Saku Sikiö

ORGANISAATIOIDEN TIETOSUOJAN HALLINNAN HAASTEET TIETOSUOJA-ASIANTUNTIJOIDEN KOKEMUKSISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Sikiö, Saku
Organisaatioiden tietosuojan hallinnan haasteet tietosuoja-asiantuntijoiden kokemuksissa
Jyväskylä: Jyväskylän yliopisto, 2022, 66 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

EU:n yleisen tietosuoja-asetuksen astuminen voimaan 2018 pakotti kaikki EU-jäsenmaat suhtautumaan uudella tavalla tietosuojaan. Yksilöiden oikeuksien, yksityisyydensuojan ja vapauksien vahvistamisen kääntöpuolena on tiukempi säätely organisaatioille. Tämän tutkielman tarkoitus on teemahaastatteluiden avulla taustoittaa, minkälaisia tietosuojan hallintaan liittyviä haasteita organisaatioissa esiintyy nyt neljä vuotta GDPR:n voimaantulon jälkeen. Lisäksi teemahaastatteluiden on tarkoitus tuoda esille keinoja, joilla näitä haasteita aiotaan ja on aikaisemmin ratkaistu. Tietosuoja-asetus on myös kasvattanut merkittävästi tietosuojaan liittyvien organisatoristen ja teknisten apuvälineiden markkinoita. Aikaisemmin ei ole tutkittu, käytetäänkö niitä tai jos käytetään, onko niistä hyötyä.

Avainsanat: tietosuoja, rekisterinpitäjä, käsittelijä, henkilötiedot, GDPR

ABSTRACT

Sikiö, Saku
The challenges of data privacy management in organizations in the experiences of data privacy specialists
Jyväskylä: University of Jyväskylä, 2023, 66 p.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

The entry into force of the EU General Data Protection Regulation in 2018 forced all EU member states to approach data protection in a new way. The flip side of strengthening the rights, privacy protection and freedoms of individuals is stricter regulation for organizations. The purpose of this thesis is to use thematic interviews to provide background information on what kind of challenges related to data protection management is occurring in organizations now four years after the entry into force of the GDPR. In addition, the theme interviews are meant to highlight ways in which these challenges are planned and have been solved in the past. The Data Protection Regulation has also significantly increased the market for organizational and technical tools related to data protection. In the past, it has not been studied whether they are used or, if used, whether they are useful.

Keywords: data protection, controller, processor, personal data, GDPR

KUVIOT

Kuvio 1 Tietosuojan viitekehyksen avainalueet IT Governance Privacy Team (2020, 84) mukaan 22

TAULUKOT

Taulukko 1 Osa tietosuojaviitekehyksen ydintaulukosta (NIST, 2020, 19–27) ... 23
Taulukko 2 Haastattelun teemat sekä esimerkkikysymykset 34

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT JA TAULUKOT

1 JOHDANTO 6

2 YLEINEN TIETOSUOJA-ASETUS 9
2.1 Käsitteiden määrittelyä 9
2.2 Tietosuoja-asetus yleisesti 10
2.3 EU:n yleisen tietosuoja-asetuksen haasteita 13
2.3.1 Oletusarvoinen ja sisäänrakennettu tietosuoja 13
2.3.2 Tietosuojaa koskeva vaikutustenarviointi 14
2.3.3 Schrems-II ja siirrot kolmansiin maihin 15
2.3.4 Tietosuojavastaava 17
2.3.5 Tietoturvaloukkaukset 18
2.3.6 Rekisteröidyn oikeudet ja tietopyynnöt 19

3 APUA TIETOSUOJAN HALLINTAAN 21
3.1 Organisatorisia apuvälineitä tietosuojan hallintaan 21
3.2 Teknisiä apuvälineitä tietosuojan hallintaan 28

4 TUTKIMUSMENETELMÄ JA TOTEUTUS 32
4.1 Teemahaastattelurungon laatiminen 32
4.2 Haastateltavien valinta ja aineistonhankinta 34
4.3 Sisällönanalyysi 36
4.4 Luotettavuuden arviointia 37

5 TUTKIMUSTULOKSET 39
5.1 Haasteet 39
5.2 Ratkaisut 44
5.3 Tekniset ja organisatoriset apuvälineet 47

6 POHDINTA 51
6.1 Tulosten tarkastelua ja johtopäätökset 52
6.1.1 Haasteet 52
6.1.2 Ratkaisut 54
6.1.3 Tekniset ja organisatoriset apuvälineet 55
6.2 Jatkotutkimusehdotukset 56

LÄHTEET 59

1 JOHDANTO

Tietosuojan merkitys digitalisaation ja uusien teknologioiden myötä tulee kasvamaan entisestään ja sen vaikutus ulottautuu nykyään väkisinkin melkein elämän joka osa-alueelle. Henkilötietoja käsitellään, kun ostat lipun netistä konserttiin, menet töihin, osallistut arpajaisiin, liityt ammattiliittoon ja jopa televisio kysyy evästeistä, kun katsot kotona Netflixiä. Varsinkin digitaalisten palveluiden käyttäminen ilman henkilötietojen käsittelyä on lähes mahdotonta. Tilannetta ei ole auttanut liiketoiminta, joka hyötyy rahallisesti henkilötietojen käsittelystä ja keräämisestä (D'Annunzio & Menichelli, 2022, 571–572). Tietosuojaa voidaan pitää ihmisoikeutena omaan yksityisyyteen, mutta tämän yksityisyyden hallinta digiaikana voi olla erittäin haastavaa. Tietosuoja-asetuksen voimaantulo toukokuussa 2018 paransi huomattavasti rekisteröityjen tietosuojaa Euroopan unionin jäsenvaltioissa, mutta lisääntynyt säätely loi organisaatioille uusia haasteita tietosuojan hallintaan liittyen.

Asetuksen oli tarkoitus tuoda luottamusta organisaatioiden henkilötietojen käsittelyä kohtaan ja parantaa rekisteröityjen oikeusturvaa. Samalla tietosuoja-asetus toi mukanaan aivan erilaisen vastuun organisaatioille, sillä sen myötä tietosuojan hallinnan laiminlyömisellä oli paljon merkittävämmät seuraukset kuin aikaisemmin. Pantelic, Jovic ja Krstovic (2022, 12) huomauttavatkin, että organisaatiot, jotka eivät noudata tietosuojasäätelyä menettävät asiakkaita, yhteistyökumppaneita ja saavat suurempia sakkoja. Esimerkiksi asetuksen mukana tulleet vaatimukset oletusarvoisesta ja sisäänrakennetusta tietosuojasta, osoitusvelvollisuudesta, riskilähtöisestä lähestymistavasta ja rekisteröityjen oikeuksien noudattamisesta loivat organisaatioille ympäristön, jossa vain pahempien tietosuojaloukkauksien välttäminen ei riittänyt. Tietosuojaa oli pakko alkaa hallitsemaan kokonaisvaltaisesti. Asetuksen jälkeen tullut Schrems-II päätös liittyen siirtoihin kolmansiin maihin ei ainakaan helpottanut organisaatioiden haasteita (Rotenberg 2020, 143–145).

Mielenkiinto ja motivaatio tutkijalle tutkia mahdollisia tietosuojan hallinnan haasteita ja ratkaisuja näihin haasteisiin liittyen, heräsi oman kokemuksen kautta. Tietosuojan hallintaan vaikutti olevan asiantuntijoiden keskuudessakin monia erilaisia lähestymistapoja. Asiantuntijoilla tuntui olevan myös erilaisia tulkintoja tietosuoja-asetuksesta ja sen vaatimuksista. Heräsi mielenkiinto tutkia, minkälaisia haasteita organisaatioissa on tietosuojan hallintaan liittyen ja miten

niitä on ratkaistu. Aiheesta löytyi vähän kokonaisvaltaista tutkimusta tai kirjallisuutta, joten aihe oli myös ajankohtainen ja tarpeellinen. Tietosuoja-asetuksen vaatimusten tulkinnallisuus tuli ilmi aikaisemmissa tutkimuksissa, mutta tietosuojan hallinnan haasteita oli silti mielekästä tutkia tarkemmin. Tietosuojaan liittyvien organisatoristen ja teknisten apuvälineiden määrä on myös räjähtänyt tietosuoja-asetuksen myötä. Mielenkiintoista oli myös tutkia, käytetäänkö niitä organisaatioissa ja onko niistä hyötyä tietosuojan hallinnan kannalta.

Tutkielma aloitettiin laajalla kirjallisuuskatsauksella, jolla kartoitettiin aikaisempaa tutkimusta tietosuojan hallinnan haasteista ja ratkaisuista. Niiden lisäksi on avattu myös muita tietosuoja-asetuksen vaatimuksia, jotka voisivat nousta esille aineistossa. Fenomenologinen tutkimusmetodi ohjasi tutkielman tekemistä. Siinä ilmiölle annetaan merkitys haastateltavien henkilökohtaisten kokemuksien kautta. Fenomenologiassa on tärkeää tutkia ilmiötä ilman ennakkoluuloja ja mahdollisimman avoimesti. Myös aikaisemman teorian ohjaavaa vaikutusta pyrittiin tutkielman teon aikana minimoimaan. Tämä näkyi myös sisällönanalyysissa, jossa asiantuntijoiden kokemukset otettiin huomioon tuloksissa mahdollisimman läpinäkyvästi ja ilman hypoteesien ohjaavaa vaikutusta.

Tutkielman tavoite oli nimenomaan tietosuoja-asiantuntijoiden kokemusten kautta löytää teemoja, jotka liittyvät tietosuojan hallinnan haasteisiin ja niiden ratkaisuihin. Näiden lisäksi tutkielmassa selvitettiin, onko organisaatioilla käytössä teknisiä tai organisatorisia apuvälineitä tietosuojan hallinnan tueksi. Tutkielma suoritettiin laadullisena tutkimuksena, jota ohjasi fenomenologinen tieteenfilosofia. Aineisto kerättiin teemahaastatteluilla ja analysoitiin aineistolähtöisellä sisällönanalyysilla, jossa painotettiin haastateltavien kokemusten kautta tulevia merkityksiä. Tutkimuskysymykset määriteltiin seuraavasti:

- **Minkälaisia haasteita organisaatioiden tietosuojan hallinnassa on?**
- **Miten näitä haasteita on ratkaistu tai pyritään ratkaisemaan?**
- **Minkälaisia organisatorisia tai teknisiä apuvälineitä/ratkaisuja organisaatioissa on käytössä tietosuojan hallintaan?**

Tutkimuskysymyksiä tarkastellaan myös ajallisessa näkökulmassa. Tämä ei tule ilmi tutkimuskysymyksissä suoraan, mutta esitetään selvästi osiossa 4.1 ''Teemahaastattelurungon laatiminen''. Ottamalla huomioon haastateltavien kokemukset tietosuoja-asetuksen alkuajoista asti, saadaan myös tietoa, ovatko haasteet, ratkaisut ja apuvälineiden käyttäminen muuttuneet asiantuntijoiden urien aikana. Lisäksi kysyttiin tulevaisuuden näkemyksistä ja suunnitelmista. Tarkastelun ulkopuolelle jätetään tarkempi määrittely, kuinka organisaatioissa toteutetaan tietosuojan hallintaa. Tutkielmassa keskitytään lisäksi tietosuoja-asetuksen jälkeiseen aikaan, koska se muutti tietosuojan hallinnan kenttää merkittävästi. Tietosuojan hallintaa katsotaan viitekehyksien kautta, jotka näyttävät suuret linjat. Tarkempaan kuvaukseen valitaan tietosuojan hallinnan alueita, jotka aikaisemman kirjallisuuden perusteella saattavat nousta haastatteluissa esille. Tarkoitus ei ole painautua tarkasti yhteen tai muutamaan tietosuojan alueeseen, vaan mahdollistaa tietosuojan hallinnan haasteiden

tutkiminen koko laajuudessaan. Teoriaosuuden tarkoitus on myös osaltaan osoittaa, että tutkielman kirjoittaja on tarpeeksi perehtynyt aiheeseen.

Tuloksista voidaan päätellä, että tietosuojan hallinnan haasteet keskittyvät kahden pääteeman ympärille. Ensimmäinen teema on tulkinnallisuus ja siitä johtuva epävarmuus. Toinen teema, tietosuojan jalkauttamisen ja tietosuojakoulutuksen haasteet tietosuojan hallinnassa tuli enemmän yllätyksenä, sillä siitä ei löytynyt yhtään aikaisempaa tutkimusta. Tämä voi olla merkittävä asia ottaa huomioon mahdollisissa jatkotutkimuksissa. Varsinaisia ratkaisuja haasteisiin ei asiantuntijoilla juuri ollut. Ainut merkittäväksi noussut ratkaisu on aikainen valmistautuminen luomalla prosesseja ja työnjakoa tietosuojaan liittyen. Teknisiä ja organisatorisia apuvälineitä käytettiin organisaatioissa hyvin vähän. Mielenkiintoista oli kuitenkin huomio, että asiantuntijat, jotka käyttivät teknisiä apuvälineitä, pitivät niitä todella hyödyllisinä. Tulokset toivat uutena huomiona tietosuojan jalkauttamisen ja tietosuojakoulutuksen haasteet. Lisäksi tutkielma on hyvä kartoittava katsaus tietosuojan hallinnan haasteisiin ja ratkaisuihin, jonka pohjalta voidaan tehdä useita jatkotutkimusehdotuksia.

2 YLEINEN TIETOSUOJA-ASETUS

Tämän kappaleen tarkoituksena on avata EU:n yleisen tietosuoja-asetuksen eli GDPR:n taustaa, merkitystä ja haasteita ja erityisesti niitä tekijöitä, jotka vaikuttavat yritysten tietosuojan hallintaan. Aluksi avataan tietosuoja-asetukseen liittyviä käsitteitä. Toisessa kappaleessa avataan yleisesti tietosuoja-asetusta ja sen taustoja. Kolmannessa kappaleessa keskitytään tietosuoja-asetuksen kohtiin, jotka todennäköisimmin aiheuttavat haasteita organisaatioille. Koska EU:n yleinen tietosuoja-asetus on tutkielman aiheen kannalta keskeisin ja kattaa myös laajasti muiden tietosuoja-asetuksien asettamia säädöksiä, jätetään muut asetukset tarkemman läpikäynnin ulkopuolelle.

2.1 Käsitteiden määrittelyä

Tässä kappaleessa avataan tietosuojan yleisiä käsitteitä, joita käytetään tutkielmassa. Lisää käsitteitä avataan tutkielmassa myöhemmissä kappaleissa, joten tämän kappaleen listaus ei ole kaikenkattava. Tietosuojaan liittyy paljon terminologiaa, jota ei käytetä juuri muuten kuin tietosuojaan liittyen.

Tietosuoja-asetuksen keskiössä ovat henkilötiedot. Henkilötiedoksi tietosuoja-asetuksessa lasketaan kaikki tieto, joka on luonnolliseen, tunnistettavaan henkilöön liitettävissä. Tämänkaltaisia tietoja ovat esimerkiksi nimi, henkilötunnus, IP-soite, sijaintitieto tai yksi tai useampi tunnistettavissa oleva fyysinen tekijä. Kuitenkin myös kaikki tiedot, joita yhdistämällä voidaan päätellä rekisteröidyn henkilötiedot, lasketaan henkilötiedoiksi. (Euroopan parlamentti ja Euroopan neuvosto, 2016).

Rekisteröitynä oleminen tarkoittaa, että henkilö on antanut tietojaan jollekin organisaatiolle tai vastaavalle, joka ylläpitää näitä tietoja jossain tietojärjestelmässä. Henkilöstä tulee siis rekisteröity tietosuoja-asetuksen silmissä siinä vaiheessa, kun hän luovuttaa henkilötietojaan rekistereiden ylläpitäjille. Rekisterinpitäjällä on velvollisuuksia rekisteröityä kohtaan ja rekisteröidyllä on tiettyjä oikeuksia, joita esitetään tarkemmin kappaleessa 2.2 ’’Tietosuoja-asetus

yleisesti''. (Henkilötietojen Käsittely; Euroopan parlamentti ja Euroopan neuvosto, 2016).

Rekisterinpitäjä on jokin henkilö tai organisatorinen kokonaisuus, joka vastaa rekisteröidyn henkilötietojen käsittelystä ja hallinnoinnista. Tästä esimerkkinä voisi olla yritys, joka kerää asiakastietoja tai järjestö, jolla on jäsenrekisteri. Rekisterinpitäjällä on velvollisuus noudattaa tietosuoja-asetuksen säännöksiä. Nämä säännökset käsittävät esimerkiksi sen, mitä tietoja saa käsitellä ja miten niitä saa käsitellä. Rekisterinpitäjän on varmistettava esimerkiksi, että tietoja käytetään vaan siihen tarkoitukseen, mihin ne on kerätty ja että tiedot ovat ajantasaisia. Rekisterinpitäjä on vastuussa henkilötietojen käsittelystä ja määrittää sen, kuinka käsittelijät käyttävät heidän keräämiään henkilötietoja. (Henkilötietojen Käsittely; Euroopan parlamentti ja Euroopan neuvosto, 2016).

Käsittelijä on jokin henkilö tai organisatorinen kokonaisuus, joka käsittelee henkilötietoja jonkin toisen henkilön tai organisatorisen kokonaisuuden puolesta. Käsittelijä voi olla esimerkiksi pilvipalveluita tarjoava yritys. Käsittelijän tehtävänä on toteuttaa rekisterinpitäjän kanssa sovitut tehtävät. Käsittelijällä ei siis ole oikeutta käyttää henkilötietoja omiin tarkoituksiinsa. Tietosuoja-asetuksessa on käsittelijöille omat säännökset, joita käsittelijän pitää noudattaa. (Henkilötietojen Käsittelijät; Euroopan parlamentti ja Euroopan neuvosto, 2016).

Käsittelyllä tarkoitetaan kaikkia toimia, joiden yhteydessä henkilö tai organisatorinen kokonaisuus työskentelee henkilötietojen kanssa jollakin tavalla. Käsittely voi olla esimerkiksi henkilötietojen tallentamista, poistamista, käyttämistä johonkin tarkoitukseen tai tietojen lähettämistä eteenpäin. Voidaan puhua myös käsittelytoimista. Käsittelyä tai käsittelytoimia voi suorittaa sekä käsittelijä että rekisterinpitäjä. Rekisterinpitäjää vaaditaan myös ylläpitämään selostetta käsittelytoimista, jos organisaatiossa on työntekijöitä enemmän kuin 250. Seloste käsittelytoimista on tehtävä myös alle 250 henkilön organisaatioissa, jos henkilötietojen käsittely ei ole satunnaista tai aiheuttaa riskejä rekisteröidyn oikeuksille tai jos henkilötietojen käsittely sisältää erityisiä henkilötietoryhmiä. (Rekisterinpitäjän Seloste Käsittelytoimista; Euroopan parlamentti ja Euroopan neuvosto, 2016).

2.2 Tietosuoja-asetus yleisesti

YK:n ihmisoikeuksien yleismaailmallisen julistuksen artiklan 12. mukaan kenenkään yksityiselämään tai kirjeenvaihtoon ei pitäisi mielivaltaisesti puuttua (United Nations). Euroopan ihmisoikeussopimuksen (63/1999 - Valtiosopimukset - FINLEX ®) Artikla 8. kohta 1. täydentää tuota YK:n ihmisoikeuksien yleismaailmallisen julistuksen näkemystä yksityisyydestä ihmisoikeutena:

> ''1. Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.''

Lissabonin sopimuksen (2007/C 306) myötä henkilötietojen suoja on jokaisen yksilön oikeus Euroopan unionissa. Ustaran (2018, 4–5) perusteleekin, että oikeudet yksityiseen elämään ja siihen liittyviin vapauksiin ovat EU:n tietosuojalainsäädännön perusta. Euroopan unionin (EU) yleinen tietosuoja-asetus (englanniksi General Data Protection Regulation, GDPR) säädettiin huhtikuussa 2016 ja se tuli voimaan täysivaltaisesti toukokuussa 2018 kaikissa Euroopan unionin maissa. Tietosuoja-asetuksen tarkoitus on taata rekisteröityjen oikeudet ja yksityisyyden suoja henkilötietojen käsittelyssä.

Tietosuoja-asetus korvasi aikaisemman direktiivin yksilöiden henkilötietojen käsittelystä ja näiden tietojen vapaasta liikkuvuudesta (95/46/EY). Vuonna 1995 voimaan tullut direktiivi ei enää pysynyt teknologioiden kehityksen mukana. Myös globalisaation aiheuttama organisaatioiden suureneva henkilötietojen käyttö vaikutti siihen, että direktiiviä tuli muovata kokonaisvaltaisempaan suuntaan. Digitalisaation sekä henkilötietojen käytön taloudelliset hyödyt saattoivatkin olla pitkään hidasteena yksityisyyden suojan parantamiselle EU:ssa (Padden & Öjehag-Pettersson, 2021, 2; Rossi, 2018, 101–103). Valvonnan ja tietojen keräämisen laajuuden nouseminen yleiseen tietoisuuteen, etenkin Snowdenin paljastusten myötä, auttoi uuden tietosuoja-asetuksen säätämisen prosessia huomattavasti eteenpäin (Rossi, 2018, 104–107). Yhdysvaltain tiedustelulait ovat aiheuttaneet tietosuojan hallinnan kannalta ongelmia myös asetuksen jälkeen. Näistä haasteista kerron lisää kohdassa 2.2.2 ''Schrems-II ja siirrot kolmansiin maihin''. Direktiivin vaihtaminen asetukseksi lisäsi yhtenäisyyttä ja luottamusta EU:n jäsenvaltioiden sisällä. Asetus toi myös jatkuvuutta EU:n jäsenmaiden tapaan suhtautua tietosuojaan ja samalla selvemmät pelisäännöt henkilötietojen taloudelliselle hyödyntämiselle. Jäsenvaltioille jätettiin mahdollisuus lisätä säännöksiä esimerkiksi erityisten henkilötietojen käsittelyn ja laillisen velvoitteen noudattamisen suhteen. (Ustaran, 2018, 13–15).

Tietosuoja-asetus ei kuitenkaan muuttanut 95/46/EY direktiiviä kokonaan, vaan vanhasta direktiivistä jäi paljon myös nykyiseen tietosuoja-asetukseen. Esimerkiksi asetuksen artiklassa 5 esitetyt henkilötietojen käsittelyn periaatteet on jatkokehitetty aikaisemman direktiivin periaatteista. EU:n yleisen tietosuoja-asetuksen (2016, artikla 5) mukaiset periaatteet ovat:

- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- säilytyksen rajallisuus
- eheys ja luottamuksellisuus
- kohtuullisuus, lainmukaisuus ja läpinäkyvyys

Artikla 5 kohta 2 lisää myös osoitusvelvollisuuden (Euroopan parlamentti ja Euroopan neuvosto, 2016). Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan, että hän noudattaa henkilötietojen käsittelyssä kohdassa 1 esitettyjä periaatteita. Osoitusvelvollisuuteen kuuluu erilaisia vaatimuksia, kuten käsittelyiden dokumentointia ja ilmoituksien tekemistä tietosuo-

javiranomaisille. Lindqvist (2018) arvioi tutkimuksessaan, että osoitusvelvollisuus olisi suurimpia tietosuoja-asetuksen tuomia muutoksia. Hänen mukaansa osoitusvelvollisuuden myötä rekisterinpitäjien tulee pystyä osoittamaan mitattavalla tavalla sen noudattavan tietosuoja-asetuksen periaatteita (Lindqvist, 2018, 57–58).

Käyttötarkoitussidonnaisuuden periaatteen mukaisesti henkilötietoja saa käsitellä vain tietyn ennalta määritellyn tarkoituksen mukaisesti. Tietojen minimointi on samansuuntainen periaate kuin käyttötarkoitussidonnaisuus. Tietojen minimoinnilla tarkoitetaan henkilötietojen keräämisen ja käsittelyn rajaamista vain siihen, mikä on käsittelylle tarpeellista. Tietojen täsmällisyyden periaate vaatii, että rekisterinpitäjä huolehtii henkilötietojen ajantasaisuudesta ja paikkansapitävyydestä. Henkilötietojen säilytyksen rajallisuus tarkoittaa, että henkilötietoja kuuluu säilyttää vain niin kauan kuin laki edellyttää tai niin kauan kuin se on tarpeellista niihin tarkoituksiin nähden, joihin se on kerätty. Tämä tarkoittaa, että tietojen säilytysaikoja on seurattava ja on arvioitava säännöllisesti, voiko joitain tietoja poistaa tarpeettomina. Eheys ja luottamuksellisuus periaatteina tarkoittavat henkilötietojen luotettavuuden, turvallisuuden ja saatavuuden takaamista. Näiden periaatteiden takaamiseksi rekisterinpitäjällä tulisi olla käytössä suojatoimenpiteitä, joiden toimivuutta tulisi arvioida säännöllisesti. Kohtuullisuus tarkoittaa, että henkilötietoja käytetään vain niihin tarkoituksiin, joihin ne on kerätty. Tämä tarkoittaa myös, että tietoja käsitellään asianmukaisesti, eikä muihin tarkoituksiin kuin rekisteröidylle on kerrottu. Läpinäkyvyys tarkoittaa, että rekisteröidylle annetaan tarpeeksi tarkasti sekä selvästi tietoa siitä, mitä tietoja hänestä kerätään ja mihin tarkoitukseen. Lainmukaisuuden periaatteen mukaan henkilötietojen käsittelyn tulee aina perustua laillisiin perusteisiin. (Alhazmi & Arachchilage, 2021, 880–882; Euroopan parlamentti ja Euroopan neuvosto, 2016; Tietosuojaperiaatteet, 2022).

