

Waltteri Vehmanen

EU:N YLEISEN TIETOSUOJA-ASETUKSEN VAIKUTUKSET
TILITOIMISTOON: CASE X

Liiketalouden koulutusohjelma
2019

EU:N YLEISEN TIETOSUOJA-ASETUKSEN VAIKUTUKSET
TILITOIMISTOON: CASE X

Vehmanen, Waltteri
Satakunnan ammattikorkeakoulu
Liiketalouden koulutusohjelma
Marraskuu 2019
Sivumäärä: 32
Liitteitä: 1

Asiasanat: tietosuoja, rekisteröity, henkilötieto, rekisterinpitäjä

Opinnäytetyössä tutkittiin EU:n yleistä tietosuoja-asetusta, tietosuoja-asetukseen valmistautumista sekä muutoksia joita tietosuoja-asetus sai aikaan. Työn tarkoituksena oli tutkia tietosuoja-asetuksen muutoksia ja tietosuoja-asetukseen valmistautumista tilitoimisto X:n näkökulmasta. Opinnäytetyö on toteutettu kvalitatiivisena tutkimuksena, jossa työn toimeksiantaja oli tilitoimisto X.

Tutkimuksessa selvisi, että tietosuoja-asetukseen valmistautuminen vei suunniteltua enemmän aikaa. Tietosuoja-asetukseen valmistautuminen oli aloitettava ajoissa, jotta asetusta pystyttiin noudattamaan sen voimaantullessa. Tietosuoja-asetus velvoittaa lähes jokaista niin pientä kuin suurta yritystä tekemään muutoksia henkilötietojen käsittelyyn.

Tilitoimistossa henkilötietojen käsittely on päivittäistä, joten on todella tärkeää ymmärtää, kuinka henkilötietojen käsittely tulee muuttumaan tietosuoja-asetuksen myötä. Tutkimuksessa on saatu hyvin koottua ne asiat, jotka tietosuoja-asetus muuttaa henkilötietojen käsittelyssä. Työn tärkeinä lähteinä toimi itse tietosuoja-asetus sekä tietosuojavaaluttetun toimisto. Lisäksi muita lähteitä työssä olivat aiheeseen liittyvät kirjat, toimeksiantajan henkilökohtainen haastattelu sekä erilaiset tietosuoja-asetusta koskevat verkkosivut.

Tietosuoja-asetus toi mukanaan lisää velvollisuuksia rekisterinpitäjälle. Dokumentaation avulla yrityksen tulee pystyä todistamaan asetuksen noudattaminen sekä tietojen käsittelyn tulee olla asianmukaista. Tietosuoja-asetus vahvisti myös rekisteröidyn asemaa ja toi rekisteröidylle enemmän oikeuksia. Lisäksi opinnäytetyössä tutkittiin, minäkalaisia seurauksia yritykselle voi koitua, mikäli tietosuoja-asetusta laiminlyödään.

IMPACT OF THE EU GENERAL DATA PROTECTION REGULATION ON THE ACCOUNTING OFFICE: CASE X

Vehmanen, Waltteri
Satakunta University of Applied Sciences
Degree Programme in Business Administration
November 2019
Number of pages: 32
Appendices: 1

Keywords: data protection, data subject, personal data, controller

The thesis explored the EU General Data Protection Regulation, the preparation for the GDPR and the changes brought about by the GDPR. The purpose of this thesis was to examine the changes in the GDPR and the preparation of the GDPR from the point of view of accounting company X. The thesis was carried out as a qualitative study, commissioned by accounting company X.

The study found that preparing for the GDPR took longer than expected. Preparations for the GDPR had to be started early enough in order to comply with the regulation when it enters into force. The GDPR obliges almost every company, small and large, to make changes to the processing of personal data.

At the accounting office, the processing of personal data is a daily matter, so it is important to understand how the processing of personal data will change after GDPR. The study has provided a good overview of the issues that the GDPR changes in the processing of personal data. Important sources at work were the GDPR itself and the office of the data protection officer. Other sources of work included related books, a personal interview with the principal and different web sites about the GDPR.

The GDPR brings additional obligations for the controller. Documentation must allow the company to prove compliance with the regulation and to process the data properly. The GDPR also strengthened the position of the data subject and gave them more rights. In addition, the thesis examined the consequences for a company if not complying with the GDPR.

SISÄLLYS

1	JOHDANTO.....	6
2	TIETOSUOJA-ASETUS.....	7
2.1	Tavoitteet	7
2.2	Velvoitteet.....	8
3	TIETOSUOJA-ASETUKSEEN VALMISTAUTUMINEN TILITOIMISTOSSA X.....	9
3.1	Informointi	9
3.2	Vaikutusten arviointi.....	9
3.3	Tietotilinpäätös	10
4	TIETOSUOJA-ASETUKSEN VAIKUTUKSET TILITOIMISTOSSA X	11
4.1	Valvonta.....	11
4.2	Sopimukset.....	12
4.3	Tietojen suojaaminen	12
5	HENKILÖTIETOJEN KÄSITTELY	14
5.1	Rekisterinpitäjän velvollisuus	14
5.2	Henkilötietojen käsittelijä	15
5.3	Sisäänrakennettu ja oletusarvoinen tietosuojaja	16
5.4	Osoitusvelvollisuus	16
5.5	Tietojenkäsittelysopimus	17
5.6	Riskiperusteinen lähestymistapa ja vaikutusten arviointi	18
5.7	Tietosuojavastaava	19
5.7.1	Tietosuojavastaavan nimeäminen.....	19
5.7.2	Tietosuojavastaavan asema	20
5.7.3	Tietosuojavastaavan tehtävät.....	20
6	REKISTERÖIDYN OIKEUDET	21
6.1	Omien henkilötietojen käsittely ja pääsy omiin tietoihin	21
6.2	Tietojen oikaisu ja tietojen poistaminen	22
6.3	Tietojen käsittelyn rajoittaminen ja tietojen siirtäminen	23
6.4	Tietojen käsittelyn vastustaminen ja automaattinen päätöksenteko	24
7	TIETOVUODOT JA SANKTIOT	25
7.1	Henkilötietojen tietoturvaloukkaukset.....	25
7.2	Hallinnolliset sakot	27
7.3	Vahingonkorvausvastuu.....	28
7.4	Rikosoikeudellinen vastuu	28
8	YHTEENVETO JA POHDINTA	29
	LÄHTEET.....	32

LIIKTEET

1 JOHDANTO

Opinnäytetyön aiheeksi valikoitui EU:n yleisen tietosuoja-asetuksen aiheuttamat vaikutukset tilitoimisto X:ssä. Opinnäytetyön aihe nousi esille keväällä 2018 suoritetun harjoittelun yhteydessä, jolloin EU:n yleinen tietosuoja-asetus oli juuri astumassa täysimääräisenä käytäntöön. Harjoittelupaikka oli auktorisoitu tilitoimisto X, johon tietosuoja-asetus toi mukanaan paljon uudistuksia. Opinnäytetyön toimeksiantaja on edellä mainittu tilitoimisto X. Keskustelimme toimeksiantajan kanssa mikä olisi mahdollinen opinnäytetyön aihe, jolloin toimeksiantaja ehdotti EU:n yleistä tietosuoja-asetusta. Opinnäytetyön tarkoitus on tuottaa tietoa aiheesta sekä tutkia sen vaikutuksia tilitoimisto X:ssä. Tietosuoja-asetus on aiheena niin uusi, joten tällainen tutkimus on todellakin tarpeellinen.

Opinnäytetyö on rajattu käsittelemään tietosuoja-asetuksen tuomia muutoksia ja vaikutuksia ainoastaan tilitoimisto X:n näkökulmasta. Työssä kerrotaan tarkemmin, miten tietosuoja-asetus vaikutti kohdeyritykseen sekä miten tietosuoja-asetuksen voimaan astumiseen valmistauduttiin. Työssä kuullaan myös toimeksiantajan mielteitä tietosuoja-asetuksesta ja sen tuottaman oheistyön lisääntymisestä. Opinnäytetyön tarkoituksena on saada lukija ymmärtämään, miten tietosuoja-asetus vaikutti tilitoimisto X:ään sekä kuinka tietosuoja-asetuksen voimaan astumiseen voidaan varautua.

Opinnäytetyö on kvalitatiivinen tutkimus eli laadullinen tutkimus, jossa tutkitaan tietosuoja-asetuksen aiheuttamia vaikutuksia tilitoimisto X:ssä. Kvalitatiivinen tutkimus on kokonaisvaltaista tiedon hankintaa, jossa tietoa kerätään todellisissa elämän tilanteissa. Työssä käytetään tiedonkeruumenetelminä erilaisten dokumenttien analysointia, tilitoimiston toimitusjohtajan haastattelua sekä havainnointia, jotka ovat laadullisen tutkimuksen tyypillisiä metodeja. (Hirsjärvi, Remes & Sajavaara 2009, 164.) Havainnointi on hyvä tiedonkeruumenetelmä, sillä sain seurata tietosuoja-asetuksen voimaan astumista harjoittelun yhteydessä. Osallistuin myös palavereihin ja keskusteluihin, joissa pohdittiin tulevia toimenpiteitä. Teoria aineistona opinnäytetyössä on käytetty internettiä sekä erilaisia tutkimuksen aiheeseen liittyviä kirjoja.

