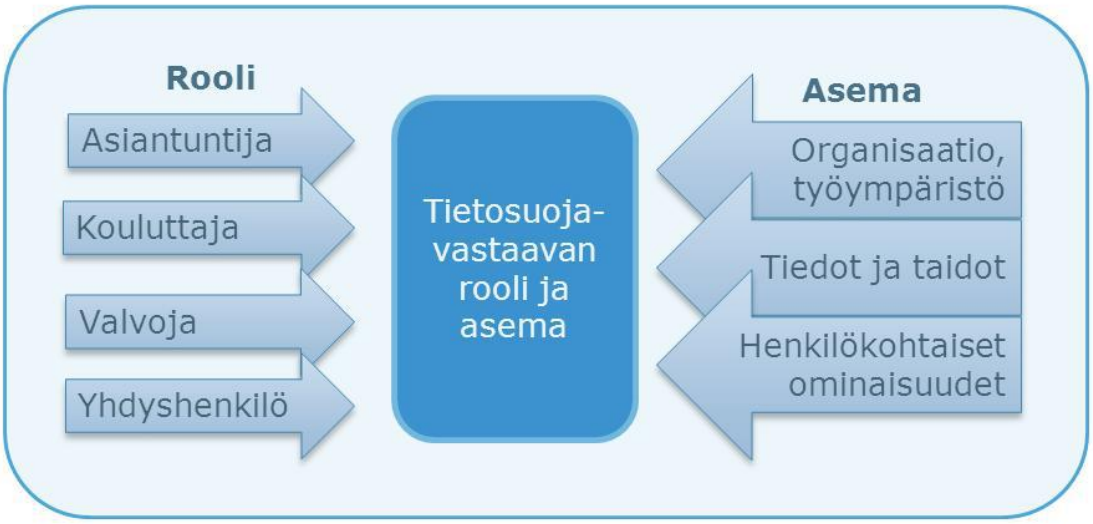
4 Tietosuojavastaava

Tässä luvussa käsitellään tietosuojavastaavan asemaa, nimittämistä ja hänen tehtäviään yleisen tietosuoja-asetuksen mukaan ja ne ovat tutkimuksen pääasiallisena kohteena. Tietosuojavastaavan nimittämistä, asemaa ja tehtäviä on käsitelty yleisen tietosuoja-asetuksen artikloissa 37, 38 ja 39. Samassa yhteydessä

käsittelen myös tietosuojavastaavan asemaan liittyviä WP29-tietosuojatyöryhmän ohjeistusta ja TATTI-työryhmän selvitystä oikeusministeriölle.

Tietosuojavastaava on keskeinen osa Euroopan unionin yleistä tietosuoja-asetusta. Tietosuojavastaava on asiantuntija, joka toimii rekisterinpitäjän tai henkilötietojen käsittelijän tukena tietosuoja-asioissa. Vaikkakin tietosuojavastaava avustaa henkilötietojen käsittelyssä ja muidenkin tietosuojakäytäntöjen laadinnassa, suunnittelussa, valvonnassa ja toimeenpanossa, hän ei ole itse suoranaisesti vastuussa tietosuojan lainmukaisuudesta. Vastuu on kaikesta rekisterinpitäjällä eli organisaation johdolla. Tietosuojavastaavalla tulee olla valmiudet hoitaa tehtäviään sekä organisaation puolesta että henkilökohtaisilta ominaisuuksiltaan. (EU 2016/679.)

Osaava tietosuojavastaava (2017) kirjassaan ovat Andreasson, Riikonen ja Ylipartanen käyttäneet Maija Vilpposen pro gradu -tutkielmassa Tietosuojavastaavan rooli ja asema sosiaali- ja terveydenhuollossa (2012) olevaa mallia kuvaamaan tietosuojavastaavan roolia ja asemaa. Kuvassa 2 on esitetty nämä roolin ja aseman muodostumiseen vaikuttavat tekijät.



Kuva 2. Roolin ja aseman muodostumiseen vaikuttavia tekijöitä. (Andreasson ym. 2017,92.)

Kuvan perusteella rooli vastaa tietosuojavastaavan pääasiallista tehtävänkuvaa, jossa tietosuojavastaava on asiantuntijan, kouluttajan ja valvojan tehtävissä sekä

toimii yhteyshenkilönä tarkastusviranomaisiin, työntekijöihin, yrityksen johtoon sekä rekisteröityihin. Asemaan, johon tietosuojavastaava asettuu organisaatiossa ja työympäristössä, vaikuttaa hyvin pitkälti tietosuojavastaavan henkilökohtaiset ominaisuudet ja hänen tietonsa ja taitonsa tehtävään nähden. Hyvät suhteet rekisterinpitäjään ja oma-aloitteisuus ovat tärkeitä ominaisuuksia, jotta tietosuojavastaavan asemasta muodostuu merkittävä osa organisaation tietosuojakulttuuria.

Tietosuoja-asetuksessa on paljon tietosuojavastaavaan liittyviä määritelmiä, joita ei määritellä suoraan asetuksessa, joten osassa määritelmiä joudutaan käyttämään kansallista määritelmää. EU-tasolla toimiva EU:n asiantuntijaryhmä WP 29 (Article 29 Working Party) on antanut tarkempaa ohjeistusta tietosuojavastaavan nimittämisestä, asemasta, tehtävistä ja tietosuoja-asetuksen määritelmistä, jotka liittyvät tietosuojavastaavaan. WP29-asiantuntijatyöryhmä on työryhmä, joka on perustettu direktiivin 95/46/EY 29 artiklalla. Se on riippumaton EU:n neuvoa-antava elin, joka käsittelee tietosuojaan ja yksityisyyden suojaan liittyviä kysymyksiä. Työryhmä on myös julkaissut soveltamisohjeita liittyen tietosuojavastaavan nimittämiseen, asemaan ja tehtäviin. Näitä soveltamisohjeita käytän avaamaan artikloiden sisältöä tarkemmin, jotta kyseiset artiklat avautuisivat paremmin sekä tietosuojavastaavalle, että organisaation johdolle. (Tietosuojatyöryhmä 2016.)

4.1 Tietosuojavastaavan nimittäminen

Yleisen tietosuoja-asetuksen artiklan 37 mukaan jokaisen viranomaisen ja julkishallinnon elimen, joka ei ole tuomioistuin, on nimitettävä tietosuojavastaava. Julkissektorin toimijoiden lisäksi myös muiden organisaatioiden on nimettävä tietosuojavastaava, jos niiden ydintehtävät muodostuvat henkilötietojen käsittelystä, joka edellyttää laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai joiden ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomiota tai rikkomuksia koskeviin tietoihin ovat velvollisia nimittämään tietosuojavastaavia.

Tietosuojavastaava voi olla organisaation henkilöstön jäsen tai hoitaa tehtäviään palvelusopimuksen perusteella. Myös yhteisen tietosuojavastaavan nimittäminen

eri yritysten välille on mahdollista, mutta se ei saa aiheuttaa intressiristiriitoja. Nimitettäessä tietosuojavastaavaa tulee ottaa huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä sekä valmiudet suorittaa artiklassa 39 tarkoitetut tehtävät. Nimettyjen tietosuojavastaavien yhteystiedot on julkistettava ja ilmoitettava ne valvontaviranomaiselle.

Edellä luetellut tapaukset kuuluvat pakollisiin tehtäviin tietosuojavastaavan nimittämisessä. Vaikka organisaation ei tarvitsisi pakollisten säännösten perusteella nimittää tietosuojavastaavaa, on se joissakin tapauksissa kuitenkin suositeltavaa. Rajatapauksien ollessa kyseessä on suositeltavaa, että organisaatio nimittää tietosuojavastaavan tai organisaatio dokumentoi sisäisen analyysin, josta selviää, että olennaiset tekijät on otettu huomioon kartoitettaessa tietosuojavastaavan nimittämistä.

Tietosuojavastaavan voi nimittää rekisterinpitäjä tai henkilötietojen käsittelijä tai molemmat yhdessä. Mikäli molempien toimijoiden on nimettävä tietosuojavastaava, niin heidän olisi hyvä tehdä asiassa yhteistyötä. Jos pakolliset kriteerit täyttyvät vain toisella, jonka on nimettävä tietosuojavastaava, olisi hyvän käytännön mukaista myös toisen toimijan nimetä tietosuojavastaava vapaaehtoisesti. (Tietosuojatyöryhmä 2016,10-11.)