Lainmukaisuuden periaatteen mukaisesti kaikkien henkilötietojen käsittely pitää perustua artiklan 6 kohdan 1 käsittelyn lainmukaisuuteen. Tietosuoja-asetuksen (2016) mukaan käsittelylle on kuusi erilaista laillista perustetta.

a) Rekisteröidyn suostumus
b) Sopimuksen täytäntöönpano
c) Lakisääteinen velvoite
d) Elintärkeän edun suojaaminen
e) yleinen etu tai julkinen valta
f) Oikeutettu etu

Rekisteröidyn suostumus tarkoittaa, että rekisteröity antaa tietoisen, yksiselitteisen ja vapaaehtoisen suostumuksensa henkilötietojensa käsittelyyn. Suostumus voidaan antaa kirjallisesti tai sähköisesti sekä sen on oltava peruutettavissa milloin tahansa. Esimerkiksi evästeiden käytössä suostumus on ainoa hyväksyttävä laillinen peruste (Traficom, 2021). Sopimuksen täytäntöönpanolla tarkoitetaan henkilötietojen käsittelyä, joka on tarpeen sopimuksen toteuttamisen kannalta. Sopimuksessa olisi hyvä määritellä selvästi henkilötietojen käsittelyn tar-

koitus ja mitä henkilötietoja saa käsitellä. Lakisääteinen velvoite voi perustua viranomaisen määräykseen tai lakiin. Silloin henkilötietoja saa käsitellä esimerkiksi verotuksen, rahoituslaitosten tai terveydenhuollon vaatimusten täyttämiseksi. Elintärkeiden etujen suojaaminen käsittää henkilötietojen käsittelyn niissä tapauksissa, joissa se on tarpeen rekisteröidyn tai muiden henkilöiden terveyden takaamiseksi. Julkinen valta tai yleinen etu käy lailliseksi perusteeksi silloin, kun henkilötietojen käsittely on tarpeellista esimerkiksi tutkimuksen tai tilastoinnin tarkoituksia varten. Henkilötietoja voidaan käsitellä rekisterinpitäjän oikeutetun edun perusteella. Niin julkiset kuin yksityisetkin toimijat voivat käyttää oikeutettua etua käsittelyn perusteena. Oikeutetun edun oikeuttaminen ja käyttäminen täytyy arvioida kuitenkin tapauskohtaisesti. Tätä tarkoitusta varten on tasapainotestit. Tasapainotestillä varmistetaan, että rekisteröidyn vapauksien ja oikeuksien toteutuminen on tasapainossa oikeutetun edun suhteen, eikä muita laillisia perusteita voida käsittelyssä käyttää (Bu-Pasha, 2022). Jäsenvaltioilla on mahdollista ottaa käyttöön tarkempia säännöksiä liittyen yleisen edun ja julkisen vallan tai lakisääteisen velvoitteen käyttämiseen laillisena perusteena (Euroopan parlamentti ja Euroopan neuvosto 2016; Henkilötietojen käsittelyperusteet, 2019).

2.3 EU:n yleisen tietosuoja-asetuksen haasteita

Tässä kappaleessa esitellään enemmän EU:n yleisen tietosuoja-asetuksen vaatimuksia ja periaatteita. Keskityn tarkastelemaan erityisesti niitä tekijöitä, jotka saattavat asettaa haasteita tietosuojan hallintaan liittyen.

2.3.1 Oletusarvoinen ja sisäänrakennettu tietosuoja

Tietosuoja-asetuksen artiklassa 25 asetetaan vaatimus oletusarvoiselle ja sisäänrakennetulle tietosuojalle. Oletusarvoinen tietosuoja tarkoittaa, että tietosuojatoimet on otettu käyttöön oletuksena. Tämä tarkoittaa, että esimerkiksi järjestelmät, toimintatavat, palvelut ja työkalut noudattavat oletusarvoisesti korkeita tietosuojastandardeja. Sisäänrakennetulla tietosuojalla tarkoitetaan, että tietosuoja on otettu huomioon alusta alkaen ja mahdollisuuksien mukaan integroitu osaksi toimenpiteitä, järjestelmiä, työkaluja ja palveluja. Näin ei vaadita erillisiä toimenpiteitä tietosuojan varmistamiseksi. Tärkeää on myös teknisten ja organisatoristen toimenpiteiden toteuttaminen riittävän tietosuojan tason takaamiseksi. (Waldman, 2020, 149–150.) Teknisiksi toimenpiteiksi luetaan esimerkiksi henkilötietojen pseudonymisointi. Organisatorisia toimenpiteitä ovat esimerkiksi henkilökunnan tietosuojakoulutukset. (Henkilötietojen Käsittelijän Velvollisuudet; Euroopan parlamentti ja Euroopan neuvosto 2016.)

Vaikka tarkoituksena on ollut ohjata rekisterinpitäjiä kokonaisvaltaisempaan ja paremmin suunniteltuun tietosuojan hallintaan, on artikla 25 silti saanut tutkijoilta jonkin verran kritiikkiä. Oletusarvoinen ja sisäänrakennettu tietosuoja eivät itsessään ole olleet kritiikin keskipiste, vaan se tapa, jolla ne on imple-

mentoitu osaksi tietosuoja-asetusta. Waldman (2020, 147–148) huomauttaa sisäänrakennetun tietosuojan tietosuoja-asetusta pidemmästä historiasta, jota artikla 25 ei ole onnistunut sisäistämään. Veale, Binns & Ausloos (2018, 105–109) sen sijaan argumentoivat, että artiklan 25 toteuttaminen voi olla ristiriidassa rekisteröityjen tietopyyntöjen kanssa, sillä sisäänrakennetun tietosuojan paradigmat ohjaavat enemmän tiedon salaamiseen. Rubinstein ja Good (2020, 40–43) nostavat esiin viisi epäkohtaa artikla 25:ssa. Näitä ovat esimerkiksi Vealen ja kumppaneiden (2018) esiintuoma ristiriita muiden tietosuoja-asetuksen kohtien kanssa, artiklan suppeus sekä muotoilun epämääräisyys. Heidän mukaansa vaatimusten täyttäminen on vaikeaa, eikä koskaan voi olla varma, toteutuuko oletusarvoinen tietosuoja artiklan mukaisesti (Rubinstein ja Good, 2020, 43–44). EDPB eli tietosuojaneuvosto (2019) on pyrkinyt luomaan tarkempaa ohjeistusta liittyen 25 artiklan mukaiseen sisäänrakennettuun ja oletusarvoiseen tietosuojaan. Ohjeistuksesta huolimatta voi olla mahdollista, että organisaatioilla on haasteita vastata artiklan vaatimuksiin. Toisaalta vaatimuksien täyttämistä voi olla vaikea myös valvoa.

2.3.2 Tietosuojaa koskeva vaikutustenarviointi

GDPR-asetus toi mukanaan tietosuojaa koskevat vaikutustenarvioinnit. Artiklan 35 mukainen vaikutustenarviointi tulee tehdä aina, kun tietojen käsittely aiheuttaa todennäköisesti korkean riskin luonnollisen henkilön oikeuksille ja/tai vapauksille. Ainakin seuraavissa tapauksissa on välttämätöntä EU:n tietosuoja-asetuksen mukaan toteuttaa tietosuojaa koskeva vaikutustenarviointi tietosuojatyöryhmän (WP29) lausunto 14/EN WP 2186 (2017) ohjeiden perusteella:

- Jos henkilötietojen käsittely sisältää erityisten henkilötietoryhmien käsittelyä
- Jos henkilötietojen käsittely sisältää laajamittaista yleisölle avoimen alueen järjestelmällistä seurantaa, tarkkailua tai valvontaa
- Jos henkilötietojen käsittely sisältää henkilökohtaisten ominaisuuksiin liittyvää automaattista arviointia, jolla on vaikutusta henkilöön liittyviin päätöksiin.
- Jos henkilötietojen käsittely on laajamittaista. Laajamittaisuuden arvioinnissa on otettava huomioon:
    - Rekisteröityjen lukumäärä tarkkana lukuna tai osuutena kyseenomaisesta väestöstä
    - Tietojen tai tietoyksikköjen määrä
    - Käsiteltyjen tietojen säilytysaika
    - Käsittelyn maantieteellinen laajuus
- Jos käsittely sisältää useiden eri tarkoitukseen tarkoitetun tietolähteiden tietojen yhdistelyä tai soveltamista, rekisteröidyn odottamattomalla tavalla

- Jos käsittely sisältää heikossa asemassa olevien rekisteröityjen tietoja
- Jos käsittely estää rekisteröityjä käyttämästä palvelua, sopimusta tai oikeuksiaan
- Jos käsittelyyn liittyy uuden teknologian käyttäminen aikaisemmasta käsittelystä poikkeavalla tavalla

Yhden tai useamman kohdan täyttyminen tarkoittaa, että vaikutustenarviointi olisi suositeltavaa tehdä. Erityisiksi henkilötietoryhmiksi lasketaan etniseen alkuperään, poliittiseen mielipiteeseen, uskonnolliseen tai filosofiseen vakaumukseen, seksuaaliseen suuntautumiseen, ammattiliiton jäsenyyteen, terveyteen sekä geneettiseen ja biometriseen tietoon liittyvät henkilötiedot (Euroopan parlamentti ja Euroopan neuvosto, 2016; Clarke, Vale, Reeves, Kirwan, Smith, Farrel, Hurl & McElvaney, 2019, 1130).

GDPR-asetuksen ohjeet vaikutustenarviointeihin liittyen ovat tulkinnanvaraisia, eikä esimerkiksi selviä mittareita ole asetettu sille, mikä on laajamittaista käsittelyä. Ferra, Wagner, Boiten, Hadlington, Psychoula ja Snape (2019, 14) huomasivat tutkimuksessaan, että tietosuojaa koskevat vaikutustenarvioinnit on tietosuoja-asiantuntijoidenkin joukossa ymmärretty osittain väärin. Yleinen virhe on, että riskejä arvioidaan organisaation, eikä rekisteröidyn näkökulmasta. (Ferra ym., 2019, 3). GDPR-asetuksen mukaan riskit on arvioitava nimenomaisesti rekisteröidyn näkökulmasta ja näin organisaation näkökulmasta tehdyt riskiarvioinnit voidaan nähdä riittämättöminä. Toinen yleinen virhe on, että suunnitellut riskien vastatoimet kohdistuvat vaikutukseen, eivätkä syyhyn (Ferra ym., 2019, 3). Vaikutustenarviointien laiminlyönnistä voi aiheutua sanktioita organisaatiolle. Esimerkiksi Cosmote-televiestintäyhtiön todettiin olevan vastuussa heikosti tehdyistä tietotosuojaa koskevista vaikutustenarvioinneista (Hellenic DPA: Fines Imposed to Telecommunications Companies Due to Personal Data Breach and Illegal Data Processing | European Data Protection Board, 03.02.2022).

2.3.3 Schrems-II ja siirrot kolmansiin maihin

Monikansalliset yritykset joutuvat usein noudattamaan muitakin asetuksia GDPR-asetusten lisäksi. Näitä ovat esimerkiksi CCPA (Kalifornia) APPI (Japani), PIPL (Kiina) ja LGPD (Calzada, 2022; Erickson, 2019; Pantos, 2021). Eri asetusten vaatimukset voivat poiketa paljonkin toisistaan, joten samat käytännöt, jotka ovat jossain maassa vaatimusten mukaisia, voivat muualla olla riittämättömiä. Esimerkiksi CCPA ei vaadi samalla tavalla käyttäjien suostumusta tietojen käsittelyyn ja kansainvälisesti toimivien yritysten onkin huomioitava yhteensovittaa liiketoimintansa noudattamaan erilaisia määräyksiä. (Jordan, 2022, 261–263) Haasteet eivät kuitenkaan koske pelkästään monikansallisia yrityksiä. Monet suomalaisetkin yritykset käyttävät erilaisia kansainvälisiä palveluita, kuten pilvipalveluita, joissa tietoja käsitellään Euroopan ulkopuolella. Tietosuoja-asetuksessa määritellään henkilötietojen siirtoperusteet, jotka ovat edellytyksiä henkilötietojen siirroille EU/ETA:n ulkopuolelle. Näitä siirtoperusteita ovat Tietosuojavaltuutetun toimiston (2022) mukaan:

- Päätös riittävästä tietosuojan tasosta (päätöksen riittävästä tietosuojasta ovat saaneet esimerkiksi Japani, Argentiina, Israel ja Korean tasavalta)
- Vakiolausekkeet
- Yritystä koskevat sitovat säännöt
- Hyväksytyt käytännesäännöt tai sertifiointimekanismit
- Tietosuojaviranomaisen luvanvaraiset sopimuslausekkeet
- Erityistilanteita koskevat poikkeukset
- Viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline
- Viranomaisen tai julkisten elinten välisiin hallinnollisiin järjestelyihin sisältyvät säännökset.

Tärkeimpiä periaatteita olisi varmistaa EU:n tasoinen tietosuojan taso (Henkilötietojen Siirrot Euroopan Talousalueen Ulkopuolelle, 2022). Tätä tasoa ei esimerkiksi ole Yhdysvalloissa pystytty kokonaisvaltaisesti takaamaan (Rotenberg 2020, 145).

Schrems-II eli EU:n tuomioistuimen päätös C-311/18 Facebook Ireland ja Schrems 2020, vaikeutti henkilötietojen siirtämistä kolmansiin maihin entisestään. Schrems II -päätöksen (C-311/18) myötä kumottiin Yhdysvaltojen ja EU:n välinen Privacy Shield -viitekehys, joka ennen päätöstä takasi tiedonsiirron näiden välillä. Privacy Shield neuvoteltiin Safe Harbour -järjestelyn tilalle, kun sen pätevyys mitätöitiin lokakuussa vuonna 2015. Tämä tapahtui EU:n tuomioistuimen päätöksen C-362/14 Maximillian Schrems v Data Protection Commissioner eli Schrems I:n myötä. Molempien päätösten taustalla oli Euroopan komission näkemys, ettei Yhdysvalloissa toimivat organisaatiot kykene ilman lisätoimenpiteitä varmistamaan EU:n tasoista tietosuojaa. Yhdeksi keskeiseksi ongelmaksi tiedonsiirron kannalta Yhdysvaltoihin on noussut CLOUD act. CLOUD act tulee sanoista Clarifying Lawful Overseas Use of Data ja se antaa Yhdysvaltojen viranomaisille mahdollisuuden vaatia henkilötietoja yhdysvaltalaisilta yrityksiltä, vaikka tiedot olisi tallennettu Eurooppaan. Toisen ongelman tuo Foreign Intelligence Surveillance Act:in (FISA) pykälä 702, joka mahdollistaa yhdysvaltalaisten viranomaisten pääsyn muunmaalaisten henkilötietoihin, kun niitä tallennetaan tai siirretään Yhdysvaltoihin. Näiden lakien seurauksena yhdysvaltalaiset organisaatiot eivät voi taata, että Yhdysvaltojen viranomaiset eivät käyttäisi heidän keräämiään henkilötietoja ilman rekisteröityjen lupaa. (Rotenberg, 2020, 142–152; Costello, 2020, 1046–1059.)

Suuria yhdysvaltalaisia pilvipalveluntuottajia ovat esimerkiksi Google, Amazon Web Services ja Microsoft Azure. Schrems-II vaikuttaa näiden lisäksi esimerkiksi Metan ja Zoomin toimintaan. Suomen yrityksistä 75 % käyttää jollain tavalla hyödyksi pilvipalveluita (SVT, 2021). Ei ole kuitenkaan tietoa, kuinka suuri osa näistä palveluista on yhdysvaltalaisia. Schrems-II on lähiaikojen merkittävimpiä päätöksiä tietosuojan hallintaan liittyen. Tietosuojaneuvosto antoi päätöksen myötä uusia suosituksia siirtovälineitä täydentävistä suojatoimista (European Data Protection Board, 2020). Tietosuojaneuvoston lisävaatimuksista organisaatioille merkittävin oli vaatimus toteuttaa erillinen arvio hen-

kilötietojen siirrosta (eng. Transfer Impact Assesment, TIA) EU/ETA-alueen ulkopuolelle. Tämä tarkoittaa kaikkia EU/ETA-alueen ulkopuolisia maita, joilla ei ole komission päätöstä riittävästä tietosuojan tasosta eli myös Yhdysvaltoja. Organisaatiot, jotka käyttävät esimerkiksi Googlen tai Amazonin pilvipalveluita, joutuvat tekemään erillisen arvion henkilötietojen siirrosta tavallisen tietosuojaa koskevan vaikutustenarvioinnin lisäksi. Tilanteeseen saattaa kuitenkin olla helpotusta tulossa. Bidenin 07.10.2022 allekirjoittaman "Yhdysvaltojen signaalitiedustelutoiminnan turvatoimien tehostaminen" toimeenpanomääräyksen myötä Euroopan komissio on laatimassa uutta päätöstä riittävästä tietosuojan tasosta EU:n ja Yhdysvaltojen välillä (European Comission, 2022). Prosessi on vasta alussa ja on liian aikaista sanoa, seuraako tapahtumista helpotusta organisaatioille. Euroopan komission uskottavuudenkin vuoksi ei ole kannattavaa hyväksyä taas yhtä väliaikaista ratkaisua, joka myöhemmin kumotaan (Costello, 2020, 1059).

2.3.4 Tietosuojavastaava

Tietosuojavastaavan nimittäminen tuli uudeksi vaatimukseksi tietosuoja-asetuksen myötä. Jokaisen organisaation ei kuitenkaan tarvinnut lähtökohtaisesti nimittää erillistä tietosuojavastaavaa. Tietosuoja-asetuksen artiklassa 37 määritellään tietosuojan nimittämisestä ja asetetaan seuraavat käsittelyn ehdot, jolloin tietosuojavastaava olisi ainakin välttämätöntä nimittää:

a. käsittelyä suorittaa julkinen viranomainen tai elin lukuun ottamatta tuomioistuimia, jotka toimivat lainkäyttötehtävissä;
b. rekisterinpitäjän tai käsittelijän ydintoimintaan kuuluu luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi käsittelyä, joka edellyttää rekisteröityjen laajaa, säännöllistä ja järjestelmällistä seurantaa; tai
c. rekisterinpitäjän tai käsittelijän ydintoimintoihin kuuluu artikla 9 mukaisten erityisluokkien tai artiklassa 10 viitattujen rikostuomioiden ja rikkomuksiin liittyvää henkilötietojen käsittelyä.

Artiklassa 37 myös huomautetaan, että tietosuojavastaavan ammatillisten ominaisuuksien ja tietosuojalainsäädännön asiantuntemuksen on oltava riittävällä tasolla suorittaakseen artikla 39 määritellyt tehtävät. Artiklassa 39 määriteltyjä tehtäviä tietosuojavastaavalle on esimerkiksi neuvoa rekisterinpitäjää ja käsittelijää henkilötietojen käsittelyyn liittyen, seurata tietosuoja-asetuksen noudattamista organisaatiossa, valvoa tietosuojaa koskevien vaikutustenarviointien toteutumista ja yhteistyön tekeminen valvontaviranomaisen kanssa. Tietosuoja-asetuksen artiklassa 38 määritellään tietosuojavastaavan asema. Artiklan on tarkoitus luoda suojaa ja tukea tietosuojavastaavalle. Organisaation on asetuksen mukaan tarjottava tietosuojavastaavalle resurssit, joiden avulla hän voi täyttää artiklassa 39 määritellyt tehtävät, eikä tietosuojavastaavaa saa erottaa tai rangaista tehtäviensä hoitamisesta. (Euroopan parlamentti ja Euroopan neuvosto, 2016).

Tietosuojavastaavalla on usein muitakin tehtäviä, mutta artiklan 38 mukaan nuo tehtävät eivät saa aiheuttaa eturistiriitaa (Euroopan parlamentti ja Euroopan neuvosto, 2016). Monissa tapauksissa tietosuojavastaava voi olla organisaation ainut tietosuoja-asiantuntija. Tästä syystä oletettavasti ainakin osa tutkielmaan osallistuvista haastateltavista toimii tai on toiminut tietosuojavastaavana. Vaatimus tietosuojavastaavan nimittämisestä tuo organisaatioille selvyyttä tietosuojan hallinnan vastuiden jakamiseen, mutta toisaalta vaatimus tuo haasteita niin organisaatioille kuin myös tietosuojavastaaville. Organisaatioille voi olla haastavaa määritellä, onko tietosuojavastaavalla tarvittavat kompetenssit. Lachaud (2014, 201–202) päätteli jo ennen tietosuoja-asetuksen voimaantuloa, että tietosuojavastaavilla tulisi olla sertifiointi, jotta he voivat työskennellä virallisesti tietosuoja-asiantuntijoina. Vielä ainakaan sertifiointi ei ole EU:n tasolla pakollista tietosuojavastaaville, vaikka erilaisia sertifiointeja tietosuoja-asiantuntemuksesta on mahdollista suorittaa. Eggl (2019) nostaa mahdollisiksi haasteiksi myös resurssoinnin ja tietosuojavastaavan aseman organisaatiossa; ulkoinen vai sisäinen? Kokopäiväinen vai osa-aikainen? Hierarkkinen asema organisaatioissa? Tämän tutkielman avulla on mahdollista saada tarkempaa tietoa siitä, minkälaisia haasteita tietosuojavastaavat kokevat työssään.

2.3.5 Tietoturvaloukkaukset

Tietosuoja-asetuksen myötä rekisterinpitäjille tuli uusia vaatimuksia myös tietoturvaloukkauksiin liittyen. Tietosuoja-asetuksen artiklassa 33 määritellään tietoturvaloukkausten ilmoittamisesta valvontaviranomaisille ja artiklassa 34 määritellään tietoturvaloukkauksista ilmoittamisesta rekisteröidylle. Tietoturvaloukkauksista on ilmoitettava 72 tunnin kuluessa siitä, kun tieto tietoturvaloukkauksesta on saatu. Ilmoitusta tietoturvaloukkauksesta ei tarvitse tehdä, jos loukkaus ei todennäköisesti aiheuta luonnollisen henkilön oikeuksiin ja vapauksiin liittyvää riskiä. Raportointivaatimus koskee kaikkia organisaatioita, jotka käsittelevät henkilötietoja. Tietoturvaloukkauksia ovat henkilötietojen luvaton muokkaaminen, luovuttaminen tai tuhoaminen. Myös luvaton pääsy henkilötietoihin lasketaan tietoturvaloukkaukseksi. Tietoturvaloukkauksessa on vähintään mainittava seuraavat asiat:

- Kuvaus tietoturvaloukkauksesta, jos mahdollista sisältäen rekisteröityjen ryhmät, henkilötyyppien ryhmät, sekä arvioitu lukumäärä.
- Tietosuojavastaavan nimi ja yhteystiedot lisätietoa varten.
- Tietoturvaloukkauksen todennäköiset seuraamukset.
- Kuvaus siitä, mitä toimenpiteitä rekisterinpitäjä on tehnyt tai suunnitellut tietoturvaloukkauksen johdosta, sekä toimenpiteet riskien vähentämiseksi.

Tietoturvaloukkauksiin liittyvät tapahtumat voivat johtua esimerkiksi hakkeroinnista, hävinneistä tai varastetuista tiedonsiirtovälineistä tai inhimillisistä virheistä. Seurauksia tietoturvaloukkauksesta voivat olla esimerkiksi identiteettivarkaus, salassa pidettävien henkilötietojen paljastuminen tai maineen vahin-

goittuminen. (Tietoturvaloukkaukset, 2022; Euroopan parlamentti ja Euroopan neuvosto, 2016; Tietosuojaryhmä, 2017).

Tietoturvaloukkauksista tiedottamisen tarkoitus on parantaa entisestään luonnollisten henkilöiden tietosuojaa. Tiedottaminen mahdollistaa tietoturvaloukkauksen kohteeksi joutuneen henkilön varautumaan tapahtumasta johtuviin haittoihin itse, esimerkiksi vaihtamalla salasanaa (Alunge, 2021, 176; Kaya, 2021, 207). Organisaatioille vaatimus tietoturvaloukkauksista ilmoittamisesta tarkoittaa myös haasteita ja uusien toimintatapojen omaksumista. Alunge (2021, 173) nostaa tutkimuksessaan haasteeksi, että rekisterinpitäjille ja käsittelijöille jää vastuu määrittää milloin tietosuojaloukkauksesta täytyy ilmoittaa loukkauksen kohteelle tai tietosuojaviranomaiselle. Tietosuojaryhmä (2017) on pyrkinyt luomaan selvyyttä antamalla suuntaviivoja tietoturvaloukkauksista ilmoittamiseen. Kaya (2021, 235, 239) tuo esille tutkimuksessaan, että organisaatioilla voi olla myös kannustimia jättää tietoturvaloukkauksista ilmoittamatta ja hävittää todisteet. Tietoturvaloukkauksista voi aiheutua esimerkiksi mainehaittaa, asiakkaiden menettämistä ja sakkoja (Pantelic, Jovic ja Krstovic, 2022, 12). Vakavien ja varsinkin lievempien tietoturvaloukkauksien yleisyys osoittaa, että organisaatioilla on vaikeuksia noudattaa tietosuoja-asetuksen vaatimuksia (Alhazmi & Arachchilage, 2021, 880).

