Hanna Niemi

EU:N TIETOSUOJA-ASETUKSEN MUUTOSTEN VAIKUTUKSET TILITOIMISTOSSA

Liiketalouden koulutusohjelma
2018

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

EU:N TIETOSUOJA-ASETUKSEN MUUTOSTEN VAIKUTUKSET TILITOIMISTOSSA

Niemi, Hanna
Satakunnan ammattikorkeakoulu
Liiketalouden koulutusohjelma
Huhtikuu 2018
Sivumäärä: 27
Liitteitä: 1

Asiasanat: tietosuoja, henkilötiedot, tilitoimistot

Opinnäytetyössä tutkittiin toukokuusta 2018 lähtien voimaan tullutta EU:n tietosuoja-asetusta. Tavoitteena oli koota yhteen tietosuoja-asetuksen keskeisimmät muutokset tilitoimiston näkökulmasta. Tutkimus toteutettiin kvalitatiivisena tutkimuksena ja työn toimeksiantajana toimi Tili-Seno Oy.

Tilitoimistossa käsitellään henkilötietoja päivittäin, joten on tärkeää tietää miten tietosuoja-asetus muuttaa henkilötietojen käsittelyä. Tietosuoja-asetuksessa on samoja velvoitteita kuin nykyisessä henkilötietolaissa, mutta se sisältää myös paljon uusia asioita, jotka on huomioitava tietojen käsittelyssä. Mielestäni onnistuin hyvin kokoamaan työhön ne asiat, joita tietosuoja-asetus muuttaa henkilötietojen käsittelyssä.

Tutkimuksessa kävi ilmi, että tietosuoja-asetukseen valmistautuminen on ollut arvioitua hitaampaa. Valmistautuminen oli aloitettava kuitenkin ajoissa, jotta asetusta pystytään noudattamaan oikein. Tietosuoja-asetus pakottaa lähes jokaisen yrityksen tekemään muutoksia henkilötietojen käsittelyyn.

Tietosuoja-asetus vahvisti rekisteröidyn asemaa aiempaa enemmän ja toi lisää vastuita ja velvollisuuksia rekisterinpitäjille. Tietojen käsittelyn tulisi olla aina asianmukaista ja olennaista. Yritysten tulisi myös pystyä todistamaan dokumentoinnin avulla, että tietosuoja-asetusta noudatetaan oikein. Opinnäytetyössä tutkittiin myös sitä, mitä seurauksia tietosuoja-asetuksen laiminlyömisestä voi seurata.

EFFECTS OF CHANGES IN EU'S DATA PROTECTION REGULATION ON ACCOUNTANCY FIRM

Niemi, Hanna
Satakunta University of Applied Sciences
Degree Programme in Business Administration
April 2018
Number of pages: 27
Appendices: 1

Keywords: data prodection, personal data, accountancy firms

In the thesis EU's General Data Protection Regulation valid from May 2018 was studied. The aim was to gather the essential changes of the data protection regulation from an accountancy firm's point of view. The research was conducted as a qualitative study and the client for the work was Tili-Seno Oy.

Personal data is handled in the accountancy firm on a daily basis, so it is important to know how the data protection regulation changes the handling of personal data. The data protection regulation includes the same obligations as the current personal data act, but it also includes many new things, which have to be considered when handling information. In my opinion, I succeeded well in gathering those things in my thesis, which will be changed in handling personal data.

It became clear in the study that preparing for the data protection regulation has been slower than anticipated. Preparations had to be started in good time though to be able to follow the regulation correctly. The data protection regulation forces almost every company to change the handling of personal data.

The data protection regulation reasserted the state of a registered more than before and brought more responsibilities and obligations to register keepers. The data handling should always be appropriate and relevant. The companies should also be able to verify with documentation that the data protection regulation is followed correctly. The thesis also studied what consequences may follow when neglecting the data protection regulation.

SISÄLLYSLUETTELO

1 JOHDANTO

Opinnäytetyö käsittelee EU:n uudistuvan tietosuoja-asetuksen (EU) 2016/679 muutoksia tilitoimistossa. Aihe on ajankohtainen, sillä EU:n yleinen tietosuojauudistus hyväksyttiin keväällä 2016. Kahden vuoden siirtymäaika loppuu toukokuussa 2018, jolloin asetusta tulee noudattaa. Tietosuoja-asetuksen myötä lähes jokaisen yrityksen on tehtävä muutoksia tietojen käsittelyyn, jotta asetusta noudatetaan oikein. Työni toimeksiantajana toimii Tili-Seno Oy, jossa tein viiden kuukauden työharjoitteluni ja sain myös idean tähän aiheeseen harjoitteluni ohjaajalta.

Opinnäytetyö on rajattu tarkastelemaan tietosuoja-asetuksen keskeisimpiä muutoksia ja olennaisimpia asioita tilitoimiston näkökulmasta. Työssä käydään läpi myös jo käytössä olevia käsitteitä ja periaatteita, jotka ovat sovellettavissa tämän hetkisessä lainsäädännössä, sillä niiden merkitys muuttuu tietosuoja-asetuksen myötä.

Työ on kvalitatiivinen tutkimus, jossa on koottuna yhteen tietosuoja-asetuksen muutokset, jotka koskevat henkilötietojen käsittelyä ja mitä sanktioita asetuksen laiminlyönnistä voi seurata. Opinnäytetyön tavoitteena on ohjeistaa toimeksiantajaa tulevista muutoksista ja tarjota vaihtoehtoja muutosten toteuttamiseen. Teorian aineisto on hankittu pääasiassa netin ja kirjojen kautta. Tietoa löytyy paljon myös viranomaisten oppaista ja ohjeistuksista. Haastattelin Tili-Seno Oy:n toimitusjohtaja Sole Jänttiä teemahaastattelun menetelmin, jolloin keskustelimme asetuksen haasteista ja miten tuleviin muutoksiin on valmistauduttu. Työssä käsitellään paljon lainsäädäntöä ja pyrin keskittymään niihin osa-alueisiin, jotka koskevat rekisterien käsittelyä sekä niiden valvontaa. (Vilkka & Airaksinen 2003, 63)

2 TIETOSUOJA-ASETUS JA LAINSÄÄDÄNTÖ

2.1 Taustaa

Suomen ja Euroopan tietosuojalait uudistuvat ja EU:n yleistä tietosuoja -asetusta sovelletaan 25.5.2018 alkaen kaikissa EU:n jäsenvaltioissa. Tietosuoja -asetusta sovelletaan lähtökohtaisesti kaikkien henkilötietojen käsittelyyn ja sitä täsmennetään sekä täydennetään lainsäädännöllä. (Tietosuojavaltuutetun toimisto 2017) Asetus korvaa henkilötietodirektiivin (95/46/EY), joka annettiin vuonna 1995. Sen myötä päivitetään ja nykyaikaistetaan tietosuojadirektiivin periaatteita. Tietosuoja-asetukseen sisältyy mm. säännökset henkilötietojen käsittelyä koskevista periaatteista, käsittelyn laillisuudesta, rekisteröidyn suostumuksen edellytyksistä ja arkaluonteisten tietojen käsittelystä. Uudistus velvoittaa rekisterinpitäjiä ja tarkistamaan tietosuojakäytäntöjen lainmukaisuuden. Myös tietoturvan riittävyys ja ongelmatilanteisiin varautuminen on syytä tarkistaa. (Andreasson ym. 2016, 35)

Tietosuoja-asetus tuo täsmennyksiä jo voimassa olevaan lainsäädäntöön sekä tuo myös täysin uusia velvoitteita ja sanktioita. Asetuksessa on lueteltu henkilötietojen käsittelyn kohteena olevan rekisteröidyn oikeudet. Esimerkiksi oikeus tulla unohdetuksi, oikeus tietojen poistamiseen tai niiden oikaiseminen ovat uusia rekisteröidyn oikeuksia. Rekisteröidyllä on oikeus saada itseään koskevat tiedot koneluettavassa muodossa sekä oikeus siirtää tiedot toiseen järjestelmään, kun tietojen käsittely perustuu suostumukseen tai sopimukseen. Lisäksi säädetään rekisterinpitäjien velvollisuudesta antaa rekisteröidylle avoimia ja helposti saatavia tietoja käsittelyprosessista. (Andreasson ym. 2016, 38)

