Yleisen tietosuoja-asetuksen vaatimusten toteuttaminen pk-yrityksessä

Jaakko Impiö

2021 Laurea

Laurea-ammattikorkeakoulu

Yleisen tietosuoja-asetuksen vaatimusten toteuttaminen pk-yrityksessä

Jaakko Impiö
Turvallisuuden ja riskienhallinnan-
koulutus
Opinnäytetyö

2021

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuuden ja riskienhallinnan koulutus

Tradenomi (AMK)

Jaakko, Impiö

Yleisen tietosuoja-asetuksen vaatimusten toteuttaminen pk-yrityksessä

Vuosi 2021 Sivumäärä 65

Tämän opinnäytetyön tarkoituksena oli kehittää suomalaisen pk-yrityksen yleisen tietosuoja-asetuksen vaatimustenmukaisuutta tavoitteena asetuksen mukainen osoitusvelvollisuus: Yrityksen tulee olla kykenevä osoittamaan viranomaisille, että vaatimuksia noudatetaan erilaisten dokumenttien ja toimenpiteiden avulla. Työn teoreettinen viitekehys rakentuu kahdesta kokonaisuudesta, jotka ovat EU-oikeus ja yritysturvallisuus. EU:n oikeus on tärkein työtä ohjaava kokonaisuus, johon tavoite oli liittää Elinkeinoelämän Keskusliiton yritysturvallisuuden näkökulma, jossa vahvimpana yhteenliittymänä toimi liiketoiminnan vaatimustenmukaisuus. Vaatimustenmukaisuus tarkoittaa liiketoiminnan kykyä täyttää lailliset velvoitteensa.

Kehittämistyö rakentui teoriaosuuden, sekä opinnäytetyön tekijän yrityksessä viettämän ajan antamien tietojen perusteella tehdystä nykytila-arviosta ja sen perusteella tehdystä kehittämistyöstä. Kehittämistyön lisäksi perehdyin erilaisiin keinoihin toteuttaa Tietosuoja-asetuksen osoitusvelvollisuus pk-yritysten kontekstissa. Suoritin tiedon hakemiseksi systemaattisen kirjallisuuskatsauksen, jossa kävin kolmea eri hakualustaa tiedonhaussa apuna käyttäen läpi 1900 tutkimusta otsikkotasolla, 55 tiivistelmän, ja joista valikoitui lopuksi 5 tutkimusta varsinaiseen kirjallisuuskatsaukseen. Systemaattinen kirjallisuuskatsaus auttoi tunnistamaan erilaisia teemoja liittyen Tietosuoja-asetukseen pk-yritysten rajapinnassa.

Kehittämisosuudessa verrattiin kirjallisuuskatsauksesta löytyneitä teemoja opinnäytetyön tekijän kokemuksiin kentällä. Kirjallisuuskatsauksen avulla selvisi, että tietosuojatyön jalkautus yrityksen arkeen on monialaista toimintaa, johon liittyy osaamistarvetta oikeuden-, tietoturvan- ja tietojenkäsittelyn aloilta. Pk-yrityksien vaatimustenmukaisen tietosuojatoiminnan kehittämisessä korostuvat tietosuojaviranomaisten, sekä erilaisten yritysetujärjestöjen suorittama tiedottaminen, jonka lisäksi näen myös erilaisten tietojenhallintaan liittyvien ohjelmistojen roolin kasvattamisen tärkeyden konkreettisen tiedonhallinnan parantamiseksi. Toimeksiantajayrityksen tietosuojatoimintaa kehitettiin perehdyttämällä henkilöstöä tietosuoja-asetuksen vaatimuksiin, sekä luomalla yritykselle tarvittavia dokumentteja osoitusvelvollisuutta varten.

Asiasanat: Yleinen Tietosuoja-asetus, GDPR, Yritysturvallisuus, Vaatimustenmukaisuus, Pk-yritys

Laurea University of Applied Sciences

Bachelor's degree

Safety, Security and Risk Management

Jaakko Impiö

GDPR requirements implementation to the SME

Year 2021 Pages 65

Abstract

The purpose of this thesis was to develop the compliance with the GDPR in a Finnish SME with the objective of ensuring that the company conforms to the accountability principle of the Regulation. The company must be able to demonstrate to the authorities that the requirements are complied with by various documents and measures. The theoretical framework of the work is built on two entities, which are EU legislation and comprehensive corporate safety and security. The EU law is the most important body of law that guides the thesis, where the objective was to incorporate the business safety and security perspective in accordance with the Confederation of Finnish Industries with the theme of business compliance. Compliance means the ability of a business to meet its legal obligations.

The development work was based on an assessment of the current situation, which again is founded on the theoretical framewok and the information provided by the company when the author of the thesis worked in there. In addition to the development work, various ways to implement the accountability principle of the Data Protection Regulation in the context of SMEs were reviewed. To acquire the research information, a systematic literature review was conducted, in which three different search platforms for information acquiring were scrutinized, using 1900 studies at the title level, 55 abstracts, and finally selecting five studies for the actual literature review. A systematic literature review helped to identify various consepts related to the GDPR at the SME interface.

In the development section, consepts found in the literature review were compared to the author's own experiences in the field and knowledge of theoretical framework. The literature review revealed that the implementation of data protection work in the everyday life of a company is a multidisciplinary activity with a need for expertise in the fields of jurisdiction, information security and data processing industry. In the development of compliant data protection activities for SMEs, emphasis is placed on information provided by data protection authorities, as well as various business groups. In addition the importance of increasing the role of various data management software to improve concrete data management is emphasized.The data protection activities of the commissioner company were developed through familiarizing personnel with the GDPR and the creation of the necessary documents needed by the company for the fulfillment of the accountability principle.

Keywords: General Data Protection Regulation, GDPR, Compliance, SME

Sisällys

1 Johdanto

Vastauksena nopeasti kehittyvään digitaaliseen ympäristöön, vuonna 2016 säädettiin GDPR-nimellä tunnettu Euroopan parlamentin ja neuvoston asetus. Vuoden 2018 keväällä voimaan tullut General Data Protection Regulation 2016/679, eli yleinen tietosuoja-asetus (jäljempänä ”tietosuoja-asetus”), on edeltäjäsääntelyn ja Euroopan Unionin (EU) aikanaan 28 jäsenmaan yhteinen ponnistus ja kompromissi parantaa EU:n kansalaisten ja asukkaiden EU:n perusoikeuskirjan 7. ja 8. artiklan mukaisia oikeuksia henkilötietojensa ja yksityisyytensä suojaan, sekä näiden tietojen vapaaseen liikkuvuuteen Euroopan talousalueen sisällä. Euroopan talousalueeseen (ETA) kuuluu EU:n jäsenmaiden lisäksi Norja, Islanti ja Liechtenstein.

Ennen tietosuoja-asetusta vuonna 1995 säädetty, ja vuonna 1998 voimaan tullut tietosuojadirektiivi 95/46/EC oli ensimmäinen askel kohti modernia tietosuojasääntelyä. Direktiivi 95/46/EC pohjautui Taloudellisen yhteistyön ja kehityksen järjestön (OECD) suosituksiin, mitkä taas pohjautuvat Yhdysvaltojen hallituksen asettamaan Fair Information Practices -ohjeeseen (FIPs) vuodelta 1973. FIPs oli ensimmäisiä ohjeistuksia vastaamaan vuonna 1962 alkaneeseen informaatioteknologian nopeaan lisääntymiseen. (Dixon 2018.) Muita saman aikakauden mainittavia sääntelyjä olivat Saksan Hessenin osavaltion tietosuojasäädös, joka oli maailmalla ensimmäinen laatuaan. Ruotsissa otettiin käyttöön tietosuojasäädös vuonna 1973. (Tikkinen-Piri, Rohunen & Markkula 2018.) Suomen kansalliseen lainsäädäntöön säädettiin EU:n tietosuojadirektiivin pohjalta henkilötietolaki 523/1999, mikä myöhemmin kumottiin tietosuoja-asetukseen perustuvalla tietosuojalailla 1050/2018. Suomessa, kuten kaikissa EU ja ETA-maissa, tärkein ohjaava lainsäädäntö tietosuojasääntelyssä tällä hetkellä on tietosuoja-asetus.

Tietosuoja-asetuksen 40. artiklassa ”käytännesäännöt”, säädetään pienten ja keskisuurten yritysten ”erityistarpeiden” ja ”eritysaseman” huomioimisesta jäsenvaltioiden viranomaisten laatiessa käytännesääntöjä tarkentamaan tietosuoja-asetusta. Tässä opinnäytetyössä perehdyttiin tietosuoja-asetukseen, sekä sen tyypillisiin pieniä ja keskisuuria yrityksiä (jäljempänä pk-yritys) koskeviin vaikutuksiin ja erityistarpeisiin. Tarkemmin työ eteni yhden suomalaisen kiinteistönhoitoalan yrityksen henkilötietojen käsittelyyn perehtymisenä tapaustutkimuksena, missä arviointi perustui teoreettisesta viitekehyksestä saatuihin tietoihin. Arvioinnin ja toimintojen kehittämisen jälkeen vertailen kentältä saatuja tuloksia systemaattisen kirjallisuuskatsauksen tuloksiin, missä kävin ennalta määrätyillä kriteereillä ensin otsikkotasolla n. 1900 tutkimusta, toisena 55 tutkimusta tiivistelmän perusteella. Valitsin lopulta 5 aiheen kannalta kokonaisvaltaista ja monialaista tutkimusta kirjallisuuskatsausta varten.

Työssä hyödyn saaja oli ennen kaikkea kohdeyritys, jonka toimintaa opinnäytetyön aikana kehitin perehdyttämällä henkilöstöä tietosuoja-asioihin ja luomalla tietosuojadokumentteja yrityksen käyttöön osoitusvelvollisuuden tueksi. Tutkimuksellisen kehittämistyön tuloksia voidaan lisäksi soveltaa muissakin samankaltaista henkilötietojen käsittelyä harjoittavissa yrityksissä, ja opinnäytetyön eri osat voivat toimia monipuolisen näkökulman saamiseksi asetukseen nähden, haasteista mahdollisuuksiin.

1.1 Kehittämistyön tavoitteet

Kehittämistyön tavoitteena oli edistää yritys x:n toiminnan jatkuvuutta ja varautumista, sekä hallita liiketoimintariskejä kehittämällä yrityksen toimintaa yleisen tietosuoja-asetuksen vaatimusten mukaisesti. Työn aloittamisen hetkellä yrityksellä ei ollut minkäänlaisia tietosuoja-asetuksen mukaisia todisteita siitä, että yritys noudattaisi asetusta, kuten käytännesääntöjä, dokumentteja tai ohjeistuksia. Opinnäytetyön aihetta ehdotti yritys, jossa olen työskennellyt opintojeni ohessa. Yrityksestä tullaan käyttämään nimeä Yritys x (jäljempänä ”kohdeyritys” tai ”toimeksiantaja”). Opinnäytetyön tavoitteena on pk-yrityksen tietosuojan hallinnan kehittäminen tietosuoja-asetuksen vaatimusten mukaisesti.

Työ rakentuu teoriaosuudesta, jossa perehdyin yleiseen tietosuoja-asetukseen, ja miten Suomen lainsäädäntö sen säädöksiä toteuttaa, sekä millaisia yleisiä vaatimuksia se asettaa yrityksille, yhteisöille ja organisaatioille. Oppinäytetyön laadullisessa kehittämistyöosuudessa tein kohdeyritykseen tietosuojan nykytila-arviota workshop-menetelmällä. Toteutin workshopin teoriaosuuden kattavien tietojen, sekä ennakkotietojeni avulla yrityksestä sekä yleisesti toimialasta, jossa yritys harjoittaa liiketoimintaa. Tiedot toimialasta, sekä sen käytännöistä on tullut tutuksi viimeisen parin kesän aikana, kun olen työskennellyt kohdeyrityksessä, sekä eräässä toisessa saman alan yrityksessä työntekijänä. Syvällisempään perehtymiseen yrityksen arkeen, esimerkiksi työntekijähaastatteluiden avulla ei näin ollen ollut tarvetta. Lopuksi laadin systemaattisen kirjallisuuskatsauksen, jossa vertasin kokemuksia workshopeista muihin vastaavanlaisen työn tehneiden tutkimuksiin, joissa käsiteltiin pk-yrityksiä ja tietosuoja-asetusta.

Työn ensimmäinen tutkimuskysymys on: ”Millaisia toimia pk-yrityksille on osoitusvelvollisuuden toteuttamiselle olemassa?”: Tietosuoja-asetus on tuonut paljon erilaisia vaatimuksia toteutettavaksi yrityksille, kokoon tai liiketoiminnan luonteeseen katsomatta. Ensimmäisen tutkimuskysymyksen tarkoituksena on selvittää, millaisia toimenpidevaatimuksia tietosuoja-asetus on tuonut ennen kaikkea pk-yrityksille. Toinen tutkimuskysymys, ”Mitkä toimet ovat riittäviä kohdeyritykselle?”, juontaa kohdeyrityksen kannalta ajallisten- ja taloudellisten resurssien harkittuun kohdentamiseen, mikä on kriittistä toiminnan jatkuvuutta ajatellen. Tämän vuoksi olisi tärkeää kohdentaa niukat resurssit tehokkaasti. Kolmas tutkimuskysymys, miten varmistaa tietosuoja-asetuksen noudatettavuus jatkossa, viittaa tietosuojanhallinnan

prosessinomaisuuteen. Tietosuoja-asetuksen jalkauttaminen yrityksen arkeen ei ole yksi, kerran alkava ja aikanaan päättyvä projekti, vaan jatkuva prosessi oletusarvoisen ja sisäänrakennetun tietosuojan periaatteiden perusteella, jolloin tietosuoja on kiinteästi, kuten yritysturvallisuus yleensäkin, mukana visiosta ja strategisista päätöksistä, aina pienimpiin päivittäisiin työaskareisiin.

Tutkimuskysymykset työlle ovat seuraavat:

1. Millaisia toimia pk-yrityksille on osoitusvelvollisuuden toteuttamiselle olemassa?

2. Mitkä toimet ovat riittäviä kohdeyritykselle?

3. Miten varmistaa tietosuoja-asetuksen noudatettavuus jatkossa

1.2 Kohdeyritys

Yritys on laajasti Etelä-Suomessa toimiva maalausalan yritys, jonka päätoimialaa ovat rakennusten ulkoseinien ja kattojen käsittely, sekä erilaisten kattoturvatuotteiden asentaminen. Yhtiön liikevaihto on vuositasolla n. 3–4 miljoonaa euroa, ja yrityksen palkkalistoilla on vakituisesti 10 henkilöä. Kesäsesongin aikana, josta muodostuu myös suurin osa liikevaihdosta, yrityksen palkollisena on noin 100 kausityöntekijää, jotka työskentelevät tyypillisesti toukokuun alusta elokuun loppuun rakennusten ulkopintojen käsittelyn parissa. Ympärivuotisesti yrityksessä työskentelee johdon lisäksi myyjiä, joiden pääasiallisena tehtävänä on valmistella yritystä kesäsesonkia varten myymällä urakkakohteita yksityisasiakkaille, sekä taloyhtiöille. Yrityksen ylimpään johtohenkilöiden tehtävinä on hallinnollisten tehtävien hoitamisen lisäksi myynti, markkinointi -ja rekrytointi. Yrityksellä on kaksi toimipistettä, yksi Uudellamaalla ja yksi Pirkanmaalla.

2 Yleinen tietosuoja-asetus

Tämän opinnäytetyön teoreettinen viitekehys rakentuu kahdesta kokonaisuudesta: Euroopan Unionin oikeudesta ja yritysturvallisuudesta. Euroopan Unionin oikeus, joka koostuu primaarilainsäädännöstä ja sekundaarilainsäädännöstä, määrää jäsenvaltioita neljällä tavalla: Asetuksilla, direktiiveillä, päätöksillä ja suosituksilla. Asetukset ovat näistä määräyksistä vahvimpia, ja ne tulevat aina voimaan jäsenmaissa sellaisenaan. Tietosuoja-asetus kuuluu Euroopan Unionin oikeuden sekundaarilainsäädännön piiriin ja siinä säädetään perussopimuksessa määritellyistä periaatteista ja tavoitteista koskien Euroopan Unionin kansalaisten yksityisyyden, ja sen kautta henkilötietojen suojaa. Tietosuoja-asetus on asetuksen luonteen mukaan suoraan velvoittava, joten työssä viitataan ensisijaisesti suoraan tietosuoja-asetukseen, ja ohjeisiin, joita Suomen kansallinen viranomainen on laatinut. (Euroopan Unionin virallinen verkkosivusto

2021a.) Toissijaisesti voidaan viitata niihin Suomen kansallisen lainsäädännön lakeihin, joilla on merkitystä liiketoiminnan vaatimustenmukaisuuden kannalta henkilötietojen suojan osalta, jotka ovat tätä kehittämistyötä koskien tietosuojalaki 1050/2018, laki yksityisyyden suojasta työelämässä 759/2004 ja laki sähköisen viestinnän palveluista 917/2014.

Kun halutaan kehittää yritysturvallisuutta, tulee silloin kysymykseen liiketoiminnan jatkuvuuden ja vaatimustenmukaisuuden, sekä turvallisuuden ja riskienhallinnan kehittäminen. Hyvänä mallina yritysturvallisuuskentän hahmottamiseen ja tarkasteluun voidaan pitää elinkeinoelämän keskusliiton yritysturvallisuus-mallia nykyaikaisen, alati muuttuvan liiketoimintaympäristön kehittämisen apuna (Kuvio 1). (Elinkeinoelämän keskusliitto 2016, 2.)

Elinkeinoelämän keskusliiton (2016) mukaan yritysturvallisuus on kaikkien toimintojen turvallisuutta, jolloin uhkien tunnistaminen, riskien arviointi ja käsittelyn kautta voidaan määritellä ja mitoittaa riittävä taso yritysturvallisuudelle. Keskeiset sidosryhmät ja yhteystyökumppanit olisi hyvä sitouttaa riskien tunnistamiseen, arviointiin ja käsittelyyn. (Elinkeinoelämän keskusliitto 2016, 2.) Näen sidosryhmien ja yhteistyökumppaneiden sitouttamisella yritysturvallisuuden kehittämiseen yhtymäkohtia tietosuoja-asetuksen 28 artiklassa määriteltyihin henkilötietojen käsittelijää koskeviin yleisiin vaatimuksiin, joilla osittainen vastuu käsittelystä siirretään henkilötietojen käsittelijälle. Yritysturvallisuusmallissa tosin puhutaan, että ”olisi hyvä sitouttaa”, kun taas tietosuoja-asetuksessa henkilötietojen käsittelijä velvoitetaan sitoutumaan vaatimuksiin, joita asetus ja kansallinen valvontaviranomainen määrittää kullekin toimijalle käsittelyyn liittyvän riskin mukaan. (Euroopan Unioni 2016.)

Kuvio 1 Elinkeinoelämän yritysturvallisuus-malli (Elinkeinoelämän keskusliitto 2016).

Jotta voidaan varmistaa käsitteiden oikeellisuus, olisi tarpeen määrittää, mitä tarkoittaa tietosuoja. Yritysturvallisuuden mallista ei suoraan löydy mainintaa tietosuojasta. Kun mallia avaavaa dokumenttia käydään läpi, huomataan tietosuojan sisältyvän tietoturvallisuuden neljänteen alakohtaan: ”Tietosuoja ja yksityisyyden suoja”, jossa mainitaan henkilötietojen käsittely, yksityisyydensuoja työelämässä, sekä viestinnän suoja. Dokumentissa ei siis varsinaisesti terminä viitata kuin kerran suoraan tietosuojaan, mutta useasta kohtaa voidaan löytää kuitenkin epäsuoria viitteitä siihen. Tiedon suojaaminen mainitaan heti yritysturvallisuuden määritelmässä: *”…voidaan suojata yritykselle tärkeitä arvoja kuten henkilöitä, tietoa, mainetta, omaisuutta tai ympäristöä…”*. Henkilötietojen tietosuojan toteuttaminen on siis erottamaton osa yritysturvallisuutta. (Elinkeinoelämän keskusliitto 2016.)

Perimmäinen lähtökohta ja syy asetuksen antamiselle on luonnollisten henkilöiden oikeuksien ja vapauksien suojeleminen henkilötietojen käsittelyn pelisääntöjen muokkaamisella mukautumaan nykyiseen massadatan ja tekoälyn maailmaan. Asetuksesta löytyy tärkeimmän teeman, tietosuojan, lisäksi kohtia myös tietoturvallisuuteen artiklassa 32, ”Käsittelyn turvallisuus”. Kyberturvallisuuteen viittaavia artikloja löytyy useampi. (Euroopan Unioni 2016.)

Mitä sitten tieto -ja kyberturvallisuus ovat, miten ne eroavat tietosuojasta, ja toisaalta mitä yhteistä niillä on? Kun otetaan tarkasteluun myös digitaalinen turvallisuus, on käsissämme useampi toistaan läpileikkaava aihe. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän asettaman erillisen työryhmän laatimassa raportissa tietosuoja liitetään osaksi digitaalisen ja kyberturvallisuuden viitekehystä (Kuvio 2). Kuvion tulkintani mukaan tietosuoja rakentuu tietoturvallisuudesta, toiminnan jatkuvuuden turvaamisesta ja varautumisesta häiriötilanteisiin, sekä riskienhallinnasta. (VAHTI 2016, 8.) Tietosuoja-asetuksen mukaisesti tietosuojan piiriin kuuluvat fyysiset dokumentit, kuten kaikki paperisessa muodossa oleva henkilötieto, joten sillä näkökulmalla tietosuoja on myös digitaalista ja kyberturvallisuutta laajempi kokonaisuus.

Kuvio 2 Digitaalinen- ja kyberturvallisuus (VAHTI 2016, 8).

Cybernetics-termi juontaa juurensa 1900-luvun puoleen väliin, milloin sillä tarkoitettiin ihmisten ja koneiden välisen kommunikaation tiedettä. Kyberturvallisuus on osa yksittäistä yhteiskuntaa isompaa, globaalia toimintaympäristöä. Kuten kyberturvallisuudessa, myös tietoturvallisuudessa suojataan samoja kolmea tiedon ydinarvoa; eheyttä, saatavuutta ja luotettavuutta. Tietoturvallisuus ei rajoitu ainoastaan verkon kautta tulevaan uhkaan, vaan on suurempi kokonaisuus sisältäen turvattavaa tietoa useassa muodossa, kuten digitaalisissa ja fyysisissä tallenteissa. Tietoturva koskee myös ihmisten tietämystä turvattavasta tiedosta, joten se koskettaa myös digitaalisten laitteiden ulkopuolista maailmaa. (Sharon, Gillis, Clark 2021.)

Teknologiateollisuus määrittää kyberturvallisuuden käsittävän tietoturvallisuuden lisäksi jatkuvuuden hallinnan ja varautumisen, sekä tietoturvan järjestelmien, ohjelmistojen, laitteiden ja verkkojen suojaamisen lisäksi myös liiketoimintaprosessien suojaamista. Teknologiateollisuuden mukaan tietoturvassa on kyse suojausohjelmien lisäksi ihmisten käyttäytymisestä ja asenteista. (Teknologiateollisuus 2020.) Digitaalinen turvallisuus on mukana tietojen turvaamisessa verkossa, kyberturvallisuus turvaa laajemmin infrastruktuuria, järjestelmiä, verkkoa, sekä tietoa, eli se on näin ollen valtioiden rajat ylittävää toimintaa.

Miten sitten nämä liittyvät henkilötietojen suojaan? Henkilötietojen suojan voi ajatella olevan näitä kaikkea ohjaava tekijä, jos sitä ajatellaan vain ja ainoastaan ihmisten perusoikeuksien kautta. Kun näkökulmana on perusoikeudet, palvelee yhtä lailla globaali kyberturvallisuus, kuin paikallinen fyysinen tietoturvallisuus niiden toteutumista. Tämä erottelu on merkittävä tämän työn kannalta; kun käsitellään tietosuojaa, silloin ei välttämättä käsitellä tietoturvallisuutta, kyberturvallisuutta tai digitaalista turvallisuutta, vaikka ne ovat tärkeässä osassa tietosuojan onnistumisessa. Osoitusvelvollisuus ei suoraan tarkoita sitä, millaisia tietoturvaratkaisuja tulee ottaa käyttöön, vaan sen avulla voidaan todistaa muun muassa, mitä henkilötietoja, miten ja miksi niitä käsitellään. Tietosuojassa tietoturva tulee kysymykseen luokittelun, sekä siihen liittyvän vaikutustenarvioinnin jälkeen. Sen kautta määräytyy tarkemmin henkilötietojen suojaustaso, ei siis varsinaisesti se, mikä on tekninen ratkaisu, jolla tieto suojataan. Yleisessä tietosuoja-asetuksessa puhutaan riittävästä tietosuojan tasosta, missä riski rekisteröidyn oikeuksille ja vapauksille määrittää täysin tietoturvan tason. Tietosuoja-asetuksesta on haluttu tehdä teknologianeutraali jatkuvasti muuttuvien teknisten ratkaisujen takia teknologian kentällä (Hansen Jagrelius 2018, 50).