2.3.6 Rekisteröidyn oikeudet ja tietopyynnöt

Tietosuoja-asetuksessa on määritetty rekisteröidyn oikeudet, jotka organisaatioiden on otettava huomioon. Tietosuoja-asetuksen artiklat 15–18 ja 20–21 säätelevät rekisteröidylle kuusi erilaista oikeutta henkilötietoihinsa liittyen. Näistä yksi tärkeimmistä on artikla 15 mukainen rekisteröidyn oikeus saada pääsy tietoihinsa. Rekisteröidyllä on oikeus tämän artiklan mukaan saada tieto rekisterinpitäjältä siitä, käsitelläänkö hänestä tietoja vai ei. Lisäksi jos tietoja käsitellään, on hänellä oikeus saada tiedot kirjallisessa tai sähköisessä muodossa. Artikla 16 määrittää rekisteröidylle oikeuden tietojen oikaisemiseen. Se tarkoittaa, että rekisteröidyllä on oikeus saada mahdollisimman nopeasti rekisterinpitäjä korjaamaan väärät ja puutteelliset tiedot. Oikeudesta tietojen poistamiseen säädetään artiklassa 17. Rekisteröidyllä on oikeus pyytää tietojensa poistamista. Rekisterinpitäjän on myös poistettava tiedot, jos artikla 17 kohdan 1 a)-f) -ehdoista jokin täyttyy, ellei rekisterinpitäjällä ole artikla 17 kohdan 3 a)-e) mukaisia esteitä poistamiselle. Artiklan 18 mukainen oikeus käsittelyn rajoittamiseen tulee kyseeseen, jos rekisteröity kiistää tietojensa aitouden, käsittely ei noudata lainsäädäntöä, tietoja ei enää tarvita alkuperäiseen tarkoitukseen tai käsittelyä on vastustettu artiklan 21 mukaisesti. Artikla 21 sisältää vastustamisoikeuden, jonka mukaan rekisteröidyn on henkilökohtaisiin syihin vedoten mahdollista vastustaa henkilötietojensa käsittelyä. Tietosuoja-asetuksen määrittelemä oikeus artiklassa 20 liittyy rekisteröidyn oikeuteen siirtää tiedot järjestelmästä toiseen. Tämä mahdollistaa rekisteröityjen tietojen siirtämisen rekisterinpitäjältä toiselle rekisterinpitäjälle, jos sille ei ole mitään muuta estettä. (Euroopan parlamentti ja Euroopan neuvosto, 2016.)

Näiden oikeuksien on ollut tarkoitus vahvistaa rekisteröityjen tietosuojaa ja valtaa omiin henkilötietoihinsa. Tarkemmat ja lisääntyneet vaatimukset ovat tuoneet kuitenkin haasteita organisaatioille. Ausloos ja Dewitte (2018, 16-18) huomasivat tutkimuksessaan, että organisaatioilla oli vaikeuksia noudattaa rekisteröityjen oikeutta saada pääsy omiin henkilötietoihinsa ja he löysivät neljä syytä, jotka aiheuttivat näitä haasteita:

1. Tietoisuuden puute
2. Organisoinnin puute
3. Motivaation puute
4. Harmonisoinnin puute

Ratkaisuksi näihin ongelmiin Ausloos ja Dewitte ehdottavat kehittämään organisaation tietosuojapolitiikkoja, tekemään valmiita malleja tietopyynnöille ja teknisten ratkaisujen muokkaamisen niin, että pääsy tietoihin helpottuu (2018, 24–25). Varsinkin tietopyynnöt voivat olla organisaatioille haasteellisia ja vaatia paljon resursseja. Tätä esiintyy etenkin tapauksissa, joissa erilaisia henkilötietoja on paljon ja niitä käsitellään useissa erilaisissa tietojärjestelmissä.

3 APUA TIETOSUOJAN HALLINTAAN

Tässä luvussa käsitellään yleisesti tietosuojan hallintaa ja siihen liittyviä ratkaisuja tai työvälineitä. Viitekehyksien avulla esitetään enemmän organisatorisia tapoja hallita tietosuojaa, kun taas teknisiä tietosuojan hallinnan apuvälineitä käsittelevässä osassa katsotaan, minkälaisia teknisiä vaihtoehtoja on luotu tietosuoja-asetusten noudattamisen helpottamiseksi. Tietosuojan hallinnalla tarkoitetaan kaikkia niitä keinoja, joilla organisaatiot pyrkivät hallitsemaan henkilötietojen käyttöä ja vastaamaan tietosuoja-asetuksien vaatimuksiin.

3.1 Organisatorisia apuvälineitä tietosuojan hallintaan

Erilaisia viitekehyksiä ja muita apuvälineitä on luotu auttamaan monimutkaisen tietosuojakokonaisuuden hallitsemista. Tässä kappaleessa esitetään näitä organisatorisia apuvälineitä ja pohditaan niiden soveltumista tietosuojan hallintaan organisaatioissa. IT Governance Privacy Teamin (2020, 83) mukaan erilaisia viitekehyksiä on useita, joista voi valita organisaatiolleen sopivan. Kuvio 1 havainnollistaa tietosuojan viitekehyksien kolme tärkeintä osa-aluetta.

Kuvio 1 Tietosuojan viitekehyksen avainalueet IT Governance Privacy Team (2020, 84) mukaan

Nämä kolme avainaluetta tulisi olla sisällytettynä tietosuojan viitekehyksessä, jotta se olisi kattava ja vaatimustenmukainen. Kyseisten avainalueiden painotus voi kuitenkin vaihdella viitekehyksestä toiseen. Kaikki viitekehykset eivät ole välttämättä tarkoitettu kokonaisvaltaiseen tietosuojan hallintaan, vaan keskittyvät enemmän johonkin tiettyyn osa-alueeseen.

U.S. National Institute of Standards and Technology (NIST) on luonut viitekehyksen (2020, 1) tietosuojan hallinnalle, jonka olisi tarkoitus olla yleispätevä organisaation koosta, käytettävistä teknologioista, lainsäädännöstä tai alasta riippumatta. Viitekehyksen lähtökohta on riskilähtöisyys, joka painottuu riskien tunnistamiseen ja vähentämiseen. NIST ei tarjoa sertifikaatteja tai takaa täyttä säännöstenmukaisuutta viitekehystä seuraaville organisaatioille. Tarkoitus on NIST:n (2020 mukaan auttaa vastaamaan kysymykseen:

> ”Kuinka otamme huomioon yksilöihin kohdistuvat vaikutukset, kun kehitämme järjestelmiämme, tuotteitamme ja palveluitamme?"

Erilaisilla tietosuojan kypsyys- tai kehitysasteilla olevien organisaatioiden vastaus voi vaihdella. NIST:n viitekehystä ei tarvitse käyttää kokonaisena, vaan siitä voi oman tarpeen mukaisesti valita osia, joilla voidaan muun muassa tehdä

kuiluanalyysia. Viitekehykseen kuuluu kolme osaa: ydin, profiilit ja toteutustasot. Ydin on nimensä mukaisesti viitekehyksen pääsisältö, joka on jaettu viiteen eri pääfunktioon:

1. Tunnista
2. Hallinnoi
3. Kontrolloi
4. Kommunikoi
5. Suojele

Funktiot on jaettu Taulukon 1 mukaisesti kategorioihin, jotka jakavat kokonaisuuden tarkempiin, hallittaviin kokonaisuuksiin. Kategoriat jaetaan vielä alakategorioihin, jotka kuvaavat tarkempia tuloksia tai toimia. Taulukossa 1 esitetään osa NIST.n viitekehyksestä uudelleen tehtynä.

Taulukko 1 Osa tietosuojaviitekehyksen ydintaulukosta (NIST, 2020, 19–27)

Funktio	**Kategoria**	**Alakategoria**
Tunnista: Kehitä organisatorista ymmärtämistä yksilöiden tietojenkäsittelyyn liittyvien tietosuojariskien hallitsemiseksi.	Riskiarviointi: organisaatio ymmärtää tietosuojariskit yksilöille ja miten nämä riskit voivat aiheuttaa jatkovaikutuksia organisaation toiminnoille, tehtäville, maineelle, työntekijöille, kulttuurille ja muille riskienhallinnan prioriteeteille.	Järjestelmiin, tuotteisiin ja palveluihin liittyvät kontekstuaaliset tekijät ja tietotoiminnot tunnistetaan (esimerkiksi yksilöön liittyvät arkaluontoiset henkilötiedot).
		Tietojen analyyttiset syötöt ja lähdöt tunnistetaan ja arvioidaan harhojen varalta.
		Mahdolliset ongelmalliset datatoiminnot ja niihin liittyvät ongelmat tunnistetaan.
		Todennäköisyyksiä ja vaikutuksia käytetään riskien määrittämiseen ja priorisoimiseen.
		Riskien vastatoimet tunnistetaan, priorisoidaan ja toteutetaan.

Taulukko 1 mukaisesti NIST on jakanut muutkin funktiot pienempiin alakategorioihin, jotka ovat tietosuojan näkökulmasta kattava joukko toimenpiteitä tietosuojan riskien hallintaan. Toinen osa, profiilit, tarkoittavat valittuja osia ydinkokonaisuudesta, jolla kuvataan esimerkiksi organisaation nykytilannetta tai tavoitetilaa tietosuojatoimintoihin liittyen. Toteutustasot taas

tarkoittavat eri tasoja siitä, kuinka kokonaisvaltaisesti tietosuojaa lähdetään toteuttamaan. Tasoa valittaessa on otettava huomioon organisaation kypsyysaste ja resurssit. Tasoja on neljä; osittainen, riskitietoinen, toistettava ja mukautuva. (NIST, 2020, 1–30.)

NIST:n tietosuojan viitekehys kattaa myös tietoturvan osa-alueita ja sisältää paljon samoja aspekteja kuin NIST:n tietoturvan viitekehys (2018). Carter, Kroll ja Bret Michael (2021, 9–13) huomauttavatkin, että samankaltaisuuden vuoksi viitekehykset voisi yhdistää yhdeksi kokonaisvaltaisemmaksi kokonaisuudeksi. Yleispätevän viitekehyksen heikkouksiksi nousevat sen suuripiirteisyys ja numeraalisten mittareiden puuttuminen (Carter ym. 2021, 9–13). Tarkkoja ohjeita ei tarjota, mikä mahdollistaa käytön lainsäädännöstä tai alasta riippumatta. Tästä syystä viitekehys jättää paljon myös implementoijan oman harkinnan ja käsityksen varaan. Tästä syystä NIST:n tietosuojan viitekehys on liian suuripiirteinen ja jää vajaaksi tietosuojan riskien hallinnan kokonaisvaltaisesta käsittelemisestä (Carter ym. 2021, 13). Tarkempia ohjeita NIST tarjoaa tietosuojan ja tietoturvan kontrollien suhteen toisessa julkaisussaan *Security and Privacy Controls for Information Systems and Organizations* (Nist, 2020b). Kontrolleihin keskittyvä ohjeistus on teknisempi sekä vahvasti tietojärjestelmiin ja tietojenkäsittelyyn painottuva, eikä ainakaan yksin toimi kokonaisvaltaisena tietosuojan hallinnan viitekehyksenä (Serrado, Pereira, Mira Da Silva & Scalabrin Bianchi, 2020, 241).

Yritys nimeltä Nymity (2018) on luonut viitekehyksen todistettavalle GDPR-vaatimustenmukaisuudelle. Viitekehys on luotu samana vuonna kuin GDPR tuli voimaan. Se on voinut olla yrityksille silloin hyvinkin arvokas, sillä siinä kerrotaan melko yksityiskohtaisesti, minkälaisia teknisiä ja organisatorisia toimenpiteitä tulee suorittaa vaatimustenmukaisuuden täyttämiseksi. Näiden lisäksi Nymity on lisännyt suositeltavia toimenpiteitä vielä vahvemman osoitusvelvollisuuden takaamiseksi. Toimenpiteet myös perustellaan viitekehyksessä tietosuoja-asetuksen artikkelien kautta, jos ne ovat sovellettavissa. Nymity jakaa viitekehyksen kolmeentoista tietosuojan hallinnan kategoriaan:

1. Hallintorakenteen ylläpito
2. Henkilötietojen tietovarastojen ja tiedonsiirtomekanismien hallinta
3. Sisäisen tietosuojakäytännön ylläpito
4. Tietosuojan sisällyttäminen prosesseihin
5. Koulutuksen ja tietoisuuden ylläpito
6. Tietoturvariskien hallinta
7. Kolmansien osapuolien riskien hallinta
8. Tietosuojaselosteiden ylläpito
9. Yksilöiden pyyntöihin ja valituksiin vastaaminen
10. Uusien toimintakäytänteiden monitorointi
11. Tietosuojaloukkausten hallintaohjelman ylläpito
12. Tietojenkäsittelyn käytäntöjen monitorointi
13. Ulkoisten kriteerien seuranta

Tietosuojan hallinnan kannalta kategorioiden ja niihin liittyvien toimenpiteiden lista on hyvin kattava. Viitekehys on 70-sivuinen ja se käyttää enemmän tilaa sen selittämiseen, miksi jotain tehdään kuin miten jotain tehdään. Esimerkiksi tietosuojapolitiikkaa koskevassa kohdassa kerrotaan vain hyvin laveasti, mitä tietosuojapolitiikkaan tulisi sisällyttää. Nymityn viitekehys on kuitenkin hyvä lähtökohta sille, mitä kaikkea tulisi ottaa huomioon. Valitettavasti viitekehyksestä ei ole myöskään päivitettyä versiota, joka ottaisi huomioon viime vuosien muutokset tietosuojalainsäädännössä. (Nymity inc., 2018).

Myös ISO/IEC 27701:2019 (ISO 27701) toimii viitekehyksenä tietosuojan hallinnalle. ISO 27701 on tietoturvastandardien ISO/IEC 27001:2017 (ISO 27001) ja ISO/IEC 27002:2022 (ISO 27002) lisäosa, joka keskittyy tietosuojan hallintajärjestelmän luomiseen organisaatiossa (International Organization for Standardization, 2019). ISO 27001 ja 27002 standardit tietoturvan hallintajärjestelmälle ovat luoneet standardisointiin erikoistuneet International Organization for Standardization (ISO) ja International Electrotechnical Commission (IEC). Standardit ovat yleisesti hyväksyttyjä parhaita käytänteitä, joiden on tarkoitus määrittää vaatimukset siihen, kuinka kehittää, ylläpitää ja implementoida tietoturvajärjestelmä yrityksen koosta tai alasta riippumatta (Culot, Nassimbeni, Podrecca & Sartor, 2021, 77). Yritykset voivat todistaa täyttävänsä ISO 27001 -vaatimukset ja hakea sertifikaattia. Culot kollegoineen (2021, 77) huomauttaa, että monet yritykset odottavat yhteistyökumppaneiltaan tätä sertifikaattia takeeksi tietoturvallisuuden riittävästä tasosta. Tämä sertifikaatti koskee kuitenkin vain tietoturvaa, eikä kerro, toimiiko yritys tietosuoja-asetuksien mukaisesti. Vaikka ISO 27001 ja ISO 27002 standardien toteuttaminen on oikea suunta GDPR-vaatimusten täyttämiseksi, on niiden rinnalle luotu tietosuojaan keskittyvä ISO 27701.

Aikaisemmin on ilmestynyt tietosuojaviitekehykseksi kutsuttu ISO/IEC 29100:2011 (ISO 29100). Laajempi, 66-sivuinen ISO 27701 sisältää kartoituksessaan kuitenkin myös ISO 29100 sisällön. Kummastakaan ei ole kuitenkaan saatavilla samanlaista sertifikaattia, joka näyttäisi, että organisaatio toimii tietosuoja-asetuksien mukaisesti. ISO 27701 on kuitenkin kattava, sillä se sisältää kartoituksen standardeista ISO/IEC 27018, ISO/IEC 29151 ja EU:n yleisestä tietosuoja-asetuksesta. Tarkoitus olisi, että ISO 27701 olisi mahdollisimman yleispätevä ohjeistus koskemaan erilaisia tietosuoja-asetuksia, mutta se on rakennettu erityisesti EU:n yleistä tietosuoja-asetusta silmällä pitäen. Ohjeistus keskittyy tietosuojajärjestelmän kehittämiseen (PIMS) ja täydentämään ISO 27002 ja ISO 27002 ohjeistusta erityisesti henkilötietojen käsittelyyn liittyen. Lisäosa onkin nimensä mukaisesti lisäosa ja tämän vuoksi organisaation on implementoitava ISO 27001, 27002 ja 29100 standardeja saadakseen täyden hyödyn sen käyttämisestä. ISO 27701 keskittyy myös paljon tietoturvan alueelle. Näistä syistä lisäosaa voi olla hankalaa ja työlästä implementoida tietosuojan hallintaan. (International Organization for Standardization, 2019.)

Tutkielmaa kirjoitettaessa on myös ilmestynyt ensimmäinen virallinen EDPB:n (tietosuojaneuvosto) hyväksymä GDPR-sertifikaatti (Howard, 2022). Tietosuoja-asetuksen artiklassa 42 on määritelty mahdollisuus ottaa käyttöön

tietosuojaa koskevia tietosuojasinettejä ja -merkkejä sekä sertifiointimekanismeja (Euroopan parlamentti ja neuvosto 2016, artikla 42). Kuitenkaan artikla 42 kohdan 5 mukaista tietosuojaneuvoston hyväksymää sertifiointia ei ole ennen ollut käytössä (Howard, 2022). Muita epävirallisia tietosuojasinettejä tai standardeja on ollut olemassa. Näiden vaikutus perustuu yhteiseen ymmärrykseen niitä toimittavien toimijoiden luotettavuudesta. Esimerkkinä voisi olla ISAE 3000, joka on yksi yleisimmin käytetty varmennusstandardi (Simnett, 2012, 90). ISAE 3000 -standardin myöntää IFAC (International Federation oF Accountants). Standardilla voidaan varmistaa ulkoisen auditoinnin kautta, että organisaatio toimii omien tietosuojaperiaatteidensa mukaan. Tämä ei kuitenkaan takaa, että organisaatio noudattaa varsinaisia tietosuoja-asetuksia. Tietosuojasinettejä tarjoaa esimerkiksi ePrivacy. Tietosuojasinetit ovat alan itsesääntelyyn perustuvia toimenpiteitä, joiden teho perustuu siihen, että ne ovat yleisesti tunnettuja ja arvostettuja. Tällöin voidaan olettaa sinetin omaavan organisaation hoitavan tietosuojan hallinnan hyväksyttävällä tavalla (Rodrigues, Barnard-Wills, De Hert & Papakonstantinou, 2016, 1–2). Varsinaista tietosuojaneuvoston hyväksyntää näillä sineteillä ei kuitenkaan ole ja ePrivacyn sivuilla mainitaankin, ettei heillä ole mahdollista myöntää sertifiointia artikla 42 kohdan 5 mukaisesti (Note GDPR Certification - ePrivacy).

Rodrigues kollegoineen (2016, 8–18) tutki GDPR-sertifioinnin mahdollisia implementointitapoja jo ennen tietosuoja-asetuksen voimaantuloa. He huomauttivat, että tietosuojasinettien heterogeenisyys ja monimuotoisuus ovat aiheuttaneet hämmennystä organisaatioissa. Artiklan 42 sertifiointimahdollisuus voisi tuoda ratkaisun tähän ongelmaan. Implementoinnin vaihtoehdoiksi he tunnistivat neljä eri vaihtoehtoa:

1. GDPR-sertifiointijärjestelmän rohkaiseminen ja tukeminen
2. Sertifiointielinten akkreditointi
3. Kansallisten tietosuojaviranomaisten hoitamat sertifioinnin
4. Edellä mainittujen vaihtoehtojen rinnakkaiselo

Jokaisessa vaihtoehdossa on hyvät ja huonot puolensa. GDPR-sertifikaatti olisi parhaimmassa tapauksessa kuin yhtenäinen tietosuojasinetti, joka pätisi maasta ja alasta riippumatta. (Rodrigues ym. 2016, 8–20.)

Vasta kuusi vuotta myöhemmin on päästy tilanteeseen, jossa GDPR-sertifikaatti on viimein otettu käyttöön. Tietosuojaneuvosto on hyväksynyt 10.10.2022 Europrivacyn sertifiointikriteerit, minkä takia voidaan ottaa käyttöön yksi yhteinen sertifikaatti (The European Data Protection Board, 2022). Rodriguesin ja kumppaneiden (2016) vaihtoehdoista Europrivacy -sertifioinnin implementointi on lähimpänä vaihtoehtoa 2. ''sertifiointielinten akkreditointi''. Europrivacylla on kumppaneita, joista osa on hyväksyttyjä sertifiointielimiä ja osa hyväksyttyjä konsultti- ja lakiyrityksiä (Europrivacy). Konsultti- ja lakiyritykset auttavat sertifioinnin implementoinnissa organisaatioissa ja sertifiointielimet hoitavat varsinaisen sertifiointiprosessin. Europrivacyn sertifiointimenetelmä perustuu aikaisemmin kehitteillä olleeseen GDPR-CARPA-sertifiointiin, jolle haettiin julkista konsultaatiota 2021 (Commission Nationale pour la Protec-

tion des Données, 2021). Sertifiointi on ISO-yhteensopiva sekä hyödyntää ISO/IEC 17065 ja ISO 17021-1 -sertifikaatteja (Europrivacy: The First Certification Mechanism to Ensure Compliance With GDPR, 2022). Sertifikaatti on myös yhteensopiva aiemmin mainitun ISO 27001-sertifikaatin kanssa (Europrivacy).

Europrivacy -sertifiointi on siis ensimmäinen koko Euroopan unionin laajuinen EDPB:n hyväksymä sertifikaatti. Sertifiointia ei haeta tietylle organisaatiolle, palvelulle tai tuotteelle vaan henkilötietojen käsittelytoimelle. Tietyn tai tiettyjen käsittelytoimien voidaan Europrivacy -sertifikaatin avulla osoittaa olevan GDPR:n mukaisia. Näitä valittuja käsittelytoimia kutsutaan arvioinnin kohteiksi (Eng, Target of Evaluation, ToE). Tarkoituksena on valita muutama kohde ja alkaa laajentamaan niistä muihin käsittelytoimiin. Vaikka organisaatio ei voi hankkia sertifikaattia virallisesti itselleen, voi se sertifioida kaikki käsittelytoimet, jolloin se kattaa kaiken, mitä yritys tekee. Käsittelytoimien lähtökohta on valittu siitäkin syystä, että erilaisissa käsittelytoimissa voidaan käyttää eri teknologioita ja niitä saattaa koskettaa erillinen lainsäädäntö. Europrivacy ottaa huomioon tämän ja tukee uusienkin teknologioiden kuten tekoälyn, lohkoteknologioiden ja asioiden internetin (eng. Internet Of Things, IOT) käyttämistä. Europrivacy pyrkii olemaan sertifiointimenetelmä, jolla on vahva viitekehys, mutta joka pystyy muovautumaan erillisten yritysten tarpeisiin. Sertifioinnissa on kolme vaihetta:

1. Valmisteluvaihe
2. Itsenäinen arviointi- ja sertifiointivaihe
3. Valvontavaihe

Ensimmäisessä vaiheessa valitaan arvioinnin kohde ja kerätään siihen liittyvää dokumentointia, jolla pyritään osoittamaan, että kyseinen käsittelytoimi on Europrivacyn sekä tietosuoja-asetuksen kriteerien mukainen. Myös kansallinen lainsäädäntö otetaan huomioon ja sitä arvioidaan kansallisten velvoitteiden vaatimustenmukaisuuden arviointiraportin (eng. National Obligation Conformity Assesment Report, NORCA) avulla. Toisessa vaiheessa sertifiointielin arvioi arvioinnin kohteen kriteerienmukaisuuden. Tässä vaiheessa auditoija voi vielä huomauttaa poikkeavuuksista ja niihin liittyvää dokumentointia voidaan korjata. Tässä vaiheessa tehdään myös päätös siitä, hyväksytäänkö sertifiointi. Sertifikaatti on voimassa kolme vuotta ja kolmannessa vaiheessa valvotaan 12 kuukauden välein, että toimet ovat vieläkin tietosuoja-asetuksen mukaisia. Kolmen vuoden päästä on mahdollisuus uusia sertifiointi. Sertifiointi vaatii, että organisaatio seuraa myös uusia säädöksiä tietosuojaan liittyen. (The First EU-wide GDPR Certification Scheme – Europrivacy (TM/®) Explained in 5 Questions | Timelex, 2022.)