2 TIETOSUOJA-ASETUS

EU:n yleinen tietosuoja-asetus 2016/679 hyväksyttiin Euroopan parlamentin ja neuvoston päätöksillä keväällä 14.4.2016. Tietosuoja-asetukselle myönnettiin kahden vuoden siirtymäaika, jonka jälkeen tietosuoja-asetus astui täysimääräisenä voimaan 25.5.2018. EU:n antama asetus tulee suoraan sovellettavaksi lainsäädännöksi samaan aikaan kaikissa EU-maissa, mukaan lukien Suomessa. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 13.) Yritysten ja rekisterinpitäjien täytyy tarkistaa tietosuojakäytäntöjen lainmukaisuus sekä oikaistava ne noudattamaan kansallisen lainsäädännön ja EU:n tietosuoja-asetuksen uusia vaatimuksia kahden vuoden siirtymäajan kuluessa. EU:n yleisen tietosuoja-asetuksen tarkoitus on korvata vanha henkilötietodirektiivi, joka otettiin käyttöön vuonna 1995. (OpiTietosuoja.fi www-sivut 2016)

Tietosuojasta -ja tietosuoja-asetuksesta puhuttaessa on paljon käsitteitä, joita lukija ei välttämättä ymmärrä. Tällaisia käsitteitä on esimerkiksi henkilötieto, rekisteröity, rekisterinpitäjä ja henkilötietojen käsittelijä. Henkilötiedolla tarkoitetaan tietoja, joiden perusteella henkilö voidaan tunnistaa. Esimerkiksi nimi, kotiosoite ja puhelinnumero ovat henkilötietoja. Rekisteröidyllä tarkoitetaan henkilöä, jota henkilötieto koskee. Rekisterinpitäjä voi olla henkilö, yritys, yhteisö tai viranomainen. Rekisterinpitäjä määrittelee, minkä takia henkilötietoja käsitellään sekä keinoja, miten tietoja käsitellään. Henkilötietojen käsittelijä on puolestaan rekisterinpitäjän ulkoinen taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. (Tietosuojavaltuutetun toimisto 2019)

2.1 Tavoitteet

EU:n yleisen tietosuoja-asetuksen tarkoitus on päivittää sekä nykyaikaistaa henkilötietodirektiivin periaatteita, yhtenäistää EU:n jäsenmaiden erilaisia tietosuoja koskevia käytänteitä sekä vahvistaa ja parantaa rekisteröityjen itsemääräämisoikeutta. Tietosuoja-asetuksen tavoitteita ovat yksilön oikeuksien vahvistaminen, sisämarkkinaulottuvuuden lujittaminen, tietosuojan globaalin ulottuvuuden huomioiminen sekä tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen. Asetuksen tavoitteena on myös luoda koko EU:lle vahva, ajanmukainen, kattava ja yhtenäinen tietosuojakehys. Lisäksi tietosuoja-asetuksen yksi päämäärä on parantaa luottamusta online-

palveluihin sekä siten edistää EU:n digitaalisten sisämarkkinoiden kehitystä. (Andreasson, Riikonen & Ylipartanen 2019, 27.)

Tietosuoja-asetus koskee henkilötietojen käsittelyä ja sen tarkoitus on turvata henkilötietojen suoja riippumatta ihmisten kansalaisuudesta tai asuinpaikasta. Tietosuoja-asetuksella vahvistetaan säännöt luonnollisten henkilöiden suojelulle henkilötietojensa käsittelyssä sekä suojellaan luonnollisten henkilöiden perusoikeuksia -ja vapauksia ja erityisesti heidän oikeuttaan henkilötietojensa suojaan. Lisäksi asetuksella vahvistetaan säännöt, jotka koskevat henkilötietojen vapaata liikkuvuutta unionin sisällä. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 34.)

2.2 Velvoitteet

EU:n yleinen tietosuoja-asetus tuo yrityksille ja rekisterinpitäjille täysin uusia velvoitteita. Tietosuoja-asetus sisältää säännöksiä muun muassa henkilötietojen käsittelyä koskevista periaatteista, käsittelyn lainmukaisuudesta ja arkaluonteisten tietojen käsittelystä. Tietojen käsittelyn on oltava asianmukaista ja sen täytyy tapahtua tiettyä tarkoitusta varten. Lisäksi tietojen käsittely täytyy tehdä asianomaisen henkilön suostumuksella tai laissa säädetyllä perusteella. Jokaisella henkilöllä on oikeus tutustua niihin tietoihin mitä hänestä on kerätty sekä vaatia niiden tietojen oikaisua. (Andreasson ym. 2019, 28.)

Rekisterinpitäjän vastuulla on pitää huolta, että tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyn vaiheissa. Osoitusvelvollisuuden takia ei riitä, että tietosuojaperiaatteita noudatetaan, vaan rekisterinpitäjän täytyy myös pystyä osoittamaan, että periaatteita on noudatettu oikein. Rekisterinpitäjän tulee suunnitella ja dokumentoida henkilötietoihin kohdistuva käsittely aiempaa tarkemmin, jotta periaatteiden noudattaminen pystytään todistamaan. (Andreasson ym. 2019, 31.)

3 TIETOSUOJA-ASETUKSEEN VALMISTAUTUMINEN TILITOIMISTOSSA X

3.1 Informointi

Asiakkaille tietosuoja-asetuksesta informoitiin ensimmäisen kerran jo kesällä 2017, jolloin asiakkaille lähetettiin asiakastiedote asetuksen voimaan tulemisesta. Ensimmäisen tiedotteen jälkeen asiakastiedotteita lähetettiin sitä mukaan, kun asiassa edettiin. Tiedotteissa asiakkaita informoitiin mm. mitä lakimuutos tarkoittaa, ketä se koskee ja miten koskee, minkälaisia valmisteluita se asiakasyrityksissä vaatii sekä tietysti, että kaikkien asiakkaiden täytyy allekirjoittaa uusi toimeksiantosopimus joko sähköinen tai paperinen ja käydä joka tapauksessa tunnistautumassa tilitoimistolla. (Leppä-Lukkala henkilökohtainen tiedonanto 5.9.2019)

Koulutukset ja työpaikalla pidetyt palaverit takasivat sen, että henkilökunta tiesi tietosuoja-asetuksesta hyvissä ajoin ennen lain voimaantuloa. Lukuisissa palavereissa koko henkilökunta kävi yhdessä läpi tilitoimiston uusien sopimusten laatimista sekä tilitoimiston käytäntöjä kaikissa tietoturva-asioissa. Tietosuoja-asetukseen alettiin valmistautua tilitoimisto X:ssä edellisenä kesänä 2017, kun asetus astui voimaan 25.5.2018. (Leppä-Lukkala henkilökohtainen tiedonanto 5.9.2019)

3.2 Vaikutusten arviointi

Rekisterinpitäjän tulee suorittaa vaikutustenarviointi, mikäli henkilötietojen käsittely sen luonne, asiayhteys, laajuus ja tarkoitukset huomioon ottaen todennäköisesti aiheuttaisi luonnolliselle henkilölle oikeuksien kannalta korkean riskin. Rekisterinpitäjän on kuitenkin vähintäänkin arvioitava, onko vaikutustenarviointi tehtävä vai ei. Vaikutustenarviointi on prosessi, jossa tarkastellaan tietosuojan noudattamiseksi suunniteltuja toimenpiteitä, mekanismeja ja suojoitoimia, joiden avulla lievennetään henkilötietojen käsittelystä rekisteröidyn oikeuksille aiheutuvia riskejä. Vaikutusten arvioinnin on tarkoitus varmistaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta sekä sillä pyritään kuvaamaan henkilötietojen käsittely ja arvioimaan käsittelyn tarpeellisuutta suhteessa aiheutuviin riskeihin. Lisäksi vaikutustenarviointi on hyödyllinen

työkalu helpottamaan tietosuoja-asetuksen mukaisen osoitusvelvollisuuden käytännön noudattamista. (Hanninen ym. 2017, 115)

Henkilötietojen käsittelyn ollessa dynaamista, voi olla, että vaikutustenarviointi on yrityksessä jatkuva prosessi. Rekisterinpitäjän tulee tarvittaessa tehdä vaikutustenarviointi uudelleen, esimerkiksi jos käsittelytoimien sisältämä riski on muuttunut. On tärkeää ymmärtää, että tietosuoja koskevan vaikutustenarvioinnin tekeminen on jatkuva prosessi, eikä kertaluontoinen tehtävä. Asianmukaiset sekä tarvittavat tekniset ja organisatoriset suojatoimet täytyy suhteuttaa henkilötietojen käsittelystä aiheutuvaan riskiin käyttämällä suojakeinoja ennalta suunnitellusti riskien poistamiseksi tai pienentämiseksi. Henkilötietojen käsittelystä aiheutunut riski tulee saada laskettua hyväksytylle tasolle käyttämällä teknisiä ja organisatorisia suojatoimia. Rekisterinpitäjä voi myös kääntyä tietosuojavaltuutetun puoleen, mikäli se ei ole omin voimin kyennyt pienentämään riskiä riittävälle tasolle. Henkilötietojen käsittely voidaan oikeutetusti aloittaa vasta, kun riskit on saatu hyväksyttävälle tasolle. (Andreasson ym. 2019, 68)