Konserniin voidaan nimittää vain yksi tietosuojavastaava, mutta on otettava huomioon, että tietosuojavastaavan on oltava helposti tavoitettavissa jokaisesta työpaikasta. Koska tietosuojavastaava toimii yhteyshenkilönä tietosuojaviranomaisiin, rekisteröityihin ja yrityksen sisäisenä yhteyshenkilönä on tärkeää, että hänen yhteystietonsa ovat helposti kaikkien saatavilla ja häneen on helppo olla yhteydessä.

Tietosuojavastaavan ei tarvitse olla yrityksen henkilöstöä, mutta se helpottaisi tietosuojavastaavan toimintaa, mikäli yritys olisi jo tuttu tietosuojavastaavalle. Tietosuojavastaava voidaan nimittää yrityksen rekrytoinnin avulla tai ostaa palvelut tietosuojavastaavan palveluja tarjoavilta konsulteilta. Mikäli palvelu ostetaan ulkopuoliselta, on erittäin tärkeää määritellä, mitkä ovat tietosuojavastaavan tehtävät, asema ja tehtävänimike. Samoin, jos yritys nimeää vapaaehtoisesti tie-

tosuojavastaavan, sovelletaan nimittämiseen, asemaan ja tehtäviin samoja vaatimuksia, kuin jos se olisi ollut pakollista. Mikäli yritykseen palkataan henkilö tai ulkopuolinen konsultti, joka hoitaa henkilötietojen suojaa koskevia tehtäviä, täytyy hänen tehtävänimikkeensä olla selkeä, jotta sitä ei sekoiteta varsinaiseen tietosuojavastaavaan. (Tietosuojatyöryhmä 2016, 7)

Artiklassa 37 mainitut viranomaiset ja julkishallinnon elimet käsite on määriteltävä kansallisen lainsäädännön perusteella (Tietosuojatyöryhmä 2016,7). Kansallisella määritelmällä voidaan käsittää viranomaiset ja julkishallinnon elimet myös muina kuin pelkkinä viranomaisina. Julkishallinnon eliminä voidaan pitää myös yksityisluontoisia organisaatioita, jotka käyttävät julkista valtaa eikä rekisteröidyllä ole mahdollisuuksia vaikuttaa siihen, miten heidän tietojaan käsitellään.

4.1.1 Ydintehtävät

Artiklassa 37 puhutaan rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävistä. Tällaisina ydintehtävinä voidaan pitää sellaista keskeistä toimintaa, johon liittyy organisaation ensisijaisiin toimintoihin kerätä henkilötietoja ja seurata rekisteröityjen kulutustottumuksia. Useassa lähteessä, esimerkiksi WP29-työryhmän ohjeessa, Osaava tietosuojavastaava -kirjassa ja tietosuojavaltuutetun sivuilla on mainittu sairaala esimerkkinä siitä, että vaikka sen ydintehtävä ei olekaan henkilötietojen käsittely vaan terveydenhoito, niin sen on nimitettävä tietosuojavastaava, tietojen arkaluonteisuuden vuoksi.

Melkein kaikki yritykset käsittelevät jollain tavalla henkilötietoja oheis- tai tukitoimintoinaan, mutta mikäli ne eivät ole yrityksen ydintehtäviä vaan välttämättömiä liiketoiminnan pyörittämiseen, ei heidän tarvitse nimittää tietosuojavastaavaa. Tällaiseksi välttämättömäksi toiminnoksi voidaan nimetä yrityksessä muun muassa palkanlaskenta, jolloin joudutaan keräämään tietoa palkansaajista, jotta heidät voidaan yksilöidä palkanmaksua varten. Mutta mikäli kyse on laaja-alaisesta toiminnasta, tietosuojavastaavan nimeäminen on pakollista. (Tietosuojatyöryhmä 2016,22.)

4.1.2 Laajamittainen, säännöllinen ja järjestelmällinen seuranta

Asetuksessa ei määritellä suoraan, mitä on laajamittainen käsittely. Laajamittaisella käsittelyllä voidaan käsittää suurta joukkoa rekisteröityjä ja heidän tietojaan, joilla on vaikutusta laajemmalla alueella. Tietosuojatyöryhmä (WP29) on antanut ohjeistuksessaan suosituksia siitä, mitä laajamittaista tietojenkäsittelyä määriteltäessä olisi otettava huomioon. Työryhmän mielestä pitäisi tarkastella rekisteröityjen lukumäärää, tietomäärää, käsittelytoiminnan kestoa ja pysyvyyttä sekä käsittelyn maantieteellistä laajuutta. Laajamittainen ei kuitenkaan tarkoita organisaation kokoa vaan henkilötietojen määrä, jota organisaatiossa käsitellään. (Tietosuojatyöryhmä 2016,23.) Asetuksen väliehdotuksessa oli rajattu tarkasti työntekijöiden määrä 250 tai rekisteritietojen määrä yli 5000 nimeä, mutta lopullisessa tietosuoja-asetuksessa näitä määriä ei ole rajattu. Koska tarkkoja määriä ja käsittelyn kestoa ei ole suoraan annettu, käytäntö tulee todennäköisesti määrittelemään kyseiset rajat.

Säännöllistä ja järjestelmällistä seurantaakaan ei ole määritelty asetuksessa, mutta asetuksen johdanto-osassa (kappale 24) on mainittu rekisteröityjen käyttäytymisen seuranta. (Tietosuojatyöryhmä 2016,9.) Yleisen tietosuoja-asetuksen kappaleessa 24 on seuraamisesta määritelty:

Jotta voidaan määrittää, voidaanko käsittelytoiminta katsoa rekisteröityjen käyttäytymisen seuraamisena, olisi varmistettava, seurataanko luonnollisia henkilöitä internetissä, mukaan lukien sellaisten henkilötietojen käsittelytekniikoiden mahdollinen myöhempi käyttö, jotka käsittävät tietyn yksilön profiloinnin erityisesti häntä koskevien päätösten tekemistä varten tai hänen henkilökohtaisten mieltymystensä, käyttäytymisensä ja asenteidensa analysointia tai ennakoimista varten.

Säännöllisellä seurannalla työryhmän mukaan tarkoitetaan jatkuvaa tai ajoittaista toimintaa tai että toiminta toistuu tietyin väliajoin tai määritettyinä aikoina. Toiminta voi olla järjestelmällistä, jos se on ennalta järjestettyä, organisoitua ja menetelmällistä. Mikäli kyseessä on osa yleistä tiedonkeruusuunnitelma, toimintaa voidaan pitää järjestelmällisenä. Samoin kuin laajamittaisuuden määritelmässä, niin säännöllinen ja järjestelmällinen seuranta tulevat muotoutumaan ajan kuluessa ja todennäköisesti määritelmät tulevat vielä tarkentumaan käytännön kautta. (Tietosuojatyöryhmä 2016,24.)

4.1.3 Asiantuntemus ja ammattipätevyys

Asiantuntemuksen ja ammattipätevyyden määrittämisen täytyy olla suhteutettuna organisaation käsittelemien tietojen määrään ja laatuun. Mitä laajemmasta ja suuremmasta tiemäärästä on kyse, sitä ammattitaitoisempi tietosuojavastaavan on oltava. Vaikka ammattipätevyyttä ei suoraan määritellä asetuksessa on olennaista, että tietosuojavastaava on perehtynyt kansallisiin ja EU:n tietosuojalainsäädäntöihin sekä tuntee yleisen tietosuoja-asetuksen perusteellisesti. Tietosuojavastaavalla olisi hyvä olla tietoa toimialasta, jolla hän toimii, sekä organisaation hallinnollisista käytännöistä ja menetelmistä. Hänellä tulee olla myös valmiudet edistää tietosuojakulttuuria organisaatiossa. (Tietosuojatyöryhmä 2016,13.)