Toisena vaihtoehtona osoittaa, että riittäviä organisatorisia ja teknisiä toimia toteutetaan organisaatiossa, on hyväksyttyjen käytännesääntöjen todistettu noudattaminen. Artiklassa 40 määritellyt käytännesäännöt ovat joukko ohjeita, jotka hahmottelevat tietyn toimialan käyttäytymistä ja toimia (Euroopan parlamentti ja Euroopan neuvosto, 2016). Käytännesäännöt ovat tarkemmin suunnattuja ja räätälöityjä ohjeistuksia tietyille toimialoille, joiden avulla toimialan or-

ganisaatiot voivat todistaa tietosuoja-asetuksen noudattamisen tietyllä henkilötietojen käsittelyn osa-alueella. Ensimmäinen EDPB:n (Tietosuojaneuvosto) hyväksymä käytännesääntö oli pilvipalveluihin keskittyvä EU Cloud Code of Conduct. Toukokuussa 2021 EDPB:n hyväksymä käytännesääntö kattaa kaikki erilaiset pilvipalvelut eli SaaS, Paas ja IaaS. EU Cloud Code of Conductin noudattamisen seuraamisessa käytetään sekä itsenäistä että ulkoista tarkkailua. Käytännesäännön todistettu noudattaminen voisi tuoda organisaatioille helpotusta Schrems II -tuomion jälkeisessä epäselvässä tilanteessa. (*About EU Cloud CoC: EU Cloud CoC*, 2022.)

Vaikka tietosuojan hallintaan on pyritty luomaan erilaisia yleispäteviä viitekehyksiä, ei mikään näistä ole vielä saanut maailmanlaajuista suosiota. Yleisesti hyväksyttyjen käytänteiden ja viitekehysten puuttuminen voi johtaa tilanteeseen, jossa samoja asioita voidaan tehdä eri organisaatioissa eri tavoilla. Tietosuojan hallinnan moninaisuus voi heikentää jopa tietosuoja-asetuksen vaikutusta, sillä yleisesti hyväksyttyjen käytänteiden sijasta organisaatiot voivat nähdä tietosuojan hallinnan eteen vain mahdollisimman pienen vaivan. Europrivacyn sertifikaatti voi tuoda muutosta alalle, sillä se voi parhaimmillaan yhtenäistää organisaatioiden tietosuojan hallintaa. Samalla sillä on mahdollisuus myös vähentää organisaatioiden jatkuvaa osoitusvelvollisuutta käsittelytoimien säännöstenmukaisuudesta (Europrivacy). Vielä on epäselvää, onko sertifiointi hyväksyttävä siirtoperuste kolmansien maiden tiedonsiirrolle. Toimivien sertifikaattien ja viitekehyksien osa hyödyistä tulee niiden suuresta tunnettavuudesta ja korkeasta käyttöasteesta. Europrivacy -sertifikaatin vaikutuksia on tässä vaiheessa mahdotonta arvioida, sillä järjestely on niin uusi, ettei yksikään organisaatio tätä tutkielmaa kirjoitettaessa ole vielä sertifikaattia onnistunut hankkimaan (Europrivacy).

3.2 Teknisiä apuvälineitä tietosuojan hallintaan

Tietosuoja-asetuksien vaatimusten myötä kasvanut tarve tietosuojan hallinnalle on ohjannut organisaatioita hakemaan erilaisia ulkoisia ratkaisuja, jotka helpottavat ja ohjaavat vaatimusten täyttämistä. Erilaisia ratkaisuja tarjotaan esimerkiksi järjestelmien, viitekehyksien, ohjeistuksien ja alustojen muodossa. Monitulkintaisten ja muuttuvien säädöksien vuoksi yrityksille voi olla turvallista tukeutua palveluntarjoajiin, jotka tarjoavat samaa palvelua useille muille organisaatioille. Nämä palveluntarjoajat myös usein seuraavat tiiviisti, mitä alalla tapahtuu ja pystyvät nopeastikin reagoimaan vaadittaviin muutoksiin. Esimerkkinä turvallisesta vaihtoehdosta evästeiden hallintaan Pantelic, Jovic ja Krstovic (2022, 2) nostavat erillisten tietosuojahallintaohjelmistojen käyttämisen.

Tietosuojan hallinnan haasteet on huomioitu laajasti niin tutkijoiden kuin myös organisaatioiden toimesta. Esimerkiksi Gil Pérez, Huertas Celdran, Mlakar, Alcaraz Calero, Garcia Clemente, Martinez Perez ja Bhuiyan (2020) ovat ehdottaneet ratkaisuksi heidän kehittämäänsä PROTECTOR-alustaa, joka toisi

yrityksille kokonaisvaltaisemman hallinnan tietosuojaan tarjoten samalla rekisteröidyille paremmat mahdollisuudet hallita heidän henkilökohtaisten tietojen käyttöä. Kokonaisvaltaista ratkaisua on pyritty luomaan myös EU:n Data gov-Ernance For supportiNg gDpr (DEFeND) -projektilla (DEFeND: The Data Governance Framework for Supporting GDPR). DEFeND -alustan tavoite on auttaa tietosuojan noudattamista tarjoamalla tukea suostumusten hallintaan, tietosuoja-analyysiin, tietoturvariskeihin ja tietoturvaloukkauksiin liittyen sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden mukaan (Tsohou, Magkos, Mouraditis, Chrysoloras, Piras, Pavlidis, Debussche, Rotoloni & Gallego-Nicasio Crespo, 2020; Piras, Ghazi Al-Obeidallah, Praitano, Tsohou, Mouraditis, Gallego-Nicasio Crespo, Bernard, Fiorani, Magkos, Castillo Sanz, Pavlidis, D'Addario & Giovanni Zorsino, 2019). Tarjolla on myös apuvälineitä, joiden avulla voidaan kartoittaa oman tietosuojan kehityskohteita. Näistä yksi on Tietosuojavaltuutetun toimiston ja Tietoyhteiskunnan Kehittämiskeskus RY:n yhteinen GDPR2DSM -hanke, joka on pyrkinyt auttamaan pieniä ja keskikokoisia yrityksiä luomalla tietosuojatyökalun, jonka avulla saa raportin suositeltavista toimenpiteistä parempaan tietosuojan hallintaan (Tietosuojatyökalu – Tietosuoja, 2022). Tietosuoja-asetuksien vaatimukset ovat aiheuttaneet tarvetta erilaisille ratkaisuille, jotka helpottavat ja ohjaavat vaatimusten täyttämistä. Tämän tarpeen tietosuojan paremmalle hallinnalle ovat huomanneet myös useat yksityiset palveluntarjoajat, jotka ovat tuoneet viime vuosien aikana runsaasti erilaisia teknisiä ratkaisuja tietosuojan hallintaan.

Vuodesta 2017 asti International Association of Privacy Professionals (IAPP) on julkaissut vuosittaisen ''IAPP Privacy Tech Vendor Raport'' -nimisen raportin, jossa esitellään mahdollisimman laajasti erilaisia tietosuojateknologiaa tarjoavia palveluntuottajia. Varsinkin GDPR-asetuksen voimaantulo on näkynyt tietosuojaratkaisujen räjähdysmäisessä kasvussa. Vuosi ennen GDPR-asetuksen voimaantuloa eli vuonna 2017, IAPP:in raportissa tunnistettiin 44 eri palveluntarjoajaa. Vuotta myöhemmin, GDPR-asetuksen voimaantulovuonna, luku oli kasvanut yli kaksinkertaiseksi sataan kahteenkymmeneenkahteen palveluntarjoajaan. Viimeisin raportti vuodelta 2021 tunnisti jo 365 erilaista palveluntarjoajaa. Merkittävä nousu ei johdu pelkästään GDPR-asetuksesta, vaan tietosuojaan liittyvät vaatimukset ovat ympäri maailmaa tiukentuneet ja vaativat yrityksiltä yhä suurempia satsauksia tietosuojan hallintaan. GDPR-asetuksen lisäksi useat muut uudemmat tietosuoja-asetukset, kuten Californian Consumer Privacy Act (CCPA) ja Brazilian General Data Protection Law (LGPD) ovat aiheuttaneet päänvaivaa myös yrityksille, jotka toimivat kokonaan EU:n ulkopuolella. Tietosuojan hallintaan liittyvät tarpeet eivät ole samoja kaikilla yrityksillä ja siksi myös palveluntarjoajien ratkaisujen laajuus ja kohdealueet vaihtelevat. IAPP-raportissa tuotteet on järjestetty kategorioittain sen mukaan, mitä tietosuojan hallinnan kohteita ne palvelevat. Palveluntarjoajien tarjonta vaihtelee kaikenkattavista GRC-ratkaisuista aina yhteen tiettyyn tietosuojan hallinnan kategoriaan keskittyviin ratkaisuihin asti. Joukosta löytyykin teknologia-alalla pitkään olleita teknologiajättejä ja konsulttitaloja, kuten IBM tai EY,

mutta myös muutamien ihmisten pyörittämiä uusia startupeja, kuten Privacy Map ja Preclusio. (Chiavetta & IAPP, 2021, 31–40)

IAPP Privacy Tech Vendor Report -raportissa (2021) tuotteiden kategorisointi on jaettu tietosuojaohjelman hallintaan ja yrityksen tietosuojan hallintaan liittyvien ominaisuuksien mukaan. Tietosuojaohjelman hallintaan liittyviä ominaisuuksia, joita ratkaisut tarjoavat ja joiden mukaan palveluntarjoajat on kategorisoitu, ovat raportin (2021, 7) mukaan:

- Arviointien hallinta
- Suostumusten hallinta
- Tiedon kartoittaminen
- Henkilötietokyselyiden hallinta
- Henkilötietoloukkauksiin vastaamisen hallinta
- Tietosuojatiedon hallinta
- Nettisivujen skannaus

Yrityksen tietosuojan hallintaan tarjottavien ratkaisujen ominaisuudet on kategorioitu IAPP-raportin (2021, 7) mukaan seuraavasti:

- Toiminnan seuranta
- Tietojen löytäminen
- Pseudonymisointi/anonymisointi
- Yritysviestintä

Kategorisointi kertoo myös tietosuojaan liittyvien haasteiden laajuudesta. Yrityksillä saattaa olla jo käytössä erilaisia työkaluja ja prosesseja, joten modulaariset ja muiden järjestelmien kanssa yhteensopivat tietosuojajärjestelmät olisivat toivottuja (Tsohou ym. 2020, 20). Modulaarisuus onkin tietosuojajärjestelmien palveluntuottajilla hyvin yleinen liiketoimintamalli. Lisäosat, moduulit, tietosuojasovellukset ja lisäpaketit, joita usein tarjotaan perusratkaisun päälle, antavat palvelunostajalle valinnanvaraa, eikä organisaatio joudu maksamaan turhaan ominaisuuksista, joita se ei tarvitse. Tämänkaltaisia liiketoimintamalleja on esimerkiksi Complyonilla, DPOrganizerilla, BigID:lla ja Mighty Trustilla (Complyon kotisivu, 2022; Dporganizer Pricing; BigID Inc, 2022; Mighty Trust | Pricing Plan). Palveluntuottajilla on myös usein erihintaisia paketteja erikokoisille yrityksille. Tämä on järkevää myös siksi, että EU:n tietosuoja-asetuksen mukaan suuremmilla yrityksillä on enemmän vastuita esimerkiksi käsittelytoimien raportointiin liittyen.

Organisaatioiden vaatimukset tietosuojajärjestelmille vaihtelevatkin paljon koosta, toimialasta ja tietosuojan hallinnan kypsyydestä riippuen. Tsohou kumppaneineen (2020, 15) tunnisti tutkimuksessaan 13 vaatimusryhmää tietosuojajärjestelmään liittyen:

1. GDPR-tietosuojasuunnitelman kehittäminen
2. Kolmansien osapuolien hallinta

3. Tietosuojavalitusten ja yksilön oikeuksien hallinta
4. Tietosuojahäiriöiden ja tietosuojaloukkausten hallinta
5. Sisäänrakennetun tietosuojan ja tietosuojan suunnittelun toteuttaminen
6. Tietojen pseudonymisointi/anonymisointi
7. Sääntelyn raportointivaatimusten täyttäminen
8. Kansainvälisten tiedonsiirtojen käsitteleminen
9. Tietoluettelon ja karttojen luominen
10. Tietosuojariskien arvioinnin (PIA/DPIA) suorittaminen
11. Käyttäjän suostumuksen hankkiminen ja hallinta
12. Sopivien teknisten ja organisatoristen turvatoimien valinta
13. Yleiset alustavaatimukset

Tsohoun tutkimusryhmän (2020, 15) listaus ei laajuudestaan huolimatta ole kaikenkattava ja vaatimusryhmiin sisältyy erilaisia alivaatimuksia, joihin liittyy vielä enemmän haluttuja toimintoja. Lisähaasteen tuo myös jatkuvasti muuttuva tietosuojalainsäädännön kenttä, joka luo uusia vaatimuksia tietosuojaratkaisuja tarjoaville tahoille. Esimerkiksi Schrems II -tuomion (C-311/18) myötä palveluntarjoajilta odotetaan tukea täydentäville suojatoimenpiteille kolmansien maiden siirtoihin liittyen, kuten tukea tietojen siirtoa kolmansiin maihin koskeville riskienarvioinnille (eng. Transfer Impact Assesment, TIA). Piras ja kumppanit (2019, 1–2) huomauttavatkin, ettei ole yhtä ratkaisua, joka täyttäisi kaikki GDPR-vaatimukset. Satojen miljoonien investoinnit tietosuojaratkaisuihin viime vuosien aikana ovat kuitenkin mahdollistaneet palveluntarjoajille resursseja tehdä yhä kokonaisvaltaisempia ratkaisuja (IAPP 2021, 32–34).

Minkälaisia ratkaisuja organisaatioiden tulisi sitten tehdä, että ne pystyisivät täyttämään GDPR-vaatimukset? Yhtä oikeaa vastausta on mahdotonta löytää, sillä organisaatioiden koko, toimiala, kypsyysaste, resurssit ja tietosuojaosaaminen vaihtelevat. Tietosuojajärjestelmistä ei ole välttämättä mitään hyötyä, jos organisaatiosta ei löydy osaamista hyödyntää niitä. Tietosuoja voidaan tarvittaessa kuitenkin ulkoistaa vaikka kokonaan organisaation ulkopuolelle. Resurssit voivat tulla nopeasti vastaan. Edulliset tai jopa ilmaiset vaihtoehdot, joita ovat esimerkiksi EU:n projektit (esim. DEFeND) tai muiden voittoa tavoittelemattomien osapuolien ratkaisut (esim. Tietosuojatyökalu – Tietosuoja, 2022) voivat olla houkuttelevia vaihtoehtoja, jos tietosuojaan käytettävät resurssit ovat vähissä. Tietosuojan jatkuvuus voi olla vaarassa, koska näiden ratkaisujen kehitys on usein sidonnainen niiden saamaan rahoitukseen. Sama koskee kuitenkin myös yksityisen puolen toimijoita. Palveluista maksettavat kovat hinnatkaan eivät takaa sataprosenttisesti, että valittu palveluntuottaja pystyy jatkamaan vuosia kovasti kilpailulla alalla. Kova kilpailu toisaalta ohjaa palveluntuottajia kehittämään palveluitaan ja pysymään ajan tasalla tietosuojalainsäädännön uusimmista käänteistä. Epäedullisimmassa tilanteessa tietosuojan hallintaa voidaan joutua rakentamaan kokonaan alusta, kun valittu ratkaisu syystä tai toisesta ei ole enää käytettävissä. Tutkielman yhtenä päämääränä onkin tarkastella, kuinka tietosuoja-asiantuntijat ovat ratkaisseet näitä ongelmia.

4 TUTKIMUSMENETELMÄ JA TOTEUTUS

Tutkielmassa tutkitaan, minkälaisia haasteita esiintyy organisaatioiden tietosuojan hallinnassa tietosuoja-asiantuntijoiden kokemuksien kautta. Empiirinen osa tutkimuksesta toteutettiin laadullisena tapaustutkimuksena, jonka avulla pyrittiin nostamaan esiin kokemuksia tietosuojan hallinnan haasteista tietosuoja-asiantuntijoiden uran alusta tähän päivään, nykyisistä haasteista sekä mahdollisista tulevaisuuden haasteista. Haasteiden lisäksi tutkielmassa haluttiin etsiä tietosuoja-asiantuntijoiden kokemuksien kautta keinoja, joilla näitä haasteita on ratkaistu tai on suunniteltu ratkaistavan. Ratkaisuihin liittyen on kysytty myös kokemuksia teknisistä ja organisatorisista apuvälineistä.

Tutkielman tutkimusote on fenomenologinen. Tieteenfilosofiana fenomenologia korostaa kokemusten merkitystä ja niiden kautta ilmiöiden tutkimista ilman ennakkoasenteita (Laine 2018, 23–24). Tätä kautta haastateltavien kokemuksia pyrittiin tulkitsemaan ilman teorian liian suurta ohjaavaa vaikutusta. Haastattelut suoritettiin puolistrukturoituina teemahaastatteluina, joita kerättiin yhteensä seitsemältä eri tietosuoja-asiantuntijalta. Tutkielman aineistonkeruussa on otettu huomioon, että haastateltavat ovat asiantuntijoita. Tutkielmaa voisi myös kuvailla eksploratiiviseksi asiantuntijahaastatteluksi, jossa tutkitaan jotain vähän tutkittua ilmiötä (Alastalo, Åkerman ja Vaittinen 2017). Aineistoa analysoitiin aineistolähtöisellä sisällönanalyysilla, antaen mahdollisimman paljon painoarvoa asiantuntijoiden omille kokemuksille. Tässä luvussa esitellään teemahaastattelunrungon laatiminen, haastateltavien valinta ja aineistonhankinta sekä aineiston analysoiminen sisällönanalyysillä. Lopuksi arvioidaan vielä tutkielman luotettavuutta.

4.1 Teemahaastattelurungon laatiminen

Empiirisen aineiston aineistonkeruumenetelmänä tässä tutkielmassa toimi teemahaastattelut, joita varten piti kehittää teemahaastattelurunko. Aineistonkeruumenetelmäksi valikoitui teemahaastattelu sen tuoman joustavuuden takia.

Joustavuus mahdollisti myös sen, ettei haastattelurunkoa tarvinnut seurata samalla tavalla kuin strukturoidussa haastattelussa, vaan haastattelussa voitiin keskustelunomaisesti siirtyä aiheesta toiseen, jos haastateltavien vastaukset yhteen kysymykseen sivusivat jotain toista kysymystä. Strukturoimatonta haastattelua ei valittu aineistonkeruumenetelmäksi, koska tutkielmaan valittiin selvät teemat, jotka loivat raamit, joiden sisällä tutkielman oli tarkoitus pysyä. Puolistrukturoitu haastattelurunko koostui kahdestatoista kysymyksestä, joiden lisäksi oli viisi taustatietokysymystä. Lisäkysymyksillä pystyttiin avaamaan tutkielman kannalta merkityksellisiä aiheita. Aihealueeseen laajasti perehtymällä pyrittiin takaamaan, että lisäkysymykset olivat järkeviä ja niiden avulla saatiin tarkempia selityksiä asiantuntijoiden vastauksiin. Tämä takasi myös sen, ettei haastattelun aikana törmätty ammatillisuusmuuriin, jossa valta-aseman epäsymmetrisyys voi vaikuttaa negatiivisesti haastatteluun (Alastalo ym. 2017). Haastattelunrungon laatimisessa ja itse haastattelutilanteessa oli ajatuksena antaa haastateltavien kertoa omista kokemuksistaan mahdollisimman vapaasti ilman liian tarkkoja kehyksiä. Tarkempiin aiheisiin pystyttiin haastattelutilanteessa paneutumaan lisäkysymyksillä.

Hyvärinen (2017, 16–17) korostaa, että teoriapohjainen teemahaastattelu voi rajoittaa haastateltavia, varsinkin kun kyse on haastateltavien henkilökohtaisista kokemuksista. Teemahaastattelun teemat ja pääkysymykset ovat myös tästä syystä melko laajoja, eivätkä kytkeydy tarkasti mihinkään teoriaan. Teemahaastattelun kysymyksien laatimisessa on kuitenkin otettu huomioon tietosuojaan liittyvä lainsäädäntö ja aiempi tutkimus. Lisäksi on otettu huomioon tietosuojan hallinnan viitekehyksissä esille tulleita aihealueita. Haastattelun kysymyksien muotoilussa käytettiin hyödyksi Hyvärisen (2017, 17–21) huomioita kyselyhaastattelujen kysymysten laatimisessa. Hyvärisen (2017, 18) mukaan tärkeimpiä tekijöitä kysymysten muotoilussa on antaa haastateltaville tarpeeksi tilaa kertoa ajatuksistaan ja kokemuksistaan.

Teemoiksi valikoitui haasteet, ratkaisut ja apuvälineet tietosuojan hallinnassa. Apuvälineisiin liittyvät kysymykset jaettiin vielä kategorisesti teknisiin ja organisatorisiin apuvälineisiin. Haastattelurungosta tehtiin ensimmäinen versio, jonka sisällöstä pyydettiin mielipidettä yhdeltä tietosuoja-asiantuntijalta. Tämän keskustelun perusteella teemahaastattelurunkoa yksinkertaistettiin ja asiantuntijan ehdotuksesta kaikissa teemoissa otettiin huomioon kronologinen näkökulma; menneisyys, nykyisyys ja tulevaisuus. Tämä mahdollisti tietosuojan hallinnan haasteiden ja ratkaisujen kehittymisen tutkimisen tietosuoja-asiantuntijoiden uran aikana sekä mahdollisten tulevaisuuden näkymien tarkastelun. Yksinkertaistaminen vähensi entisestään kysymysten ohjaavaa vaikutusta. Tarkoitus oli tehdä kyseisen asiantuntijan kanssa myös harjoitteluhaastattelu, joka ei aikataulullisten haasteiden vuoksi kuitenkaan onnistunut. Taulukossa 1 on esitelty haastattelun kolme teemaa sekä esimerkkikysymyksiä jokaisesta teemasta.

Taulukko 2 Haastattelun teemat sekä esimerkkikysymykset

Tutkimuskysymys:	**Teema:**	**Esimerkkikysymys:**
Minkälaisia haasteita organisaatioiden tietosuojan hallinnassa on?	Haasteet	Minkälaisia haasteita näet tulevaisuudessa tietosuojan hallintaan liittyen?
Miten näitä haasteita on ratkaistu tai pyritään ratkaisemaan?	Ratkaisut	Minkälaisia ratkaisuja aikaisempiin haasteisiin on löydetty?
Minkälaisia organisatorisia tai teknisiä apuvälineitä/ratkaisuja organisaatiossa on käytössä tietosuojan hallintaan?	Tekniset apuvälineet	Onko suunnitteilla ottaa käyttöön uusia teknisiä ratkaisuja/apuvälineitä tulevaisuudessa?
	Organisatoriset apuvälineet	Onko teillä käytössä viitekehyksiä, kolmannen osapuolen sertifiointeja tai standardeja apuna tietosuojan hallinnassa?

Esimerkkikysymyksissä näkyy myös, kuinka tutkimuksessa on otettu huomioon ajallisesti menneisyys, nykyinen tilanne ja tulevaisuus. Varsinkin menneisyyden huomioon ottaminen osoittautui hyödylliseksi. Tietosuoja-asetuksen tuoreuden vuoksi aihealueesta on hyvin vähän pitkittäistutkimusta. Tutkielma ei korvaa kunnon pitkittäistutkimusta, mutta antaa kuvaa siitä, kuinka tietosuoja-asiantuntijat kokevat tietosuojan hallinnan haasteiden ja ratkaisujen muuttuneen uriensa aikana. Teemoihin liittyvien kysymysten lisäksi haastattelurunkoon kuului viisi taustakysymystä, joissa kysyttiin esimerkiksi tehtävänimikettä ja työnkuvaa.

4.2 Haastateltavien valinta ja aineistonhankinta

Aineistonhankinnassa oli kaksi vaihetta; kirjallisuuskatsaus ja empiirinen osa. Kirjallisuuskatsauksen tarkoitus oli syventyä aikaisempaan tutkimukseen ja kirjallisuuteen aiheesta. Aluksi kerrotaan yleisesti tietosuoja-asetuksesta ja rakennetaan pohjaa tietosuojan ymmärtämiselle. Mitä syvemmälle teoreettisen aineiston etsimisessä edettiin, sitä enemmän painotettiin mahdollisia haasteita, jotka liittyvät tietosuojan hallintaan. Läpikäydyn kirjallisuuden perusteella valittiin osa-alueita tietosuojasta ja tietosuoja-asetuksesta, joiden odotettiin hypoteettisesti nousevan esille asiantuntijoiden haastatteluissa. Näistä osa-alueista ja niiden mahdollisesti aiheuttamista haasteista kirjoitettiin tarkemmin. Teoreet-

tisemman osan lisäksi luvussa 3, ''Apua tietosuojan hallintaan'' esitetään organisatorisia ja teknisiä apuvälineitä pääasiallisesti hyödyntämällä vähemmän tieteellisiä lähteitä. Kirjallisuuskatsaus myös ohjasi haastattelurungon laatimista sekä lisäsi mahdollisuuksia lisäkysymysten kysymiseen.