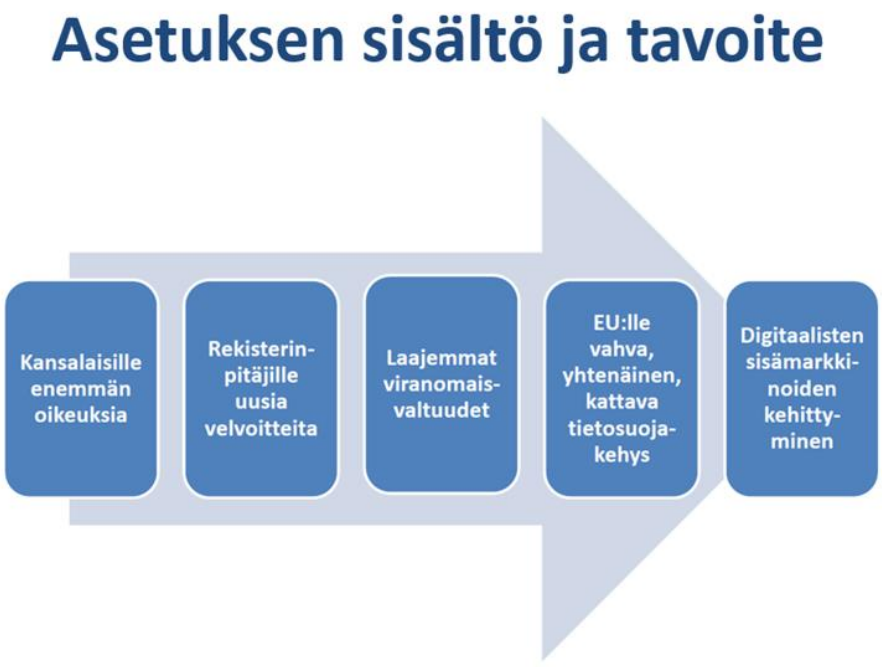
Henkilötietojen käsittelijöiden vastuut on määritelty tarkemmin tietosuoja-asetuksessa ja tämä koskee erityisesti rekisterinterinpitäjiä sekä myös rekisterinpidossa avustavien käsittelijöiden osalta. Organisaatiolle ei enää riitä se, että asetusta noudatetaan, joten on pystyttävä todistamaan, että asetusta noudatetaan oikein. Tietoturvaloukkauksista ilmoittaminen tulee pakolliseksi ja organisaatioiden on nimettävä tietosuojavastaava julkisella sektorilla. Yrityksille tietosuojavastaavan nimeäminen on pakollista, kun

päätoiminnassa seurataan henkilötietoja laajassa mittakaavassa tai käsittelyn kohteena on arkaluonteisia tietoja. (Andreasson ym. 2016, 39)

Tietosuoja-asetuksessa säädetään tietosuojaviranomaisen toimivallasta, tehtävistä ja valtuuksista. Tietosuojaviranomaisella on toimivalta oman jäsenvaltionsa alueella. Valvontaviranomaisella on valtuudet langettaa hallinnollisia seuraamuksia määräämällä sakkoja tapauksien olosuhteet huomioon ottaen. (Andreasson ym. 2016, 39)

2.2 Tavoitteet

EU:n yleisen tietosuoja-asetuksen tavoitteina ovat yksilön oikeuksien vahvistus, lujittaa sisämarkkinaoikeutta, huomioida tietosuojan globaali ulottuvuus ja tehostaa tietosuojasääntöjen täytäntöönpanon valvontaa. Asetuksella pyritään myös luomaan EU:lle ajanmukainen, vahva, yhtenäinen sekä kattava kehys tietosuojalle. Lisäksi tarkoituksena on parantaa luottamusta online -palveluihin ja sen avulla edistää EU:n digitaalista sisämarkkinoiden kehittämistä. (Andreasson ym 2016, 35) Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten. Käsittely vaatii asianomaisen henkilön suostumuksen tai laissa säädetyn perusteen tietojen käsittelyyn. (Andreasson ym. 2017, 29)



kuva 1. Asetuksen sisältö ja tavoite (opitietosuojaa.fi 2018)

2.3 Henkilötietolaki (22.4.1999/523)

Henkilötietolaki on tietosuojaa koskeva yleislaki, joka tuli voimaan vuonna 1.6.1999. Se korvasi henkilörekisterilain ja -asetuksen, joissa määriteltiin yleiset tietosuojaperiaatteet tilanteissa, joissa henkilötietoja käsitellään. Samat periaatteet sisältyvät myös henkilötietolakiin. Henkilötietolailla saatettiin voimaan myös Euroopan unionin henkilötietodirektiivin määräykset. Henkilötietoja käsiteltäessä on noudatettava sitä, mitä henkilötietolaissa on säädetty. Toissijaisuuden mukaisesti henkilötietolaki väistyy, mikäli muussa laissa jokin henkilötietojen käsittelyä koskeva asia on järjestetty henkilötietolaista poikkeavalla tavalla. (Andreasson ym. 2016, 34)

Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietojen käsittelyssä sekä pyrkii edistämään hyvän tietojenkäsittelytavan kehittämistä ja sen noudattamista. (Henkilötietolaki 1 luku 1§) Lain säännöksiä tulee soveltaa kaikkeen henkilötietojen käsittelyyn, ellei muissa laeissa ole mainittu vastaavia erityissäännöksiä. Henkilötietolailla on myös saatettu voimaan Euroopan Unionin henkilötietodirektiivi. (Tietosuojavaltuutetun toimisto www-sivut)

3 VELVOITTEISIIN VALMISTAUTUMINEN

Muutoksiin varautuminen on hyvä aloittaa rekisterien nykytilan arvioimisella, jossa selvennetään esimerkiksi se, mistä henkilötietoja hankitaan, miten niitä käsitellään ja mihin niitä voidaan mahdollisesti luovuttaa. Nykyisen tilanteen pohjalta tehdään ratkaisuja siihen mitä muutoksia tulee tietosuoja-asetuksen johdosta tehdä. Lähes kaikissa tapauksissa jonkinlaiset muutokset ovat tarpeellisia. Yrityksien tulisi arvioinnissaan lähteä liikkeelle riskilähtöisesti, sillä se on myös asetuksen lähtökohtana. Rekisterinpitäjä ja henkilötietojen käsittelijä ovat velvollisia tekemään arvioita henkilötietojen käsittelyyn liittyvistä riskeistä ja valitsemaan riskitason mukaan vaadittavat

hallintatoimenpiteet. Tietojen käsittelyn on aina oltava suunnitelmallista. (Hanninen ym. 2017)

3.1 Vaikutustenarviointi

Tietosuoja-asetuksen keskeisimpiä vaatimuksia on riskienarvioinnista seuraava vaikutustenarviointi. Asetus määrää vaikutuksenarvioinnin pakolliseksi sellaisille henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa saattaa olla todennäköistä, että käsittelytoimintoihin liittyy riskejä, jotka koskevat yksilöiden oikeuksia ja vapauksia. Yritysten tulee ottaa huomioon käsiteltäessä harjoittamiensa henkilötietojen luonne, laajuus, asiayhteys ja tarkoitukset sekä myös luonnosten henkilöiden vapauksiin kohdistuvat riskit. Niiden pohjalta on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja osoitetaan että asetusta noudatetaan oikein. Teknisiä ja organisatorisia toimenpiteitä ovat mm.: henkilöstön koulutus, käsittelyyn annetut ohjeet ja määräykset, salassapitosopimukset sekä tilojen, laitteiden ja ohjelmistojen käytönvalvonta. Toimenpiteitä tulee myös päivittää ja tarkastaa aina tarvittaessa. Jokaisen yrityksen on tehtävä arvio omasta toiminnastaan ja mahdollisista tietosuojaan liittyvistä riskeistä sekä sopeutettava ja suunniteltava tietojen käsittely niiden mukaisesti. (Hanninen ym. 2017)

