SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
YHTEISKUNTATIETEIDEN, LIIKETALOUDEN JA HALLINNON ALA

TIETOSUOJALAINSÄÄDÄNNÖN UUDISTUKSEN VAIKUTUKSET PAIKALLISIIN YRITYKSIIN

TEKIJÄT: Emma Halonen
Manja Puruskainen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Yhteiskuntatieteiden, liiketalouden ja hallinnon ala	
Koulutusohjelma/Tutkinto-ohjelma Liiketalouden koulutusohjelma	
Työn tekijä(t) Emma Halonen, Manja Puruskainen	
Työn nimi Tietosuojalainsäädännön uudistuksen vaikutukset paikallisiin yrityksiin	
Päiväys 13.5.2019	Sivumäärä/Liitteet 46/2
Ohjaaja(t) Jukka Honkanen, Kaisa Hämäläinen	
Toimeksiantaja/Yhteistyökumppani(t) -	

Tiivistelmä

Opinnäytetyössä tutkittiin tietosuojalainsäädännön uudistuksen vaikutuksia yritystoimintaan. Toukokuun 25. päivä 2018 alettiin Euroopan unionin alueella soveltamaan kahden vuoden siirtymäajan jälkeen EU:n yleistä tietosuoja-asetusta, jota rekisterinpitäjien tulee noudattaa kaikessa henkilötietojen käsittelyssä. Tietosuoja-asetusta täydentämään säädettiin kansallinen tietosuojalaki 1050/2018, joka astui voimaan 1.1.2019.

Työn tarkoituksena oli selvittää, mitä todellisia muutoksia lainsäädännön uudistuminen toi, sekä kuinka muutos koettiin yleisesti paikallisissa pk-yrityksissä. Opinnäytetyöllä ei ollut toimeksiantajaa, vaan aiheen valinta perustui tekijöiden henkilökohtaiseen kiinnostukseen aiheesta. Opinnäytetyöhön kuuluu teoriaosuus, sekä laadullinen tutkimus, joka toteutettiin teemahaastatteluina. Opinnäytetyössä käytettiin kolmea pääteemaa: taustatiedot, muutokset yritystoiminnassa ja kokemukset / tuntemukset tietosuojalainsäädännön uudistuksesta.

Tutkimusta varten haastateltiin neljää paikallista pk-yritystä. Haastateltaviksi valittiin yritysten tietosuojasta vastaavat tai tietosuoja-asioita osana työtään käsitteleviä henkilöitä. Opinnäytetyön pohjana toimi laaja teoriaosuus, jossa on määritelty tietosuojaan liittyvät keskeiset käsitteet, esitelty lukijalle kansallista ja Euroopan unionin lainsäädäntöä, sekä kerrottu tietosuojalainsäädännön keskeisestä sääntelystä. Lainsäädäntöön tulleita muutoksia pyrittiin korostamaan. Kvalitatiivisen tutkimuksen tulokset on esitetty teoriaosuuden yhteydessä vetoketjumallia käyttäen.

Tutkimustulosten perusteella varsinaisia muutoksia yritysten liiketoiminnoissa oli odotettua vähemmän. Muutokset kohdistuivat lähinnä keväälle 2018, kun asetusta alettiin soveltamaan. Erityisesti aiheeseen perehtyminen ja osoitusvelvollisuuden vaatimien dokumenttien tekeminen on ollut työlästä. Tutkimuksessa kävi ilmi pk-yritysten tarve selkeälle ja käytännönläheiselle ohjeistukselle tietosuojalainsäädännöstä. Opinnäytetyötä ei ole tarkoitettu ohjekirjaksi tietosuojan toteuttamiseen, mutta työn lukeminen voi auttaa lukijaa ymmärtämään tietosuojalainsäädäntöä paremmin.

Avainsanat
Tietosuoja-asetus, tietosuoja, henkilötietojen käsittely, laadullinen tutkimus, rekisterinpitäjä

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Social Sciences, Business and Administration			
Degree Programme Degree Programme in Business Administration			
Author(s) Emma Halonen, Manja Puruskainen			
Title of Thesis The impact of data protection legislation reform on local enterprises			
Date	13.5.2019	Pages/Appendices	46/2
Supervisor(s) Jukka Honkanen, Kaisa Hämäläinen			
Client Organisation /Partners -			

Abstract

The purpose of the thesis project was to introduce the reform of data protection legislation and its implications for businesses. After a two year transition period, on 25th of May 2019, The General Data Protection Regulation (EU) 2016/ 679 took effect around all of the European Union. The national Data Protection Act 1050/2018 was legislated to reinforce GDPR and it came into effect 1.1.2019.

The purpose of the thesis research was to find out what real changes the reformed legislation brought forth and how the changes were generally experienced in local small and medium-sized enterprises. The topic of the thesis was selected based on personal interests of the authors, therefore there were no actual commissioners for the study. The thesis report includes a theory section and a qualitative research section, the latter of which was carried out by theme interviews. There were three main themes: background information, changes in the business and experiences of/ feelings about the legislative reformation.

Four interviews were conducted with local small and medium-sized enterprises for the research. The companies' data protection officers or the persons whose duties include dealing with data protection were chosen as interviewees. The basis of the thesis project was an extensive theory section determining the essential concepts related to data protection. Furthermore, national and the European Union's legislation as well as the enforcement of the core regulation were presented to the reader. The aim was to emphasize the amendments and reforms executed in the legislation. The results of the qualitative research have been presented within the theory part of the thesis.

To conclude, the results of the research showed that there were fewer changes in businesses than expected. Changes fell upon May 2018, when the GDPR took effect. In relation to that period, having acquainted with the topic and after preparation of all the documents demanded by accountability had been experienced challenging. The research also indicated the need of clear and practical guidance related to data protection legislation. The thesis is not designed to be a manual of any sort, however reading it might help the reader to understand data protection legislation more easily.

Keywords
General data protection regulation, data protection, processing of personal data, qualitative research, controller

SISÄLTÖ

1 JOHDANTO

Toukokuun 25. päivä 2018 Euroopan unionin alueella alettiin soveltaa kahden vuoden siirtymäajan jälkeen Euroopan parlamentin ja neuvoston asetusta 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä, sekä näiden tietojen vapaasta liikkuvuudesta, ja direktiivin 95/46/EY kumoamisesta (jäljempänä EU:n yleinen tietosuoja-asetus). Keväällä 2018 aiheesta uutisoitiin laajasti, erityisesti huomattavien sanktioiden vuoksi. Samaan aikaan pinnalla oli eräiden suurten kansainvälisten yritysten kyseenalaiset ratkaisut henkilötietojen käsittelyssä. Tämän jälkeen tietosuoja-asetusta täydentämään säädettiin vielä kansallinen tietosuojalaki 1050/2018, joka tuli voimaan vuoden 2019 alussa.

Yleisen tietosuoja-asetuksen on tarkoitus yhtenäistää tietosuojalainsäädäntö unionin jäsenvaltioissa, ja näin ollen edesauttaa digitaalitalouden kehittymistä sisämarkkina-alueella. Tietosuoja-asetus lisää henkilötietojen käsittelyn läpinäkyvyyttä ja vahvistaa rekisteröityjen oikeuksia. Se myös luo rekisterinpitäjille uusia velvollisuuksia ja hallinnollisia tehtäviä.

Opinnäytetyö käsittelee tietosuojalainsäädännön uudistuksen vaikutuksia yritystoimintaan. Työn tarkoituksena on selvittää tietosuojalainsäädännön sisällölliset muutokset, sekä kuinka nuo muutokset on koettu paikallisissa pk-yrityksissä. Työssä haluttiin selvittää, onko uudistus esimerkiksi lisännyt työmäärää yrityksissä, muuttanut toimintatapoja, vaatinut investointeja tai tuonut muutoksia yritysten tarjoamiin palveluihin. Konkreettisten muutosten lisäksi haluttiin selvittää, mitä tuntemuksia uudistus on herättänyt; onko koettu positiivisia vaikutuksia, onko asetuksen tulkinnassa ollut ongelmia tai onko uudistus koettu hankalana? Opinnäytetyöllä ei ole toimeksiantajaa, vaan aiheen valinta perustui tekijöiden henkilökohtaiseen kiinnostukseen. Tietosuojalainsäädäntöön perehtyminen koettiin myös tärkeäksi työelämän kannalta. Opinnäytetyöhön kuuluu teoriaosuus, sekä laadullinen tutkimus, joka on toteutettu teemahaastatteluina. Tutkimusmenetelmän valinnasta ja aineiston käsittelystä kerrotaan tarkemmin luvussa 2.

Opinnäytetyön pohjana toimii laaja teoriaosuus, jossa aluksi määritellään tietosuojaan liittyvät keskeiset käsitteet, sekä esitellään kansallista ja Euroopan unionin tietosuojalainsäädäntöä. Teoriaosuus painottuu tietosuoja-asetuksen ja tietosuojalain keskeiseen sääntelyyn. Keskeisimpään sääntelyyn kuuluvat henkilötietojen käsittelyn yleiset periaatteet, käsittelyn lainmukaisuusperusteet, rekisteröityjen oikeudet ja rekisterinpitäjän velvollisuudet. Teoriaosuudessa käsitellään myös muuttuneita sanktiokäytäntöjä ja henkilötietojen siirtoa kolmansiin maihin. Laadullisen tutkimuksen tulokset esitetään teoriaosuuden yhteydessä vetoketjumallia käyttäen.

Teoriaosuudessa tärkeimpinä lähteinä on käytetty Euroopan unionin yleistä tietosuoja-asetusta, kansallista tietosuojalakia 1050/2018 sekä tietosuojavaltuutetuntoimiston sivuja. Tietoa on hankittu myös muista viranomaislähteistä, uutisista sekä alan kirjallisuudesta.

2 TUTKIMUKSEN TOTEUTUS

2.1 Tutkimusmetodin valinta

Tutkimus toteutettiin laadullisesti, eli kvalitatiivisesti, sillä tutkimuksella pyrittiin selvittämään haastateltavien kokemuksia ja tuntemuksia tietosuojalainsäädännön uudistumisen myötä. Laadullisen tutkimuksen tarkoituksena ei ole tuottaa tilastollisia yleistyksiä, vaan pyrkimyksenä on esimerkiksi kuvailla jotain ilmiötä, ymmärtää jotain toimintaa, tai löytää mielekäs tulkinta jollekin ilmiölle. Haastattelun vahvuutena on joustavuus. Haastattelijan on mahdollista tarvittaessa toistaa kysymys, selventää ilmauksia ja oikaista väärinkäsitykset. (Tuomi ja Sarajärvi 2018, 85, 98.)

Tutkimusmenetelmäksi valittiin yksilöhaastattelu, sillä haluttiin saada erilaisia näkökulmia eri toimialoilla toimivien yritysten tietosuojasta vastaavilta henkilöitä. Tutkimusmetodiksi valittiin teemahaastattelu, joka on strukturoitua haastattelua vapaampi. Teemahaastattelussa kaikkien haastateltavien kanssa käydään läpi ennalta valitut teemat, mutta eri haastatteluissa eri teemoja saatetaan käsitellä laajemmin. Haastatteluissa käytettiin kolmea pääteemaa: taustatiedot, muutokset yritystoiminnassa ja kokemukset, sekä tuntemukset tietosuojalainsäädännön uudistuksesta. Teemoja ei tarvitse käydä läpi tietyssä järjestyksessä, vaan olennaista on se, että kaikki teemat käsitellään. Teemahaastattelussa kysymykset eivät ole tarkassa järjestyksessä ja tarkoin muotoiltuja, toisin kuin strukturoiduissa haastattelussa. Teemahaastattelu valikoitui tutkimusmetodiksi juuri sen vapauden vuoksi. Haastateltaville pystyttiin esittämään tarvittaessa tarkentavia jatkokysymyksiä tai haastateltavat kykenivät poikkeamaan aiheesta, jos näin koettiin tarpeelliseksi. (Valli 2018, 29 - 30.)

Teemahaastattelussa haastateltavien tulkinta ja heidän antamansa merkitys asioille korostuu, minkä vuoksi haastateltavien valinta on tehtävä harkitusti. On tärkeää, että haastateltavilla henkilöillä on mahdollisimman paljon tietoa tai kokemusta tutkittavasta ilmiöstä. Opinnäytetyössä haastateltaviksi valikoitiin yritysten tietosuojasta vastaavat tai tietosuoja-asioita osana työtään käsittelevät henkilöt. (Tuomi ym. 2018, 88 ja 98.)

Laadullisessa tutkimuksessa haastateltavien määrä on usein määrällistä tutkimusta pienempi, joten haastateltavien määrä päätettiin rajata 3 - 5 haastateltavaan. Loppujen lopuksi haastateltavia valittiin neljä kappaletta. Otos koettiin riittäväksi aineiston käsittelyyn käytetyn ajan ja tekijöiden aikataulujen perusteella. Näin myös pystyttiin keskittymään tiiviimmin jokaiseen haastatteluun, kun aikaa oli sopivasti kaikille. (Tuomi ym. 2018, 98.)

2.2 Tutkimushaastattelut

Haastattelut toteutettiin kevään 2019 aikana, maalis- ja huhtikuussa. Haastateltaviksi haluttiin paikallisia yrityksiä, joihin otettiin suoraan yhteyttä puhelimitse ja sähköpostin välityksellä. Yritysten yhteystiedot löydettiin internetin kautta. Haastateltaviksi valittiin Kuopion alueella toimivia pienyrityksiä, joiden henkilöstön koko vaihtelee kahdesta kymmeneen työntekijään. Haastateltaviksi valittiin tarkoituksella eri toimialojen yrityksiä, jotta saataisiin riittävän kattava kuva paikallisten pienyritysten

kokemuksista tietosuojalainsäädännön uudistuksesta, eikä yksittäisen toimialan erityislainsäädäntö vaikuttaisi tuloksiin liikaa. Lopulta haastatteluihin valittiin neljä paikallista yritystä. Opinnäytetyössä heistä käytetään nimityksiä Yritys A, B, C ja D. Yritys A on optisen alan vähittäiskaupan toimija, yritys B:n toimiala on vähittäiskauppa, yritys C tuottaa hammaslääkäripalveluita ja yritys D:n päätoimiala on tietojenkäsittelyn ja laitteistojen käyttö- ja hallintapalvelut. Haastateltaviksi pyrittiin saamaan henkilöitä, jotka vastaavat yrityksen tietosuoja-asioista, tai kenen työtehtäviin kuuluu tietosuojaa koskevia tehtäviä.

Haastattelut toteutettiin kasvotusten yritysten omissa toimipisteissä tai Savonian tiloissa ja ne nauhoitettiin haastateltavien luvalla. Yksityisyydensuojan takaamiseksi haastattelut anonymisoitiin, jotta ketään tiettyä yritystä tai henkilöä ei voida tunnistaa opinnäytetyöstä. Haastattelut etenivät siten, että haastattelujen alussa selvitettiin yrityksen taustatiedot, minkä jälkeen siirryttiin tietosuojauudistuksen muutoksia koskeviin kysymyksiin. Viimeisen teeman kysymykset koskettivat puhtaasti haastateltavien tuntemuksia ja kokemuksia uudistuksista ja sen tuomista muutoksista. Haastattelukysymykset valittiin ja muotoiltiin siten, että haastateltavat saatiin kertomaan uudistuksen tuomista muutoksista totuudenmukaisesti. Haastateltavat eivät saaneet haastattelukysymyksiä ennakkoon, jotta he eivät olisi voineet valmistautua kysymyksiin liikaa. Jokainen haastattelu vei odotusten mukaisesti noin 20 minuuttia, paitsi viimeinen haastattelu, jonka pituudeksi kertyi noin 40 minuuttia.

2.3 Aineiston käsittely

Haastattelutilaisuuksien jälkeen nauhoitteet litteroitiin, eli nauhoitettu haastattelu kirjoitettiin tekstiksi. Opinnäytetyössä käytettävän vetoketjumallin takia sanatarkka, eli eksakti litterointi, tai referoiva litterointi eivät olleet sopivia. Liian tarkka tai lavea lainaaminen olisi sitaattien käyttämisen kannalta sopimatonta. Käytimme litterointitapana peruslitterointia, eli haastattelut litteroitiin sanatarkasti, mutta täytesanat, turhat sanojen toistot ja muut epäselvät ilmaukset jätettiin litteroinnin ulkopuolelle. Tämä helpotti myös sitaattien siirtoa opinnäytetyöhön. Peruslitterointia voi käyttää tällaisissa tapauksissa, joissa nimenomaan haastattelun sisältö on analysoinnin kohteena. (Aineistonhallinnan käsikirja.)

Litteroitua haastatteluaineistoa käsiteltiin ennen sen sijoittamista teoreettiseen viitekehykseen. Ensin aineistoista koodattiin esiin tärkeitä ja huomionarvoisia kommentteja, jonka jälkeen aineisto teemoiteltiin opinnäytetyön teemojen mukaisesti. (Kesänen a.)

2.4 Tutkimuksen etiikka ja luotettavuus

Tutkimus toteutettiin eettisiä periaatteita noudattaen. Haastatteluihin osallistuminen oli vapaaehtoista ja haastateltavia informoitiin opinnäytetyön tavoitteista kattavasti. Yksityisyyden suojaa painotettiin, ja täten kaikki haastattelumateriaali, myös litteroinnit, anonymisoitiin. Kun sitaatit oli siirretty opinnäytetyöhön, nauhoitettu ja kirjallinen haastatteluaineisto hävitettiin. Tutkimuksen luotettavuutta pyrittiin parantamaan toimimalla erityisen huolellisesti. Aineisto käsiteltiin tarkasti ja varoen litteroidessa, teemoittelussa ja opinnäytetyöhön siirrettäessä, jotta tulkinnat säilyisivät muuttumattomina koko käsittelyn ajan. (Kesänen b.)

3 TIETOSUOJA

Tietosuojalla tarkoitetaan yleisesti laissa säädettyjä, henkilötietojen käsittelyä koskevia periaatteita, joiden mukaan toimimalla varmistetaan luonnollisen henkilön yksityisyyden suoja ja oikeusturva. Euroopan unionin tietosuoja-asetuksessa periaatteiksi määritellään mm. käyttötarkoitussidonnaisuus, lainmukaisuus, tietojen minimointi, eheys ja luottamuksellisuus. Tietoturvalla taas tarkoitetaan toimenpiteitä, joiden avulla varmistetaan tietosuojan toteutuminen. Tällaisia toimenpiteitä voivat olla esimerkiksi tiedon laadun, eheyden ja luottamuksellisuuden takaaminen erilaisin organisatorisin ja teknisin keinoin. (Andreasson, Koivisto ja Ylipartanen 2016, 15 - 16; EU:n yleinen tietosuoja-asetus 2016/679, artikla 5.)

Yksityiselämän suoja määritellään Suomen perustuslaissa yhdeksi perusoikeuksista. Perustuslaissa todetaan, että henkilötietojen suojasta on säädettävä lailla tarkemmin. Yleisesti tietosuojalainsäädännön tarkoituksena on turvata perusoikeudeksi luokiteltu yksityiselämän suoja, sekä oikeus henkilötietojen suojaan. Esimerkiksi Euroopan Unionin tietosuoja-asetuksen yhdeksi tavoitteeksi määritellään ”Tällä asetuksella suojellaan luonnollisten henkilöiden perusoikeuksia ja -vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan”. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 1; Perustuslaki 731/1999, § 10.)

Yritystoiminnan kannalta tietosuojaosaaminen on tärkeää, sillä lainvastainen henkilötietojen käsittely voi johtaa erilaisiin oikeudellisiin ja taloudellisiin seurauksiin. Esimerkiksi tietovuodolla on taloudellisia seurauksia, kun yritys joutuu suuntaamaan resursseja tietovuodon haltuun saamiseksi ja järjestelmien tekniseen korjaukseen. Tietovuodosta johtuva mainehaitta voi myös johtaa asiakkaiden menettämiseen. Tietosuoja-asioissa ennaltaehkäiseminen on kustannustehokkainta, minkä vuoksi riskienhallinta on tärkeää. (Andreasson ym. 2016, 107; Ponemon institute 2018, 23, 30.)