Tietoperustaa työlle luo alan kirjallisuus, asiantuntijapodcastit, EU:n ja suomen tietosuojavaltuutettujen julkaisut, artikkelit ja yliopisto -sekä ylemmän AMK:n opinnäytetyöt/gradut aiheesta. Tietosuoja-ammattilaisten keskustelut esimerkiksi Linkedin -verkkoyhteisöpalvelussa ovat toimineet lisäksi hyvänä tiedonlähteenä ajankohtaisille aiheille, joihin osasin paremmin kiinnittää huomiota työn edetessä.

2.1 Yleinen tietosuoja-asetus

Vuoden 2018 keväällä voimaan tullut, tämän työn kirjoittamisen hetkellä 2,5 vuotta voimassa ollut Euroopan parlamentin ja neuvoston asetus 679/2016, jäljempänä tietosuoja-asetus, velvoittaa yrityksiä ja julkisyhteisöjä toimimaan asetuksessa säädetyllä tavalla. Henkilötietojen suojaamiseen ei ole havahduttu näin myöhään, vaan asetuksella korvattiin vuonna 1995 säädetty direktiivi 95/46/EC, joka ohjasi yrityksiä ja organisaatioita niin ikään henkilötietosuoja-asioissa. Vuonna 1998 voimaan tulleen EU-direktiivin mukainen kansallinen lainsäädäntö suomessa, vuodesta 1999 asti voimassa ollut henkilötietolaki (523/1999) kumottiin tietosuojalailla 1050/2018.

Tietosuoja-asetuksella on ollut merkittäviä vaikutuksia maailmanlaajuisesti. Yhdysvalloissa Kalifornian osavaltiossa California Consumer Privacy Act, eli CCPA tuli voimaan tammikuussa 2020, minkä lisäksi useat maat ovat ottaneet mallia tietosuoja-asetuksen ideasta - Kiinassa Personal Information Protection Law (PIPL), Brexitin jälkeisessä Isossa-Britanniassa, josta tuli virallisesti ETA:n ulkopuolinen maa, säädettiin oma Data Protection Act vuonna 2018, joka perustuu täysin uuden tietosuoja-asetuksen vaatimuksiin, ja joka toimii sellaisenaan edelleen post-Brexit aikakaudella. Brasilia, Singapore ja Australia tulevat perässä niin ikään tietosuoja-asetuksen innoittamana henkilötietolakien päivityksissä – yleinen tietosuoja-asetus sai aikaan ympäri maapalloa tietosuojalakien päivityssuman, jolle ei oleteta tulevan hetkeen loppua. (Coos 2021.)

Henkilötietojen suojaa on harjoitettu ennenkin, aiempi lainsäädäntö havaittiin vanhentuneeksi sen kykenemättömyyttänsä varmistaa henkilötietojen suoja kasvavassa massadatan maailmassa. ”Direktiivin 95/46/EY tavoitteet ja periaatteet ovat edelleen pätevät, mutta sen avulla ei ole pystytty estämään tietosuojan täytäntöönpanon hajanaisuutta eri puolilla unionia, oikeudellista epävarmuutta tai laajalle levinnyttä näkemystä, jonka mukaan erityisesti verkkoympäristössä toimimiseen liittyy luonnollisten henkilöiden suojelun kannalta huomattavia riskejä.” (Euroopan Unioni 2020.) Kuviossa 3 esitellään yleisen tietosuoja-asetuksen tavoitteita, johon asetuksen antamisella pyritään pääsemään (Kuvio 3).

Kuvio 3 Yleisen tietosuoja-asetuksen tarkoitus (Euroopan Unioni 2016).

Uudessa Tietosuoja-asetuksessa lähtökohtana on henkilötietojen käsittelyä koskevat tarkat vaatimukset, jotka koskevat Euroopan Unionin alueella -sekä Unionin ulkopuolella toimivia yrityksiä ja organisaatioita, missä käsitellään Euroopan Unionin kansalaisten henkilötietoja. Uuden tietosuoja-asetuksen tarkoituksena oli nykyaikaistaa tietosuojaympäristöä tarjoamalla EU:n kansalaisille paremman suojan dataintensiivisessä maailmassa. (Euroopan Unioni 2020.)

2.2 Riskiperusteinen lähestymistapa tietosuoja-asetuksessa

Ahteensuun (2014) mukaan riski on vahingonuhka; ”vahingonuhka syntyy, kun yksilö ”liittää” tietyn tapahtuman tai asiaintilan esiintymiseen negatiivisen arvo-ominaisuuden.” (Ahteensuu, M, 2014.) Kansankielellä Suomen Riskienhallintayhdistys (2021) tarjoaa määritelmää ”Riski on mahdollisuus, että haitallinen tapahtuma toteutuu. On siis mahdollista, mutta ei täysin varmaa, että esiintyy ei-toivottu tapahtuma, jolla on haitallisia seurauksia. (Suomen Riskienhallintayhdistys 2021.) Tietosuoja-asetuksessa riskeillä tarkoitetaan ”henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon, pseudonymisoinnin kumoutumiseen tai vaikka

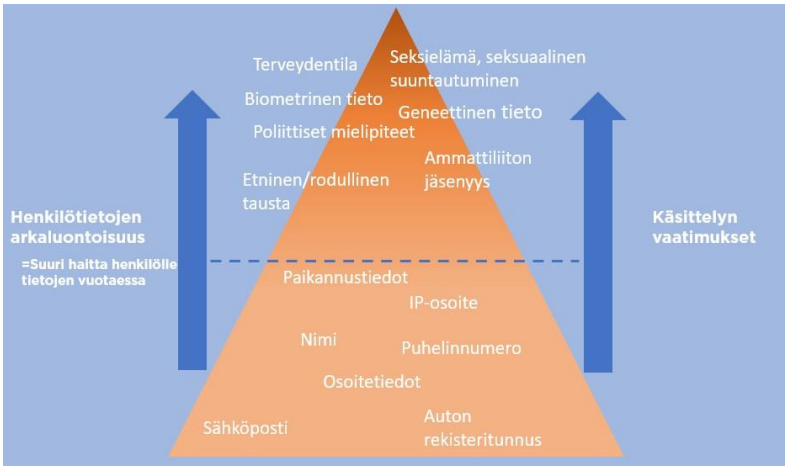
arkaluontoisten tietojen paljastumiseen sivulliselle.” (Andreasson, Riikonen & Ylipartanen 2019, 29.)

Yksilön oikeuksien kannalta tietosuoja-asetuksen määrittelemät vahingolliset tapahtumat ovat siis ei-toivottuja tapahtumia, joiden hallitsemiseen tarvitaan hyvin perusteltuja hallintamekanismeja. Uudessa tietosuoja-asetuksessa on vakiintunut tapa lähestyä henkilötietojen käsittelyä riskiperusteisuuden mukaan. Andreassonin ym. (2019, 29) ja Taluksen, Aution, Hänninese ja Kantosen (2017, 16) mukaan riskiperusteisuus tarkoittaa velvoitteiden ja suojatoimien mitoittamista henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Toisaalta halutaan, että yksilön perusoikeuksia kunnioitetaan, mutta toisaalta halutaan välttää vähäriskisen toiminnan ylisääntelyä ja sitä kautta aiheutuvaa turhaa kitkaa liiketoiminnan pyörittämiselle. (Andreasson, Riikonen & Ylipartanen 2019, 29; Talus, Autio, Hänninen & Kantonen 2017, 16.)

2.3 Henkilötiedon määritelmä

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön (jäljempänä rekisteröity), sekä sellaiset erilliset tiedot, joita yhdistelemällä tunnistetaan tietty henkilö. Esimerkkejä henkilötiedoista ovat nimi, henkilötunnus, sijaintitiedot, online-tunniste (sähköposti tai IP-osoite), terveydelliset, fyysiset, geneettiset tai biometriset tiedot, sekä luonnollisen ihmisen kulttuurinen tai sosiaalinen identiteetti.

Tiettyjen henkilötietojen käsittely on lähtökohtaisesti kielletty tietosuoja-asetuksen 9. artiklan mukaisesti, ellei sille ole sopivaa perustetta. Tällaisia henkilötietoja ovat etninen alkuperä, poliittiset mielipiteet, uskonnolliset tai filosofiset vakaumukset, geneettiset tiedot, biometriset tiedot, terveys, seksielämä ja seksuaalinen suuntautuminen. Edellä mainittuja tietoja pidetään erityisinä henkilötietoina. Tietosuoja-asetuksessa luetellaan tiettyjä tapauksia, joiden nojalla organisaatiot voivat käsitellä arkaluontoisia henkilökohtaisten tunnistetietojen ryhmää. Kuviossa 4 havainnollistetaan tietosuoja-asetuksen mukaista henkilötietojen kenttää (kuvio 4). Kuviosta käy ilmi, että mitä arkaluontoisemmista henkilötiedoista on kyse, sitä vaikuttavammat toimenpiteet niiden suojaamiselle tulee tehdä. (Euroopan Unioni 2016.)



Kuvio 4 Esimerkkejä suojattavista henkilötiedoista

2.4 Yleisen tietosuoja-asetuksen periaatteet

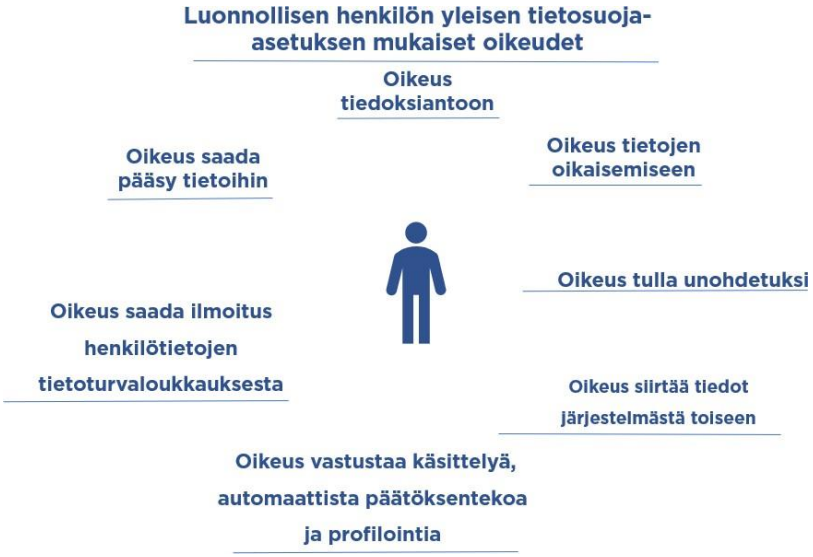
Tietosuoja-asetuksen viidennessä artiklassa kuvataan periaatteet, joihin organisaatioiden tulisi kiinnittää huomiota käsitellessään henkilökohtaisia tunnistetietoja. Periaatteita ovat seuraavat: Henkilötietoja on käsiteltävä laillisesti, oikeudenmukaisesti ja läpinäkyvästi (Lainmukaisuus, kohtuullisuus ja läpinäkyvyys), henkilötietoja on kerättävä määriteltyihin, nimenomaisiin ja laillisiin tarkoituksiin, eikä niitä saa käsitellä tavalla, joka ei ole yhteensopiva näiden tarkoitusten kanssa (käyttötarkoitussidonnaisuus), Henkilötietojen on oltava asianmukaisia, relevantteja ja rajoitettuja tarkoituksiin, joita varten niitä käsitellään (tietojen minimointi), henkilötietojen on oltava paikkansa pitäviä, ajan tasalla ja organisaatioiden on varmistettava tietojen oikeellisuus (täsmällisyys), henkilötiedot on säilytettävä muodossa, joka sallii rekisteröidyn tunnistamisen vain niin kauan kuin se on välttämätöntä (säilytyksen rajoittaminen), henkilötietoja on käsiteltävä tavalla, joka on suojattu luvattomalta tai laittomalta käsittelyltä. Tietoja ei saa kadota, tuhoutua tai vahingoittua (eheys ja luottamuksellisuus). (Euroopan Unioni 2016.)

Yleisen tietosuoja-asetuksen pääperiaatteet esitellään kootusti kuviossa 5 (kuvio 5). Näiden periaatteiden toimivuuden tulee rekisterinpitäjän kyetä osoittamaan. Pääperiaatteita noudattamalla rekisterinpitäjä tulisi pärjätä vaatimustenmukaisesti. Tietosuoja-asetuksessa ei määritellä suoraan konkreettisia toimenpiteitä, miten asetuksen mukaiset periaatteet toteutuvat, vaan sen tulee määrittää kansallinen tietosuojaviranomainen. (Euroopan Unioni 2016.)

Kuvio 5 Yleisen tietosuoja-asetuksen periaatteet

2.5 Rekisteröidyn yleisen tietosuoja-asetuksen mukaiset oikeudet

Rekisterinpitäjällä on velvollisuus toteuttaa asianmukaiset toimenpiteet rekisteröidyn tietosuojaoikeuksien toteuttamiseksi, sekä helpottaa rekisteröidyn oikeuksien käyttämistä. Kuviossa 6 on koottuna rekisteröidyn oikeudet (Kuvio 6). Tietosuoja-asetuksessa on lisäksi määritelty eräitä tilanteita, joiden perusteella rekisteröity ei voi käyttää oikeuksiaan esimerkiksi tilanteessa, jossa viranomainen käsittelee rekisteröidyn henkilötietoja. (Tietosuojavaltuutetun toimisto 2021a.)



Kuvio 6 Luonnollisen henkilön yleisen tietosuoja-asetuksen mukaiset oikeudet

2.5.1 Oikeus tiedoksiantoon

Tietosuoja-asetuksen 13. ja 14. artiklan mukaisesti, ennen kuin henkilötietojen kerääminen on asetuksen mukaisesti mahdollista, tulee rekisterinpitäjällä olla informointivelvoitteen täyttämiseksi tieto käsittelytoimista jossain tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa, mikäli rekisterinpitäjällä ei ole sellaista oikeusperustaa, joka kumoaa tiedonantovelvoitteen. Informaatiovelvoite ei koske eräitä tilanteita, kuten viranomaisen valvontatehtäviin liittyvää henkilötietojen käsittelyä, tai tilannetta, jossa informointivelvoite aiheuttaa kohtuutonta vaivaa rekisterinpitäjälle, tai kun tiedot ovat saatu jostain muualta, kuin rekisteröidyltä itseltään. Lähtökohtaisesti rekisteröityjä on informoitava käsittelystä tavalla tai toisella, kuitenkin rekisteröidyn oikeudet huomioon ottaen. Joissain tilanteissa informoinnista voi olla jopa haittaa rekisteröidylle. (Tietosuojavaltuutetun toimisto 2021b; Euroopan Unioni 2016.)

Tietosuojaseloste on tällä hetkellä vakiintunut tapa esittää käsittelyä koskevat tiedot sen sisältäessä esimerkiksi seuraavia tietoja: Rekisterinpitäjän ja tietosuojavastaavan yhteystiedot, henkilötietojen käyttötarkoitus ja käsittelyn oikeusperusta, säännönmukaiset tietolähteet, henkilötietojen luovutuksesta kolmansille osapuolille, henkilötietojen luovutuksesta

kolmansiin maihin, henkilötietojen säilytysajasta ja sen kriteereistä, oikeudesta tehdä valitus valvontaviranomaiselle, millaisia tietoja kerätään, automaattisesta päätöksenteosta ja profiloinnista. (Euroopan Unioni 2016.)

2.5.2 Oikeus saada pääsy tietoihin ja oikeus tietojen oikaisemiseen

Tietosuoja-asetuksen 15. artiklan mukaan rekisteröidyllä on oikeus saada tietää, millaisia tietoja hänestä säilytetään. Jos rekisteröity haluaa tietää henkilötietojensa käsittelystä, tulee rekisterinpitäjän toimittaa rekisteröidylle jäljennös käsiteltävistä tiedoista. Jos rekisteröity pyytää useampaa jäljennöstä, pyynnöstä voidaan periä ”hallinnollisiin kustannuksiin perustuvan kohtuullisen maksu”. Tietojen lähettämisen yhteydessä tulee pyytäjälle lähettää lisäksi seuraavat tiedot: Käsittelyn tarkoitukset, kyseessä olevat henkilötietoryhmät, vastaanottajat tai vastaanottajaryhmät, erityisesti kolmansissa maissa olevat vastaanottajat tai kansainväliset järjestöt, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa, mahdollisuuksien mukaan henkilötietojen suunniteltu säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit, rekisteröidyn oikeus pyytää rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista tai poistamista taikka henkilötietojen käsittelyn rajoittamista tai vastustaa tällaista käsittelyä, oikeus tehdä valitus valvontaviranomaiselle, jos henkilötietoja ei kerätä rekisteröidyltä, kaikki tietojen alkuperästä käytettävissä olevat tiedot, automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle. Rekisteröity voi vaatia virheelliset tietonsa oikaistuksi välittömästi ja riippuen käsittelytarkoituksesta, rekisteröidyllä on oikeus saada myös puutteelliset henkilötiedot täydennettynä esimerkiksi lisäselvityksen muodossa. (Euroopan Unioni 2016.)

46 Artiklan mukaisesti rekisteröidyllä on oikeus tietää, jos hänen tietojaan ollaan siirtämässä kolmanteen maahan tai kansainväliselle järjestölle, jos kyseinen maa tai järjestö ei ole tietosuojan tasoltaan valvontaviranomaisten mukaan turvallinen. Tällaisissa tapauksissa rekisterinpitäjä tulee varmistaa tarvittavat suojatoimet, jotta henkilötietojen siirto ja säilytys olisi mahdollista. Tehokas suojatoimi voi olla esimerkiksi mallisopimuslauseke osapuolten välillä. (Euroopan Unioni 2016.) Tietosuoja-asetuksen voimaan tulon myötä EU:n ja USA:n välille muodostettiin lähinnä USA:n toimesta Privacy Shield -järjestely, jolla aikanaan taattiin EU:n kansalaisten henkilötiedoille Yhdysvalloissa EU:n tietosuojaa vastaava taso. Privacy Shield järjestely kumottiin myöhemmin kesällä 2020 Euroopan tietosuojaneuvoston toimesta, milloin Schrems 2 -päätöksen myötä aiempi järjestely todettiin riittämättömäksi tietojen siirtoon USA:n ja EU:n välillä, missä suurin osa EU:n kansalaisten henkilötiedosta liikkuu, kun huomioidaan kaikki ”kolmannet maat”. Schrems 2 -päätöksen vuoksi perinteinen mallisopimuslauseke ei ole enää yksistään pätevä ratkaisu, vaan sen tueksi tulee tehdä tietosuojan arviointia. Tolvanen ja Pökkylä (2021) mukaan lopullista järjestelyä, jota rekisterinpitäjien olisi vaivaton

noudattaa vaatimustenmukaiseen henkilötietojen siirtoon USA:han, ei ole vielä tehty. (Tolvanen & Pökkylä 2021.)

2.5.3 Oikeus tulla unohdetuksi ja oikeus siirtää tiedot järjestelmästä toiseen

Yhtä helposti kuin henkilötietojen käsittelyyn on saatu suostumus, tulisi myös henkilötietojen käsittelyn kieltäminen olla yhtä helppoa. Poistamisen syynä voi olla esimerkiksi vanhentuneet henkilötiedot. Tietosuoja-asetus ei suoraan määritä sellaisia teknisiä toimenpiteitä, joilla henkilötiedot tulisi poistaa. Poistamiselle on olemassa VAHTI-Raportin (2016, 15) mukaan ainakin henkilötietojen merkitseminen siten, että niiden käsittely järjestelmässä estyy, taikka luomalla yksittäiselle henkilötiedolle salaus, jota ei käytännössä katsoen voida ohittaa. Henkilötiedot voivat olla järjestelmässä ”poiston” jälkeen, niiden käsittely ei kuitenkaan ole mahdollista. Poikkeuksen vaatimukselle henkilötietojen poistamiseen tekevät sellaiset rekisterit, joihin tulee olla pääsy lakisääteisiä tehtäviä hoidettaessa. (VAHTI 2016, 15.)

Rekisteröidyllä on oikeus tietojensa siirtämiseen rekisterinpitäjältä toiselle. Siirron toteuttamiselle löytyy erilaisia mahdollisuuksia riippuen siitä, minkälaisia teknisiä mahdollisuuksia sen toteuttamiselle löytyy. Jos kahden eri rekisterinpitäjän järjestelmät ovat keskenään yhteensopivia tietojen siirron suhteen, voi tiedot lähettää automatisoidusti suostumuksen tai sopimuksen salliessa. Järjestelmien ollessa erilaisia, tulee siirron tapahtua yleisesti käytössä olevilla tiedonsiirto -välineillä, esimerkiksi siirrettävällä muistivälineellä. Siirto-oikeus ei velvoita eri järjestelmien yhteensovittamista tietojen siirron mahdollistamiseksi. (VAHTI 2016, 16.)

2.5.4 Oikeus vastustaa käsittelyä, automaattista päätöksentekoa ja profilointia

”Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu 6 artiklan 1 kohdan e tai f alakohtaan, kuten näihin säännöksiin perustuvaa profilointia” (VAHTI 2016, 16). Käsittelyn vastustaminen ei ole mahdollista, jos rekisterinpitäjä osoittaa, että käsittelyn tärkeys perustellusti syrjäyttää rekisteröidyn oikeudet ja vapaudet, tai jos käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi (VAHTI 2016, 16).

Rekisteröidyllä on oikeus olla joutumatta automatisoidun päätöksenteon, kuten profiloinnin kohteeksi, jos sillä on merkitystä hänen oikeusvaikutuksiinsa, tai vaikuttaa häneen muulla vastaavalla tavalla. Edellä olevaa kohtaa ei sovelleta, jos päätöksenteko on välttämätön rekisterinpitäjän ja rekisteröidyn välisen sopimuksen täytäntöönpanoa varten, päätöksenteko on hyväksytty rekisterinpitäjään sovelletun lainsäädännön mahdollistamana, jossa kuitenkin vahvistetaan asianmukaiset toimenpiteet ”rekisteröidyn oikeuksien ja vapauksiin sekä oikeutettujen etujen suojaamiseksi” tai päätös perustuu rekisteröidyn suostumukseen. (VAHTI 2016, 16.)

2.5.5 Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta

Tietoturvaloukkauksen tapahtuessa rekisteröidyllä on oikeus saada siitä tieto, jos loukkaus aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille, esimerkiksi identiteetinvarkauksien, maksuvälinepetosten tai muun rikollisen toiminnan muodossa. Jos tietomurron uhreja on lukuisia, eikä yksittäisten viestien lähettämistä nähdä järkevänä vaihtoehtona, voi rekisterinpitäjä tiedottaa tietomurron kohteeksi joutuneita median välityksellä. (VAHTI 2016.) Psykoterapiakeskus Vastaamo tiedotti asiakkaitaan median välityksellä 21.10.2020 julkaistessaan tiedotteen tietomurrosta. Tiedote sai nopeasti ansaitsemansa mediahuomion ja kansa tuli tietoiseksi tapahtuneesta lyhyen ajan kuluttua tiedotteen julkaisusta. (Vastaamo 2020.)

Rekisteröidylle annettavan ilmoituksen tulee antaa ilmaan aiheetonta viivästystä. Ilmoituksen tulisi sisältää ”selkeän ja yksinkertaisen kuvauksen tapahtuneesta, Tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta rekisteröidyt voivat halutessaan kysyä lisätietoja, tiedot siitä, millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidyille, Kuvaus niistä toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi riittävän yleisellä tasolla”. (VAHTI 2016, 17.) Tietosuojavaltuutetun www-sivuilta löytyy suuntaviivat rekisterinpitäjälle tietoturvaloukkauksesta ilmoittamiseen, jossa sivuilla 32–35 on taulukko esimerkkitilanteista, joista rekisterinpitäjä saa kuvan siitä, missä tilanteessa ilmoitus tulisi tehdä. (Tietosuojaryhmä 2018, 32–35.)