Dokumentoinnin merkitys korostuu selvästi nykytilaan verrattuna. Henkilörekisterin ylläpidon on oltava suunnitelmallista ja dokumentoitua. Tämä tarkoittaa sitä, että yrityksen on pystyttävä todistamaan, että tietoja on käsitelty lainmukaisesti. Pelkän asetuksen noudattaminen ei enää riitä ja rekisterinpitäjän on pystyttävä osoittamaan, miten tietosuojavelvollisuudet on toteutettu teknisin, organitorisin ja hallinnollisin toimenpitein. (Hanninen ym. 2017). Käytännössä esimerkiksi palkanlaskennan osalta tilitoimiston tulisi käydä läpi koko palkanlaskennan prosessi, miten tietojen välitys aiotaan toteuttaa, liittymät, järjestelmien sekä hakemistojen käyttöoikeudet. Prosessia ja dokumentaatiota tulee myös tarkastella kohtuullisin väliajoin. (Männistö 2017)

3.2 Tietotilinpäätös

EU:n tietosuoja-asetukseen valmistauduttaessa tietotilinpäätöstä voi hyödyntää työkaluna. Sen käyttöä voidaan soveltaa myös henkilötietojen haltuunottoon, sekä auttaa myös osoitusvelvollisuuden toteuttamisessa. Sen tarkoituksena on yhdistellä organisaation osat ja ihmisten osaaminen sekä kuvata se tavalla, jota kaikki pystyvät hyödyntämään. Tietosuojan toteuttaminen on kuitenkin prosessi, joka jatkuu koko ajan ja tietotilinpäätös on nimensä mukaisesti tietotilinpäätöshetken tilanne. Tietotilinpäätöksen voisi sitoa esimerkiksi organisaation vuosikelloon, niin että ajantasainen tietotilinpäätös on mahdollista liittää taloudellisen tilinpäätöksen mukaan ikään kuin liitteeksi. (Heiskanen 2017)

Tietotilinpäätöksen teko vaatii paljon työtä ja organisaation sisäistä yhteistyökykyä. Sen tekoon on varattava paljon aikaa, koska jokainen organisaation henkilötietoja käsittelevä prosessi on kuvattava, tarkasteltava ja dokumentoitava erikseen. Laajuuteen vaikuttaa mm. liiketoiminnan luonne, koko ja sen vaikutukset tietosuojalle, verkkopalveluihin liittyvät prosessit ja dokumentointi, tietosuojan alaista tietoa käsittelevät prosessit ja järjestelmät, tietosuojaan liittyvät ohjeistukset sekä henkilötietojen käsittelyyn liittyvien sopimusten tarkastelu. Tietotilinpäätöksen tarkoitus on luoda analysoidut dokumentit ja ohjeistukset, analysoidut henkilötietoja käsittelevät prosessit ja niihin liittyvät tietojärjestelmät, tietovarannot ja tietovirrat, kehittämissuunnitelma ja varmistaa suunnittelun eteneminen. (Heiskanen 2017) Tietotilinpäätös raportoi mitkä ovat organisaation heikkoudet ja vahvuudet. Sen tarkoituksena on kuvata yrityksen tietojen laatua, niiden käytettävyyttä, tietoturvaa, tiedon valvontaa ja mitä tietovarantoja organisaatiolla on halussaan. (Andreasson ym 2016, 146)

Tietosuojavastaavalla on keskeinen asema tietotilinpäätöksen laadintaan liittyvässä koordinoinnissa ja tunnuslukujen sekä mittarien kehityksessä. Tietotilinpäätöksen avulla on helpompi seurata tunnuslukuja, jotka liittyvät organisaation tietojen käsittelyyn. Tietotilinpäätöstä laadittaessa tulisi pohtia mitä mittareita ja tunnuslukuja siihen otetaan mukaan, kuka tietotilinpäätöksen tekee ja miten, kuinka usein se laaditaan, missä tietotilinpäätöksen käsittely suoritetaan ja miten havaitut puutteet korjataan. (Andreasson ym 2016, 146)

3.3 Informointi

Tietosuoja-asetuksen informointikäytännöt poikkeavat osittain henkilötietolain tietojen käsittelystä. Tässä kappaleessa on kuvattu tulevat muutokset, jotka tulee ottaa huomioon tietosuoja-asetuksen tullessa voimaan. (Tietosuojavaltuutetun toimisto 2018)

Rekisteröidylle tulee antaa tiedot niistä tarkoituksista, joita varten käsitellään sekä mihin tietosuoja-asetuksen artiklaan käsittely perustuu. Käsittelyn oikeutetut edut on tunnistettava ja yksilöitävä sekä hyvän henkilötietojen käsittelytavan edistämiseksi rekisterinpitäjän tulisi tarjota ennakkoon tasapainotestiä, joka tulee tehdä, jotta rekisterinpitäjä voi vedota käsittelyn oikeusperusteeseen. (Tietosuojavaltuutetun toimisto 2018)

Tietojen säilytysaika voidaan johtaa laissa määrätyistä säilytysajoista tai toimialojen käytännesäännöistä. Säilyttämisaika tulee olla määriteltynä niin, että rekisteröity voi arvioida itse, mikä on tietojen säilytysaika tietyissä tarkoituksissa. Ei siis pelkästään riitä, että henkilötietoja säilytetään niin kauan kuin on tarpeellista laillisten tarkoitusten saavuttamiseksi. Erilaisille henkilötietoryhmille ja käsittelytarkoituksille tulee määritellä omat säilytysajat. (Tietosuojavaltuutetun toimisto 2018)

Rekisteröityä tulee informoida siitä, miten hänen antamansa suostumus tietojen käsittelyyn voidaan perua. Suostumuksen peruuttamisen tulee olla yhtä helppoa kuin suostumuksen antaminen. Tietosuoja-asetuksen mukaan jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos väitetty tietosuoja-asetuksen rikkominen on tapahtunut. (Tietosuojavaltuutetun toimisto 2018)

Rekisteröidyn tulisi olla tietoinen siitä, onko henkilötietojen antaminen lakisääteinen tai vaatimus, joka perustuu sopimuksen tekemiseen sekä tuleeko rekisteröidyn toimittaa henkilötiedot. Selosteesta tulee myös käydä ilmi seuraukset tarvittavien tietojen antamatta jättämisestä. Esimerkiksi työsuhteessa voi olla sopimukseen perustuva vaatimus antaa tiettyjä tietoja työnantajalle. Informointi vaadittavista pakollisista tiedoista tulee olla selkeää. Rekisteröidyllä on myös oikeus saada tiedot siitä, mistä häntä koskevat henkilötiedot on saatu. Esimerkiksi onko tiedonlähteenä julkisesti vai yksityisesti ylläpidetty tietolähde, sekä mikä organisaatio on kyseessä, sen toimiala tai sektorin tyyppi. Nimenomainen tietolähde tulee mahdollisuuksien mukaan tarjota, sekä tieto

siitä mistä tieto on peräisin (esim. EU tai ei-EU). (Tietosuojavaltuutetun toimisto 2018)

4 TILI-SENO OY

4.1 Yritysesittely

Tili-Seno Oy on täyden palvelun auktorisoitu tilitoimisto, jolla on toimipiste Turun lisäksi myös Kaarinassa. Yritys on toiminut alalla jo 30 vuotta. Jokainen henkilöstöstä tekee yritysten kirjanpitoa ja osa laskee palkkoja. Yrityksessä on erikoisasiantuntijoita verotuksen, kirjanpidon, perinnän, rahoituksen, budjetoinnin, yritysjärjestelyn alueella ja henkilökunnan jäsenet ovat erikoistuneet eri aiheisiin. Tili-Seno Oy tarjoaa kokonaisvaltaista tietämystä yrittäjyyden osa-alueilla. Asiakkaina on sekä pieniä että suuria yrityksiä eri liiketoiminnan aloilta. (Tili-Seno Oy:n www-sivut 2018)

4.2 Nykytilan kartoitus ja muutoksiin valmistautuminen

Opinnäytetyön toimeksiantaja on jo tehnyt kartoituksen tietojen käsittelyn nykytilanteesta. Excel-taulukossa on listattu kuvaus toiminnoista, jossa yritys toimii rekisterinpitäjänä. Näitä toimintoja ovat: asiakasrekisteri, toimittajarekisteri, palkanlaskenta, työssä oppijoiden tiedot, Facebook, Google Analytics ja sähköpostilista asiakkaista. Taulukossa on määritelty toimintojen käsittelyn tarkoitus, oikeusperuste ja kuvaus rekisteröityjen eri kategorioista. Näiden lisäksi taulukossa on kuvattu käsiteltävät henkilötiedot, missä järjestelmässä tieto sijaitsee, henkilö joka on vastuussa käsittelystä ja missä maassa tieto sijaitsee. (Jäntti henkilökohtainen tiedonanto 6.3.2018)