3.1 Keskeiset käsitteet

Henkilötieto

Henkilötieto on tieto, jonka perusteella voidaan selvittää, kuka luonnollinen henkilö on kyseessä. Kaikki tiedot, jotka voidaan liittää johonkin tiettyyn henkilöön, ovat henkilötietoja. (Hanninen, Laine, Rantala, Rusi ja Varhela 2017, 19 - 20.)

Henkilötietojen käsittely

Kaikki toiminnot, myös automaattiset toiminnot, jotka kohdistuvat henkilötietoihin, ovat niiden käsittelyä. Käsittelyä voi olla myös esimerkiksi tietojen tallentaminen, säilyttäminen, saataville asettaminen ja poistaminen. (Hanninen ym. 2017, 20 - 21.)

Henkilötietojen käsittelijä

Henkilötietojen käsittelijä on rekisterinpitäjän alaisena tai tämän käskystä toimiva ja tämän ohjeita noudattava luonnollinen henkilö, oikeushenkilö, viranomainen tai muu elin, joka käsittelee henkilötietoja (Hanninen ym. 2017, 22).

Rekisteröity

Rekisteröity on luonnollinen henkilö, eli ihminen, jonka henkilötietoja käsitellään (Hanninen ym. 2017, 20).

Rekisteri

Tässä tapauksessa rekisteri on henkilötietoja sisältävä joukko tietoja, jotka on kerätty tiettyä käyttötarkoitusta varten, ja josta tiedot voidaan löytää helposti tietyillä perusteilla (Hanninen ym. 2017, 22).

Rekisterinpitäjä

Rekisterinpitäjä on taho, kuten luonnollinen henkilö, oikeushenkilö tai viranomainen, joka päättää henkilötietojen käsittelyn tarkoitukset ja keinot itsekseen tai yhdessä toisen tahon kanssa (Hanninen ym. 2017, 22).

Anonymisointi

Anonymisointi tarkoittaa sitä, että henkilötiedoista riisutaan tunnistettavuutta siten, ettei tietoja voida enää yhdistää rekisteröityyn henkilöön (Hanninen ym. 2017, 21).

Pseudonymisointi

Pseudonymisoinnilla tarkoitetaan toimenpidettä, jolla varmistetaan, ettei henkilötietoja voi yhdistää rekisteröityyn ilman lisätietoja. Lisätiedot on myös säilytettävä henkilötiedoista erillään, jottei yhdistämistä tapahdu. (Hanninen ym. 2017, 21.)

Profilointi

Profiloinnilla tarkoitetaan automaattista käsittelyä, joka kohdistuu henkilötietoihin, ja jonka perusteella arvioidaan rekisteröidyn ominaisuuksia. Tällaisia voivat olla esimerkiksi taloudellisen tilanteen tai kiinnostuksen kohteiden analysointi. (Tietosuojavaltuutetun toimisto b.)

3.2 EU-lainsäädäntö

Suomi on Euroopan unionin jäsenvaltio, jonka vuoksi kansallisen lainsäädännön lisäksi Suomessa noudatetaan myös Euroopan unionin lainsäädäntöä. Euroopan unionilla on oma lainsäädäntöelin, joka koostuu parlamentista ja neuvostosta. Toimeenpanoelimenä toimii komissio, ja lakien soveltamista valvoo unionin tuomioistuin. Lisäksi EU:lla on kahdeksan muuta pääelintä ja 40 erillisvirastoa. Näitä ovat esimerkiksi Euroopan tietosuojavaltuutettu ja tietosuojaneuvosto. Euroopan tietosuojaneuvoston tehtävänä on varmistaa, että yleistä tietosuoja-asetusta noudatetaan koko EU:n alueella. Neuvosto myös ohjeistaa asetuksen tulkinnassa ja ratkaisee rajanylittäviä käsittelyjä koskevia riitatapauksia, jotta asetuksen soveltaminen valtioiden välillä olisi johdonmukaista. Euroopan tietosuojaneuvosto koostuu tietosuojaviranomaisten johtajista ja Euroopan tietosuojavaltuutetusta. Euroopan tietosuojavaltuutettuna toimii opinnäytetyön laatimisen ajankohtana Giovanni Buttarelli, joka aloitti tehtävänsä 2014 joulukuussa. (European Data Protection Supervisor; Euroopan komissio b; Euroopan Unioni b.)

EU:n määräyksistä yleisimmät ovat suositus, päätös, direktiivi ja asetus. Suositus on määräyksistä lievin ja se on vapaaehtoinen, eikä sen noudattamatta jättämisellä ole oikeudellisia seuraamuksia. Suosituksia annetaan, jotta jäsenmaiden toiminta tulisi yhtenäisemmäksi. Päätös taas on kohdistettu määräys ja se annetaan yleensä vain tietyille jäsenvaltioille tai taholle, joka toimii jäsenvaltioiden alueella. Päätökset ovat sitovia ja velvoittavia, ja niillä täydennetään muita määräyksiä. Direktiivi ei ole suora säädös, vaan se ohjaa jäsenvaltioiden sisäisiä lakeja. Siinä määrätään jäsenvaltioita toimenpiteisiin direktiivin täyttymiseksi. Se antaa jäsenvaltioille käskyn toimeenpanna direktiivin vaatimukset, mutta antaa valtioille päätäntävallan siitä, miten tavoitteisiin ylletään. Asetus, kuten EU:n yleinen tietosuoja-asetus, on suora säädös ja se tulee voimaan muuttumattomana jokaiseen EU:n jäsenmaahan ja sitä sovelletaan sellaisenaan ilman muutoksia. (Lainlaatijan EU-opas 2017; Euroopan Unioni a; Europarlamentti.info.)

Ennen EU:n yleistä tietosuoja-asetusta EU:n alueella toimivien yritysten tuli ottaa huomioon 28 eri tietosuojalakia. Ensimmäinen tietosuojasuositus tuli voimaan 1981 ennen internetiä. Vuodesta 1995 noudatettiin henkilötietodirektiiviä 95/46/EY, joka ohjasi jokaisen jäsenvaltion lainsäädäntöä. Suomessa sen perusteella luotiin henkilötietolaki 523/1999. Teknologia on kuitenkin kehittynyt ja digitalisaatio on kasvanut voimakkaasti viimeisen kymmenen vuoden aikana, ja täten tietosuojan päivittäminen EU-alueella oli ajankohtaista. Eri valtioissa oli myös erilaiset tietosuojakäytännöt ja lait, mikä aiheutti useammassa valtiossa toimiville yrityksille lisäkustannuksia ja byrokratiaa. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 kumosi edellisen henkilötietodirektiivin ja yhdisti EU:n jäsenvaltioiden tietosuojakäytännöt. (Aarnio 2019; Euroopan unionin julkaisutoimisto 2018, 1; Pietikäinen 2016.)

3.3 Kansallinen lainsäädäntö

Suomessa on paljon tietosuojaa koskevaa lainsäädäntöä. Julkisoikeuden professori Tomi Voutilainen arvioi Yleisradion haastattelussa Suomessa olevan noin 700 - 800 lakia, joissa säädetään henkilötietojen suojasta. Hajanainen ja sekava lainsäädäntö on riski oikeusturvalle, kun lakien

yhteensovittaminen ja tulkinta on hankalaa asiantuntijoillekin. Haasteita luo henkilötietojen suojan, julkisuusperiaatteen ja tiedon avoimuuden periaatteiden yhteen sovittaminen. (De Fresnes 2018.)

Yhtenä esimerkkinä hajanaisen lainsäädännön tuomille ongelmille voidaan pitää Liikenne- ja viestintävirasto Traficomin (entinen Liikenteen turvallisuusvirasto Trafi) kuljettajatietonettipalveluita. Kuljettajatietopalvelua käyttämällä pystyi selvittämään henkilön henkilöturvatunnuksen nimen ja asuinpaikan perustella. Asiasta syntyneen kohun myötä kuljettajatietopalvelu suljettiin. Vuotilaisen mukaan tässä tapauksessa on sotkeutunut tietopalveluiden ja asiakirjan julkisuuden toteuttaminen, eikä tietosuojan sääntelyä ole otettu huomioon riittävästi. (De Fresnes 2018; Salmi 2018.)

Henkilötietojen käsittelystä säädetään tietosuoja-asetuksen lisäksi kansallisessa lainsäädännössä useassa eri laissa. Näistä huomionarvoisin on vuoden 2019 alussa voimaan tullut tietosuojalaki 1050/2018, joka täydentää Euroopan unionin tietosuoja-asetusta. Tämän lisäksi henkilötietojen käsittelystä säädetään mm. laissa yksityisyyden suojasta työelämässä (759/2004), laissa sähköisen viestinnän palveluista (917/2014), laissa henkilötietojen käsittelystä rajavartiolaitoksessa (579/2005) ja laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007). (Korpisaari, Pitkänen, Warma-Lehtinen 2018, 3.)

Ennen EU:n uutta tietosuoja-asetusta Suomessa henkilötietojen käsittelystä määräsi henkilötietolaki 523/1999. Tietosuojalaki 1050/2018 kumosi henkilötietolain astuessaan voimaan 1.1.2019. Ennen tietosuojalain voimaantuloa henkilötietolakia sovellettiin EU:n uuden tietosuoja-asetuksen rinnalla. (Tietosuojavaltuutetun toimisto c.)

3.3.1 Tietosuojalaki

Vuoden 2019 alussa voimaan tulleen tietosuojalain tarkoituksena on täydentää ja täsmentää Euroopan Unionin tietosuoja-asetusta. Tietosuoja-asetuksessa on osoitettu liikkumavaraa kansalliselle lainsäädännölle, ja tämän liikkumavaran käyttö on sallittua vain tilanteissa, joissa se nimenomaisesti tietosuoja-asetuksessa on osoitettu. (Aarnio 2018, 1; Oikeusministeriö 2018.)

Tietosuojalaissa säädetään esimerkiksi kansallisesta valvontaviranomaisesta, sekä erityistilanteista henkilötietojen käsittelyssä. Näitä eritystilanteita ovat esimerkiksi henkilötietojen käsittely journalististen tai akateemisten ilmaisun tarkoitusta varten, sekä tieteellistä ja historiallista tutkimusta varten. Laissa säädetään henkilötunnuksen käsittelystä erikseen. Tietosuojalaissa tarkennetaan, milloin henkilötietojen käsittelyn laillisuusperusteena voidaan käyttää yleistä etua tai julkisen vallan käyttöä. Tietosuojalaissa täsmennetään myös tilanteita, jolloin rekisterinpitäjä saa käsitellä erityisiä henkilötietoryhmiä, sekä toimenpiteitä, jotka rekisterinpitäjän on suoritettava, mikäli se aikoo näitä tietoja käsitellä. (Tietosuojalaki 1050/2018, § 4, § 6, § 8 - 24, § 27 - 34.)

Tietosuojalaissa säädetään myös ikäraja tietoyhteiskunnan palveluiden tarjoamisesta alaikäiselle. Suomessa tietoyhteiskunnan palveluita saa tarjota 13-vuotiaille ja sitä vanhemmille lapsille. Tätä nuoremmalla täytyy olla vanhempien suostumus sellaisten palveluiden käyttämiseen, jotka edellyttävät

henkilötietojen luovuttamista. Rekisterinpitäjän vastuulla on näissä tapauksissa varmistaa suostumuksen olemassaolo. Euroopan unionin yleisessä tietosuoja-asetuksessa ikärajaksi on määritelty 16 vuotta, mutta asetus antaa jäsenvaltioille mahdollisuuden säätää ikärajan alemmaksi kansallisella lainsäädännöllä. Tietosuojalain säädöksiä avataan vielä lisää kappaleessa neljä. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 8; Talus, Autio, Hänninen, Pihamaa ja Kantonen 2017, 20.)

3.3.2 Rikoslaki

Rikoslaissa säädetään yksityisyyden, rauhan ja kunnian loukkaamisesta, sekä tieto- ja viestintärikoksista. Luvussa 38 säädetään esimerkiksi salassapitorikoksesta, viestintäsalaisuuden loukkaamisesta, tietomurrosta, sekä tietosuojarikoksesta. Rekisterinpitäjä tai henkilötietojen käsittelijä voidaan tuomita tietosuojarikoksesta sakkoon tai vankeuteen enintään vuodeksi, jos hän hankkii, siirtää tai luovuttaa henkilötietoja tietosuojalainsäädännön vastaisesti. Tietosuojalainsäädäntöön kuuluvat Euroopan unionin yleinen tietosuoja-asetus, tietosuojalaki (1050/2018), laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018), sekä muut kansalliset lait, joissa säädetään henkilötietojen käsittelystä. (Rikoslaki 39/1889, luku 38, § 9.)

4 YLEISET SÄÄNNÖKSET JA PERIAATTEET

Henkilötietoja käsitellään aikaisempaan verrattuna huomattavasti enemmän kuin ennen. Kuten edellä mainittu, ennen EU:n yleisen tietosuoja-asetuksen voimaan tuloa henkilötietojen käsittelystä säädettiin henkilötietolailla, joka perustui EU:n henkilötietodirektiiviin vuodelta 1995. Tämän jälkeen teknologia on kehittynyt huomattavasti, ja myös henkilötietojen hyödyntäminen liiketoiminnassa on muuttunut merkittävästi digitalisaation myötä. Palvelut ovat digitalisoituneet ja paremman asiakaskokemuksen tuottamiseksi hyödynnetään uudenlaisia teknologioita, joissa käytetään esimerkiksi puhe- ja katseohjausta, sijaintitietoja ja pilvipalveluita. (Valtiovarainministeriö 2016, 5 - 6.)

Toimintaympäristön muutoksen takia Euroopan Unionissa nähtiin tarve tietosuojalainsäädännön uudistamiselle. Tarve nähtiin erityisesti riskilähtöiselle, teknologiasta riippumattomalle sääntelylle, joka ottaa huomioon uudet mahdolliset teknologiat. Tietosuoja-asetuksen on tarkoitus edistää yksityisyyden suojaa verkkoympäristössä, vahvistaa unionin alueen digitalouden kehitystä ja kasvattaa kuluttajien luottamusta verkkoympäristöä kohtaan. Koko unionin alueen yhtenäisen lainsäädännön tavoitteena on myös vähentää yritysten hallintokustannuksia. (Valtiovarainministeriö 2016, 6, 35.)

Nämä hyödyt tietosuojalainsäädännön uudistuksessa näki myös yritys D. *"Kun tulee näitä uusia tekniikoita, niin nyt, kun on tää tietoturvaelementti, niin se pitäs aina muistaa jokaisessa, kun tulee joku elämää helpottava juttu, niin ku itsestään ajava auto. Niin on hyvä, että löytyy tuommonen lainsäädäntö (…) että varmistutaan siitä, ettei sieltä tule sen hyvän asian myötä niitä tietoturvareikiä."*

Tietosuoja-asetuksessa on kuitenkin paljon yhteneväisyyksiä aikaisemman lainsäädännön kanssa, vaikka se luo rekisterinpitäjille vielä uusia velvollisuuksia ja hallinnollisia tehtäviä. Enää ei riitä, että rekisterinpitäjä noudattaa sääntelyä, vaan sen tulee myös pystyä osoittamaan, että asetusta on noudatettu ja että tietosuoja on huomioitu. (Valtiovarainministeriö 2016, 6; Elinkeinoelämän keskusliitto 5.2.2.)

Jos henkilötietojen käsittely oli toteutettu ennen lainsäädännön uudistumista aikaisemman lainsäädännön vaatimusten mukaisesti, ei uudistus tuonut välttämättä paljoa muutoksia yritysten arkeen. *"No niitä muutoksia on aika vähän, mikä vaan kertoo siitä, että meijän asiat on sitte kuitenki ollu kunnossa alun perinkin."* (Yritys B.)

4.1 Aineellinen ja alueellinen soveltamisala

Euroopan unionin yleisessä tietosuoja-asetuksessa aineellinen soveltamisala on aikaisemmin voimassa olleen henkilötietolain kanssa yhteneväinen. Molempia sovelletaan henkilötietojen automaattiseen käsittelyyn, sekä henkilötietojen käsittelyyn silloin, kun ne muodostavat, tai niiden on tarkoitus muodostaa, rekisterin osa. Tietosuoja-asetuksen ja henkilötietolain soveltamisalaan ei kuulu henkilötietojen käsittely, jonka suorittaa luonnollinen henkilö henkilökohtaiseen tai kotitalouttaan koskevaan tarkoitukseen. Tietosuoja-asetusta ei myöskään sovelleta tietyissä tapauksissa toimivaltaisen viranomaisen

suorittamaan henkilötietojen käsittelyyn. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 2; Henkilötietolaki 523/1999, § 2.)

Aineellinen soveltamisala ulottuu näin ollen myös tietyissä tapauksissa henkilötietojen käsittelyyn silloinkin, kun ne eivät ole osa henkilörekisteriä, mutta henkilötietojen käsittely on automatisoitu. Tietosuoja-asetuksen suomennoksessa käytetään tästä huolimatta määritelmiä ”rekisteröity” ja ”rekisterinpitäjä”. Rekisterinpitäjä on osapuoli, joka ” yksin tai yhdessä toisen kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot”. Rekisteröity on taas luonnollinen henkilö, kenen henkilötietoja käsitellään, myös siinä tilanteessa, kun henkilötiedot eivät ole henkilörekisterissä. Korpisaari, Pitkänen ja Warma-Lehtinen (2018) pitävät näitä käännöksiä tämän vuoksi epäonnistuneina ja mahdollisesti harhaanjohtavina. (Korpisaari ym. 2018, 28; EU:n yleinen tietosuoja-asetus 2016/679, artikla 4.)

Aikaisemmin voimassa olleeseen henkilötietolakiin verrattuna on Euroopan Unionin tietosuoja-asetuksen alueellinen soveltamisala laajempi. Tämä on ilmeistä jo sen vuoksi, että henkilötietolaki oli osa Suomen kansallista lainsäädäntöä, kun taas tietosuoja-asetusta sovelletaan sellaisenaan koko Euroopan unionin alueella. Tietosuoja-asetusta voidaan kuitenkin soveltaa myös rekisterinpitäjiin tai henkilötietojen käsittelijöihin, jotka eivät ole sijoittuneet unionin alueelle tiettyjen ehtojen täyttyessä. Jos henkilötietojen käsittely koskee tavaroiden tai palveluiden tarjoamista rekisteröidyille, tai rekisteröityjen käyttäytymisen seurantaan unionin alueella, voidaan tietosuoja-asetusta soveltaa. Näin myös silloin kun henkilötietoja käsitellään unionin alueella sijaitsevan toimipaikan toiminnan yhteydessä, riippumatta siitä suoritetaanko käsittely unionin alueella. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 3.)

4.2 Henkilötietojen käsittelyn yleiset periaatteet

Henkilötietojen käsittelyä koskevat periaatteet ovat tietosuoja-asetuksen keskeisintä sääntelyä, ja ne koskettavat kaikkea tietosuoja-asetuksen soveltamisalaan kuuluvaa käsittelyä. Tietosuoja-asetuksessa määritellyt periaatteet vastaavat pitkälti aikaisemmin voimassa olleen henkilötietolain mukaisia henkilötietojen käsittelyn yleisiä periaatteita, mutta niitä on jonkin verran täsmennetty. Henkilötietojen käsittelyä koskevat periaatteet ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, sekä käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus. Tietosuoja-asetuksessa säädetään myös osoitusvelvollisuudesta, jonka mukaan rekisterinpitäjän on pystyttävä osoittamaan, että näitä periaatteita on noudatettu. (Elinkeinoelämän keskusliitto, 5.1.1; Hanninen ym. 2017, 47.)