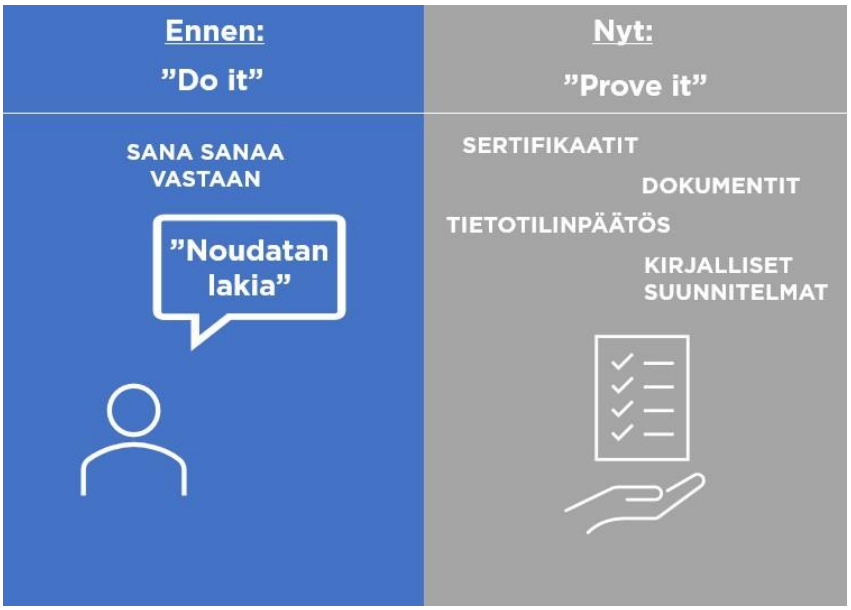
2.6 Tietosuojan hallinnointi, roolit ja vastuu

Luonnollista, tai oikeushenkilöä, yleisesti yritystä tai organisaatiota, joka on määritellyt miten ja miksi henkilötietoja käsitellään, nimetään rekisterinpitäjäksi. Rekisterinpitäjän tehtävänä on toteuttaa rekisteröidyn oikeudet varmistamalla riittävä tekniset ja organisatoriset toimet tietosuojan toteuttamiseksi.

Tietosuoja-asetuksen mukaisesti rekisterinpitäjän riskiperusteinen vastuu on ensisijainen rekisteröidyn henkilötietojen suojan kannalta. Jotta henkilötietojen käsittely olisi lainmukaista, tulee rekisterinpitäjän toteuttaa asianmukaiset ja tehokkaat toimenpiteet, mitkä määritellään käsittelyn luonteesta, laajuudesta, asiayhteydestä, tarkoituksista sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien riskien arvioinnista. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 269.)

25. artiklan mukainen sisäänrakennettu ja oletusarvoinen tietosuoja korostaa Andreasson ym. (2019, 23–24) mukaan rekisterinpitäjän velvollisuuksia ottaa tietosuojatyö vahvasti mukaan kaikkeen toimintaan yrityksissä ja organisaatioissa. Sisäänrakennetun ja oletusarvoisen tietosuoja lisäksi tietosuoja-asetus toi mukanaan accountability-periaatteen, eli rekisterinpitäjän osoitusvelvollisuuden, mikä käytännössä tarkoittaa sitä, että pelkkä lain noudattaminen ei

riitä (do it), vaan lain noudattamisen lisäksi rekisterinpitäjän tulee kyetä todistamaan lain noudattamisen esimerkiksi dokumentein, kirjallisin suunnitelmin, käytännesäännöin, sertifioinnein tai tietotilinpäätöksin (prove it) (Kuvio 7). (Andreasson, Riikonen & Ylipartanen 2019, 25.)



Kuvio 7 Do it vs. Prove it (Andreasson, Riikonen & Ylipartanen 2019, 25).

2.6.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

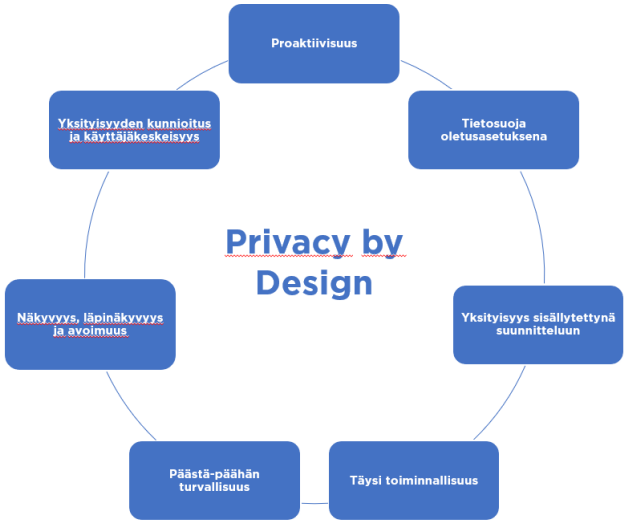
Sisäänrakennettu tietosuoja juontaa juurensa Ann Cavoukianin luomaan termiin privacy by design, minkä ideoinnin hän aloitti 1990-luvulla. Cavoukianin tavoitteena oli luoda sellainen tietosuojan käsittelytapa, joka alusta alkaen olisi tietojärjestelmien suunnittelussa ja henkilötietojen käsittelytoiminnassa mukana. (Hes & Borking 1995.) Privacy by design -malli julkaistiin virallisesti vuonna 2009, ja tietosuoja-ammattilaiset ottivat termin käyttöön vuonna 2010 kansainvälisessä tietosuojan ja -turvan ammattilaisten konferenssissa.

Cavoukianin (2010, 2) mallissa (kuvio 8) keskeistä on seitsemän periaatetta. Ensimmäisen periaatteen mukaan tietosuojan tulee olla proaktiivista, ei reaktiivista; ennaltaehkäisevää ei hoitavaa. Tietosuojan tulee olla ennakoivaa, milloin riskit tunnistetaan etukäteen ja vahinkojen hoitamisen sijasta yksityisyyden loukkaukset ja tietosuojariskit ennaltaehkäistään. Toisen periaatteessa voidaan huomata, että oletusarvoinen tietosuoja on Cavoukianin mallin mukaan osa sisäänrakennettua tietosuojaa. Oletusarvoisessa tietosuojassa henkilötiedot suojataan

tietojärjestelmissä, tai järjestelmässä automaattisesti, millä tahansa toimintatavalla. Käyttäjän ei siis tarvitse tehdä mitään suojatakseen yksityisyytensä. (Cavoukian 2010, 2–3.)

Kolmannen periaatteen mukaan yksityisyys tulee sisällyttää järjestelmiin siten, että käyttäjä ei edes huomaisi sitä; tietosuoja on luonnollinen ja keskeinen osa järjestelmää heikentämättä toiminnallisuutta. Neljäs periaate kuvaa täyttä toiminnallisuuden tilaa, jossa pyritään tuottamaan lisäarvoa, eikä nollasummapelin kaltaista tilannetta, jossa ajatellaan järjestelmien ominaisuuksien kumoavan toisiaan; edistyksellinen käytettävyys ei kumoa yksityisyydensuojaa, järjestelmän turvallisuus ei yksityisyyttä. Cavoukian (2010, 3-4) kuvaa 4. periaatteen toteutumista kultaisen standardin saavuttamisena. (Cavoukian 2010, 3-4.)

Viidennessä periaatteessa korostetaan päästä-päähän-turvallisuutta. Kun tietosuoja on sisäänrakennettu, on silloin jokainen tiedonjyvänen suojattu koko elinkaarensa ajan, alusta loppuun, jolloin tiedonjyvänen tulee tuhota asianmukaisesti. Kuudennen periaatteen mukaan tietosuojaprosessit -ja käytännöt tulee olla selkeästi ja läpinäkyvästi toteutettuja, sekä kaikkien osapuolten saatavilla. Cavoukian (2010, 4) alleviivaa yksilön vastuuta, jolloin hajautettu vastuu ei vaaranna tiedon suojaa. Seitsemännen ja viimeisen periaatteen tavoitteena on käyttäjän yksityisyyden kunnioitus, milloin sisäänrakennettu tietosuoja vaatii ohjelmistosuunnittelijoita ja operaattoreita pitämään ohjelmistot loppukäyttäjäkeskeisinä. Käyttäjän kunnioitus onnistuu seuraavien toimien tukemana; suostumuksen pyytäminen, tietojen täsmällisyys, tietojen saavutettavuus ja toimintojen määräystenmukaisuus. (Cavoukian 2010, 4-5.)



Kuvio 8 Sisäänrakennettu tietosuoja (Cavoukianin 2010, 2-5).

Korpisaari ym. (2018, 279-280) mukaan sisäänrakennettu tietosuoja edellyttää tietosuoja-asetuksen mukaan rekisterinpitäjältä teknistä ja organisatorista toteutustapaa suunnittelusta käsittelyvaiheeseen. Käytännössä se tarkoittaa sitä, että käytössä oleva järjestelmä on kykenevä automaattisesti esimerkiksi tietojen minimointiin (tekninen), sekä sitä, että kaikki organisaation työntekijät osaavat ottaa huomioon tietojen minimoinnin kaikissa työtehtävissään (organisatorinen). (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 279–280.)

Yleinen tietosuoja-asetus velvoittaa rekisterinpitäjiä punnitsemaan toimenpiteitä; henkilötietojen suojan kannalta pieniriskiselle harrastustoiminnalle ei voida asettaa samanlaisia vaatimuksia, kuin arkaluontoisia henkilötietoja käsittelevälle psykoterapiapalvelulle. Vaatimusten tulee perustua riskiarvioon käsiteltävien henkilötietojen arkaluontoisuudesta. Mitä arkaluontoisemmat tiedot rekisteröidyn oikeuksien kannalta, sitä vaativammat ovat tekniset ja organisatoriset toimenpiteet, joilla näitä henkilötietoja tulisi suojata. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 280-281.)

Digitaalisten palveluiden lisääntyminen ja niiden monimutkaisuus tuo haasteen yksilön henkilötietosuojan toteutumiselle. Suuri palveluiden lukumäärä ei edistä sitä, että ihmiset kiinnostuisivat, osaisivat tai heillä olisi aikaa perehtyä säätämään asetuksia heille itselleen turvalliseksi. Oletusarvoinen tietosuoja tarjoaa mahdollisuuden turvalliseen palveluiden käyttöön, kun käyttäjien ei tarvitse perehtyä jokaisen palveluntarjoajan käyttöehtoihin

yksityiskohtaisesti, vaan käyttäjä voi olettaa, että palvelu on turvallinen henkilötietojen käsittelyn osalta. Harvoin itselläkään tulee luettua tietosuojakäytänteitä ja säätämään henkilötietoasetukset turvalliseksi, vaikka sille olisi aihetta varsinkin sellaisten rekisterinpitäjien kohdalla esimerkiksi rapakon toisella puolella, jotka eivät pyri tietojen minimointiin, vaan käyttävät surutta laajaa henkilötietojen kirjoa muun muassa ylläpitääkseen omaa ansaintamallia. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 280-281.)

2.6.2 Rekisterinpitäjän ja henkilötietojen käsittelijän vastuut

Henkilötietojen käsittelijällä on mahdollisuus käsitellä henkilötietoja rekisterinpitäjän lukuun yrityksen tai organisaation ulkopuolisena tahona. Esimerkkinä tällainen voi olla tilanne, jossa tilitoimisto käsittelee yrityksen työntekijöiden henkilötietoja, kuten palkkatietoja. Ennen kuin henkilötietojen käsittely on mahdollista yrityksen ulkopuolisena tahona, tulee osapuolten välille laatia sopimus henkilötietojen käsittelystä (Data Processing Agreement, DPA). (Andreasson, Riikonen & Ylipartanen 2019, 27.)

Kirjallisessa tietosuojasopimuksessa tulee määritellä yksikohtaisesti, mitä, miten ja kuinka kauan henkilötietoja käsitellään ja mikä on rekisteröityjen ryhmä. Edellä mainituilla tiedoilla yksilöidään, mitä käsittelytehtäviä ulkoistetaan (esim. palkanmaksu), keitä se koskee (esim. työntekijät) ja mitä tietoluokkia käsitellään (esim. työntekijöiden osoitetiedot). Näiden lisäksi sopimuksessa määritellään muista henkilötietojen käsittelijän vastuista, joilla edistetään rekisteröidyn henkilötietojen suojaa tietosuoja-asetuksen artiklojen 32–36 mukaisesti. Kaiken kaikkiaan henkilötietojen käsittelijää koskee samat velvollisuudet, kuin rekisterinpitäjää, joskin tilivelvollisuus henkilötiedoista viimekädessä säilyy rekisterinpitäjällä. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 295.)

2.6.3 Henkilötietojen käsittelyn oikeusperustan arviointi

Henkilötietojen käsittelylle tulee olla asetuksen mukainen oikeusperusta, eli käytännössä se voi olla rekisteröidyn vapaaehtoinen suostumus, joka on pyydetty henkilötietojen keräämisen yhteydessä, sellaisen sopimuksen täytäntöön paneminen, jossa rekisteröity on osapuolena, rekisterinpitäjän lakisääteinen velvoite tai rekisterinpitäjän oikeutettu etu. Edellä mainitut oikeusperustat ovat yleisiä yksityisellä puolella. Esimerkiksi viranomaisten käsittelemistä henkilötiedoista säädetään eri tavalla, kuin elinkeinoelämän henkilötietojen käsittelystä. Viranomaisten käsittelyn perusteena on yleisesti julkisen vallan käyttäminen, jolloin rekisteröity ei voi vastustaa henkilötietojensa käsittelyä. (VAHTI 2016, 18; Tietosuojavaltuutetun toimisto 2021c.)

Tietosuoja-asetuksen mukaisesti henkilötietojen käsittelyssä sopimuksen täytäntöön panemiseksi tulee varmistua siitä, että henkilötietojen käsittelylle on todellinen tarve. Esimerkiksi yritys voi käsitellä osoitetietoja, jotta tilattu tuote voidaan toimittaa perille. Asetus

velvoittaa kuitenkin rajamaan käsittelyn koskemaan vain välttämättömiä henkilötietoja. Lakisääteinen velvoite koskee Tietosuojavaltuutetun toimiston (2021c) mukaan sekä yksityistä, että julkista puolta; lakisääteinen velvoite toteutuu esimerkiksi silloin, kun työnantaja ilmoittaa työntekijän palkkatiedot veroviranomaisille. Rekisterinpitäjän oikeutettu etu tulee voimaan tilanteissa, joissa esimerkiksi rekisterinpitäjällä ja rekisteröidyllä on jokin merkityksellinen suhde. Merkityksellinen suhde voi toteutua esimerkiksi yrityksen työntekijän ja yrityksen (rekisterinpitäjän), tai asiakkaan ja yrityksen välillä. (Tietosuojavaltuutetun toimisto 2021c.)

Jackson (2018) käsittelee artikkelissaan oikeutettua etua käsittelyperusteena. Hänen mukaansa oikeutettu etu voisi olla houkuttelevin vaihtoehto, koska se on joustavin peruste tietojen käsittelylle. Houkuttelevuudella kirjoittaja tarkoittaa sitä, että oikeutetun edun vuoksi rekisterinpitäjän ei tarvitse erikseen pyytää suostumusta henkilötietojen käsittelyyn, minkä organisaatiot tulkitsevat helposti keinoksi luistaa suostumuksen pyytämisestä; tietosuoja-asetus ei velvoita suostumuksen pyytämiseen, jos käsittelylle on olemassa jokin asetuksen mukainen oikeudellinen peruste. Kuten Jackson (2018), myös Tietosuojavaltuutetun toimisto (2021c) suosittelee toisien korttien katsomista ennen oikeutetun edun käyttämistä käsittelyperusteena. Yleinen käsittelyn peruste esimerkiksi yrityksillä on sopimus asiakkaan kanssa, jolloin erillistä suostumusta ei tarvita. Jos käsittelyn perusteeksi rekisterinpitäjän arvion mukaan riittää oikeutettu etu, tulee siitä Jacksonin (2018) ja Tietosuojavaltuutetun toimiston (2021) mukaan laatia tasapainotesti. Tasapainotestissä (legitimate interests assessment LIA) tulee arvioida sitä, käykö oikeutettu etu henkilötietojen käsittelyperusteeksi. (Jackson 2018; Tietosuojavaltuutetun toimisto 2021d.)

Tietosuojavaltuutetun toimiston internet-sivuilta löytyvässä suomenkielisessä kuusivaiheisessa tasapainotestissä kuvataan päätöksen teon vaiheet ja jos käsittelyn tarkoitus, luonne tai asiayhteys muuttuu, tulee testi tehdä uudelleen ja kuvauksen tulee päivittää uutta käsittelyä vastaavaksi. Testissä ensimmäisenä tulee pohtia, onko oikeutettu etu sopivin käsittelyperuste verrattuna muihin käsittelyperusteisiin (sopimus, suostumus jne.). Jos muut käsittelyperusteet eivät sovellu, voi testissä siirtyä kohtaan kaksi, jossa tulee pohtia edun lainmukaisuutta sekä sitä, onko edulle todellista ja välitöntä tarvetta. Etu ei voi olla millään tavalla olla spekulatiivinen. Kohdassa kaksi velvoitetaan ilmaisemaan etu selkeästi, jotta sen tasapainoa rekisteröidyn etuihin ja oikeuksiin voidaan arvioida. Kohdan kaksi täyttyessä siirrytään kolmanteen kohtaan, jossa tulee harkita keinoja, joilla samaan lopputulokseen päästäisiin puuttumalla rekisteröidyn yksityisyyteen vähemmän. Mikäli keinoja ei löydy, tulee siirtyä kohtaan neljä. (Tietosuojavaltuutetun toimisto 2021d.)

Kohta neljä koostuu kolmesta kysymyksestä, joiden avulla arvioidaan henkilötietojen käsittelyn tosiasiallisia vaikutuksia: 1. Rekisterinpitäjän tai kolmannen osapuolen etu; oikeutettu etu voi tarkoittaa esimerkiksi jonkin perusoikeuden, kuten sanan-, taiteen ja tutkimuksen- tai elinkeinovapauden toteutumista tai muusta oikeutetusta edusta esimerkiksi silloin, jos

käsittely menee lähelle jotain muuta käsittelyperustetta olematta kuitenkaan varsinaisesti sen käsittelyperusteen alalla. 2. tulee pohtia vaikutuksia rekisteröityyn. Vaikutuksista tulee pohtia henkilötietojen luonnetta, mitä henkilötietoa käsitellään ja miten käsittelytoimenpiteet vaikuttavat rekisteröityyn. Esimerkiksi henkilötietojen luonteen näkökulmasta kriittistä on erityisesti arkaluontoisten tietojen käsittely. Mitä negatiivisempia ja epävarmempia käsittelyn seuraukset voivat rekisteröidylle olla sitä epätodennäköisemmin käsittelyä pidetään oikeutettuna. Tasapainotestin tarkoituksena on estää rekisteröidyn näkökulmasta kohtuuttomat vaikutukset. (Tietosuojavaltuutetun toimisto 2021d.)

Tasapainotestin viidennessä kohdassa kehotetaan varmistamaan tietosuojan lisätakeet. Tasapainotestin lopputulos riippuu kokonaiskuvasta, milloin oikeanlaisen vaikutustenarvioinnin perusteella tehdyt toimet henkilötiedon suojaamiseen tasapainottavat lopputulosta, tehden henkilötietojen käsittelystä perusteltua. Erilaiset tekniset ja organisatoriset toimenpiteet, laajat anonymisointitekniikoiden käyttö, yksityisyyden suojaa parantavien tekniikoiden hyödyntäminen ja henkilötietojen salaus voivat toimia tietosuojavaltuutetun toimiston mukaan lisätoimenpiteinä tasapainon saavuttamiseksi. Kuudennessa, ja viimeisessä kohdassa tulee osoittaa toiminnan lainmukaisuus ja varmistaa avoimuus viimeistelemällä ja säilyttämällä tasapainotestissä laadittu kirjallinen kuvaus. Avoimuus on tärkeässä osassa ja rekisteröidylle tulee olla valmis perustelemaan käsittelyn oikeudellinen perusta. (Tietosuojavaltuutetun toimisto 2021d.)

2.6.4 Tietosuojavastaava

Tietosuojavastaavan tulee nimittää julkishallinnon elimet, viranomaiset, sekä sellaiset organisaatiot, joiden ydintehtävien luonteeseen kuuluu rekisteröityjen säännöllistä ja laajamittaista seurantaa, käsittely koskee erityisiä henkilötietoryhmiä, rikostuomioita, tai rikoksia koskevia tietoja. Tietosuojavastaavan tehtäviin kuuluu olla asetuksen mukaisesti itsenäinen erityisasiantuntija, jonka toimeen on kohdistettava riittävät resurssit. (Andreasson, Riikonen & Ylipartanen 2019, 15.) Sotka (2017) vertaa tietosuojavastaavan asemaa luottamusmiehen asemaan, milloin hänellä tulee olla riippumaton asema organisaatiossa ja hänellä tulee olla mahdollisuus raportoida tietosuojapuutteista suoraan yrityksen johdolle ja valvontaviranomaiselle. Tietosuojalainsäädännön ja alan käytäntöjen tuntemus on ensisijaista, ja tietosuojavastaavan on otettava mukaan kaikkeen tietosuojaan liittyviin kysymyksiin. Kirjoittaja näkee tietosuojavastaavan nimittämisen tarpeettomaksi toimenpiteeksi, jos se ei tuota lisäarvoa vaatimusten mukaisuuden täyttämiseksi, esimerkiksi tietosuoja nykytilan ja tavoitetilan kuilun kuromiseksi umpeen. (Sotka 2017.) Huolimatta siitä, että tietosuojavastaava nimetään vapaaehtoisesti, tulee nimittämiseen, asemaan ja tehtäviin soveltaa tietosuoja-asetuksen vaatimuksia siten, kuin kyseessä olisi pakollinen nimeäminen (Tietosuojavaltuutetun toimisto 2021d).

Tietosuojavastaavan nimittäminen ei koske suurinta osaa suomalaisista yrityksistä, mutta se ei poista rekisterinpitäjän vastuuta hallinnoida ja organisoida tietosuojatyötä asetuksen mukaisesti. Tietosuojavastaavan tyylistä toimenkuvaa voisi Sotkan (2017) mukaan harjoittaa jokin henkilö yrityksen sisältä, jota ei virallisesti nimetä tietosuojavastaavaksi, vaan olisi muuten vastuussa tietosuojan toteuttamisessa yrityksessä. (Sotka 2017.)

2.6.5 DPIA ja PIA

Tietosuoja-arjessa on alkanut esiintymään lyhenteitä liittyen uuteen tietosuoja-asetukseen, jotka vaikuttavat ensisilmäyksellä samanlaisilta. Itselle tätä työtä kirjoittaessa DPIA ja PIA vaikuttivat lähes identtisiltä tarkoitusperineen. Suomen kielessä kummatkin lyhenteet tarkoittavat vaikutustenarviointia. Tässä luvussa selvennän, miten nämä kaksi toimintatapaa eroavat toisistaan, ja toisaalta, mitä yhtäläisyyksiä ne jakavat keskenään.

DPIA ja PIA ovat omina tietosuojan hallintatapoina tärkeitä riskienhallintakeinoja, joten ne palvelevat tietosuojaa omalla tavallaan. PIA ei ole DPIA ilman D-kirjainta, vaikka ne jakavatkin samoja perusteita. Infopulse SCM tiivistää eron seuraavasti: PIA:n (Privacy Impact Assessment) tarkoituksena on analysoida, miten yritys kerää, käyttää, jakaa ja ylläpitää henkilötietoja peilaten olemassa oleviin riskeihin, esimerkiksi sisäänrakennetun tietosuojan suojausprosessissa, kun yritys tai organisaatio käynnistää tai ostaa uuden liiketoiminnan itselleen, jalkauttaa uuden prosessin, tai lanseeraa uuden tuotteen. DPIA:ssa (Data Protection Impact Assessment) on kyse korkean riskin henkilötietojen käsittelyyn liittyvien riskien tunnistamisessa ja pienentämisessä. (Infopulse SMC 2019.)