Yrityksen asiakkaita on informoitu muutoksista sähköpostitse, johon on liitetty linkki tietosuoja-asetuksen oppaaseen ja heille on tehty video, joka käsittelee perusteellisesti tietosuoja-asetusta. Tämän lisäksi asiakkaita on ohjeistettu ottamaan yhteyttä omaan kirjanpitäjäänsä asetukseen liittyvissä kysymyksissä. Asiakkaille tarjotaan myös tarkempaa koulutusta ja ohjausta asetukseen liittyen. Heille järjestetään infotilaisuus,

jossa perehdytään paremmin tuleviin muutoksiin. (Jäntti henkilökohtainen tiedonanto 6.3.2018)

Nykytilan tunnistamisen jälkeen on hyvä laatia tietosuoja-asetuksen vaatimuksia varten tietosuojasuunnitelma, jota toteutetaan siirtymäajalla ennen asetuksen voimaan tuloa. Suunnitelman avulla valmistaudutaan toteuttamaan tietosuoja-asetuksen vaatimukset. Tili-Seno Oy:ssä on vielä tehtävä tietojen poistoa varten prosessikaavio, joka liittyy asetuksessa määriteltyyn tietojen säilytyksen rajoittamiseen. (Jäntti henkilökohtainen tiedonanto 6.3.2018) Säilytyksen rajoittamisen periaate velvoittaa rekisterinpitäjää tekemään kriteerit tietojen säilyttämistä varten. On tärkeää huomioida myös mahdolliset lakisääteiset velvollisuudet tietojen säilyttämiseen ja niiden hävittämiseen. Tietojen säännöllinen tarkastelu ja se, mitä tietoja voidaan säilyttää ja kuinka kauan, tulee varmasti olemaan yksi vaikeimmista asioista tietosuoja-asetuksen noudattamisessa. (Harjunheimo 2017)

5 HENKILÖTIETOJEN KÄSITTELY

5.1 Rekisterinpitäjän yleiset periaatteet

Tietosuoja-asetuksessa säädetään henkilötietojen käsittelyä koskevista periaatteista, joiden avulla rekisterinpitäjä tekee käsittelyn tavalla, joka kunnioittaa rekisteröidyn oikeuksia ja vapauksia. (Oikeusministeriö & Tietosuojavaltuutetun toimisto 2017) Tietojen käsittelyn on perustuttava johonkin lailliseen perusteeseen, kuten asiakas- tai työsuhteeseen perustuvaan oikeutettuun etuun. Tämän lisäksi henkilötietojen käsittelyn tulee tapahtua lainmukaisesti eli tietosuoja-asetusta ja muita lakeja noudattaen, jotka liittyvät henkilötietojen käsittelyyn. (Hanninen ym. 2017)

Läpinäkyvyyden vaatimus tarkoittaa sitä, että rekisteröidyn tulisi olla selvillä siitä, miten ja kuinka paljon heitä koskevia henkilötietoja kerätään, käsitellään ja aiotaan käsitellä. Tietojen käsittelystä tulee viestiä rekisteröidyille ymmärrettävästi selkeää ja yksinkertaista kieltä käyttäen. Tiedon tulee myös olla helposti rekisteröityjen saatavilla. (Hanninen ym. 2017) Rekisterinpitäjällä tulee olla laillinen peruste henkilötietojen

käsittelyyn. Asetuksessa on määritelty lailliset käsittelyperusteet, joita voivat olla esimerkiksi rekisterinpitäjän oikeutettu etu, rekisteröidyn antama suostumus tai lakisääteinen tehtävä. Läpinäkyvyyden vaatimus edellyttää rekisterinpitäjää informoimaan rekisteröityjä ymmärrettävällä tavalla henkilötietojen käsittelystä ja mihin käyttötarkoitukseen tiedot on kerätty. (Harjunheimo 2017)

Tietojen käsittelyn on oltava olennaista ja asianmukaista. Käsiteltävien tietojen tulee olla riittäviä, mutta myös rajoituttava siihen, mikä on välttämätöntä tietojen kannalta. Esimerkiksi työnhakijalta voidaan kerätä vain työntekijän valitsemisen kannalta olennaisia tietoja. Asianmukaisen henkilön suostumus tietojen käsittelyyn ei kuitenkaan oikeuta käsittelemään henkilötietoja tarpeettomasti. Tietojen on oltavia täsmällisiä ja niitä on päivitettävä tarpeen mukaan. Yrityksen on pidettävä huolta, että virheelliset ja vanhentuneet tiedot poistetaan viipymättä. (Hanninen ym. 2017) Rekisterinpitäjän on käsiteltävä tietoja lain mukaisesti, noudattaa huolellisuutta ja hyvää tietojen käsittelytapaa. Käsittelyn tulee toimia muutenkin niin, ettei rekisteröidyn yksityisen elämän suojan turvaaviin perusoikeuksiin kohdistu rajoitteita ilman perustetta, joka on säädetty laissa. Velvollisuus koskee myös sitä, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun. (Henkilötietolaki 2 luku 5§)

Henkilötiedot on säilytettävä sellaisessa muodossa, että rekisteröity pystytään tunnistamaan vain niin kauan kuin tietojen käsittelyn toteuttaminen on tarpeellista. Henkilötietoja on käsiteltävä siten, että varmistetaan henkilötietojen asianmukainen turvallisuus ja luottamuksellisuus. Tiedot tulee myös suojata luvattomalta ja lainvastaiselta käsittelyltä sekä häviämiseltä, tuhoutumiselta tai vahingoittumiselta. (Hanninen ym. 2017)

5.2 Henkilötietojen käsittelijä

Henkilötietojen käsittelijä voi olla luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Käsittelijä ei tee päätöstä tietojen keräämisestä tai käyttämisestä vaan sen hoitaa rekisterinpitäjä. Henkilötietoja voi käsitellä ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti. (Hanninen ym. 2017) Esimerkiksi tilitoimisto on henkilötietojen

käsittelijä silloin, kun jokin yritys on ulkoistanut sille palkanlaskennan tai kirjanpidon tekemisen. (Männistö 2017)

Henkilötietojen käsittelijän vastuut kasvavat huomattavasti uudistuvan tietosuoja-asetuksen voimaantulon myötä. Ennen vastuut ja velvoitteet koskivat lähinnä vain tietoturvaan liittyviin edellytyksiin ja sopimusvelvoitteisiin. Henkilötietojen käsittelijän roolin rajat on määriteltävä tarkasti. (Hanninen ym. 2017)

5.3 Osoitusvelvollisuus

Osoitusvelvollisuus edellyttää käsittelyyn liittyvien prosessien ja tietosuoja-asetuksen käytännön toteuttamisen dokumentointia. Vastuun toteuttamiseksi rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että asetusta noudatetaan. Aiemmin on ollut riittävää, että säännöksiä noudatetaan eikä erityistä dokumentointivelvollisuutta ole ollut. (Oikeusministeriö & Tietosuojavaltuutetun toimisto 2017)

Rekisterinpitäjän on tehtävä arvio, mitä tietosuojaperiaatteet käytännössä tarkoittavat ja miten ne käytännössä toteutuvat omassa toiminnassa. Osoitusvelvollisuus edellyttää suunnittelua, varautumista ja vaatii osoittamaan toteutetut toimenpiteet dokumentaation avulla. Yrityksen tulisi koota yhteen omat tietosuojaperiaatteensa ja käytäntönsä siten, että ne ovat helposti löydettävissä ja että niistä voidaan muodostaa kokonaiskuva yrityksen henkilötietojen käsittelystä ja niiden suojaamisesta. (Hanninen ym. 2017)