Tietosuoja-asetuksessa kaikkea ei ole säännelty ehdottomilla säädöksillä, mutta käsittelyn yleiset periaatteet ohjaavat kaikkea henkilötietojen käsittelyä. Periaatteiden pohjalta rekisterinpitäjä voi monessa tapauksessa valita itse toimintatapansa niiden noudattamiseksi. Periaatteiden ymmärtäminen voi auttaa tulkitsemaan monimutkaista ja vaikeaselkoista tietosuoja-asetusta. Periaatteet ovat keskenään jonkin verran päällekkäisiä ja limittäisiä, minkä vuoksi ne kannattaa mieltää yhtenä kokonaisuutena. Kuviossa 1 esitetään henkilötietojen käsittelyn yleiset periaatteet, joista kerrotaan tässä luvussa vielä tarkemmin. (Korpisaari ym. 2018, 23, 97.)

KUVIO 1. Henkilötietojen käsittelyn periaatteet (EU:n yleinen tietosuoja-asetus 2016/679, artikla 5 - 6).

4.2.1 Lainmukaisuus, läpinäkyvyys ja kohtuullisuus

Henkilötietoja on käsiteltävä aina lainmukaisesti, asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi. Lainmukaisuus tarkoittaa sitä, että henkilötietojen käsittelylle tulee aina olla tietosuoja-asetuksessa määritelty lainmukainen peruste. Näitä perusteita ovat esimerkiksi sopimus, suostumus ja rekisterinpitäjän oikeutettu etu. Läpinäkyvyyden periaatteen mukaan rekisteröidyille tulee antaa tiedot siitä, miten, mitä ja mihin tarkoituksiin heitä koskevia tietoja käsitellään. Tietojen tulee olla helposti saatavilla, sekä selkeällä ja yksinkertaisella kielellä ilmaistuna. Tietosuoja-asetuksessa säädetään vielä erikseen siitä, mitä tietoja rekisteröidyille tulee toimittaa. Henkilötietojen käsittelyn tulee olla myös kohtuullista; tämä tarkoittaa sitä, että rekisterinpitäjän tulee ottaa huomioon rekisteröityjen edut sekä odotukset. Kohtuullisuus edellyttää myös sitä, ettei tietoja väärinkäytetä, ja se suojaa

rekisteröityjä salaa tapahtuvalta henkilötietojen keräämiseltä. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 5; Korpisaari ym. 2018, 24, 89 - 91.)

4.2.2 Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuus velvoittaa, että henkilötiedot on kerättävä ennalta määriteltyjä, nimenomaisia ja laillisia käyttötarkoituksia varten, eikä kerättyjä tietoja saa käsitellä näiden käyttötarkoitusten kanssa yhteensopimattomalla tavalla. Käyttötarkoitussidonnaisuus sallii siis henkilötietojen käsittelyn myös muihin tarkoituksiin, silloin kun käsittely on yhteensopivaa alkuperäisten käyttötarkoitusten kanssa. Jos rekisterinpitäjä aikoo käsitellä henkilötietoja jotain muuta kuin alkuperäistä käyttötarkoitusta varten, tulee sen informoida tästä rekisteröityä ennen jatkokäsittelyä. (Elinkeinoelämän keskusliitto, 5.1.1; EU:n yleinen tietosuoja-asetus 2016/679, artikla 5.)

Tietosuoja-asetuksessa säädetään erikseen, mitä rekisterinpitäjän tulee ottaa huomioon varmistuakseen siitä, että muuhun tarkoitukseen tapahtuva käsittely on yhteensopivaa alkuperäisten tarkoitusten kanssa. Huomioon tulee ottaa alkuperäisen tarkoituksen ja aiotun käsittelyn väliset yhteydet, henkilötietojen luonne, sekä aiotun käsittelyn mahdolliset seuraukset rekisteröidylle. Rekisterinpitäjän tulee huomioida asianmukaisten suojatoimien olemassaolo. Tärkeää on myös pohtia henkilötietojen keruun asiayhteys, erityisesti rekisterinpitäjän ja rekisteröidyn välisen suhteen kannalta. Tällöin voi miettiä, onko suunniteltu henkilötietojen käsittely odottamatonta rekisteröidyn kannalta, ja kuinka rekisteröity voisi odottaa hänen tietojaan käsiteltävän. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 6; Korpisaari ym. 2018, 126.)

4.2.3 Tietojen minimointi ja täsmällisyys

Kerättyjen henkilötietojen tulee olla asianmukaisia ja olennaisia sen käyttötarkoituksen kannalta, jota varten niitä käsitellään. Tietojen tulee olla rajoitettu vain siihen, mikä on tarpeellista näitä käyttötarkoituksia varten. Rekisterinpitäjä ei siis saa kerätä tai säilyttää henkilötietoja kaiken varalta, eikä kerätyt tiedot saa olla liian laajoja käsittelyn tarkoituksiin nähden. Rekisteröidyn antama suostumuskaan ei oikeuta käsittelemään tai keräämään tietoja tarpeettomasti. (Elinkeinoelämän keskusliito, 5.1.1; Hanninen ym. 2017, 49; Korpisaari ym. 2018, 93.)

Yritykset ovat kiinnittäneet huomiota tietojen minimointiin: *"Se lakihan on hyvä, ja se itessään on herättäny kaikki valveutuneet yrittäjät, että hei, aina ku käsitellään näitä tietoja, niin nyt pitää olla näin, tai ylipäätään kyseenalaistetaan, että tarviiko kaikkee ees tallentaa."* (Yritys D.)

Käsittelyn kohteena olevien henkilötietojen tulee olla täsmällisiä ja ne tulee tarvittaessa päivittää. Rekisterinpitäjän tulee varmistaa, että epätarkat ja virheelliset tiedot poistetaan tai korjataan viipymättä. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 5.)

4.2.4 Säilytyksen rajoittaminen

Rekisterinpitäjä saa säilyttää henkilötietoja muodossa, jossa rekisteröity on tunnistettavissa, ainoastaan niin kauan, kuin se on tarpeen käsittelyn tarkoituksen toteuttamista varten. Tietoja voidaan säilyttää esimerkiksi asiakassuhteen ajan, ja jos asiakassuhde päättyy, on syytä tarkastella, tulisiko henkilötiedot poistaa. Tietoja saatetaan kuitenkin tarvita vielä asiakassuhteen päättymisestä huolimatta laskutusta, perintää tai reklamaatiota varten. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 5; Hanninen ym. 2017, 50.)

Tietoja on mahdollista säilyttää pitempään, mikäli ne säilytetään muodossa, jossa rekisteröityä ei pystytä enää tunnistamaan, eikä tietoja ole enää mahdollista yhdistää rekisteröityyn, esimerkiksi tilastollisia syitä varten. Tietojen säilyttämisestä yleisen edun mukaista arkistointia, tieteellistä tai historiallista tutkimusta varten säädetään erikseen. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 5; Hanninen ym. 2017, 50.)

Säilytysajan tarkka määrittäminen on usein hankalaa; rekisterinpitäjän tulee kuitenkin määritellä säilytysaikaan vaikuttavat kriteerit. Rekisterinpitäjä saattaa olla myös velvollinen säilyttämään tietoja pidempään kuin käyttötarkoituksen kannalta olisi tarpeen, silloin kun lakisääteinen velvollisuus niin vaatii. Esimerkiksi finanssialalla laki rahanpesun ja terrorismin rahoittamisen estämisestä vaatii, että asiakkaan tuntemistietoja säilytetään viiden vuoden ajan vakituisen asiakassuhteen päättymisestä. (Elinkeinoelämän keskusliitto, 5.1.1; Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017, luku 3, § 3.)

Tietosuojalainsäädännön uudistus on tuonut huomiota säilytyksen rajoittamiseen. Yritys B kommentoi asiaa seuraavasti: *"Semmosia muutoksia, että on siivottu vanhoja toimintamalleja pois ja niitten vanhojen tietojen säilytyksestä on luovuttu." "Vanhoja rekistereitä esim. vanhoja vuokraustietoja, joissa oli osotetietoja, ni hävitettiin."*

4.2.5 Tietojen eheys ja luottamuksellisuus

Henkilötietojen käsittelyn on tapahduttava siten, että tietojen turvallisuus ja luottamuksellisuus varmistuvat. Käsittelyn on tapahduttava siten, että tiedot on suojattu luvattomalta ja lainvastaiselta käsittelyltä, tai vahingossa tapahtuvalta vahingoittumiselta, kuten tuhoutumiselta. Henkilötietoja luovuttaessa kolmannelle taholle, on rekisterinpitäjän sitä ennen varmistettava, että myös vastaanottajalla on oikeus tietojen käsittelyyn. (Elinkeinoelämän keskusliitto, 5.1.1; Hanninen ym. 2017, 51.)

Luottamuksellisuus ja tiukentunut tietojen suojaaminen tuli ilmi varsinkin yritys A:n kommentista: *"Me ollaan kuuluttu terveydenhoidon piiriin aikasemminki, et se on ollu itestään selvää, että se on tarkkaa. Mutta sitten on esimerkiks semmosia, että kun me tilataan asiakkaalle linssejä tietokoneella, niin aikasemmin me ollaan voitu laittaa siihen asiakkaan nimi ja ne voimakkuustiedot ja lähetetään se linssihiomolle, tai tuonne tehtaalle, niin nykysin me ei enää siis sitä asiakkaan nimee ja sitä linssitietoja, edes niitä voida laittaa, ennen kun asiakkaan luvalla. Eli pitäis jokaiselta asiakkaalta kysyä lupa, että*

" saammeko näiden sinun silmälasilinssitietojen yhteyteen kirjoittaa myös sinun nimesi?", jos ei, niin sit se pitää koodata jollain numerolla, tai usein käytetään niin sanotusti vajaavaista nimee, et siitä ei pysty tunnistamaan, mutta me tunnistetaan kenelle ne lasit kuuluu."

4.2.6 Sisäänrakennettu ja oletusarvoinen tietosuoja

Rekisterinpitäjän tulee toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta voidaan varmistaa, että organisaatiossa toteutuu sisäänrakennettu ja oletusarvoinen tietosuoja. Tällaisia toimenpiteitä voivat olla mm. henkilöstön asianmukainen koulutus ja ohjeistus, henkilötietojen salaaminen tai anonymisointi, tai erilaisten valvontajärjestelmien käyttöönotto. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 25; Hanninen ym. 2017, 55.)

Sisäänrakennettu tietosuoja, "data protection by design", on huolellisuuden suunnittelun periaate, jossa EU:n yleisen tietosuoja-asetuksen säännökset ja varsinkin tietojen käsittelyn yleiset periaatteet ja rekisteröityjen oikeudet otetaan huomioon jo etukäteen suunniteltaessa henkilötietojen käsittelyä. Oletusarvoinen tietosuoja, "data protection by default", taas on periaate, jonka mukaan rekisterinpitäjän tulee varmistaa, että organisaatiossa käsitellään vain niitä henkilötietoja, joita on tarpeen käsitellä kyseisessä tapauksessa. Velvollisuus käsittää artiklan 25 mukaan varsinkin "henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa". Rekisterinpitäjän on myös varmistettava, etteivät henkilötiedot pääse rajoittamattoman henkilömäärän saataville ilman, että luonnollinen henkilö myötävaikuttaa siihen. (Andreasson, Riikonen ja Ylipartanen 2017, 24; EU:n yleinen tietosuoja-asetus 2016/679, artikla 25; Hanninen ym. 2017, 54.)

4.2.7 Osoitusvelvollisuus

Osoitusvelvollisuus on tietosuoja-asetuksen myötä tullut uusi velvoite, joka ei itsessään luo uusia sisällöllisiä velvoitteita, mutta lisää edellä määriteltyjen tietosuojaperiaatteiden vaikuttavuutta. Sen mukaan rekisterinpitäjän on pystyttävä osoittamaan, että se noudattaa tietosuoja-asetuksen mukaisia tietosuojaperiaatteita; pelkkä lainsäädännön noudattaminen ei siis enää riitä. Osoitusvelvollisuus edellyttää rekisterinpitäjältä tarkempaa suunnittelua, dokumentointia ja sisäistä ohjeistusta, mukaan lukien henkilöstön koulutukset. (Elinkeinoelämän keskusliitto, 5.2.1; Korpisaari ym. 2018, 95.)

Suomen tietotuojavaltuutetun internetsivuilla kerrotaan, että "osoitusvelvollisuus on keskeinen periaate tietosuoja-asetuksessa", jonka tarkoitus on lisätä rekisterinpitäjään kohdistuvaa luottamusta. Osoitusvelvollisuuden laajuus riippuu organisaation koosta, henkilötietojen luonteesta ja määrästä. Tietosuojavaltuutetun internetsivuilla luetellaan toimenpiteet ja dokumentit, joita voidaan käyttää osoitusvelvollisuuden toteuttamiseksi. Näitä dokumentteja ovat mm. seloste käsittelytoimista, käsittelyn oikeusperustetta koskevat arviot, riskiarvioita koskeva dokumentaatio, tietoturvaloukkausten dokumentointi sekä tietosuojavastaavan asemaan ja tehtäviin liittyvä dokumentaatio. Se mitä dokumentteja osoitusvelvollisuuden noudattamiseksi tarvitaan, riippuu esimerkiksi henkilötietojen käsittelystä aiheutuvan riskin tasosta, käsittelyn oikeusperusteesta ja siitä käytetäänkö tietojen käsittelyyn erillistä henkilötietojen käsittelijää, tai onko kyseessä yhteisrekisteri. Käytännössä rekisterinpitäjän tulee

kuvata henkilötietojen käsittelyyn liittyvät prosessit ja dokumentoida kuinka tietosuojaperiaatteita noudatetaan. Dokumentaation tulee pitää ajantasaisena, ja asiakirjat on päivitettävä tarpeen vaatiessa. (Tietosuojavaltuutetun toimisto e; Hanninen ym. 2017, 51, 53.)

Tietosuoja-asetuksen voimaantullessa keväällä 2018 osoitusvelvollisuuden vaatimien dokumenttien teko lisäsi työmäärää osalla haastatelluissa yrityksissä. *"Just se kartotus, että jos tietosuojavaltuutettu tulee tarkistamaan, että meillä on joka toimipisteessä ne paperit sitte tehty (…) se kyllä lisäs minun työmäärää paljo, sillä tavalla se perehtyminen."* (Yritys C.) Myös Yritys B toteaa, että selosteiden päivittäminen oli työlästä: *"Siinä vaiheessa piti niitä selosteita tehä, niin se oli työ kyllä. Siitä syystä, että joutu ettimään sitä tietoa aika paljon, kun sitä ei ollu missään saatavana."*

Eräs haastateltavista arveli, etteivät kaikki pk-yritykset ole tehneet vielä dokumentaatiota: "*Osa otti sen ihan tosissaan ja teki ne dokumentit, mutta kyllä mä veikkaan, että ne on aika pieni osa."* (Yritys D.)

4.3 Käsittelyn lainmukaisuus

Tietosuoja-asetuksessa määritellään perusteet, joiden nojalla henkilötietoja voi käsitellä. Nämä perusteet esitetään kuviossa 2. Henkilötietojen käsittelylle on aina oltava lainmukainen peruste. Uusi tietosuojasääntely on tältä osin yhteneväinen aikaisemmin voimassa olleen henkilötietolain kanssa. Joissain tapauksissa käsittelyperusteita voi olla useampiakin. Rekisterinpitäjän kannattaa kuitenkin huomioida, että käsittelyperuste voi vaikuttaa rekisteröidyn oikeuksiin, kuten oikeuteen siirtää tiedot järjestelmästä toiseen. (Elinkeinoelämän keskusliitto, 5.1.2; EU:n yleinen tietosuoja-asetus 2016/679, artikla 20.)

KUVIO 2. Henkilötietojen käsittelyn lainmukaiset perusteet (EU:n yleinen tietosuoja-asetus 2016/679, artikla 6).

4.3.1 Suostumus

Henkilötietoja voidaan käsitellä, jos rekisteröity on antanut suostumuksensa tietojensa käsittelyyn yhtä tai useampaa käyttötarkoitusta varten. Suostumus on ollut jo ennen tietosuoja-asetuksen voimaantuloa yksi henkilötietojen käsittelyperusteista. Tietosuoja-asetus on kuitenkin tuonut suostumukselle tarkemmat kriteerit ja asetuksessa oleva osoitusvelvollisuus koskee myös suostumusta. (Talus, Autio, Hänninen, Pihamaa ja Kantonen 2017, 20.)

Suostumuksen tulee olla vapaaehtoinen ja yksilöity. Jos suostumus pyydetään kirjallisessa muodossa, joka käsittelee myös muita asioita, on suostumuksen antamista koskeva pyyntö esitettävä selkeästi ja muusta informaatiosta erillään. Suostumus tulee pyytää helposti ymmärrettävästi, selkeästi ja yksinkertaisella kielellä esitettynä. Jos suostumus koskee erityisten henkilötietoryhmien mukaisien henkilötietojen käsittelyä, on suostumuksen oltava nimenomainen. Suostumus ei voi syrjäyttää tietosuoja-asetuksessa määriteltyjä henkilötietojen käsittelyn periaatteita, kuten käyttötarkoitussidonnaisuutta tai tietojen minimointia. Rekisteröity ei siis voi antaa suostumusta, jonka nojalla hänen henkilötietojaan voitaisiin käyttää mihin vain tarkoitukseen ja miten tahansa. Suostumus, joka on pyydetty tietosuoja-asetuksen vastaisesti, ei ole sitova. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 7; Korpisaari ym. 2018, 102; Talus ym. 2017, 20.)

Suostumusta henkilötietojen käsittelyyn ei voi antaa vaikenemalla tai valmiiksi rastitetulla ruudulla. Suostumusta ei voi myöskään antaa jättämällä jonkin toimen toteuttamatta. Suostumuksen vapaaehtoisuutta arvioidessa voidaan ottaa huomioon, onko suostumuksen antaminen asetettu sellaisen palvelun tai sopimuksen ehdoksi, jonka olisi voinut täyttää ilman niitä henkilötietoja, joiden käyttöä varten suostumus pyydetään. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 7; Talus ym. 2017, 20.)

Jos suostumusta käytetään henkilötietojen käsittelyn perusteena, kannattaa kiinnittää huomioita siihen, kuinka suostumus pyydetään. Rekisterinpitäjän tulee pystyä todistamaan suostumuksen olemassaolo, joten suostumus kannattaa pyytää tavalla, jolla suostumuksen pystyy dokumentoimaan. Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa, ja sen on oltava yhtä helppoa kuin suostumuksen antaminen. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 7; Korpisaari ym. 2018, 101.)

4.3.2 Sopimus

Henkilötietoja saa käsitellä sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena. Rekisteröidyn pyynnöstä henkilötietoja voidaan käsitellä myös sopimuksen tekemistä edellyttävien toimenpiteiden toteuttamiseksi. Tällainen sopimusta edeltävä toimenpide voisi olla kyseessä esimerkiksi silloin, kun rahalaitos käsittelee henkilötietoja luottopäätöksen tekoa varten. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 6; Korpisaari ym. 2018, 102 - 103.)

Sopimusta voi käyttää käsittelyperusteena erilaisissa sopimus- ja asiakassuhteissa. Oikeus henkilötietojen käsittelyyn on silloin, kun sopimusta ei voida täyttää ilman näiden henkilötietojen käsittelyä.

Sopimus oli määritelty henkilötietojen käsittelyperusteeksi jo ennen tietosuoja-asetuksen voimaantuloa aikaisemmassa lainsäädännössä. (Korpisaari ym. 2018, 102.)

