Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

PÄIVI WALLIN

EU:n yleisen tietosuoja-asetuksen osoitusvelvollisuus

Tietosuojaperiaatteiden toteuttaminen kohdeyrityksessä

LIIKETALOUDEN KOULUTUSOHJELMA
2020

Tekijä
Wallin, Päivi

Julkaisun laji
Opinnäytetyö, AMK

Päivämäärä
Kesäkuu 2020

Sivumäärä
43

Julkaisun kieli
Suomi

Julkaisun nimi
EU:n yleisen tietosuoja-asetuksen osoitusvelvollisuus: Tietosuojaperiaatteiden toteuttaminen kohdeyrityksessä

Tutkinto-ohjelma
Liiketalous

Opinnäytetyön tarkoituksena oli tutkia ja kehittää EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisten tietosuojaperiaatteiden toteuttamista kohdeyrityksessä. Asetuksen keskeinen periaate, osoitusvelvollisuus, edellyttää rekisterinpitäjän ei vain noudattavan henkilötiedon käsittelyä koskevia normeja, vaan myös noudattamisen toteennäyttämistä. Tavoitteena oli luoda osoitusvelvollisuutta tukeva dokumentointi ja käytänteet. Osoitusvelvollisuuden toteuttamisessa noudatettiin riskiperusteista näkökulmaa, jossa rekisterinpitäjän toteuttamat toimenpiteet rekisteröidyn oikeuksien suojaamiseksi ovat oikeassa suhteessa henkilötiedon käsittelyn rekisteröidylle aiheutuvaan riskiin nähden. Osoitusvelvollisuuden voidaan nähdä toteutuvan kolmella eri tasolla: yleisissä toimintaperiaatteissa ja politiikoissa, käytännön tietosuojan toteutuksessa ja sen dokumentoinnissa sekä todentamisessa mm. auditointien ja mittareiden avulla.

Opinnäytetyö kuului yritysjuridiikan alaan, ja sen menetelmällinen lähtökohta oli laintulkinta. Tutkimuksen keskeinen lähdeaineisto muodostui tietosuoja-asetuksesta sekä oikeusoppineiden ja tietosuojaviranomaisten laintulkinnoista ja ohjeistuksista. Opinnäytetyö oli toiminnallinen tutkimus, jossa pyrittiin ongelman kuvaamisen lisäksi ratkaisemaan se käytännössä. Toiminnallisessa tutkimuksessa tutkija ei ole kehitettävään kohteeseen nähden ulkopuolinen, vaan osallistuu aktiivisesti organisaation käytänteiden kehittämiseen. Nykytila-analyysia varten hankittiin taustatietoa laadullisin menetelmin kyselylomakkeen ja teemahaastattelun avulla tarkoituksena selvittää henkilökunnan osaaminen ja kohdistaa toimintaan oikeita kehitystoimenpiteitä. Kehitystyötä varten perustettiin ryhmä, jossa oli edustajat keskeisistä toiminnoista.

Tutkimuksen tuloksena kohdeyrityksen dokumentointi ja käytänteet luotiin osoitusvelvollisuuden toteuttamiseksi. Tietotilinpäätöksessä määriteltiin tietosuojan kannalta olennaiset asiat. Siinä kuvattiin mm. yrityksen nykyinen tietoturvan toteuttaminen tietoteknisissä järjestelmissä, tietovarannot, tietosuojaorganisaatio sekä henkilötietojen käsittelykäytännöt. Tietosuoja-asetuksen keskeiset tietosuojaperiaatteet tuotiin käytäntöön laatimalla henkilötiedon lainmukaisen käsittelyn ohjeistus sekä koulutusmateriaali. Tietosuojaorganisaation vastuiden sekä tietosuojan seurantamenetelmien määrittäminen ovat seuraavia askeleita yrityksen tietosuojakulttuurin vakiinnuttamiseksi osaksi yrityksen käytäntöjä.

Asiasanat
EU:n yleinen tietosuoja-asetus, GDPR, henkilötieto, osoitusvelvollisuus, tietosuojaperiaatteet, rekisterinpitäjä

Author
Wallin, Päivi

Type of Publication
Bachelor's thesis

Date
June 2020

Number of pages
43

Language of publication:
Finnish

Title of publication
Accountability in the general data protection regulation – Implementing data protection principles in the target organization

Degree program
Business and administration

The purpose of the thesis was to study and develop company's compliance regarding the data protection principles of EU's general data protection regulation (GDPR). The accountability as a key principle of the regulation means not only compliance with the personal data processing norms but also demonstration of the compliance. The target was to create documentation and practices to support accountability. In order to accomplish accountability, risk based approach was applied. The measures to protect data subject's rights must be balanced with the risk caused to the data subject. The accountability realizes in three level: in general principles and policies, in data protection implementation and documentation and in verification e.g. through auditing and measuring.