Yritykset voivat käyttää velvollisuuksien noudattamisen osoittamiseksi tietosuojaa koskevia sertifikaatteja tai käytännesääntöjä. Sertifikaattien tarkoituksena on helpottaa rekisteröidyn tuotteiden ja palveluiden tietosuojan tason arviointia. Alakohtaisilla käytännesäännöillä voidaan helpottaa tietosuoja-asetuksen soveltamista, sillä niissä voidaan huomioida eri aloilla suoritettavat käsittelyiden erityispiirteet ja mm. erikoisten organisaatioiden tarpeet henkilötietojen käsittelyyn liittyen. (Oikeusministeriö & Tietosuojavaltuutetun toimisto 2017) On myös mahdollista käyttää tietotilinpäätöksen ensimmäistä versiota osoitusvelvollisuuden todentamiseen, jos yritys on tehnyt sellaisen. (Heiskanen 2017)

Rekisteröidyn suostumus tarkoittaa mitä tahansa vapaaehtoista, yksilöytyä, tietoisesti tehtyä ja yksiselitteistä tahdon ilmaisua. Tämä voi esimerkiksi olla ruudun rastittaminen paperilomakkeelle tai internetsivulle. Suostumus tarkoittaa sitä, että rekisteröity on antanut luvan henkilötietojensa käsittelyä varten. Rekisterinpitäjällä tulee olla dokumentoituna rekisteröidyn suostumus, koska se pitää osoitusvelvollisuuden mukaan pystyä todentamaan. Suostumus tulee antaa tarkoituksellisesti, joten sitä ei voi antaa vaikenemalla tai valmiiksi rastitetulla ruudulla tai jättämättä jotakin tekemättä. (Holopainen 2018)

5.4 Riskiperusteinen lähestymistapa

Tietosuoja-asetuksessa rekisterinpitäjän velvoitteiden osalta on omaksuttu riskiperusteinen lähestymistapa. Tämä tarkoitta sitä, että tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet tulee suhteuttaa henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Tällä tavalla voidaan välttää matalariskisen toiminnan liiallista sääntelyä ja pyritään suhteuttamaan tarvittavat toimenpiteet kunkin henkilötietojen liittyvän riskin mukaan. (Oikeusministeriö & Tietosuojavaltuutetun toimisto 2017)

Rekisterinpitäjän tulee tehdä perusteellinen arvio riskeistä, jotka liittyvät henkilötietojen käsittelyyn, jotta voidaan toteuttaa tietosuoja-asetuksen sisäänrakennettua ja oletuksen arvoista tietosuojaa. Tietosuoja-asetuksessa riskeillä tarkoitetaan käsittelyn aikana rekisteröidylle mahdollisesti aiheutuvia aineellisia, aineettomia tai fyysisiä vahinkoja esimerkiksi silloin, kun käsittely voi johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudelliseen menetykseen, sosiaaliseen vahinkoon tai pseudonymisoinnin kumoutumiseen. Pseudonymisoiminen on uusi käsite tietojen käsittelyssä. Se tarkoittaa henkilötietojen käsittelemistä niin, ettei tietoja voida enää yhdistää rekisteröityyn käyttämättä lisätietoja. Lisätiedot tulee säilyttää erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla pystytään varmistamaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu. (Hanninen ym. 2017)

5.5 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennettu ja oletusarvoinen tietosuoja on asetuksen yksi keskeisimmistä periaatteista. Sen tarkoituksena on kannustaa yrityksiä uusien ideoiden kehittämiseen toimintatapoja, tekniikoita henkilötietojen turvallisuutta ja suojausta varten. (Tietosuojavaltuutetun toimisto www-sivut 2016) Sisäänrakennetun tietosuojan velvoite edellyttää, että tietosuojaperiaatteita sovelletaan henkilötietojen käsittelyssä. Oletusarvoisen tietosuojan velvoite tarkoittaa sitä, että rekisterinpitäjä käsittelee vain niitä tietoja, jotka ovat käsittelyn kannalta tarpeellisia. Samalla tulee toteuttaa toimenpiteet, joilla varmistetaan, että henkilötietoja ei oletusarvoisesti saateta rajoittamattomalle henkilömäärälle ilman luonnollisen henkilön myönteistä vaikutusta. Molemmat velvoitteet ovat pääosin päällekkäisiä tietosuoja-asetuksen määrittämien muiden velvollisuuksien kanssa ja ne vastaavat pitkälti tietojen käsittelyn huolellisuuden ja suunnittelun velvoitteita. (Sulin 2017)

5.6 Sopimusvaatimukset

Henkilötietojen käsittelijän suorittamaa tiedon käsittelyä on määritettävä sopimuksella. Mikäli rekisterinpitäjä ja henkilötietojen käsittelijä ovat eri tahoja, niiden välinen suhde on määritettävä asetuksen mukaisessa sopimuksessa. Siinä tulee käsitellä mm. käsittelyn tarkoitus ja sen kesto, käsittelyn luonne, minkä tyyppisiä henkilötiedot ovat, rekisteröityjen ryhmät, sekä rekisterinpitäjän velvollisuudet ja oikeudet. (Sulin 2017)

Tietosuoja-asetus määrittelee tarkasti henkilötietojen käsittelijän roolin ja lainsäädännössä olevia velvoitteita on täsmennetty suhteessa henkilötietolain sääntelyyn. Asetuksen mukaan henkilötietojen käsittelijä ei saa esimerkiksi käyttää omia alihankkijoita ilman rekisterinpitäjän suostumusta tai yleistä kirjallista ennakkolupaa. Rekisterinpitäjä voi käyttää vain sellaisia henkilötietojen käsittelijöitä, jotka pystyvät toteuttamaan riittävät suojatoimet teknisten ja organisatoristen toimien käytössä niin, että käsittely on tietosuoja-asetuksen mukaista. Myös oletusarvoisen ja sisäänrakennetun tietosuojan vaatimuksella on vaikutusta sopimuksiin. Rekisterinpitäjällä on velvollisuus määrittää omien henkilötietotoiminnan vaatimukset käytäntöihin. Ehdot on huomioitava sopimuksissa. (Sulin 2017)

Sopimukset joiden kohteena on joko välittömästi tai välillisesti henkilötietojen käsittely, on uudelleenarvioitava asetuksen näkökulmasta mahdollisten muutosten takia. Tämän tyyppisiä sopimuksia voivat olla esimerkiksi palvelujen ulkoistamissopimukset, ostosopimukset, tietojärjestelmiin liittyvät sopimukset, mikäli näissä käsitellään henkilötietoja. (Sulin 2017)

5.7 Loukkausilmoitukset

Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena tapahtuu lainvastainen tuhoaminen, häviäminen, muuttaminen, luovutus luvattomasti tai pääsy tietoihin. Rekisterinpitäjä on velvollinen ilmoittamaan tietoturvaloukkauksista rekisteröidylle ja tietosuojaviranomaiselle. Loukkausta koskeva ilmoitus on tehtävä viranomaiselle mahdollisuuksien mukaisetsi 72 tunnin kuluessa loukkauksen ilmitulosta, riippumatta siitä, onko loukkaus tapahtunut omassa vai käsittelijän toimesta. Ilmoituksen voi jättää tekemättä ainoastaan silloin, kun loukkauksesta ei mahdollisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Henkilötietojen käsittelijän on ilmoitettava viipymättä tietoturvaloukkauksista rekisterinpitäjälle heti saatuaan tiedon. (Sulin 2017)

5.8 Tietosuojavastaavan nimeäminen, asema ja työnkuva

Tietosuoja-asetuksen mukaan tietosuojavastaavan nimittäminen on pakollista silloin, kun kyse on julkisesta sektorista, pois lukien tuomioistuimet. Asetus velvoittaa myös niitä yrityksiä nimeämään tietosuojavastaavan, jos yrityksessä seurataan päätoimisesti henkilötietoja laajassa mittakaavassa tai käsittelyn kohteena on arkaluontoisia tietoja. Tietosuojavastaavan tehtävien laajuus sovitaan erikseen työsopimuksessa ja tehtäväkuvassa. Yleensä tehtäviin kuuluu esimerkiksi omavalvontasuunnitelman ja tietotilinpäätöksen valmistelua. Tietosuojavastaavan tehtäviin voi kuulua myös erilaisia suunnittelu- ja toimeenpanotehtäviä, kuten asiakastietojen käsittelyohjeiden ja eri lomakkeiden laadintaa sekä henkilökunnan kouluttamista. Luvatonta asiakastietojen käsittelyä selvittäessä tietosuojavastaavan rooli on koordinoiva. (Andreasson ym 2016, 57)