3.3 Tietotilinpäättös

Tietotilinpäättös on yrityksen itse laatima raportti, mikä on vapaaehtoinen. Tietotilinpäättöksen on tarkoitus antaa kokonaiskuva yrityksen tietojenkäsittelyn nykytilasta. Raportti on tarkoitettu johdon työkaluksi sekä lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa tietosuoja-asetuksen mukaista tietojenkäsittelytapaa henkilötietojen käsittelyssä. Tietotilinpäättöstä voidaan käyttää myös keinona tietosuoja-asetuksen osoitusvelvollisuuden toteuttamisessa. (GDPR.fi www-sivut 2016)

Tietotilinpäättöksen tarkoitus on toimia dynaamisena työkaluna, joka tukee organisaation tehokkuutta, kilpailukykyä sekä vaikuttavuutta. Tietotilinpäättöksen avulla opitaan tunnistamaan ja suunnittelemaan tärkeät seurattavat tunnusluvut, jotka liittyvät yrityksen tietojen käsittelyyn. Tietotilinpäättös on organisaation sisäisen tarkastuksen tulos, joka toimii sisäisen ja ulkoisen valvonnan apuvälineenä. Tietotilinpäättös toimii johdon tietosuojan ja toiminnan suunnittelun, seurannan sekä kehittämisen työkaluna, mutta sen lisäksi tietotilinpäättös raportoi organisaation tiedonhallinnan vahvuuksista ja heikkouksista. Tietotilinpäättös kuvaa parhaimmillaan, että henkilötietojen käsittelyn

valvonta on onnistunut lainsäädännön ja määräysten mukaisesti, mutta sen lisäksi tietotilinpäätös ohjaa tarkastelemaan tietosuoja-asioita kriittisemmin. Mikäli tietojenkäsittelyn valvonnassa on havaittu kehittämiskohteita tai poikkeamia, tietotilinpäätös kuvaa hyvin toimenpiteet, joihin on ryhdytty. (Andreasson ym. 2019, 192-194)

Tietotilinpäätöksen tekeminen vaatii paljon työtä ja yhteistyökykyä organisaation sisällä sekä sen tekemiseen tulee varata riittävästi aikaa. Organisaation laatiessa tietotilinpäätöstä on pohdittava, mitä mittareita ja tunnuslukuja otetaan mukaan tarkkailuun, kuka tietotilinpäätöksen kokoaa ja miten, kuinka usein tietotilinpäätös tulee laatia, missä tietotilinpäätös käsitellään sekä kenelle se lähetetään tiedoksi ja miten havaittuja puutteita korjataan. (Andreasson ym. 2019, 194)

4 TIETOSUOJA-ASETUKSEN VAIKUTUKSET TILITOIMISTOSSA X

4.1 Valvonta

Rekisterinpitäjää valvotaan entistä tarkemmin, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. Rekisterinpitäjällä on siis osoitusvelvollisuus, joka tarkoittaa entistä tarkempaa dokumentointia henkilötietojen lainmukaisesta käsittelystä. Opinnäytetyön toimeksiantaja kertoi haastattelussa, että tietosuoja-asetus aiheutti yllättävän paljon oheistyötä, sillä kaikki täytyi dokumentoida. Tietosuojaselosteet dokumentoitiin sekä julkaistiin yrityksen nettisivuille kaikkien nähtäviksi, jolloin osoitusvelvollisuus toteutuu. (Leppä-Lukkala henkilökohtainen tiedonanto 5.9.2019)

Ennen tietosuoja-asetusta, rekisterinpitäjän tuli laatia vain rekisteriseloste, mutta tietosuoja-asetuksen astuttua voimaan rekisterinpitäjällä on velvollisuus laatia seloste käsittelytoimista. Rekisterinpitäjän selosteen tulee sisältää mm. tiedot:

- Rekisterinpitäjän, tämän edustajan sekä tietosuojavastaavan nimi sekä yhteystiedot
- Henkilötietojen käsittelyn tarkoitukset
- Kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
- Henkilötietojen vastaanottajat, joille henkilötietoja mahdollisesti luovutetaan tai on luovutettu
- Eri tietoryhmien poistamisen suunnitellut määräajat
- Tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle sekä suoja-toimia koskevat asiakirjat
- Yleinen kuvaus teknisistä ja organisatorisista turvatoimista (Hanninen ym. 2017, 125-126)

4.2 Sopimukset

Tietosuoja-asetuksen seurauksena toimeksiantaja joutui tekemään kaikkien asiakkaiden toimeksiantosopimukset uudelleen. Toimeksiantaja käytti sopimuskoneen sähköistä sopimus pohjaa, jonka laki-ihmiset olivat tehneet yhteistyössä taloushallintoliiton kanssa. Sopimus pohja oli kuitenkin valmis vasta 2018 keväällä, joten se oli aiheuttanut paineita toimeksiantajalle ajankäytönsuhteen. Lisäksi sopimusten laatiminen oli vienyt runsaasti aikaa ja työtä, sillä sopimukset ovat monisivuisia ja sopimukseen täytyi täydentää kunkin asiakkaan tiedot yksitellen. Asiakas pystyi allekirjoittamaan sopimuksen joko sähköisesti tai tulemalla paikan päälle allekirjoittamaan paperinen sopimus. Jokainen asiakas täytyi tunnistaa sekä skannata ajokortti, passi tai henkilökortti ja lisätä se salaiseen kansioon. (Leppä-Lukkala henkilökohtainen tiedonanto 5.9.2019)

4.3 Tietojen suojaaminen

Tilitoimiston omat rekisterit koskevat yritystietoja, jotka eivät varsinaisesti koske tietosuoja-asetuksen piirissä olevaa tietoa, mutta tilitoimiston asiakkaiden tiedot ovat

salasanoilla suojatussa ohjelmistossa. IT asiat kuten suojaukset, palomuurit ja pilvipalvelut on suojattu tehokkailla systeemeillä, mitkä IT kumppani on tarjonnut. Tilitoimisto X:n IT kumppani auttoi myös tietoturvaan liittyvissä asioissa, joista syntyi erillinen monisivuinen asiakirja. Toimeksiantaja oli tyytyväinen asiakirjasta, mikä koostui tietoturva-asioista, sillä se saatiin hyvissä ajoin valmiiksi ennen taloushallintoliiton viisivuotis tarkastusta. (Leppä-Lukkala henkilökohtainen tiedonanto 5.9.2019)

Tilitoimisto X:n palveluihin kuuluu myös palkanlaskenta, johon tietosuoja-asetus toi mukanaan tarkennuksia. Palkanlaskijan tietoihin pääsevät ainoastaan tietoihin oikeutetut henkilöt. Lisäksi palkanlaskijan ovi on lukollinen, ettei asiattomat pääse käsiksi palkanlaskijan tietoihin. (Leppä-Lukkala henkilökohtainen tiedonanto 5.9.2019)

Tilitoimisto X:n käytössä oleva sähköposti lähetetään turvapostilla, mikäli lähetettävä tieto on tietosuoja-asetuksen alaista, kuten henkilön sotu-tieto. Toimeksiantajan mukaan turvaposti on kuitenkin ollut yrityksellä käytössä jo vuodesta 2005, joten tilitoimisto X on ollut aikaansa edellä. Lisäksi tilitoimisto X:llä on ollut useamman vuoden käytössä tietoturvalaatikko, johon tuhottavat tulosteet laitetaan sekä tuhoetaan asiallisesti siihen sertifioidun yhtiön toimesta. (Leppä-Lukkala henkilökohtainen tiedonanto 5.9.2019)

5 HENKILÖTIETOJEN KÄSITTELY

5.1 Rekisterinpitäjän velvollisuus

Rekisterinpitäjä voi olla luonnollinen henkilö eli ihminen, yritys, viranomainen tai vastaava taho, joka määrittelee henkilötietojen käsittelyn keinot ja tarkoitukset. Rekisterinpitäjällä on henkilötietojen käsittelyssä aina viimesijainen vastuu tietojen lainmukaisesta käsittelystä. Lisäksi tietosuoja-asetuksen mukaan rekisterinpitäjä vastaa siitä, että henkilötietojen käsittelijät noudattavat soveltuvaa lainsäädäntöä. Rekisterinpitäjälle olisi suotuisaa valita sopimuskumppani, joka huolehtisi asianmukaisesta tietosuoja- ja tietoturva vaatimusten noudattamisesta. (Hanninen ym. 2017, 26)