Tietosuoja-asetuksen alkumetreillä oli hyvin yleistä, että ihmiset sekoittivat termin keskenään, ja jossain määrin sitä tehdään edelleen. Ranskan kansallinen tietojenkäsittely- ja vapauskomissio määrittelee oppaassaan (CNIL 2018) PIA:n tarkoittavan samaa, kuin DPIA. Kyse voi toki olla erehdyksestä, onhan opas kirjoitettu alun perin vuonna 2015, mutta päivitetty vuonna 2018. (CNIL 2018.) Ehkä on niin, että termejä on luvallista käyttää toisiinsa sekoittaen, kuten CNIL asian on esittänyt. Tietosuojamakasiini -podcastissa kuvailtiin näitä kahta lyhennettä käytettävän ”iloisesti sekaisin” (Järvinen & Lankinen 2020).

Aiheen teorian kannalta on tärkeää käyttää oikeanlaista terminologiaa, eli mitä tietosuoja-asetuksessa on määritelty käytettäväksi riskienarvioinnista henkilötietojen käsittelyyn liittyen. Asetuksen 35 artiklan mukaisesti DPIA:a tulee käyttää tietyissä henkilötietojen käsittelyissä. PIA:sta taas ei säädetä asetuksessa, joten se ei ole velvoitettu toimenpide, vaikka tietosuojan kannalta se on erinomainen riskienhallintakeino, minkä käyttäminen tukee osoitusvelvollisuutta.

Tietosuoja-asetuksessa säädetään vaikutustenarvioinnin (DPIA) suorittamisesta ennen henkilötietojen käsittelyä tapauksissa, joissa on arvioitu käsittelytoimiin liittyvän korkea riski

luonnollisen henkilön oikeuksille ja vapauksille, esimerkiksi julkisten alueiden kameravalvonnan yhteydessä. Tietosuojavaltuutetun toimiston (2021) mukaan vaikutustenarvioinnissa tulee kuvata henkilötietojen käsittelyä, arvioida käsittelyn tarpeellisuutta, oikeasuhteisuutta ja henkilötietojen käsittelystä aiheutuvia riskejä sekä toimenpiteitä, joilla riskeihin puututaan. Tarvittavien toimenpiteiden jälkeen arvioidaan jäännösriskin oikeellisuutta, sekä salliiko sen hetkiset olosuhteet riskin hyväksymisen. Yksittäinen vaikutusten arviointi käsittelee vain yhtä käsittelytoimea- tai ryhmää. Kun yksittäistä vaikutustenarviointia käytetään muussa käsittelytoimessa- tai ryhmässä, tulee niiden olla alkuperäisen arvioinnin kohteen kanssa samanlaisia. DPIA:n yhteydessä tulee kuulla lisäksi paikallista valvontaviranomaista. (Tietosuojavaltuutetun toimisto 2021e.)

Vaikutustenarvioinnin velvoite voi seurata tietosuoja-asetuksessa yksilöidyistä käsittelytilanteista. Lisäksi velvoite voi seurata, jos käsittelytoimi löytyy tietosuojaviranomaisen luettelosta tai kansallinen lainsäädäntö on muuten velvoitteesta säätänyt. Tietosuoja-asetuksessa yksilöidyissä käsittelytilanteissa, joissa vaikutustenarviointi tulee suorittaa ennen käsittelyä, ovat muun muassa henkilötietojen käsittely uudella teknologialla, automaattinen käsittely, jolla on oikeusvaikutuksia, automaattinen henkilökohtaisien ominaisuuksien laajamittainen arviointi, jolla niin ikään on oikeusvaikutuksia tai muita merkittäviä vaikutuksia henkilöön. (Tietosuojavaltuutetun toimisto 2021e.) Tyypillinen liiketoiminnan esimerkki vaikutustenarvioinnin vaativasta käsittelytoimenpiteestä on kotisivuilla vieraileville tehtävä pisteytys sivuilla tapahtuvan seurannan avulla, jonka perusteella arvioidaan potentiaalisen asiakkaan tarvetta, eli kuinka kiinnostunut henkilö on yrityksen tuotteista. Pisteytys onnistuu käyttäjän päätelaitteelle asennettujen evästeiden avulla, jotka seuraavat käyttäjän vierailuja yrityksen kotisivujen eri osissa.

EU:n tietosuoja-asioissa neuvoa antavan elimen, tietosuojaryhmän, julkaisemassa ohjeessa on annettu kriteeristö, joiden kaksi kohtaa täyttymällä vaikutustenarviointi on yleensä tehtävä. Mitä useampi kriteeristön kohdista sopii käsittelyn luonteeseen, sitä todennäköisemmin käsittely aiheuttaa korkea riski rekisteröidyn oikeuksille ja vapauksille. Osoitusvelvollisuuden näkökulmasta DPIA on hyvä toteuttaa, vaikka siihen ei suoraan velvoiteta. Tietosuoja-asetuksessa ei määritellä tapaa, jolla DPIA:n tulisi suorittaa, vaan tyyli on jokaisen rekisterinpitäjän päätäntävallan alla. Tietosuojavaltuutetut suosittelevat kuitenkin käytettävän mahdollisimman yhdenmukaisia malleja sen toteuttamiseen, joita kansainväliset tietosuojaviranomaiset ovat laatineet. (Tietosuojavaltuutetun toimisto 2021e.)

2.7 Yleisen tietosuoja-asetuksen haasteet

Yleisen tietosuoja-asetuksen voimaantulo ei ole ollut kivuton prosessi. Erityisesti muotoseikat ovat aiheuttaneet päänvaivaa varsinkin pienemmissä yrityksissä, joilla ei esimerkiksi ole varaa palkata lakimiehiä selventämään niitä. Haasteet koettiin suurimpana ennen asetuksen

voimaantuloa; erityisesti pelättiin (ja on peloteltu) hallinnollisia seuraamuksia, jotka ovat kuitenkin paljastuneet epätodennäköisiksi erityisesti pieniriskisten henkilötietojen käsittelyä harjoittavien rekisterinpitäjien kannalta. (Enroth & Neuvonen 2017, 10.) Vuonna 2020 Suomessa jaettiin yleisen tietosuoja-asetuksen määrittämiä valvontasakkoja viisi kappaletta, joista suurin yksittäinen sakko oli 100000 euroa (Korhonen 2021). Yritysrekisterin mukaan vuonna 2019 suomessa oli vuonna 292 377 yritystä, ja jos tuohon lukuun lisätään kaikki rekisterinpitäjä -nimikettä pitävät oikeus -ja luonnolliset henkilöt, yksittäiselle rekisterinpitäjälle langettavan sanktion riski on tapauksien perusteella hyvin vähäinen (Suomen yrittäjät 2021). On kuitenkin oletettavissa, että sanktiofrekvenssi tulee nousemaan tulevaisuudessa, muiden EU:n jäsenvaltioiden tapaan. Suomen kokoluokan valtioista esimerkiksi Ruotsissa on jaettu 17 ja Norjassa 22 GDPR-sakkoa 7.4.2021 mennessä (Enforcementtracker 2021). Sanktioiden lisäksi tulee perään kuuluttaa ennen kaikkea tietosuojanhallinnan hyötyjen merkitystä, jolloin keskustelu sanktioista ei olisi ainoa hallitseva tekijä tietosuoja-asetuksen vaatimusten noudattamisessa.

Enroth ja Neuvonen (2017) tuottivat vuoden 2017 lokakuussa valtioneuvoston toimeksiannosta selvityksen EU:n tietosuoja-asetuksen yritysvaikutuksista. Selvityksessä menetelminä käytettiin sähköistä kyselyä sekä teemahaastattelua. Perusjoukkona selvityksessä on kaikki suomen yritykset. Selvityksen keskeisimpiä pk-yrityksiä koskevia löydöksiä olivat epätietoisuus sääntelyn tuomista vaatimuksista, erityisesti muotovaatimukset koettiin hankalaksi sisäistää. Asetuksen vaikutukset pk-yrityksiin, yrittäjyyteen ja yritysten kasvumahdollisuuksiin positiivisesti ajateltiin selvityksen valossa tulevan vain siinä tapauksessa, jos tiukentuva lainsäädäntö lisäisi kuluttajien luottamusta digitaalisiin palveluihin ja sitä kautta lisäisi niiden käyttöä pitkällä aikavälillä. Yleisesti tiukentuva sääntely nähtiin negatiivisena asiana. (Enroth & Neuvonen 2017, 7.)

Enroth ja Neuvonen (2017, 10) tiivistävät selvityksen yhteenvedon lyhyesti: Ohjausta ja yhteistyötä. Pienet yritykset sisäistävät huonommin tietosuoja-asetuksen uudet vaatimukset ja niiden noudattamisen lisäämiseksi määritellyt hallinnolliset sakot koettiin epäoikeudenmukaisiksi. Yritykset toivoivat kansallisen liikkumavaran sijaan oikeustilan täsmentymistä tulkinnanvaraisten käsitteiden osalta. Selvityksen mukaan epätietoisuutta aiheuttavat oikeudelliset termit ovat muun muassa seuraavat termit: Portability – missä muodossa ja kuinka laajana tiedot on saatava siirrettyä, oikeus tulla unohdetuksi – mikä on tietojen poistamisen laajuus, osoitusvelvollisuuden käytännesäännöt, mikä käytännössä riittää anonymisoinniksi ja pseudonymisoinniksi, yleinen etu, lakisääteinen tehtävä, oikeutettu etu, yksityisen yrityksen toiminen osittain myös julkisessa roolissa, konsernin käsite – suhde muihin yhteenliittymiin. (Enroth & Neuvonen 2017, 10.)

Huolimatta siitä, että Enrothin ja Neuvosen (2017) selvitys on lainsäädännön kehittymisen kannalta jo osittain vanhaa tietoa, on siitä löydettävissä paljon sellaista arvokasta tietoa, mikä koskee tavallista suomalaista yrittäjää asetuksen vaikutusten kannalta vielä tänäkin päivänä. Uskon 2017 kyselyyn vastanneiden pk-yrittäjien ajatusten olevan osittain vielä samanlaisia, joskin tietosuoja-asetuksen voimaantulon ja sen soveltamisen aloittamisen jälkeen suomessa vaikutukset eivät varsinkaan pienille yrityksille ole olleet niin mittavia, millaisiksi yrittäjät ne selvityksen mukaan ovat ajatelleet. Tästä syystä asenneilmapiiri voi olla tällä hetkellä neutraalimpi.

Korpisaari ym. (2018, 648-650) kuvailevat tietosuoja-asetuksen vaikutuksia puoli vuotta asetuksen voimaan tulon jälkeen, milloin organisaatioita työllistävät eniten tietojenkäsittelysopimukset, yksittäiset rekisteröityjen esittämät pyynnöt tarkastaa omat tietonsa, tietoturvaloukkausten ilmoitusvelvollisuuden täyttävän kynnyksen täyttymisen arviointi ja tarvittavan dokumentaation laatiminen erilaisissa henkilötietojen käsittelytilanteissa. Myös henkilötietojen käsittelyyn liittyvät riita•tilanteet ja erilaiset prosessit ovat voimakkaassa kasvussa. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 648–650.)

Sankarin ja Wibergin (2019) mukaan tietosuoja-asetus ei toimi. Kirjoittajat pohtivat, miten pitkät ja vaikeaselkoiset tietosuojaselosteet vahvistavat yksilöiden tietosuojaa, ovatko rekisterinpitäjien käytännöt tietosuojaselosteiden mukaisia, ja voiko yksilö varmistua rekisterinpitäjien toimien lainmukaisuudesta. Yritysten käyttämät tietojenkeräys- ja hyödyntämisalgoritmit ovat kilpailuetua tuovia kokonaisuuksia, ja näin ollen ne kuuluvat liikesalaisuuslain 595/2018 piirin. (Sankari & Wiberg 2019, 340.) Tällä kirjoittajat todennäköisesti halusivat viestiä siitä, mikä on loppujen lopuksi läpinäkyvyyden taso, joka luonnollisille henkilöille tulee taata, eli sen perusteella voidaan pohtia, onko tarpeen raportoida kaikesta avoimesti, vai riittääkö toimien yleinen kuvailu?

Kirjoittajat havaitsivat kahdeksalle eri rekisterinpitäjälle suunnatun kyselyn vastauksissa puutteita läpinäkyvyydessä, käyttötarkoitussidonnaisuudessa, tietojen minimoinnissa ja säilytyksen rajoittamisessa. Apple, Traficom, Veikkaus, Sanoma ja Yle, eli 5/8 yrityksestä vastasivat. Kirjoittajien mukaan merkittävin muutos asetusta edeltäneeseen aikaan on rekisterinpitäjien internet-sivuille päivitetyt tietosuojaselosteet. Asiakasrajapinnassa ei ole tapahtunut merkittävää muutosta. Erityisesti käsittelyperusteista suostumus nähtiin toimimattomana; suostumuksen peruuttaminen on vaikeampaa, kuin antaminen. Vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu ei toteutunut ainakaan vuonna 2019, ei edes Suomen suurimpien yhtiöiden ja virastojen toimesta. Kirjoittajien mukaan asetus ei ole onnistunut monitulkinnallisuuden takia sen edellyttäessä henkilöiltä ”kohtuuttoman paljon” taustatietoja, sekä käsittelijöiltä ja rekisterinpitäjiltä ammattitaidon lisäämistä nykytasoon peilattuna. Useat käsittelyperusteet, sekä kansallisesti säädettävät kohdat eivät tee selväksi, mitä lakia tai asetusta eri tilanteissa tulisi soveltaa. Päätelminä kirjoittajat toivoisivat yksilöiltä

tietoisuuden lisäämistä oikeuksistaan ja vaatimusta tietosuoja-asetuksen noudattamisesta, rekisterinpitäjiltä koulutuksen lisäämistä, valvontaviranomaisilta valvonnan lisäämistä ja tulkintaerojen täsmentämistä, poliitikoilta paneutuvuutta asiaan muun muassa lisäsääntelytarpeen (toim. huom. Lisäsääntelyarviointia ja lisäsääntelyä on tehty vuoden 2019 jälkeen) arvioinnin muodossa. Medialta kirjoittajat vaativat kiinnittämään enemmän huomiota asiaan uutisoimalla enemmän aiheesta. (Sankari & Wiberg 2019, 344–346.)

Euroopan Unionin tasolla tuotetussa kyselytutkimuksessa (GDPR 2019) hankittiin 716 eurooppalaiselta yritysjohtajalta (alle 500 työntekijän yritykset) tietoa siitä, miten he ovat suoriutuneet yleisen tietosuoja-asetuksen vaatimuksista. Kyselyn tuotti GDPR.eu, jota ylläpitää suojattua sähköpostia tarjoava sveitsiläinen yritys, Proton Technologies AG. GDPR.eu -sivuston ylläpitoa rahoittaa lisäksi EU:n Horizon 2020 hanke. Kyselytutkimuksen avainlöydöksiä olivat yrittäjien heikko motivaatiotaso hoitaa tietosuojaa vaatimustenmukaisesti sekä heikko ymmärrys teknisistä vaatimuksista. Kyselyn yritykset ovat sijoittaneet runsaasti pääomaa vaatimustenmukaisuuden täyttämiseen ulkopuolisien asiantuntijoiden avun muodossa. Kyselyn mukaan puolet yrityksistä eivät, asiantuntija-avusta huolimatta, kykene vastaamaan tietosuoja-asetuksen perusperiaatteita koskeviin vaatimuksiin, kuten tietojenkäsittelyn informoinnista rekisteröidyille ja oikeusperustan arvioinnista ennen uuden tietojenkäsittelyn aloittamista. Lisäksi tietoisuus tietoturvaratkaisusta henkilötietojen turvaamiseen oli vähäistä. (GDPR 2019.)

Ensivaikutelmana kyselytutkimuksesta paistoi epäpätevyys ensimmäiseksi niukan, kuusisivuisen raportin perusteella, ja toiseksi siinä näkyy osittain myös Proton Technologies AG:n oma tuotemarkkinointi-intressi, muun muassa suojattuun sähköpostiin liittyvien kysymysten esittämisessä. Toisaalta GDPR.eu -sivuston tarkoituksena on auttaa EU:n pk-yrityksiä ymmärtämään tietosuoja-asetusta selkein opastuksin eri asetuksen vaatimuksista, mikä voi selittää raportin niukkuuden, ja millä osaltaan on haluttu vaikuttaa sen sisäistettävyyteen.

Yksi suurimmista tietosuoja-asetuksen vaatimustenmukaisuuden haasteista on nykyisen lainsäädännön jatkuva muuttuminen, sekä paikallisen valvontaviranomaisen kyky vastata kansallisilla ohjeilla muutoksiin. Nykyhetken haasteista kaiken kokoisille yrityksille tuli EU:n tuomioistuimen heinäkuussa 2020 antaman ratkaisun, C-311/18, eli Schrems II:en myötä, mikä koski henkilötietojen siirron Yhdysvaltoihin mahdollistaman Privacy Shieldin kumoamista. Privacy Shield tarjosi ennen ratkaisun astumista voimaan mahdollisuuden suhteellisen helppoon tietojen siirtoon EU:sta Yhdysvaltoihin mallisopimuslausekkeella.

Tuomioistuimen kanta oli se, että yhdysvaltalainen palveluntarjoaja ei kykene suojaamaan EU:n kansalaisten henkilötietoja erityisesti paikallisten tiedustelulakien vuoksi, joiden mahdollistamana Yhdysvaltojen tiedusteluviranomaisilla on mahdollisuus päästä käsiksi yksityisten palveluntarjoajien hallussa pitämiin tietoihin. Uuden ratkaisun myötä vanhojen

mallisopimuslausekkeiden lisäksi tulisi tehdä muitakin toimenpiteitä oikeudellisesti pätevän siirron toteuttamiseksi. (Tietosuojavaltuutetun toimisto 2020.)

Tietojen siirron tuoma haaste on jopa yrittäjien tiedostamatta yksi suurimmista yleisen tietosuoja-asetuksen tuomista haasteista tällä hetkellä. Kaikki Yhdysvaltoihin yrityksen rekisteripitäjistä tietoa siirtävät palvelut, esimerkiksi perinteiset pilvipalvelut, kuten Google Drive, One Drive ja Dropbox eivät ole uuden ratkaisun myötä mahdollisia alustoja riittävän tietosuojantason varmistamiseksi, jos siirron mahdollistamia juridisesti haastavia toimenpiteitä ei suoriteta. Riittävä toimenpide on nykyohjeiden mukaan seuraava: ”Ennen mallisopimuslausekkeiden käyttöä tietojen viejän on tehtävä tietosuojan tasosta arviointi, jossa huomioidaan mallisopimuslausekkeiden sisältö, erityiset siirtoon liittyvät olosuhteet sekä tietojen tuojan maan oikeudellinen järjestelmä.” Ohjeen lisäksi tietosuojaneuvosto aikoi tutkia, mitä nämä lisätoimenpiteet voisivat sisältää. Tutkimisen perusteella EU:n tietosuojaneuvosto julkaisi marraskuussa 2020 kuuden kohdan oppaan tietojensiirtoarvioinnin tekemiseksi. (Tietosuojavaltuutetun toimisto 2020.) Jos asiaa ajatellaan Yhdysvalloissa sijaitsevaa pilvipalvelua käyttävän yrityksen kannalta, tietojen siirron vaatimustenmukaisuus on todella haastava toteutettava, minkä jälkeen voidaan pohtia, mikä on loppujen lopuksi riski, jos yritys jättäisi suorittamatta tietosuojan arvioinnit tiedonsiirrossa, kun vastapainona on hyvin toimiva pilvipalveluratkaisu? Mikä on riski rekisteröidyn oikeuksille ja vapauksille, jos Yhdysvaltojen tiedusteluviranomainen pääsee käsiksi hänen ei-arkaluontoisiin henkilötietoihinsa? Jos tiedän, että minusta siirtyy rekisterinpitäjän toimesta Yhdysvaltoihin henkilötietoja, kuten evästeiden avulla asetettu ID-tunnus, sekä IP-osoite, ja vastapainona on tämän rekisterinpitäjän markkinoinnin toimivuus, onko silloin mielekästä heikentää yritysten toimintamahdollisuuksia heikentyneiden markkinointimahdollisuuksien vuoksi? Mielestäni ei tulisi korostaa liikaa yksilön oikeuksia, jos vastapainona on kansantalouden tuottavuuden nousu, ja sitä kautta hyvinvoinnin nousu.

Paras ratkaisu rekisteröityjen kannalta olisi käyttää sellaista palvelua, jonka toiminta on täysin EU:n tai ETA:n alueelle sijoittunutta, ja näin ollen tarjoaisi henkilötiedoille tietosuoja-asetuksen mukaisen suojan. Tähän aiheeseen liittyy ajankohtainen, erään tietosuojajuristin kommentti, jossa henkilö arvelee tietojen siirtoon tulevan muutos Yhdysvaltain uuden presidentin valtakaudella. Hänen mukaansa se tarkoittaisi etenkin suurien teknologiajättien kohdalla sitä, ettei mitään näiden jättien, kuten Googlen, Facebookin, Amazonin tai Microsoftin hallussa pitämiä tietoja siirrettäisi Yhdysvaltoihin. Sen sijaan ne jäisivät kaikissa tapauksissa fyysisesti EU:n alueella sijaitseville palvelimille, eikä Yhdysvalloista olisi mahdollisuuksia päästä niihin käsiksi.

Haasteet liittyen uuteen tietosuoja-asetukseen ovat valtavia, ja saavat jatkuvasti uusia mittasuhteita. Tämän vuoksi olisi todella tärkeää, että kansallinen tason tietosuojaviranomainen pysyisi ajan tasalla jatkuvasta muutoksesta tiedottamalla ja ohjeistamalla asianmukaisesti rekisterinpitäjiä vaatimustenmukaisuuden hoidosta etenkin pk-yrityksiä, jotka ovat tämän maan

talouden selkäranka. pk-yrityksiä talouden selkärankana perustelen Suomen Yrittäjien kokoamilla tiedoilla tilastokeskukselta, joiden mukaan pk-yrityksistä tuotetaan arviolta koko bruttokansantuotteesta 40 % (2019) ja vuosien 2001-2016 aikana pk-yrityksiin (työntekijämäärä <250) on tullut työntekijämäärän nettolisäystä 119305 henkilöä. Jos samaa lukua verrataan suuryritysten (työntekijämäärä >250) vastaavaan lukuun -42215, on pk-yritysten rooli ilmeinen kansantalouden kehityksessä. (Suomen yrittäjät 2021.) Schrems II -ratkaisu osoittaa muun muassa selkeiden ja helposti noudatettavien ohjeiden merkityksen liiketoiminnalle. Nykyinen kuuden kohdan ratkaisu on kaikkea muuta, kuin selkeä.

Valoisan puolen koen haasteille löytyvän palveluntarjoajista, jotka voisivat kantaa oman kortensa kekoon auttamalla yrityksiä selviämään sääntelyviidakosta erilaisin teknisin ja organisatorisin ratkaisuin. Tietosuoja-asetuksen soveltaminen on hyvin rekisterinpitäjäkohtaista, joten tapauskohtaisen kehittämisten tarve lisääntyy, ja on lisääntynyt jatkuvasti. Kansallisella valvontaviranomaisella on myös oma roolinsa etenkin ohjeistuksen suhteen. Rekisterinpitäjiä tulee kannustaa ottamaan tietosuoja tiiviiksi osaksi liiketoiminnan harjoittamista, erityisesti silloin, kun tehdään palveluntarjoajasopimuksia, tai tehdään uusia järjestelmähankintoja. Sisäänrakennettu tietosuoja olisi tärkeä sisäistettävä kaikille rekisterinpitäjille, huolimatta henkilötietojen käsittelyn laajuudesta.

2.8 Suomen lainsäädäntö ja yleinen tietosuoja-asetus

Perustuslain (731/1999) 1 § ja 10 § säätävät suomen kansalaisten ihmisarvon loukkaamattomuudesta, yksilön vapauksista ja oikeuksista, oikeudenmukaisuudesta yhteiskunnassa, sekä yksityiselämän suojasta; jokaisen yksityiselämä, kunnia ja kotirauha tulisi olla turvattu. (Suomen perustuslaki 731/1999.)

Opinnäytetyön aihetta ohjaava EU:n Yleinen Tietosuoja-asetus on annettu turvaamaan myös edellä mainittuja suomalaisten perusoikeuksia, tarkemmin henkilötietojen suojaa itsenäisenä perusoikeutena. Koillisen (2013) mukaan yksityisyyden -ja henkilötietojen suojaa ei pitäisi perusoikeuksina sekoittaa keskenään; kaikki henkilötiedot eivät ole yksityisyyden suojan alle kuuluvia, vaikka kaikki yksityisyyden suojaan liittyvät tiedot ovat henkilötietoja. Yksityisyyden suoja ei esimerkiksi kykene antamaan suojaa tilanteessa, jossa tiedonmurusia louhimalla pyritään muodostamaan ja käsittelemään kokonaiskuvia. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 5–7.)