Asiakastietojen käsittelyn seurannan ja valvonnan toteuttamisen tulee pohjautua toiminta- ja vuosisuunnitelmaan, jonka vastaava johtaja on hyväksynyt. Tietosuojavastaava voi syyllistyä rikokseen, jos valvonnan suunnitelmista poiketaan tai toimitaan rekisterinpitäjän ohjeiden vastaisesti. Tietosuojavastaavan työ aloitetaan yleensä organisaation nykytilanteen kartoituksella. Ne perusasiat, jotka liittyvät rekisterinpitäjän henkilötietojen käsittelyyn tulee hoitaa ensimmäisenä kuntoon. Tietosuojavastaavan tehtäviin kuuluu tarkistaa henkilötietojen käsittelyn lainmukaisuuden ja korjata mahdolliset puutteet. Organisaatiolle tulee laatia ohjeet ja menettelytavat, jos niitä ei ole vielä tehty. Ne tietojärjestelmät, joita käytetään henkilötietojen käsittelyyn, tulee tarkastaa tietosuojavastaavan toimesta. Tämän lisäksi toimenkuvaan kuuluu antaa koulutusta henkilöstölle koskien lainsäädäntöä, henkilötietojen käsittelyä sekä luoda rutiinit käsittelytapoihin. (Andreasson ym 2016, 58)

6 REKISTERÖIDYN OIKEUDET

EU:n tietosuoja-asetuksessa on lueteltu rekisteröidyn oikeudet. Näitä oikeuksia ovat omia henkilötietoja koskeva tiedonsaantioikeus, oikeus saada tiedot oikaistua, oikeus tulla unohdetuksi sekä oikeus tietojen poistoon ja oikeus vastustaa tietojen käsittelyä. Asetuksessa säädetään myös rekisterinpitäjien velvollisuudesta antaa rekisteröidylle helposti saatavia tietoja siitä, miten henkilötietoja käsitellään. (OpiTietosuojaa.fi www-sivut 2016)

6.1 Pääsy tietoihin ja oikeus siirtää tietoja

Tietosuoja-asetuksessa säädetty rekisteröidyn oikeudesta saada pääsy tietoihin, jonka mukaan rekisteröity on oikeutettu saamaan informaatiota siitä, mitä häntä koskevia tietoja henkilörekisteriin on tallennettu. Rekisteröidyn pyyntöön tulee reagoida kuukauden kuluessa pyynnöstä. Määräaikaa voidaan pidentää kahdella kuukaudella, jos pyynnöt ovat monimutkaisia tai niitä on monia. Rekisterinpitäjän on tässä tapauksessa ilmoitettava rekisteröidylle määräajan jatkumisesta kuukauden kuluessa pyynnön vastaanottamisesta sekä ilmoitettava syyt viivästymiselle. Jos rekisteröidyn pyynnöt ovat

ilmeisen perusteettomia tai kohtuuttomia ja jos niitä esitetään jatkuvasti, rekisterinpitäjä voi kieltäytyä suorittamasta pyydettyä toimenpidettä tai periä kohtuullisen maksun huomioiden tietojen toimittamisesta aiheutuvat hallinnolliset kustannukset. (Harjunheimo 2017)

Jos rekisteröity esittää pyyntönsä sähköisesti, rekisterinpitäjän on pääsääntöisesti annettava tiedot yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity ei toisin pyydä. Rekisteröidyn oikeus saada pääsy tietoihin ei saa vaikuttaa haitallisesti muiden oikeuksiin tai vapauksiin. Tämän arvioiminen jää rekisterinpitäjälle itselleen. Asetuksen mukaan muiden oikeudet ja vapaudet voivat liittyä esimerkiksi tarpeeseen suojata liikesalaisuuksia. (Harjunheimo 2017)

Rekisteröidyn oikeutta siirtää tietoja sovelletaan silloin kun kyse on tietojen automaattisesta käsittelystä. Henkilötietojen tulee myös olla itse rekisteröidyn toimittamia ja tietojen käsittely perustuu suostumukseen tai sopimukseen. Tietojen siirto järjestelmästä toiseen ei saa myöskään vaikuttaa haitallisesti kolmansien osapuolten oikeuksiin tai vapauksiin. Jos nämä ehdot täyttävät, on rekisteröidyllä oikeus siirtää kyseiset henkilötiedot toiselle rekisterinpitäjälle. (Tietosuojavaltuutetun toimisto 2017)

6.2 Vastustamisoikeus ja käsittelyn rajoittaminen.

Rekisteröidyllä on erityiseen tilanteeseen liittyvällä perusteella oikeus vastustaa omien tietojensa käsittelyä, joka perustuu yrityksen oikeutettujen etujen toteutukseen. Rekisteröidyn vastustaessa käsittelyä yritys ei saa käsitellä tietoja, ellei se pysty osoittamaan, että käsittelyä varten on olemassa tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn oikeuden. Käsittelyä voidaan myös jatkaa, jos se on tarpeellista oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Rekisteröidyllä on myös oikeus vastustaa tietojensa käsittelyä milloin tahansa, jos kyseessä on käsittely suoramarkkinointia varten. Rekisteröityä tulee informoida selkeästi ja viimeistään siinä vaiheessa, kun häneen ollaan ensimmäisen kerran yhteydessä. (Harjunheimo 2017)

Rekisterinpitäjän on joissakin tilanteissa rekisteröidyn pyynnöstä rajoitettava henkilötietojen aktiivista käsittelyä. Rekisteröidyllä on oikeus kiistää henkilötietojen

paikkaansa pitävyys, jolloin käsittelyä tulee rajoittaa sen aikaa, kunnes tiedot on tarkistettu oikeiksi. Jos tietoja käsitellään lainvastaisesti, voi rekisteröity vaatia tietojen poistamisen sijaan tietojen käsittelyn rajoittamista. Rekisteröity saa vaatia rajoittamista myös silloin, jos rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi, tai puolustamiseksi (Harjunheimo 2017) Rekisterinpitäjällä on edelleen lupa säilyttää henkilötietoja rajoittamisen jälkeen, mutta niitä ei saa käsitellä ilman rekisteröidyn suostumusta. Rekisteröidylle on tehtävä ilmoitus ennakkoon siitä, jos tietojen käsittelyn rajoitus aiotaan poistaa. (EU:n yleinen tietosuoja-asetus 3 luku, 18 artikla)

6.3 Tietojen oikaiseminen ja poistaminen

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee tiedot, jotka ovat virheellisiä tai epätarkkoja. Tietojen oikaisu tulee tehdä ilman aiheetonta viivytystä. Rekisteröidyllä on oikeus saada puutteelliset tiedot täydennettyä esimerkiksi lisäselvityksen avulla. (EU:n yleinen tietosuoja-asetus 3 luku, 16 artikla) Tietojen oikaisussa tulee kuitenkin huomioida tietojen käsittelyn tarkoitukset. Kun käsitellään esimerkiksi historiatietoja, ei voi tehdä vaatimusta, että ne korvattaisiin vaatimushetken voimassa olevilla tiedoilla. (Hanninen ym. 2017)

Rekisteröidyllä on ”oikeus tulla unohdetuksi” eli oikeus saada yritys poistamaan henkilötiedot tietyin perustein. Henkilötiedot voidaan poistaa silloin, kun niitä ei enää tarvita niihin käyttötarkoituksiin, joita varten ne on kerätty tai niitä ei enää käsitellä. Tietojen käsittely perustuu rekisteröidyn suostumukseen ja rekisteröity peruuttaa suostumuksensa eikä käsittelylle ole muuta perustetta laillisesti. Tiedot voidaan poistaa rekisteröidyn vastustaessa käsittelyä vastustamisoikeutensa nojalla tai silloin kuin tietoja on käsitelty lainvastaisesti, jolloin tietojen poistoa on pyydetty. Henkilötiedot voidaan poistaa myös silloin kun vedotaan lainsäädäntöön perustuvan yrityksen velvoitteen noudattamiseksi. Kuten tästä luettelosta käy ilmi, rekisteröidyn oikeus tulla unohdetuksi on rajoitettu. Lisäksi oikeutta tulla unohdetuksi ei sovelleta esimerkiksi silloin, jos käsittely on tarpeen oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi. (Hanninen ym. 2017)