Rekisterinpitäjän vastuulla on ryhtyä tarvittaviin teknisiin ja organisatorisiin toimenpiteisiin, jotta voidaan varmistua ja osoittaa, että tietosuoja-asetusta noudatetaan lainmukaisesti. Teknisiä ja organisatorisia toimenpiteitä suunniteltaessa ja toteutettaessa on rekisterinpitäjän otettava huomioon henkilötietojen käsittelyn luonne, laajuus, tarkoitukset ja asiayhteys sekä henkilötietojen käsittelyyn liittyvät riskit. Tällainen riskiperusteinen lähestymistapa tarkoittaa, että suojatoimet suhteutetaan henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille liittyvään riskiin. Rekisterinpitäjän tulee arvioida, millaisia riskejä henkilötietojen käsittely sisältää sekä millaisia vahinkoja käsiteltävien tietojen paljastuminen ulkopuolisille saattaa aiheuttaa rekisteröidylle. (Hanninen ym. 2017, 26)

Rekisterinpitäjän on kiinnitettävä erityistä huomiota tietojen käsittelyyn, mikäli käsiteltäviin henkilötietoihin kuuluu arkaluonteisia henkilötietoja tai jos käsitellään esimerkiksi lasten henkilötietoja, sillä kyseisissä tilanteissa tietojenkäsittelyyn liittyvä riski on tavallista suurempi. Tavallista korkeampi riski voi olla myös, kun käsittelyn kohteena on suuri määrä henkilötietoja tai jos henkilötietojen käsittely koskee suurta rekisteröityjen määrää, vaikka tiedot itsessään eivät olisikaan erityisen arkaluonteisia. Mitä suurempi määrä käsiteltäviä henkilötietoja on tai mitä arkaluonteisempia käsiteltävät tiedot ovat, sitä suurempi on riski ja sitä huolellisempaa rekisterinpitäjän toiminnan on oltava sekä sitä enemmän toimenpiteitä voidaan odottaa rekisterinpitäjältä. (Hanninen ym. 2017, 27)

Rekisterinpitäjän tulee noudattaa tietosuoja-asetuksessa säädettyjä henkilötietojen käsittelyä koskevia periaatteita. Nämä tietosuojaperiaatteet ovat käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, tietojen täsmällisyys, tietojen säilytyksen rajoittaminen, tietojen eheys ja luottamuksellisuus sekä rekisterinpitäjän osoitusvelvollisuus. Henkilötietojen käsittelyn on perustuttava lailliseen perusteeseen, esimerkiksi asiakas -tai työsuhteeseen perustuvaan etuun. Henkilötietoja tulee käsitellä ainoastaan jonkun tietyn tehtävän suorittamiseksi eli henkilötiedot on kerättävä aina tiettyä laillista ja nimellistä tarkoitusta varten. Henkilötietojen on myös aina oltava täsmällisiä ja tarpeen tullen niitä on päivitettävä. Henkilötietoja tulee säilyttää vain niin kauan kuin on tarpeen tietojen käsittelyn tarkoituksen toteuttamista varten. Lisäksi henkilötietoja on käsiteltävä siten, että varmistutaan henkilötietojen turvallisuudesta ja luottamuksellisuudesta. (Hanninen ym. 2017, 48-51)

5.2 Henkilötietojen käsittelijä

Henkilötietojen käsittelijä on organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijällä on oikeus käsitellä henkilötietoja ainoastaan rekisterinpitäjältä saamien dokumentoitujen ohjeiden mukaisesti. Mikäli henkilötietojen käsittelijä rikkoisi tietosuoja-asetusta esimerkiksi määrittämällä henkilötietojen käsittelyn keinot ja tarkoitukset rekisterinpitäjän sijaan, pidetään henkilötietojen käsittelijää rekisterinpitäjänä. (Hanninen ym. 2017, 24)

Henkilötietojen käsittelijän vastuut ovat kasvaneet huomattavasti tietosuoja-asetuksen myötä. Ennen tietosuoja-asetuksen voimaantuloa henkilötietojen käsittelijän velvoitteet koostuivat lähinnä tietoturvaan liittyviin edellytyksiin sekä sopimusvelvoitteisiin. Asetuksen voimaantulon myötä henkilötietojen käsittelijän on tarkasti huomioitava roolinsa rajat. Esimerkiksi jos henkilötietojen käsittelijänä toiminut yritys määrittelee käsittelytoimissaan itsenäisesti tietojen käsittelyn tarkoituksia, tulkitaan käsittelijä rekisterinpitäjäksi, jolloin yritys on myös syyllistynyt sopimusrikkomukseen. (Hanninen ym. 2017, 27)

Henkilötietojen käsittelijää koskee myös vaitiolovelvollisuus. Mikäli henkilötietojen käsittelijä on toimenpiteitä suorittaessaan saanut tietoonsa jotakin toisen henkilön ominaisuuksista, taloudellisesta asemasta tai henkilökohtaisista oloista, henkilötietojen käsittelijä ei saa oikeudettomasti ilmaista sivullisille saamiaan tietoja tai käyttää niitä omanaan tai toisen hyödyksi tai toisen vahingoksi. (Tietosuojalaki 1050/2018, 6 luku 35 §)

5.3 Sisäänrakennettu ja oletusarvoinen tietosuojaja

Sisäänrakennetulla ja oletusarvoisella tietosuojalla on tärkeä merkitys osoitusvelvollisuuden toteutumiseksi välttämättömiin teknisiin ja organisatorisiin keinoihin. Sisäänrakennetulla tietosuojalla velvoitetaan tietosuojaperiaatteiden toteutumista kaikissa tietojen käsittelyn vaiheissa, joten yrityksen kannattaa ottaa tietosuojakäytännöt huomioon jo suunnitellessaan ja kehittäessään tuotteita, palveluita ja sovelluksia. Sisäänrakennetun tietosuojan vaatimus ei velvoita ohjelmistojen -ja teknisten ratkaisujen suunnittelijoita tai tarjoajia, vaan rekisterinpitäjää, sillä rekisterinpitäjä on vastuussa varsinaisesta henkilötietojen käsittelystä. (Andreasson ym. 2019, 188)

Oletusarvoisen tietosuojan periaate puolestaan tarkoittaa, että rekisterinpitäjä käsittelee vain kunkin käyttötarkoituksen kannalta tarpeellisia tietoja. Oletusarvoinen tietosuojaja velvoite koskee esimerkiksi kerättyjen henkilötietojen määrää, käsittelyn laajuutta sekä tietojen säilytysaikaa. Edellä mainittujen toimenpiteiden avulla pyritään muun muassa varmistamaan, ettei henkilötietoja saatettaisi oletusarvoisesti rajoittamattoman henkilömäärän saataville. (Hanninen ym. 2017, 54)

5.4 Osoitusvelvollisuus

Tietosuojaperiaatteita on noudatettava kaikissa henkilötietojen käsittelyn vaiheissa, mutta osoitusvelvollisuuden myötä rekisterinpitäjän on myös pystyttävä osoittamaan, että näin on toimittu. Rekisterinpitäjän on suunniteltava ja dokumentoitava henkilötietojensa käsittely aiempaa tarkemmin, jotta hän voi osoittaa noudattavansa tietosuojaperiaatteita. Aiemmin on ollut riittävää, että säännöksiä noudatetaan eikä dokumentaatiovelvollisuutta ole ollut. (Hanninen ym. 2017, 51)

Rekisterinpitäjän tulee ensinnäkin toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, jotta voidaan olla varmoja, että käsittelyssä noudatetaan tietosuojasetusta. Tietosuoja-asetuksen lainsäädännössä ei määritellä yksityiskohtaisesti, miten osoitusvelvollisuutta tulisi käytännössä toteuttaa, vaan rekisterinpitäjälle on jätetty valinnanvapaus parhaaksi katsomiensa keinojen määrittelemiseen ja käyttämiseen. On kuitenkin suositeltavaa, että yritys laatii omat sisäiset tietosuojaperiaatteensa, kirjaa ylös kaikki tietosuojakäytäntönsä sekä kokoaa kaikki tietosuojaan liittyvät dokumentit ja selosteet siten, että ne ovat helposti löydettävissä ja että niiden avulla pystytään muodostamaan kokonaiskuva yrityksen henkilötietojen käsittelystä ja tietosuojasta. Yritys voi esimerkiksi liittää verkkosivuilleen omat tietosuojaan liittyvät dokumenttinsa ja tietosuojaperiaatteensa, jolloin ne ovat esillä ja helposti löydettävissä. (Andreasson ym. 2019, 187-188)

Osoitusvelvollisuuden täyttämiseksi yrityksen olisi hyvä kirjata ylös tietoja tietosuojaavasta tai muusta tietosuojaorganisaatiosta, käsiteltävistä tietoryhmistä, käsittelyn perusteista, käsiteltävien henkilötietojen käyttötarkoituksesta sekä siitä, miten kyseisiä henkilötietoja käsitellään ja miten rekisteröityä informoidaan henkilötietojen käsittelystä. (Hanninen ym. 2017, 52) Yritys voi myös hyödyntää tietosuoja koskevien sertifiointimekanismien ja tietosuojasinetien käyttöä. Sertifiointimekanismien ja tietosuojasinetien tarkoitus on osoittaa rekisterinpitäjän ja henkilötietojen käsittelijän noudattavan tietosuojasetusta käsittelytoimissaan. (Hanninen ym. 2017, 114)