Empiirisen osan aineistonhankinta suoritettiin yksilöhaastatteluilla. Haastateltavien henkilöiden tulee toimia vähintään asiantuntijatehtävissä tietosuojaan liittyen. Tarkoitus oli löytää hieman erilaisia rooleja eri organisaatioista, jotta voidaan vertailla, toistuvatko jotkin teemat työtehtävästä ja organisaatiosta riippumatta. Monfared, Benslimane ja Yang (2018, 1004) tunnistivat erilaisia teknisiä taitoja ja kompetensseja, joita tietosuoja-asiantuntijoilla tulisi olla:

- Tietosuojariskien arviointi ja hallinta
- Tietotekniikkataidot
- Tietosuojan hallinta ja kontrollit
- Tietosuojapolitiikkojen ja -ohjelmien kehittäminen ja implementointi
- Tietosuojan vaatimustenmukaisuuden noudattaminen ja tarkastaminen
- Tietoturvallisuuden kontrollit
- Tietoturvallisuuden hallinta

Näiden lisäksi tietosuoja-asiantuntijoiden olisi hyvä omata organisatorisia ja henkilökohtaisia ominaisuuksia kuten johtajuutta, kykyä tiimityöskentelyyn sekä ongelmanratkaisu- ja kommunikaatiotaitoja (Monfared, Benslimane & Yang 2018, 1004). Monfared, Benslimane ja Yang (2018, 1003) tunnistivat myös, että tietosuoja-asiantuntijoilla olisi hyvä olla joitain sertifikaatteja, kuten Certified Information Privacy Professional (CIPP), Certified Information System Auditor (CISA) ja Certified Information Systems Security Professional (CISSP).

Haastateltavilta ei kuitenkaan odotettu sertifikaatteja, eikä niistä kysytty tutkielmassa. Monfaredin ja kumppaneiden (2018) huomioita tietosuoja-asiantuntijoiden kompetensseista käytettiin tutkielmassa lähinnä viitekehyksenä, jonka avulla pyrittiin löytämään sopivat haastateltavat. Alastalo kollegoineen (2017) tiivistää asiantuntijuuden seuraavasti:

> ''Nyrkkisääntönä voi pitää sitä, että asiantuntijoita ovat henkilöt, joilla on sellaista erityistä tietoa tutkittavasta asiasta, jota ei ole kenelläkään toisella tai jota on vain hyvin harvoilla.''

Tietosuojan parissa työskentelevät ovat yhä melko harvinainen joukko ja useammalla haastateltavalla oli jo useamman vuoden ura tietosuojan parissa. Tärkeimpiä kriteereitä olivat haastateltavien kokemus tietosuojan parissa työskentelystä ja nykyisen työnkuvan liittyminen jollakin tasolla organisaation tietosuojan hallintaan. Haastateltavat tavoitettiin pääasiassa sähköpostilla. Haastattelut oli tarkoitus hoitaa pääasiassa etäyhteydellä, mutta mahdollisuuksien mukaan haastattelut olisi voitu järjestää myös kasvotusten. Seitsemästä haastattelusta kuusi hoidettiin etäyhteydellä ja vain yksi haastattelu tehtiin kasvotusten. Se, oliko haastattelu etänä vai kasvotusten, ei kuitenkaan vaikuttanut itse haastattelun sisältöön.

Haastateltavia oli sekä yksityiseltä että julkiselta sektorilta. Haastattelun aikana 3 haastateltavaa työskenteli yksityisellä ja 4 julkisella sektorilla. Asiantuntijoiden taustat ja työnkuvat vaihtelivat. Osa oli työskennellyt konsultteina tai muissa tehtävissä tietosuojan parissa aikaisemmin ja haastattelun hetkellä viisi asiantuntijaa oli organisaatiossa myös tietosuojavastaavana, vaikka se ei välttämättä ollut haastateltavan työnimike. Haastatteluiden aikana haastateltavista välittyi asiantuntijuus, eikä yhtäkään haastattelua tarvinnut tiputtaa pois tutkielman aineistosta.

4.3 Sisällönanalyysi

Haastattelut litteroitiin pian haastattelujen jälkeen. Litteroinnin aikana merkittiin ja kategorisoitiin kohtia, joiden oletettiin olevan tutkielman kannalta merkityksellisiä. Aineiston alustava analysointi ja tarkastelu helpottavat siirtymistä analyysivaiheeseen (Ruusuvuori, Nikander ja Hyvärinen, 2010, 10). Haastattelut litteroitiin perustasolla ilman äänenpainoja, huokauksia tai muita ääniä, jotka eivät olleet tutkielmalle oleellisia. Täytesanat kuitenkin sisällytettiin litterointiin ja ne näkyvät myös lainauksissa, joita käytetään kappaleessa 5, ''Tutkimustulokset ''. Tutkielmassa oltiin kiinnostuneita asiantuntijoiden kokemuksista ja siitä, mitä heillä oli sanottavaa, ei miten he sen sanovat. Haastatteluiden kestot vaihtelivat 19 minuutin ja 40 minuutin välillä. Yhteensä haastattelut kestivät 3 tuntia ja 14 minuuttia.

Analyysivaiheessa käytettiin sekä teoriaohjaavaa että aineistolähtöistä analyysia. Ruusuvuori kollegoineen (2010, 19–21) toteaa, että absoluuttinen aineistolähtöisyys on mahdotonta, sillä teoria on vaikuttanut joka tapauksessa jo tutkielman tulkintoihin ja valintoihin. Tämä näkyi esimerkiksi haastatteluissa, sillä kysymyksillä oli pohja aikaisemmassa teoriassa ja kirjallisuudessa. Näistä analyysimenetelmistä korostuu enemmän kuitenkin aineistolähtöinen analyysi ja fenomenologisen tutkimusmetodin mukaisesti asiantuntijoiden kokemukset pyrittiin ottamaan huomioon sellaisinaan. Samoin kuin haastattelurungon luomisessa ja haastatteluissa, sisällönanalyysissa pyrittiin avoimuuteen sekä ennakkoluulottomuuteen.

Fenomenologisessa tieteenfilosofiassa analyysin avulla aineistosta etsitään merkityskokonaisuuksia yhteenkuuluvuuden ja samanlaisuuden perusteella (Laine, 2018, 32). Samalla yksilöllinen kokemus ei tarkoita, että kokemus olisi jotenkin vähemmän arvokas kuin yleisesti koettu (Laine, 2018, 34). Sisällönanalyysissa ei jätetty siis huomioimatta asiantuntijoiden kokemuksia, vaikka ne saattoivat olla yksilöllisiä. Painoarvoa annettiin asioille, jotka vaikuttivat haastattelun aikana olevan merkityksellisiä haastateltaville. Merkityksellisten kokonaisuuksien ymmärtämisessä auttavat tutkijan intuitio ja elämänkokemus (Laine, 2018, 32). Ei voida sanoa, että tutkijalla olisi haastatteluiden aikana vielä erityisen paljon elämänkokemusta. Kokemus ja tieto tietosuojasta kuitenkin auttoivat ihmisymmärryksen lisäksi huomioimaan ne haastattelun tilanteet, jotka asiantuntijat kokivat merkityksellisiksi. Tästä syystä oli myös hyödyllistä, että

sisällönanalyysi tehtiin mahdollisimman pian haastatteluiden jälkeen ja että haastattelut nauhoitettiin. Tutkijan ei tarvinnut päätellä vain litteroinnin perusteella, mikä vaikutti merkitykselliseltä haastateltavalle. Haastattelutilanteista oli analyysia tehdessä vielä niin lyhyt aika, että tutkijalla oli muistikuvia myös itse haastattelutilanteista.

4.4 Luotettavuuden arviointia

Tässä alaluvussa arvioidaan tutkielman luotettavuutta. Yleisesti tutkimusten luotettavuutta on tutkittu validiteetin ja reliabiliteetin käsitteiden kautta. Reliabiliteetti tarkoittaa toistettavuutta, mukaan lukien analyyttisten menetelmien johdonmukaisuus ja validiteetti tarkoittaa sitä, kuinka hyvin tutkimuksen tulokset vastaavat sitä, mitä on tutkittu (Noble & Smith, 2015, 34). Vaikka molempien, validiteetin ja reliabiliteetin käsitteiden merkitys ja osuvuus laadullisessa tutkimuksessa on kyseenalaistettu, nähdään validiteetti yleensä laadullisessa tutkimuksessa tärkeämpänä (Saaranen-Kauppinen, & Puusniekka, 2006). Toistettavuus voikin olla hankalammin määriteltävissä laadullisessa tutkimuksessa kuin tiedon paikkansapitävyys. Saaranen-Kauppinen ja Puusniekka (2006) ovat nostaneet seuraavia yleisesti hyväksyttyjä toimia luotettavuuden parantamiseksi:

- Kategorisointi ja koodaus analysointivaiheessa
- Esitestaus ja harjoittelu
- Videointi tai nauhoittaminen
- Tutkijan ja tutkittavien käsitteiden erottaminen
- Tilannesidonnaisuuden ymmärtäminen
- Tutkimuksen luonteen ja aiheen vaikutuksen tiedostaminen

Tutkielmassa nämä keinot toteutuivat kiitettävästi. Kategorisointia ja koodausta tehtiin analyysivaiheessa, jolloin aineistosta etsittiin teemoja, jotka asiantuntijat kokivat merkityksellisiksi. Esitestaus ja harjoittelu eivät toteutuneet niin hyvin kuin oli suunniteltu. Haastattelurunko käytiin läpi tietosuoja-asiantuntijan kanssa ennen haastatteluja, mutta suunniteltua esitestausta ei keretty asiantuntijan aikataulullisten haasteiden vuoksi tekemään, ennen kuin varsinaiset haastattelut jo alkoivat. Kuitenkin jo ensimmäisessä haastattelussa osoittautui, että haastattelurunko oli toimiva. Haastattelurunkoa olisi voinut vielä tässä vaiheessa muuttaa ja jättää ensimmäinen haastattelu ulos aineistosta, mutta sille ei ollut tarvetta. Kaikki haastattelut käytiin läpi samalla rungolla ja samankaltaisella haastattelutilanteella, mikä nostaa myös tutkielman reliabiliteettia. Haastattelut myös videoitiin ja nauhoitettiin, mikä mahdollisti haastatteluihin palaamisen myöhemmin. Tutkijan ja tutkittavien käsitteiden erottamiselle ei ollut tarvetta, sillä kaikki osapuolet puhuivat tietosuojakäsitteillä, jotka olivat kaikille tuttuja. Tässä auttoi tutkijan perehtyneisyys aihealueeseen ja oma kokemus tietosuojan parissa työskentelystä. Tutkimuksen luonteen ja aiheen vaikutuksen tiedosta-

minen sekä tilannesidonnaisuuden ymmärtäminen sitoutuivat tutkielmassa samojen haasteiden ympärille. Haasteena oli, kuinka vapaasti haastateltavat uskaltavat kertoa oman työn ja organisaation haasteista sekä mahdollisista epäkohdista. Näitä vaikutuksia pyrittiin tutkielmassa taklaamaan suojaamalla asiantuntijoiden anonymiteettia parhaimman mukaan. Vahva anonymiteetti voi toisaalta olla tutkielman luotettavuudelle myös negatiivinen tekijä.

Luotettavuutta arvioitaessa on hyvä tuoda esille myös tekijät, jotka mahdollisesti heikentävät tutkielman luotettavuutta. Yksi näistä on haastateltavien vahva anonymiteetti. Tutkielmassa ei esimerkiksi tuoda esille edes haastateltavien tarkempia työnkuvia tai työnimikkeitä. Tämä on tietoinen valinta tunnistamisen vaikeuttamiseksi. Tietosuojan kenttä on kuitenkin Suomessa melko pieni ja jotkut työnimikkeet voivat olla hyvinkin organisaatiospesifejä. Poikkeus tehtiin mainitsemalla joidenkin asiantuntijoiden kokemuksista tietosuojakonsultteina. Syynä tässä oli, että analyysin kannalta on tärkeä erottaa, oliko kokemukset omasta organisaatiosta vai organisaatioista, joille tehtiin töitä ulkopuolisena. Työnimikkeiden ja työnkuvan pois jättäminen kuitenkin heikentää hieman tutkielman luotettavuutta etenkin reliabiliteetin kannalta. Toisaalta kaikkien haastateltavien työnkuva liittyi jollakin tavalla tietosuojan hallintaan. Anonymiteetista huolimatta luotettavuutta voi heikentää myös aihe, jossa joutuu tuomaan mahdollisesti esiin oman organisaation haasteita. Haastateltavat tuntuivat puhuvan asioista kuitenkin rehellisesti ja kaunistelematta, mikä näkyy myös tuloksissa. Myös ajallisesti vanhojen kokemusten kysyminen voi olla kyseenalaista luotettavuuden kannalta. Ihminen saattaa muistaa väärin tai muistot voivat olla niin heikentyneitä, että sellaisen aineiston käyttäminen voidaan nähdä kyseenalaisena. Tietosuoja-asetuksen voimaantulosta vuonna 2018 on kuitenkin verrattain vähän aikaa ja vain harva haastateltava kertoi ajasta ennen sitä. Kronologisen näkökulman ottaminen tutkielmaan toi kuitenkin paljon hyödyllistä ainestoa aiheesta, josta tutkimusta ei ole paljon saatavilla.

Luotettavuutta tavoiteltiin Saaranen-Kauppisen ja Puusniekan (2006) mainitsemien toimien lisäksi myös muilla tavoilla. ”Tutkimustulokset” -luvussa on pyritty tuomaan paljon haastateltavien sitaatteja esille tukemaan ja todistamaan analysoinnin paikkansapitävyyttä. Tutkielmaa varten on tehty myös laajaa taustatyötä, esimerkiksi kirjallisuuskatsauksen muodossa, jolla on pyritty todistamaan myös tutkijan asiantuntijuutta aiheesta. Nämä yhdessä vahvistavat johtopäätöksien paikkansapitävyyttä, mikä parantaa varsinkin tutkielman validiteettia. Tutkimusprosessi on pyritty esittelemään mahdollisimman läpinäkyvästi ja totuudenmukaisesti. Samoin kuin haastattelurungon laatimisessa, niin itse haastatteluissa ohjenuorana oli avoimuus ja ennakkoluulottomuus, mikä on tärkeää varsinkin fenomenologisessa tutkimuksessa (Laine 2018, 23–24). Haastateltavia ei ohjailtu, vaan heidän annettiin avoimesti kertoa omista kokemuksistaan.

5 TUTKIMUSTULOKSET

Tutkielman avulla pyrittiin vastaamaan kolmeen tutkimuskysymykseen:

1. Minkälaisia haasteita organisaatioiden tietosuojan hallinnassa on?
2. Miten näitä haasteita on ratkaistu tai pyritään ratkaisemaan?
3. Minkälaisia organisatorisia tai teknisiä apuvälineitä/ratkaisuja organisaatioissa on käytössä tietosuojan hallintaan?

Näihin tutkimuskysymyksiin lähdettiin hakemaan vastauksia tietosuoja-asiantuntijoiden kokemuksien kautta. Empiirinen aineisto kerättiin puolistrukturoiduilla teemahaastatteluilla. Seuraavaksi esitellään tutkimustulokset, joihin päädyttiin aineistolähtöisen ja teoriaohjaavan sisällönanalyysin avulla. Aineistosta ei tuoda esille mitään tekijöitä, joiden avulla vastaajia tai heidän organisaatiotansa voisi tunnistaa. Tällä on pieni vaikutus aineistolähtöisen analyysin kannalta, sillä joidenkin vastausten sisältö linkittyi henkilön työnkuvaan. Asiantuntijoista kaksi oli työskennellyt tietosuojan parissa konsultteina, joten heillä oli kokemusta myös muiden kuin oman työpaikan tietosuojan hallinnasta. Tämä on kuitenkin tiedostettu tutkielmassa ja pyritty tuomaan asiantuntijoiden kokemukset esille mahdollisimman läpinäkyvästi, kuitenkaan anonymiteettia loukkaamatta. Haastateltavat on anonymisoitu käyttämällä asiantuntijoista tunnisteita A1-A7. Haastattelija on merkitty tunnisteella H.

5.1 Haasteet

Vaikka haastattelut kulkivat usein keskustelunomaisesti omalla painollaan ja kysymysten järjestys muuttui sen mukaan, oli melkein kaikissa tapauksissa ensimmäinen kysymys taustatietojen kysymisen jälkeen: ''minkälaisia haasteita kohtaat työssäsi tietosuojan hallintaan liittyen tällä hetkellä'' tai ''minkälaisia haasteita olet kohdannut tietosuojan hallintaan liittyen urasi aikana''. Haasteet liittyvät muihin teemoihin eli ratkaisuihin ja apuvälineisiin, joten oli luonnollis-

ta pitää nämä haasteisiin liittyvät kysymykset keskustelun avaavina kysymyksinä. Vaikka kysymyksen asettelu on melko laaja, vain yksi haastateltava kysyi tarkennusta siihen, mitä haasteilla tarkoitetaan. Haastateltavilla oli lähes kaikissa tapauksissa muutama selvä pääteema, joita he halusivat tuoda esiin.

Asiantuntijoiden kokemuksissa tietosuojan jalkauttaminen organisaatioissa nousi esille muita haasteita useammin. Haastateltavat nostivat jalkauttamiseen liittyen haasteeksi myös tietosuojaan liittyvän koulutuksen. Nämä nähtiin eräänlaisena päähaasteena, josta monet muut tietosuojan hallintaan liittyvät haasteet johtuivat. Esimerkiksi eräässä suuressa organisaatiossa haasteena oli saada kaikki työntekijät ylipäätänsä tietoisiksi tietosuojan olemassaolosta. Yksi ongelma oli myös vaihtuvuus:

> ''…iso organisaatio ja tietysti on niinku paljon vaihtuvuuttakin. Niin niin tota. Kaikki ei sitten kuitenkaan ole tietoisia niinku tietosuojalainsäädännön niinku edellytyksistä, niin se on kyllä iso haaste.''(A5)

Toisena koulutukseen liittyvänä ongelmana haastateltava A6 toi esille koulutuksen tason eri ryhmille organisaatiossa:

> ''Käytännön haaste, että miten niitä hommata ja sitten jos yrittää sitä niinku kouluttaa niin se, että kun se taso millä tasolla tarvitsi ihmistä kouluttaa, niin on hyvin erilainen hyvin eri rooleissa.'' (A6)

Asiantuntija toi esille myöhemmin, miksi tämä on haaste ja minkälaisia ongelmia riittämättömästä koulutuksesta voi seurata:

> ''Joillekin se menee niinku tää ihan liian yli tavallaan, että sitä on aivan liikaa ja toisille taas sekään ei vielä kuitenkaan tuo sitä niin kuin tarpeeksi siihen, että oikeesti nyt niin kun tässä pitää niinku huomata pysähtyä. Tää on ehkä semmoinen eniten semmoinen ongelma. Siitä sitten oikeastaan tulee se seuraava, että milloin myöskin huomata se, että millon tulee tietosuojapoikkeama eli sen havainnointi, että tavallaan ymmärtää, että nyt oikeasti minun pitäisi ilmoittaa.''(A6)

Osa asiantuntijoista piti tätä jalkauttamisen ongelmana. Yhdelle asiantuntijoista organisaation vaihto organisaatioon, jossa oltiin vähemmän tarkkoja tietosuojan kanssa, tuotti haasteita:

> ''On lähtenyt niinku loppujen lopuksi ihan perusteista, että henkilöstön kouluttaminen ja ohjaaminen henkilötiedon käsittelyyn on sitten aivan erilaista siihen nähden… …itse ymmärtää, mutta se että osaako saada sen tietämyksen tonne kentälle, niin se on vaikeata.''(A7)

Jalkauttaminen ja koulutus olivat haasteellisia, koska tietosuojalainsäädäntöä ei haluttu ymmärtää merkitykselliseksi. Asiantuntijoiden kokemukset resurssien rajallisuudesta heijastuivat myös kouluttamiseen sekä jalkauttamiseen. Aika ja osaavat henkilöt eivät riittäneet aina jalkauttamaan tietosuojaa sen tarvitsemalla tavalla. Yksi haastateltava koki myös tietosuoja-asetuksen alkuaikoina esiintyneen muutosvastarintaa.

Yhdeksi keskeiseksi haasteeksi nousi vaatimustenmukaisuuden varmistaminen tietosuojalainsäädännön tulkinnallisuuden vuoksi. Tulkinnallisuus, joka tuli esille jo mahdollisena haasteena kirjallisuuskatsauksessa, tuli haastateltavien vastauksissa esille eri tavoin. Haaste oli myös kulkenut asiantuntijoiden kokemuksien mukaan mukana koko uran ajan, aina tietosuoja-asetuksen alkuajoista lähtien. Tulkinnallisuuden koettiin tuovan haasteita myös siinä mielessä, että omista toimintatavoista ei voida olla koskaan täysin varmoja. Haastateltavat tunnistivat, että tietosuojaan liittyviä tapahtumia ja asioita tulee seurata tarkasti, jotta voidaan pysyä perillä, mitkä käytännöt ovat vaatimustenmukaisia. Viranomaisohjeetkin tuntuvat välillä riittämättömiltä. Asiantuntijat kuvailivat tulkinnallisuuden haasteita seuraavasti:

> ''Asetus on kuitenkin niinku säädetty silleen aika periaatetasolla ja niinku tarkoituksella silleen et se on niinku jättää sitten liikkumavaraa ja näin niin sen sehän on sinänsä ihan ok lähestymistapa, mutta kyllähän sen kaveriksi tarvittaisiin sitten sitä niinku, että mitä se käytännön tasolla tarkoittaa, että tulee sitten ohjeistuksesta tai tai oikeuskäytännöstä tai mistä ikinä, niin ei tavallaan nyt meillä on sitten se periaatetasoinen sääntely, mutta ei kuitenkaan kauheasti sitä niinku oikeesti tietoa siitä, että mitä se milloinkin vaatii, että sitten siellä on sellaisia niinku yksittäisiä osa-alueita, mistä saattaa olla niinku tosi yksityiskohtaistakin ohjeistusta.''(A1)

> ''Hirveästi ei niin kun varmaan kukaan uskalla lähteä tulkitsemaan, että jos ei ole mitään mitään ennakkotapauksia tai muita.''(A2)

> ''Eli tietosuoja asetus on sillä tavalla niinku haasteellista sääntelyä, että se on luonteeltaan niinku yleislakia, jota sitten on täsmennetty erilaisilla viranomaisohjeistuksilla. Mutta kuitenkin sitten myös ratkaisuja niihin vasta saadaan oikeastaan oikeuskäytäntöjen kautta lopullisena niinku ratkaisuina. Eli jos viranomainen esimerkiksi on ohjeistanut jotakin, niin sekin vielä jättää pahimmillaan paljon tulkinnanvaraisuutta ja sitten vasta kun nähdään, että miten niitä ratkaisuja on oikeasti loppupeleissä käsitelty. Onko niistä esimerkiksi valitettu ja mahdollisesti sitten jostakin oikeudesta saatu niihin ratkaisu, niin sitten me vasta niinku oikeastaan pahimmillaan tiedetään ne tosi vaikeat tulkinnalliset asiat mitä ne sitten lopulta on ja se keskeinen haaste onkin just tämä tulkinnallisuus. ''(A3)

Myöhemmin, kun haastattelija kysyi tarkennukseksi, että johtuiko haastateltavan mielestä haasteet suurimmaksi osaksi asetuksesta ja sen epäselvyydestä, sanoi haastateltava vastauksensa lopuksi yksiselitteisesti seuraavasti:

> ''Meillä on tavallaan niinku hyvin tämmöinen, niinku monitulkintainen sääntely tässä käsillä ja minun nähdäkseni suurimmat haasteet johtuu tästä.''(A3)

Tulkinnallisuus luo selvästi haasteita tietosuojariskien hallintaan. Esimerkiksi ongelmallisina käsitteinä tietosuojalainsäädännössä koettiin oikeutettu etu ja riskilähtöisyys. Voi olla vaikea arvioida riskien vaikutuksia, jos viranomaispäätöksiä kyseiseen riskiin liittyen ei vielä ole tehty. Yksi haastateltavista näki myös, että tulkinnallisuuden vuoksi suhteellisuus esimerkiksi riskeihin liittyen on heikkoa:

> ''Niinku suhteellisuus niissä asioissa, että mä ymmärrän niinku tavallaan, että sitä pitäisi pystyä myös sitä osoitusvelvollisuutta niinku skaalaamaan pikkusen sen riskin mukaan ja se ei mun mielestä ainakaan nyt niin kuin siis näissä mitä tulee ohjeistuksia valtuustolta sun muilta, se ei ihan täysin mun mielestä niinku toteudu. Siinä nähdään niinku riski vähän joka paikassa, missä se ei välttämättä ei sitten oikeasti ole.''(A6)

Tulkinnallisuus ja lainsäädännön epäselvyys koettiinkin ylätason ongelmana, josta monet pienemmät ongelmat johtuvat. Siitä johtuvat esimerkiksi ongelmat dokumentaatiossa ja sitä kautta osoitusvelvollisuudessa. Ei olla täysin varmoja, minkälainen dokumentaatio on tarpeeksi osoitusvelvollisuuden täyttämiseksi, joten dokumentaatiota tehdään paljon. Joidenkin asiantuntijoiden mielestä jopa liikaa. Mennään enemmänkin dokumentaatio edellä, eikä keskitytä oikeasti kehittämään tietosuojaa. Asiantuntijoiden kokemuksissa tuli ilmi epävarmuus oman organisaation tietosuojan hallinnan riittävyydestä. Muutama haastateltava myös tunnisti, kuinka Tietosuojavaltuutetun toimiston kiireellisyys on luonut mahdollisuuden hoitaa tietosuojan hallintaa vähän sinne päin.