4.3.3 Elintärkeä etu ja lakisääteisen velvollisuuden noudattaminen

Yksi henkilötietojen käsittelyn peruste on elintärkeän edun suojaaminen. Henkilötietolaissa oli määritelty, että henkilötietojen käsittely on sallittua yksittäistapauksessa, jos se on tarpeen rekisteröidyn elintärkeän edun suojelemiseksi. Tietosuoja-asetus laajentaa tätä oikeutta hieman pidemmälle, sillä siinä säädetään, että tietoja saa käsitellä, mikäli se on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Elintärkeä etu voisi olla käsittelyn perusteena esimerkiksi elintarvikkeen hengenvaarallisesta myrkyllisyydestä varoittaessa. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 6; Henkilötietolaki 523/1999, § 8; Korpisaari ym. 2018, 106.)

Tietosuoja-asetuksessa säädetään, että henkilötietoja saa käsitellä silloin, kun se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Näistä lakisääteisistä velvoitteista on voitu säätää joko unionin oikeudessa tai kansallisessa lainsäädännössä. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 6.)

4.3.4 Yleinen etu ja julkisen vallan käyttäminen

Tietosuoja-asetuksessa säädetään, että henkilötietojen käsittely on sallittua silloin, kun se on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Tietosuoja-asetuksessa annetaan tässä kohtaa liikkumavaraa kansalliselle lainsäädännölle, samoin kun rekisterinpitäjän lakisääteisen velvoitteen kohdalla. Henkilötietojen käsittelystä yleisen edun ja julkisen vallan käyttämistä varten säädetään tarkemmin kansallisessa tietosuojalaissa, jota sovelletaan tietosuoja-asetuksen rinnalla. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 6.)

Tietosuojalaissa yleisen edun nojalla henkilötietoja saa käsitellä tieteellistä ja historiallista tutkimusta varten, tutkimusaineistojen ja kulttuuriperintöaineistojen arkistoimisessa, sekä silloin, kun se on tarpeen viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi, tai jos tiedot kuvaavat henkilön asemaa, tehtäviä sekä niiden hoitoa julkisyhteisössä, elinkeinoelämässä tai järjestötoiminnassa. Jos henkilötietoja käsitellään edellä mainittuja tarkoituksia varten, tulee käsittelyn olla oikeasuhtaista sillä tavoiteltuun yleisen edun mukaiseen päämäärään nähden. (Tietosuojalaki 1050/2018, § 4.)

4.3.5 Oikeutettu etu

Kun yrityksen on käytettävä henkilötietoja suorittaakseen liiketoimintaan liittyviä tehtäviä, eikä henkilötietojen käsittelyä voida välttämättä perustella tehdyn sopimuksen perusteella tai lakisääteisellä velvoitteella, voi yritys perustella henkilötietojen käsittelyä oikeutetulla edulla. Oikeutettua etua voidaan käyttää käsittelyperusteena silloin, kun rekisterinpitäjän ja rekisteröidyn välillä on merkityksellinen suhde, kuten esimerkiksi asiakkuus tai palvelussuhde. Rekisterinpitäjän oikeutettua etua saatettaisiin käyttää käsittelyperusteena esimerkiksi silloin, kun on kyse yksityisen omaisuuden videovalvonnasta,

asiakastietojen analysoinnista uusien tuotteiden tai palveluiden kehittämistä varten, tai asiakkaiden luottokelpoisuuden arvioimisesta. (Euroopan komissio a; Korpisaari ym. 2018, 122; Tietosuojavaltuutetun toimisto f.)

Henkilötietoja ei saa käsitellä oikeutetun edun perusteella, mikäli rekisteröidyn edut ja oikeudet syrjäyttävät rekisterinpitäjän tai kolmannen osapuolen edut. Lähtökohtaisesti yksityishenkilön edut ja oikeudet ovat suojatumpia, varsinkin jos rekisteröity on lapsi. Rekisterinpitäjä voi arvioida tasapainotestin avulla voiko hän käyttää oikeutettua etua oikeusperusteena henkilötietojen käsittelemiseen. (Tietosuojavaltuutetun toimisto f.)

Tasapainotestissä punnitaan rekisterinpitäjän tai kolmannen osapuolen etuja rekisteröidyn oikeuksiin ja etuihin. Tasapainotestissä on kuusi vaihetta. Ensimmäiseksi tulee miettiä, onko oikeutettu etu käsittelyperusteena sopivin, toisena tulee miettiä täyttyvätkö perusvaatimukset. Oikeutetun edun tulee olla lainmukainen, selkeästi ilmaistu ja edustaa todellista ja välitöntä tarvetta. Etu ei saa olla spekulatiivinen. Kolmanneksi tulee harkita, onko henkilötietojen käsittely välttämätöntä edun saavuttamiseksi. Tämän jälkeen punnitaan, syrjäyttääkö oikeutettu etu rekisteröidyn oikeudet ja edut. Tällöin tulee ottaa huomioon, millaisesta edusta on kyse, miten henkilötietojen käsittely olisi hyödyksi ja mitä haittaa käsittelemättä jättämisestä olisi. Sen jälkeen tulee selvittää, miten henkilötietojen käsittely voisi vaikuttaa rekisteröityyn; minkä luonteisia käsiteltävät henkilötiedot ovat, miten henkilötietoja käsiteltäisiin ja miten toimenpiteet vaikuttaisivat rekisteröityyn? Mitä arkaluonteisempia käsiteltävät tiedot ovat, sitä enemmän käsittelystä voi tulla seurauksia rekisteröidylle. (Tietosuojavaltuutetun toimisto f.)

Henkilötietojen käsittely ei saa olla rekisteröidylle odottamatonta ja ennakoimatonta. Kannattaa pohtia, osaisiko rekisteröity odottaa, että hänen tietojaan käsitellään näin, ja onko todennäköistä, että rekisteröity pitäisi tietojensa käsittelyä kyseenalaisena tai vastustaisi käsittelyä. (Tietosuojavaltuutetun toimisto f.)

Jos punninnan jälkeen oikeutettua etua voidaan käyttää henkilötietojen käsittelyn perusteena, tulee sen jälkeen tarkistaa tietosuojan lisätakeet. Käsittelyn mahdollisia vaikutuksia rekisteröidylle voidaan lieventää tietosuojaa takaavilla toimenpiteillä, kuten laajalla anonymisointitekniikan käytöllä, henkilötietojen salauksella sekä erilaisilla teknisillä ja organisatorisilla toimenpiteillä, joilla varmistetaan, ettei tietoja käytetä muihin tarkoituksiin. Viimeisenä rekisterinpitäjän tulee osoittaa toiminnan laillisuus ja avoimuus. Tasapainotestin käytöstä tulee laatia kirjallinen ja tarkka kuvaus osoitusvelvollisuuden täyttämiseksi. Rekisterinpitäjän kannattaa varautua perustelemaan rekisteröidylle, miksi henkilötietojen käsittely on oikeutetun edun mukaista. (Tietosuojavaltuutetun toimisto f.)

Kun oikeutettua etua käytetään henkilötietojen käsittelyn perusteena, on rekisteröidyllä oikeus vastustaa tietojensa käsittelyä. Mikäli rekisteröity vastustaa henkilötietojensa käsittelyä, tulee käsittelyn tarve arvioida uudemman kerran. Aikaisemmassa lainsäädännössä yhtenä henkilötietojen käsittelyperusteena toimi asiallinen yhteys, jonka nojalla yritykset saattoivat käsitellä työntekijöidensä tai asiakkaidensa tietoja. Nykyään näissä tapauksissa yritys voi perustaa käsittelyn oikeutettuun etuun. (Elinkeinoelämän keskusliitto 5.1.2; Tietosuojavaltuutetun toimisto f.)

4.3.6 Erityiset henkilötietoryhmät

Erityisten henkilötietoryhmien käsittely on lähtökohtaisesti kielletty, niitä saa käsitellä vain poikkeustapauksissa silloin, kun siitä on tietosuoja-asetuksessa, kansallisessa lainsäädännössä tai EU-oikeudessa säädetty. Erityisiin henkilötietoryhmiin kuuluu tietosuoja-asetuksen mukaan rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot, terveyttä koskevat tiedot sekä geneettiset ja biometriset tiedot silloin, kun niitä käsitellään tunnistamista varten. Erityisten henkilötietoryhmien käsittely on yksityisyyden kannalta riskialtista, minkä vuoksi ne tarvitsevat erityistä suojaa. (Elinkeinoelämän keskusliitto 2019 5.1.3; Korpisaari ym. 2018, 148.)

Lista erityisistä henkilötietoryhmistä vastaa pitkälti aikaisemmin voimassa olleen henkilötietolain ”arkaluonteisia henkilötietoja”, joiden käsittely oli niin ikään kiellettyä. Tietosuoja-asetuksessa uutena on biometristen ja geneettisten tietojen tunnistamista varten tehdyn käsittelyn kielto. Tietosuoja-asetuksen erityisiin henkilötietoryhmiin eivät kuulu sosiaalihuollon tarve tai sosiaalihuollosta saadut palvelut, niin kuin ne kuuluivat arkaluontoisiin henkilötietoihin. Arkaluontoisiin henkilötietoihin kuuluivat myös rikollisia tekoja, rangaistuksia ja seuraamuksia koskevat tiedot, tietosuoja-asetuksessa niistä säädetään erikseen artiklassa 10. (Korpisaari ym. 2018, 149 - 151.)

Erityisten henkilötietoryhmien käsittelykieltoa ei voida kiertää käsittelemällä sellaisia tietoja, jotka välillisesti paljastavat rekisteröidystä erityisiin henkilötietoryhmiin kuuluvia tietoja. Esimerkiksi henkilön vaatetuksen, nimen, äidinkielen ja vanhempia koskevien tietojen yhdistelmä voisi paljastaa hänen etnisen alkuperänsä. Henkilön seksuaalisen suuntautumisen voisi taas paljastaa hänen partnerinsa nimi. (Korpisaari ym. 2018, 151.)

Tietosuoja-asetuksen artiklassa 9 on säädetty poikkeustapauksista, jolloin erityisten henkilötietoryhmien käsittely on sallittua. Näin on esimerkiksi silloin, kun rekisteröity on antanut nimenomaisen suostumuksen kyseisten henkilötietojen käsittelyyn, paitsi jos unionin oikeudessa tai kansallisessa lainsäädännössä säädetään, ettei käsittelykieltoa voida kumota rekisteröidyn suostumuksella. Poikkeustapauksia on useita, ja tietosuojalaissa niitä tarkennetaan vielä lisää. Tietosuojalaissa säädetään myös tarkemmin toimenpiteistä, jotka henkilötietojen käsittelijän ja rekisterinpitäjän on toteutettava erityisiä henkilötietoryhmiä käsiteltäessä. Näitä toimenpiteitä ovat mm. tietosuojavastaavan nimittäminen, henkilötietojen pseudonymisointi, sisäiset toimenpiteet, joilla estetään pääsy tietoihin, tietosuoja-asetuksen mukaisen vaikutusten arvioinnin laatiminen, sekä muut tekniset ja organisatoriset toimenpiteet. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 9; Tietosuojalaki 1050/2018, § 6.)

Henkilötunnuksen käsittelystä säädetään erikseen tietosuojalaissa. Henkilötunnusta saa käsitellä rekisteröidyn suostumuksella, tai jos käsittelystä säädetään laissa sekä silloin kun rekisteröidyn yksiselitteinen yksilöiminen on tärkeää. Esimerkiksi yritys D toteaa: *”Hetuja meillä ei tarkotuksella ole, et niitä me ei missään nimessä kerätä.”* (Tietosuojalaki 1050/2018, § 29.)

5 REKISTERÖIDYN OIKEUDET JA REKISTERINPITÄJÄN VELVOLLISUUDET

5.1 Rekisteröidyn oikeudet

EU:n yleinen tietosuoja-asetus määrittää rekisteröityjen henkilöiden oikeudet edeltävää lainsäädäntöä tarkemmin artikloissa 12 - 22. Oikeudet esitellään kuviossa 3. Näistä oikeuksista osa on lainsäädännöllisesti täysin uusia. Rekisteröityjen oikeuksien toteutuminen on organisaatioiden velvollisuutena. Oikeuksien toteutumista tulee myös edesauttaa esimerkiksi siten, että ohjeet oikeuksien toteutuksista ovat helposti saatavilla rekisteröidyille. (Hanninen ym. 2017, 56 - 57.)

Jos rekisteröity päättää toteuttaa oikeuksiaan, kuten oikeutta saada siirtää tietonsa järjestelmästä toiseen, tulee organisaation toteuttaa pyyntö oletusarvoisesti kuukauden sisällä pyynnöstä ja maksutta. Jos pyyntöjä on paljon, tai ne ovat huomattavan monimutkaisia, voidaan määräaikaa jatkaa mahdollisesti kahdella kuukaudella. Tapauksessa, jossa pyynnöillä ei ole kunnollisia perusteita tai jos ne ovat kohtuuttomia, voidaan rekisteröidyltä myös periä kohtuullinen maksu pyynnön toteuttamiseksi. (Hanninen ym. 2017, 58 - 59.)

Haastateltavat eivät kokeneet, että rekisteröidyt pyrkisivät käyttämään oikeuksiaan enemmän, kuin aikaisemmin. *"Aina on ollu mun mielestä ehkä vuodessa yks asiakas, semmonen, joka haluaa, että hänestä ei saa jäädä mitään tietoja, tai että voitteko poistaa hänen tiedot."* (Yritys A.) Yritys D:n kokemuksien mukaan taas rekisteröidyiltä ei ollut tullut pyyntöjä ollenkaan: *"Me ei tiedetä yhtään tapausta esimerkiks meidän asiakkaittenkaan kautta, missä ois tullu. Meihin varmaan otettas yhteyttä todennäkösesti, jos ois tullu, että hei asiakas haluaa tietää hänen tietonsa tän meidän yritysasiakkaan järjestelmissä, niin ei oo tullu tuommosia."*

KUVIO 3. Rekisteröidyn oikeudet (EU:n yleinen tietosuoja-asetus 2016/679, artikla 12 - 22).

5.1.1 Rekisteröidyn tunnistaminen ja oikeus saada pääsy tietoihin

Jotta vältyttäisiin toisten rekisteröityjen oikeuksien loukkaamiselta, on organisaation tunnistettava rekisteröity hänen halutessa käyttää yleisen tietosuoja-asetuksen mukaisia oikeuksiaan, mutta vain silloin, jos organisaation toiminta edellyttää rekisteröidyn tunnistamista. Rekisteröidyn tunnistaminen voidaan hoitaa esimerkiksi paikan päällä kuvallisella henkilöllisyystodistuksella tai verkossa tapahtuvissa tapauksissa asiakas voi kirjautua palveluun omilla tunnuksillaan. (Hanninen ym. 2017, 57 - 58; Valtiovarainministeriö 2016, 13.)

Rekisteröidyllä on oikeus saada pääsy omiin tietoihinsa, ja rekisteröidyllä on oikeus saada tietää, käsitelläänkö hänen tietojansa vai ei. Henkilötietolaissa 523/1999 §:ssä 26 kerrotaan tarkistusoikeudesta, joten oikeus saada pääsy tietoihin ei ole kansallisessa lainsäädännössä täysin uusi asia. Jos tietoja käsitellään, rekisteröidyn pyynnöstä rekisterinpitäjän tai henkilötietojen käsittelijän on toimitettava jäljennös tiedoista, joita rekisteröidyn osalta organisaatiossa käsitellään. Lisäksi hänelle on toimitettava artiklassa 15 mainitut lisätiedot, joita ovat mm. tietojen säilytysaika, käsittelyn tarkoitus ja

oikeus tehdä valitus valvontaviranomaiselle. Nämä tiedot voivat myös löytyä esimerkiksi yrityksen tietosuojaselosteesta. Koska tiedot voivat olla organisaatiossa hajallaan eri järjestelmistä, on järjestelmien kehittäminen organisaation sisällä yhtenäiseksi suotavaa. Tietoja luovuttaessa rekisteröidylle on huomioitava, että se ei saa aiheuttaa haittaa toisten oikeuksille ja vapauksille. Oikeutta on myös rajattu tietosuojalaissa 1050/2018 § 34:ssä mm. sellaisissa tapauksissa, joissa tietojen antaminen voi olla uhkana yleiselle turvallisuudelle tai rikosten ehkäisylle, tai jos tietojen luovuttaminen voi aiheuttaa vaaraa rekisteröidyn terveydelle. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 15; Hanninen ym. 2017, 59 - 61; Valtiovarainministeriö 2016, 14 - 15.)

5.1.2 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

Oikeus tietojen oikaisemiseen vastaa hyvin pitkälti henkilötietolain 523/1999 § 29 tiedon korjaamista. Rekisteröidyllä on siis oikeus vaatia, että häntä koskevat henkilötiedot muokataan totuutta vastaavaksi niiden ollessa virheellisiä, tai että niitä täydennetään, jos ne ovat puutteellisia. (Henkilötietolaki 523/1999, § 29; Valtiovarainministeriö 2016, 15.)

Oikeus tietojen poistamiseen, eli ”oikeus tulla unohdetuksi” on yksi EU:n uuden tietosuoja-asetuksen uusista ja puhutuimmista rekisteröidyn oikeuksista. Rekisteröidyllä on oikeus vaatia rekisterinpitäjää poistamaan häntä koskettavat tiedot järjestelmästään tietyissä tapauksissa. Esimerkiksi tapauksessa, jossa hän on aikaisemmin antanut suostumuksen henkilötietojensa käsittelyyn, mutta haluaakin peruuttaa suostumuksen jälkikäteen. Jos henkilötiedot ovat vanhentuneet, niitä ei tarvita enää alkuperäiseen käyttötarkoitukseensa, tai niitä on käsitelty lainvastaisesti, ovat myös mahdollisia tilanteita, joissa rekisteröity voi velvoittaa rekisterinpitäjän poistamaan tietonsa. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 17; Hanninen ym. 2017, 61 - 62.)

Oikeutta tulla unohdetuksi on lisäksi rajattu tietyin edellytyksin. Esimerkiksi tilanteissa, joissa organisaatiossa oikeutettujen etujen toteuttaminen on henkilötietojen käsittelyn voimassa olevana perusteena, tai jos kyseessä on lakisääteinen rekisteri, ei henkilöllä ole välttämättä oikeutta saada tietojaan poistetuksi kyseisestä järjestelmästä. Rekisteröidyn esittäessä pyynnön tietojensa poistamiseen, ja kun tietojen poistolle ei ole mitään lainmukaista estettä, on rekisterinpitäjän poistettava tiedot järjestelmästään viivyttelemättä, ellei viivästykselle ole erillistä perustetta. Asetus ei ota kantaa tietojen konkreettiseen poistamiseen. Jos tietoja ei pystytä poistamaan esimerkiksi teknisistä syistä kokonaan, on rekisterinpitäjän varmistettava, että tietoja ei tulla enää jatkossa käsittelemään, esimerkiksi salaamalla ne luotettavalla salausavaimella. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 17; Hanninen ym. 2017, 62 - 63; Valtiovarainministeriö 2016, 15 - 16.)

5.1.3 Oikeus käsittelyn rajoittamiseen

Tietyissä tapauksissa rekisteröidyllä on oikeus vaatia organisaatiota rajoittamaan henkilötietojensa käsittelyä. Konkreettisesti käsittelyn rajoittaminen tarkoittaa sitä, että tietoja saa käsitellä pelkästään rekisteröidyn luvalla tai lakiperusteisista syistä. Esimerkiksi tilanteessa, jossa rekisteröidyn mielestä järjestelmässä olevat henkilötiedot ovat virheellisiä, käsittelyä voidaan rajoittaa henkilötietojen

oikeellisuuden todentamisen ajaksi. Henkilötietojen rajoittaminen voi olla ajankohtaista myös tapauksissa, joissa rekisteröity on pyytänyt henkilötietojensa poistoa ja rekisterinpitäjä vastustaa tätä, tai jos henkilötietojen käsittely ei ole ollut lainmukaista. Jos rekisterinpitäjä aikoo jatkaa henkilötietojen käsittelyä, on sen ilmoitettava asiasta rekisteröidylle ennakkoon. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 18; Hanninen ym. 2017, 63 - 64.)