5.5 Tietojenkäsittelysopimus

Tietosuoja-asetuksen artikla 28:n mukaan henkilötietojen käsittelijän suorittamaa tiedon käsittelyä on määritettävä sopimuksella, jonka rekisterinpitäjä ja henkilötietojen käsittelijä tekevät keskenään. Sopimuksen tulee olla kirjallinen, jossa määritellään rekisterinpitäjän ja henkilötietojen käsittelijän suhde toisiinsa. Lisäksi sopimuksessa kerrotaan mm. käsittelyn luonne ja tarkoitus, käsittelyn kohde ja kesto, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet. (Sulin 2017)

Tietosuoja-asetus määrittelee henkilötietojen käsittelijän roolin sekä henkilötietojen käsittelijän lainsäädännöstä johtuvia velvoitteita on täsmennetty suhteessa henkilötietolain sääntelyyn. Asetuksessa mainitaan myös, ettei henkilötietojen käsittelijä saa käyttää omia alihankkijoitaan käsittelyssä ilman rekisterinpitäjän erityistä lupaa tai yleistä kirjallista ennakkolupaa. (Sulin 2017)

Sopimuksessa mainittujen tietojen avulla voidaan yksilöidä, mitä tietojenkäsittelytehtäviä ulkoistetaan, keitä ulkoistus koskee sekä mitä tietoluokkia käsitellään. Esimerkiksi palkanmaksu voidaan ulkoistaa, jolloin se koskee työntekijöitä ja heidän tiedoistaan käsitellään työntekijöiden yhteystietoja. (Korpisaari ym. 2018, 294)

5.6 Riskiperusteinen lähestymistapa ja vaikutusten arviointi

Tietosuoja-asetuksessa on ymmärretty riskiperusteinen lähestymistapa, joka tarkoittaa, että rekisterinpitäjän on suhteutettava tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Riskillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvaa fyysistä, aineellista tai aineetonta vahinkoa. Henkilötietojen käsittelijän on siis arvioitava henkilötietojen käsittelyyn liittyvät riskit ja toteutettava tarpeelliset toimenpiteet riskien lieventämiseksi. (Tietosuojavaltuutetun toimisto 2019)

Rekisterinpitäjän on tehtävä riskiarvio rekisteröidyn näkökulmasta ja arvioitava mitä rekisteröidyn vapauksia ja oikeuksia käsittely saattaa vaarantaa sekä mitä vahinkoja rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Henkilötietojen käsittelystä aiheutuva vahinko tarkoittaa rekisteröidylle riskiä joutua esimerkiksi identiteettivarkauden tai petoksen kohteeksi, sosiaaliseen vahinkoon, taloudellisiin menetyksiin tai henkilötietojen pseudonymisoinnin kumoutumiseen. Henkilötiedot on siis suojattava siten, että suojaustoimenpiteet vastaavat henkilötietojen käsittelyyn liittyvää riskiä. Käsitellessä arkaluonteisia henkilötietoja, kuten lasten tietoja tai erityisiin henkilötietoryhmiin kuuluvia tietoja riskin taso voi olla korkeampi. Tällaisissa tapauksissa vaaditaan myös tehokkaampia teknisiä ja organisatorisia suojausmekanismeja.

Lisäksi riskien tason arvioinnissa on otettava huomioon henkilötietojen käsittelyn laajuus, luonne, asiayhteys ja tarkoitukset. (Tietosuojavaltuutetun toimisto 2019)

5.7 Tietosuojavastaava

Tietosuojavastaava toimii organisaation sisäisenä asiantuntijana rekisterinpitäjän apuna sekä auttaa rekisterinpitäjää saavuttamaan korkean tietosuojan tason organisaatiossa. Tietosuojavastaava seuraa henkilötietojen käsittelyä ja auttaa tietosuojasääntösten noudattamisessa sekä antaa asiantuntevaa apua henkilöstölle ja johdolle. Organisaatio ei voi kuitenkaan ulkoistaa rekisterinpidon vastuutaan tietosuojavastaavalle, sillä organisaation johto on rekisterinpitäjänä vastuussa rekisterinpidosta sekä henkilötietojen lainmukaisesta käsittelystä. (Andreasson ym. 2019, 92)

5.7.1 Tietosuojavastaavan nimeäminen

Tietosuoja-asetuksessa edellytetään, että organisaatioon nimitetään tietyissä tilanteissa tietosuojavastaava rekisterinpitäjän tai henkilötietojen käsittelijän toimesta. Tietosuojavastaava tai tietosuoja-asioista vastaava henkilö voidaan nimittää myös vapaaehtoisesti, mikä on monessa tavassa suositeltavaa. (Korpisaari ym. 2018, 347) Tietosuojavastaavaksi voidaan nimittää organisaation oman henkilökunnan henkilö tai hänet voidaan valita tehtävään palvelusopimuksen perusteella. Tietosuojavastaavaa valittaessa on syytä tarkastaa henkilön ammattipätevyys, asiantuntemus tietosuojalainsäädännöstä ja tietosuojakäytänteistä sekä henkilön valmiudet selviytyä hänelle määrätyistä tehtävistä. Tietosuojavastaavaksi valitulta henkilöltä ei varsinaisesti edellytetä tietosuojavastaavan koulutusta tai kokemusta, mutta vastuiden monimuotoisuuden vuoksi, tehtävään valitulta henkilöltä odotetaan perehtyneisyyttä sekä mieluusti useamman vuoden kokemusta tietosuoja-asioista. (Hanninen ym. 2017, 121)

Tietosuojavastaavan yhteystiedot on julkistettava ja ilmoitettava ne valvontaviranomaisille. Tietosuojavastaavan yhteystiedot julkistetaan, jotta hänet tavoitettaisiin helposti ja vaivattomasti. Yrityksen on ilmoitettava vähintään tietosuojavastaavan puhelinnumero, osoite sekä sähköpostiosoite. (Hanninen ym. 2017, 122)

5.7.2 Tietosuojavastaavan asema

Tietosuojavastaava ei saa ottaa vastaan ohjeita hoitaessaan tehtäviään, joilla pyrittäisiin vaikuttamaan esimerkiksi siihen, miten hän tekee valvontatyötä, milloin hän konsultoi valvontaviranomaista tai miten hänen kuuluisi tulkita tietosuojalainsäädäntöä. Näin ollen tietosuojavastaavan aseman tulee olla riippumaton. Tietosuojavastaavan riippumattomasta asemasta kertoo myös se, että hänellä on oikeus ja velvollisuus raportoida suoraan organisaation ylimmälle johdolle. (Andreasson ym. 2019, 95)

Tietosuojavastaava on otettava ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn. Vaikka tietosuojavastaava toimiikin yrityksen johdon keskustelu kumppanina tietosuojaan liittyvien asioiden suunnittelussa ja toteutuksessa, hän ei kuitenkaan saa osallistua yrityksen päätöksentekoon, sillä kyse on vain konsultoivasta tehtävästä. (Hanninen ym. 2017, 122)

5.7.3 Tietosuojavastaavan tehtävät

Tietosuojavastaavan tehtäviin kuuluu tietosuoja-asetuksen sekä muun lainsäädännön ja ohjeistuksen täytäntöönpano sekä soveltaminen organisaatiossa. Tietosuojavastaavan työhön kuuluvat myös neuvonta, ohjaus sekä tukitehtävät. Koska tietosuojavastaavan työ on pääasiassa konsultointia ja johdolle raportointia, hänen työnkuvassaan korostuvat seuranta -ja valvontatehtävät. Tietosuojavastaavan vastuulla on nimenomaan seurata ja valvoa, että lainsäädäntöä noudatetaan oikein. Tietosuojavastaavan tulee antaa tietosuoja koskevaa ohjausta ja neuvontaa organisaation lisäksi myös rekisteröidyille, varsinkin rekisteröityjen oikeuksiin liittyvissä asioissa. (Andreasson ym. 2019, 92-93)

Lainsäädäntö kuitenkin muuttuu sekä uusia määräyksiä ja ohjeistuksia annetaan aika ajoin, joten tietosuojavastaavan on aktiivisesti seurattava tulevia muutoksia ja arvioitava niiden mahdollisia tietosuojavaikutuksia organisaatiossa. Tietosuojavastaavan täytyy seurata ja valvoa näiden tietosuojavaatimusten noudattamista ja rekisteröityjen oikeuksien toteutumista. (Andreasson ym. 2019, 93)