4.1.4 Valmiudet tehtävän hoitamiseen

Valmiuksiin hoitaa tietosuojavastaavan tehtävä voidaan lukea henkilökohtaiset ominaisuudet sekä että oman aseman tiedostaminen organisaatiossa. Henkilökohtaisia ominaisuuksia ovat ennen kaikkea rehellisyys ja korkea ammattietiikka. Tietosuojavastaavan tulee olla esimerkkinä tietosuoja-asetuksen noudattamisesta ja tietosuojan edistämisestä yrityksessä. Koska hänen tehtäviinsä kuuluu tietosuoja-asetuksen noudattamisen seuraaminen, on hänen oltava erityisen hyvin perillä organisaation tietosuojakäytänteistä, rekisteröityjen oikeuksista, käsittelyn turvallisuudesta ja tietoturvaloukkausten ilmoittamisesta. (Tietosuojatyöryhmä 2017,13.)

4.1.5 TATTI-työryhmän esitys nimittämiseen

Koska artikla 37 antaa mahdollisuuden kansalliseen liikkumavaraan niin, että jäsenvaltio voi edellyttää tietosuojavastaavan nimittämistä myös muissa kuin pakollisissa tilanteissa, TATTI-työryhmä esittää, että asiasta voitaisiin säätää kansallisella erityislailla. (Oikeusministeriö. 35/2017.) Kyseinen erityislaki olisi Tietosuoja-asetuksen yhteydessä voimaan tuleva uusi kansallinen tietosuojalaki. Kansallista poikkeamaa voitaisiin käyttää esimerkiksi vakuutusyhtiöiden osalta suojatoimena.

Velvollisuus tietosuojavastaavan nimeämiseen koskisi vain rajatusti henkilötietoja 85 artiklassa tarkoitetuissa tilanteissa käsitteleviä tahoja. Näitä tahoja artiklan

85 mukaan ovat tahot, jotka ovat journalistisia tarkoituksia ja akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten. Mikäli kansallisesti halutaan tehdä muutoksia näihin säännöksiin ja jos ne ovat tarpeen henkilötietojen suojaa koskevan oikeuden sovittamiseksi yhteen sananvapauden ja tiedonvälityksen kanssa, on niistä tehdyt säännökset ilmoitettava komissiolle mahdollisimman pian. Työryhmän mukaan tätä velvollisuutta ei rajattaisi entisestään. (Oikeusministeriö. 35/2017,162.)

Työryhmän esityksessä asia ilmaistaan seuraavasti; *Tietosuojalailla ehdotetaan kuitenkin merkittäviä rajauksia rekisteröidyn oikeuksiin käsiteltäessä henkilötietoja journalistissa tarkoituksissa. Sitä vastoin tietoturvaa koskevista säännöksistä ei ehdoteta poikettavan tietosuojalailla. Siten 37 artiklan mukainen velvollisuus tietosuojavastaavan nimeämiseen tulisi sovellettavaksi käsiteltäessä henkilötietotoja 85 artiklassa tarkoitetuissa tilanteissa.* (Oikeusministeriö. 35/2017,162.)

4.2 Tietosuojavastaavan asema

Yleisen tietosuoja-asetuksen artiklassa 38 on säädetty tietosuojavastaavan asemasta organisaatiossa. Artiklan mukaan tietosuojavastaavan on oltava riippumaton eikä hän saa ottaa vastaan ohjeita tehtäviensä hoitamisen yhteydessä. Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle. Organisaation on otettava tietosuojavastaava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn ja hänelle on asetuksen mukaan annettava riittävät resurssit tehtävien hoitamiseen sekä pääsy henkilötietoihin ja käsittelytoimiin.

4.2.1 Osallistuminen henkilötietojen käsittelyyn

Organisaation johdon tulisi jo alusta alkaen ottaa tietosuojavastaava mukaan johdon kokouksiin, jossa käsitellään organisaation tietosuojakäytäntöjä ja henkilötietojen käsittelyn periaatteita. Häneltä pitäisi kysyä neuvoja ja ohjeistusta tietosuoja-asioiden käsittelyssä ja hänelle pitää toimittaa olennaiset tiedot tietosuojakäytännöistä, jotta hän osaa antaa riittävät ja asianmukaiset neuvot asiaa koskien. Tietosuojatyöryhmä WP29 suosittelee, että erimielisyystilanteissa dokumentoidaan perusteet, mikäli tietosuojavastaavan neuvoja ja ohjeistusta ei noudateta. Tietoturvaloukkausten tapahtuessa organisaatiossa olisi hyvä olla ohjeistus siitä missä tilanteessa otetaan yhteyttä tietosuojavastaavaan. Pääsääntöisesti tällaisissa tapauksissa yhteyttä pitäisi ottaa aina tietosuojavastaavaan, jolla

on todennäköisesti paras tietämys siitä, miten toimitaan kyseisessä tilanteessa. (Tietosuojatyöryhmä 2016,15.)

4.2.2 Tarvittavat resurssit

Organisaatiosta ja henkilötietojen käsittelyn luonteesta riippuen täytyisi tietosuojavastaavalle on järjestää riittävät ja tarvittavat resurssit, jotta hän pystyy hoitamaan tehtävänsä moitteettomasti. Yksi tärkeimmistä resursseista on, että ylempi johto tukee tietosuojavastaavaa hänen tehtävissään. Tietosuojavastaavalle on annettava mahdollisuus päästä käsiksi henkilötietosuojaa koskeviin aineistoihin, jotta hän voisi hoitaa tehtävänsä moitteettomasti. Kuitenkin tärkein tarvittava resurssi on aika: tietosuojavastaavalla täytyy olla riittävästi aikaa työtehtäviensä hoitamiseen. Etenkin jos tietosuojavastaavan tehtäviin kuuluu muutakin kuin vain tietosuojavastaavan tehtävät, on organisaation järjestettävä resurssit niin, että tietosuojavastaava pystyy tekemään hänelle määritellyt tehtävät. (Tietosuojatyöryhmä 2016,16.)

Budjetointivaiheessa on organisaation huomioitava asianomaiset tilat ja työvälineet tietosuojavastaavalle. Tarvittaviin resursseihin kuuluvat myös tietosuojavastaavan kouluttautumismahdollisuudet, etenkin jos kyseessä on juuri aloittanut tietosuojavastaava. Kouluttautumisen avulla tietosuojavastaava kestää ajan tasalla tehtäviensä hoitamisessa alati muuttuvassa tietosuojaympäristössä. Organisaation on myös virallisesti ilmoitettava henkilöstölle tietosuojavastaavan nimeämisestä, jotta henkilöstö on tietoinen tietosuojavastaavan olemassa olosta organisaatiossa. (Tietosuojatyöryhmä 2016,16.)

4.2.3 Riippumattomuus

Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa antaa ohjeita siihen, kuinka tietosuojavastaavan on tehtäviään hoidettava ja mitä tietoja hän käsittelee ja millä tavalla. Mikäli tietosuojavastaavalla on muitakin tehtäviä tietosuojavastaavan tehtävän lisäksi, ne eivät saa olla ristiriidassa keskenään. (Tietosuojatyöryhmä 2016,17.)

Tietosuojalainsäädännön noudattamisesta vastaa rekisterinpitäjä tai henkilötietojen käsittelijä, mutta mikäli he tekevät päätöksiä, jotka eivät ole asetuksen tai tietosuojavastaavan ohjeiden mukaisia, on tietosuojavastaavalle annettava mahdollisuus esittää ylimmälle johdolle mielipiteensä (Tietosuojatyöryhmä 2016,17). Vuosikertomuksen laatiminen ylimmälle johdolle varmistaa sen, että he tietävät tietosuojavastaavan antamista neuvoista ja ohjeista rekisterinpitäjälle tai henkilötietojen käsittelijälle (Tietosuojatyöryhmä 2016,26).

4.2.4 Erottaminen tai rankaiseminen

Tietosuojavastaavaan ei saa erottaa tai rankaista siitä, että hän suorittaa tehtäviään hänelle määrätyllä tavalla. Tämä antaa tietosuojavastaavalle mahdollisuuden suorittaa tehtäviään itsenäisesti ja riippumattomasti. Tietosuojavastaavaa ei saa rangaista siitä, että hän esittää eriäviä mielipiteitä tai antaa ohjeita, joita rekisterinpitäjä tai henkilötietojen käsittelijä eivät halua noudattaa. Erottaminen ja rankaiseminen voi kuitenkin tulla kysymykseen, mikäli kyse ei ole työtehtävien hoitamisesta. Tällainen voi olla muun muassa seksuaalinen häirintä tai muu vakava rikkomus. (Tietosuojatyöryhmä 2016,18.) On kuitenkin huomattava, että tietosuoja-asetuksessa ei tarkkaan määritellä, milloin tietosuojavastaava voidaan erottaa. Tietosuojatyöryhmä kannustaakin tietosuojavastaavia tekemään pysyviä sopimuksia, jotta epäselviin erottamistilanteisiin ei jouduttaisi.