Useimmissa yrityksissä henkilötietojen käsittelyn perusteena on yrityksen oikeutettujen etujen toteutus. Jos tämä on käsittelyperusteena, ja peruste on voimassa, ei rekisteröidyllä ole oikeutta tulla unohdetuksi. Esimerkiksi yrityksen työntekijöillä ei pääasiassa ole oikeutta tulla unohdetuksi. (Hanninen ym. 2017)

Jos rekisteröidyllä on oikeus tulla unohdetuksi, yrityksen on ilman aiheetonta viivytystä poistettava häntä koskevat henkilötiedot. Tietojen ollessa julkisia, sen tulee käytettävissään oleva teknologia ja toteuttamiskustannukset huomioiden tehdä kohtuulliset toimenpiteet, jotta voidaan tehdä henkilötietoja käsitteleville rekisterinpitäjille ilmoitus, että rekisteröity on tehnyt pyynnön kyseisille rekisterinpitäjille poistamaan henkilötietoihin liittyvät linkit tai henkilötietojen jäljennökset tai kopiot. (Hanninen ym. 2017)

Asetuksessa ei ole määritelty, miten tiedot tulee teknisesti poistaa. Jos tietojen poistaminen on mahdollista kokonaan, on se suositeltavin tapa. Mikäli tämä ei ole mahdollista, niin tiedot voidaan poistaa aktiivisesti käytöstä, ettei niitä pystytä käsittelemään. Viranomaisilta voi kysyä tarkempaa ohjeistusta tietojen poistoa varten. (Hanninen ym. 2017)

7 SANKTIOT JA VALVONTA

7.1 Selosteet käsittelytoimista

Uusi tietosuoja-asetus velvoittaa rekisterinpitäjää laatimaan selosteen tietojen käsittelytoimista. Aiemmin rekisterinpitäjien tuli laatia rekisteriseloste. Nykyiset rekisteriselosteet ovat hyvä lähtökohta laadittaessa asetuksen mukaista selostetta käsittelytoimista, sillä niillä on monia yhteneväisyyksiä. (Hanninen ym. 2017) Tietosuojavaltuutetun toimiston mukaan on mahdollista, että selosteen laadintaan käytetään rekisteriselosteen kaltaista lomakepohjaa yleisen tietosuoja-asetuksen 30 artiklan mukaisen velvoitteen toteuttamiseksi, mikäli tietosisältö on päivitetty vastaamaan kyseisen artiklan vaatimuksia. Selosteen tulisi olla keskeinen osa osoitusvelvollisuuden

toteuttamisessa. Sen tarkoituksena on, että dokumentaatiosta saisi ajantasaisen kokonaiskuvan organisaation harjoittamasta henkilötietojen käsittelystä. (Tietosuojavaltuutetun toimisto www-sivut 2018)

Jokaisen rekisterinpitäjän tulee ylläpitää selostetta vastuullaan olevista käsittelytoimista. Selosteen on käsitettävä ainakin seuraavat tiedot: rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot, käsittelyn tarkoitukset, kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä, henkilötietojen vastaanottajien ryhmät, joille tietoja on luovutettu tai aiotaan luovuttaa, tarvittaessa tiedot henkilötietojen siirrosta kolmanteen maahan tai kansainväliselle järjestölle, tähän kuuluu myös tieto siitä mihin maahan tietoja luovutetaan, sekä asianmukaisia suojatoimia koskevat asiakirjat, mahdollisuuksien mukaan eri tietoryhmien poistamisen suunnitellut määräajat ja yleinen kuvaus teknisistä ja organitorisista turvatoimista. (EU:n yleinen tietosuoja-asetus 1 luku 30 artikla)

7.2 Hallinnolliset sakot

Yksi merkittävimmistä muutoksista tietosuoja-asetuksessa on viranomaisten valtuudet määrätä sanktioita niille toimijoille, jotka rikkovat tietosuoja-asetusta. Tietosuoja-asetuksen myötä valvontaviranomaiset voivat määrätä hallinnollisia sakkoja. (Harjunheimo 2017)

Merkittävä muutos tietosuoja-asetuksessa on viranomaisten valtuudet määrätä merkittäviä sanktioita tietosuoja-asetusta rikkoville toimijoille. Tietosuoja-asetus tuo valvontaviranomaiselle uuden valtuuden määrätä hallinnollisia sakkoja. Hallinnollisten sakkojen määräämiseen ja määrään vaikuttavat mm. seuraavat seikat:

- rikottu velvollisuus, rikkomisen luonne, sen vakavuus ja kesto huomioiden tietojenkäsittelyn luonne, laajuus sekä tarkoitus
- rekisteröityjen lukumäärä, joihin rikkomisella on vaikutus sekä heihin kohdistuvan vahingon suuruus
- yrityksen toimet rikkomisen korjaamiseksi ja haittavaikutusten lieventämiseksi

- tapa, jolla käsittelyn laiminlyönti tuli viranomaisten tietoon: tekikö rekisterinpitäjä vai henkilötietojen käsittelijä ilmoituksen ja missä laajuudessa (Harjunheimo 2017)

Hallinnollisten sakkojen enimmäismäärä on perustavanlaatuisten velvoitteiden rikkomisesta 20 miljoonaa euroa tai 4 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Esimerkiksi kohdassa 4.1 kuvattujen velvoitteiden rikkomisesta määrättävän sakon enimmäismäärä on 20 miljoonaa euroa tai 4 % liikevaihdosta. Käsittelyn turvallisuuden laiminlyönti tai tietoturvaloukkauksen ilmoittamatta jättäminen voi enimmäismäärältään olla 10 miljoonaa euroa tai 2 % liikevaihdosta. (Harjunheimo 2017) Muita mahdollisia seuraamuksia ovat muun muassa varoitukset, huomautukset ja määräykset sekä henkilötietojen käsittelyn rajoittaminen tai kieltäminen. (Tietosuojavaltuutetun toimisto www-sivut 2018)

7.3 Vahingonkorvausvastuu

Jos rekisteröidylle aiheutuu tietosuoja-asetuksen laiminlyönnistä aineellista tai aineetonta vahinkoa, rekisterinpitäjän tai henkilötietojen käsittelijän on maksettava korvaus aiheutuneesta vahingosta. Maksuvelvollisuus tulee sille yritykselle, joka on vastuussa vahingon aiheuttaneesta tapahtumasta. Henkilötietojen käsittelijänä toiminut yritys on kuitenkin vastuussa vahingosta vain, jos se ei ole noudattanut oikein henkilötietojen käsittelijöille määrättyjä tietosuoja-asetuksen velvoitteita tai se on laiminlyönyt rekisterinpitäjän lainmukaisen ohjeistuksen. Jos useampi yritys on vastuussa käsittelystä aiheutuneesta vahingosta, jokainen yrityksistä on vastuussa koko vahingosta suhteessa vahingon kohdistuneeseen rekisteröityyn. Rekisteröity voi siis vaatia koko korvausta yhdeltä vahingosta vastuussa olevalta yritykseltä. (Hanninen ym. 2017)

Sellaisessa tilanteessa, jossa yksi yritys joutuu maksamaan täyden korvauksen vahingosta rekisteröidylle, vaikka useampi yritys on vastuussa vahingon aiheuttamisesta, on korvauksen maksaneella yrityksellä oikeus periä muiltakin osallistuneilta yrityksiltä se osuus korvauksesta, joka vastaa niiden vastuulla olevaa osuutta aiheutuneesta vahingosta. (Hanninen ym. 2017)

7.4 Rikosoikeudellinen vastuu

Hallinnollisten sakkojen myötä tietosuojalainsäädäntään liittyvä seuraamusjärjestelmä muuttuu perustavanlaatuisesti. Rikosoikeudellinen vastuu tulisi jatkossa voimaan vain niissä tilanteissa joissa lainvastainen henkilötietojen käsittely ei olisi hallinnollisten sakkojen piirissä. Nykyinen henkilörekisteririkosta koskeva säännös korvattaisiin siis tietosuojarikosta koskevalla säännöksellä. (Hanninen ym. 2017)