5.1.4 Oikeus siirtää tiedot järjestelmästä toiseen

Myös uutena oikeutena rekisteröidyllä on oikeus artikla 20. mukaan saada henkilötietonsa siirrettyä rekisterinpitäjältä toiselle ”jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa”, mutta vain siinä tapauksessa, jos rekisteröidyn henkilötietojen käsittely perustuu suostumukseen tai sopimukseen ja on automatisoitu. Tämä voi velvoittaa rekisterinpitäjän päivittämään tarvittaessa järjestelmänsä siten, että yllä olevat vaatimukset toteutuvat. Rekisterinpitäjien järjestelmien ei tarvitse kuitenkaan olla toistensa kanssa yhteneviä. Jos organisaatiossa henkilötietojen käsittely ei ole automaattista, vaan esimerkiksi tiedot ovat paperisena, tai jos henkilötietojen käsittelyn perusteena on jokin muu kuin sopimus tai suostumus, ei rekisteröidyllä ole tietojensa siirto-oikeutta. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 20; Hanninen ym. 2017, 64 - 66; Valtiovarainministeriö 2016, 16.)

Pelkästään tiedot, jotka rekisteröity on luovuttanut organisaatiolle, kuuluvat siirto-oikeuden piiriin. Taas tieto, joka on kerätty rekisteröidyn toiminnasta ei täten kuulu oikeuden alle. Oikeus siirtää tiedot järjestelmästä toiseen ei saa myöskään aiheuttaa haittaa toisten rekisteröityjen oikeuksiin ja vapauksiin. Kolmansien tietojen siirtäminen ei silti välttämättä ole este, sillä esimerkiksi sähköpostipalveluun rekisteröidyt voivat saada sähköpostin osoitekirjan siirrettyä toisen tarjoajan vastaavanlaiseen palveluun. (Hanninen ym. 2017, 66.)

5.1.5 Oikeus vastustaa käsittelyä eli vastustamisoikeus

Vastustamisoikeus on suomen lainsäädännössä tuttu jo henkilötietolaissa 523/1999 § 30 kielto-oikeuden nimellä. Pykälässä mainitaan, että rekisteröidyllä on oikeus kieltää henkilötietojensa käsittelyn mm. suoramarkkinointi ja -myyntitapauksissa. Yleisessä tietosuoja-asetuksen artiklassa 21 mainitaan, että rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä suoramarkkinointia varten. Lisäksi asetus ottaa kantaa suoramarkkinoinnissa tapahtuvaan profilointiin ja siihen, että rekisteröidyllä on oikeus vastustaa myös tätä. Artiklassa mainitaan, että ”henkilökohtaiseen erityiseen tilanteeseen liittyvällä perusteella” rekisteröity voi vastustaa henkilötietojensa käsittelyä, kun henkilötietojen käsittelyn lainmukaisuus perustuu organisaation oikeutettujen etujen toteuttamiseen tai jos tietojen käsittely on tarpeen 6 artiklan mukaan ”yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuluvan julkisen vallan käyttämiseksi”. Jos rekisterinpitäjällä ei ole merkittävän tärkeätä ja perusteltua syytä, tulee sen lopettaa tietojen käsittely. Perusteltujen syiden tulee olla niin huomattavia, että ne ohittavat rekisteröidyn oikeudet. Oikeus vastustaa käsittelyä tulee informoida rekisteröidylle erikseen ja heti, kun häneen ollaan yhteydessä ensimmäistä kertaa. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 21; Hanninen ym. 2017, 67 - 69.)

5.1.6 Oikeus vastustaa omien tietojen käyttöä automatisoidussa päätöksenteossa

Jos henkilötietojen käsittely tapahtuu täysin automaattisesti, on rekisteröidyllä oikeus olla joutumatta sellaisen automaattisen päätöksen kohteeksi, joka vaikuttaa häneen merkittävästi. Automatisoidun päätöksen, kuten profiloinnin, voi kuitenkin perustella, jos päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai toteuttamista varten, tai jos päätös perustuu lakiin tai suostumukseen. Tällöin päätös voi olla täysin automatisoitu. Täysin automaattinen käsittely voi olla esimerkiksi sähköisesti tapahtuva rekrytointikäytäntö, johon ei osallistu ihmistä. Jos prosessiin osallistuu jossain vaiheessa ihminen, ei rekisteröidyllä ole oikeutta olla joutumatta päätöksen kohteeksi. Oikeus ei koske myöskään lain perusteella pidettyjä julkisen sektorin rekistereitä. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 22; Hanninen ym. 2017, 69 - 70; Valtiovarainministeriö 2016, 16.)

5.1.7 Läpinäkyvä rekisteröityjen informointi

Ennen henkilötietojen käsittelemistä, rekisterinpitäjän tulee informoida avoimesti ja läpinäkyvästi henkilötietojen käsittelyä koskevista asioista. Informointi henkilötietojen käsittelystä on säädetty jo henkilötietolaissa 523/1999 § 24, mutta EU:n yleinen tietosuoja-asetus tarkentaa rekisterinpitäjän velvollisuuksia. (Hanninen ym. 2017, 73.)

Rekisteröidylle tulee informoida helposti ymmärrettävässä muodossa ja maksutta mm. käsittelyn oikeusperuste ja henkilötietojen käsittelyn tarkoitus, henkilötietojen säilytysaika ja rekisteröidyn oikeudet. Jos henkilötietoja ei kerätä suoraan rekisteröidyltä, vaan ne hankitaan muuta kautta, on rekisteröidylle lisäksi ilmoitettava tiedot, jotka hänestä on kerätty ja se, mistä tiedot on saatu. Toimitettavien tietojen yksityiskohdat löytyvät artiklasta 12. Velvollisuutta luovuttaa artiklan mukaiset tiedot rekisteröidylle on rajoitettu tietosuojalaissa 1050/2018 § 33. Velvollisuutta voidaan olla toteuttamatta, jos se on tarpeen esimerkiksi rikosten ehkäisemiseksi tai yleisen turvallisuuden vuoksi. (EU:n tietosuoja-asetus 2016/679, artikla 12; Valtiovarainministeriö 2016, 14.)

Rekisterinpitäjän tulee antaa yllä mainitut tiedot rekisteröidylle henkilötiedot vastaanottaessaan, jos ne kerätään suoraan rekisteröidyltä. Jos henkilötiedot taas hankitaan muuta kautta, tiedot käsittelystä tulee toimittaa rekisteröidylle kohtuullisen ajan kuluttua, mutta joka tapauksessa kuukauden kuluessa tietojen vastaanottamisesta. Tapauksessa, jossa henkilötietoja luovutetaan eteenpäin, tulee rekisteröityä informoida viimeistään silloin, kun tiedot ensimmäisen kerran luovutetaan. Rekisteröityä on informoitava myös tapauksessa, jossa hänen henkilötietojaan käytetään muuhun tarkoitukseen, kun siihen, mihin ne ovat alun perin kerätty. EU:n yleinen tietosuoja-asetus ei kerro tarkasti, miten henkilötietojen käsittelystä tulee informoida rekisteröidylle, kunhan se ilmaistaan selkeästi ja helposti ymmärrettävästi. Tiedot voidaan toimittaa mm. kirjallisesti tai jos tiedot on kerätty sähköisesti, voi tietojen toimituskin tapahtua sähköisessä muodossa. Rekisteröity voi myös pyydettäessä saada informoinnin suullisesti, mutta tällöin rekisterinpitäjän tulee varmistua rekisteröidyn henkilöllisyydestä. Tietosuoja-asetus ei velvoita yrityksiä tekemään rekisteri- tai tietosuojaselosteita, toisin kuin henkilötietolaki 523/1999, mutta tietosuojaselosteet voivat olla tuttu ja helppo tapa tietojen toimittamiseen rekisteröidylle jatkossakin, kunhan siitä löytyy vaadittavat tiedot. Informaatio henkilötietojen käsittelystä

tulee olla julkisesti saatavilla ja ajantasaista. (Hanninen ym. 2017, 74 - 77; Valtiovarainministeriö 2016, 14.)

5.2 Rekisterinpitäjän vastuut ja velvollisuudet

Tietosuoja-asetus tuo rekisterinpitäjälle uusia velvollisuuksia. Aikaisemmasta tietosuojalainsäädännöstä poiketen, asetuksessa säädetään velvollisuuksia myös henkilötietojen käsittelijälle. Tässä opinnäytetyössä huomio on kuitenkin kohdistettu rekisterinpitäjän velvollisuuksiin. Uusissa velvollisuuksissa korostuu riskilähtöinen ajattelu, ja riskitaso vaikuttaa suoraan toimenpiteisiin, jotka rekisterinpitäjän on toteutettava. (Valtiovarainministeriö 2016, 18, 21.)

5.2.1 Rekisterinpitäjän ja henkilötietojen käsittelijän roolit ja vastuut

Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot, se voi kuitenkin käyttää henkilötietojen käsittelijää, joka suorittaa käsittelytoimenpiteet osittain tai kokonaan hänen lukuunsa. Rekisterinpitäjä saa käyttää vain sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet, niin että käsittely täyttää tietosuoja-asetuksen mukaiset vaatimukset. Jotta rekisterinpitäjä voisi varmistua henkilötietojen käsittelijän riittävästä osaamisesta, luotettavuudesta sekä resursseista, voi henkilötietojen käsittelijä osoittaa tämän käyttämällä hyväksyttyjä käytännesääntöjä tai hyväksyttyä sertifiointimekanismia. Viimekädessä rekisterinpitäjä on kuitenkin vastuussa sen lukuun tehdystä käsittelystä. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 24; Korpisaari ym. 2018, 269, 293.)

Artiklassa 28 säädetään henkilötietojen käsittelijästä, sekä tämän ja rekisterinpitäjän välisen sopimuksen sisällöstä. Sopimuksen sisällöstä säädetään yksityiskohtaisesti. Artiklassa säädetään myös, että henkilötietojen käsittelijä ei saa käyttää alihankkijana toista henkilötietojen käsittelijää, ilman rekisterinpitäjän ennakkolupaa. Mikäli alihankkijaa käytetään, tulee tästä ilmoittaa rekisterin pitäjälle, jotta tämä voi halutessaan vastustaa tällaista muutosta. Henkilötietojen käsittelijän ja alihankkijan on tehtävä henkilötietojen käsittelystä vastaava sopimus kuin rekisterinpitäjänkin kanssa. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 28; Korpisaari ym. 2018, 267.)

Henkilötietojen käsittelijä saa käsitellä tietoja vain rekisterinpitäjän ohjeiden mukaisesti. Poikkeuksena ovat tilanteet, joissa unionin tai jäsenvaltion lainsäädännössä määrätään toisin. Mikäli henkilötietojen käsittelijä käsittelee tietoja rekisterinpitäjän ohjeiden vastaisesti tai alkaa käyttämään tietoja omiin tarkoituksiinsa, tulee siitä itsestään rekisterinpitäjä ja näin ollen tähän kohdistuu myös rekisterinpitäjän vastuut. (Korpisaari ym. 293, 297.)

Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ovat ne yhteisrekisterinpitäjiä. Yhteisrekisterinpitäjien tulee määritellä läpinäkyvästi ja selkeästi vastuualueet, tietosuoja-asetuksessa säädettyjen velvoitteiden noudattamiseksi. Tämän järjestelyn keskeiset osiot tulee olla rekisteröidyn saatavilla. Rekisteröity voi tästä järjestelystä huolimatta käyttää tietosuoja-asetuksessa määriteltyjä oikeuksiaan, kaikkia yhteisrekisterinpitäjiä kohtaan. Yhteisrekisteri tarkoittaa

näin ollen yhteistä vastuuta, joka ulottuu myös korvausvastuuseen. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 26; Korpisaari ym. 2018, 285.)

5.2.2 Riskiperusteinen lähestyminen

Yhdeksi tietosuoja-asetuksen keskeiseksi periaatteeksi nousee riskiperusteinen lähestymistapa, jonka tarkoituksena on estää matalan riskin toiminnan ylisäätely, ja toisaalta korostaa henkilötietojen suojaa korkean riskin toiminnoissa. Riskiperusteinen lähestymistapa voi vaikuttaa suurestikin siihen, miten erilaisissa yrityksissä sääntelyä on noudatettava. (Aarnio 2018, 4; Dittmar & Indrenius 2016, 4.)

Riskiperusteisesta lähestymistavasta ei ole erikseen määritelty missään artiklassa, mutta se nousee esille useassa eri kohdassa. Esimerkiksi tietosuoja-asetuksen artikla 25 mukaan luonnollisen henkilön oikeuksille ja vapauksille aiheutuvat riskit on sisäänrakennettua ja oletusarvoista tietosuojaa toteuttaessa otettava huomioon. Artiklassa 32 säädetään, että yrityksen tietoturvan on vastattava riskin tasoa. Tietoturvaa toteuttaessa on myös otettava huomioon uusin tekniikka, toteuttamiskustannukset, käsittelyn luonne, laajuus sekä tarkoitus. Matalan riskin toiminnassa riittävät siis kevyemmät turvamekanismit, verrattuna korkean riskin toimintaan. (Korpisaari ym. 2018, 25, 308.)

Rekisterinpitäjän on siis tehtävä riskiarvio, jotta voisi noudattaa tietosuoja-asetusta. Riskiarvio on toteutettava rekisteröidyn näkökulmasta, ottaen huomioon mitä rekisteröidyn vapauksia ja oikeuksia henkilötietojen käsittely voisi vaarantaa ja mitä vahinkoja rekisteröidylle voisi mahdollisesti aiheutua käsittelystä. Rekisteröidylle aiheutuvia vahinkoja voivat olla esimerkiksi petoksen kohteeksi joutuminen, taloudellinen vahinko, maineen menetys, muu sosiaalinen vahinko tai henkilötietojen pseudonymisoinnin peruuntuminen. Osoitusvelvollisuuden vuoksi rekisterinpitäjän on pystyttävä todistamaan, että riskiperusteista lähestymistapaa on noudatettu. (Tietosuojavaltuutetun toimisto a.)

Yksi haastateltavista yrityksistä näki riskiperusteisen lähestymistavan hyödyllisenä: "*Nyt tämä minkä se toi, että pitää ne riskit kartottaa. Minusta se oli se hyvä pointti. Että missä voi tulla se tietovuoto.*" (Yritys C.) Riskien kartoittamisen yhteydessä kartoitettiin myös, kuinka yrityksen sisällä henkilötietoja käytetään: *"Se oma riskien kartotus, niin minusta se on hyöty, ja mitenkä se tieto kulkee, että vaikka ois kuinka pieni yritys, niin siellä se tieto kulkee silti, että sen kartottaminen, niin ku meillekki se tulee puhelimen kautta, tai asiakas kävelee sisään. Ja sitte kaikki nää uhkat tosiaan, että ulkoset uhkat."* (Yritys C.)

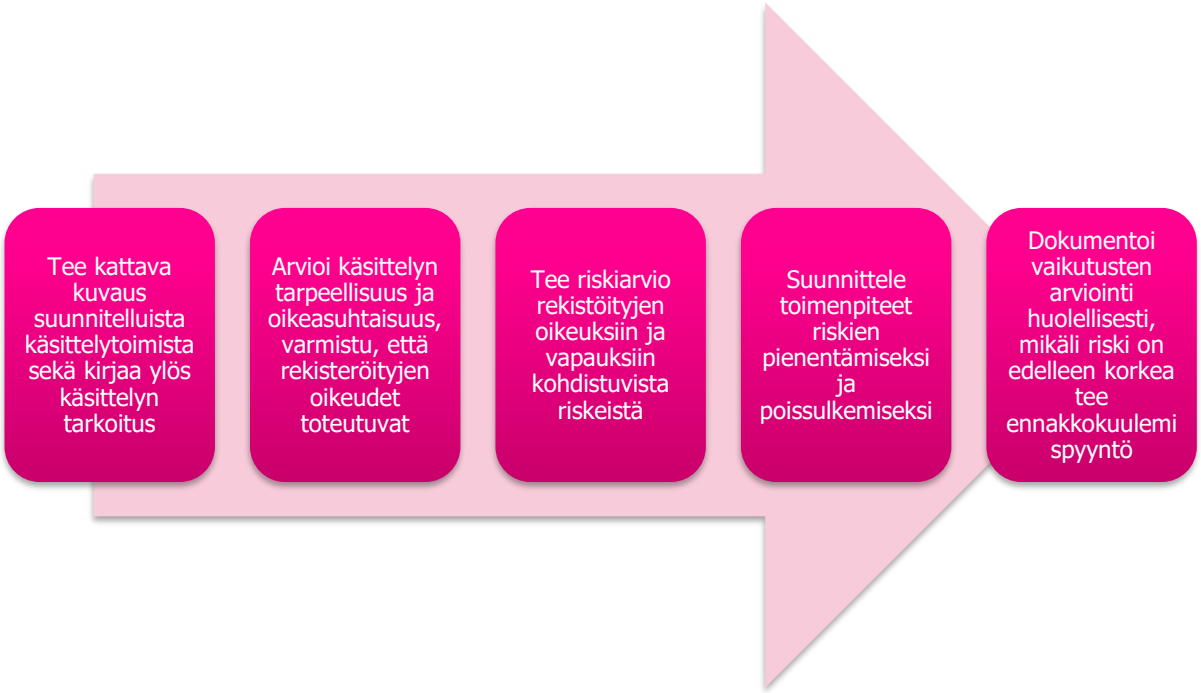
5.2.3 Vaikutustenarviointi

Tietosuoja-asetuksen mukaan rekisterinpitäjän on tehtävä vaikutustenarviointi, mikäli henkilötietojen käsittely aiheuttaisi todennäköisesti korkean riskin rekisteröityjen oikeuksille ja vapauksille. Vaikutustenarviointi on tehtävä erityisesti tilanteissa, jolloin otetaan käyttöön uutta teknologiaa, henkilötietojen käsittely on laajamittaista ja kohdistuu erityisiin henkilötietoryhmiin. Vaikutusten arviointi on tehtävä myös, jos käsittely kohdistuu rikostuomioihin tai rikkomuksia koskeviin tietoihin, sekä tilanteissa, joissa luonnollisten henkilöiden ominaisuuksia arvioidaan järjestelmällisesti ja kattavasti automaattisen käsittelyn avulla, ja tämä johtaa päätöksiin, jotka vaikuttavat henkilöihin merkittävästi.

Vaikutustenarviointi on myös tehtävä yleisölle avoimen alueen järjestelmällisen ja laajamittaisen valvonnan yhteydessä. (Tietosuojavaltuutetun toimisto h.)

Rekisterinpitäjä voi käyttää vaikutustenarviointia työkaluna riskienhallinnassaan myös silloin, kun se ei ole pakollista. Vaikutustenarvioinnin on tarkoitus auttaa rekisterinpitäjää tunnistamaan, arvioimaan ja hallitsemaan käsittelyyn liittyviä riskejä. Vaikutustenarvioinnin jälkeen voidaan päätellä, onko käsittelystä aiheutuva riski tietoturvatoimenpiteiden jälkeen hyväksyttävissä. Jos henkilötietoja käsittelee rekisterinpitäjän sijasta kokonaan tai osittain henkilötietojen käsittelijä, on tätä kuultava vaikutustenarviointia tehtäessä. Vaikutustenarviointi tulee tehdä ennen käsittelyn aloittamista, ja tarpeen vaatiessa se on päivitettävä. (Tietosuojavaltuutetun toimisto h.)

Tietosuoja-asetuksessa ei säädetä varsinaisesti, mitä vaikutustenarviointi pitää sisällään, mutta tietosuojaviranomaisen verkkosivuilla annetaan vaikutustenarvioinnin tekemisestä tarkat ohjeet. Kuviossa 4 kuvataan vaikutustenarvioinnin vaiheet. Verkkosivuilta löytyy myös tietosuoja-asetuksen velvoittama erillinen listaus käsittelytoimista, jotka vaativat vaikutustenarvioinnin. (Tietosuojavaltuutetun toimisto h.)