Varsinkin haastateltavat, jotka olivat työskennelleet tietosuojan parissa tietosuoja-asetuksen voimaan astumisen aikana tai pian sen jälkeen, tunnistivat samankaltaisia haasteita tietosuoja-asetuksen alkuajoilta. Näihin haasteisiin tietosuoja-asetuksen täysimääräisen voimaantulon aikoihin toukokuussa 2018 ja pari vuotta sen jälkeen liittyi vahvasti myös asetuksen tulkinnallisuus. Asiantuntijoiden vastauksista tuli esille, kuinka sekavaksi asetuksen alkuajat koettiin:

> ''Alkuvaiheessa aiheutti niin kuin aika paljon hämmennystä, että kun oli näitä niinku sekoilua siitä, että nyt nyt kielletään niinku kerrostaloista nimitaulut ja ja tuota saunavuorolistat.''(A1)

> ''Niin se siis olihan siinä alkuun se on niinku semmoinen totaalinen kaaos se, että miten tämän nyt tästä niinku järjestäis että toki se on niin kuin poistunut.''(A6)

> ''Että hei tämmöinen tietosuoja-asetus on tulossa, mutta kukaan organisaatiosta ei oikein osannut vastata, että no mitä me ollaan tehty? Mitä meiltä puuttuu? Millä niinku tuota, että mitä tää niinku lainsäädäntömuutos vaikuttaa meidän omaan organisaation toimintaan? Mitkä on meidän riskit, millaisia puutteita meidän toiminnassa on?''(A4)

Koettiin hyvinkin haastavana tietää, mitä asetus oikeasti loppujen lopuksi merkitsee. Tietosuojan parissa jo henkilötietodirektiivin aikana työskennelleet huomauttivat, että vasta tietosuoja-asetuksen myötä tulleet mahdolliset sanktiot saivat organisaatiot kiinnittämään tietosuojaan enemmän huomiota. Tämän voidaan tulkita tarkoittavan sitä, että monessa tapauksessa tietosuojan hallinnassa lähdettiin lähes tyhjästä liikkeelle. Tämä näkyi myös suoraan yhden haastateltavan vastauksesta:

> ''Saada ihmiset tietoiseksi, mitä tietosuoja tarkoittaa ja vaikka oli ollut niinku henkilötietolaki aikaisemmin niin tuntui, että se ei kuitenkaan ollut ehkä jalkautunut niin

> hyvin, että vaikka moni asia ei muuttunut, niin tuntui että ne asiat oli aika uusia uusia sitten tota ihmisille.''(A5)

Haastateltava A4 koki, että yksityisyyden itseisarvoa ei organisaatioissa ainakaan aluksi tajuttu ja organisaatioissa ajateltiin, että nyt kun tarvittava dokumentointi on tehty, ei tarvitse enää huolehtia tietosuojasta. Vasta viranomaisen sanktiot saivat organisaatiot taas kiinnostumaan tietosuojan hallinnasta uudelleen:

> ''Oliko se nyt 2020 kesällä vasta kun tuli ensimmäinen, niinku tää hallinnollisen hallinnollinen niinku sakko tai seuraamusmaksu, niin melkein siihen asti oli vähän semmoista, että ne ne jotka ei sitten ollut niin syvällä siinä tai jotenkin ehkä eivät nähneet sitä tietosuojan tai yksityisyydensuojan itseisarvoa.''(A4)

Viranomaisen kyvyttömyys reagoida tietosuojarikkomuksiin tai seurata vaatimustenmukaisuutta nähtiin toisaalta myös pienenä helpotuksena ja ''lisäaikana'' saada tietosuoja paremmin hallintaan. Tietosuoja-asetuksen voimaantulon jälkeen organisaatioissa pyrittiin saamaan aikaan edes jonkunlaista dokumentointia, jolla osoittaa vaatimustenmukaisuus. Monet haastateltavat tunnistivat, että aluksi paljon energiaa ja resursseja meni pelkästään sellaisten toimien tunnistamiseen, joita nyt tietosuoja-asetuksen mukaan pitäisi alkaa tekemään. Alussa suurena haasteena oli myös resurssien ja tietämyksen puute. Organisaatioissa hyvin harvalla henkilöllä oli etukäteen asiantuntijuutta tietosuojaan liittyen. Tilanne kuitenkin parani myös tulkinnallisuuden kannalta ajan kuluessa. Koettiin, että viranomaispäätökset sekä lisääntyneet ohjeet jättivät vähemmän tulkinnan varaa, kuin mitä se oli asetuksen alussa. A3 tunnisti myös, että tilanne on parantunut paljon siitä, mitä se oli asetuksen alkuaikoina. Tilanteen edetessä haastateltavat kokivat, että tietosuoja oli paremmin hallittavissa ja pystyttiin oikeasti tekemään asioita tietosuojan edistämiseksi. Asiantuntijoilla tuntui myös olevan yhteinen ajatus siitä, että organisaatiot panostivat enemmän tietosuojan hallintaan.

Ajatukset olivat silti tulevaisuutta koskien epätietoisia ja pessimistisiäkin. Tulkinnallisuuteen ei uskottu tulevan ihmeellistä parannusta, vaan se nähtiin tietosuojan hallintaan liittyvänä haasteena myös tulevaisuudessa. Toisaalta nähtiin, että tilanne voi hieman parantua, kun yleinen tietoisuus lisääntyy ja uusia päätöksiä sekä ohjeita tulee lisää. Samalla oltiin huolissaan mahdollisesta muusta sääntelystä, jonka voi sekoittaa tietosuojan hallintaa. Yksi haastateltavista luetteli tulevia asetuksia, joilla voi olla vaikutuksia myös tietosuojaan:

> ''Sieltä on niinku ainakin kolme keskeistä niinku asetusta tällä hetkellä jo tulossa. Ja ja vielä niinku lisää, mutta tällaiset kun data markets act, data services act, data governance act ja sitten vielä esimerkiksi AI:sta on tulossa vielä niinku oma regulaatio eli tekoälystä. Niillä kaikilla on niinku liittymä myös tähän tietosuojaan tavalla tai toisella.'' (A3)

Asiantuntija (A3) tiedosti, että säädökset voivat osaltaan helpottaakin tietosuojan hallintaa, mutta toisaalta lisäävät taas tulkinnallisuutta. Myös A1 koki muun

lainsäädännön kietoutumisen tietosuojalainsäädäntöön mahdollisena haasteena tulevaisuudessa. Epävarmuutta hän näki tulevaisuudessakin Schrems-II päätöksen takia:

> ''Ehkä se epävarmuus liittyy nimenomaan siihen, että että jos ne jossa käsittely tapahtuu EU-alueella, mutta se yhtiön tai palveluntarjoajan kuitenkin niinku käytännöt yhdysvaltalaisen määräysvallassa, niin miten se vaikuttaa siihen?''(A1)

Hän myös lisäsi, ettei ongelma koske pelkästään Yhdysvaltoja, vaan muitakin maita, kuten Kiinaa. Myös kaksi muuta asiantuntijaa nostivat haasteeksi tietojen siirron EU:n ulkopuolelle ja Schrems-II päätöksen. Haasteelliseksi nähtiin varsinkin pilvipalvelut ja alikäsittelijät. Erityisen haasteellista oli se, että tunnistettaisiin, missä tapauksissa on kyse siirroista EU/ETA alueen ulkopuolelle. Siirtoihin tarttuneilla asiantuntijoilla oli myös yhteinen toive, että ratkaisu tilanteeseen tulisi mahdollisimman nopeasti.

Haastatteluissa painottui tietosuojan hallinnan suuremmat linjat, kuten koulutus, jalkauttaminen, tulkinnallisuus ja epävarmuus oman organisaation tietosuojan hallinnan vaatimustenmukaisuudesta. Osa haastateltavista nosti esiin kuitenkin myös pienempiä kokonaisuuksia, kuten tietoturvapoikkeamat, tarkastuspyynnöt, tietoturvarikkomukset ja toimittajien kanssa työskentelyn. Haasteeksi tunnistettiin myös yhdessä organisaatiossa hallintamallien ja työkalujen puute. Aineistossa esiintyi myös asiantuntijoita, jotka olivat kokeneet haasteeksi sen, että tietuojan hallinta oli organisaatiossa saavuttamatonta tai etäistä. Tämänkaltaisesta tilanteesta kokemusta oli esimerkiksi asiantuntijalla (A4), joka oli työskennellyt ulkoisena tietosuojavastaavana. Osalla haasteet myös liittyivät paljon työnkuvaan tai organisaatioon, jossa he olivat töissä. Organisaatioissa saattoi olla paljon työntekijöitä tai kerättiin paljon henkilötietoja, joista oli mahdotonta olla täysin perillä. Nämä organisaatioon liittyvät haasteet olivat loppujen lopuksi lähtöisin resurssien ja jalkauttamisen puutteista sekä lainsäädännön tulkinnallisuudesta. Tulkinnallisuuden ja jalkauttamisen haasteet voivat myös kietoutua toisiinsa, mikä tuli esille ainakin yhdessä haastattelussa:

> ''Sitten jos siihen että niinku ymmärrä sitä asiaa niin se on aika vaikeata lähteä jotain vaikutustenarviointia tekemään, kun et tiedä, että mitä se niinku tarkoittaa. Ja sitä paitsi sekin on niin vaikeata. Hyvä että tietosuojavastaavaakaan ymmärtää sen niin niin sitten se on vaikea jalkauttaa tuonne kentälle.''(A7)

5.2 Ratkaisut

Tunnistetut ratkaisut tulivat haastatteluissa esille laajemmin haastattelun eri vaiheissa. Jotkut haastateltavat sivusivat aihetta jo kertoessaan haasteista. Kysymys ratkaisuista, joita asiantuntijat ovat löytäneet tai pyrkineet löytämään, liitettiin haastattelussa haastateltavien tunnistamiin haasteisiin. Ratkaisuista saatettiin siis kysyä esimerkiksi näin:

''No minkälaisia ratkaisuja olette pyrkineet löytämään näihin haasteisiin? ''(H)

Tarpeen vaatiessa kysyttiin tarkentavia kysymyksiä tietyistä aihealueista, mikäli haastateltava oli maininnut ne aiemmin.

Tulkinnallisuudesta kumpuaviin haasteisiin pyrittiin vastaamaan olemalla mahdollisimman hyvin ajan tasalla siitä, mitä tietosuojan saralla tapahtuu ja peilaamalla omaa tekemistä siihen, minkälaisia päätöksiä on tehty EU:ssa. Riskiperusteinen lähestymistapa, jossa arvioidaan jatkuvasti tietosuojaan liittyviä riskejä, koettiin yhdeksi tavaksi hallita haasteita ja mahdollisia tietosuoja-asetuksesta koituvia ongelmia. Epävarmuus kuitenkin näkyi vastauksissa:

> ''Pyritty niinku tekemään sen mitä voidaan ja sitten perustelemaan, että miksi näin, että siinä on myös ollut paljon sitä niinku dokumentointi Jumppaa mitä siihen on liittynyt.'' (A1)

Kokemuksia leimaa, ettei tietosuojan suhteen voida olla täysin varmoja siitä, mikä on riittävää vaatimustenmukaisuuteen. Dokumentointi nousi monen haastateltavan vastauksessa esille ratkaisuksi vallitsevaan epätietoisuuteen. Pyritään siis kattavalla dokumentaatiolla noudattamaan vaatimuksia, vaikka ei olla aivan varmoja siitä, mitä se edellyttää.

Tulkinallisuuden ja epäselvyyksien ratkaisemiseksi haastateltavat kokivat vaihtoehtojen olevan vähissä. Käytännössä uusia ratkaisuja oli tulevaisuuden varalle todella vähän ja tarkoituksena oli jatkaa oman tekemisen ja lainsäädännön kartoittamista. Omat keinot vaikuttamiseen koettiin vähäisiksi:

> ''Että se on ehkä enemmän sitten sellainen, että pyritään vaan niinku seuraamaan sitä. viranomaiskäytäntöä ja ja noit tuomioistuinratkaisuja ja muuta se on ehkä niinku se ongelma luonteeltaan sellainen, että ei siihen oikein voi voi muuta tehdä.''(A1)

Eräs haastateltavista totesi, että mahdollisia ratkaisuja voisi tulla, kun EU:n komissio tekee seuraavaksi kattavan tarkastelun (eng. review) tietosuoja-asetuksesta.

Tietosuojan koulutuksen ja jalkauttamisen haasteisiin ratkaisua asiantuntijat olivat hakeneet luonnollisesti koulutuksen kehittämisestä. Jalkauttamisen ja ymmärtämisen kannalta koettiin tärkeäksi myös, että tietosuojaan liittyviin kysymyksiin olisi apu helposti saatavilla. Tätä pyrittiin toteuttamaan organisaatioissa koulutusten lisäksi esimerkiksi jakamalla tietosuojaan liittyvää tietoutta intranetin kautta. Toisaalta kun jossain organisaatioissa etäisyydet, ulkoistettu tietosuoja tai suuret henkilömäärät koettiin haasteeksi, nähtiin organisaatioiden tietosuoja-asiantuntijan tai tietosuojavastaavan saatavuuden olevan yksi ratkaisu tehokkaampaan jalkauttamiseen. A6 toi tämän esille seuraavasti:

> ''…Että sitten kun on ihmisenä tutumpi, niin se on helpommin lähestyttävä ja silloin niitä vähän niinku semmoisiakin kysymyksiä, jotka aikaisemmin antoi olla… sulla on se ihminen joka sitä vastaa siinä niinku läsnä ja sä tunnet sen niin silloin tavallaan siinä käy niin että silloin se kysyit sen pienemmänkin kysymyksen.''(A6)

Ratkaisuna voidaan nähdä sisäisen tietosuojan järjestäminen ulkoisen palveluntarjoajan sijaan. Koulutuksen ja jalkauttamisen tehostamiseksi oli suunnitteilla ratkaisuja tulevaisuudessa muutamilla asiantuntijoilla:

> ''Tuotaisiin niin kun tietoturva ja tietosuoja niinku tosi lähelle sitä niinkun työntekijää, että meillä on tämmöinen hieno visio, että me tehtäisiin semmoisia lyhyitä pikku videoita mitä kaikki voisi käydä katsomassa, että joo että hei että siellä käytäisiin aina joku joku tämmöinen pikkutilanne niinku läpi.''(A2)

Näillä keinoilla pyritään myös tulevaisuudessa jalkauttamaan tietosuojatekemistä organisaatiossa niin, että se huomioitaisiin paremmin jokapäiväisessä tekemisessä. Yksi haastateltava oli myös viemässä eteenpäin teknisten ratkaisujen käyttöönottoa organisaatiossaan. Organisaatioissa voi olla vaikea perustella tietosuojatyökaluihin investoimista, koska prosessit ovat toimineet aikaisemminkin ilman niitä.

Tietosuoja-asetuksen alun sekavuutta pyrittiin myös ratkaisemaan sillä, että dokumentoitiin kaikkea mahdollista tietosuojaan liittyvää. Tiedon jakaminen ja koulutus koettiin tärkeäksi alusta asti:

> ''Tiedon jakaminen ja ja koulutus oli se niinku pääasiallinen keino.''(A1)

> ''En niinku ihan säännöllisesti pystynyt käymään pitämään itse koulutuksia, kun se oli siinä oman toimen ohella, niin sitten meille hankittiin se verkkokoulutus ympäristö, että henkilöstö kouluttautui siinä verkkokoulutuksessa ja sitten minä tarpeen mukaan kävin aina ja jalkauduin niinku erilaisiin tilaisuuksiin kouluttamaan''(A7)

> ''Elikkä siinä niin kun toteutuu niinku se, että koulutetaan ja seurataan ja täytetään se osoitusvelvollisuus, että ollaan ollaan toimittu niinku oikein.'' (A2)

Haastateltava A1 nosti esille resurssoinnin ja vastuunjaon olleen hyvä ratkaisu näihin ongelmiin, vaikka oli myös uransa aikana huomannut, ettei kaikissa organisaatioissa näihin ollut panostettu tarpeeksi. Asiantuntijan A5 kokemuksien mukaan aikainen jalkauttaminen ja prosessien luominen olivat helpottaneet paljon myöhempää tietosuojatyötä:

> ''…mutta toisaalta sitten se näkyy niinku nykypäivänä, että koska niihin panostettiin niin paljon niin niin tota nyt on sitten suht toimivat prosessit.''(A5)

Heti tietosuoja-asetuksen alussa luodut selkeät prosessit esimerkiksi tietoturvaloukkauksille, vaikutustenarvioinneille ja tietopyynnöille koettiin suureksi avuksi tietosuojan hallinnan kannalta. Prosesseja on sitten kehitetty lainsäädännön ja kokemuksen mukaan. A5:n organisaatiossa myös vastuunjako tietosuojan hallinnassa oli toteutettu asetuksen alusta asti toimivalla ja tietosuojan hallintaa tukevalla tavalla. Asetuksen voimaantulon jälkeen tärkeäksi nostettiin tilanteen kartoittaminen ja kuiluanalyysin tekeminen. Tämä mahdollisti prosessien luomisen ja tietosuojan jalkauttamisen:

> ''niinku sisäisiä politiikkoja rekisteröidyn oikeuksien toteuttamisen ohjeita, tietoturvaloukkaus dokumentaatio tai tietoturvaloukkauksista ohjeita, että miten näitä käsitellään niinku lähdettiin luomaan niitä ohjeistuksia ja prosesseja''(A4)

Vahvasti strukturoitu ja organisoitu organisaatio vaikutti kärsivän valmiiksi jo vähemmän haasteista. Asiantuntijoiden mukaan näissä organisaatioissa tekeminen oli jalkautettu hyvin ja prosessit rakennettu tukemaan tietosuojan hallintaa. Haastateltavat kokivat näissä organisaatioissa, että heillä oli mahdollisuuksia myös vaikuttaa paremmin organisaation toimintaan.

5.3 Tekniset ja organisatoriset apuvälineet

Teknisistä ja organisatorisista apuvälineistä kysyttäessä vastaukset olivat lähtökohtaisesti lyhyempiä, eikä asiantuntijoilla ollut näistä niin paljon sanottavaa. Kysymys teknisisistä apuvälineistä ymmärrettiin hyvin ja haastateltavat alkoivat myös itsenäisesti kertomaan, oliko käyttöönottoa suunniteltu, miksei ollut otettu käyttöön tai aikaisemmista kokemuksista teknisten apuvälineiden kanssa. Kysymys organisatorisista apuvälineistä tarkennettiin mainitsemalla, että ne voivat olla esimerkiksi viitekehyksiä, kolmannen osapuolen sertifiointeja tai standardeja.

Haastatteluissa tuli ilmi, että suurin osa käytti ja oli käyttänyt työssään apuna lähinnä Microsoft Officen työkaluja. Pääsääntöisesti tietosuojan hallinnan apuvälineenä käytettiin Microsoft Wordia ja Exceliä. Tämä tuli selväksi useimpien haastateltavien vastauksista nopeasti:

> ''Ei ole, että meillä sit tai siis meillä on Excelissä on meidän niinku ROPA ja käytännössä sitten meillä on SharePoint sivustolla on koottuna meidän selosteita ja kaikki tavallaan siihen liittyvää materiaalia.'' (A6)

> ''Ensisijaisesti on pakko vastata, että Microsoft Excel. Tuota se on se on niin kun ollut kyllä se keskeisin siis on ollut joissain on ollut ollut käytössä jotain työkaluja.''(A1)

> ''Minä niin kun pyöritän pääsääntöisesti ihan tuolla Microsoftin työkaluilla Excel Word linjalla, mutta sitten asiahallintaan vien esimerkiksi tietoturvaloukkaukset''(A7)

> ''Joo pitkälti Excel, Word''(A4)

Osalla Excel ja Word -dokumenteista oli tehty valmiita lomakkeita ja arviointeja, joita voitiin jakaa eteenpäin organisaatiossa. A1 oli työskennellyt tietosuojakonsulttina ja nähnyt tietosuojan hallintaa useammassa organisaatiossa. Monessakaan organisaatiossa hän ei ollut kuitenkaan nähnyt käytettävän teknisiä apuvälineitä juuri tietosuojan hallintaan. Kolmessa organisaatiossa oli käytössä hallintajärjestelmiä, joissa oli mahdollisuus myös tietosuoja-asetukseen liittyviin toiminnallisuuksiin, mutta niitä ei ollut laajemmin käytetty hyväksi. Jotain helpotusta niistä yksi asiantuntija kuitenkin sai dokumentoinnin hallinnan kautta.

Monissa haastatteluissa tuli ilmi, että organisaatioissa on apuna jonkinlainen verkkokoulutusympäristö, jonka kautta hoidetaan myös tietosuojakoulutuksia. Organisaatioiden intrat oli monissa tapauksissa jalostettu tietosuojan jalkauttamisen ja koulutuksen käyttöön. Yhdessä organisaatiossa oli myös käytössä tietoturvaloukkauksiin ja tietopyyntöihin tiketointijärjestelmä, jota ilman olisi asiantuntijan mukaan melkein mahdotonta pärjätä.

Harvemmalla organisaatiolla oli käytössä teknistä apuvälinettä juuri tietosuojan hallintaan. Kuitenkin nämä, joissa oli otettu tai oltiin ottamassa käyttöön, oli positiivisia kokemuksia. Näissä organisaatioissa nähtiin apuvälineiden helpottavan tietosuojan hallintaa. Yhden haastateltavan organisaatiossa oltiin juuri ottamassa käyttöön uutta järjestelmää apuvälineeksi tietosuojan hallinnalle. Haastateltava perusteli hankintaa juuri tietosuojan hallinnan kautta:

> ''Tavallaan se tietosuojaan liittyvä kaiken dokumentaation ja voisiko sanoa osoitusvelvollisuuden kattavan dokumentaation hallinta on niinku aika hankalaa tämmöiselle erillisille tiedostoille, joita käsitellään erikseen ja niin sanotusti niinku pyöritellään niinku erillisenä. Niillä on vaikea saada ja hallita kokonaiskuvaa ja tota tän takia sitten niinku lähdettiin tosiaan kartoittamaan soveltuvia välineitä.'' (A3)

Haastateltava näki apuvälineen tuoneen ja tuovan hyötyä myös tulevaisuudessa:

> ''Näetkö, että siitä on ollut hyötyä?''(H)

> '' No vaikka nyt ollaankin vielä vielä alussa niin niin itse niin kun näen sen sillä, että on ollut hyötyä ja mä uskon siihen, että tulee olemaan hyötyä. Että, se että ton ratkaisun avulla me pystytään saamaan tällaiset sanotaan niinku asiat, joita muutoin hallitaan perinteisillä dokumenteilla, kuten esimerkiksi tietosuojan vaikutustenarvioinnit. Mahdolliset muut tämmöiset niin kun arvioinnit, kuten esimerkiksi nämä kolmansiin maihin tehtävät tai kansainvälisiä tiedonsiirtoja koskevat niinku tarpeelliset arvioinnit.'' (A3)

A3 lisäsi vastauksessaan vielä myöhemmin tasapainotestien tekemisen apuvälineellä. Yhdeksi hyödyksi hän näki, että kyselyt on helppo toteuttaa ja niiden lähettäminen edestakaisin on helpompaa kuin staattisilla dokumenteilla sähköpostin välityksellä. Yhden asiantuntijan organisaatiossa oli käytössä PrivacyAnt -ohjelmisto. Ohjelmistoa käytettiin esimerkiksi vaikutustenarviointien suorittamiseen. Ohjelmiston käyttö koettiin myös tämän organisaation tapauksessa hyödylliseksi:

> ''Just eilen oli niinku just, että jos meidän työpajassa niinku tää käytiin siitä keskustelua että me saadaan sinne aivan niin kun tosi loistava tietopankki. Että, kun me saadaan niin kun, kun me on niinku toteutettu sitä silleen, että me ollaan niitä niin kun niitä yksikön yksiköiden henkilöitä haastateltu ja tehty heidän kanssa niitä tietovirtakarttoja.''(A2)

Erityisen hyödylliseksi ominaisuudeksi tässä tapauksessa koettiin tietovirtakarttojen tekeminen, joka mahdollisti paremman kuvan tietosuojan hallintaan.