Tietosuojarikoksesta olisi kyse silloin, jos henkilö muutoin kuin rekisterinpitäjänä tai henkilötietojen käsittelijänä tarkoituksella tai törkeästä huolimattomuudesta käsittelee henkilötietoja ilman oikeaa käyttötarkoitusta, luovuttaa tietoja tai siirtää niitä tietosuoja-asetuksen vastaisesti. Tämän seurauksena voi tapahtua rekisteröidyn yksityisyyden suojan loukkaus tai siitä voi aiheutua muuta olennaista haittaa. Tällä perusteella tietosuojarikokseen voisi syyllistyä esimerkiksi työntekijä, joka uteliaisuuttaan tutkii rekisteröidyn henkilötietoja, vaikkei hänellä tehtäviensä perusteella olisikaan oikeutta niiden käsittelyyn. (Hanninen ym. 2017)

Tietosuojarikos voisi tulla kyseeseen myös silloin kun laiminlyödään käsittelyn turvallisuutta koskevaa periaatetta. Esimerkiksi menettely, jossa rekisterinpitäjän alaisuudessa toimiva henkilö heittää pois henkilörekisteristä otettuja asiakirjoja huolehtimatta niiden turvallisesta hävittämisestä. (Hanninen ym. 2017)

8 YHTEENVETO JA POHDINTA

Tietosuoja-asetus tuo paljon haasteita yrityksille. Valmistautuminen on ollut haastavaa, sillä viranomaisten ohjeet ja tietosuoja-asetukseen liittyvää tietoa on julkaistu hitaalla aikataululla. Esimerkiksi tietosuojavaltuutetun toimiston www-sivut päivittyvät tietosuojaviranomaisen sivuiksi vasta sinä päivänä, kun tietosuoja-asetusta tulee jo noudattaa. Moni yritys olisi varmasti kaivannut uudistusta jo aikaisemmin, jolloin virallisten sivujen sisältöön olisi voinut jo aikaisemmin tutustua. Valmistautumisen aikataulu on myös voinut kärsiä tiedon puutteet takia. Toivottavasti yritykset ovat tästä

huolimatta pystyneet aloittamaan valmistautumisen ajoissa, sillä se vaatii paljon aikaa. Myös opinnäytetyöhön oli välillä haastavaa löytää tarpeeksi tietoa, vaikka asetuksen voimaantulo on jo todella lähellä. On mielenkiintoista seurata, että miten hallituksen esitys tietosuojalaista täydentää voimaan tullutta tietosuoja-asetusta.

Rekisterinpitäjän ja henkilötietojen käsittelijän kannalta tietosuoja-asetuksessa on paljon uusia vastuita ja velvollisuuksia sekä periaatteita. Myös tietojen käsittelyn rajoittamisen periaatetta on hankala ylläpitää. Monessa pienessäkin yrityksessä voi olla satojen asiakkaiden henkilötietoja rekisteröitynä, joten valvonta ja käsittely vaatii paljon aikaa ja resursseja.

Tietosuoja-asetus vahvistaa todella paljon rekisteröidyn asemaa. Mielestäni on tärkeää, että rekisteröidylle tulee informoida omien tietojensa käsittelystä. Moni ei varmasti ajattele kuinka tärkeä asia tietosuoja on ennen kuin mahdollinen tietoturvamurto tapahtuu ja omat tiedot päätyvät vääriin käsiin. Opinnäytetyön aihe oli minulle vieras ja työn edetessä ymmärsin kuinka tärkeä ja olennainen asia tietosuoja on jokaiselle. Tietosuojaan liittyvistä opituista tiedoista on varmasti hyötyä minulle myös tulevaisuudessa.

Tietosuojavastaavalle asetuksen voimaantulon hetki vaatii järjestelmällisyyttä, sillä töitä tulee olemaan paljon. Samanaikaisesti tulisi valvoa sitä, että asetusta noudatetaan oikein ja korjata puutteet, pitää huolta henkilökunnan koulutuksesta sekä opastuksesta. Vaikeinta asetuksen toteuttamisessa tulee erityisesti olemaan osoitusvelvollisuuden toteuttaminen ja tietojen säilytyksen rajoitus. Yrityksille suuria vaatimuksia aiheuttaa varmistuminen siitä, että henkilökunta on varmasti tarpeeksi koulutettua tietojen käsittelyä varten.

Jatkotutkimuksena voisi tarkastella, miten asiat käytännössä ovat toimineet ja miten niitä voisi kehittää paremmaksi asetuksen voimaan tulon jälkeen. Tietosuoja-asetus muuttaa suuresti yritysten toimintamalleja ja järjestelmiä. Uskon, että tämä uudistus on sekä yrityksille että rekisteröidyille hyvä asia, sillä tietoturvamurtoja tapahtuu todella paljon nykyään. Asetusta tullaan todennäköisesti vielä myöhemmin päivittämään ja täydentämään entistä paremmaksi.

LÄHTEET

Andraesson A., Koivisto J. & Ylipartanen A. 2016. Tietosuojakäsikirja johdolle. 3 uud. p. Tallinna: Printon

Andreasson A., Ylipartanen A. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. https://opitietosuojaa.fi

Andreasson, A., Riikonen, J. & Ylipartanen A. 2017. Osaava tietosuojavastaava. Tallinna: Printon

Euroopan Parlamentin ja neuvoston asetus (EU) 2016/679. Viitattu 23.2.2018 http://eur-lex.europa.eu

Hanninen, M., Laine, E., Rantala, K. & Rusi M. 2017. Henkilötietojen käsittely: EU:n tietosuoja-asetuksen vaatimukset. Helsinki: Kauppakamari. Viitattu 10.1.2018. https://kauppakamaritieto-fi.lillukka.samk.fi/fi/s/ak/kirjat/henkilotietojen-kasittely-eu-tietosuoja-asetuksen-vaatimukset-2017/

Harjunheimo N. Tietopaketti yrityksille: On tärkeätä valmistautua EU:n tietosuoja-asetukseen 2017. Viitattu 16.2.2018. https://ek.fi

Heiskanen, V-M. 2017. Tietotilinpäätös helpottamaan EU:n tietosuoja-asetukseen valmistautumista. Viitattu 3.3.2018. www.sytyke.org

Henkilötietolaki 22.4.1999/523 muutoksineen

Holopainen P. Yrittäjän tietosuojaopas 2018. Viitattu 2.3.2018. https://www.yrittajat.fi

Jäntti S, 2018. Toimitusjohtaja, Tili-Seno Oy. Kaarina. Henkilökohtainen haastattelu. 6.3.2018. Haastattelijana Hanna Niemi. Muistiinpanot haastattelijan hallussa.

Männistö E. Tietosuoja-asetus ja ulkoistettu palkanlaskenta - Mitä huomioitava? Luento Taloushallintoliiton jäsenille 26.10.2017

Oikeusministeriö & Tietosuojavaltuutetun toimisto. Miten valmistautua EU:n tietosuoja-asetukseen? 2017. Viitattu 20.2.2018. http://www.tietosuoja.fi

OpiTietosuojaa 2018. Asetuksen sisältö ja tavoite. Viitattu 15.1.2018. https://opitietosuojaa.fi

Sulin I. Yleinen tietosuoja-asetus 2017. Viitattu 15.2.2018. https://www.kuntaliitto.fi

Tietosuojavaltuutetun toimisto www-sivut. 2018. Viitattu 15.1.2018. http://www.tietosuoja.fi

Tili-Seno Oy:n www-sivut. Viitattu 10.1.2018. https://www.tiliseno.fi

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

LIITE 1

HAASTATTELU

1. Mitä toimenpiteitä tulee vielä tehdä ennen tietosuoja-asetuksen voimaantuloa?

2. Minkälaisella aikataululla vaatimuksiin on valmistauduttu?

3. Miten henkilökuntaa on perehdytetty asiaan?

4. Onko asiakkaita informoitu muutoksista?

5. Minkälaisia tietoturvamenetelmiä on käytetty turvaamaan rekisterit? Organisatoriset/ tekniset keinot?

6. Tuleeko sopimuskäytäntöihin muutoksia?

7. Mikä on ollut haasteellisinta muutosten toteuttamisessa?