KUVIO 4. Vaikutustenarvioinnin vaiheet (Tietosuojavaltuutetun toimisto g).

Tietosuojavaltuutetun verkkosivujen mukaan vaikutustenarvioinnin tulisi ensinnäkin sisältää systemaattinen kuvaus suunnitelluista käsittelytoimista ja siitä mihin tarkoituksiin henkilötietoja käsiteltäisiin. Verkkosivuilta löytyy tarkemmat ohjeet kuvauksen sisällöstä. Tämän jälkeen tulisi arvioida käsittelytoimien tarpeellisuus ja oikeasuhtaisuus tarkoituksiin nähden, sekä tehdä arvio rekisteröityjen oikeuksiin ja vapauksiin mahdollisesti kohdistuvista riskeistä. Kun riskit on tunnistettu, voidaan laatia suunnitelma toimenpiteistä, joiden avulla riskejä ja niiden toteutumisen todennäköisyyttä voidaan laskea. Vaikutustenarviointi tulee dokumentoida huolellisesti, jotta rekisterinpitäjä pystyy osoittamaan, että tietosuoja-asetusta on noudatettu. Kaikkien tunnistettujen riskien osalta tulee kirjata mihin

toimenpiteisiin riskien pienentämiseksi ryhdytään, ja arvio siitä, voidaanko toimenpiteiden avulla riski poissulkea, vähentää tai hyväksyä. Mikäli vaikutusten arvioinnissa käy ilmi, että riski on korkea, eikä riskin tasoa pystytä toimenpiteillä laskemaan, tulee rekisterinpitäjän tehdä ennakkokuulemispyyntö tietosuojaviranomaiselle ennen käsittelyn aloittamista. (Tietosuojavaltuutetun toimisto g.)

5.2.4 Ilmoitusvelvollisuus

Tietosuoja-asetuksessa säädetään, että rekisterinpitäjän tulee tietyissä tilanteissa ilmoittaa tietoturvaloukkauksesta tietosuojaviranomaiselle. Tietoturvaloukkaus määritellään asetuksen neljännessä artiklassa loukkaukseksi, jonka seurauksena on vahingossa tapahtuva tai lainvastainen henkilötietojen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 4, 33 - 34.)

Rekisterinpitäjän on ilmoitettava tietosuojaviranomaiselle tietoturvaloukkauksesta ilman aiheetonta viivästystä, mahdollisuuksien mukaan 72 tunnissa, paitsi jos tietoturvaloukkaus ei todennäköisesti aiheuta riskiä luonnollisen henkilön oikeuksille tai vapauksille. Ilmoituksen voi tehdä Suomessa tietosuojavaltuutetun verkkosivuilla sähköisellä lomakkeella. Tietosuoja-asetuksessa säädetään myös siitä, mitä tietoja tietosuojaviranomaiselle tehtävän ilmoituksen tulee sisältää. Henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivästystä, heti saatuaan tietoturvaloukkauksen tietoonsa. (EU:n yleinen tietosuoja-asetus 2016/967, artikla 33; Tietosuojavaltuutetun toimisto d.)

Jos tietoturvaloukkaus aiheuttaa todennäköisesti korkean riskin luonnollisen henkilön oikeuksille ja vapauksille, on rekisterinpitäjän ilmoitettava tietoturvaloukkauksesta myös rekisteröidylle ilman aiheetonta viivästystä. Rekisteröidylle tehtävässä ilmoituksessa tietoturvaloukkauksen luonne ja sen todennäköiset seuraukset on kuvattava selkeällä ja yksinkertaisella kielellä. Tiettyjen asetuksessa mainittujen edellytysten täyttyessä, ilmoitusta ei kuitenkaan tarvitse tehdä. Jos ilmoituksen tekeminen vaatisi esimerkiksi kohtuutonta vaivaa, tulisi rekisterinpitäjän käyttää julkista tiedonantoa tai vastaavaa toimenpidettä rekisteröidyn informoimiseksi. Rekisterinpitäjän tulee dokumentoida kaikki henkilötietojen tietoturvaloukkaukset. Dokumentoinnista tulee selvitä tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimenpiteet. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 33 - 34.)

Henkilötietojen käsittelyä suunniteltaessa kannattaa myös suunnitella prosessit kriisitilanteiden, kuten tietoturvaloukkauksen varalle. Organisaation kannattaa varautua siihen, kuinka tietoturvaloukkaus tunnistetaan, miten ja missä tapauksissa ilmoitus tehdään, mitkä ovat korjaavat toimenpiteet ja kuinka tapaus dokumentoidaan. Näin organisaatio pystyy tietoturvaloukkauksen sattuessa tehokkaaseen toimintaan vahingon minimoimiseksi, ja palauttamaan toimintakykynsä mahdollisimman nopeasti. (Talus ym. 2017, 33.)

Tietosuojavaltuutetun toimiston helmikuussa 2019 julkaisemassa tiedotteessa kerrotaan, että siitä lähtien, kun ilmoitusvelvollisuus alkoi vuoden 2018 toukokuussa, on tietosuojavaltuutetun toimistolle

saapunut noin 2700 ilmoitusta henkilötietojen tietoturvaloukkauksesta (Tietosuojavaltuutetun toimisto 2019).

5.3 Tietosuojavastaava yrityksessä

Tietosuojavastaavan rooli organisaatiossa voi olla hyvin huomattava. Kaikissa organisaatiossa ei ole tarvetta ja velvoitetta tietosuojavastaavalle, mutta organisaatioissa, joihin sellainen on valittu, rooli on hyvin keskeinen. Hän toimii organisaatiossa asiantuntijana tietosuojalainsäädäntöä koskevissa asioissa ja kriittisessä roolissa EU:n yleisen tietosuoja-asetuksen toteutuksen ja ohjeistuksen osalta. (Andreasson ym. 2017, 86 - 87; EU:n yleinen tietosuoja-asetus 2016/679, artikla 37.)

Yritys A ja C olivat nimittäneet tietosuojavastaavan. *"Minä opiskelin tässä välillä, niin sitten minä samalla, ehkä enemmän vielä paneuduin näihin, siihen liittyviin seikkoihin, tietosuojalakiin ja muuhun. Sillä perusteella minä oon varmaan siinä (tietosuojavastaavana)."* (Yritys A.) *" Itse yrittäjä on tietosuojavastaava, hänet on nimitetty kyllä."* kommentoi haastateltava yritys C ja perusteli nimitystä: *"Hänhän se vastaa yrityksestä, niin hän vastaa myös tästä."* Muissa yrityksissä toimii tietosuojasta vastaava henkilö*. "Koska oon yrittäjä, niin lähinnä sen takia, mutta ei oo niin ku mitään nimikettä."* (Yritys D.) *"No se sattu vaa, kenelle nakki napsahtaa."* (Yritys B.)

5.3.1 Tietosuojavastaavan historiaa

Tietosuojavastaavan rooli ei ole Suomessa täysin uusi tehtävä ja monessa organisaatiossa se on ollut olemassa jo yli kymmenen vuotta. Vuodesta 2007 alkaen on tietosuojavastaavien tehtäviin täytynyt nimittää henkilö SOTE-sektorilla eli sosiaali- ja terveydenhuollon palvelujen antajilla. Tietosuojavastaava on täytynyt nimittää myös apteekkialalla ja Kansaneläkelaitoksessa. Tietosuojakyselyjen perusteella on huomattu käytännön perusasioissa lukuisia vajavaisuuksia. Esimerkiksi henkilökunta ei ole ollut välttämättä tarpeeksi koulutettua asiakas- ja potilastietojen käsittelyssä vaadittavissa tietosuojaasioissa. Valvontaa ei ole toteutettu tarpeeksi ja tietosuojavastaavan tehtävänkuvaus on voinut olla puutteellista. Andreassonin ym. (2017) mukaan Riikonen (2013) on kertonut tutkielmassaan, että yhtenä ongelmista on ollut se, että tietosuojavastaavan tehtäviä ovat hoitaneet useilla erilaisilla tehtävänimikkeillä työskentelevät henkilöt. Tehtävänimikkeinä olivat mm. arkistosihteeri, terveydenhoitaja, palvelupäällikkö ja tietohallintokoordinaattori. Loppujen lopuksi nimikkeitä löytyi jopa 66 kappaletta. EU:n tietosuoja-asetus määrittelee artikloissa 37 - 39 tietosuojavastaavan nimittämisen, aseman ja tehtävät huomattavasti tarkemmiksi ja helpommin toteutettaviksi. (Andreasson ym. 2017, 25, 82 - 83.)

5.3.2 Nimittäminen

Kaikkia organisaatioita ei velvoiteta nimittämään tietosuojavastaavaa. EU:n yleisen tietosuoja-asetuksen myötä määrätyn laisten rekisterinpitäjien on nimitettävä tietosuojavastaava. Artiklan 37 mukaan sellainen on nimitettävä esimerkiksi silloin, kun henkilötietojen käsittelyä harjoittaa julkishallinnon elin tai käsittely kohdistuu 9 artiklassa mainittuihin erityisiin henkilötietoryhmiin. Artiklassa 9 mainitut erityiset henkilötietoryhmät ovat mm. etninen alkuperä, filosofinen vakaumus tai esimerkiksi terveyttä

koskevat tiedot. Artiklassa 37 mainittujen ehtojen mukaan tietosuojavastaavan nimittäminen suuntautuu varsinkin julkisen sektorin organisaatioille, mutta organisaatioissa, joissa käsitellään laajamittaisesti henkilötietoja, on tietosuojavastaavan nimittämistä harkittava. Valtionneuvoston selvitys- ja tutkimustoiminnan teettämän kyselyn perusteella on kuitenkin huomattu, että yrityksillä ei ole vielä kattavaa käsitystä siitä, että tarvitaanko heidän yritykseensä tietosuojavastaavan virkaa. Nimitettävän henkilön kriteereihin kuuluvat riittävä ammattitaito ja tuntemus tietosuojalainsäädännöstä. Hänellä on oltava kattava tieto alasta, sekä resurssit tietosuojavastaavaan kohdistuvien tehtävien suorittamiseen. (Enroth ja Neuvonen 2017, 6; EU:n yleinen tietosuoja-asetus 2016/679, artikla 9, 37 - 38.)

5.3.3 Asema

EU:n tietosuoja-asetuksessa tietosuojavastaavan asemalle asetetaan selkeät raamit. Artiklassa 38 kerrotaan esimerkiksi, että tietosuojavastaavan tehtävänä on raportoida suoraan organisaation johdolle ja hänet on otettava mukaan henkilötietojen suojaamista koskevien ongelmien tarkasteluun. Asema vaatii myös, että vaadittavat resurssit tulee turvata tietosuojavastaavalle ajoissa ja hänelle tulee taata pääsy henkilötietoihin ja käsittelytoimiin tehtäviensä täyttämiseksi. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 38.)

Tietosuojavastaavan asemassa toimivan henkilön tulee olla organisaatiossaan tiedetty ja hänen yhteystietonsa tulee olla vaivatta saatavissa. Kaikissa organisaatioissa tietosuojavastaavan aseman on oltava riippumaton ja tehtävässä on salassapitovelvollisuus. Rekisterinpitäjän ja henkilötietojen käsittelijän on pidettävä huoli siitä, että tietosuojavastaava ei vastaanota tehtäväänsä vaikuttavia ohjeita. Tällaiset ohjeet voivat olla esimerkiksi tietosuojaa käsittelevään laintulkintaan liittyviä tai hänen valvontatyöhönsä liittyvää. Riippumattomuutta kuvaa myös se, että tehtäviensä hoitamisen takia tietosuojavastaavaa ei saa asetuksen mukaan irtisanoa, eikä rangaista. Tietosuojavastaava voi toimia yhtäaikaisesti myös muissa organisaation tehtävissä, kunhan tehtävät eivät tule aiheuttamaan eturistiriitoja. Tietosuojavastaavan roolin voi myös ulkoistaa palveluntuottajille. (Andreasson ym. 2017, 89 - 90; EU:n yleinen tietosuoja-asetus 2016/679, artikla 38.)

5.3.4 Tehtävät

Tietosuojavastaavan toimenkuva koostuu asiantuntijaroolista ja valvonnasta, ja hän on yhdyshenkilönä valvontaviranomaiseen. Asiantuntijana hänen tulee olla tietosuojakysymyksissä neuvovassa ja auttavassa roolissa niin henkilöstölle, kuin organisaation johtavalle portaallekin. Hän voi toimia myös henkilötietojen käsittelyä ja tietosuojalainsäädäntöä koskevissa perehdytyksissä kouluttajana. Tietosuojavastaava valvoo, että organisaatiossa toimitaan tietosuoja-asetuksen mukaisesti, myös dokumentaation osalta, ja on tarvittaessa yhdyshenkilönä valvontaviranomaiseen ja tekee tämän kanssa yhteistyötä. Tietosuojavastaava ei kuitenkaan ole vastuussa rekisterin pitämisestä tai lainmukaisesta henkilötietojen käsittelystä, sillä organisaation johto on aina lopuksi vastuussa organisaationsa toimista. (Andreasson ym. 2017, 86 - 88; EU:n yleinen tietosuoja-asetus 2016/679, artikla 39.)

5.4 Henkilötietojen luovuttaminen tai siirto EU:n ulkopuolelle

Tiedonsiirtoa EU-alueelta sen ulkopuolelle tapahtuu paljon ja varsinkin maailman globalisoituessa yhä enenevissä määrin. Esimerkiksi monet pilvipalveluiden tarjoajat käyttävät palvelimia, jotka ovat Euroopan unionin ulkopuolisissa maissa, niin kutsutuissa kolmansissa maissa. Henkilötietojen siirto kolmansiin maihin on säädeltyä yleisessä tietosuoja-asetuksessa ja se asettaa tarkat kriteerit, joiden perusteella tietojen siirto on sallittua. Yleisen tietosuoja-asetuksen perusteella tietoja saa luovuttaa EU:n ulkopuolelle, jos Euroopan Unionin komissio on päättänyt, että kyseinen valtio on varmistanut riittävän tietosuojan tason. Lista päätöksen saaneista valtioista löytyy esimerkiksi komission omilta verkkosivuilta ja sitä päivitetään tarvittaessa. (Hanninen ym. 2017, 97.)

Tapauksessa, jossa komissio on antanut kyseisestä valtiosta, alueesta tai kansainvälisestä järjestöstä päätöksen, ei erillistä lupaa valvontaviranomaiselta tietojen siirtoon tarvita. Vaikka komissio ei olisi antanut tietojen siirron kohteesta erillistä päätöstä, voi tietoja silti siirtää ilman valvontaviranomaisen lupaa asetuksen artiklassa 46 annetuin asianmukaisia suojatoimia soveltavin perustein. Tällaisia perusteluita ovat mm. komission vahvistamien vakiolausekkeiden käyttö ja yritystä koskevat sitovat säännöt, ”binding corporate rules, bcr”, jotka on mainittu artiklassa 47. Vaikka asianmukaisia suojatoimia sovelletaan tiedonsiirrossa kolmansiin maihin, on silti rekisterinpitäjän ja henkilötiedon käsittelijän varmistettava, että rekisteröidyillä on tarvittaessa käytettävissä oikeussuojakeinoja ja täytäntöönpanokelpoisia oikeuksia. Lisäksi henkilötietojen siirto kolmansiin maihin voidaan toteuttaa tietyissä poikkeuksellisissa erityistilanteissa, jotka on mainittu artiklassa 49. Tällainen tilanne voi olla esimerkiksi se, että rekisteröity on suostunut tietojen siirtoon, kun hänelle on ensin kerrottu siirtoon koskevista riskeistä. (Elinkeinoelämän keskusliitto, 5.4; EU:n yleinen tietosuoja-asetus 2016/679, artikla 45 - 49; Hanninen ym. 2017, 98 - 100, 104.)

5.4.1 Privacy shield

Yhdysvallat on tunnettu henkilötietojen siirtämisen kohdemaa ja monet yritykset käyttävät valtion maaperällä sijaitsevia palvelimia. EU:n komissio ei ole kuitenkaan antanut päätöstä, että Yhdysvalloissa olisi riittävä tietosuojan taso. Tämän vuoksi on luotu EU:n ja Yhdysvaltojen välille Privacy Shield -järjestelmä, jossa siihen liittyneet yhdysvaltalaiset organisaatiot lupaavat noudattaa tiettyjä yksityisyyden suojaa koskevia periaatteita. Privacy Shieldiin liittyneistä yrityksistä löytyy Yhdysvaltojen kauppaministeriön ylläpitämä lista, josta rekisterinpitäjä voi varmistaa, että henkilötietoja vastaanottavan yrityksen kanssa tiedonsiirto on lainmukaista. (Hanninen ym. 2017, 99.)

5.4.2 Brexit

Brexit, eli Iso-Britannian ero Euroopan unionista on tällä hetkellä hyvin keskusteltu ja ajankohtainen aihe. Eron oli määrä tulla voimaan 29.3.2019, mutta EU myönsi brexitille jatkoaikaa 31. lokakuuta asti. Jos erosopimusta ei saada aikaiseksi, on mahdollista, että Britanniaa tullaan käsittelemään EU:n ulkopuolisena maana tietosuoja-asetuksen mukaan. Tällöin henkilötietojen siirtoa Iso-Britannian kanssa tulee käsitellä velvoitteiden mukaisesti. On kuitenkin huomioitava, että Britanniassa on noudatettu yleistä tietosuoja-asetusta sen Euroopan unioniin kuulumisen aikana ja maassa on voimassa

kansallinen tietosuojalaki, joka täydentää tietosuoja-asetusta. On siis todennäköistä, että komissio antaisi tietosuojan riittävyyttä koskevan päätöksen maan osalta. Myös alustavassa erosopimuksen mallissa on arveltu, että Britannia voisi noudattaa tietosuoja-asetusta niin kauan, kunnes päätös annetaan. Täten henkilötietojen siirrolle EU:n ja Iso-Britannian välillä ei koituisi ylimääräisiä ongelmia. (Lexia Asianajotoimisto 2019; Myöhänen 2019.)

Britannian eroaminen Euroopan unionista vaikuttaa mahdollisesti myös yhden haastateltavan yritystoimintaan. Yritys B vastasi tiedusteluun henkilötietojen siirrosta kolmansiin maihin seuraavasti: *"Periaatteessa kyllä, käytännössä ei, mutta ku brexit tulee voimaan ni se… Meillä menee Englantiin henkilötietoja, mutta sehän on tällä hetkellä vielä EU:n sisällä."* Brexit herättää haastateltavassa myös epätietoisuutta: *"Mä en tiiä oikein, et mitä se muuttaa, että senkään ei periaatteessa pitäisi muuttaa mitään. (…) eikä kukaan tiiä. Että oikeestaan siinä ootetaan ohjeistusta sieltä Englannin päästä, koska heijän ongelmahan se on, että mitä siellä tapahtuu. (…) Tää ei oo ainut asia minkä se voi sotkee. Se tulee olemaan aika iso ongelma sitte jossaki vaiheessa."*

5.5 Valvonta ja sanktiot

Ennen yleisen tietosuoja-asetuksen voimaantuloa, henkilötietojen käsittelystä säädettiin henkilötietolailla. Henkilötietolaissa säädettiin, että lainvastaisesta henkilötietojen käsittelystä rekisterinpitäjä voidaan toimita rikoslain mukaisesti henkilörekisteririkkomuksesta sakkoihin. Rekisterinpitäjä on kuitenkin ollut velvollinen korvaamaan lainvastaisesta henkilötietojen käsittelystä aiheutuvan vahingon. Tietosuoja-asetuksen myötä jokaisen jäsenvaltion on nimitettävä valvontaviranomainen, jonka tehtävänä on varmistaa, että tietosuoja-asetusta noudatetaan. Tietosuoja-asetus antaa valvontaviranomaiselle laajemmat valtuudet, joihin kuuluvat esimerkiksi henkilötietojen käsittelykielto ja määrältään huomattavat hallinnolliset sakot. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 51, 57; Henkilötietolaki 532/1999, § 47 - 48.)