6 REKISTERÖIDYN OIKEUDET

Rekisterinpitäjällä on velvollisuus toimittaa rekisteröidylle kaikki käsittelyä koskevat tiedot tiiviisti esitetystä, läpinäkyvässä, helposti ymmärrettävissä sekä saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Rekisteröityä on informoitava muun muassa siitä, kuka toimii rekisterinpitäjänä, tietojen käsittelyn tarkoituksista, tietojen säilytysajoista, mihin tietoja luovutetaan sekä kuinka rekisteröity voi käyttää oikeuksiaan. (Andreasson ym. 2019, 165-166) Tietosuoja-asetuksen mukaan rekisteröidyn oikeuksia ovat tiedon saanti omien henkilötietojensa käsittelystä, pääsy omiin tietoihinsa, oikeus oikaista tietojansa, poistaa tiedot tai tulla unohdetuksi, rajoittaa tietojen käsittelyä, oikeus siirtää tiedot järjestelmästä toiseen, vastustaa tietojen käsittelyä sekä olla joutumatta automaattisen päätöksenteon kohteeksi. (Tietosuojavaltuutetun toimisto 2019)

6.1 Omien henkilötietojen käsittely ja pääsy omiin tietoihin

Tietosuoja-asetuksen myötä henkilöllä on tietojen tarkastusoikeus. Henkilöllä on oikeus saada tietää, käsitelläänkö hänen henkilötietojaan vai ei sekä minkälaisia henkilötietoja hänestä on tallennettu. Rekisteröidyn pyytäessä tietoja, rekisterinpitäjän on toimitettava tiedot ilman aiheetonta viivytyksiä. Asetuksessa on säädetty määräajaksi kuukausi tietojen toimittamiselle sekä tietopyyntöön liittyvien lisätietojen antamiselle pyynnön vastaanottamisesta. Mikäli rekisteröidyn tietopyyntö on poikkeuksellisen monimutkainen ja laaja, voidaan määräaika poikkeuksellisesti jatkaa kahdella kuukaudella. (Andreasson ym. 2019, 167)

Rekisteröidyn pyytämät tiedot toimitetaan lähtökohtaisesti maksutta, mutta mikäli jäljennöksiä pyydetään useita kappaleita, voi rekisterinpitäjä halutessaan periä jäljennöksistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Rekisteröidyn pyytämien tietopyyntöjen ollessa kohtuuttomia ja ilmeisen perusteettomia, kuten tietopyyntöjen toistuva esittäminen, voi rekisterinpitäjä periä tietojen toimittamisesta aiheutuneita hallinnollisia kustannuksia tai kieltäytyä kokonaan toimittamasta tietoja. Tällaisen tilanteen sattuessa rekisterinpitäjän on osoitettava pyynnön kohtuuttomuus. Rekisterinpitäjän kieltäytyessä toimittamasta tietoja, on asiasta annettava kirjallinen

todistus. Lisäksi samassa yhteydessä rekisteröidylle kerrotaan oikeudesta oikeussuojakeinoihin, kuten mahdollisuudesta tehdä valitus tietosuojavaltuutetulle. (Andreasson ym. 2019, 167)

Tietosuoja-asetuksen 15 artiklassa säädetään rekisteröidyn oikeudesta saada pääsy häntä koskeviin henkilötietoihin. Tätä oikeutta on rekisteröidyn voitava toteuttaa vaittomasti ja kohtuullisin väliajoin. Näin ollen hän voi arvioida onko käsittely ollut lainmukaista sekä tarkistamaan ovatko tiedot oikein. Mikäli rekisteröity esittää tietopyynnön sähköisesti, myös tiedot toimitetaan yleisesti käytetyssä sähköisessä muodossa, ellei rekisteröity toisin pyydä. Tietojen antamiselle ei muutoin ole määräämuotoa. Tiedot voidaan antaa esimerkiksi tulosteena, sähköisesti yleisesti käytetyssä tiedostomuodossa tai suullisesti rekisteröidylle. (Korpisaari ym. 2018, 209-211)

6.2 Tietojen oikaisu ja tietojen poistaminen

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää oikaisemaan tai täydentämään virheelliset ja puutteelliset henkilötiedot ilman aiheetonta viivytystä. Rekisteröidyllä on myös oikeus vaatia tarpeettomien henkilötietojensa poistamista ja ”oikeus tulla unohdetuksi”. Henkilötietojen virheellisyyttä ja tarpeettomuutta arvioidaan tietojen tallennushetken mukaan. Mikäli rekisterinpitäjä ei hyväksy oikaisupyynnöä, rekisteröidylle annetaan kirjallinen todistus asiasta, missä kerrotaan kyseiset syyt, joiden perusteella vaatimusta ei ole hyväksytty. Samalla rekisterinpitäjä voi taas informoida rekisteröityä hänen oikeudestaan oikeussuojakeinoihin, kuten mahdollisuudesta tehdä valitus tietosuojavaltuutetulle. (Andreasson ym. 2019, 168)

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää poistamaan itseään koskevia henkilötietoja ilman aiheetonta viivytystä, sekä rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä, mikäli perustelut poistamiselle täyttyvät. Perusteita henkilötietojen poistamiselle ovat muun muassa:

- henkilötietoja ei enää tarvita samoihin tarkoituksiin, mitä varten ne oli kerätty tai mitä varten niitä käsiteltiin
- rekisteröity haluaa peruuttaa suostumuksen, johon käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta
- rekisteröity vastustaa käsittelyä eikä käsittelyyn ole perusteltua syytä
- rekisterinpitäjä on käsitellyt henkilötietoja lainvastaisesti
- henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi
- rekisterinpitäjä on kerännyt henkilötiedot 8 artiklan 1 kohdassa tarkoitetun tietoyhteiskunnan palvelujen tarjoamisen yhteydessä (EU:n yleinen tietosuojasetus 3 luku, 17 artikla)

6.3 Tietojen käsittelyn rajoittaminen ja tietojen siirtäminen

Henkilötietoja käsitellessä on poikkeustilanteita, jossa rekisteröidyllä on oikeus pyytää henkilötietojensa käsittelyn rajoittamista siksi aikaa, kunnes rekisteröidyn tiedot on asianmukaisesti tarkistettu ja korjattu tai tarpeen vaatiessa täydennetty. Tietojen käsittelyn rajoittaminen voi tulla kyseeseen, jos esimerkiksi henkilö kiistää henkilötietojensa paikkaansa pitävyyden tai kun tietoja ei enää tarvita niiden alkuperäiseen tarkoitukseen. (Andreasson ym. 2019, 168)

Tietojen rajoittamistilanteessa rekisterinpitäjällä on edelleen oikeus säilyttää tietoja, mutta niitä ei saa käsitellä muutoin kuin rekisteröidyn suostumuksella. Tietojen säilyttäminen voi tulla tarpeen esimerkiksi myöhempien kanteiden tai vaatimusten esittämisen varalta. Rekisterinpitäjä saa loogisesti käsitellä tietoja oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi, sillä tietosuoja ei voi estää rekisterinpitäjää tai kolmatta tahoja toteuttamasta heidän lainmukaisia oikeuksiaan eikä puolustautumasta mahdollisia lainvastaisia vaatimuksia vastaan. (Korpisaari ym. 2018, 236-237)

Rekisteröidyllä on oikeus saada siirtää toimittamansa itseään koskevat tiedot toiselle rekisterinpitäjälle koneluettavassa muodossa, mikäli se vain on teknisesti mahdollista. Esimerkiksi työntekijällä on oikeus saada palkkatiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, sillä palkanmaksu perustuu työsopimuksen täyttämiseen. (Hanninen ym. 2017, 65) Oikeus rekisteröidyn tietojen siirtämisestä ei kuitenkaan koske sellaista henkilötiedon käsittelyä, joka on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Käytännössä siirto-oikeutta järjestelmästä toiseen toteutetaan vain, mikäli henkilötietojen käsittelyn oikeusperuste on peräisin rekisteröidyn suostumuksesta tai sopimuksesta. Rekisterinpitäjän kieltäytyessä pyynnöstä, on rekisterinpitäjän perusteltava kieltäytyminen sekä informoitava rekisteröityä oikeuksistaan. (Andreasson ym. 2019, 169)

6.4 Tietojen käsittelyn vastustaminen ja automaattinen päätöksenteko

Rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä, milloin tahansa henkilökohtaisen tai erityisen tilanteensa perusteella. Rekisteröidyllä on vastustamisoikeus silloinkin, kun käsittely perustuu rekisterinpitäjälle kuuluvan julkisen vallan käyttöön tai yleistä etua koskevan tehtävän suorittamiseen. Tällaisen tapauksen sattuessa, voi rekisterinpitäjä käsitellä edelleen tietoja, mikäli siihen on huomattavan tärkeä tai perusteltu syy, joka pystytään osoittamaan. Tällöin syyn on syrjäytettävä rekisteröidyn vapaudet, oikeudet sekä edut. Henkilötietojen käsittelyn tarve oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi on myös peruste henkilötietojen käsittelylle. (Andreasson ym. 2019, 169)

Jos rekisterinpitäjällä ei ole huomattavan tärkeää tai perusteltua syytä henkilötietojen käsittelylle, tulee yrityksen lopettaa henkilötietojen käsittely, jos rekisteröity näin pyytää. Tällöin yrityksen tulee joko poistaa rekisteröidyn tiedot kokonaan tai poistaa tiedot aktiivisesta käytöstä niin, että pääsy tietoihin on estetty. (Hanninen ym. 2017, 68)