4.2.5 Eturistiriidat

Eturistiriidat ja riippumattomuus liittyvät hyvin läheisesti toisiinsa. Organisaation rakenteesta riippuen eturistiriidat on käsiteltävä tapauskohtaisesti. Yleisesti ottaen eturistiriita voi syntyä siitä, jos tietosuojavastaavaksi nimetään yrityksen johtoa, tietoturvapäällikköä tai muita, joiden tehtäviin kuuluu tietosuojaperiaatteiden määrittely organisaatiossa. WP29-työryhmän mukaan eturistiriitatilanne syntyy myös silloin, jos tietosuojavastaavan edustaa rekisterinpitäjää tai henkilötietojen käsittelijää esimerkiksi tuomioistuimessa. (Tietosuojatyöryhmä 2016,18.)

Organisaatioiden koosta riippuen olisi hyvä määritellä ne tehtävät, jotka eivät sovi tietosuojavastaavalle eturistiriita tilanteiden takia. Lisäksi olisi määritellä sään-

nöstö sille, mitä ovat eturistiriita tilanteita ja kuinka niitä vältetään. Hyvänä keinona eturistiriitojen välttämiseksi olisi määritellä tarkkaan tietosuojavastaavan palvelusopimus tai työsopimus tehtävänkuvineen ennen sopimusten tekemistä.

4.2.6 TATTI-työryhmän esitys tietosuojavastaavan asemasta

Yleinen tietosuoja-asetus antaa kansallista liikkumavaraa tietosuojavastaavan asemaa koskien. TATTI-työryhmä mietinnössään ehdottaakin tämän vuoksi, että uuteen Tietosuojalakiin säädettäisiin henkilötietolain 33 §:ä vastaava rekisterinpitäjän, henkilötietojen käsittelijän ja tietosuojavastaavan tms. vaitiolovelvollisuutta koskeva säännös. Nykyisen henkilötietolain 33 §:n mukaan, mikäli henkilötietojen käsittelijä on saanut tietoonsa jotain toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, ei hän saa ilmaista tietojaan sivulliselle. Tietosuojavastaavaa sitoo hänen tehtäviensä suorittamista koskeva salassapitovelvollisuus unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti.

Työryhmän mietinnön mukaan artiklan 38 soveltamista ei rajattaisi kansallisella tietosuojalailla, koska tietosuojavastaavan asemaa koskevilla säännöksillä pyritään varmistamaan, että tietosuojavastaavalla on asianmukaiset toimintaedellytykset tehtäviensä hoitamiselle.

4.3 Tietosuojavastaavan tehtävät

Tietosuojavastaavan toimenkuvaan kuuluvat neuvonta, ohjaus, tukitehtävät, seuranta ja valvontatehtävät. Hänellä voi olla myös muita erikseen määriteltyjä tehtäviä. Yleisen tietosuoja-asetuksen artiklan 39 mukaan tietosuojavastaavalla on oltava ainakin seuraavat tehtävät. Tietosuojavastaavan on annettava rekisterinpitäjälle tai henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat tietosuojasäännösten mukaisia velvollisuuksia. Lisäksi tehtäviin kuuluvat henkilötietosuojaan liittyvät vastuunjako, tiedon lisääminen sekä koulutus ja niihin liittyvät tarkastukset. Tehtävät sisältävät myös neuvojen antamisen vaikutuksenarvioinnista ja sen valvonta, yhteistyö valvontaviranomaisen kanssa ja toiminen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä asioissa sekä ennak-

kokuuleminen vaikutuksenarvioinneissa. Kun tietosuojavastaava suorittaa tehtäviään, on hänen huomioitava niihin liittyvät riskit, huomioon ottaen käsittelyn luonne laajuus, asiayhteys ja tarkoitus.

Tietosuojavastaava antaa tietosuojaan liittyen tietoja neuvoja sekä työnantajalleen että muille työntekijöille henkilötietojen käsittelyyn liittyen. Hän seuraa asetuksen noudattamista omassa organisaatiossaan ja hänen vastuulleen kuuluu myös tietosuojan tietoisuusohjelman rakentaminen ja kouluttaminen henkilöstölle organisaatiossa. Tietosuojavastaava neuvoo vaikutustenarviointeihin liittyen ja toimii valvontaviranomaisen yhteistyöpisteenä. (Kuntaliitto 2017.)

4.3.1 Yleisen tietosuoja-asetuksen noudattamisen seuraaminen

Asetuksen noudattamisen tueksi tietosuojavastaava voi kerätä tietoa käsittelytoiminnan tueksi, analysoida tiedot ja verrata, ovatko ne vaatimusten mukaisia. Tietosuojavastaavan on hyvä antaa tietoa ja neuvoja rekisterinpitäjälle ja henkilötietojen käsittelijöille asetuksen noudattamiseksi. (Tietosuojatyöryhmä 2016,19.)

Tietosuoja-asetuksen noudattaminen ei kuitenkaan ole tietosuojavastaavan vastuulla, vaan vastuun siitä kantaa loppujen lopuksi rekisterinpitäjän organisaatio. Yleistä tietosuoja-asetusta lainaten asetuksessa sanotaan, että rekisterinpitäjän *on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta* (EU 679/2016).

4.3.2 Tietosuojavastaavan rooli vaikutuksenarvioinneissa

Rekisterinpitäjän tehtävänä on tehdä tietosuojaa koskevat vaikutuksenarvioinnit. Tietosuojavastaavalla vaikutuksenarvioinnissa on lähinnä avustava rooli. Yleisen tietosuoja-asetuksen mukaan rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta vaikutuksenarviointia tehdessään ja vastaavasti tietosuojavastaavan on annettava neuvoja pyydettäessä.

WP29-tietosuojatyöryhmä suosittelee, että neuvoja vaikutuksenarvioinnin tekemiseen pyydettäisiin jo heti alussa, kun selvitetään, tehdäänkö vaikutuksenarviointi organisaatiolle, millaisia menetelmiä noudatetaan, tehdäänkö vaikutuksenarviointi organisaation sisällä vai ulkoistetaanko tehtävä ja mitä suojatoimia olisi otettava huomioon riskien vähentämiseksi rekisteröityjen osalta.

Tietosuojavastaavan on tarkistettava, vastaako vaikutuksenarviointi yleisen tietosuoja-asetuksen vaatimuksia. Mikäli näkökannat eroavat toisistaan, vaikutuksenarvioinnin asiakirjoissa olisi perusteltava miksi tietosuojavastaavan neuvoja ei ole noudatettu. Tietosuojavastaavan työsopimuksessa olisi hyvä olla täsmälliset tehtävät ja niiden laajuus koskien vaikutuksenarvioinnin toteutusta. (Tietosuojatyöryhmä 2016,20.)

4.3.3 Yhteistyö valvontaviranomaisen kanssa

Tietosuojavastaavan on tarkoitus tehdä yhteistyötä valvontaviranomaisen kanssa ja auttaa asiakirjojen ja tietojen saamisessa valvottavista kohteista. Tietosuojavastaavaa sitoo kuitenkin salassapitovelvollisuus unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. Tietosuojavastaava voi kuitenkin ottaa yhteyttä valvontaviranomaiseen ja kysyä tältä neuvoja. Tietosuojavastaava toimii myös yhteyspisteenä valvontaviranomaisen ja rekisteröityjen välillä. (Tietosuojatyöryhmä 2016,20.)