Suomessa henkilötietojen suojaa säädetään yli hallinnonalojen, Korpisaaren, Pitkäsen ja Korhosen (2017, 1–9) selvityksen mukaan yli kahdeksassasadassa säädöksessä (Korpisaari, Pitkänen & Korhonen 2017, 1–9) Tietosuojan kansallinen lainsäädäntö on siis melko sirpaleista, mikä Korpisaari ym. (2018, 3) mukaan ”on aiheuttanut epätietoisuutta yksityisyyttä ja julkisuutta koskevan sääntelyn keskinäisistä suhteista sekä eri viranomaisten toimivaltuuksista informaation käsittelyssä. Lisäksi sääntelyn pirstaleisuus vaikeuttaa tietosuojasääntelyn

sisällöllistä osaamista ja oikeaa soveltamista ja siten myös tehokkaaseen informaatiohallintoon siirtymistä.” (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 5–7.)

Tietosuojalakia 2018/1050 sovelletaan tietosuoja-asetuksen 2 artiklan soveltamisalan mukaisesti. Tietosuojalaki on säädetty täsmentämään ja tarvittaessa säätämään poikkeuksia tietosuoja-asetukseen. Tietosuojalaki toimii yhdessä tietosuoja-asetuksen lisäksi opinnäytetyön kokonaisuutta ohjaavana lainsäädännöllisenä elementtinä ja Laki yksityisyyden suojasta työelämässä ohjaa tarkemmin työntekijöiden henkilötietojen käsittelyä.

Tietosuoja-asetuksen mukaan jokaisen jäsenvaltion on annettava lakisääteisesti tai työehtosopimuksilla yksityiskohtaisempaa tietoa työntekijöiden henkilötietojen käsittelystä työsuhteen yhteydessä. Suomessa 88. artiklasta säätää laki yksityisyyden suojasta työelämässä, eli niin sanottu ”työelämän tietosuojalaki”. ”Laissa säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta” (Laki yksityisyyden suojasta työelämässä 2004/759). Laissa sähköisen viestinnän palveluista 2014/917 säädetään sähköisen viestinnän luottamuksellisuudesta ja siihen liittyvästä yksityisyyden suojasta.

Tässä luvussa mainitut lait toimivat osittain tietosuoja-asetuksen kansallisena lainsäädäntönä. Tietosuojalaki ja työelämän tietosuojalaki täsmentävät tietosuoja-asetusta. Näiden kahden lisäksi löytyy myös viranomaispuolta ja julkista sektoria koskevia lakeja, joiden asettamisesta niin ikään säädetään myös tietosuoja-asetuksessa. Laki sähköisen viestinnän palveluista on säädetty EU:n sähköisen viestinnän tietosuojadirektiivin 2002/58/EY ohjaamana. Euroopan tietosuojaneuvoston mukaan tietosuoja-asetuksen pohjalta säädettävä uusi sähköiseen viestinnän asetus ei saa missään olosuhteissa alentaa vuonna 2002 säädetyn direktiivin vaikuttavuutta, vaan direktiivin 2002/58/EY:n tulee säilyttää sellainen asema, jonka kautta sitä voidaan pitää jatkossakin pätevänä ohjeena liittyen sähköiseen viestintään (Euroopan Tietosuojaneuvosto 2020). Uusi sähköisen viestinnän asetus, E-privacy, tulee voimaan lähivuosina, joten suomessa, asetuksen luonteen mukaisesti, sitä käytetään ensisijaisena lainsäädäntönä. E-privacy-asetuksen määräämänä, kuten oli myös tietosuoja-asetuksen kanssa, tullaan suomessakin säätämään sitä tarkentava kansallinen lainsäädäntö.

3 Kehittämistyön toteutus ja menetelmät

Opinnäytetyön teoriaosuuden jälkeinen kehittämistyövaihe aloitettiin suunnitelman mukaisen valittujen menetelmien avulla tutkimuskysymyksiin vastausta etsien. Työn teoriaosuus antoi jo paljon tietoa vaatimustenmukaisuudesta, varsinkin ensimmäiseen tutkimuskysymykseen, ”Millaisia toimia osoitusvelvollisuuden toteuttamiselle löytyy?”. Aiheen teorian tiedoilla

kykenin kartoittamaan yrityksen nykytilannetta kahdella tunnin mittaisella workshopilla, jotka käytiin aikavälillä 22.2- 3.3.2021. Workshopin lisäksi käytin nykytila-arviossa apuna ennakkotietoja, jotka perustuivat yrityksessä viettämääni aikaa kesätöiden merkeissä. Tietojen perusteella osasin luoda yritykselle tietosuoja-asetuksen kannalta kriittisimpiä dokumentteja ja suosituksia toimintatavoista.

Nykytila-arvion, ja alustavan tietosuojadokumentoinnin jälkeen syvennyin pk-yritysten ja tietosuoja-asetuksen rajapintaan systemaattisen kirjallisuuskatsauksen avulla, missä kävin läpi monialaisesti tietosuoja-asetukseen ja pk-yrityksiin liittyvää teoriaa, sekä vahvaa monimenetelmällistä empiriaa, mikä tutkimuksista tuli ilmi. Kehittämisosuuden tarkoituksena oli siis vahvistaa teoriaosuuden tietoa monialaisten tutkimusten avulla, joilla kykenin luomaan selkeät raamit pk-yritysten tietosuojan kehittämiselle. Raamit tässä tapauksessa tarkoittavat parhaita ja monialaisia keinoja toteuttaa tietosuoja-asetuksen vaatimustenmukaisuutta. Vahvan teoriaosuuden jälkeen tavoitteena ei ollut enää luoda laajaa ja konkreettista lopputuotetta, vaan keskitin ajatukset siihen, mikä ylipäätään on paras keino toteuttaa osoitusvelvollisuus. Sen avulla voi olla varmempi siitä, mitkä toimet oikeasti ovat järkeviä yritykselle, esimerkiksi hyöty/hinta -suhdetta ajatellen: Toisin sanoen, millaisia panostuksia yritysten kannattaisi laittaa vaatimustenmukaisuuteen, kun punnitaan siitä saatavaa hyötyä, ja vaatimustenmukaisuuden hintaa, oli se sitten rahaa tai aikaa.

Teoriaosuuden perusteella selkeää yksittäistä, kaikille sopivaa polkua ei osoitusvelvollisuuteen ole. Lisäksi havaitsin, että ainoastaan julkisivuna toimiva tietosuojaseloste ei itsessään takaa riittäviä näyttöjä tietosuojan toimivuudesta, kuten Sankari ja Wiberg (2019) osoittivat; osoitusvelvollisuus on paljon muutakin, ja yritykset helposti epäonnistuvat siinä, kun lähdetään tutkimaan asioita tietosuojaselostetta syvemmälle (luku 2.6). Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden mukaisesti tietosuoja tulee liittää osaksi jokapäiväistä toimintaa, osaksi kaikkia prosesseja, ja vuosia sitten päivätty tietosuojaseloste ei sellaisenaan sitä ole. Teoriaosuuden perusteella osaan myös kertoa, että johdon sitoutuminen on tärkeää onnistuneelle tietosuojatyölle. Kaikki lähtee arjesta ja näin ollen ulkopuolinen konsultti ei välttämättä takaa vaatimustenmukaisuutta pitkässä juoksussa, kuten nähtiin kyselytutkimuksessa EU:n alueen pk-yrityksille, jossa monet yritysjohtajat olivat satsanneet tietosuojan kehittämiseen, mutta eivät kuitenkaan kyenneet itse vastaamaan perustavaa laatua oleviin kysymyksiin aiheesta (Luku 2.6).

Nykytilanarvioinnin perusteella tehdyssä teoriapainiotteisessa kehittämistyössä painotettiin siis ennen kaikkea tutkimuskysymyksiä 2 ja 3, jotka mielestäni ovat kohdeyrityksen onnistuneen tietosuojatyön edellytykset. Oletukseni oli, kun pohditaan tietosuojatoimien riittävyyttä, puhutaan henkilötietojen suojan riskiperusteisuudesta, ja kun puhutaan tietosuoja-asetuksen noudatettavuudesta jatkossa, on kyseessä silloin vaikuttavan tietosuojatyön

implementointi yrityksen arkeen sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden mukaisesti.

3.1 Kehittämistyön lähestymistapa

Opinnäytetyössä käytin tutkimuksellisen kehittämistyön -käytäntöä. Ojasalo, Ritalahti ja Moilanen (2014, 17) mukaan tutkimuksellinen kehittämistyö on käytännön ongelmien ratkaisuun tai käytäntöjen uudistamiseen tai niihin uuden tiedon luomiseen tarkoitettu tapa kehittää esimerkiksi organisaation toimintaa. Tutkimukselliseen kehittämistyöhön kuuluu yleisesti käytännön ongelmien ratkaisua ja uusien ideoiden, käytäntöjen, tuotteiden tai palvelujen tuottamista ja toteuttamista. Tieteellinen tutkimus ja tutkimuksellinen kehittämistyö eroaa toiminnan päämäärissä; tieteellinen tutkimus pyrkii tuottamaan ilmiöstä uuttaa teoriaa ja tutkimuksellisessa kehittämistyössä pyritään saada aikaan myös käytännön parannuksia tai uusia ratkaisuja. Kuviossa 10 selvennetään tutkimuksellisen kehittämisen sijoittumista tutkimuksen ja kehittämisen kentällä (Kuvio 9). (Ojasalo, Ritalahti & Moilanen 2014, 17.)

Tutkimuksellisen kehittämistyön toteuttamiseksi tulee valita sopiva lähestymistapa työlle. Lähestymistavan valinta kehittämistyössä vastaa lähinnä tutkimusstrategian valintaa tieteellisessä tutkimuksessa. Case -study, eli tapaustutkimus on sopiva keino, kun halutaan selvittää läpi luotaavasti yksittäisen kohteen toimintaa. Case -study on tutkimusstrategia, joka painottaa ennen kaikkea suuren tietomäärän hankkimista pienestä otannasta, entä kuin pienen määrän tietoa suuresta otannasta. Ideana on siis kohdistaa resursseja tarkoin valittuun kohteeseen. (Ojasalo, Ritalahti & Moilanen 2009, 52.)

Kuvio 9 Tutkimuksellinen kehittäminen (Ojasalo, Ritalahti & Moilanen 2009).

3.2 Menetelmät ja aineiston analyysi

Kohdeyrityksen nykytilan kartoitukselle ajattelin parhaan keinon olevan ensiksi vapaamuotoinen keskustelu yrityksen johdon kanssa tavoitteena saada yhteinen käsitys ilmiöstä. Liiketoiminnan riski, oli se sitten vaatimustenmukaisuudesta, tai muusta syystä aiheutuva, on aina yrityksen itse otettava, minimoitava tai poistettava. Sen vuoksi koin tärkeäksi jalostaa

tietosuojan jalkauttamista kertomalla yritykselle tietosuoja-asetuksen vaatimustenmukaisuudesta, sekä todellisista liiketoiminnallisista riskeistä siihen liittyen.

3.2.1 Workshop

Ensimmäisenä menetelmänä työssä, teoriaosuuden jälkeisessä nykytila-arviossa käytin workshop -menetelmää. Aallon (2015) mukaan workshop perustuu ryhmäideointiin, jos esimerkiksi halutaan kehittää uusia konsepteja. Monialaisen workshop-työskentelyn tavoitteena on erilaisten ajatusten ja ideoiden kehittäminen saattamalla ne muotoon, jossa niitä on helpompi käsitellä, tai niiden avulla halutaan luoda lisäideoita. Kirjoittaja lähestyy workshopin tekemistä viiden estävän tekijän kautta, jossa ideoinnissa voi tapahtua yksittäisen ja vahvan jäsenen ideoiden suosimista tai keskustelu on liian rajoittunutta; liikaa ohjattu toiminta rajoittaa ideoiden luomista. (Aalto 2015.) Toisaalta tässä on hyvä muistaa aikaresurssi. Aikaa ei aina ole, ja ideoinnin kohteen luonne voi olla sellainen, jossa ei ole vara joustaa rajatusta aiheesta.

Aalto (2015) varoittelee lisäksi liian rajoittuneeseen keskusteluunkin liittyvän itsesensuurin esiintymistä; ympäristön tulee olla avoin kaikenlaisille ideoille, toki aiheen sisällä pysytellen, josta tullaan ehkä tärkeimpänä pitämääni kirjoittajan mainitsemaan arvoon workshopeissa: Teeman epäselvyys ennen workshopia. Jos aihe on osalle osallistuvista henkilöistä liian abstrakti tai epäselvä, osallistujat eivät tällöin kykene toimimaan tilanteessa luonnollisesti, tuoden sen kautta hyviä ideoita esille. Kirjoittaja suositteleekin selkeyttämään, mitä workshopilla halutaan saada aikaan, sekä mihin ja kenen hyödyksi tuloksia käytetään. (Aalto 2015.)

Brainstorming, eli aivoriihi -menetelmä vastaa hyvin paljon workshopin tavoitteita. Alex Osbornin vuonna 1953 kirjoitetussa kirjassa Applied Imagination: Principles and Procedures of Creative Thinking, Osborne loi seuraavan ikonisen lauseen: “It is easier to tone down a wild idea than to think up a new one”. Tällä Osborne tarkoittaa sitä, että on helpompaa kesyttää villi-idea, kuin keksiä uusi; alussa hurjalta kuulostava idea voi olla tärkeä jonkin ratkaisun, idean tai konseptin kannalta. Ideoita voidaan aina jalostaa jälkikäteen ilmiöön sopivammaksi, oli Osbornen pääajatus.

Näillä ajatuksilla tietosuojatyön aloittamiseksi, kohdeyrityksessä pidettiin kaksi workshopia, joiden tavoitteena oli löytää yhteinen maaperä vaikuttavan tietosuojatyön ja yrityksen arkirealiteettien väliltä. Palaverit pidettiin brainstorming-workshop tyyppisesti, eli tavoitteena oli Osbornin aivoriihen ja Aallon (2015) esittelemän workshopin käyttäminen, sekä sen yleisimpien sudenkuoppien väistely. Käytännössä se tarkoitti molemmin puolista kunnioitusta toisen tietämystä kohtaan; minulla ei ollut täydellistä tietoa yrityksen arkirealiteeteista, eikä yrityksellä tietosuoja-asetuksen vaatimustenmukaisuudesta. Konsensuksen löytämiseksi oli tarpeen soveltaa edellä mainittuja menetelmiä. Workshopin osallistujiin kuului minun lisäksi

yrityksen johtoryhmää. Osallistujien valitseminen tapahtui kohdeyrityksen yhteyshenkilön, eli tässä tapauksessa yrityksen toimitusjohtajan toimesta.

3.2.2 Systemaattinen kirjallisuuskatsaus

Toisena menetelmänä työssä käytetään systemaattista kirjallisuuskatsausta. Kirjallisuuskatsauksen ajatellaan perinteisesti olevan tutkimusta tutkimuksesta, ja toimii näin ollen myös pohjana uudelle tutkimukselle (Salminen 2011, 1). Systemaattisesta kirjallisuuskatsauksesta puhutaan silloin, kun kiinnitetään huomiota käytettyjen lähteiden keskinäiseen yhteyteen ja tekniikkaan, jolla siteeratut tulokset on hankittu; sillä tiivistetään aihepiirin aiempien tutkimusten olennaista sisältöä. (Salminen 2011, 9.) Systemaattinen kirjallisuuskatsausta pidetään perinteisesti luotettavana, ennen kaikkea järjestelmällisesti toteutettuna. Kirjallisuuskatsauksiin liittyy kuitenkin monesti myös ihmisten taipumuksista ja ennakko-oletuksista johtuvia vinoumia, joiden seurauksena voi tapahtua esimerkiksi lähdemateriaalin valinnan puolueellisuutta, tai julkaisuharhasta johtuvaa positiivisävytteisten ja ennalta odotettujen tutkimusten julkaisua negatiivissävytteisten ja ennalta odottamattomien tulosten sijaan. (Almeida & Goulart 2017.)

Kirjallisuuskatsaus pohjautui tässä työssä kolmeen eri lähteeseen, joiden perusteella kykenin luomaan raamit luotettavan katsauksen perustaksi. Ensimmäinen lähde on Ari Salmisen ”johdanto kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin”, jossa käydään yleisesti läpi eri kirjallisuuskatsaustyyppejä, sekä itse katsauksen tekemisen perimmäistä kysymystä. Salmisen (2011) tarkoituksena on kuvata raportissaan kirjallisuuskatsausta eri metodologisin perustein ja esimerkein hallintotieteellisessä tutkimuksessa. (Salminen 2011, 1.)

Toisessa lähteessä ”Procedures for Performing Systematic Reviews” kirjoittaja Barbara Kitchenham (2004 ,1) ehdottaa suuntaviivoja systemaattiselle katsaukselle ohjelmistoinsinöörialalla suunnattuna tutkijoille, mukaan luettuna väitöstyöntekijät. Suuntaviivat on johdettu kolmen eri lääketieteentutkijoille suunnattujen kirjallisuuskatsausoppaan annista vastaamaan tutkijoiden tarpeita ohjelmistoalalla. Kitchenhamin (2004, 1) johtavana ajatuksena raportissa on kolmivaiheinen kirjallisuuskatsausmalli, joka koostuu katsauksen suunnittelusta, suorittamisesta ja raportoinnista. (Kitchenham 2004, 1.)

Kolmannessa, ja viimeisessä lähteessä Watsonin ja Websterin (2002) vieraskynäkirjoituksessa MIS Quarterly -akateemiselle julkaisulle kirjoittajat pohtivat systemaattisen kirjallisuuskatsauksen käyttöä yleisesti, ja erityisesti osana tietojärjestelmätieteiden tiedon akkumulaation, eli kerääntymisen/kasaantumisen avustamista oppaan muodossa. Raportin tiedonannin arvon huomasin verratessani omaa, sekä Watsonin ja Websterin (2002, 14) tarkoitusta pohjimmiltaan suorittaa kirjallisuuskatsaus; olimme lähes yhtä mieltä siitä, että omien aikojemme nuori ja poikkitieteellinen ala (Tietojenkäsittely vs. Tietosuoja) voi kehittyä, kun aiempaa tutkimusta kerätään kokoon systemaattisesti. (Watson & Webster 2002, 14.) Sen lisäksi, että

molemmat alat ovat poikkitieteellisiä, ovat ne myös lähellä toisiaan itse aloina. Tietosuojaan liittyy ennen kaikkea esimerkiksi oikeustiede, tietojenkäsittelytiede, sekä tietyssä mielessä myös käyttäytymistiede, jos halutaan esimerkiksi tutkia ihmisten käyttäytymistä tietyssä ilmiökentässä, kuten tämän työn tapauksessa yrityksessä. Listaa voisi vielä jatkaa tämän opinnäytetyön viitekehyksen mukaisesti myös yritysturvallisuudella, johon liittyvät jatkuvuuden, vaatimustenmukaisuuden, sekä turvallisuuden ja riskienhallinnan teemat luovat tietosuojasta hyvin monipuolisen ilmiön sen saadessa useita tieteenaloja osakseen.

Salminen (2011, 3) perustelee kirjallisuuskatsauksen toimivuutta seuraavilla kohdilla: Sillä voidaan kehittää jo olemassa olevaa teoriaa, sekä rakentaa uutta teoriaa, sillä voidaan arvioida teoriaa ja rakentaa kokonaiskuva aihealueesta, lisäksi sillä pyritään tunnistamaan ongelmia, sekä kyetään jonkin tietyn teorian historiallisen kehityksen kuvaamiseen. Lisäksi kirjoittaja mainitsee kirjallisuuskatsauksessa olevan käytössä näyttöön perustuvaa, parhaimman sen hetkisen tiedon hankkimiseen tarkoitettu työkalu, jossa on paljon samankaltaisuutta ’best practices’ ja ’benchmarking’ -tekniikoihin. Tiedon määrän nopea kasvu luo tarpeen saada tietoa nopeasti avuksi päätöksentekoon, ja näin ollen systemaattiselle kirjallisuuskatsaukselle löytyy hyvä käyttöperuste. (Salminen 2011, 10.)

Kitchenham (2004, 6) mainitsee artikkelissaan yleisiä syitä systemaattisen kirjallisuuskatsauksen tekemiseen, joita ovat aiemman tiedon yhteenveto, aukkojen tunnistaminen aiemmassa tutkimuksessa lisätutkimuksen tekemisen tueksi, sekä lisätutkimuksille valmiin teoreettisen viitekehyksen- tai taustan tuottaminen (Kitchenham 2004, 6). Yhtenäisiä keskenään julkaisujen kirjallisuuskatsauksen hyödyistä ovat pohdintani perusteella aiemman tiedon yhteenveto (Kitchenham 2004, 6) ja historiallisen kehityksen kuvaaminen (Salminen 2011, 3). Kummatkin kirjoittajat ovat yhtä mieltä siitä, että kirjallisuuskatsaus on hyvä tapa kuvata menneitä kehityskulkuja jonkin tietyn aiheen piirissä. Lisäksi Kitchenham (2004, 6) ja Salminen (2011, 3) ovat yhtä mieltä oman käsitykseni mukaan myös aukkojen tunnistamisesta aiemmassa tutkimuksessa; Salminen kirjoittaa kirjallisuuskatsauksella tunnistettavan ongelmia aiemmassa teoriassa ja Kitchenham näkee asian aukkojen tunnistamisena (identifying gaps). Varsinaisesti Salminen (2001,6) ei määrittele, mitä ongelmien tunnistaminen teoriassa on, tai onko Kitchenhamin (2004, 6) mukaan aukot ongelmia. Olettaisin aukkojen tunnistamisessa ja ongelmien tunnistamisessa olevan osittain ainakin sama tarkoitusperä.

Watsonin ja Websterin (2002) vieraskynäkirjoituksessa “Analyzing The Past To Prepare For The Future: Writing A Literature Review” kirjallisuuskatsauksen idea on tiivistetty jo artikkelin otsikossa: Menneisyyden analysointi auttaa valmistautumaan tulevaisuuteen. Artikkelin otsikko on mielestäni linjassa erityisesti Salmisen (2011, 3) teorian historiallisen kehityskulun ymmärtämisen kanssa, ja näin osittain myös Kitchenhamin (2004, 6) aiemman tiedon yhteenvedon kanssa, historiallisen kehityskulun kuvaamista sekin. (Kitchenham 2004, 6; Salminen 2011, 3; Watson & Webster 2002.)

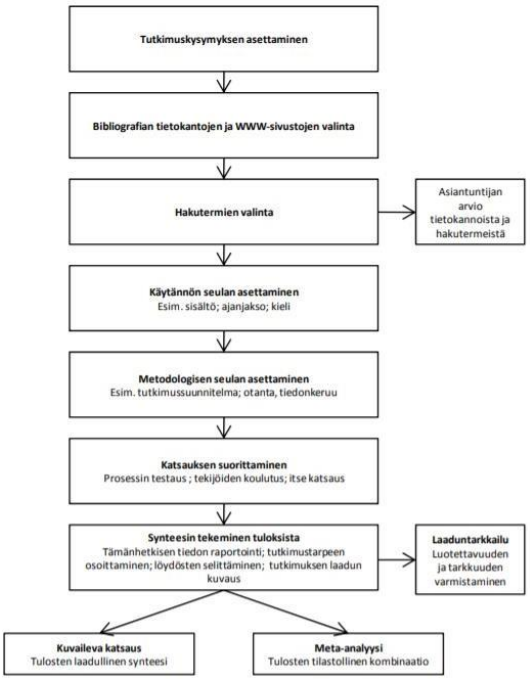
Watson ja Webster (2002, 13) pitävät relevantin kirjallisuuden hankkimista olennaisena osana kaikkia akateemisia projekteja. Kirjoittajien mukaan tehokas katsaus luo vahvan perustan kehittyvälle tiedolle fasilitoimalla teorian kehittymistä, sulkemalla pois alueet, joista löytyy jo tarpeeksi tietoa, sekä paljastamalla ne paikat, mistä ei tietoa ole tarpeeksi löydettävissä. (Watson & Webster 2002, 13.) Näin ne luovat Salmisen (2011, 9) ja Kitchenhamin (2004, 6) perustelujen tavoin puitteet lisätutkimukselle, sekä mahdollisuuden sijoittaa oma tuleva tutkimus verrokkeihinsa nähden tieteen kentällä (Kitchenham 2004, 6; Salminen 2011, 3; Watson & Webster 2002).