Myös konsulttina työskennellyt asiantuntija koki, että organisaatiot olivat hyötyneet erillisten tietosuojan hallinnan apuvälineiden käytöstä:

> ''Nääks sie että ne on auttaneet niissä niissä tapauksissa, joissa niitä on ollut käytössä ni onks ne helpottanut työtä?''(H)

> ''Niissä tapauksissa missä niitä on käytetty niin joo on on auttanut.'' (A1)

Yhdessäkään haastattelussa ei tullut ilmi, että käytetyt apuvälineet olisivat tehneet työstä vaikeampaa tai haastavampaa kuin aikaisemmin. Näin oli myös tapauksissa, joissa asiantuntijat eivät enää työskennelleet organisaatiossa, jossa se oli käytössä, joten syy myönteisyyteen ei ollut pelkästään tietosuojainvestointien puolustaminen tai oikeuttaminen.

Konsulttina työskennellyt asiantuntija myös muisteli, että monissa organisaatioissa oli suunniteltu teknisten apuvälineiden käyttöönottoa. Myös A7 pyrki edistämään tilannetta organisaatiossaan, jotta sinne saataisiin teknisiä apuvälineitä tietosuojan hallintaan. Haastateltavat, joilla oli käytössä apuvälineitä, aikoivat käyttää niitä jatkossakin. A2 luotti tulevaisuudessa toimittajan tukeen PrivacyAntin ohjelmistojen kehittämisen kanssa. Tulevaisuudelta toivottiin, että käytettävät järjestelmät sopivat jatkossakin organisaation tarpeisiin, mutta myös riskit tiedostettiin:

> ''Nää välineet on kuitenkin ja työkalut on luonteeltaan aina sellaisia, että niihin liittyy kuitenkin aina tavallaan semmoinen tietynlainen markkina ja toimittaja riski, että että tota toiminta ja elää ja kuolee.'' (A3)

Lisäksi haastateltava (A3) tiedosti, että myös organisaation tarpeet voivat muuttua. Asiantuntijat tunnistivat myös muita haasteita teknisisissä apuvälineissä. Kaksi asiantuntijaa nosti esille, että teknisissä ratkaisuissa joudutaan usein kuvaamaan esimerkiksi organisaation järjestelmiä liian yksityiskohtaisesti. Tämä voi tehdä käyttöönotosta liian työlästä ja monimutkaista:

> ''Vähän niiku kaatunut siihen että joutuu liian yksityiskohtaisesti niiku järjestelmät tuomaan tai sillee, että ne ei oo taipunut niihin niiku mitä on haettu.''(A1)

> ''Niinkun käsittelytoimen näkökulmasta niin sitten sitten se että se oli tämmöinen niinku järjestelmäpohjainen niin se ei oikein ihan siihen palvellut.''(A4)

Käyttöönotto ja käyttäminen tuo yleensä mukanaan kustannuksia ja riskejä, jotka voivat estää teknisten apuvälineiden hankintaa. Haastateltavilta ei kuitenkaan kysytty järjestelmien kustannuksista.

Organisaatioilla ei ollut suoranaisesti käytössä viitekehyksiä tai kolmannen osapuolen sertifiointeja tai standardeja tietosuojan hallintaan liittyen. Kolmelta haastateltavalta tuli kysymykseen lyhyt ja nopea ''ei'' vastaus. Yleisesti organisaatioissa oli menty tietosuoja-asetuksen mukaan:

> ''Ei ole jos puhutaan tyyliin jostakin standardi malleista niin ei ole. Että ihan olen pitänyt ohjenuorana vaan GDPR ja sen artikloita. ''(A7)

Osa haastateltavista mainitsi kuitenkin, että käytössä on tietoturvan puolella standardeja kuten ISO 27001:

> ''Eikä kyllä ihan selkeästi ole niinku mitään semmoista suunnitelmaa vielä, että että jotakin sellaista niinku tehtäisiin, että ainoastaan niinku tietoturvan puolella meillä on niinku meidän järjestelmissä tota niin ISO 27001.'' (A3)

> ''Miten paljon siellä (tietoturvan puolella) on käytössä, vaikka sitä niinku iso 27001 tai sitten sitä Nistin niitä frameworkkeja tai muuta, niin siihen nähden on niinku tietosuoja puolella, niin ehkä vähemmän. ISO 27701 laajennus niin niin aika vähän se mun mielestä on ottanut tuulta alleen.''(A1)

Kuten A3:sen sitaatista käy ilmi, ei organisaatioilla ollut myöskään suunnitelmissa ottaa käyttöön tämänkaltaisia organisatorisia apuvälineitä. Asiantuntijat tiedostivat, että tietoturvan puolella standardien käyttö on paljon yleisempää. Tietosuojan puolella standardien perään ei myöskään kysellä samalla tavalla. Haastateltavista kaksi näki tärkeämmäksi tietosuojan jalkauttamisen jatkamisen organisaatiossa. Muutama haastateltava toi esiin, että käytössä on oma tietosuojan hallintamalli. Hallintamallit eivät perustuneet suoraan mihinkään standardiin tai viitekehykseen, mutta niistä oli saatettu ottaa joitain osia käyttöön oman työn tueksi:

> ''En ole pyörittänyt semmoista hallintomallia, joka olisi esimerkiksi suoraan jonkun ison standardin pohjalle, mutta oon tehnyt ohjeistuksia niinku siitä näkökulmasta.''(A4)

Osa kertoi, että eivät ole kokeneet eri organisatoristen apuvälineiden sopivan suoraan heidän organisaationsa käyttöön erilaisista syistä. Vastauksista tuli ilmi, ettei tietosuojan viitekehyksiä, standardeja tai sertifiointeja ole haluttu ottaa käyttöön suomalaisissa organisaatioissa, joka voi osaltaan selittää, miksi tietosuojan hallinnassa ei tahdo löytyä yhtenäisiä toimintamalleja. Jokaisella organisaatiolla tuntuukin olevan enemmän ja vähemmän erilaisia tapoja, joilla tietosuojaa hallitaan. A3 kuitenkin peräänkuulutti haastattelun lopuksi, että yhtenäistä standardia tietosuojan hallintaan kaivattaisiin ihan maailmanlaajuisesti:

> ''On sekin niinku niinku kuitenkin nyt se yks kehitysvaihe, että että jos niinku ajatellaan pitkässä juoksussa järkevää, niin tietyllä tavallahan meillä pitäisi olla niinku hyvin standardi tapa niinku hoitaa tätä tietosuojaa maailmanlaajuisesti.''(A3)

Yleisesti hyväksytyt ja laajasti käytetyt viitekehykset, standardit tai sertifioinnit voisivat toisaalta auttaa myös tietosuoja-asetuksen tulkinnallisuuden kanssa. Epävarmuus poistuisi, jos tiedettäisiin, että kaikki tai ainakin suurin osa organisaatioista hoitaisi tietosuojan hallinnan yhteisillä hallintamalleilla.

6 POHDINTA

Tutkielman tavoitteena oli teemahaastatteluiden avulla tarkastella tietosuoja-asiantuntijoiden kokemia haasteita, ratkaisuja sekä käytettyjä apuvälineitä organisaatioiden tietosuojan hallinnan näkökulmasta. Vastauksia haettiin kolmeen tutkimuskysymykseen:

1. **Minkälaisia haasteita organisaatioiden tietosuojan hallinnassa on?**
2. **Miten näitä haasteita on ratkaistu tai pyritään ratkaisemaan?**
3. **Minkälaisia organisatorisia tai teknisiä apuvälineitä/ratkaisuja organisaatioissa on käytössä tietosuojan hallintaan?**

Tässä kappaleessa tarkastellaan tutkielman tuloksia ja tehdään niistä johtopäätökset. Lopuksi vielä esitetään jatkotutkimusehdotuksia. Tuloksia tarkastellaan sisällönanalyysin tapaan aineistolähtöisesti sekä fenomenologisen metodin mukaisesti asiantuntijoiden kokemuksien kautta. Tutkielma laadullisena tutkimuksena ja suomalaisten asiantuntijoiden kokemukset suomalaisissa organisaatioissa spesifinä kontekstina on otettu huomioon pohdinnoissa. Tämä tarkoittaa, että haastatteluaineisto antaa tietoa vain pienen joukon kokemuksista, eikä ole siinä mielessä yleistettävissä edes Suomen tasolla. Kokemuksissa on aina myös yhteisöllinen ja kulttuurinen puoli, joten tutkielma paljastaa myös jotain yleistä ainakin omassa kulttuurisessa ympäristössään (Laine, 2018, 24). Kuitenkaan tutkielman tulosten vertailu aikaisempiin tutkimustuloksiin laajemmassa mittakaavassa ei tässä mielessä ole tutkielman kannalta tarkoituksenmukaista. Kuten Ruusuvuori kollegoineen (2010, 19–20) huomauttaa, aikaisempi teoria vaikuttaa vääjäämättä jollakin tasolla tulkintoihin ja valintoihin, joten pohdinnassa pyritään ottamaan huomioon myös nämä vaikutukset. Tutkielman on tarkoitus tarjota ymmärrystä asiantuntijoiden kokemuksien kautta heidän omassa kontekstissaan sekä mahdollistaa syvällisempää pohdintaa tietosuojan hallinnan haasteista ja ratkaisuista.

6.1 Tulosten tarkastelua ja johtopäätökset

Tutkielmalle ei ollut asetettu erityisiä hypoteeseja, etteivät ne ohjaisi esimerkiksi tulosten tulkitsemista. Kirjallisuuskatsauksessa nostettiin kuitenkin esiin mahdollisia aihealueita, jotka voisivat nousta haastatteluissa esille. Tulosten tarkastelussa nähdään, että teorian liiallinen ohjaava vaikutus olisi voinut vaikuttaa vastauksiin. Koska haastateltavat saivat kertoa laajasti kokemuksistaan ilman liian tarkkoja raameja, esiintyi tutkielmassa tuloksia, joita ei osattu odottaa. Tässä luvussa tarkastellaan tuloksia liittyen haasteisiin, ratkaisuihin sekä lopuksi teknisiin ja organisatorisiin apuvälineisiin.

6.1.1 Haasteet

Tietosuojan hallinnan haasteisiin liittyvien kysymysten vastauksissa nousi kaikista merkityksellisimmiksi neljä aihetta:

1. Tietosuojan jalkauttaminen
2. Tietosuojakoulutus
3. Tietosuoja-asetuksen tulkinnallisuus
4. Epävarmuus tietosuojaan liittyvästä vaatimustenmukaisuudesta

Nämä voidaan tiivistää tarkemmin vielä kahdeksi teemaksi niiden samankaltaisuuksien vuoksi. Asiantuntijat myös puhuivat näistä tekijöistä yleensä sekaisin, joten niiden voidaan myös sen puolesta olettaa kiinnittyvän toisiinsa. Tietosuojan hallinnan haasteiden kaksi pääteemaa, joita tässä kappaleessa käsitellään yhdessä ovat

- Tietosuojan jalkauttaminen ja koulutus
- Tietosuoja-asetuksen tulkinnallisuus ja siitä johtuva epävarmuus

Nämä haasteet toistuivat ajankohdasta huolimatta. Ne olivat olleet haasteita aikaisemmin ja koettiin, että tulevat olemaan haasteita myös tulevaisuudessa. Teemat eivät olleet myöskään täysin irrallisia toisistaan, vaan esimerkiksi jalkauttamisen yhtenä haasteena nähtiin tietosuoja-asetuksen tulkinnallisuus. Näitä teemoja yhdisti myös kokemus resurssien puutteesta, mutta resurssien puutetta ei nähty haasteena itsessään, vaan enemmänkin hidasteena tai esteenä aikaisemmin mainittujen haasteiden ratkaisemiselle. Näiden kahden pääteeman kanssa tarkastellaan myös lyhyemmin muita aihealueita, kuten siirtoja kolmansiin maihin. Näiden aihealueiden nähtiin kuitenkin aina jollakin tavalla johtuvan näistä kahdesta pääteemaasta.

Ensimmäinen teema oli tietosuoja-asetuksen jalkauttaminen ja koulutus organisaatiossa. Seitsemästä haastateltavasta viisi mainitsi nämä haasteiksi tietosuojan hallinnassa. Koulutus ja jalkauttaminen esiintyivät haastateltavien kokemuksissa samassa kontekstissa. Tietosuojakoulutukseen liittyviä haasteita

olivat vaikeudet saada tietosuojan merkitys ymmärretyksi organisaatiossa ja opetettua monimutkainen tietosuoja-asetus tarvittavalla tavalla. Tämä vaikutti suoraan myös jalkauttamisen haasteisiin. On vaikea saada työntekijät ottamaan huomioon tietosuoja jokapäiväisessä työssä, jos sen arvoa ei ymmärretä tai ylipäätänsä ei ymmärretä, mitä pitäisi ottaa huomioon. Konkreettisia esimerkkejä vastauksissa oli esimerkiksi, kuinka jalkauttaa tietoturvapoikkeamista ilmoittaminen. Riittävä kouluttaminen ja jalkauttaminen on ongelma tietosuojan hallinnassa erityisesti siitä syystä, että tietosuojan toteuttaminen on lähes poikkeuksetta koko organisaation laajuinen tehtävä. Yksikään asiantuntija tai tietosuojavastaava ei voi hallita yksin vähänkään isomman organisaation tietosuojaa, vaan tekeminen pitää olla sisäänrakennetun tietosuojan periaatteen mukaisesti osa koko organisaation toimintaa.

Koulutus ja jalkauttaminen oli nähty haasteena tietosuoja-asiantuntijoiden urien alusta asti, eikä helpotusta nähty tulevaisuudessakaan, joten myös tämä teema on ollut haasteena koko tietosuoja-asetuksen ajan. Mielenkiintoista oli, että siitä huolimatta kirjallisuuskatsausta tehdessä, ei tullut vastaan edes mainintaa samankaltaisista haasteista. Tutkimusta aiheesta ei löytynyt, vaikka hakusanoja tarkensi jälkikäteen hakemaan nimenomaisesti tietosuojan jalkauttamista ja kouluttamista. Syynä voi olla, että tutkimusaiheena se liikkuisi enemmän kasvatustieteen alueella. Tietosuoja tutkimusalueena on perinteisesti liitetty enemmän tietotekniikkaan ja oikeustieteisiin. Haastatteluiden tuloksia ei voida tässä mielessä verrata aikaisempaan kirjallisuuteen, koska sitä ei löytynyt.

Toinen teema eli tulkinallisuus ja siitä johtuva epävarmuus nousi kirjallisuuskatsauksessa esille. Esimerkiksi Rubinstein ja Good (2020, 43–44) toteavat artiklan oletusarvoisesta tietosuojasta olevan epäselvä, mikä voi johtaa siihen, ettei voida olla varmoja, toteuttaako organisaatio sitä riittävällä tasolla. Yllätyksenä ei tullut sekään, että asiantuntijatkin pitivät tietosuoja-asetusta liian tulkinnanvaraisena, sillä samanlaisia tuloksia oli saatu esimerkiksi vaikutustenarviointeihin liittyen (Ferra ym., 2019, 14). Haastatteluissa tulkinnallisuus ja epävarmuus tulivat yleisemmin esille, eikä asiantuntijat liittäneet niitä yleensä mihinkään tiettyyn tietosuojan osa-alueeseen. Tästäkin voidaan tulkita, että haaste on tietosuojan hallinnan kannalta kokonaisvaltainen, eikä esiinny vain tiettyjen artiklojen yhteydessä. Muutama haastateltava nosti kuitenkin esimerkkinä osoitusvelvollisuuden ja riskilähtöisyyden hankalaksi asetuksen tulkinnallisuuden takia. Tulkinnallisuus vaikuttaa myös jalkauttamisen ja koulutuksen haasteisiin. Kuinka opastaa esimerkiksi tietoturvaloukkauksista ilmoittamista, jos niiden määrittely on epäselvää (Alunge, 2021, 173).

Historian valossa tilanteen nähtiin kuitenkin parantuneen tietosuoja-asetuksen alkuajoista. Erityisesti asetuksen voimaan tulon jälkeen tietosuojan parissa työskennelleet huomauttivat, että alkuun epävarmuus oli vielä pahempaa, eikä minkäänlaista varmuutta oman tietosuojan hallinnan riittävyydestä ollut. Lisääntyneet viranomaisohjeet ja osaltaan myös sanktiopäätökset ovat ajan saatossa selventäneet tilannetta, mutta haasteita silti riittää. Tulkinnallisuus ja epävarmuus nähtiin haasteena tulevaisuudessakin, eikä ihmeellistä parannusta tilanteeseen odotettu. Toisaalta odotettiin, että lisääntyvä ohjeistus ja

lainsäädäntö voisivat helpottaa tulkinnallisuutta, kun taas toisaalta pelättiin, että tilanne vain pahenee. Muutama haastateltava odotti, että uudet päätökset Schrems-II tilanteeseen voisivat tuoda selvyyttä siirtoihin kolmansiin maihin.

Siirrot kolmansiin maihin olivatkin yksittäisistä tietosuojan hallinnan alueista ainut, jonka useammat asiantuntijat mainitsivat kysymykseen haasteista. Toisaalta haasteet liittyen siirtoihin kolmansiin maihin ja Schrems-II päätökseen linkittyivät vahvasti myös tulkinnallisuuteen ja epävarmuuteen. Muita haasteita, joita löytyi tuloksista, olivat esimerkiksi tietoturvapoikkeamat, tarkastuspyynnöt, tietoturvarikkomukset, toimittajien kanssa työskentely ja työkalujen puute. Haasteet kuitenkin tiivistyvät näihin kahteen pääteemaan, joista pienemmät kokonaisuudet enemmän tai vähemmän johtuivat.

6.1.2 Ratkaisut

Tuloksien perusteella varmat, kaikenkattavat ratkaisut olivat asiantuntijoiden kokemusten mukaan vähissä. Ratkaisuissa oli myös suurempaa hajontaa, eikä yhtä selviä pääteemoja vastauksista löytynyt, niin kuin niitä löytyi haasteisiin liittyen. Tulkinnallisuuteen ja epävarmuuteen ei koettu olevan melkein ollenkaan pysyviä ratkaisuja tai asiantuntijat kokivat, että mahdolliset ratkaisut haasteisiin eivät olleet heidän käsissään. Epävarmuuteen ja tulkinnallisuudesta johtuviin haasteisiin löytyi muutamia helpottavia toimenpiteitä, jotka nousivat esille useammassa haastattelussa:

- Dokumentointi
- Tietosuojaan liittyvän lainsäädännön kartoittaminen
- Prosessien ja tehtävänjaon kehittäminen

Yhden asiantuntijan organisaatiossa prosessien kehitystä ja selvää vastuunjakoa oli tehty tietosuoja-asetuksen alusta asti. Tehtävänkuvia ja prosesseja kehitetään sen mukaan, kun uusia tarpeita esiintyy. Kyseinen haastateltava ei kokenut haasteita yhtä pahoiksi kuin muut haastateltavat. Organisaatiot ja kokemukset ovat tietysti erilaisia, mutta aikainen valmistautuminen vaikutti tehokkaalta keinolta haasteiden ratkaisemiseksi. Muut ratkaisut olivat enemmän tilanteen kanssa pärjäämistä kuin varsinaisia ratkaisuja, joilla voitaisiin ratkaista haasteita.

Ratkaisut olivat pysyneet myös asiantuntijoiden urien aikana melko samanlaisina. Aivan tietosuoja-asetuksen alussa dokumentointi oli korostuneemmassa roolissa, koska tietoa oli vähemmän. Tietosuoja-asetus koettiin epämääräiseksi, eikä viranomaisohjeistuksia tai sanktioita ollut vielä tullut, jotka olisivat ohjanneet tietosuojan hallintaa. Tulevaisuuden suhteen melkein kaikki asiantuntijat aikoivat jatkaa samoilla ratkaisuilla. Yksi asiantuntija kuitenkin suunnitteli uusien teknisten tietosuojan hallinnan apuvälineiden käyttöönottoa organisaatiossaan.

Ratkaisut tietosuojan jalkauttamisen ja koulutuksen haasteisiin olivat myös vähissä, eikä yksikään organisaatio tuntunut olevan ratkaissut ongelmaa kokonaan. Kaksi mahdollista ratkaisua nousi kuitenkin esille:

- Tietosuojakoulutuksen kehittäminen
- Tietosuoja-asiantuntijoiden/tietosuojavastaavan lähestyttävyys

Kovinkaan konkreettisia esimerkkejä haastateltavat eivät kertoneet siihen, minkälaisia toimia näiden ratkaisujen eteen on tehty. Yhden asiantuntijan tapauksessa hän oli pyrkinyt tekemään itsensä helposti lähestyttäväksi niin, että pienemmistäkin asioista uskallettaisiin kysyä häneltä. Yhdellä asiantuntijalla oli konkreettinen suunnitelma tulevaisuuden varalle: luoda oppimisympäristö, jossa tietosuojaa tuotaisiin lyhyiden videoiden avulla lähemmäs työntekijöitä. Suurimmaksi osaksi asiantuntijat aikoivat pyrkiä ratkaisemaan haasteita tulevaisuudessa samalla tavalla kuin niitä ratkaistiin asetuksen alkuaikoina eli kouluttamalla ja kehittämällä koulutusta. Prosessien kehittäminen ja tehtävien jakaminen tehokkaasti vaikutti yhdessä organisaatiossa pienentävän tulkinnallisuudesta johtuvien haasteiden lisäksi myös jalkauttamisesta johtuvia haasteita. Kyseisessä organisaatiossa työskennellyt asiantuntija vaikutti kaikin puolin kärsivän tietosuojan hallinnan haasteista vähemmän kuin muut haastateltavat. Toisaalta on otettava huomioon, että tutkielmassa ei otettu selvää, mitkä taustat ovat johtaneet siihen, että yhdessä organisaatiossa tehtävänjako ja prosessit on voitu luoda tehokkaasti sekä pystytty jatkuvasti kehittämään myös omaa tietosuojan hallintaa ajan kuluessa. Tähän voi vaikuttaa, että kyseisessä organisaatiossa on ollut alusta asti paremmat resurssit tietosuojan hallintaan ja tietosuojan merkitys on tiedostettu koko henkilöstön tasolla.

6.1.3 Tekniset ja organisatoriset apuvälineet

Asiantuntijat olivat käyttäneet kaikissa tapauksissa teknisinä apuvälineinä tietosuojan hallinnassa Microsoftin työkaluja, kuten Wordia, Exceliä ja SharePointia tiedostojen hallitsemiseen. Tämä ei tullut yllätyksenä niiden yleisyyden ja monipuolisten käyttömahdollisuuksien vuoksi. Myös muita apuvälineitä, joiden alkuperäinen tarkoitus on joku muu kuin tietosuojan hallinta, käytettiin tietosuojan hallinnassa apuna. Näitä olivat esimerkiksi organisaatioiden intrat, verkkokoulutusympäristöt, hallintajärjestelmät ja tiketointijärjestelmät. Yhdellä asiantuntijalla oli aikomus ottaa käyttöön teknisiä apuvälineitä tulevaisuudessa ja toisen organisaatiossa oltiin kehittämässä omaa apuvälinettä helpottamaan tietosuojan hallintaa.

Varsinaisia tietosuojan hallintaan tarkoitettuja apuvälineitä oli käytössä kahden haastateltavan organisaatiossa. Tämän lisäksi kahdella muulla asiantuntijalla oli jonkunlaista kokemusta vastaavista järjestelmistä aikaisemmin uralla. Kaikissa tapauksissa kokemukset olivat hyvinkin positiivisia ja asiantuntijat kokivat, että apuvälineistä oli oikeasti hyötyä tietosuojan hallinnassa. Haastatteluissa tuli ilmi seuraavia ominaisuuksia, jotka koettiin erityisen hyödyllisiksi:

- Erilaisten arviointien suorittaminen (esim. tietosuojaa koskeva vaikutustenarviointi, tasapainotesti ja arviointi siirroista kolmansiin maihin)

- Järjestelmän toimiminen tietopankkina
- Tietovirtojen mallintaminen
- Mallinnus selosteen käsittelytoimista

Tekniset apuvälineet eivät kuitenkaan ratkaisseet näiden organisaatioiden haasteita, vaan olivat muuten tukemassa ja auttamassa tietosuojan hallintaa. Myös asiantuntijat, jotka olivat aiemmin urallaan työskennelleet organisaatioiden parissa, joissa oli käytössä tämän kaltaisia teknisiä apuvälineitä, kokivat ne hyödyllisiksi. Konsulttina työskennellyt asiantuntija myös muisteli, että monissa organisaatioissa oli suunniteltu tulevaisuudessa ottaa käyttöön järjestelmiä tietosuojan hallintaan. Yhden haastateltavan organisaatiossa oli myös suunnitteilla ottaa käyttöön teknisiä apuvälineitä tulevaisuudessa. Muissa organisaatioissa ei ollut suunnitelmia ottaa käyttöön uusia apuvälineitä. Kahdessa organisaatiossa, joissa oli jo käytössä teknisiä tietosuojan hallinnan apuvälineitä, aiottiin jatkaa niiden käyttöä tulevaisuudessa, jos vain mahdollista.