4.3.4 Riskiperusteinen lähestymistapa

Riskiperusteisella lähestymistavalla artiklassa tarkoitetaan yleistä ja järkevää toimintatapaa, joka liittyy tietosuojavastaavan päivittäiseen työhön. Tarkoituksena on, että tietosuojavastaava priorisoi toimiaan ja keskittyy ensisijaisesti työssään tehtäviin, joissa tietosuojariski on suurimmillaan. Tämä ei kuitenkaan tarkoita sitä, että hän jättäisi huomioimatta säännösten seuraamisen osa-alueilla joissa riskit ovat pienemmät. (Tietosuojatyöryhmä 2016,21.)

Tämä valikoiva ja käytännönläheinen lähestymistapa auttaa tietosuojavastaavaa neuvomaan rekisterinpitäjää vaikutuksenarvioinnissa käytettävistä menetelmistä, sisäisistä ja ulkoisista tietosuojan tarkastuskohteista, sisäisistä koulutustarpeista henkilöstölle ja johdolle ja mitkä käsittelytoimet vievät eniten tietosuojavastaavan aikaa ja resursseja. (Tietosuojatyöryhmä 2016, 21)

4.3.5 Tietosuojavastaavan rooli selosteen ylläpidossa

Yleisen tietosuoja-asetuksen 30 artiklan mukaan selosteen ylläpidosta vastaa rekisterinpitäjä tai henkilötietojen käsittelijä, ei tietosuojavastaava. Käytännössä

kuitenkin tietosuojavastaavan tehtäviin kuuluu usein luetteloiden ja käsittelytoimien rekisteröinti niiden tietojen perusteella, joita hän saa muualta organisaatiosta.

Artiklassa 39 mainituissa tehtävissä ei mainita selosteen ylläpidon kuuluvan tietosuojavastaavan tehtäviin, mutta tämä tehtävä voidaan antaa tietosuojavastaavan tehtäväksi. Tämä selosteen pitäminen tietosuojavastaavan toimesta, helpottaisi hänen omaa varsinaista tehtäväänsä eli sääntöjen noudattamisen seuraamista sekä tietojen ja neuvojen antamista rekisterinpitäjälle tai henkilötietojen käsittelijälle. Koska tällöin hän saisi suoraan selville, kuinka sääntöjä on noudatettu organisaatiossa. Selosteen ansiosta myös valvontaviranomainen saisi pyynnöstä yleiskatsauksen henkilötietojen käsittelytoimista organisaatiossa. (Tietosuojatyöryhmä 2016,21.)

4.3.6 TATTI-työryhmän esitys artiklaan 39 liittyen

TATTI-työryhmä on mietinnössään todennut, että koska yleisen tietosuoja-asetuksen artiklassa 39 eli tietosuojavastaavan tehtäviä määriteltäessä on kansallista liikkumavaraa, niin siitä voidaan tarvittaessa säätää erityislailla. Koska lista tietosuojavastaavan tehtävistä ei ole tyhjentävä, niin ainakin niissä tilanteissa, joissa velvollisuudesta tietosuojavastaavan nimittämiseen säädetään kansallisella lailla, voitaneen myös muista kuin 39 artiklassa luetelluista tehtävistä säätää kansallisella lailla. (Oikeusministeriö. 35/2017,56.)

Artikla 39 tulisi sovellettavaksi soveltuvin osin työryhmän mukaan. Työryhmä ehdottaakin, että artiklassa mainittu kohta, jossa tietosuojavastaava antaisi pyydettäessä neuvoja vaikutuksenarvioinnista ja valvoisi sen toteutusta ei tulisi sovellettavaksi, sillä 35 artiklaa ei sovellettaisi henkilötietojen käsittelyyn 85 artiklassa tarkoitetuissa tilanteissa. Lisäksi 39 artiklan alakohta e rajautuisi soveltamisen ulkopuolelle siltä osin kuin siinä asetetaan tietosuojavastaavalle tehtävä toimia yhteyspisteenä ennakkokuulemisessa. (Oikeusministeriö. 35/2017,165.)

Tietosuojavastaavan tehtäviä rajaisivat myös yleisen tietosuoja-asetuksen 85 artiklan nojalla tietosuojalailla säädettäväksi suunnitellut rajaukset. Tämän mukaan tietosuojavastaavan tehtävät eivät sisältäisi rekisterinpitäjän tai käsittelijän neuvontaa, kun kyseessä on rekisteröidyn oikeudet. *Näin ollen tietosuojavastaavan*

neuvontatehtävät koskisivat lähinnä tietosuojaa ja tietojen turvaamista koskevia rekisterinpitäjän velvollisuuksia. (Oikeusministeriö. 35/2017,165.)

Nykyisin henkilötietolain 33 §:ssä säädetään yleisestä vaitiolovelvollisuudesta, siinä mainittuja tietoja ei saa henkilötietolain mukaan ilmaista sivulliselle. Säännöstä ehdotetaan tarkistettavaksi siten, että vaitiolovelvollisuus lisättäisiin koskemaan myös tietoja, jotka henkilö on saanut tietää jonkin toisen henkilön liike- tai ammattisalaisuudesta. Vaitiolovelvollisuus koskisi kaikkia joiden tehtäviin liittyisi henkilötietojen käsittelyä. Tässä tapauksessa se koskisi esimerkiksi rekisterinpitäjän tai henkilötietojen käsittelijän palveluksessa olevia henkilöitä, kuten esimerkiksi tietosuojavastaavaa. Henkilötietolain sanamuotoa myös tarkistettaisiin nykyisestä muodosta *tietoja ei saa henkilötietolain vastaisesti ilmaista sivulliselle* muotoon *tietoja ei saisi oikeudettomasti ilmaista sivulliselle*. (Oikeusministeriö. 35/2017,171-172.)

4.4 Tietosuojavastaavan tehtävät käytännössä

Tietosuojavastaavan tehtävät on hyvä määritellä työsopimuksessa tai toimeksiantosopimuksessa tehtäessä hyvin tarkasti, jotta ei tule epäselvyyksiä tehtävien hoitamisesta. Mikäli tietosuojavastaavalle määritellään muitakin tehtäviä kuin yleisessä tietosuoja-asetuksessa määritellyt tehtävät, on hyvä määritellä myös tehtäviin käytettävä aika ja muut mahdolliset resurssit, joita tietosuojavastaava tulee tarvitsemaan hoitaakseen asianmukaisesti tehtäviään. Lisäksi on otettava huomioon, etteivät tehtävät ole ristiriidassa keskenään.

Andreassonin mukaan tietosuojavastaavan on oltava oma-aloitteinen ja rohkea lähestyessään organisaation johtoa, jotta hän pääsisi mukaan valmisteluvaiheisiin. Johdon olisi ymmärrettävä, että tietosuojavastaava on erityisasiantuntija tietosuoja-asioissa ja erittäin hyvä lisäresurssi organisaatiolle.

Yleisen tietosuoja-asetuksen mukaan tietosuojavastaava on otettava mukaan henkilötietojen suojaan liittyvien asioiden käsittelyyn jo varhaisessa vaiheessa. Tietosuojavastaavan resursseja kuluu ainakin alussa erilaisiin kokouksiin ja työryhmiin osallistumiseen. Henkilötietojen käsittelyn liittyvät seikat on oltava kirjattuna erilaisten sopimusten ja hankintojen dokumentteihin. Johdon on hyvä olla

yhteydessä tietosuojavastaavaan, kun sopimuksia tehdään, jotta kaikki oleelliset tietosuojaan liittyvät näkökohdat tulevat otettua huomioon.

Johdon tuki on erityisen tärkeä tietosuojavastaavalle, ilman sitä hän ei voi hoitaa tehtäviään asianmukaisesti. Johdolta saatu tuki käsittää toiminnan edellytykset, kannustuksen ja luottamuksen. (Andreasson ym. 2017,105.) Toiminnan edellytyksiin kuuluvat mm. resurssit, yhteistyö, osallistuminen suunnitteluun ja yhteiset tavoitteet päämääriin pääsemiseksi. Johdon kannustus ja luottamus motivoivat tietosuojavastaavaa tekemään työnsä paremmin. Kannustusta voi olla hyvin rakennettu palkkiojärjestelmä tai positiivisen palautteen saaminen hyvin tehdystä työstä. Luottamus perustuu aina avoimuuteen ja tietojen vaihtamiseen tietosuojavastaavan ja johdon välillä. Luottamuksen osoituksena näkyy myös vastuunantaminen, mielipiteiden kuunteleminen ja arvostaminen ja toimiva kommunikointi puolin ja toisin. Vastuunantamisesta ja tietosuojavastaavan velvollisuuksista on hyvä sopia selkeistä pelisäännöistä kirjallisesti. (Andreasson ym. 2017,111.)