Tämä työ on määritelty olevan tutkimuksellinen kehittämistyö, joten sillä lähtökohdalla ei uuden tiedon luominen ole välttämätöntä; keskittyminen on enemminkin kehittämisessä, kuin uuden tiedon luomisessa. Käytännössä kuitenkin uutta tietoa luodaan, kun tehdään tapaustutkimukselle tyypillistä yhden tarkkaan määritellyn ilmiön kehittämistä. Kysymys on sitten vain enää siitä, voidaanko tätä työtä toistaa, eli esimerkiksi soveltuuko työn tuottama tieto muihin pk-yrityksiin, ja jos soveltuu, kuinka kauan? Aiheena tuoreen, sekä alati muuttuvan tietosuojakentän jollekin alueelle tehty kirjallisuuskatsaus voi olla osittain epävalidi lyhyenkin ajan päästä kirjallisuuskatsauksen tekemisestä. Eritysesti sen vuoksi olisi hyvä tunnistaa muuttujia, jotka ovat herkkiä esimerkiksi sääntelyn tarkennusten vuoksi. Tästä esimerkkinä on Schrems II -ratkaisu, jolla muutettiin rekisterinpitäjän kannalta merkittävästi tietojen siirron oikeusperustetta; yhdellä ratkaisulla tehtiin monen liiketoiminnan harjoittamisesta laitonta (Luku 2.6).

Tässä työssä kirjallisuuskatsaus määritellään, mukaillen Watsonia ja Websteriä (2002, 13), Salmista (2011,3) ja Kitchenhamia (2004, 6), tarkoittavan menetelmätapaa, jonka avulla pyritään ennen kaikkea saamaan käsitys aiemmasta tutkimuksesta, rakentamaan niiden tämän kehittämistyön kannalta tärkeimmistä osista kokonaiskuva, sekä mahdollisesti tunnistamaan sellaisia aukkoja aiemmassa tutkimuksessa, joiden perusteella voidaan tehdä lisätutkimusta. Kirjallisuuskatsauksen luomaa viitekehystä voidaan käyttää tulevaisuuden lisätutkimuksessa koskien pk-yrityksiä ja tietosuojaa, sekä siihen liittyvää vaatimustenmukaisuutta. (Kitchenham 2004, 6; Salminen 2011, 3; Watson & Webster 2002, 13.) Uuden teorian luominen, ja sen käyttäminen tulevaisuudessa uusissa tutkimuksissa voi olla liikaa vaadittu AMK-tason opinnäytetyöltä.

Itse työstämisvaiheeseen Watson ja Webster (2002), Kitchenham (2004) ja Salminen (2011) tarjoaa hyvin erilaisia lähestymistapoja, kun puhutaan konkreettisista toimista tehdä systemaattinen kirjallisuuskatsaus. Kitchenham (2004, 3) näkee useita erilaisia olemassa olevia suuntaviivoja, joilla systemaattista kirjallisuuskatsausta voisi lähteä rakentamaan. Artikkelissa kirjoittaja kuitenkin mainitsee kolme pääkohtaa, jolla kirjallisuuskatsausta voisi lähteä suorittamaan: 1. Katsauksen suunnittelu, 2. Katsauksen suorittaminen, ja 3. Katsauksen raportointi. Kolme kohtaa on jaoteltu myös alakohtiin, joissa otetaan tarkemmin kantaa kunkin

kohdan sisältöön. (Kitchenham 2004, 3.) Salminen (2001, 10) ehdottaa systemaattisessa kirjallisuuskatsauksessa käytettävän suoraviivaista Finkin-mallia, jossa kirjallisuuskatsaus tehdään seitsenvaiheisen jaottelun avulla (kuvio 10) (Salminen 2001, 10). Watson ja Webster (2002) eivät tarjoa selkeää viitekehystä Salmisen (2011, 10) ehdottaman Finkin-taulukon tai Kitchenhamin (2004, 3) konkreettisten, tekstissä auki kirjoitettujen kohtien tavoin, vaan he muun muassa painottavat enemmän tiedonhaun tutkimuksellisesta arvoa painottamalla esimerkiksi vertaisarviointia, sekä tiedon hankkimista suoraan lähteiden julkaisijoilta itseltään. (Watson & Webster 2002,14.) Vertaisapua toisaalta tarjoaa myös Kitchenham (2004, 7–8) hänen ehdottaessaan pyytää apua kirjastonhoitajilta ja alan ammattilaisilta, erityisesti hakustrategiaa laatiessa (Kitchenham 2004, 7-8).



Kuvio 10 Kirjallisuuskatsaus vaiheittain Finkin (2005: 54) mallia mukaillen (Salminen 2011, 11).

Kaikki edellä mainitut tavat palvelevat varmasti hyvin systemaattisen kirjallisuuskatsauksen tekemistä, huolimatta akateemisesta tasosta, jolla tutkimus suoritetaan. Salmisen (2011, 11) esittämä malli (kuvio 10) palvelee todennäköisimmin kirjallisuuskatsauksiin vähän

perehtynyttä, ja näin ollen tarjoaa hyvin selkeän viitekehyksen katsauksen suorittamiseen. Watsonin ja Websterin (2002), sekä Kitchenhamin (2004) ohjeet kirjallisuuskatsauksen tekemiseen kannustaa enemmän tutkimuksellisuuteen, toisaalta onhan nämä kaksi vieraskielistä artikkelia keskittynyt täysin systemaattisen kirjallisuuskatsauksen tekemiseen, kun taas Salminen (2011) kirjoittaa yleisemmin kaikenlaisista kirjallisuuskatsauksista; systemaattiselle kirjallisuuskatsaukselle löytyi hänen artikkelistaan tilaa 2 sivua, Kitchenhamin (2004) käsittelee 33 sivua nimenomaan systemaattista kirjallisuuskatsausta, Watson ja Webster (2002) puolestaan 11 sivua. Näkisin näistä kolmesta Kitchenhamin (2004) tarjoavan parhaimman konkreettisen viitekehyksen kirjallisuuskatsauksen tekemiselle kolmella auki kirjoitetulla kohdallaan, toki Finkin-malli (kuvio 10) ja Watsonin ja Websterin (2002, 16-17) esittelemä konseptilähtöinen katsausmalli ovat lisäksi toimivia viitekehyksiä katsaukselle. (Watson & Webster 2002, 16–17.) Finkin-mallin tarjotessa ylivoimaisesti selkeimmän viitekehyksen, tavoitteeni oli sen innoittamana käydä mallia läpi, ylhäältä alas, ja yrittää löytää Kitchenhamin (2004) sekä Watsonin ja Websterin (2002) julkaisuista kutakin kohtaa parhaiten vastaavat perusteet mallin kohtien toimintojen suorittamiselle.

Finkin -mallin mukaan ensimmäinen kohta on tutkimuskysymysten asettaminen (Kuvio 10), joka on Kitchenhamin (2004, 5) protokollan mukaan kaikista tärkein vaihe kirjallisuuskatsauksen vaiheista. Watson ja Webster (2002, 16) ehdottavat lähinnä työn tarkkaa rajausta sisältäen kohtia ilmiön tasosta välillä globaali – yksilö, ajallinen ja asiayhteydellinen rajoitus, katsauksen tarkoitus sekä implisiittiset arvot, kirjoittajien ottamatta kuitenkaan kantaa tutkimuskysymyksiin. Systemaattisen kirjallisuuskatsauksen tavoitteena tässä työssä oli löytää kohdeyritykselle sopivia toimenpiteitä, joilla noudatetaan tietosuoja-asetuksen vaatimustenmukaisuutta, mitkä toimenpiteistä ovat riittäviä kohdeyrityksen kannalta, sekä miten yritys voisi jatkossa varmistaa tietosuoja-asetuksen vaatimustenmukaisuus.

Relevantteja lähteitä etsiessä tulee Finkin -mallin toisen kohdan mukaan valita Bibliografian tietokannat ja WWW-sivustot (Salminen 2011, 11). Watson ja Webster (2002, 16) mainitsevat tietokannoista tuloksia etsiessä laadukkaiden lähteiden etsimisen esimerkiksi siteerauksien määrän perusteella, sekä mahdollisesti monialaisten tutkimusten etsimistä eri näkökulmien löytämiseksi (Watson & Webster 2002, 16). Näkemykseni mukaan lähdeviittauksien määrä ei kuitenkaan kerro tehdyn kirjallisuuskatsauksen perusteella lähteen luotettavuudesta. Jotkin tutkimukset voivat olla useita vuosia työstettyjä, ja näin ollen ne eivät ole ehkä kerenneet saamaan huomiota akateemisella kentällä viittausten muodossa. Kitchenham (2004, 7–8) opastaa tekemään ennakkohakuja mahdollisista aiemmista ilmiön kirjallisuuskatsauksista sekä potentiaalisten tutkimusten määrästä erilaisilla hakusanoilla käyttämällä synonyymeja, lyhenteitä ja vaihtoehtoisia kirjoitusasuja. (Kitchenham 2004, 7–8.) Salminen (2011, 10) opastaa käyttämään sanoja ja fraaseja, joiden perusteella löydetyt tutkimukset tulisivat vastata tutkimuskysymystä (Salminen 2011, 10).

Johdin tutkimuskysymyksistä muutamia hakusanoja, sekä synonyymit, että englanninkieliset vastineet johdetuille sanoille. Sanat ovat esitelty taulukoissa 1 (Taulukko 1). Synonyymeja sanoille hain Googlesta esimerkiksi hakusanoilla ”Pk-yritys synonyymi”, ja ”SME synonym”. Käytin lisäksi myös ”hakusana + lyhenne” suomenkielisten- ja ”hakusana + acronym” englanninkielisten hakusanojen kohdalla. Thesaurus.com toimi hyvin englanninkielisten hakusanojen kohdalla, synonyymit.fi suomenkielisten.

Tutkimuskysymykset jaettuna osiin	Hakusanat
Yleinen tietosuoja-asetus	1. GDPR 2. General Data Protection 3. Tietosuoja-asetus
Tietosuoja-asetuksen mukainen osoitusvelvollisuus	1. GDPR accountability principle 2. GDPR compliance
PK-yritys	1. SME 2. Small and medium-sized enterprise 3. Small business 4. Micro business 5. Micro enterprise 6. Pieni yritys 7. Keskisuuri yritys
Riittävyys	1. Adequacy 2. Sufficient
Toimi	1. Toimenpide 2. Procedure 3. Step 4. Action 5. Implementing
Noudattavuus jatkossa	1. Ensuring GDPR compliance in future 2. GDPR compliance continuity 3. Tietosuoja-asetuksen vaatimustenmukaisuuden jatkuvuus

Taulukko 1 Tutkimuskysymykset jaettuna osiin

Määritin seuraavaksi kuvion 12 mukaisen käytännön seulan, jossa määritellään hyväksyttävän muun muassa sisältö, ajanjakso ja kieli/kielet (Kuvio 11). Kitchenham (2004, 9–10) kirjoittaa tutkimusten valintakriteereistä, joilla viitataan Salmisen (2011, 11) käytännön seulaan. Kitchenhamin (2004, 9) mukaan kriteereillä halutaan tunnistaa sellainen tutkimus, jossa tarjotaan suoraa näyttöä tutkimuskysymykseen. Lähteiden hyväksymis- ja hylkäämis-, jäljempänä inkluusio- ja ekskluusiokriteerit tulisivat näin ollen perustua täysin tutkimuskysymyksiin ja seulaa tulisi sen vuoksi testata luotettavuuden lisäämiseksi. (Kitchenham 2004, 9.) Watson ja Webster (2002, 15–16) ehdottavat Kitchenhamin 2004, 9) tavoin laajaa otantaa tutkimusten valitsemiseksi (Watson & Webster 2002, 15–16).

Määrittelin käytännön seulaan tutkimuskysymyksiä palvelevia määrityksiä, joiden avulla kykenin saamaan riittävän hyvät lähtökohdat tulosten seulomiselle. Lisäksi toisin kuin Kitchenham (2004, 10) antaa olettaa systemaattisessa kirjallisuuskatsauksessa tehtävän (koko aineiston lukeminen), Määrittelin alustavasti lähteille tehtävän monivaiheisen seulan, jonka avustamana päätös ekskluusiosta, tai inkluusiosta tehtiin (Kitchenham 2004, 10). Ajanjaksoseulan perusteena on tietosuoja-asetuksen antamisen ajankohta, eli vuoden 2016 huhtikuun 14. päivä. Ennen kyseistä päivämäärää julkaistut lähteet sisältävät todennäköisesti vain spekulaatioita asetuksen sisällöstä, puhumattakaan sen soveltamisesta. Kieliseulaksi valikoitui suomi ja englanti oman kielitaitoni perusteella. Sähköisiä lähteitä suosin erityisesti niiden saatavuuden takia. Suurin epäilykseni systemaattisen kirjallisuuskatsauksen kriteerien täyttämiseksi yhtenä seulana lähteiden valintaan oli otsikon ja tiivistelmän lukeminen; systemaattisessa kirjallisuuskatsauksessa olisi suotavaa, että lopullisten lähteiden inkluusio/ekskluusio -kriteereissä koko aineisto tulisi käydä läpi (Kitchenham 2004, 10). Lopullinen inkluusio/ekskluusio löytyi kompromissin omaisesti otsikon ja tiivistelmän, sekä koko aineiston lukemisen välistä: Tarkistus sisälsi tiivistelmän, johdannon, tutkimuskysymysten asettelun ja johtopäätösten läpikäymisen.

Käytännön seula esitellään taulukossa 2 (Taulukko 2) ja kuviossa 13 (Kuvio 13), sekä tietokannat/arkistot taulukossa 3 (Taulukko 3).

Kirjallisuuden inkluusio	Kirjallisuuden ekskluusio
1. Lähde on julkaistu 14.4.2016-Nykyhetki välillä. 2. Kielenä suomi tai englanti 3. Tiedostomuotona sähköisesti saatavilla oleva materiaali 4. Aiheen tulee käsitellä Pk-yrityksiä koskevia tietosuoja-asetuksen vaatimuksia. 5. Lähteen otsikko ja tiivistelmä antavat olettaa siinä käsiteltävän tutkimuskysymyksiin liittyviä asioita	1. Lähde on julkaistu ennen vuotta 2016 2. Lähteen kielenä muu kuin suomi tai englanti 3. Alkuperäisiä dokumentteja ei ole olemassa 4. Lähde on ammattikorkeakoulutason, tai alemman akateemisen asteen opinnäytetyö, tai muu vastaava työ. 5. Suuri osa lähteessä käsiteltävistä aiheista koskee jotain muuta, kuin pk-yrityssektoria. 6. Lähteessä käsitellään sosiaali –ja terveysalan yritysten, julkishallinnon tai viranomaisten henkilötietojen käsittelyä. 7. Lähteen otsikko ja tiivistelmä eivät anna olettaa siinä käsiteltävän tutkimuskysymyksiin liittyviä asioita 8. Tutkimus ei koko tekstin perusteella kykene arvioni mukaan vastaamaan tutkimuskysymyksiin

Taulukko 2 Lähteiden inkluusio- ja ekskluusiokriteerit

Tietokanta/Arkisto	Kuvailu
Finna.fi	Tiedonhakupalvelu, joka tarjoaa vapaan pääsyn noin sadan suomalaisen arkiston, kirjaston ja museon digitaalisiin aineistoihin ja kokoelmaluetteloihin
Google Scholar	Google Scholar on yhdysvaltalaisen Googlen tuottama maksuton hakupalvelu, jonka avulla voi etsiä tieteellisiä julkaisuja.
Bielefeld Academic Search Engine (BASE)	Akateeminen hakukone, josta löytyy yli sata miljoona dokumenttia yli 6000 lähteestä.

Taulukko 3 Tietokannat

Seuraavaksi tein määritellyillä hakusanoilla taulukossa 3 esitellyistä tietokannoista (Taulukko 3). Haussa käytin apuna Suomilammin (2014, 17) kokoamaa aineistohankinnan työkaluja (kuvio 11), jossa tarkoituksena on haun tarkentaminen, rajaaminen ja hakutuloksien käsiteltävyys (Suomilammi 2014, 7).

Kuvio 11 Hakutermien ja – lausekkeiden soveltamisen työkalut (Suomilammi 2014, 17).

Kuvion 12 mallin mukaisesti suoritin seuraavaksi itse katsauksen, jonka perusteella kävin tutkimukset läpi kolmen eri seulan perusteella. Ensimmäinen seula poisti tutkimukset, jotka täsmäävät tutkimusten ekskluusiokriteerien (Taulukko 2; kuvio 12) kohtien 1–4 kanssa. Toisen seulan avulla kävin ensimmäisen seulan läpäisseiden tutkimusten tiivistelmät läpi, minkä perusteella tein ekskluusiopäätöksen taulukon 2 kohtien 5–7 perusteella (Taulukko 2; kuvio 12). Viimeisen seulan perusteella tehtiin ekskluusiopäätös taulukon 2, kohdan 8 perusteella (Taulukko 2; kuvio 12).

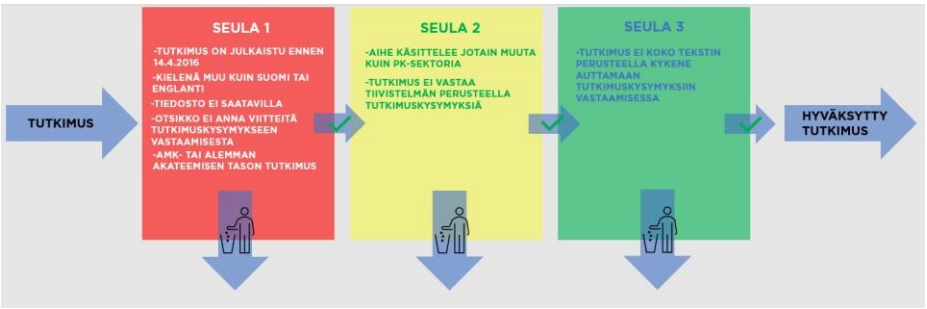
Ensimmäisen seulan läpi päässeet hakutulokset ovat listattuna taulukkoon 6 (Taulukko 6). Tässä vaiheessa huomasin myös käytännön ongelman; miten erottelen tutkimuskysymykset toisista? Kuinka monta tutkimusta otan kutakin tutkimuskysymystä koskien? Useampi, kuin yksi

tutkimuskysymys vaikutti työn alussa hyvältä tavalta toimia, mutta myöhemmin kirjallisuuskatsaus vaiheessa havaitsin sen tuovan haasteen tehdä päätös valittavien tutkimusten välillä. Ensimmäinen tutkimuskysymys ei varsinaisesti kerro, minkä tasoisia organisaatioita tutkimuskysymys koskee, joten sen perusteella jätin ensimmäisen tutkimuskysymyksen pois hakuprosessista; osittain ensimmäistä tutkimuskysymystä on avattu jo teoriaosuudessa. Toinen tutkimuskysymys on sen sijaan tarkemmin rajattu koskemaan vain pk-yrityksiä (kohdeyritys), ja niiden yleisen tietosuoja-asetuksen mukaista vaatimustenmukaisuutta. Kolmas tutkimuskysymys liittyy taas selkeimmin noudatettavuuden varmistamiseen tulevaisuudessa, minkä huomasin tarkoittavan laajemmin esimerkiksi kouluttamista ja ohjeistusta.

Lisäsin näiden tuumailujen perusteella tutkimuskysymyksiin vastaavien lähteiden kriteeriksi kokonaisvaltaisuuden, missä lähteissä tulisi löytyä 2. ja 3. tutkimuskysymystä vastaavat vastaukset. 1. tutkimuskysymykseen vastaamisen jätin tällä päätöksellä tiedonhaun ulkopuolelle tiedonhaun tehostamiseksi. Taulukossa 4 on listattuna hakusanat, joilla tietoa haettiin valituista tietokannoista (Taulukko 4). *-merkki hakusanojen joukossa ei tässä tapauksessa tarkoita katkaisumerkkiä, vaan sillä viitataan synonyymien ja lyhenteiden käyttöön kyseisen käsitteen kohdalla. Katkaisumerkkiä käytettiin joka tapauksessa useamassa haussa; esimerkiksi ”tietosuoja-asetus” korvattiin hakusanalla ”tietosuoja-asetu*” taivutettujen sanamuotojen löytämiseksi.

Suomenkieliset hakusanat	Englanninkieliset hakusanat
“Yleinen tietosuoja-asetus” AND “PK-yritys” **1**	“General Data Protection Regulation” AND “SME” **2**
“Yleinen tietosuoja-asetus” AND “Henkilöstö” AND “Koulutus” **3**	“General Data Protection Regulation” AND “Personnel” AND “training” **4**
“Yleinen tietosuoja-asetus” AND “Privacy by design” AND “PK-yritys” **5**	“General Data Protection Regulation” AND “SME” AND “Privacy by design” **6**
“Yleinen tietosuoja-asetus” AND “Toimepiteet” AND “PK-yritys” **7**	“General Data Protection Regulation” AND “SME” AND “Implementing” **8**
“Yleinen tietosuoja-asetus” AND “PK-yritys” AND “viitekehys” **9**	“General Data Protection Regulation” AND “SME” AND “Framework” **10**

Taulukko 4 Hakusuunnitelman mukaiset haut



Kuvio 12 Kolmivaiheinen tutkimusseula

Ensimmäisen seulan ohjaamana valitsin tutkimuksia seulan 1 perusteella aikavälillä 17. - 18.3.2020. Käytännössä kävin valittuja tietokantoja läpi (Scholar, Finna, Base). Hakuprosessin toteutin merkitsemällä ensiksi kaikki hakutulokset sulkuihin taulukkoon. Merkitsemisen jälkeen kävin hakutuloksia läpi seulan 1 mukaisesti. Periaatteessa seulan 1 sisällä oli prosessin aikana useampi seula, mutta ajattelin sen olevan turhan laaja taulukossa esille tuotavaksi; todellisuudessa seulan 1 sisällä tarkistin ensimmäiseksi otsikon ja kielen, jonka jälkeen tein päätöksen jatkaa selaamista. Toiseksi, jos havaitsin artikkelit otsikon/kielen kelvolliseksi, perehdyin tarkemmin linkin sisältöön, jossa tarkistin artikkelin saatavuuden; jos artikkeli ei ollut saatavilla, yritin vielä sen lisäksi tarkistaa, olisiko artikkelia jossain muussa tietokannassa saatavilla erityisesti, jos artikkelin otsikon perusteella kykenin olettamaan sen koskevan vahvasti tutkimuskysymyksiä. Seulan 1 toisessa kohdassa perehdyin lisäksi työn akateemiseen tasoon. Seulan 1 avulla toteutetut haut tuottivat 104 tulosta seulan 2-tason hakuvaiheeseen. Taulukossa 6 on listattuna kokonaishakutulokset (punainen), läpikäydyt tulokset (keltainen), ja hyväksytyt tulokset (vihreä) (Taulukko 6). Mitä pidemmälle selasin hakutuloksia, sitä vähemmän tulokset vastasivat itse hakusanoja, mikä näkyi tulosten osuvuusfrekvenssin pienenemisenä heti ensimmäiseltä sivulta lähtien. Aikaa 1. seulan hakuprosessiin meni kokonaisuudessaan noin 8 tuntia. Otsikon tasolla läpikäytyjä tutkimuksia oli n. 1900 kappaletta, missä alkoi jo eri hakusanoilla tulemaan vastaan samoja tutkimuksia.

Havaitsin myös muutamia useasti toistuvia käsitteitä hakuprosessin aikana, jonka perusteella päätin tehdä hakutuloksille teemoittelun, eli jaoin tutkimukset tiettyjen avainsanojen alle, mikä vastaa Watsonin ja Websterin (2002, 17) konseptointia. Konseptoinnin ideana on pyrkiä luomaan konseptimatriisi (Taulukko 5), jossa kuvataan eri artikkelien vaikuttavuutta eri konseptien/teemojen alalla.