Rekisteröidyllä on oikeus olla joutumatta automaattisen päätöksenteon kohteeksi. Rekisteröity voi siis vaatia, että häntä koskevat päätökset suorittaa ihminen. Rekisteröidyn oikeus on olla joutumatta sellaisen päätöksenteon kohteeksi, mikä perustuu ainoastaan automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen merkittävästi vastaavalla tavalla. (Andreasson ym. 2019, 170)

On tilanteita, joissa yritys saa käyttää automaattista päätöksentekojärjestelmää, kuten profilointia, riippumatta rekisteröidyn oikeudesta olla joutumatta automaattisen päätöksenteon kohteeksi. Yritys saa käyttää automaattista päätöksentekojärjestelmää, mikäli päätös on hyväksytty lainsäädännössä, päätös perustuu rekisteröidyn omaan suostumukseen tai päätös on välttämätön yrityksen ja rekisteröidyn välisen sopimuksen tekemistä tai täytäntöönpanoa varten. Tällöin yrityksen on kyettävä osoittamaan, että automatisoitu päätöksenteko on välttämätöntä. (Hanninen ym. 2017, 70)

7 TIETOVUODOT JA SANKTIOT

7.1 Henkilötietojen tietoturvaloukkaukset

Rekisterinpitäjä tai henkilötietojen käsittelijä on syylistynyt henkilötietojen tietoturvaloukkaukseen, mikäli henkilötietoja on hävinnyt, tuhoutunut, henkilötietoja on luovutettu luvottomasti tai henkilötietoihin on päässyt käsiksi taho, jolla ei ole niihin käsittelyoikeutta. Tietoturvaloukkauksia voi olla esimerkiksi hävitetty työtietokone, tiiliotteen postitus väärälle henkilölle, kadonnut USB-tikku, kyberhyökkäys tai hakkeointi. Tietoturvaloukkauksen seurauksia voi olla identiteettivarkaus tai petos, henkilötietojen valvontaoikeuden menettäminen, maineen vahingoittuminen sekä

salassapitovelvollisuuden alaisten henkilötietojen paljastuminen. (Tietosuojavaltuutetun toimisto 2019)

Rekisterinpitäjän tulee olla varautunut mahdollisiin tietoturvaloukkauksiin. Tietoturvaloukkauksiin voidaan varautua laatimalla toimintaohjeet mahdollisia tietoturvaloukkaustilanteita varten. Rekisterinpitäjän on pystyttävä reagoimaan nopeasti tietoturvaloukkauksiin. Lisäksi rekisterinpitäjän tai henkilötietojenkäsittelijän tulee suojata henkilötiedot niin, että suojaustoimenpiteet vastaavat henkilötietojen käsittelyyn liittyvät riskit. Rekisterinpitäjän on arvioitava, minkä tasoinen riski voi aiheutua tietoturvaloukkauksesta sen kohteena olevalle henkilölle, esimerkiksi ei aiheuta riskiä, aiheuttaa riskin ja aiheuttaa korkean riskin. (Tietosuojavaltuutetun toimisto 2019)

Riskin taso määrittää mihin toimenpiteisiin rekisterinpitäjän on ryhdyttävä. Toimenpiteitä ovat esimerkiksi ilmoitus valvontaviranomaiselle, ilmoitus rekisteröidylle sekä tietoturvaloukkauksen dokumentointi. Rekisterinpitäjän kannattaa dokumentoida kaikki henkilötietojen tietoturvaloukkaukset, niiden vaikutukset sekä toteutuneet korjaus toimet, sillä dokumentointivelvollisuuden tai ilmoituksen tekemisen laiminlyöminen on tietosuoja-asetuksen vastaista. Niiden laiminlyöminen saattaa johtaa tietosuoja-asetuksessa määrättyihin seuraamuksiin. (Tietosuojavaltuutetun toimisto 2019)

Rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta ilman aiheutonta viivytystä sekä mahdollisuuksien mukaan 72 tunnin kuluessa sen huomaamisesta 55 artiklan mukaisesti toimivaltaiselle valvontaviranomaiselle, paitsi jos tietoturvaloukkauksesta ei todennäköisesti aiheudu henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä. Mikäli ilmoitusta ei anneta 72 tunnin kuluessa, on rekisterinpitäjän toimittava valvontaviranomaiselle perusteltu selitys. Henkilötietojen käsittelijän on puolestaan ilmoitettava tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheutonta viivytystä saatuaan sen tietoonsa. (EU:n yleinen tietosuoja-asetus 4 luku, 33 artikla) Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, mikäli tietoturvaloukkaus todennäköisesti tulee aiheuttamaan korkean riskin rekisteröidyn oikeuksille ja vapauksille. Rekisterinpitäjän tulee ilmoittaa tietoturvaloukkauksesta rekisteröidylle ilman aiheutonta viivytystä. Rekisteröidylle on annettava ilmoitus, jossa kuvataan selkeällä ja yksinkertaisella kielellä henkilötietojen luonne sekä annettava 33

artiklan 3 kohdassa tarkoitettut tiedot ja toimenpiteet. (EU:n yleinen tietosuoja-asetus 4 luku, 34 artikla)

7.2 Hallinnolliset sakot

Tietosuoja-asetuksessa merkittävä muutos on viranomaisille myönnettyt valtuudet määrätä sanktioita tietosuoja-asetusta laiminlyöneille toimijoille. Viranomaisten määräämien hallinnollisten sakkojen määrään ja määräämiseen vaikuttavia tekijöitä ovat muun muassa:

- mitä velvollisuutta toimija on rikkonut
- yrityksen toimenpiteet rikkomisen korjaamiseksi sekä haittavaikutusten lieventämiseksi
- rikkomisen luonne, kesto ja vakavuus ottaen huomioon tietojenkäsittelyn luonne, laajuus ja tarkoitus
- rekisteröityjen lukumäärä, joihin rikkominen vaikuttaa sekä heille aiheutuneiden vahinkojen suuruus
- tapa, jolla rikkominen on tullut viranomaisen tietoon eli ilmoittiko rekisterinpitäjä tai henkilötietojen käsittelijä rikkomisesta ja missä laajuudessa (Hanninen ym. 2017, 129)

Tietosuoja-asetuksen 83 artiklan mukaan hallinnollisia sakkoja on kahden tasoisia. Suuremmat sakot voivat olla korkeintaan 20 miljoonaa euroa tai 4% yrityksen liikevaihdosta. Suuremmat sakot voidaan määrätä yritykselle, mikäli henkilötietoja on käsitelty ilman lainmukaisia perusteita, rekisteröidyn oikeuksia on rikottu tai henkilötietoja on siirretty kolmanteen maahan asetuksen vastaisesti. Rekisterinpitäjän muiden velvollisuuksien rikkomisesta voidaan määrätä sakko, joka on enintään 10 miljoonaa euroa tai 2% yrityksen liikevaihdosta. Huomioitavaa on, että tietoturvaloukkaus ei itsessään ole sakon peruste, vaan tietoturvatöiden toteuttamatta jättäminen on, vaikka loukkausta ei tapahtuisikaan. (CastilSecin www-sivut 2019) Mikäli kyseessä on vähäinen rikkominen tai määrättävä sakko olisi luonnolliselle henkilölle kohtuuton raskaus, voidaan hallinnollisen sakon sijasta antaa varoitus tai huomautus asiaan liittyen olosuhteiden konkreettisen arvioinnin perusteella. (Korpisaari ym. 2018, 537)

7.3 Vahingonkorvausvastuu

Mikäli tietosuoja-asetuksen rikkomisesta aiheutuu rekisteröidylle aineellista tai aineetonta vahinkoa, rekisterinpitäjällä tai henkilötietojen käsittelijällä on velvollisuus maksaa korvaus aiheutuneesta vahingosta. Korvauksen maksuvelvollisuus on yrityksellä, joka on vastuussa vahingon aiheuttamisesta. Henkilötietojen käsittelijänä toiminut yritys on vastuussa vahingoista vain siinä tapauksessa, jos se ei ole noudattanut nimenomaan henkilötietojen käsittelijöille asetettuja tietosuoja-asetuksen velvoitteita tai mikäli yritys on toiminut rekisterinpitäjän lainmukaisen ohjeistuksen ulkopuolella tai sen vastaisesti. (Hanninen ym. 2017, 130-131)

Useamman yrityksen ollessa vastuussa käsittelystä aiheutuneesta vahingosta, kukin yritys on vastuussa koko vahingosta suhteessa vahingon kärsineeseen rekisteröityyn. Joten tällaisessa tapauksessa, rekisteröity voi vaatia koko korvausta yhdeltä yritykseltä, joka on vastuussa vahingosta. Yhden yrityksen maksaessa täysi korvaus vahingosta rekisteröidylle, vaikka vahingon aiheuttamisesta on vastuussa useampi yritys, on täyden korvauksen maksaneella yrityksellä oikeus periä muilta yrityksiltä se osuus korvauksesta, joka vastaa niiden vastuulla olevaa osuutta aiheutuneesta vahingosta. (Hanninen ym. 2017, 131)