Aivan ensimmäisenä tehtävänään tietosuojavastaavan tulee tehdä organisaation tietosuojakäytänteiden nykytilan kartoitus ja analyysi. Kartoituksen tarkoituksena on selvittää nykyiset ohjeet ja määräykset ja ovatko ne nykyisen lainsäädännön mukaisia. Organisaation tietojärjestelmiin tutustuminen ja henkilötietojen käsittelyn periaatteet ovat keskeisessä asemassa kartoituksessa. Analyysin kohteena ovat mm. asiakastiedot, henkilöstöhallinnon tiedot, ulkoistukset, ulkomaille siirrot, sopimukset sekä tietoturva (Andreasson & Ylipartanen 2016.)

Andreassonin mukaan henkilötietojen käsittelyn osalta selvitetään, kuinka tietoja käsitellään eli ketkä, mitä ja miten käsittelyt suoritetaan. Mitkä ovat käsittelijöiden käyttövaltuudet, onko salassa pidettäviä tietoja ja kuka vastaa mistäkin osa-alueesta käsittelyprosessissa. Kartoituksessa on hyvä selvittää myös se millä tavalla organisaation johto suhtautuu tietosuojaan ja tietoturvaan yleensäkin. Tämä kartoitus- ja analysointivaihe on aikaa vievää ja paljon resursseja vaativaa työtä, johon organisaation johto pitäisi saada sitoutettua, jotta tarvittavat resurssit olisivat käytössä.

Ohjeiden laatiminen ja niiden päivittäminen ovat jatkuvaa prosessityötä. Työntekijöiden perehdyttämisen tiesuoja- ja tietoturvakäytäntöihin on hyvä tapahtua samojen ohjeiden mukaan koko organisaatiossa. Tällöin niiden valvominen on helpompaa, kun tietää mitä ohjeita on henkilökunnalle ja johdolle annettu.

Viestinnän merkitystä ei pidä missään tapauksessa vähätellä tietosuojakäytännöistä puhuttaessa. Organisaatiossa on hyvä tehdä päätös siitä, mitä viestintäkanavia käytetään millekin kohderyhmälle. Pelkät kirjalliset ohjeet eivät välttämättä ole kaikkein toimivimpia, koska ne jäävät usein lukematta sekä johdolta että henkilökunnalta.

Yksi tärkeistä tietosuojavastaavan tehtävistä on myös henkilöstön ja mahdollisesti myös organisaation johdon kouluttaminen ja opastaminen tietosuoja-asioissa. Kannattaa ensin kartoittaa henkilöstön tietosuoja osaaminen ja sillä perusteella suunnitella koulutukset. Ensisijaisesti kannattaa kiinnittää huomiota käyttövaltuuksiin ja salasanojen käsittelyyn. Hyvin usein käyttövaltuuksia arkaluonteisiin henkilötietoihin on jaettu sillä periaatteella, että kaikki pääsevät kaikkiin tietoihin (ainakin pienemmissä yrityksissä). Henkilötietojen käsittelyn tarkoituksena on kuitenkin, että henkilötietoja käsittelevät vain ne henkilöt, joiden työtehtäviin ne oleellisesti kuuluvat. Toinen yleinen epäkohta on salasanojen käyttö. Salasanat ovat helposti arvattavia, kuten oma nimi tai lemmikkieläimen nimi, tai salasanoja ei käytetä laisinkaan.

Rekisteröityjen tiedustelut omien tietojensa käsittelystä työllistävät myös paljon tietosuojavastaavaa. Rekisteröidyt haluavat tietää esimerkiksi, kuka on käsitellyt tietoja ja missä tarkoituksissa tietoja käytetään. Lokitiedostojen selaaminen ja tietojen etsiminen vievät paljon tietosuojavastaavan aikaa.

Tietotilinpäätös on organisaation työkalu, jolla tuetaan tehokkuutta, vaikuttavuutta ja kilpailukykyä organisaatiossa. Tietosuojavastaava on keskeisessä osassa, kun tietotilinpäätöstä laaditaan. Tunnuslukujen ja mittareiden kehittämisessä ja laadinnassa tietosuojavastaavalla on asiantuntijana paras näkemys siitä, mitä tunnuslukuja ja mittareita käytetään. Tietotilinpäätöksestä saa yrityksen johto myös selkeän kuvan yrityksen tietosuojan tilasta ja lakien noudattamisesta. (Andreasson ym. 2017, 145.)

Tietosuojavaltuutetun toimiston laatiman oppaan *Laadi Tietotilinpäätös* (2012) mukaan tietotilinpäätöksessä voidaan kuvailla, millaisia tietovarantoja organisaatiolla on ja millainen tietoarkkitehtuuri organisaatiolla on käytössään. Hallussa olevien tietojen laadusta ja käytettävyydestä voidaan tehdä selvityksiä sekä menettelytavoista että periaatteista, kuinka tietoja käsitellään. Tietojen suojausten ja valvonnan käytännön toimista voidaan raportoida tietotilinpäätöksessä. Tarkemmin voidaan selvittää, kuinka rekisteröityjen oikeudet on otettu huomioon käsittelyprosesseissa.

Tietotilinpäätöksessä käsitellään myös tietojen käsittelyssä havaittuja kehittämiskohteita ja niiden kehittämistoimenpiteitä. Tietotilinpäätös voidaan kohdistaa erikseen organisaation johdolle, sidosryhmille, työntekijöille tai tietosuojaviranomaisille. (Tietosuojavaltuutetun toimisto 2012.)

4.5 Tietosuojavastaavan nimittäminen tilitoimistoon

Tietosuojavastaavaan nimittämistä varten vertaan yleistä tietosuoja-asetusta pienessä yrityksessä tapahtuvaan henkilötietojen käsittelyyn ja sillä perusteella mietin, onko yritykseen nimettävä tietosuojavastaava. Suomessa on hyvin paljon yksityisyrittäjiä, jotka pitävät tilitoimistoa pienimuotoisesti. Heillä ei välttämättä ole palkattua henkilöstöä vaan he hoitavat kaiken itse. Empiirisessä tutkimuksessani tutustun yhteen pieneen tilitoimistoon, jossa yrittäjä hoitaa yksin tilitoimiston hoitamisen.

Vaikka henkilötietojen käsittely, rekisteritietojen ylläpito ja niiden käyttö on ulkoistettu tilitoimistolle, varsinainen rekisterinpitäjä on toimeksiantaja. Hän määrittelee rekistereiden käyttötarkoituksen ja niiden tietojen ylläpidon keinot. Henkilötietojen käsittelijänä toimii tilitoimistoyrittäjä. Yrityksellä on noin parikymmentä toimeksiantajaa ja suurin osa niistä on yksityisyrittäjiä. Palkkalaskentaa yritys hoitaa noin 25 kappaletta kuukaudessa. Tilitoimisto käsittelee myös toimeksiantajien osto- ja myyntilaskuja yrityksille ja yksityishenkilöille.

Rekisteriselosteiden mukaan tilitoimistolla on tavallisimmat työntekijöiden henkilörekisterit toimeksiantajien palkansaajista. Niihin on rekisteröity työntekijän nimi, osoite, henkilötunnus, pankkitilin numero, veroprosentti ja kuukausittain maksettava palkan määrä. Tämän lisäksi voi olla ulosottomaksuja ja ammattiyhdistys

jäsenmaksuja. Lisäksi tilitoimistossa on toimeksiantajan asiakasrekistereitä osto- ja myyntitapahtumia varten.

Henkilötietojen käsittelyä tapahtuu palkanlaskennassa aina kun toimeksiantaja ilmoittaa uudesta työntekijästä, jolloin henkilötiedot kirjataan palkanlaskentajärjestelmään. Poislähtevien työntekijöiden tietoja käsitellään, kun tiedot henkilöstä arkistoidaan lainmääräämäksi ajaksi tai kun työntekijän tiedot poistetaan rekisteristä. Palkanlaskennan yhteydessä työntekijöistä kirjataan lisäksi sairauslomat, vuosilomat ja muut mahdolliset vapaat. Kuukausittain tai muuten määräajoin tapahtuvia henkilötietojen käsittelyjä ovat jäsenmaksujen, ulosottomaksujen tai muiden perintöjen tilitykset.