Table 2. Concept Matrix					
Articles	**Concepts**				
	A	B	C	D	…
1		✖	✖		✖
2	✖	✖			
…			✖	✖	

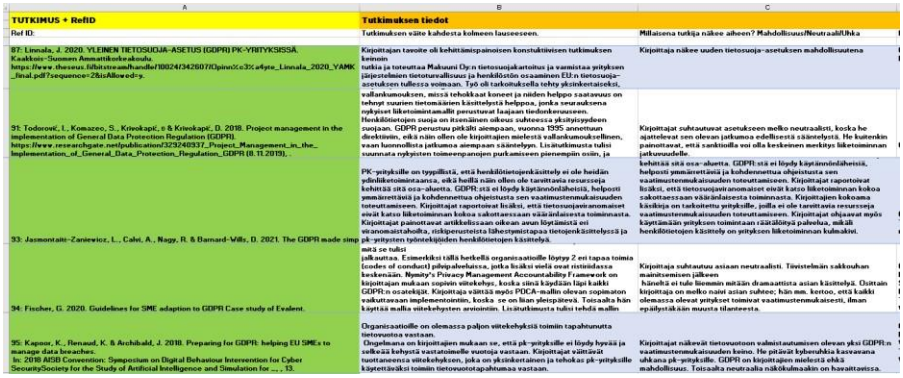
Taulukko 5 Konseptimatriisi (Watson & Webster 2002, 17).

SEULA 1			
#Koodi	Google Scholar	Finna	Base
1	2 (35/35)	2 (3/3)	1 (2/2)
2	59 (1350/2270)	0 (3/3)	5 (24/24)
3	0 (40/282)	0 (1/1)	0 (0/0)
4	0 (30/394)	0 (7/7)	0 (10/10)
5	1 (2/2)	0 (0/0)	0 (0/0)
6	0 (50/227)	0 (0/0)	0 (0/0)
7	0 (0/0)	0 (0/0)	0 (0/0)
8	7 (200/1050)	0 (0/0)	1 (2/2
9	0 (7/7)	0 (0/0)	0 (0/0)
10	3(200/1460)	0 (0/0)	0 (1/1)

Taulukko 6 Seulan 1 tasoinen haku

Kävin ensimmäisen seulan perusteella hyväksytyistä artikkeleista läpi yleisesti esiintyviä avainsanoja; avainsanojen esiintyvyyden perusteella kykenin luomaan kokonaiskuvaa siitä, millaisiin konteksteihin pk-yritykset ovat liitetty, kun puhutaan tietosuoja-asetuksen vaatimusten mukaisuudesta. Avainsanat auttoivat tärkeiden teemojen luomisessa, joihin osasin kiinnittää huomiota tutkimusten tarkemmassa läpikäymisessä. Loin konseptikartan Excel taulukkotyökalua apuna käyttäen, mikä teki suuren kokonaisuuden hallinnasta helpompaa. Kehittäessäni taulukkotyökalua teemojen esille tuomiseen, havaitsin sen toimivan ylipäätään hyvänä kirjallisuuskatsauksen hallintatyökaluna. Lopputulemana siirryin tekemään kirjallisuuskatsausta täysin Excel -ohjelmaan (kuvio 13), jossa käytin Thomsonin (2012b) luomaa kysymyspatteristoa. Blogin kirjoittaja, tohtoriopiskelijoiden ohjaaja, on laatinut kysymykset

kirjallisuuskatsauksen tekijöiden tueksi arvioimaan relevanttia kirjallisuutta. (Thomson 2012b.) Tärkeimpiä kirjoittajan ohjeita oli löytää läpikäytävän tutkimuksen väite, ja tiivistää se 2–3 lauseeseen; käytännössä siis tehtävänä oli käydä läpi artikkelin runko (otsikko, tiivistelmä, tutkimuskysymysten asettelu, johdanto ja johtopäätökset). Kysymykset auttoivat merkittävästi tutkimusartikkeleiden kriittisessä tarkastelussa. Tutkimuksen läpikäymisessä havaitsin lisäksi osaamisen kehittymistä tutkimusten arvioijana. Järjestelmällinen tarkistusprosessi alkaen työn rungon tarkistuksesta helpottui tutkimus tutkimukselta.



A	B	C
TUTKIMUS + RefID	**Tutkimuksen tiedot**	
Ref ID:	Tutkimuksen väite kahdesta kolmeen lauseeseen.	Millaisena tutkija näkee aiheen? Mahdollisuus/Neutraali/Uhka
87: Linnala, J. 2020. YLEINEN TIETOSUOJA-ASETUS (GDPR) PK-YRITYKSISSÄ. Kauhkois-Suomen Ammattikorkeakoulu. https://www.theseus.fi/bitstream/handle/10024/342607/Opinn%c3%a4yte_Linnala_2020_YAMK_final.pdf?sequence=2&isAllowed=y.	Kirjoittajan tavoite oli kehittämispainoisen konstruktiivisen tutkimuksen keinoin tutkia ja toteuttaa Maksuni Oy:n tietosuojakartoitus ja varmistaa yrityksen järjestelmien tietoturvallisuus ja henkilöstön osaaminen EU:n tietosuoja-asetuksen tullessa voimaan. Työ oli tarkoituksella tehty yksinkertaiseksi,	Kirjoittaja näkee uuden tietosuoja-asetuksen mahdollisuutena
91: Todorović, I., Komazec, S., Krivokapić, o & Krivokapić, D. 2018. Project management in the implementation of General Data Protection Regulation (GDPR). https://www.researchgate.net/publication/323240337_Project_Management_in_the_Implementation_of_General_Data_Protection_Regulation_GDPR (8.11.2019).	vallankumouksen, missä tehokkaat koneet ja niiden helppo saatavuus on tehnyt suurien tietomäärien käsittelystä helppoa, jonka seurauksena nykyiset liiketoimintamallit perustuvat laajaan tiedonkeruuseen. Henkilötietojen suoja on itsemäinen oikeus suhteessa yksityisyydeen suojaan. GDPR peruttuu pitkälti aiempaan, vuonna 1995 annettuun direktiiviin, eikä näin ollen ole kirjoittajien mielestä vallankumouksellinen, vaan luonnollista jatkumoa aiempaan sääntelyyn. Lisäuhkumusta tulisi suunnata nykyisten toimeenpanojen purkamiseen pienempiin osiin, ja	Kirjoittajat suhtautuvat asetukseen melko neutraalisti, koska he ajattelevat sen olevan jatkumoa edellisestä sääntelystä. He kuitenkin painottavat, että sanktioilla voi olla keskeinen merkitys liiketoiminnan jatkuvuudelle.
93: Jasmontaitė-Zaniewicz, L., Cahn, A., Nagy, R. & Barnard-Wills, D. 2021. The GDPR made simp	PK-yrityksille on tyypillistä, että henkilötietojenkäsittely ei ole heidän ydinliiketoimintaansa, eikä heillä näin ollen ole tarvittavia resursseja kehittää sitä osa-aluetta. GDPR:stä ei löydy käytännönläheisiä, helposti ymmärrettäviä ja kohdennettua ohjeistusta sen vaatimustenmukaisuuden toteuttamiseen. Kirjoittajat raportoivat lisäksi, että tietosuojavaivanomaiset eivät katso liiketoiminnan kokoa sakottaessaan vääränlaisesta toiminnasta. Kirjoittajien mukaan pk-yritysten työntekijöiden henkilötietojen käsittelyä.	kehittää sitä osa-aluetta. GDPR:stä ei löydy käytännönläheisiä, helposti ymmärrettäviä ja kohdennettua ohjeistusta sen vaatimustenmukaisuuden toteuttamiseen. Kirjoittajat raportoivat lisäksi, että tietosuojavaivanomaiset eivät katso liiketoiminnan kokoa sakottaessaan vääränlaisesta toiminnasta. Kirjoittajien kokoama käsitkija on tarkoitettu yrityksille, joilla ei ole tarvittavia resursseja vaatimustenmukaisuuden toteuttamiseen. Kirjoittajat ohjaavat myös käyttämään yrityksen toiminnan räätälöityä palveluja, mikäli henkilötietojen käsittely on yrityksen liiketoiminnan kulmakivi.
94: Fischer, G. 2020. Guidelines for SME adaption to GDPR Case study of Evalent.	mitä se tulisi jalkauttaa. Esimerkiksi tällä hetkellä organisaatioille löytyy 2 eri tapaa toimia (codes of conduct) pilvipalveluissa, jotka lisäksi sieltä ovat riittämässä keskenään. Nymity's Privacy Management Accountability Framework on kirjoittajien mukaan sopiein viitekehys, koska siinä käydään läpi kaikki GDPR:n osatekijät. Kirjoittaja väittää myös PDCA-mallin olevan sopimaton vaikuttavaan implementointiin, koska se on liian yleispätevä. Toisaalta hän käyttää mallia viitekehysten arvioinnin. Lisätutkimusta tulisi tehdä mallin	Kirjoittaja suhtautuu asiaan neutraalisti. Tiivistelmän sakkouhan mainitsemisen jälkeen hänelkä ei tule liiemmin mitään dramaattista asian käsittelyä. Osittain kirjoittaja on melko naivi asian suhtee; hän mm. kertoo, että kaikki olemassa olevat yritykset toimivat vaatimustenmukaisesti, ilman epäilystäkään muusta tilanteesta.
95: Kapnor, K., Renaud, K. & Archibald, J. 2018. Preparing for GDPR: helping EU SMEs to manage data breaches. In: 2018 AISB Convention: Symposium on Digital Behaviour Intervention for Cyber Security/Society for the Study of Artificial Intelligence and Simulation for ... 13.	Organisaatiolle on olemassa paljon viitekehyksiä toimiin tapahtunutta tietovuotoa vastaan. Ongelmana on kirjoittajien mukaan se, että pk-yrityksille ei löydy hyvää ja selkeää kehystä vastatoimille vuotoja vastaan. Kirjoittajat väittävät tuottaneensa viitekehyksen, joka on yksinkertainen ja tehokas pk-yrityksille käytettäväksi toimin tietovuotot tapahtumaa vastaan.	Kirjoittajat näkevät tietovuotoon valmistautumisen olevan yksi GDPR:n vaatimustenmukaisuuden keino. He pitävät kyberuhkia kasvavana uhkana pk-yrityksille. GDPR on kirjoittajien mielestä ehkä mahdollisuus. Toisaalta neutraalia näkökulmaakin on havaittavissa.

Kuvio 13 Systemaattinen kirjallisuuskatsaus taulukkotyökalua apuna käyttäen

Seulaan 2 jäi 42 tutkimusta, jotka lisääntyneen tutkimusten kriittisen tarkastelun osaamisen siivittämänä oli osittain myös helpompi pudottaa pois. Eri teemojen merkityksen vahvaksi tai heikoksi toteamisen jälkeen kykenin myös poistamaan otsikkotasolla useita tutkimuksia, joita olin ohi tarkan rajauksen valinnut. Hakukriteereistä alkoi erityisesti kevään mittaan tiukan aikataulun vuoksi korostumaan tutkimusten kokonaisvaltaisuus.

96 tutkimuksesta valitsin loppujen lopuksi 3. seulan avulla 5 tutkimusta, joilla pyrin vastaamaan 2. ja 3. tutkimuskysymykseen. Valituissa tutkimuksissa korostui monipuolisuus; tarkoituksena oli laittaa sellainen kirjallisuus keskustelemaan keskenään, joissa on monipuolisia ja hyvin perusteltuja näkökulmia aiheeseen liittyen.

Monipuolisuus tässä tapauksessa tarkoittaa monialaisuutta erilaisten näkökulmien esille tuomiseksi, kuten oikeustiedettä, organisaatiotutkimusta, tietotekniikkajohtamista, tietojärjestelmätiedettä sekä tietoturva-alaa. Eri alojen tutkimuksista nousee esille toisaalta aiheen monimutkaisuus, mutta toisaalta valtava potentiaali aiheen selkeyttämiselle ymmärrettävään muotoon. Ajattelen, että helposti omaksuttavat vaatimukset ovat avain niiden onnistumiselle. Lopulliset lähteet käsittivät artikkeleja oikeustieteen, tietoturvatutkimuksen, tieto- ja sähkötekniikan, teknologia osaamisen, johtamiskoulutuksen, ja organisaatiotieteen aloilta.

4 Tulokset

Systemaattisen kirjallisuuskatsauksen avulla saatujen tulosten mukaan suurimmat esteet vaatimustenmukaisuudelle ovat resurssien ja osaamisen puute (Hansen Jagrelius 2018, 51; Texeira, da Silva & Pereira 2019, 414; Brodin 2019, 262). Osa yrittäjistä kokevat erilaiset viitekehykset hyvin vaikeaselkosina, eivätkä ne näin ollen sopisi pk-yrityksen tietosuojan kehittämiseen. Jalkauttamisen onnistumisessa painotettiin projektijohtamista, missä organisaatiotutkijat korostivat monialaista lähestymistapaa kehittämistyössä (Todorović, Komazec, Krivokapić Da. & Krivokapić Do. 2018, 60).

Kaiken kaikkiaan kirjallisuuskatsauksessa tuli vahvasti esille resurssien ja tiedon puute, jolloin kansallisen viranomaisen tiedotus- ja ohjausvastuuta korostettiin useasti tietosuoja-asetuksessakin mainitun pk-yritysten ”erityisten tarpeiden” ja ”erityisen aseman” mukaisesti: Olisi koko EU:n kannalta hyvä löytää tasapaino liiketoiminnan harjoittamisen ja yksilön oikeuksien väliltä (Hansen Jagrelius 2018, 51). Toista ei voida korostaa liikaa, jotta toinen ei siitä kärsisi.

Kahden eri menetelmän avulla saaduista tuloksissa oli paljon yhteneväisyyksiä. Workshopin ja kirjallisuuskatsauksen tulosten perusteella esille nousivat ennen kaikkea pk-yritysten haaste toteuttaa yleisen tietosuoja-asetuksen vaatimustenmukaisuutta. Oman empirian perusteella kohdeyrityksessä suurin haaste oli ajan löytyminen tietosuojan kehittämiselle; taloudellisista resursseista ei niinkään ollut puutetta, vaan toteutunut ajan määrän löytyminen palavereille ei ollut omalta osaltani toivottua. Osittain ajanpuute johtunee myös siitä, että työn kehittämisosuus oli suunniteltu tehtävän vähemmän kiireisenä ajankohtana syksyllä, mutta opinnäytetyön aikataulun pidetessä kehittäminen ajoittui kutakuinkin sesongin alkuun, milloin yrityksellä ei ollut varaa panostaa kehittämiseen ajallisesti riittävän paljon. Toisaalta virhe saattoi olla myös viestinnällinen; parempi kommunikointi jalkauttamistyöstä olisi saattanut toimia paremmin, ja aikaa olisi tässä tapauksessa saattanut löytyä enemmän itse kehittämiselle.

Tutkimuskysymysten mukaan keskittyminen menetelmätyössä tuli olla toisen tutkimuskysymyksen mukaan tavoissa toteuttaa osoitusvelvollisuus, ja kolmannen tutkimuskysymyksen mukaan vaatimustenmukaisuuden ylläpitämisessä. Toisin kuin aiemmin mainitsin ensimmäisen tutkimuskysymyksen pois jättämisestä, tuli kirjallisuuskatsauksessa perehdyttyä lähes automaattisesti lisää myös siihen, mikä vahvisti tietoa eri tavoista, riittävien toteutustapojen jatkoksi. Kirjallisuuskatsauksessa koin haasteelliseksi pitää keskittymisen tutkimuskysymyksissä, mikä näkyi omalta osaltani liiallisessa keskittymisessä esteisiin tietosuoja-asetuksen vaatimustenmukaisuuden kehittämiselle. Haasteet ja esteet on hyvä tiedostaa, mutta kun tavoitteena on vaatimustenmukaisuus, niin silloin keskittyminen tulisi olla itse asian kehittämisessä, eikä tukehtumisessa hallinnollisen kuorman alla. Päätin keskittyä kirjallisuuskatsauksen raportoinnissa mahdollisuuksiin, haasteiden sijaan. Näkemykseni on, että jos esimerkiksi halutaan

tuotteistaa tietosuoja-asetuksen jalkauttamiseen keskittyvä palvelu, tulisi tällöin perustelujen yritysjohtajille olla pitkälti mahdollisuuksissa, vaatimustenmukaisuuden lisäksi.

4.1 Workshopin tulokset

Ensimmäisessä, 22.2.2021 pidetyssä, reilun tunnin mittaisessa workshopissa kävimme yrityksen toimitusjohtajan, sekä henkilöstöstä vastaavan henkilön kanssa läpi yleistä tietosuoja-asetusta, sekä sen vaikutuksesta yritykseen. Teemoina workshopissa oli vastuut, velvollisuudet, oikeudet ja kehittäminen. Tein ensimmäistä täysin aiheeseen liittyvää tapaamista varten kalvosulkeiset, missä olin silloisten kykyjeni mukaan listannut tietosuoja-asetuksen tarkoitusta, sekä sen vaikutuksia yritykseen. Kohdeyrityksen puolelta esitettiin aiheellisia kysymyksiä liittyen eri toimintoihin, joihin vastailin parhaan kykyni mukaan. Tapaamisessa sovittiin seuraavan workshopin ajankohta, sekä tehtävät kummallekin osapuolelle ennen seuraavaa palaveria; yrityksen tehtävänä oli käydä läpi henkilötietojen käsittelyprosesseja annettujen esimerkkien mukaisesti. Sain itse tehtäväksi kohdeyrityksen henkilötietojen käsittelyä vastaavan tietosuojaselosteen laatimisen, sekä workshopissa käytyjen Powerpoint-materiaalin lähettämisen yritykselle opetus- ja koulutusmateriaaliksi.

Toisessa, 3.3.2021 pidetyssä workshopissa paikalla oli koko yrityksen johtoryhmä. Tavoitteena tapaamisessa oli tietosuojakäytäntöjen suunnittelu, joiden perusteella yrityksen toimintaa lähdettiin kehittämään heti tapaamisen jälkeen. Toisessa palaverissa ongelmana oli ajanpuute: Kesäsesongin alku on yrityksen avainhenkilöille kiireistä aikaa, joten toiselle workshopille ei löytynyt heidän kalenteristaan kuin reilu 1 tunti. Yksi tunti oli riittämätön määrä vaikuttavalle jalkauttamiselle, etenkin kun en ollut hionut niin sanotusti hissipuhetta kuntoon. Ensimmäinen puolituntinen meni hieman jaaritellen niitä näitä tietosuoja-asetuksen yleismaailmallisista piirteistä; keskittyminen olisi alun alkaen pitänyt olla täysin vaatimustenmukaisuuden ja yrityksen rajapinnassa. Tästä jälkeenpäin ajatellen varoitteli Aalto (2015), mainitessaan selkeän teeman olemassaoloa ennen workshopia (Aalto 2015). Selkeän teeman puuttuessa kallista aikaa meni hukkaan. Parempi tapaamisen suunnittelu olisi varmasti auttanut asian esille tuomisessa, ja sen sisäistämisessä.

Loppujen lopuksi yritykselle tuli hyvin tietoon vaatimukset, joita uusi tietosuoja-asetus heille on asettanut. Tutkimuksellisen kehittämisen, ja osaltaan myös tapaustutkimuksen vaatimia konkreettisia osoitusvelvollisuuteen liittyviä tuotoksia olivat ainakin seuraavat kokonaisuudet: 1. Workshopit, eli toisin sanoen tietosuoja-asioista on puhuttu, ja puhutut asiat on dokumentoitu 2. Tietosuojaseloste 3. Henkilötietojen käsittelijöiden listaus 4. Tietojenkäsittelysopimusten (DPA-sopimus) laatiminen yrityksen henkilötietoja käsittelevien yritysten osalta.

Tunnistetut käsittelyprosessit liittyivät asiakassuhteisiin, potentiaalisten asiakkaiden, eli ”liidien” henkilötietojen käsittelyyn, rekrytointiin ja työntekijöiden henkilötietojen käsittelyyn eri yhteyksissä, esimerkiksi palkkahallinnon ja työterveyshuollon osalta. Arkaluontoiset

tiedot, joita yrityksessä käsitellään, liittyvät työntekijöiden terveystietojen, ja yrityksen kotisivuilla tapahtuvaan pisteytykseen, millä automattinen markkinointityökalu pisteyttää yrityksestä kiinnostuneiden henkilöiden liikkeitä kotisivuillaan. Profilointi on terveystietojen lisäksi vaikutustenarviointia vaativa käsittelytoimenpide, eli tietosuoja-asetuksen mukaisesti vaikutustenarviointia tulisi tehdä aina ennen uuden käsittelyn aloittamista, mikä yrityksen tapauksessa olisi vaatinut vaikutustenarvioinnin tekemistä heti tietosuoja-asetuksen voimaan astumisen jälkeen. Vaikutustenarvioinnissa tulee arvioida mahdollisia haitallisia seurauksia, joita rekisteröidylle voi käsittelyn seurauksena aiheutua.

Yritys siirtää rekisteröityjen (ml. Työntekijät, asiakkaat ja kotisivuilla vierailevat henkilöt) henkilötietoja Yhdysvaltoihin, mikä Schrems II -päätöksen jälkeisellä aikakaudella tarkoittaa vaativia juridisia toimenpiteitä siirtojen mahdollistamiseksi. Yrityksen käyttämä ”lead-scoring” -palvelu on paljon käytetty, edullinen ja toimiva markkinointityökalu -plugin heidän kotisivuillaan, joka pisteyttää kotisivulla vierailevan toimintaa. Kun sivustolla vieraileva jättää yhteydenottopyynnön lomakkeella, markkinointityökalun tekemän pisteytyksen avulla yritys tietää, missä kohden asiakas on menossa ”myyntiputkessa”. Myyntiputki tarkoittaa myyntikielessä prosessia, jossa tunnistetaan potentiaalisen asiakkaan sijoittuminen myyntiputken asteikolla 1. tietoisuus, 2. kiinnostus, 3. ostohalu ja viimeiseinä 4., toiminta, eli ostopäätös (Lead Forest 2019). Yrityksen käyttämän markkinointityökalun tavoitteena on selvittää ennen kaikkea asteikon toisen kohdan edistymistä; kuinka kiinnostunut potentiaalinen asiakas on yrityksen palveluista. Kiinnostusaste selviää evästeiden avulla, jotka seuraavat vierailijan toimintaa yrityksen kotisivulla; missä kotisivujen osassa vierailija viettää aikaa ja kuinka kauan?

Kohdeyrityksen toinen henkilötietojen siirtoa kolmanteen maahan, niin ikään Yhdysvaltoihin siirtävä tietoja siirtäviä palveluita ovat kaikki yhdysvaltalaiset alustat. Tärkein niistä on pilvipalvelu, missä saatetaan säilyttää hyvin kirjava joukko henkilötietoja vanhoista työntekijöistä työntekijäprospekteihin. Kaikki tiedot majailevat Googlen datakeskuksissa.

Kokonaisuudessaan yrityksen automatisoitu markkinointityökalu on tärkeä osa yrityksen liiketoiminnalle - yrityksen palveluista kiinnostuneet henkilöt saavat kohdennetun ratkaisun tarpeisiinsa, ja yritys kykenee kasvattamaan liikevaihtoaan tarjotessaan palveluita asiakkailleen. Uusi tietosuoja-asetus on hankaloittanut, ja tulee edelleen hankaloittamaan tällaista uusiin teknologioihin perustuvaa markkinointitoimintaa, millä voi olla negatiivisia seurauksia kannattavan liiketoiminnan harjoittamiseen. Toisaalta esimerkiksi monen tietosuoja-asetuksen markkinointivaikutus -tutkimusten mukaan vaikutukset saattavat olla liiketoiminnalle hyödyllisiä kasvaneen läpinäkyvyyden ja luottamuksen kautta.