Organisatorisia apuvälineitä nimenomaan tietosuojan hallintaan ei ollut käytössä yhdenkään haastateltavan organisaatiossa. Haastateltavat huomauttivat, ettei tietosuojan standardeja, viitekehyksiä tai sertifiointeja ollut käytetty aikaisemminkaan, eikä niitä ollut tarkoitus ottaa käyttöön tulevaisuudessa. Muutamassa organisaatiossa olemassa olevia viitekehyksiä oli käytetty hyväksi oman hallintamallin kehittämisessä. Koettiin, etteivät mahdolliset organisatoriset apuvälineet toimineet suomalaisissa organisaatioissa sellaisinaan. Mitkään tietosuojan standardit, viitekehykset tai sertifioinnit eivät ole saaneet sellaista asemaa, että niitä noudattamalla voisi suoraan osoittaa oman organisaation vaatimustenmukaisuuden. Tietoturvan puolella tilanne on toinen, sillä esimerkiksi ISO 27001 on yleisesti hyväksytty sertifiointi ja organisaatiot voivat sillä suoraan osoittaa, että tietoturva-asiat ovat kunnossa. Tämän nosti esille myös muutama haastateltava. Näistä syistä organisaatiot olivatkin hallinneet tietosuojaa lähinnä tietosuoja-asetuksen ja viranomaisohjeiden mukaisesti. Voidaan nähdä, että nämä organisatoriset apuvälineetkin useasti loppujen lopuksi perustuvat samoihin säädöksiin. Yleistä standardia, joka yhdistäisi tietosuojan hallinnan ympäri maailmaa kuitenkin toivottiin.

6.2 Jatkotutkimusehdotukset

Laadullisessa tutkimuksessa hyviä puolia on, että sen kautta jotain ilmiötä voidaan tutkia syvemmin. Tämä voi parhaillaan avata uusia mahdollisuuksia jatkotutkimuksille, kun ilmiötä ymmärretään paremmin. Näin oli myös tämän tutkielman kohdalla, sillä se avasi vähän tutkittua aluetta laajasti asiantuntijoiden kokemuksien kautta. Tämän tutkielman parhaita puolia onkin, että se mahdollistaa paljon potentiaalisia jatkotutkimuskohteita.

Tietosuojan hallinnan haasteista tutkielman tulokset toivat esille jotain uutta ja jotain odotettua. Lainsäädännön, tietosuoja-asetuksen ja ohjeistuksen

tulkinnallisuus sekä siitä johtuva epävarmuus on tullut esille myös aikaisemmassa tutkimuksessa ja tämä tutkielma toi lisää todisteita siitä, että se todella on haaste tietosuojan hallinnalle. Kuitenkin myös tätä ilmiötä voidaan tutkia lisää. Tässä tutkielmassa haasteita käsiteltiin useimmiten hyvin yleisellä tasolla, koska kysymyskin oli aseteltu hyvin laajaksi. Onko asetuksessa esimerkiksi jotkin tietyt artiklat, jotka koetaan erityisen tulkinnallisiksi? Mitkä tekijät tekevät juuri tietosuojalainsäädännön niin tulkinnalliseksi? Asetelmaa voitaisiin tutkia määrällisessä mielessä. Suurella otannalla saisi paremman kuvan siitä, kuinka iso prosentti tietosuoja-asiantuntijoista kokee asetuksen tulkinnalliseksi ja sen takia tietosuojan hallinnan haasteelliseksi.

Vaikka tässä tutkielmassa hyvinkin yleiseksi haasteeksi koettiin tietosuojan jalkauttaminen ja tietosuojakoulutus, on aiheesta kansainvälisestikin vähän tutkimusta. Jatkotutkimuskohteita on myös tästä syystä todella laajasti. Haastateltavien vastaukset jalkauttamisen ja tietosuojakoulutuksen haastavuudesta tietosuojan hallinnan kannalta olivat myös melko yleistasoisia. Tarkempaa tutkimusta, mikä näissä on erityisen haasteellista, olisi tarpeellista tehdä. Lisäksi syitä, miksi jalkauttaminen ja tietosuojakoulutus ovat haasteellisia, olisi mielenkiintoista tutkia tarkemmin. Johtuvatko haasteet esimerkiksi myös tulkinnallisuudesta, jolloin jalkauttaminen ja koulutuskin on hankalampaa? Tai nähdäänkö tietosuojaan liittyvät kysymykset organisaatioissa epämerkityksellisiksi verrattuna tietoturvaan? Tietosuojan jalkauttamisen ja koulutuksen haasteiden esiintyvyyttä voitaisiin tutkia määrällisesti, jotta niiden yleisyyttä voitaisiin paremmin arvioida.

Ratkaisuja näihin tietosuojan hallinnan haasteisiin löytyi aineistosta vain muutamia, eivätkä nekään suoranaisesti poistaneet ongelmia. Merkittävää tutkimusta voitaisiin tehdä siitä, kuinka tietosuojaan liittyvää tulkinnallisuutta voitaisiin vähentää. Tarkoittaisiko se lisää ohjeistusta vai koko tietosuoja-asetuksen uudelleenrakentamista? Näihin haasteisiin oman vaikuttamisen mahdollisuudet tietosuoja-asiantuntijat kokivat kuitenkin olevan vähäisiä ja ratkaisujen pitäisi tulla esimerkiksi Euroopan komission tasolta. Jalkauttamisen ja tietosuojakoulutuksen haasteiden ratkaisemiseksi voitaisiin tutkia, onko jotain keinoja, joilla näitä voitaisiin tehostaa. Ratkaisut voisivat kehittyä, jos haasteiden juurisyitä ymmärrettäisiin paremmin.

Tehokkain ratkaisu tietosuojan hallinnan haasteisiin vaikutti olevan aikainen prosessien ja työnjaon kehittäminen. Hyödyllistä olisi tutkimus, jonka avulla voitaisiin löytää keinoja, kuinka tietosuojan hallinnan työnjakoa ja prosesseja voitaisiin organisaatioissa kehittää tehokkaasti. Myös näitä tekijöitä, jotka vaikuttavat niiden kehittämiseen, olisi mahdollista tutkia tarkemmin. Vaikuttaako siihen esimerkiksi saatavilla olevat resurssit tai organisaation läpinäkyvyys tietosuojaan liittyen? Miten näitä prosesseja kannattaa alkaa kehittämään organisaatiossa, jotta ne auttavat organisaatioita vastaamaan aiemmin mainittuihin haasteisiin.

Vaikka tekniset ja varsinkin organisatoriset apuvälineet olivat asiantuntijoiden organisaatioissa harvinaisia, mahdollistavat tulokset jatkotutkimuskohteita. Mitkä ovat ne syyt, miksei organisaatioissa käytetä viitekehyksiä, stan-

dardeja tai sertifiointeja tietosuojan hallinnassa? Ovatko ne riittämättömiä, hankalia ottaa tehokkaasti käyttöön vai onko kyse tässäkin resursseista? Minkälaisia muutoksia tarvittaisiin, jotta myös tietosuojan hallinnassa otettaisiin näitä organisatorisia apuvälineitä käyttöön? Tietoturvan puolella esimerkiksi sertifiointien käyttö vaikuttaa olevan paljon yleisempää. Mistä tämä johtuu? Teknisiin apuvälineisiin liittyen voitaisiin tehdä jatkotutkimusta siitä, tuoko juuri tietosuojan hallintaan kehitetyt apuvälineet merkittävää lisähyötyä tavallisiin Microsoft Officen työkaluihin verrattuna. Tämän tutkielman haastateltavien kokemusten mukaan tuo, mutta lisää tutkimusta aiheesta tarvittaisiin. Tarkempaa tutkimusta myös niistä ominaisuuksista, joita tietosuojan hallintaan liittyviltä apuvälineiltä odotetaan, voitaisiin tehdä. Teknisten apuvälineiden vaikutuksista tehokkuuteen ja organisaation kustannuksiin olisi mielekästä tehdä jatkotutkimusta, mutta se voi olla vaikea toteuttaa. Tietosuoja on vieläkin vähän tutkittu aihealue verrattuna siihen, miten merkittävä osa se on ihan jokaisen elämää. Jokainen tutkimus, joka tuo lisää ymmärrystä tietosuojasta ja tietosuojan hallinnasta on varmasti tervetullutta.

LÄHTEET

About EU Cloud CoC: EU Cloud CoC. (2022) Haettu 23.12.2022 osoitteesta https://eucoc.cloud/en/about/about-eu-cloud-coc

Alastalo, Åkerman ja Vaittinen (2017) Asiantuntijahaastattelu. Teoksessa Hyvärinen, M., Nikander, P., Ruusuvuori, J., Aho, A. L., & Granfelt, R. (2017). Tutkimushaastattelun käsikirja. Vastapaino.

Alhazmi, A., & Arachchilage, N. A. G. (2021). I'm all ears! Listening to software developers on putting GDPR principles into software development practice. Personal and Ubiquitous Computing, 25(5), 879–892. https://doi.org/10.1007/s00779-021-01544-1

Alunge, R. (2021). Breach of security vs personal data breach: Effect on EU data subject notification requirements. International data privacy law, 11(2), 163-181. https://doi.org/10.1093/idpl/ipaa021

Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Haettu 29.09.2022 osoitteesta https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

Ausloos, J., & Dewitte, P. (2018). Shattering one-way mirrors – data subject access rights in practice. International data privacy law, 8(1), 4-28. https://doi.org/10.1093/idpl/ipy00

BigID Inc. (2022, September 12). Privacy Management Suite. BigID. Haettu 09.07.2022 osoitteesta https://bigid.com/privacy-suite/

Bu-Pasha, S. (2022). Legal aspects, public interest, and legitimate interest in processing personal data to operate autonomous buses in the regular transportation system. Security and privacy, 5(5). https://doi.org/10.1002/spy2.247

Calzada, I. (2022). Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). Smart Cities, 5(3), 1129-1150. https://doi.org/10.3390/smartcities5030057

Carter, T., Kroll, J. A., & Bret Michael, J. (2021). Lessons Learned From Applying the NIST Privacy Framework. IT Professional, 23(4), 9–13. https://doi.org/10.1109/MITP.2021.3086916

Chiavetta, R. C. & IAPP. (2021, September). Privacy Tech Vendor Report 2021. https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf. IAPP. Haettu 13.09.2022 osoitteesta https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf

Clarke, N., Vale, G., Reeves, E. P., Kirwan, M., Smith, D., Farrell, M., Hurl, G., & McElvaney, N. G. (2019). GDPR: an impediment to research? *Irish Journal of Medical Science (1971 -)*, *188*(4), 1129–1135. https://doi.org/10.1007/s11845-019-01980-2

Commission Nationale pour la Protection des Données. (2021). GDPR-Certified assurance Report-Based processing activities certification criteria. https://cnpd.public.lu/content/dam/cnpd/fr/actualites/national/CNPD-GDPR-CARPA-Certification-Criteria-Consultation-publique.pdf.

Costello, R. Á. (2020). Schrems II: Everything is Illuminated? [Text/html,PDF]. European Papers - A Journal on Law and Integration, 2020 5(2) 1045-1059. 10451059. https://doi.org/10.15166/2499-8249/396

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

D'Annunzio, A., & Menichelli, E. (2022). A market for digital privacy: Consumers' willingness to trade personal data and money. Economia e politica industriale, 49(3), 571-598. https://doi.org/10.1007/s40812-022-00221-5

Data Protection Commissioner v. Facebook Ireland Ltd, M. S. C. o. F. R. o. t. E. U. & Regulation, A. 2. (2020). Facebook Ireland and Schrems: Decision of the European Court of Justice (Grand Chamber) 16 July 2020 – Case No. C-311/18 (ECLI:EU:C:2020:559). IIC - International Review of Intellectual Property and Competition Law, 51(7), 901-902. https://doi.org/10.1007/s40319-020-00967-2

Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems Charter of Fundamental Rights of the European Union (CFR), Arts. 7, 8, 47; Regulation (EU) 2016/679 (GDPR), Arts. 2(2), 45, 46, 58. (2020). "Facebook Ireland and Schrems": Decision of the European Court of Justice (Grand Chamber) 16 July 2020 – Case No. C-311/18 (ECLI:EU:C:2020:559). IIC - International Review of Intellectual Property and Competition Law, 51(7), 901–902. https://doi.org/10.1007/s40319-020-00967-2

DEFeND: the data governance framework for supporting GDPR. (n.d.). www.defendproject.eu. Haettu 20.09.2022 osoitteesta https://www.defendproject.eu/

Densmore, R. (2022). Privacy Program Management, Third Edition: Tools for Managing Privacy Within Your Organization (3rd ed.). International Association of Privacy Professionals.

Eggl, B. (2019). Learning to walk a tightrope: Challenges DPOs face in the day-to-day exercise of their responsibilities. Journal of Data Protection & Privacy, 3(1), 69-81. https://hstalks.com/article/5172/learning-to-walk-a-tightrope-challenges-dpos-face-/

Erickson, A. (2019). Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD. Brooklyn Journal of International Law, 44(2), 859. https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1941&context=bjil

European Commission. (2022). Questions & Answers: EU-U.S. Data Privacy Framework. Haettu 23.11.2022 osoitteesta https://ec.europa.eu/commission/presscorner/detail/fi/QANDA_22_6045

European Data Protection Board. (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. In https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

European Data Protection Board. (2019). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Haettu 04.01.2023 osoitteesta: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

Europrivacy. Euro Privacy. Haettu 19.11.2022 osoitteesta https://www.europrivacy.org/en/ep

Europrivacy: the first certification mechanism to ensure compliance with GDPR. (2022). Shaping Europe's Digital Future. Haettu 02.11.2022 osoitteesta: https://digital-strategy.ec.europa.eu/en/news/europrivacy-first-certification-mechanism-ensure-compliance-gdpr

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

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta

Evästeet ja muut käyttäjien päätelaitteille tallennettavat tiedot sekä näiden tietojen käyttö – Opas palveluntarjoajille. (2021). Haettu 14.12.2022. osoitteesta https://www.traficom.fi/sites/default/files/media/file/Ev%C3%A4steohjeistus_palveluntarjoajille.pdf

Faraj, S. & Sambamurthy, V. (2006). Leadership of information systems development projects. IEEE Transactions on Engineering Management, 53(2), 238–249.

Ferra, F., Wagner, I., Boiten, E., Hadlington, L., Psychoula, I., & Snape, R. (2020). Challenges in assessing privacy impact: Tales from the front lines. Security and Privacy, 3(2). https://doi.org/10.1002/spy2.101

Hellenic DPA: Fines imposed to telecommunications companies due to personal data breach and illegal data processing | European Data Protection Board. (03.02.2022). Haettu 21.09.2022 osoitteesta https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-imposed-telecommunications-companies-due-personal-data_en

Henkilötietojen käsittelijän velvollisuudet. Tietosuojavaltuutetun Toimisto. Haettu 23.12.2022 osoitteesta osoitteesta https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet

Henkilötietojen käsittelijät. Tietosuojavaltuutetun Toimisto. Haettu 23.12.2022 osoitteesta https://tietosuoja.fi/henkilotietojen-kasittelijat

Henkilötietojen käsittely. Tietosuojavaltuutetun Toimisto. Haettu 23.12.2022 osoitteesta https://tietosuoja.fi/henkilotietojen-kasittely

Henkilötietojen käsittelyperusteet. Tietosuojavaltuutetun Toimisto. Haettu 14.12.2022 osoitteesta https://tietosuoja.fi/kasittelyperusteet

Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle. (2022). Tietosuojavaltuutetun Toimisto. https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle

Howard, R. J. (2022). First GDPR Certification Scheme Adopted by Luxembourg. Cybersecurity Policy Report, 1–1.

Huertas Celdrán, A., Gil Pérez, M., Mlakar, I., Alcaraz Calero, J. M., García Clemente, F. J., Martínez Pérez, G., & Bhuiyan, Z. A. (2020, November). PROTECTOR: Towards the protection of sensitive data in Europe and the US. Computer Networks, 181, 107448. https://doi.org/10.1016/j.comnet.2020.107448

Hyvärinen, M. (2017) Haastattelun maailma. Teoksessa Hyvärinen, M., Nikander, P., Ruusuvuori, J., Aho, A. L., & Granfelt, R. (2017). Tutkimushaastattelun käsikirja. Vastapaino.

International Organization for Standardization. (2019, August). ISO/IEC 27701:2019(en) Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Haettu 19.10.2022 osoitteesta https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

IT Governance Privacy Team. (2020). EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition: Vol. Fourth edition. ITGP.

Jordan, S. (2022). A Proposal for Notice and Choice Requirements of a New Consumer Privacy Law. Federal communications law journal, 74(3), 251-328. https://ssrn.com/abstract=3956101

Kaya, M. (2021). Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law. Annales de la Faculté de droit d'Istanbul, 70, 195-241. https://doi.org/10.26650/annales.2021.70.0007

Kotivu. (2022). Complyon. Haettu 20.09.2022 osoitteesta https://complyon.com

Lachaud, E. (2014). Should the DPO be certified. International data privacy law, 4(3), 189-202. https://doi.org/10.1093/idpl/ipu008

Laine, T. (2018). Valli, R., Aaltola, J., & Herkama, S. (2018). Ikkunoita tutkimusmetodeihin: 2, Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin (5., uudistettu ja täydennetty painos.). PS-Kustannus. 22-43.

Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International Journal of Law and Information Technology*, *26*(1), 45–63. https://doi.org/10.1093/ijlit/eax024

Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta, allekirjoitettu Lissabonissa 13 päivänä joulukuuta 2007 (2007/C 306/01)

Maximillian Schrems v Data Protection Commissioner, Ireland, C-362/14 (CJEU, 6 October 2015) ECLI:EU:C:2015:650.

Mighty Trust | Pricing Plan. Haettu 20.09.2022 osoitteesta https://www.themightytrust.com/pricing-plan.php

Monfared, Y. A., Benslimane, Y. & Yang, Z. (2018). Information Privacy Practices in Organizations: Activities, Knowledge and Skill Requirements for Information Technology Professionals. IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). 1001-1005. Haettu osoitteesta https://dx.doi.org/10.1109/IEEM.2018.8607336.

National Institute of Standards and Technology. (2020, January). The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. Haettu 04.10.2022 osoitteesta https://ec.europa.eu/newsroom/article29/items/611236/en

National Institute of Standards and Technology. (2020b, September). Security and Privacy Controls for Information Systems and Organizations. Haettu 12.10.2022 osoitteesta https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

National Institute of Standards and Technology. (2018, April 16). Framework for Improving Critical Infrastructure cybersecurity. Haettu 05.10.2022 osoitteesta https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. Evidence-based nursing, 18(2), 34-35. https://doi.org/10.1136/eb-2015-102054

Note GDPR certification – ePrivacy Haettu 26.10.2022 osoitteesta https://www.eprivacy.eu/en/privacy-seals/eprivacyseal-2022/note-gdpr-certification/

Nymity inc. (2018). Framework for Demonstrable GDPR Compliance. Haettu 05.10.2022 osoitteesta https://iapp.org/media/pdf/resource_center/Nymit-Accountability-Roadmap-GDPR-Compliance.pdf

Padden, M., & Öjehag-Pettersson, A. (2021). Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR). Critical policy studies, 15(4), 486-503. https://doi.org/10.1080/19460171.2021.1927776

Pantelic, O., Jovic, K., & Krstovic, S. (2022). Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations. Sustainability (Basel, Switzerland), 14(9), 5015. https://doi.org/10.3390/su14095015

Pantos. (2021). How the World's Largest Economies Regulate Data Privacy: Drawbacks, Benefits, & Proposed Solutions. Indiana Journal of Global Legal Studies, 28(2), 267. https://doi.org/10.2979/indjglolegstu.28.2.0267

Pricing. DPOrganizer Haettu 20.09.2022 osoitteesta https://www.dporganizer.com/pricing/

Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J. B., Fiorani, M., Magkos, E., Sanz, A. C., Pavlidis, M., D'Addario, R., & Zorzino, G. G. (2019). DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance. Teoksessa S. Gritzalis, E. R. Weippl, S. K. Katsikas, G. Anderst-Kotsis, A. M. Tjoa, & I. Khalil (Toim.), Trust, Privacy and Security in Digital Business (Vsk. 11711, ss. 78–93). Springer International Publishing. https://doi.org/10.1007/978-3-030-27813-7_6

Rekisterinpitäjän seloste käsittelytoimista. Tietosuojavaltuutetun Toimisto. Haettu 23.12.2022 osoitteesta https://tietosuoja.fi/rekisterinpitajan-seloste-kasittelytoimista

Rodrigues, R., Barnard-Wills, D., De Hert, P., & Papakonstantinou, V. (2016). The future of privacy certification in Europe: An exploration of options under article 42 of the GDPR. International Review of Law, Computers & Technology, 30(3), 248–270. https://doi.org/10.1080/13600869.2016.1189737

Rotenberg, M. (2020). Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection. European law journal : review

of European law in context, 26(1-2), 141-152. https://doi.org/10.1111/eulj.12370

Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation. The International spectator, 53(4), 95-111. https://doi.org/10.1080/03932729.2018.1532705

Rubinstein, I. S., & Good, N. (2020). The trouble with Article 25 (and how to fix it): the future of data protection by design and default. International Data Privacy Law, 10(1), 37–56. https://doi.org/10.1093/idpl/ipz019

Ruusuvuori, J., Nikander, P., & Hyvärinen, M. (2010). Haastattelun analyysi. Vastapaino.

Serrado, J., Pereira, R. F., Mira da Silva, M., & Scalabrin Bianchi, I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. Digital Policy, Regulation and Governance, 22(3), 227–244. https://doi.org/10.1108/DPRG-02-2020-0019

Simnett, R. (2012). Assurance of sustainability reports: Revision of ISAE 3000 and associated research opportunities. Sustainability Accounting, Management and Policy Journal, 3(1), 89–98. https://doi.org/10.1108/20408021211223570

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu 10.03.2023 osoitteesta https://www.fsd.tuni.fi/menetelmaopetus

Suomen virallinen tilasto (SVT). (2021) Tietotekniikan käyttö yrityksissä ISSN=1797-2957. 2021, 3. Pilvipalvelut . Helsinki: Tilastokeskus. Haettu 16.11.2022 osoitteesta http://www.stat.fi/til/icte/2021/icte_2021_2021-12-03_kat_003_fi.html

The European Data Protection Board. (2022). Opinion 28/2022 on the Europrivacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR). https://edpb.europa.eu/system/files/2022-10/edpb_opinion_202228_approval_of_europrivacy_certification_criteria_as_eu_data_protection_seal_en.pdf.

The first EU-wide GDPR certification scheme – Europrivacy (TM/®) explained in 5 questions | Timelex. (2022). Haettu 08.11.2022 osoitteesta https://www.timelex.eu/en/europrivacy

Tietosuojaperiaatteet. (n.d.). Tietosuojavaltuutetun Toimisto. Haettu 11.12.2022 osoitteesta https://tietosuoja.fi/tietosuojaperiaatteet

Tietosuojaryhmä. (2017). Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta. Haettu 13.01.2023 osoitteesta https://tietosuoja.fi/documents/6927448/8316711/Tietoturvaloukkaukse

n+ilmoittaminen+fi/9c0f2f46-33b1-4b01-9a50-9320d59bd605/Tietoturvaloukkauksen+ilmoittaminen+fi.pdf?t=1535696174000

Tietosuojatyökalu – Tietosuoja. Haettu 07.09.2022 osoitteesta https://www.tietosuojaapkyrityksille.fi/tyokalun_etusivu/

Tietoturvaloukkaukset. Tietosuojavaltuutetun Toimisto. Haettu 13.01.2023 osoitteesta https://tietosuoja.fi/tietoturvaloukkaukset

Tsohou, A., Magkos, E., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., Debussche, J., Rotoloni, M., & Gallego-Nicasio Crespo, B. (2020). Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. Information & Computer Security, 28(4), 531–553. https://doi.org/10.1108/ICS-01-2020-0002

Ustaran, E. (2018). European Data Protection Law and Practice. International Association of Privacy Professionals.

United Nations. (n.d.). Universal Declaration of Human Rights. Haettu 19.10.2022 osoitteesta https://www.un.org/en/about-us/universal-declaration-of-human-rights

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. International data privacy law, 8(2), 105-123. https://doi.org/10.1093/idpl/ipy002

Waldman, A. E. (2020). Data protection by design?: A critique of Article 25 of the GDPR. Cornell international law journal, 53(1), 147-167.

63/1999 - Valtiosopimukset - FINLEX ®. Haettu 19.10.2022 osoitteesta https://www.finlex.fi/fi/sopimukset/sopsteksti/1999/19990063

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. International data privacy law, 8(2), 105-123. https://doi.org/10.1093/idpl/ipy002