Tapaturmavakuutus- ja eläkevakuusyhtiöiden kanssa asioitaessa myös henkilötietoja käsitellään ilmoittamalla kunkin työntekijän henkilötunnuksen perusteella tapahtuvat vakuutusmaksut. Sairauspäivärahojen tai vanhempainpäivärahojen hakemisen yhteydessä Kansaneläkelaitokselta, joudutaan antamaan henkilöstä tietoja, jotka kuuluvat arkaluonteisiin tietoihin. Vuosittain annettavat ilmoitukset verottajalle työntekijän ansaitsemista palkoista ja muista etuuksista tai vähennyksistä ovat myöskin henkilötietojen käsittelyä. Tilitoimistolla on myös toimeksiantajiensa asiakasrekistereitä, joissa on muiden yritysten yhteyshenkilöiden tietoja, jotka liittyvät laskutukseen, myyntiin tai muihin liiketoimintojen hoitamiseen.

Yleisen tietosuoja-asetuksen mukaan yrityksen on nimettävä tietosuojavastaava, jos se on viranomainen tai julkishallinnon elin. Tämä kriteeri ei toteudu kyseisessä yrityksessä, koska kyseessä ei ole kumpikaan edellä mainituista ryhmistä. Toinen kriteeri nimittämiselle on, että ydintehtävät muodostuvat laajamittaisesta, säännöllisestä ja järjestelmällisestä rekisteröityjen tietojen käsittelystä.

Tutkimuksessa tulin siihen tulokseen, että tilitoimistoyrittäjän ydintehtävänä ei ole laajamittainen rekisteröityjen tiedonkäsittely, vaan hän suorittaa tehtäviä toimeksiantajan lukuun. Vaikka laajamittaisen käsittelyn määritelmä onkin avoin, niin kyseessä ei laajamittaisen käsittelyn kriteerit toteudu, henkilötietojen käsittelyn vähyyden vuoksi. Säännöllisestä ja järjestelmällisestä toiminnasta ei myöskään ole kyse, vaikka henkilötietoja käsitellään kuukausittain, niin tarkoituksena ei ole työntekijöiden profilointi, vaan pelkästään palkanmaksun ja sen oheistoimintojen

suorittaminen toimeksiantajan lukuun. Tilitoimiston toiminnassa ei ole myöskään kyse erityisten henkilötietoryhmien ja rikostuomioita tai rikkomuksia koskevien tietojen käsittelystä, joten tietosuojavastaavan nimittämistä ei tämän kohdan mukaan tarvitse tehdä.

Tutkimuksen tuloksena tulin siihen tulokseen, että yleisen tietosuoja-asetuksen mukaan tietosuojavastaavan nimittäminen kyseisessä yrityksessä ei ole pakollista. Vaikkakin henkilötietojen käsittely on säännöllistä ja järjestelmällistä, niin käsiteltävien tietojen määrä on niin pieni, ettei tarvetta tietosuojavastaavalle ole. Mikäli tilitoimisto ei halua myöskään vapaaehtoisesti nimittää tietosuojavastaavaa, olisi hänen hyvä dokumentoida tarkasti tosiasiat, miksi hän ei niin tee.

Tilitoimistoyrittäjän on kuitenkin dokumentoitava, kuinka hän käsittelee arkaluontoisia tietoja, kuten sairauspoissaoloja. Tällaisten tietojen on hyvä olla lukitussa arkistossa tai mikäli ne ovat sähköisessä muodossa, niin hakemistossa, jossa on rajatut käyttöoikeudet. Arkaluontoisia tietoja ei tule myöskään lähettää sähköpostitse tai ainakin niillä siinä tapauksessa täytyy olla vahva salaus. Toimeksiantajien kanssa on hyvä sopia myös siitä, voivatko työntekijät olla suoraan yhteydessä tilitoimistoon, koska tilitoimiston voi olla hankala tunnistaa työntekijä luotettavasti. Joka tapauksessa tilitoimistoyrittäjän on hyvä tehdä kirjalliset sopimukset toimeksiantajien kanssa siitä, kuinka henkilötietoja käsitellään sekä kummankin osapuolen vastuut käsittelyssä ja salassapitovelvollisuudet.

5 Johtopäätökset

Tässä opinnäytetyössä on tutkittu tietosuojavastaavan asemaa, nimittämistä ja tehtäviä EU:n yleisen tietosuoja-asetuksen mukaan. Selventämään tietosuoja-asetuksen artikloita tukeuduttiin WP29-tietosuojatyöryhmän julkaisemaan Tietosuojavastaavia koskeviin ohjeisiin. Ohjeista pyrittiin saamaan selville, mitä yleisen tietosuoja-asetuksen määritelmillä ja sanamuodoilla tarkoitetaan käytännössä. Ohjeista haettiin myös tietoa siitä, mitä käytännössä ovat tietosuojavastaavan asema, nimittäminen ja ennen kaikkea tehtävät. Kansalliseen lainsäädäntöön liittyen tutkin mitä TATTI-työryhmä on ehdottanut hallitukselle yleisen tietosuoja-asetuksen vaikutuksista mahdolliseksi uudeksi tietosuojalainsäädännöksi.

Tietosuojavastaavan työ on hyvin haasteellista, koska resurssit voivat olla hyvinkin minimaaliset. Työssä täytyy pystyä keskittymään moneen eri asiaan yhtä aikaa. Töiden priorisointi ja järjestelmällisyys tulee korostumaan tietosuojavastaavan tehtävässä. Koska aikataulun pitävyys ei aina johdu pelkästään tietosuojavastaavan omasta aikataulusta, on haasteellista saada myös muutkin huomioimaan aikataulutuksen tärkeys.

Työssä jaksamisen edellytyksenä on, että tietosuojavastaava osaa hahmottaa omat voimavaransa ja osaa pyytää apua tehtäviensä hoitamiseen. Mikäli tietosuojavastaava toimii yksin organisaation vastaavana, niin mahdollinen tietosuojatyöryhmän perustaminen helpottaisi myös tietosuojavastaavan työkuormitusta. Ennen kaikkea tietosuojavastaavan on huolehdittava omasta jaksamisestaan, jotta hän pystyy täysipainoisesti hoitamaan tehtävänsä.

Henkilökohtaisen koulutussuunnitelman laatimisen avulla tietosuojavastaava pystyy organisoimaan oman ammattitaitonsa ylläpitämisen. Koko ajan muuttuvassa tietosuojamaailmassa, lakien, säädösten ja ohjeiden muuttuessa, on erittäin tärkeää, että tietosuojavastaava on muutoksista ajan tasalla. Koska tietosuojavastaava on organisaation tietosuoja asiantuntija, hänellä täytyy olla viimeisin tieto siitä, mitä uusia käytäntöjä tulee organisaatiossa ottaa käyttöön. Tutkimuksen perusteella laadin tietosuojavastaavan huoneentaulun, jonka tarkoituksena on auttaa hahmottamaan konkreettisesti tietosuojavastaavan vastuita ja velvollisuuksia.

Empiirisessä tutkimuksessa tutustuin pienen tilitoimiston rekistereihin ja niiden perusteella selvitin, tulisiko yritykseen nimittää tietosuojavastaavaa. Vaikka kyseinen tilitoimisto toimii tietojenkäsittelijänä, ei sen toiminta ole kuitenkaan niin laaja-alaista, että sen perusteella pitäisi tietosuojavastaava nimittää. Tutkimustuloksena ilmeni myös, että kyseinen tilitoimisto käsittelee myös arkaluonteisia tietoja, mutta tietojen määrän vähäisyyden vuoksi sen ei tarvitsisi tietosuojavastaavaa nimittää. Vapaaehtoisesta tietosuojavastaavan nimittämisestäkään ei varsinaisesti olisi haittaa yritykselle. Toisaalta hyvällä dokumentoinnilla ja osoittamalla niillä perustellen, että noudattaa yleistä tietosuoja-asetusta ei yrityksen olisi tarvetta tietosuojavastaavan nimittämiseen.