7.4 Rikosoikeudellinen vastuu

Tietosuojalainsäädäntöä koskeva seuraamusjärjestelmä muuttuu perustavanlaatuisesti tietosuoja-asetuksen sisältämien hallinnollisten sakkojen seurauksena. Jatkossa rikosoikeudellinen vastuu tulee kyseeseen vain niissä tilanteissa, joissa lainvastainen henkilötietojen käsittely ei ole hallinnollisten sakkojen piirissä. Tämä tarkoittaa käytännössä sitä, että aikaisempaa henkilörekisteririkosta koskeva säännös korvataan tietosuojarikosta koskevalla säännöksellä. (Hanninen ym. 2017, 131)

Tietosuoja-rikoksesta on kyse, kun henkilö, joka ei ole rekisterinpitäjä tai henkilötietojen käsittelijä tahallaan tai törkeästi huolimattomuudesta hankkii henkilötietoja ilman oikeaa käyttötarkoitusta, siirtää henkilötietoja tai luovuttaa henkilötietoja vastoin tietosuoja-asetusta. Tämän seurauksena todennäköisesti loukataan rekisteröidyn yksityisyyden suojaa tai aiheutetaan rekisteröidylle muuta vahinkoa tai olennaista haittaa. Tietosuoja-rikokseen voi syyllistyä esimerkiksi työntekijä, joka uteliaisuuttaan tutkii rekisteröidyn tietoja, vaikka hänellä ei ole oikeutta niitä käsitellä. Lisäksi tietosuoja-rikoksesta voi olla kyse, kun toimitaan vastoin sitä, mitä tietosuoja-asetuksessa on säädetty henkilötietojen käsittelyn turvallisuudesta. Esimerkiksi tilanne, jossa työntekijä heittää pois henkilörekisteristä tulostettuja asiakirjoja huolehtimatta niiden tietoturvalisesta hävittämisestä. (Hanninen ym. 2017, 131-132)

Henkilö, joka tahallaan hankkii henkilötietoja niiden käyttötarkoituksen kanssa yhteensopimattomalla tavalla, luovuttaa henkilötietoja tai siirtää henkilötietoja vastoin asetusta ja siten loukkaa rekisteröidyn yksityisyyden suojaa, on rikoslain mukaan tuomittava tietosuoja-rikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. (Rikoslaki 39/1889, 38 luku 9 §)

8 YHTEENVETO JA POHDINTA

Tietosuoja-asetuksen täytäntöönpano aiheutti paljon lisätyötä varsinkin pienemmille yrityksille, sillä pienemmissä yrityksissä tietosuojaa ei ole aiemmin huomioitu ainaakaan asetuksen velvoittamalla laajuudella. Sen lisäksi tietosuoja-asetukseen valmistautuminen oli osittain haastavaa, sillä tietosuoja-asetukseen liittyvää tietoa ja ohjeistusta julkaistiin hitaalla aikataululla. Esimerkiksi toimeksiantosopimusten sopimus pohja oli valmis vasta keväällä 2018, joka aiheutti ainakin toimeksiantajalle huolta. Kaikesta huolimatta tilitoimisto X:ssä valmistautuminen tietosuoja-asetukseen sujui aikarajojen puitteissa ja kaikki oli tietosuoja-asetuksen määräysten mukaisesti kunnossa 25.5.2018 mennessä. Suuri kiitos tästä kuuluu myös tilitoimisto X:n IT kumppanille, joka auttoi tilitoimistoa tietoturva-asioissa.

Tämän työn tavoitteena oli selvittää minkälaisia muutoksia tietosuoja-asetus toi mukanaan henkilötietojen käsittelyyn sekä miten tietosuoja-asetukseen pystyttiin varautumaan. Näitä kysymyksiä tarkasteltiin tilitoimisto X:n näkökulmasta eli miten tietosuoja-asetukseen oli varauduttu juuri tilitoimisto X:ssä sekä miten muutokset vaikuttivat tilitoimiston toimintaan. Opinnäytetyö toteutettiin kvalitatiivisena tutkimuksena, jonka lisäksi haastateltiin tilitoimisto X:n toimitusjohtajaa, joka kuvaili henkilökohtaisesti tietosuoja-asetuksen tuomat muutokset sekä siitä aiheutuneet valmistelut. Työn tuloksena selvisi, että tietosuoja-asetuksen aiheuttamat suurimmat muutokset liittyvät rekisteröidyn oikeuksien laajenemiseen, rekisterinpitäjän lisääntyneisiin velvollisuuksiin sekä mahdollisiin sanktiouhkiin.

Tietosuoja-asetus vei paljon aikaa toimeksiantajalta sekä aiheutti paljon ylimääräistä oheistyötä, sillä kaikki tiedot täytyi dokumentoida ja jokaisen asiakkaan toimeksiantosopimus täytyi tehdä uudestaan. Toimeksiantosopimusten tekeminen jäi pääasiassa toimitusjohtajan vastuulle. Lisäksi asiakkaat kävivät vilkkaasti toimistolla allekirjoittamassa uusia sopimuksia sekä tunnistautumassa, joka vei paljon työskentely aikaa.

Opinnäytetyön kirjoittaminen oli haastavaa, sillä en ole aiemmin kirjoittanut vastaavanlaisia laajoja tekstejä, jossa tietoa täytyy jatkuvasti kerätä kirjoista ja luotettavista internet lähteistä. Esimerkiksi haastattelu oli minulle täysin uusi kokemus, sillä minulla ei ollut aikaisempaa kokemusta haastattelemisesta. Haastattelu sujui kuitenkin mielestäni hyvin sekä kokemuksena haastattelu oli positiivinen kokemus. Itsenäinen työskentely osoittautui hieman haastavaksi, sillä opinnäytetyötä tehdessä olin koko ajan työsuhteessa, joten aikaa ei tuntunut riittävän aina opinnäytetyön tekemiselle. Opinnäytetyön tekeminen työsuhteen ohessa saattoi olla osa syynä, minkä takia opinnäytetyön valmistuminen venyi hieman tavoitellusta aikataulusta. Lisäksi työtä tehdessä mietitytti riittävän aineiston saaminen. Opinnäytetyön ansioista kehityin ainakin tiedonhaussa sekä tiedon tarpeellisuuden arvioinnissa.

Tietosuoja-asetus säädettiin pohjimmiltaan parantamaan ihmisten luottamusta verkosta löytyviin palveluntarjoajiin, heidän suorittamaansa henkilötietojen käsittelyyn sekä parantamaan digitaalisten palveluiden tarjoamista yli kansallisten rajojen. Tämän seurauksena yritysten kannattaisi ottaa asetus sekä sen mukana tulleet muutokset ja haasteet vastaan avoimin ja positiivisin mielin, sillä asetuksen voimaantulolla on todennäköisesti paljon enemmän positiivisia kuin negatiivisia vaikutuksia yrityksille.

LÄHTEET

Andreasson A., Riikonen J. & Ylipartanen A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Tallinna: Printon.

Andreasson A., Ylipartanen A. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. Viitattu 12.8.2019. <https://opitietosuoja.fi>

CastilSecin www-sivut 2019. Viitattu 4.9.2019. <http://castilsec.fi>

Euroopan Parlamentin ja neuvoston asetus (EU) 2016/679. Viitattu 26.8.2019. <https://eur-lex.europa.eu>

GDPR www-sivut 2016. Viitattu 12.10.2019. <https://gdpr.fi>

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

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. uud. p. Helsinki: Tammi.

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

Rikoslaki 19.12.1889/39 muutoksineen.

Sulin I. Yleinen tietosuoja-asetus 2017. Viitattu 23.9.2019. <https://www.kuntaliitto.fi>

Tietosuojalaki 5.12.2018/1050 muutoksineen.

Tietosuojavaltuutetun toimisto. 2019. Henkilötietojen käsittely yhdistystoiminnassa. Viitattu 9.9.2019. <https://tietosuoja.fi>

Tietosuojavaltuutetun toimisto www-sivut 2019. Viitattu 21.8.2019. <https://tietosuoja.fi>

Leppä-Lukkala L, 2019. Toimitusjohtaja, Tilitoimisto X. Forssa. Henkilökohtainen haastattelu 5.9.2019. Haastattelijana Waltteri Vehmanen. Muistiinpanot haastattelijan hallussa.

HAASTATTELU

- 1) Millaisilla toimenpiteillä valmistauduttiin tietosuoja-asetukseen?
- 2) Milloin tietosuoja-asetukseen aloitettiin valmistautua?
- 3) Mitä asiakkaille on informoitu tulevista muutoksista?
- 4) Minkälaisia muutoksia asetus sai aikaan sopimuskäytäntöihin?
- 5) Minkälaista perehdytystä henkilökunta on saanut tietosuoja-asetuksesta?
- 6) Minkälaisia keinoja käytetään rekisterien suojaamiseen?
- 7) Kuinka paljon tietosuoja-asetus aiheutti oheistyötä?
- 8) Osoittautuiko mikään haasteelliseksi muutosten toteuttamisessa?