Korpisaari, Pitkänen ja Warma-Lehtinen (2018) arvelevat, että näillä keinoilla voi olla paljon suurempi vaikutus organisaatiolle kuin rikosoikeudellisilla suojakeinoilla. Myös oikeusministeriön asianajotoimisto Dittmar & Indreniukselta tilaamassa vaikutustenarvioinnissa arvellaan, että ennen yleisen tietosuoja-asetuksen voimaantuloa, tietosuojalainsäädännössä ei ollut määrältään alhaisten uhkasakkojen lisäksi muita taloudellisia sanktioita, mikä on puolestaan voinut vaikuttaa siihen, ettei tietosuojasääntelyä ole koettu suomalaisissa yrityksissä yhtä keskeiseksi kuin EU:n muissa jäsenvaltioissa toimivissa yrityksissä. (Dittmar & Indrenius 2016, 4 - 5; Korpisaari ym. 2018, 18.)

5.5.1 Valvontaviranomainen

EU:n yleisen tietosuoja-asetuksen artiklassa 51 määrätään, että kunkin jäsenvaltion on nimitettävä riippumaton viranomainen, joka valvoo asetuksen soveltamista. Suomessa valvontaviranomaisen tehtäviä hoitaa opinnäytetyön kirjoittamishetkellä tietosuojavaltuutettu Reijo Aarnio, joka toimii tehtävässään 2020 vuoden lokakuun loppuun saakka, ja on toiminut tietosuojavaltuutetun tehtävässä vuodesta 1997. Hän on Suomen edustaja Euroopan tietosuojaneuvostossa. Tietosuojavaltuutetun tukena toimii

tietosuojavaltuutetun toimisto, johon tietosuojavaltuutettu nimittää henkilöstön. Toimistossa toimii myös asiantuntijalautakunta, joka toimii kolme vuotta kerrallaan, ja sen nimittää valtioneuvosto. Valtioneuvosto vastaa myös tietosuojavaltuutetun nimittämisestä, ja hänen toimintakautensa kestää viisi vuotta. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 51; Tietosuojalaki 1050/2018, § 8 - 12, § 14; Virkkunen 2017.)

Valvontaviranomaisen tehtäviin kuuluvat mm. tietosuoja-asetuksen noudattamisen valvonta, yhteistyö muiden jäsenvaltioiden valvontaviranomaisten kanssa, kuten avunanto ja tietojen vaihtaminen, ja tutkimuksien suorittaminen EU:n yleisen tietosuoja-asetuksen toteutumisesta. Valvontaviranomaisella on myös kattavat valtuudet tehtäviensä toteuttamiseksi. Hänellä tulee olla myös oikeus saada pääsy rekisterinpitäjän ja henkilötietojen käsittelijän tiloihin ja tiedostoihin, jos valvontaviranomaisen tehtävä niin vaatii. Valvontaviranomainen voi tarvittaessa antaa varoituksia ja määräyksiä rekisterinpitäjille, joita ovat mm. oikeus rajoittaa rekisterinpitäjän henkilötietojen käsittelyä tai määrätä hallinnollisia sakkoja. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 57 - 58; Hanninen ym. 2017, 124 - 125.)

Valtionneuvoston selvitys- ja tutkimustoiminnan teettämän tutkimuksen mukaan suomalaiset pk-yritykset toivovat tietosuojaviranomaisen taholta selkeää ja luotettavaa ohjeistusta. Yksi huolista kohdistui tulkinnanvaraisiin oikeudellisiin termeihin, jotka täsmentyvät vasta myöhemmän oikeuskäytännön myötä. Oikeustilan epäselvyys herättää pk-yrityksissä jopa turhautuneisuutta. (Enroth ym. 2017, 1, 5, 8, 10.)

Tarve käytännönläheiselle ja selkeälle ohjeistukselle tuli esiin myös tutkimuksen aikana.
"Toivottavaa nyt on, että se organisaatio, joka valvoo, niin heiltä tulee jotain vinkkejä siitä, kun teette näin, tai seuraatte vaikka näitä julkasuja, niin siellä julkaisuissa mainitaan, niin sehän on hirvee apu kaikille yrittäjille. (…) Mitkä on ne käytännölliset toimet, mitkä kannattaa tehä, jotta GDPR:ää pystytään sitten soveltamaan. Lähinnä ihan perusteista lähtien: tällä kysymyksellä yritys näkee, onko heillä ylipäätään minkälaisia GDPR-velvoitteita, tai siis jokaisella on, mutta jos vastaat kolmeen ensimmäiseen että ei, niin sitten voi olla vastauksena, että joo, sillon riittää, kun teet tämän toimen." (Haastateltava yritys D.)

Myös yritys B toteaa: *"Se on ollu tosi vaikee, vaikee selvittää, että mistä tässä nyt ylipäätään on kysymys, ja ketä se koskee, täsmällisesti ketä, että kaikki se tieto, mitä on annettu, on hirveen ympäripyöreetä."* Kaksi muuta haastatelluista yrityksistä oli saanut tietoa tietosuoja-asetuksesta muun muassa toimialajärjestön ja yrittäjät -järjestön kautta. Järjestöjen antama tieto ja luennot oli koettu hyödyllisiksi. Kaikista haastateltavista yksi koki, ettei tietosuoja-asetuksen tulkinnassa ollut ongelmia. Toinen yritys kommentoi: *"Ennen ku hahmotat ite sen, että mikä tässä se punainen lanka on. Niin siinä meni minulla sitä aikaa, että minä annoin sen hautua välillä ja jatkoin jossain vaiheessa."* (Yritys C.)

5.5.2 Rekisteröidyn valitusoikeus ja one-stop-shop -mekanismi (yhden luukun periaate)

EU:n yleisen tietosuoja-asetuksen mukaan kaikilla rekisteröidyillä henkilöillä on oikeus valituksen tekemiseen valvontaviranomaiselle, jos hän kokee henkilötietojensa käsittelyssä tapahtuneen tietosuoja-asetuksen vastaista toimintaa (Hanninen ym. 2017, 125).

Organisaatio voi halutessaan asioida ainoastaan yhden valvontaviranomaisen kanssa, vaikka sen toiminta ulottuisi useaan EU:n jäsenvaltioon. Tätä kutsutaan yhden luukun periaatteeksi, eli one-stop-shop mekanismiksi. Organisaatio asioi tällöin sen valtion valvontaviranomaisen kanssa, jossa yrityksen päätoimipaikka sijaitsee ja sitä valvontaviranomaista kutsutaan johtavaksi valvontaviranomaiseksi. (Hanninen ym. 2017, 125.)

5.5.3 Hallinnolliset sakot

Uutena asiana EU:n yleisessä tietosuoja-asetuksessa on valvontaviranomaisen oikeus määrätä sanktioita henkilötietojen käsittelyssä tapahtuneesta velvoitteiden laiminlyönnistä rekisterinpitäjälle ja henkilötietojen käsittelijälle (Hanninen ym. 2017, 129; Valtiovarainministeriö 2016, 30).

Valvontaviranomainen voi määrätä organisaatiolle hallinnollisia sakkoja velvoitteiden rikkomisesta. Niiden määräämiseen ja määrään vaikuttavista seikoista kerrotaan EU:n yleisen tietosuoja-asetuksen artiklassa 83. Sakkojen määrä perustuu rikkeen vakavuuden mukaisesti kolmeen luokkaan ja enimmäismäärältään sakko voi olla 20 miljoonaa euroa, tai jos kyseessä on yritys, määrä voi olla 4 % sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Sakko määräytyy sen mukaisesti, kumpi edellä mainituista summista on suurempi. (EU:n yleinen tietosuoja-asetus 2016/679, artikla 83; Hanninen ym. 2017, 129 - 130.)

Esimerkiksi teknologiayhtiö Googlea vastaan tehtiin vakavia syytöksiä EU:n yleisen tietosuoja-asetuksen nimissä viime vuoden puolella. Google käyttää mainosten kohdentamiseen käyttäjiensä tietoja ja valitusten tehneet ryhmät pitävät tätä toimintatapaa asetuksen vastaisena. Ranskan tietosuojaviranomainen CINL on määrännyt n. 50 miljoonan euron sakot Googlelle ja perustelee sen sillä, ettei Google tiedottanut käyttäjiään tarpeeksi tietojen keräämisestä mainoksia varten ja että se on tehnyt yksityisyysasetusten löytymisestä käyttäjälle liian hankalaa. Tiedotteessaan Google ilmoitti, että aikoo tutkia päätöstä tulevia toimenpiteitä varten. (Fox 2019.)

Kukaan haastateltavista ei kuitenkaan kokenut uhkaa sanktioiden osalta. Sakkojen suuruus koettiin uutisoinnissa liioitellulta. *"Siitä oli aika paljon kaiken maailman uhkailua ja 20 miljoonan sakkorangaistusta ja kaikkee muuta höpöhöpöö, ja sitte ku tämä meni ohi tämä tilanne, ni sitte sen jälkeen ei oo kuulunu asiasta yhtään mitään."* (Yritys B.) Myös yritys C oli samoilla linjoilla sanktioiden laajuudesta: *"Se oli ihan vitsi, yrittäjä heitti minulle, että " vai haluatko sinä maksaa 600 000 euroa" (naurua). Minä sitte, että "no hohhoijjaa." Siis sehän on naurettavaa, semmoset sanktiot. Tää Suomi on just tämmönen, siis tulee joku laki, niin Suomessa ollaan heti sanktiota."*

Yritykset toivoivatkin valvontaviranomaiselta ensisijaisesti neuvovaa toimintaa, sillä tietosuojauudistuksen uutisointi on keskittynyt sanktioihin. *"Kun heidän tehtävä on antaa sitä neuvontaa. Että sen pitäs mennä just niin päin, eikä sanktioilla. Jotenki minä otin sen ite vitsinä, sen sanktion. Ja just se, jos tulis nyt joku tietosuojavaltuutettu, niin meillä olis esittää, että meillä on tehty, ja se vois neuvoo, jos ei oo oikein, että mitä sitä puuttuu."* (Yritys C.) Haastateltavat myös odottavat ennakkotapauksia, joista voidaan päätellä mahdollisten sanktioiden suhteellisuus. *"Me ootetaan sitä päätöstä tai ratkasua, et kun tää tietosuojakomitea, tai lautakunta kokoontuu, ja tulee tapaus, missä on hävinny asiakkaan yhteystiedot, kuluttaja-asiakkaiden yhteystietoja, niin mikä se on se sanktio"* (Yritys D.)

5.5.4 Vahingonkorvausvastuu ja uhkasakko

Jos organisaatio ei ole noudattanut EU:n yleisen tietosuoja-asetuksen mukaisia velvoitteita tai on toiminut niiden vastaisesti, ja rekisteröidylle on koitunut rikkomuksista aineellista tai aineetonta haittaa, on organisaatio vahingonkorvausvastuussa. Jos henkilötietojen käsittelyssä tapahtuneessa vahingosta on vastuussa useampi yritys, on jokainen niistä vastuussa täydellisesti koko vahingosta. Rekisteröity voi siis vaatia korvauksen kokonaan yhdeltä vastuussa olevista yrityksistä. Maksanut yritys voi kuitenkin velvoittaa muut vahingosta vastuussa olevat yritykset korvaamaan maksaneelle yritykselle osuutensa. (Hanninen ym. 2017, 130 - 131.)

Tietosuojavaltuutettu voi asettaa uhkasakon tietojen luovuttamista koskevan määräyksen tehosteeksi esimerkiksi silloin, kun organisaatio ei suostu luovuttamaan tarvittavia tietoja tietosuojavaltuutetulle tämän tehtävien toteuttamiseksi. Uhkasakosta määrätään tarkemmin uhkasakkolaissa 1113/1990. (Tietosuojalaki 1050/2018, § 18, § 22.)

5.6 Yrityksissä koetut muutokset

Tietosuojalainsäädännön uudistuminen ei loppujen lopuksi tuonut paljoa muutoksia haastateltavien yrityksien toimintaan. Yritys B:n mukaan: "*Tehtiin niitä selosteita ja laitettiin asioita kuntoon ja tarkisteltiin rekistereitä ja todettiin, että ei tässä oo oikein mitään sen kummallisempaa, et asiat jatkuu aika pitkälti niin ku ennenkin. Ja ennenkin tietenkin on ollut se lähtökohta, että ei tuommosia henkilötietoja ja rekistereitä luovuteta täältä meiltä minnekkää."* Samoin koki yritys A, kysyttäessä onko työmäärä lisääntynyt uudistuksen myötä: **"***Ei nyt voi sanoo, että hirveesti lisääntynyt, niin ku on sanottu, me ollaan kuuluttu terveydenhoidon piiriin aikasemminki, et se on ollu itestään selvää, että se on tarkkaa."*

Uudistus on kuitenkin tuonut tietosuoja-asiat esille laajasti, minkä vuoksi yritykset ovat kiinnittäneet enemmän huomiota tietosuoja-asioihin. "*Kaikki on joutunu tavallaan vähän terästäytymään (…) vähän silleen, ku uudestaan kouluttautumista ja siitä ajatellen, että jos on päässy unohtumaan."* (Yritys A.)

Haastateltavista yrityksistä kaksi kertoi, että tietosuoja-asetuksen voimaantulon myötä on sopimuksia yhteistyökumppaneiden kanssa jouduttu päivittämään ja yrityksistä yksi kertoi joutuneensa tekemään investointeja lainsäädännön vuoksi. Myös suoramarkkinointia oli yrityksissä harkittu uudemman kerran. *"Ehkä aikasempina vuosina helpommin lähetettiin jotain suoramarkkinointia. Ollaan tarkempia*

vielä sen suhteen, että on luvat asiakkailta siihen, että voi lähettää." (Yritys A). Yritys B kertoo: "*Meillä on ollu jotain sähköpostilista -tyyppisiä ratkasuja, mutta niitä ei aktiivisesti oo käytetty muutenkaa viimevuosina, että ne ei oo niin ku markkinoinnillisesti niin tehokkaita, että sitte helpompi oli niin ku hyllyttää se koko juttu ja tuhota se lista."* Muut haastateltavat kertoivat, etteivät he ole tehneet suoramarkkinointia alun perinkään.

Yrityksien tuntemukset lainsäädännön uudistuksesta vaikuttavat ristiriitaisilta. Toisaalta tietosuojalainsäädännön tarkoitukset ymmärretään, ja tavoitetta yksityiselämän suojan toteutumisesta pidetään itsessään hyvänä. Yritys D toteaa: *"Joo, kyllä se lain tarkotus on hyvä, ja näin ollen se hyödyttää alaa ja ylipäätään digitaalisuutta."* Sekä yritys A: *"Välillä tuntuu tosi turhauttavalta, siis silleen, että vähän helpomminki vois jonkun tehä, mutta toisaalta kyllä mä sen ymmärrän, että mikä siinä on lähtökohta, että mihin pyritään."* Samaan aikaan itse tietosuoja-asetus on kokonaisuutena varsin sekava, ja tarve viranomaistaholta saatavalle selkeälle ja käytännölliselle ohjeistukselle korostuu. "*Päällimmäinen ajatus on se, että ihan huuhaata oli koko homma, että omalla tavalla hienoa, että siistittii ja mietittii ja tehtiin vähä asioita parempaan suuntaan, mutta kyllä se ilman semmosia järkeviä ohjeita on lähestulkoon mahdotonta."* (Yritys B.) Positiivisena ja asetuksen eräänä kantava periaatteena nähtiin riskiperusteinen lähestyminen. "*Nyt tämä minkä se toi, että pitää ne riskit kartottaa. Minusta se oli se hyvä pointti.*" (Yritys C.)

6 POHDINTA

Opinnäytetyössä pyrittiin käsittelemään kattavasti ja selkeästi EU:n yleisen tietosuoja-asetuksen ja tietosuojalain tärkeimmät kohdat ja niiden tuomat muutokset. Työn tarkoituksena oli saada käsitys paikallisten pk-yritysten kokemuksista ja tuntemuksista lähes vuosi tietosuojalainsäädännön uudistuksen jälkeen.

Yleisen tietosuoja-asetuksen soveltaminen alkoi toukokuussa 2018, ja se herätti opinnäytetyön tekijöissä suurta mielenkiintoa niin uutisoinnin, kuin heidän työtehtäviensäkin vuoksi. Opinnäytetyöprojekti alkoi pian tämän jälkeen ja aihetta pidettiin pitkään ainoastaan ajatuksen tasolla. Varsinainen työ aloitettiin tammikuussa 2019, ja teoriaosuus valmistui parin seuraavan kuukauden aikana. Tutkimusta ja kokonaisuutta työstettiin kevään aikana ja lopullinen opinnäytetyö oli valmis toukokuussa 2019. Varsinainen tutkimuksen kohde ja tarkoitus muodostuivat teoriaosuuden edetessä, ja täten työ toteutettiin ilman toimeksiantajaa. Tutkimusmenetelmänä käytettiin laadullista, eli kvalitatiivista tutkimusta, joka toteutettiin teemahaastattelun menetelmin. Tutkimusmenetelmä valittiin, koska haluttiin kuvata ilmiötä tietosuojalainsäädännön uudistuksen ympärillä yritysnäkökulmasta.

Teoriaosuuden pohjalta tietosuojalainsäädännön uudistuksen keskeisimmiksi muutoksiksi nousivat osoitusvelvollisuus, riskiperusteinen lähestymistapa, sekä oletusarvoinen ja sisäänrakennettu tietosuoja. Merkittävää oli myös läpinäkyvyyden korostuminen henkilötietojen käsittelyssä. Rekisterinpitäjien velvollisuus on viestiä henkilötietojen käsittelystä läpinäkyvästi, sekä kertoa rekisteröidyille heidän oikeuksistaan. Uudistuksen myötä myös valvonta ja sanktio -käytännöt muuttuivat huomattavasti. Teoriaosuutta tehdessä ihmetystä herätti se, ettei tietojen siirrosta kolmansille osapuolille oltu säädetty tarkemmin. Kolmas osapuoli oltiin kyllä määritelty, ja esimerkiksi läpinäkyvä rekisteröityjen informointi edellyttää, että rekisteröidyille kerrotaan tietojen siirrosta kolmansille osapuolille. Tekijät odottivat kuitenkin huomattavasti täsmällisempää sääntelyä.

Tutkimustulosten perusteella varsinaisia muutoksia yritysten liiketoiminnoissa oli odotettua vähemmän. Muutokset toimintatapoihin kohdistuivat pääsääntöisesti soveltamisen alkamisen vaiheille. Esimerkiksi selosteiden laatiminen, riskien kartoittaminen ja yleinen turhan tiedon siistiminen ja hävittäminen olivat toimenpiteitä, joita yritykset toteuttivat. Muutoksien vähäisyys selittynee sillä, että kaksi yrityksistä kuuluivat terveydenhuollon lainsäädännön piiriin, jossa säätely on ollut jo aikaisemmin tiukempaa. Yritykset myös toimivat ainoastaan Suomen alueella, joten lainsäädännön yhtenäistäminen EU:n alueella ei vaikuttanut haastateltaviin yrityksiin.

Uudistus herätti haastateltavissa niin positiivisia, kuin negatiivisiakin tuntemuksia. Melkein jokaisen haastateltavan mielestä lainsäädännön uudistus koettiin hyvänä ja tarpeellisena uudistuksena, joka herättelee yritykset tarkastelemaan omia toimintatapojaan. Toisaalta taas tietosuojauudistuksen saama laaja mediahuomio, joka käsitteli varsinkin suuria hallinnollisia sakkoja, herätti haastateltavissa jopa hilpeyttä. Negatiiviset puolet uudistuksessa nousivat kuitenkin voimakkaammin esille, sillä vaikka lopulta uudistus koettiin hyödylliseksi, aiheutti sen tuoma hämmennys vahvaa turhautumista kohdeyrityksissä.