Kun kyse on kotisivuista, on kyse kaikista näkyvimmästä osasta ulkopuoliselle maailmalle - kotisivut ovat yrityksen näyteikkuna, missä hyvin laadittujen tietosuojaselosteiden lisäksi tulisi olla asianmukainen evästekysely, missä vierailijalla tulisi olla yhtäläinen mahdollisuus joko

hyväksyä, tai hylätä muun muassa seurantaan perustuvat evästeet. Näkisin, että suurin kynnyskysymys liittyen tulevaisuuteen, ja tietosuoja-asetusta tarkentavaan e-privacy asetukseen yrityksen näkökulmasta tulee liittymään ns. evästebannereiden käyttöön; kuinka paljon yritykset tulevat häviämään taloudellisesti siinä, kun rekisteröityjen oikeuksia on vahvennettu markkinointityökalujen käytön yhteydessä. Kysymys markkinoinnin onnistumisesta tulevaisuudessa olisi mahdollisuus kattavalle tutkimukselle, jossa selvitetään tarkemmin sen todellisia yritysvaikutuksia,

Selkeästi kehittämättömiksi asioiksi jäivät vaikutustenarvioinnin, tietojen siirron kolmanteen maahan mahdollistavien toimien, sekä tietojen minimointiin liittyvät konkreettiset teot, joka oli itselle silloisilla tiedoilla haastava toteutettava. Tietojen minimointiin olen havainnut käytettävän ohjelmistoja, jotka osaavat automaattisesti luokitella esimerkiksi rakenteetonta tietoa, ja eri lähteiden mukaan rakenteeton, eli tieto, jota laitteet eivät osaa itse jäsennellä, ovat suuri ja alati kasvava tieto-omaisuuserä kaiken kokoisissa yrityksissä. Tietojen siirto kolmanteen maahan, toisin sanoen hyvin useasti Yhdysvaltoihin vaatii toimenpiteitä, jotka ovat tällä hetkellä monimutkaisia pk-yritysten kannalta. Vallitseva siirron mahdollistama menetelmä on SCC, eli Standard Contractual Clauses (Euroopan komissio 2021).

Tietosuoja-asetuksen teoriaan perustuneen yrityksen kehittämisen haastavin tekijä oli ajan puute, sekä toisena oma osaaminen. Merkittävin haaste omaan osaamisen liittyen oli tehdä yritykselle selväksi se, mikä on kaikista tärkeintä tietosuoja-asetuksessa. Vastaus ei ole yksinkertainen, ja se tekee täydellisestä vaatimustenmukaisuudesta haastavan toteutettava; toisaalta voidaan perustellusti kysyä, että täytyykö pk-yrityksen toiminta olla täysin vaatimustenmukaista, jos vastapainona on tärkeiden resurssien käyttö. Tämä sai minut pohtimaan, mikä on kohdeyrityksen tyyppisille pk-yrityksille kaikista tärkeintä ymmärtää tietosuoja-asetuksessa.

4.2 Kirjallisuuskatsauksen tulokset

Kirjallisuuskatsauksen tuloksissa halusin painottaa tutkimusartikkelien monialaisuutta. Ensimmäinen tutkimus on pääosin oikeustieteen maisterityö osittain myös tietojärjestelmätieteen näkökulmalla “The Specific Situation and Needs of SMEs and the GDPR – Taking the account of small enterprises and smaller data subjects (Hansen Jagrelius 2018). Hansen Jagreliuksen (2018) keskeinen väite tutkimuksessa tietosuojan riittävyyttä ja jatkuvuutta koskien on tietosuoja-asetuksen 13. resitaali, missä säädetään pk-yritysten "erityisen aseman ja "erityistarpeiden" huomioon ottamisesta. Kirjoittajan mukaan pk-yrityksiltä puuttuu henkilöstöresursseja, sekä useasti systemaattinen liiketoimintasuunnitelma, keskittymisen ollessa edellä mainittujen sijaan päivittäisessä liiketoiminnassa. Kirjoittaja kritisoi hallinointijärjestelmiä, sekä kalliita, yksittäiselle yritykselle räätälöityjä ratkaisuja. Kirjoittajan luomaa kysymyspatteristoa voidaan käyttää pohjana riskienarvioinnille liittyen käsittelyyn liittyviin

riskeihin. Kirjoittaja näkee pk-yritysten tarvitsevan oikeudellista varmuutta. Kehittämisen tulisi tapahtua myös rekisteröidyn oikeuksien kannalta järkevästi, sekä tietosuojan, että taloudellisen toimivuuden tasapaino tulisi säilyä. (Hansen Jagrelius 2018.)

Toinen tutkimus, Project Management In The Implementation Of General Data Protection Regulation (Gdpr), tuo kirjallisuuskatsaukseen organisaatiotieteen näkökulman. Tutkimuksessa korostetaan tietosuoja-asetuksen jalkauttamisen projetktinhallinnallista kokonaisuutta, missä projektissa käytettäisiin osaajia oikeustieteen alalta, tietoturvan- ja tekniikan alalta, sekä organisaatioympäristön tuntevia asiantuntijoita. (Todorović ym. 2018.) Todorovićin ym. (2018) ajatukset eivät ole linjassa Hansen Jagreliuksen (2018) ajatusten kanssa. Toinen kannattaa vahvaa räätälöityä ratkaisua, toinen vastustaa sitä. Tähän varmasti vaikuttaa eniten yrityksen koko, sekä käsittelyn luonne. Mitä korkeammat riskit käsittelyssä, sitä vaikuttavampi tulisi tietosuojaprojetkin olla.

Brodin (2019) tarjoaa esittelemällään viitekehyksellä hyvin eri yrityskokoihin skaalautuvaa ratkaisua tehdä vaikuttavaa tietosuojatyötä. Kirjoittaja esittelee tutkimusartikkelissaan kolmella case-yrityksellä testatun viitekehyksen, milloin kokoonpano voi vaihdella useista yrityksen jäsenistä ja asiantuntijoista hyvin pieneen kokoonpanoon. Vahvuus Brodinin viitekehyksessä on ennen kaikkea skaalautuvuudessa, sekä selkeässä toteutuskulussa. (Brodin 2019.) Vahvaa viitekehystä jalkauttamiseen tarjoaa lisäksi Fischer (2020) artikkelissaan ”Guidelines for SME adaption to GDPR Case study of Evalent”. Kirjoittajan artikkelin kirjallisuuskatsaus perustui parhaimman viitekehyksen löytämiseen, ja sen soveltamiseen kohdeyrityksessä. Löydetty viitekehys muokattiin kohdeyritykselle sopivaksi. Viitekehys on tätä nykyä Trust Arcin omistaman Nymityn laatima malli, jossa kirjoittajan mukaan tulee ilmi kaikki tietosuoja-asetuksen osat. Viitekehys väitetään olevan omiaan juuri osoitusvelvollisuuden toteuttamiseen. (Fischer 2020.) Kun verrataan Fischerin ja Brodinin esittelemiä viitekehyksiä, on Fischerin viitekehys ehdottomasti kattavampi, mutta paljon monimutkaisempi toteutettava etenkin yrityksessä, jossa henkilötietojen käsittely ei ole yrityksen päätoiminen liiketoimintamalli. Brodin (2019) tarjoaa näin ollen selkeimmän mallin tarpeeksi kattavan tietosuojaprojektin toteuttamiseksi.

Viimeisinä nostan esille kokonaisvaltaisen, Suomessa tehdyn tietosuojaprojektin, jossa on ansiokkaasti otettu esille tämänkin työn mukaisesti yritysturvallisuuden. Tutkimustyössä ”Yleinen tietosuoja-asetus (Gdpr) pk-yrityksissä”, kirjoittaja painottaa laajasti tietosuojan lisäksi tieto- ja kyberturvaa onnistuneen tietosuojatyön edellytyksenä. Henkilöstön tietosuoja- ja tietoturvakoulutus ja järjestelmien suojaaminen, sekä fyysisen- että digitaalisen tietoturvan keinoin ovat edellytyksiä tietosuojan onnistumiselle. (Linnala 2020.) Linnalan (2020) työstä voidaan löytää hyviä käytäntöjä muun muassa tieto- ja kyberturvaa koskien, mistä näin ollen voidaan päätellä, että tieto- ja kyberturva tulee olla vahvasti mukana tietosuojatyössä.

4.3 Yhteenveto

Nostin aiemmin työssä esille viitekehyksen toimimattomuuden erityisesti niiden monimutkaisuuden vuoksi. Yrittäjät ovat kokeneet, että ne ovat liian vaikeaselkoisia toteuttaa yrityksessä. Näkisin kuitenkin, että viitekehykset ovat oikeasti toimivia, mutta silloin viitekehyksen jalkauttamisessa tulisi olla mukana ainakin yksi tietosuojaa ymmärtävä henkilö. Kohdeyrityksen tapauksessa olisi varmasti hyvä käydä läpi tarkemmin vaatimuksia hyvin suunnittelun projektin voimin, jolloin kaikki tietosuoja-asetuksen vaatimukset tulisi käytyä huolellisesti läpi.

Läpikäytäviä asioita tulisi olla vaikutustenarvioinnin, tietojen siirron kolmanteen maahan mahdollistavien toimien, sekä tietojen minimointiin liittyvät konkreettiset teot. Jokaisen yrityksen henkilön tulisi saada ohjeistuksen lisäksi selkeän ja ytimekkään koulutuksen, jonka avulla tietosuoja toimisi paremmin kohdeyrityksen arjessa. Pääosin yrityksen käsittelytoiminta on kuitenkin vähäriskistä, ja henkilöstöstäkin vain pieni osa käsittelee työssään laajamittaisesti henkilötietoja. Suurin yrityksen tietosuojatoimintaan liittyvä kysymys koskee automaattisia, Yhdysvalloista hostattuja markkinointityökaluja, jotka ovat kyseenalaisia, kun tarkastellaan vain ja ainoastaan tietosuoja-asetusta.

Yrityksen toiminnan luonteen huomioon ottaen, sekä eri tietosuoja-ammattilaisten kanssa keskustelleena väittäisin, että paras keino yrityksen kohdalla paremmalle tietosuojatyölle on yksinkertaisen viitekehyksen implementointi, sekä sellaisten yritysten palveluiden säännöllinen käyttö järjestelmien vaatimustenmukaisuuden skannaamisessa, joiden hinta/hyöty suhde olisi optimaalinen liiketoiminnan kannalta. Kaiken kaikkiaan onnistunut tietosuojatyö on yritysten kilpailukykyä parantava tekijä. Keinoja kilpailukyvyn toteen näyttämiseksi tulisi tuoda esille vielä nykyistä vahvemmin.

5 Loppupäätelmät

Käytin tässä työssä kolmea tutkimuskysymystä. Kokemukseni oli, että kolme tutkimuskysymystä oli toimiva strategia päästä tavoitteeseen. Jälkiviisaana tutkimuskysymyksillä toimien riittävyydestä kohdeyritykselle ja tietosuojatoiminnan jatkuvuudesta tulevaisuudessa olisi varmasti tavoitteeseen päässyt. Toisaalta ottaen huomioon tietämättömyyteni aihetta kohtaan, polku tietosuoja-asetuksen yleismaailmallisesta luonteesta kohti pk-yritysten, sekä lopulta kohdeyrityksen rajapintaa oli käytävä aiheen tiedon syväoppimisen omaksumiseksi; lukijalle laaja teoriaosuus voi näyttäytyä raskaalta ja koukeroiselta, tyypilliseltä EU:n tason lainsäädännöltä. Itselle se oli oppimisen kannalta äärettömän tärkeä ei pelkästään itse asetuksen, vaan laajemmin asetuksen säätämiseen johtaneiden syiden pohdintaa. Raportointia kokonaisuudessaan olisi voinut tehdä jäntevämmin ja selkeämmin, ainakin kerrottaessa asetuksen sisällöstä teoriaosuudessa.

Ensimmäiseen tutkimuskysymykseen, ”millaisia toimia pk-yrityksille on osoitusvelvollisuuden toteuttamiselle olemassa”, vastattiin kattavasti jo teoriaosuudessa. Toisessa tutkimuskysymyksessä, ”mitkä toimet ovat riittäviä kohdeyritykselle”, korostui tarkemmin kohdeyrityksen vaatimukset. Laaja kirjallisuuskatsaus toi hyviä käytäntöjä vaatimustenmukaisuuteen kaiken kokoisille pk-yrityksille koko EU:n alueelta; vaatimukset yksityisen sektorin yrityksille ovat kaikille lähes samat, joten koko EU:n alueella kirjoitettujen artikkelien läpikäynti oli perusteltua tehdä.

Vastauksena kolmanteen tutkimuskysymykseen, ”miten varmistaa tietosuoja-asetuksen noudatettavuus jatkossa, vaatimusten toteutumisessa osana yrityksen jokapäiväistä toimintaa on liittää tietosuojatoiminta yrityksen toimintakulttuuriin; henkilöstön tietoisuus on ensiarvoisen tärkeää. Yrityksen tietosuojaympäristö muuttuu myös jatkuvasti, joten säännöllinen vaatimustenmukaisuustarkastus olisi paikallaan, etenkin silloin, kun suunnitellaan uuden palvelun tai järjestelmän hankkimista, tai sopimusten tekemistä uuden yhtiökumppanin kanssa. Yritysfuusiot ovat monesti kriittisiä tietosuojan kannalta, ja silloin yrityskauppaan liittyviä riskejä ja vastuita tulee varsinkin GDPR-aikana pohtia tarkoin tietosuojan näkökulmasta. Ajatuksesta, että tietosuoja-asetus on taakka yrityksen toiminnalle, tulisi päästä vihdoin pois, ja tilalle tulisi omaksua ajatus sen tuomista mahdollisuuksista läpinäkyvämmän liiketoiminnan edistämiseksi kehittyneen, vahvan ja järjestelmällisen tiedonhallinnan, sekä vahvojen ja luotettavien asiakassiteiden kehittämisen kautta.

Ottaen huomioon ainoastaan kohdeyrityksen, eli asiakkaan tarpeet, työn tavoitteeseen päästiin; kesällä 2020 tullut toive yrityksen toimitusjohtajalta toteutui ja yritys on tällä hetkellä tietosuoja-asetuksen suhteen valveutuneempi, mitä tätä työtä edeltävänä aikana oli. Tietosuoja-asetuksen vaatimusten näkökulmasta kehitettävää jäi osaltaan oman osaamisen-, ja osaltaan yrityksen ajanpuutteen vuoksi. Vaatimustenmukaisuudesta tuleva tavoite kuitenkin toteutui; yrityksen toimintaa kehitettiin konkreettisin toimenpitein, huolimatta siitä, että kaikkia vaatimuksia ei saatu toteutettua. Työn luotettavuutta arvioitaessa korostan, että työssä esitellyt toimenpiteet eivät ole kattavia, ja näin ollen en suosittelisi työn yleistä käyttöä tietosuoja-asetuksen jalkauttamis- projektissa. Tällä en kuitenkaan poista mahdollisuutta, etteikö työtä voisi käyttää tietosuoja-asetuksen ymmärryksen lisäämisessä. Työn teoreettinen arvo jäi mielestäni ehkä jopa suuremmaksi, mihin kehittämisen arvo jäi: Teoriaosuuden tieto siitä, mitä aiheesta on aiemmin kirjoitettu, on kattava. Kirjallisuuskatsauksen tulokset toimivat hyvänä ohjenuorana tulevaisuuden työlle; suosittelen laajemminkin kirjallisuuskatsauksen tekemistä etenkin silloin, kun aihe on monialainen ja kokonaisuutena vähän jäsennelty. Ammattilaishaastattelut olisivat voineet tuoda kirjallisuuskatsauksen tueksi luotettavaa kansallista näkökulmaa tietosuojatyön parhaimmista käytännöistä Suomessa.

Yhteenvetona kattava tietosuojatyö, sisäänrakennetun- ja oletusarvoisen tietosuojan mukaan, on kaikkien yritysten saavutettavissa. Mahdollistavien tekijöiden korostaminen suurilla

sanktioilla uhkailun sijaan tulisi olla ensisijaisesti tärkein tietosuoja-asetuksen päämäärien edistämiseen tarkoitettu keino. Monipuolisesti eri toimialoille suunnatuilla, ja hyvin johdetuilla tiedotuskampanjoilla yrityksille, sekä sertifikaateilla voidaan luoda mahdollisuuksia erottua kilpailijoista hyvien tietosuojakäytäntöjen omaajina. Kun yrityksen johto ymmärtää, mitä tarkoittaa laillinen, oikeudenmukainen ja avoin käsittely, on silloin tietosuojatyölle rakennettu hyvä pohja yrityksessä. Tämä onnistuu ennen kaikkea valvontaviranomaisen selkeällä ja johdonmukaisella viestintätoiminnalla, sekä kehittyvillä tiedonhallintaratkaisuilla, joita eri yritykset voivat tarjota. Tietosuojan tärkeys tulee kasvamaan tulevaisuudessa, ihmisistä tulee yhä tietoisempia siitä, missä henkilötietoja säilytetään ja miten niitä käsitellään. Yrityksien tulee ymmärtää, että sujuva henkilötietojen käsittely johtaa yleensä sujuvaan tiedonhallintaan yleisesti, mikä näin ollen tehostaa liiketoimintaa, ja lisää ihmisten luottamusta yritykseen. Toivon, että tietosuojasta tulee samalla tavalla kilpailutekijä yrityksille, kuin työturvallisuus tällä hetkellä on.

Lähteet

Painetut

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

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. 3. uud. p. Helsinki: Sanoma Pro.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro.

Sähköiset

Laki yksityisyyden suojasta työelämässä 759/2004.

Suomen perustuslaki 731/1999b.

Aalto, T. 2015. Workshopien viisi sudenkuoppaa – ja miten vältät ne. Viitattu 8.4.2021. https://yle.fi/aihe/artikkeli/2015/04/15/workshopien-viisi-sudenkuoppaa-ja-miten-valtat-ne

Ahteensuu, M. Riskianalyysi ja ennaltavarautumisen periaate 2008. Viitattu 21.1.2021. https://filosofia.fi/fi/ensyklopedia/riskianalyysi-ja-ennaltavarautumisen-periaate.

Almeida, C. & Goulart, B. 2017. How to avoid bias in systematic reviews of observational studies. Revista CEFAC, 19 (4), 551-555.

Brodin, M. 2019. A Framework for GDPR Compliance for Small-and Medium-Sized Enterprises. European Journal for Security Research, 4 (2), 243-264.

Cavoukian, A. 2010. Privacy by Design - The 7 Foundational Principles.

Coos, A. 2021. Data Protection Legislation Around the World in 2021. Viitattu 9.4.2021. https://www.endpointprotector.com/blog/data-protection-legislation-around-the-world/.

Dixon, P. 2018. A Brief Introduction to Fair Information. Viitattu 23.4.2021. https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

Elinkeinoelämän keskusliitto 2016. Elinkeinoelämän yritysturvallisuusmalli.

Enroth, T. & Neuvonen, R. 2017. EU:n tietosuoja-asetuksen yritysvaikutukset. Valtionneuvoston selvitys ja tutkimustoiminta.

Euroopan Komissio 2021. Standard Contractual Clauses (SCC). Viitattu 10.4.2021. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

Euroopan tietosuojaneuvosto 2020. Lausuma sähköisen viestinnän tietosuoja-asetuksesta sekä valvontaviranomaisten ja Euroopan tietosuojaneuvoston tulevasta roolista.

Euroopan Unioni 2020. Tietosuoja EU:ssa. Viitattu 11.9.2020.

Euroopan Unioni 2016. Euroopan Parlamentin Ja Neuvoston Asetus (Eu) 2016/679.

Euroopan Unionin virallinen verkkosivusto 2021. EU:n oikeus. Viitattu 6.4.2021. https://europa.eu/european-union/law_fi.

Fischer, G. 2020. Guidelines for SME adaption to GDPR Case study of Evalent.

Hansen Jagrelius, R. 2018. The Specific Situation and Needs of SMEs and the GDPR–Taking the account of small enterprises and smaller data subjects.

Hes, R. & Borking, J. 1995. Privacy-Enhancing Technologies: The Path to Anonymity.

Infopulse, S. 2019. PIA or DPIA: What's the Difference? Viitattu 7.4.2021. https://infopulse-scm.com/blog/blog-pia-or-dpia/

Jackson, O. 2018. Businesses retreating from consent under GDPR. International Financial Law Review.

Järvinen, H. & Lankinen, H. 2020. 10. Tietosuojamakasiini - Astetta parempi (D)PIA eli vaikutustenarviointi 2.0.

Kitchenham, B. 2004. Procedures for Performing Systematic Reviews.

Korpisaari, P. H., Pitkänen, O., & Korhonen, R. 2017. Miten kansallista lainsäädäntöämme pitää muuttaa EU:n yleisen tietosuoja-asetuksen vuoksi? teoksessa P. Korpisaari (Toimittaja), Viestintäoikeuden vuosikirja 2016: Viestinnän muuttuva sääntely (Sivut 1-9). (Forum iuris). Helsingin yliopisto, oikeustieteellinen tiedekunta.

Korhonen, S. 2021. Viime vuonna gdpr-sakot sai 5 suomalaista yritystä – Postille suurin sakko. Viitattu 8.3.2021. https://www.tekniikkatalous.fi/uutiset/viime-vuonna-gdpr-sakot-sai-5-suomalaista-yritysta-postille-suurin-sakko/48436117-edb2-42be-a63c-91ab526eadba.

Linnala, J. 2020. YLEINEN TIETOSUOJA-ASETUS (GDPR) PK-YRITYKSISSÄ. Kaakkois-Suomen Ammattikorkeakoulu.

Salminen, A. 2011. Mikä kirjallisuuskatsaus? johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasa: Vaasan yliopisto.

Sankari, V. & Wiberg, M. 2019. GDPR ei toimi - Tietosuojakäytännöt eivät noudata asetusta.

Sharon, S., Gillis, A.S. & Clark, C. 2021. What is Cybersecurity? Everything You Need to Know. Viitattu 7.4.2021. https://searchsecurity.techtarget.com/definition/cybersecurity.

Sotka, J. 2017. Tietosuojavastaavan asema ja tehtävät yrityksessä | Arter Blogi. Viitattu 28.1.2021. https://www.arter.fi/vieraskyna-tietosuojavastaavan-asema-ja-tehtavat-yrityksessa/

Suomen Asiakastieto 2021. Viitattu 7.4.2021. https://www.asiakastieto.fi/web/fi/?gclid=CjwKCAjwjbCDBhAwEiwAiudBy7r1rgfsc4knRYwDWxWnS1hctPB9a7uz5ib2JPaadBwYO0ymGUtPIBoC2VkQAvD_BwE

Suomen riskienhallintayhdistys 2021. Usein kysyttyjä kysymyksiä riskienhallinnasta. Viitattu 28.1.2021. https://Pk-rh.fi/riskienhallinta/ukk.html

Suomen yrittäjät 2021. Yrittäjyys Suomessa. Viitattu 3.3.2021. https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363

Talus, A., Autio, E., Hänninen, A., Pihamaa, H. & Kantonen, S. Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön ja tietosuojavaltuutetun toimiston selvityksiä ja ohjeita. 2017.

Teknologiateollisuus 2020. Digitaalinen turvallisuus on yhä tärkeämpää.

Tietosuojaryhmä 2018. Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta.

Tietosuojavaltuutetun toimisto 2021a. Henkilötietojen käsittely. Viitattu 21.1.2021. https://tietosuoja.fi/henkilotietojen-kasittely

Tietosuojavaltuutetun toimisto 2021b. Milloin henkilötietoja saa käsitellä? Viitattu 21.1.2021. https://tietosuoja.fi/kasittelyperusteet

Tietosuojavaltuutetun toimisto 2021c. Oikeus saada tietoa henkilötietojen käsittelystä. Viitattu 21.1.2021. https://tietosuoja.fi/oikeus-saada-tietoa-kasittelysta

Tietosuojavaltuutetun toimisto 2021d. Rekisterinpitäjän oikeutettu etu. Viitattu 27.1.2021. https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu

Tietosuojavaltuutetun toimisto 2021e. Vaikutustenarviointi. Viitattu 1.2.2021. https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto 2020. Euroopan tietosuojaneuvosto otti kantaa Schrems II -päätökseen ja käsitteli PSD2-maksupalveludirektiiviä koskevaa ohjetta. Viitattu 8.3.2021. https://tietosuoja.fi/-/euroopan-tietosuojaneuvosto-otti-kantaa-schrems-ii-paatokseen-ja-kasitteli-psd2-maksupalveludirektiivia-koskevaa-ohjetta

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34 (1), 134-153.

Todorović, I., Komazec, S., Krivokapić, Đ & Krivokapić, D. 2018. Project management in the implementation of General Data Protection Regulation (GDPR).

Tolvanen, H. & Pökkylä, P. 2021. Tietosuojapod #14 - Millainen oli tietosuojavuosi 2020?

VAHTI 2016. EU-tietosuojan kokonaisuudistus. Viitattu 19.2.2021. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75065/VAHTI-raportti%201_2016.pdf?sequence=1&isAllowed=y.

Vastaamo 2020. Ajankohtaista. Viitattu 20.1.2021. https://vastaamo.fi/ajankohtaista/.

Watson, R.T. & Webster, J. 2002. Analyzing the past to prepare for the future: writing a literature review.

Julkaisemattomat

Kuviot

Taulukot