6 Pohdinta

Tietosuoja-asetuksen käyttöönotto Suomessa ei tule olemaan ongelmatonta sen laaja-alaisuuden vuoksi. Etenkin tietosuojavastaavaa koskevissa määräyksissä on paljon myös sellaista, mitä voidaan kansallisesti säätää ja kansallinen lainsäätäminen oli tätä opinnäytetyötä kirjoitettaessa vielä kesken. Hallituksen esitystäkin luvattiin eduskunnalle vasta vuoden 2018 alkupuolella. Koska tietosuoja-asetusta pitää alkaa soveltaa toukokuussa 2018, tulee Suomen lainsäätäjille kiire saada esimerkiksi uusi lainsäädäntö valmiiksi siihen mennessä.

Tietosuojavastaavan nimittäminen tulee olemaan vaikeaa etenkin pk-yrityksille, koska se kysyy paljon resursseja, joita yrityksillä ei kuitenkaan ole. Mikäli kyse on esimerkiksi nettikauppaa pitävästä yrittäjästä, joka pääsääntöisesti hoitaa yritystään yksin, niin täytyisikö hänen ulkoistaa tietosuojavastaavan tehtävät? Tämä tulee maksamaan yritykselle todennäköisesti enemmän kuin siitä saatava hyöty. Tietosuojavastaava voi olla yritykselle myös tietoturvariski, mikäli hänellä ei ole vaadittavaa ammattitaitoa tehtäviensä hoitamiseen. Tietoturvariskinä voidaan pitää myös sitä, että resurssit ovat liian pienet, jotta tietosuojavastaava pystyisi pitämään ammattitaitoaan yllä ja kehittämään itseään.

Tietosuojavastaavien verkostoituminen joko seudullisesti tai peräti valtakunnallisesti auttaa tietosuojavastaavaa työssään. Silloin hän ei tunne olevansa yksin hankalienkaan asioiden kanssa, vaan hänellä on mahdollisuus kysyä neuvoa muilta vastaavassa asemassa olevilta.

Tätä opinnäytetyötä kirjoittaessani on vielä paljon yrityksiä, jotka eivät ole tehneet mitään yleisen tietosuoja-asetuksen määräysten soveltamiseksi. Tällä hetkellä on tietosuojavastaavan koulutuksia järjestäviä tahoja useita, joten voitaisiin melkein sanoa, että on kouluttajien markkinat. Koulutuksien hinnat ovat huimaavia, mutta koska kyse on pakollisesta tehtävästä joillekin yrityksille, koulutuksiin kannattaa osallistua. Mistä voi tietää, miltä kouluttajalta saa parhaimmat tiedot tietosuojavastaavan tehtäviin? Tietosuojavaltuutetun toimisto järjestää yhteistyössä eri toimijoiden kanssa koulutuksia ja niiden koulutuksien voidaan olettaa olevan ainakin asiantuntevia.

Hallituksen esityksen tutkiminen ja mahdollinen tietosuojalaki tulevat olemaan vielä hyvin mielenkiintoisia tutkimuksen kohteita. Toukokuun 2018 jälkeen, jolloin EU:n yleistä tietosuoja-asetusta aletaan soveltaa, tulee varmasti paljon uusia asioita vastaan, jota ei ole huomioitu asetusta laatiessa. Siitä johtuen Euroopan tietosuojaryhmällä tulee varmasti olemaan työtä uusien ohjeiden laatimisessa. Vaikka yleinen tietosuoja-asetus tulee voimaan kaikissa maissa samaan aikaan ja saman sisältöisenä, niin kansalliset eroavaisuudet tulevat varmaankin esille. Näiden yhteensovittaminen voi olla hankalaa ja ne tulevat työllistämään oikeuslaitoksia tulkintojen osalta. On kuitenkin todella hyvä asia, että on vihdoinkin saatu yhtenäinen käytäntö Euroopan tietosuoja-asioihin.

Kuvat

Lähteet

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Helsinki. Tietosanoma Oy.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Helsinki. Tietosanoma Oy.

Andreasson, A. & Ylipartanen, A. 2016. Näin teet tietosuojan nykytila-analyysin.OpiTietosuojaa.fi. https://opitietosuojaa.fi/index.php/fi/extrat/blogi/109-nait-teet-tietosuojan-nykytila-analyysin. Luettu 25.11.2017.

Eduskunta 2017. Eduskunnan lakihankkeiden tietopaketit (LATI) – EU:n tietosuojauudistus ja sen kansallinen täytäntöönpano. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx. Luettu 7.10.2017.

European Data Protection Supervisor. The History of the General Data Protection Regulation. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation. Luettu 10.11.2017.

EU 2016/679. Euroopan parlamentin ja neuvoston asetus (EU) 679/2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

Euroopan parlamentin ja neuvoston tietosuojadirektiivi 2016/680. http://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1494253391960&uri=CELEX%3A32016L0680. Luettu 1.10.2017.

Henkilötietolaki 523/1999

Husa, J., Mutanen, A. & Pohjolainen, T. 2008. Kirjoitetaan juridiikkaa. Tampere. Esa Print Oy.

Kolehmainen, A. 2005. Tutkimusongelma ja metodi lainopillisessa työssä. Teoksessa Miettinen, T. (toim.) Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edilex. Edita Publishing Oy,

Kuntaliitto 2017. Yleiskirje 14/2017, 29.5.2017, Ida Sulin. Yleinen tietosuoja-asetus. https://www.kuntaliitto.fi/yleiskirjeet/2017/yleinen-tietosuoja-asetus. Luettu 1.10.2017.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain muuttamisesta 250/2014.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159

Oikeusministeriö 35/2017. Oikeusministeriön julkaisu. Mietintöjä ja lausuntoja. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Oikeusministeriö. Helsinki. 2017. http://urn.fi/URN:ISBN:978-952-259-612-3. Luettu 1.10.2017

Oikeusministeriö OM1/41/2016. Asettamispäätös. Henkilötietojen suojaa koskevan kansallisen lainsäädännön tarkistaminen. https://api.hankeikkuna.fi/asiakirjat/38ae644f-e25d-4da8-aa74-a5070c53a1f4/f473c5a5-8a1f-4a0e-b44d-1580a51acc3f/ASETTAMISPAATOS_20160219031503.pdf Luettu 25.10.2017.

Oikeusministeriön viestintäosasto 2017. Sähköpostiviesti 22.11.2017. Hallituksen esityksen ajankohta liittyen tietosuoja-asetukseen.

Tietosuojatyöryhmä 2016. 16/FI.WP 243 rev.01. Tietosuojavastaavia koskevat ohjeet. Tarkistettu ja hyväksytty 5. huhtikuuta 2017.

Tietosuojavaltuutetun toimisto 2012. Laadi tietotilinpäätös. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf. Luettu 25.10.2017.

Vilpponen, M. 2012. Tietosuojavastaavien rooli ja asema sosiaali- ja terveydenhuollossa. Itä-Suomen yliopisto. Sosiaali- ja terveydenhuollon tietohallinto. Pro gradu -tutkielma.

TIETOSUOJAVASTAAVAN HUONEENTAULU:

Hoida tehtäväsi ammattitaitoisesti ja rehellisesti.

Ota asioihin kantaa ja uskalla tuoda esille omat mielipiteesi.

Kehitä tietosuojakäytäntöjä organisaatiossa.

Laadi itsellesi työjärjestys ja priorisoi tehtäväsi.

Raportoi ylimmälle johdolle kirjallisesti ja säännöllisin väliajoin.

Huolehdi rekisteröityjen oikeuksien noudattamisesta.

Osallistu henkilötietojen käsittelyn suunnitteluun jo alkuvaiheessa.

Järjestä säännöllisesti koulutusta sitä tarvitseville.

Huolehdi ammattitaitosi ylläpidosta kouluttautumalla itsekin.

Älä jää yksin!

Verkostoidu muiden tietosuojavastaavien kanssa.

Pidä huolta jaksamisestasi, älä kuvittele olevasi yli-ihminen.

Seuraa uusien tietosuojasuojakäytäntöjen kehittymistä.

Ole ajantasalla lainsäädännön ja ohjeiden viidakossa seuraamalla niitä aktiivisesti.

Ole tarvittaessa yhteydessä tietosuojavaltuutettuun.