Tietosuojauudistuksen aiheuttamien investointien vähäisyys haastateltavilla yrityksillä oli yllättävää. Haastateltavista vain yhdelle uudistus oli tuonut kustannuksia, mutta silloinkin vain ohjelmistopäivitysten myötä. Yllättävänä koettiin myös rekisteröityjen omien oikeuksien käytön vähyys. Kukaan haastateltavista ei kokenut, että rekisteröidyt olisivat käyttäneet oikeuksiaan enemmän kuin ennen, kuten vaatineet tietojensa poistoa. Nämä yllättävät seikat voivat selittyä yritysten henkilötietojen käsittelyn laajuudella, sillä kohdeyrityksissä henkilötietojen käsittely on ollut hyvin vähäistä, tai käsittely on jo aiemmin ollut tarkkaa oman alan erityislainsäädännön vuoksi. Kohdeyritykset ovat kooltaan myös verrattain pieniä, joten investointien tuoma lisäarvo olisi ollut todennäköisesti hyvin vähäistä.

Päällimmäisenä tutkimuksessa nousi esiin haastateltavien tyytymättömyys tietosuojauudistuksen informointiin, ja tarve käytännönläheiselle ja ohjeistavalle viestinnälle. Ennakkotapauksien ja ohjeistuksen puute nosti epävarmoja tuntemuksia oman yrityksen tietosuojan tilasta. Varsinkin tiedonhankinta uudistukseen liittyen koettiin hankalaksi. Seminaareista saatu ja internetistä löydetty informaatio koettiin hyödylliseksi, mutta sekavaksi ja vaikeaselkoiseksi. Varsinaisen punaisen langan löytyminen ja ymmärtäminen siitä, mitä toimenpiteitä uudistus yrityksiltä vaatii, vei huomattavan paljon aikaa ja vaivaa kiireisiltä haastateltavilta. Asetus myös velvoittaa yrityksiä itse määrittämään oman vaadittavan tietoturvan tason, ja tämä tuntui aiheuttavan monelle haastateltavista päänvaivaa. Yksi suurin yhteneväisyys yritysten asenteista olikin tarve aiheeseen liittyvälle selkeälle ja helposti löytyvälle informaatiolle ja neuvonnalle.

Luotettavuutta eli reliabiliteettia tarkasteltiin niin teoriaosuuden, kuin tutkimuksenkin pohjalta. Luotettavuutta lisäsi se, että kerätty tutkimusaineisto käsiteltiin tarkasti, ja opinnäytetyöprosessin ja tutkimustulosten analysointi raportoitiin laajasti. Myös lähteiden monipuolinen käyttö lisäsi luotettavuutta. Koska työssä tutkittiin kokemuksia, oli haastattelujen luotettavuus tärkeää. Haastattelujen tulokset koettiin luotettaviksi, sillä haastateltavien vastauksista ja kehonkielestä pystyi päättelemään heidän puhuvan totuudenmukaisesti. Tätä olettamusta puolsi myös haastattelujen anonymisointi, jolloin haastateltavilla ei ollut tarvetta valehtelulle. Aiheena tietosuojauudistus on todella mittava, ja tämä osoittautui opinnäytetyön haasteeksi ja vähensi täten työn luotettavuutta. Ajanpuutteen vuoksi haastateltavien määrä jäi neljään, ja tutkimustulokset olisivat olleet hieman luotettavampia, jos haastateltavia olisi ollut muutama enemmän. Kokonaisuudessaan työtä voi kuitenkin pitää luotettavana.

Haastateltavien omat kokemukset ja mielipiteet tulivat tutkimuksessa selkeästi ilmi, joten työtä voidaan pitää pätevänä eli validina. Myös laaja ja tarkka teoriaosuus vaikuttaa pätevyyteen positiivisesti. Vaikka yleistyksiä ei pyritty luomaan, haastateltavien kokemukset olivat melko yhteneväisiä ja ne kuvaavat suhteellisen hyvin paikallisten pk-yritysten mielipiteitä tietosuojauudistuksesta. Työn tarkoituksena ei ole toimia ohjekirjana, mutta työn lukeminen voi auttaa lukijaa ymmärtämään lainsäädäntöä tietosuojauudistuksen ympärillä, sekä huomaamaan lainsäädännön ongelmakohdat pienyritysten näkökulmasta.

LÄHTEET JA TUOTETUT AINEISTOT

AINEISTONHALLINNAN KÄSIKIRJA. Kvalitatiivisen datatiedoston käsittely. Yhteiskuntatieteellinen tietoarkisto. [Viitattu 2019-04-25.] Saatavissa: https://www.fsd.uta.fi/aineistonhallinta/fi/kvalitatiivisen-datan-kasittely.html

AARNIO, Reijo 2018. Tietosuojavaltuutetun lausunto Dnro 830/031/2018. [Viitattu: 2019-01-09.] Saatavissa: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-178545.pdf?fbclid=IwAR2i0PhVj7tyIN9fNqljikwkwbqFps-OEc6NcosV0Pxl66saFSUeBe_cuks

AARNIO, Reijo 2019. Hyvää Tietosuojapäivää 28.1.2019. [Viitattu 2019-02-12.] Saatavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/hyvaa-tietosuojapaivaa-28-1-2019

ANDREASSON, Ari, KOIVISTO, Juha ja YLIPARTANEN, Arto 2016. Tietosuojakäsikirja johdolle. 2. painos. Helsinki: Tietosanoma.

ANDREASSON, Ari, RIIKONEN, Jaana ja YLIPARTANEN, Arto 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma oy.

DE FRESNES, Tulikukka 2018. Professori synkkänä – Trafi sotku seurausta ennätyksellisen sekavasta lainsäädännöstä: ”Suomi epäonnistunut aivan täysin”. Yle. [Viitattu 2019-01-09.] Saatavissa: https://yle.fi/uutiset/3-10556716?origin=rss

DITTMAR & INDRENIUS 2016. EU:n yleisen tietosuoja-asetuksen vaikutukset suomalaisiin yrityksiin. Oikeusministeriö. [Viitattu 2019-01-09.] Saatavilla: https://api.hankeikkuna.fi/asiakirjat/38ae644f-e25d-4da8-aa74-a5070c53a1f4/741e2185-7b23-4a8d-b1b7-d3a6b1cee293/MUISTIO_20180227234502.pdf

ELINKEINOELÄMÄN KESKUSLIITTO. Tietopaketti yrityksille: EU:n yleinen tietosuoja-asetus ja tietosuojalaki. [Viitattu 2019-02-06.] Saatavissa: https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/#5-Yleisen-tietosuoja-asetuksen-keskeinen-sis-lt-

ENROTH, Timo ja NEUVONEN, Riku 2017. EU:n tietosuoja-asetuksen yritysvaikutukset, Policy Brief 10/2017. Valtioneuvoston selvitys- ja tutkimustoiminta. [Viitattu 2019-01-16.] Saatavissa: https://tietokayttoon.fi/documents/1927382/2116852/10_2017_+EUn+tietosuoja-asetuksen+yritysvaikutukset/7f043abc-2068-45f2-8470-0b2df19f7189/10_2017_+EUn+tietosuoja-asetuksen+yritysvaikutukset.pdf?version=1.0

EUROOPAN KOMISSIO a. Mitä tarkoittaa ’oikeutettu etu’? [Viitattu 2018-10-12.] Saatavissa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_fi

EUROOPAN KOMISSIO b. Mikä on Euroopan tietosuojaneuvosto? [Viitattu 2019-02-21.] Saatavissa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_fi

EUROOPAN UNIONI a. Asetukset, direktiivit ja muut säädökset. [Viitattu 2018-10-22.] Saatavissa: https://europa.eu/european-union/eu-law/legal-acts_fi

EUROOPAN UNIONI b. Institutionaaliset asiat. [Viitattu 2019-02-21.] Saatavissa: https://europa.eu/european-union/topics/institutional-affairs_fi

EUROOPAN UNIONIN JULKAISUTOIMISTO 2018. EU:n tietosuojauudistus: paremmat säännöt Euroopan yrityksille. [Viitattu 2019-02-21.] Saatavissa: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business_fi.pdf

EUROOPAN UNIONIN TIETOSUOJA-ASETUS 2016/679. EUR-Lex. Lainsäädäntö. [Viitattu 2018-09-23.] Saatavissa: https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX%3A32016R0679

EUROPARLAMENTTI.INFO. Euroopan unionin toimintaperiaatteet. [Viitattu 2018-10-22.] Saatavissa: https://europarlamentti.info/fi/Euroopan-unioni/toimintaperiaatteet/

EUROPEAN DATA PROTECTION SUPERVISOR. Giovanni Buttarelli. [Viitattu 2019-02-21.] Saatavissa: https://edps.europa.eu/about-edps/members-mission/supervisors/giovanni-buttarelli_en

FOX, Chris 2019. Google hit with £ 40m GDPR Fine over ads. BBC. [Viitattu 2019-01-25.] Saatavissa: https://www.bbc.com/news/technology-46944696

HANNINEN, Minna, LAINE, Elli, RANTALA, Kati, RUSI, Mari ja VARHELA, Markku 2017. Henkilötietojen käsittely: Eu-tietosuoja-asetuksen vaatimukset. Helsinki: Kauppakamari.

HENKILÖTIETOLAKI 523/1999. Finlex. Lainsäädäntö. [Viitattu 2018-10-24.] Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/1999/19990523

KESÄNEN, Anni a. Aineiston käsittely: Teemoittely, tyypittely ja litterointi [sähköinen materiaali]. [Viitattu 2019-04-26.] Sijainti: Kuopio: Savonia-ammattikorkeakoulun Moodle [verkko-oppimisympäristö]. Tutkimus- ja kehittämismenetelmät -kurssi.

KESÄNEN, Anni b. Eettiset periaattet ja luotettavuus tutkimuksessa [sähköinen materiaali]. [Viitattu 2019-04-27.] Sijainti: Kuopio: Savonia-ammattikorkeakoulun Moodle [verkko-oppimisympäristö]. Tutkimus- ja kehittämismenetelmät -kurssi.

KORPISAARI, Päivi, PITKÄNEN Olli ja WARMA-LEHTINEN, Eija 2018. Uusi Tietosuojalainsäädäntö. Helsinki: Alma Talent Oy.

LAINLAATIJAN EU-OPAS 2017. Finlex. [Viitattu 2018-10-23.] Saatavissa: http://eu-opas.finlex.fi/1-eu-oikeus-osana-suomen-oikeusjarjestysta/1-3/

LAKI RAHANPESUN JA TERRORISMIN RAHOITTAMISEN ESTÄMISESTÄ 444/2017. Finlex. Lainsäädäntö. [Viitattu 2019-02-26.] Saatavissa: https://www.finlex.fi/fi/laki/alkup/2017/20170444#Pidp447213440

LEXIA ASIANAJOTOIMISTO OY 2019. Brexit ja GDPR – Miten Brexit vaikuttaisi henkilötietojen siirtoon Britanniaan? [Viitattu 2019-02-05.] Saatavissa: https://www.lexia.fi/fi/brexit-ja-gdpr/

MYÖHÄNEN, Pasi 2019. Analyysi: Brexitiin tuli kaivattu hengähdystauko, mutta kestääkö brittien pää lokakuun takarajaan saakka? Yle. [Viitattu 2019-04-28.] Saatavissa: https://yle.fi/uutiset/3-10734355

OIKEUSMINISTERIÖ 2018. Uusi tietosuojalaki voimaan vuoden 2019 alusta. [Viitattu 2019-01-09.] Saatavissa: https://oikeusministerio.fi/artikkeli/-/asset_publisher/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta%20

PIETIKÄINEN, Suvi 2016. Lainsäädännön taustaa. Valtiovarainministeriö. [Viitattu 2019-02-21.] Saatavissa: https://www.vahtiohje.fi/web/guest/lainsaadannon-taustaa

PITKÄNEN, Olli, TIILIKKA, Päivi ja WARMA, Eija 2013. Henkilötietojen suoja. Helsinki: Talentum.

PONEMON INSTITUTE 2018. 2018 Cost of a Data Breach Study: Global Overview. [Viitattu 2019-04-14.] Saatavissa: https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

RIKOSLAKI 39/1889. Finlex. Lainsäädäntö. [Viitattu 2019-01-16] Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

SALMI, Sara 2018. Kenen tahansa ajokorttitiedot voi selvittää netissä ilmaiseksi – ihmiset huolestuivat, Trafi sulki palvelun. Yle. [Viitattu 2019-01-09] Saatavissa: https://yle.fi/uutiset/3-10545929

SUOMEN PERUSTUSLAKI 731/1999. Finlex. Lainsäädäntö. [Viitattu 2018-10-24.] Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

TALUS, Anu, AUTIO, Elina, HÄNNINEN, Anna, PIHAMAA Heljä-Tuulia ja KANTONEN, Silja 2017. Miten valmistua EU:n tietosuoja-asetukseen? Oikeusministeriö. [Viitattu 2019-01-16.] Saatavissa:

http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79316/OMSO_04_2017_OM_TSV_EU_tietosuoja.pdf?sequence=1&isAllowed=y

TIETOSUOJALAKI 1050/2018. Finlex. Lainsäädäntö. [Viitattu 2019-01-09.] Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

TIETOSUOJAVALTUUTETUN TOIMISTO a. Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi. [Viitattu 2019-01-25.] Saatavissa: https://tietosuoja.fi/arvioi-riskit

TIETOSUOJAVALTUUTETUN TOIMISTO b. Automaattinen päätöksenteko ja profilointi. [Viitattu 2019-04-14.] Saatavissa: https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi

TIETOSUOJAVALTUUTETUN TOIMISTO c. Henkilötietolaki. [Viitattu 2018-10-23.] Saatavissa: https://tietosuoja.fi/henkilotietolaki

TIETOSUOJAVALTUUTETUN TOIMISTO d. Ilmoitus tietoturvaloukkauksesta. [Viitattu 2019-02-12.] Saatavissa: https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

TIETOSUOJAVALTUUTETUN TOIMISTO e. Osoita noudattavasi tietosuojasäännöksiä. [Viitattu 2019-02-26.] Saatavissa: https://tietosuoja.fi/osoitusvelvollisuus

TIETOSUOJAVALTUUTETUN TOIMISTO f. Rekisterinpitäjän oikeutettu etu. [Viitattu 2018-10-12.] Saatavissa: https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu

TIETOSUOJAVALTUUTETUN TOIMISTO g. Vaikutustenarvioinnin tekeminen. [Viitattu 2019-02-06.] Saatavissa: https://tietosuoja.fi/vaikutustenarvioinnin-tekeminen

TIETOSUOJAVALTUUTETUN TOIMISTO h. Vaikutustenarviointi. [Viitattu 2019-02-06.] Saatavissa: https://tietosuoja.fi/vaikutustenarviointi

TIETOSUOJAVALTUUTETUN TOIMISTO 2019. Tietosuojavaltuutetun toimistolle on ilmoitettu jo 2700 henkilötietojen tietoturvaloukkausta. [Viitattu 2019-02-22.] Saatavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutetun-toimistolle-on-ilmoitettu-jo-2700-henkilotietojen-tietoturvaloukkausta

TUOMI, Jouni ja SARAJÄRVI, Anneli 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki: Tammi.

VALLI, Raine (toim.) 2018. Ikkunoita tutkimusmetodeihin 1, Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. 5., uudistettu painos. Jyväskylä: PS-kustannus.

VALTIOVARAINMINISTERIÖ 2016. VAHTI-raportti 1/2016. [Viitattu 2018-11-25.] Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

VIRKKUNEN, Jussi 2017. Reijo Aarnio jatkaa tietosuojavaltuutettuna. Yle. [Viitattu 2019-02-11.] Saatavissa: https://yle.fi/uutiset/3-9855911

LIITE 1: HAASTATTELUKYSYMYKSET

Haastattelurunko:

Hei, saammehan tallentaa tämän haastattelun ja käyttää sitä osana opinnäytetyötämme? Litteroinnin jälkeen tallenteet poistetaan, ja tiedot anonymisoidaan.

Taustatiedot:

- Yrityksen nimi, toimiala, haastateltavan nimi?
- Henkilöstön koko?
- Mitä tarkoituksia varten henkilötietoja käsitellään?
- Käsitelläänkö erityisiä henkilötietoryhmiä?
- Oman alan erityisvaatimukset tietosuojan kannalta, esimerkiksi sote?

Muutokset yritystoiminnassa:

- Kuka vastaa tietosuoja-asioista yrityksessä? Onko teillä tietosuojavastaavaa?
    - Millä perusteella valittu?
- Onko työmäärä lisäytynyt?
- Onko tullut konkreettisia muutoksia työhön/käytäntöihin? Jos on, niin mitä? Esimerkiksi:
    - Tunnistukseen liittyen?
    - Onko tullut uusia tietosuojaan liittyviä dokumentteja annettavaksi asiakkaille?
    - Onko tullut muutoksia käsiteltävien henkilötietojen suojaamiseen?
- Henkilöstön tietosuojaosaaminen ennen ja nyt? Onko kehitystä? Esimerkiksi:
    - Onko järjestetty enemmän koulutuksia henkilökunnalle?
    - Annettu enemmän sisäistä ohjeistusta, kuin ennen?
- Miten olette hankkineet tai saaneet tietoa tietosuojauudistukseen liittyen? Esimerkiksi:
    - Onko itse tutustuttu aiheeseen suoraan?
    - Käyty seminaareissa?
    - Luettu valmiita oppaita? Jos on, niin mitä?
    - Onko ostettu osaamista muualta?
    - Onko saatu yrittäjien järjestöiltä tietoa?
- Onko uudistus vaatinut investointeja esimerkiksi uusiin järjestelmiin?
    - Jos on, niin mitä ja miten paljon?
- Onko tarvinnut päivittää sopimuksia esimerkiksi yhteistyökumppaneiden tai henkilötietojen käsittelijöiden kanssa?
- Onko tullut muutoksia liiketoimintaan?
    - Esimerkiksi tarjottuihin palveluihin?
- Tapahtuuko henkilötietojen siirtoa kolmansiin maihin?
    - Jos tapahtuu, miten toimintaperiaate on muuttunut?
- Onko markkinointiin tullut muutoksia? Jos on, niin mitä?
- Jos yrityksellä on verkkokauppa, mitä muutoksia/päivityksiä tietosuojauudistus on vaatinut?
- Tuleeko mieleen muita muutoksia?

Kokemukset / tuntemukset:

- Onko koettu ongelmia uuden tietosuoja-asetuksen tulkitsemisessa? Jos näin, mikä on ollut hankalaa?
- Mitkä ovat henkilöstön kokemukset tietosuojauudistuksesta?
- Koetteko omalle liiketoiminnalle pelkoa/uhkaa sanktioiden takia? (Esimerkkeinä todella korkeat sanktiot ja tietosuojavaltuutetun oikeus määrätä henkilötietojen käsittelykielto.)
- Onko asiakkaat kyselleet tietosuoja-asetuksesta? Esimerkiksi:
    - Käyttäneet oikeuksiaan, kuten pyytäneet saada pääsyä omiin tietoihinsa?
    - Pyytäneet saada siirtää tietojaan järjestelmästä toiseen?
    - Vaatineet tietojensa poistoa?
- Koetteko saaneet hyötyä lainsäädännön muuttumisesta? (Esimerkiksi jos käy kauppaa EU-alueella, onko lainsäädännön yhtenäistyminen koettu hyödylliseksi?)
- Muita kokemuksia ja tuntemuksia asian tiimoilta? Onko kritiikkiä tai positiivista sanottavaa?
- Onko haastateltavalla kysyttävää?