The thesis was in the field of business law and it's methodological starting point was legal dogmatics. A central source material consisted of the data protection law and interpretation and guidelines created by the data protection officials and legal scholars. The type of the thesis was action research the purpose of which was not only to describe but also to solve the practical problem. The researcher was not external observer but she participated actively in the development of the organization's practices. The current state was analyzed through questionnaire formula and thematic interview in order to get background information on personnel's knowledge and to allocate development measures. The development team was created with participants of all key functions.

As a result of this action based research the documentation and practices were created to accomplish accountability. In the data balance sheet central issues concerning data protection were defined. The current status of data protection in technological systems, data resources, data protection organization and practices were described. The data protection principles were implemented in lawful processing guidelines of personal data. Training material was also created. Next steps in establishing data protection culture in the organization is to define data protection organization's responsibilities and follow up methods.

Key words
General data protection regulation, GDPR, personal data,, accountability, data protection principles, data processor

SISÄLLYS

1 JOHDANTO

Euroopan Unionin yleinen tietosuoja-asetus (GDPR, General Data Protection Regulation) astui voimaan 24.5.2016 ja sen soveltaminen alkoi 25.5.2018. Informaatioteknologian, globalisaation ja digitalouden kehittyminen ovat ulottaneet vaikutuksensa laajasti koko yhteiskuntaan. Siksi koko EU:n alueella on katsottu tarpeelliseksi entisestään vahvistaa tietosuojaa ja –turvaa sekä harmonisoida lainsäädäntöä. Asetuksen tavoitteena on suojata luonnollisen henkilön perusoikeutta henkilötietojensa suojaan ja samalla turvata toimivat sisämarkkinat ja talousunionin kehittäminen. (EU:n yleinen tietosuoja-asetus, 27.4.2016, 2016/679/EU, EUVL L 119, 4.5.2016.)

Tietosuoja nousi laajan huomion kohteeksi viimeistään keväällä 2018, jolloin EU:n yleinen tietosuoja-asetus oli astumassa voimaan kahden vuoden siirtymäajan jälkeen. Näinä kahtena vuotena yritykset hioivat käytäntöjään kuntoon ja uudistivat prosessinsa vastaamaan uusia vaatimuksia. Viimeistään vuonna 2018 verkkosivustot ja lehdet alkoivat täyttyä aihetta koskevasta kirjoittelusta otsikolla ”Oletko valmis GDPR:ään?” Nämä kirjoittelut suunnattiin erityisesti niille organisaatioille, jotka eivät olleet aiemmin tiedostaneet lainsäädännön koskevan jokaista rekisterinpitäjää, myös yksityisyrittäjiä, järjestöjä ja yhdistyksiä.

Tietosuoja-asetusta edeltänyt henkilötietodirektiivi (95/46/EY) ja kansalliset lainsäädännöt eivät antaneet edellytyksiä yhtenäiselle soveltamiskäytännölle tietosuoja-asioissa Euroopan Unionissa (Yleinen tietosuoja-asetus 679/2016, resitaali 9). Uudistetun lainsäädännön keskeisenä periaatteena oleva osoitusvelvollisuus asettaa käytännössä jokaisen yrityksen ja yhteisön uusien haasteiden eteen. Yritykset ovat velvollisia osoittamaan, miten tietosuoja-asetuksen periaatteet konkreettisesti toteutetaan sen eri prosesseissa ja järjestelmissä. Noudattamatta jättämisestä on asetuksessa säädetty tuntuvia hallinnollisia sakkoja. Kansalaisten lisääntynyt tietoisuus tietosuojasta ja omista oikeuksista pakottaa niin ikään yritykset huolehtimaan tietosuojastaan entistä paremmin.

Tämän työn tarkoituksena on tutkia kohdeyrityksen tietosuojan nykytila ja parantaa sen käytäntöjä dokumentoinnin, käytänteiden luomisen ja koulutuksen avulla ja siten tuoda tietosuojaperiaatteet osaksi prosesseja osoitusvelvollisuuden täyttämiseksi riskiperusteisesta lähtökohdasta käsin. Tietosuojaperiaatteet eivät ole yksiselitteisiä ja siksi oikeustieteellisessä kentässä huomio on

keskittynyt voimakkaasti juuri niiden tulkintaan. Periaatteiden muuttaminen käytännön toiminnaksi ei siis ole itsestään selvää, ja jokaisen rekisterinpitäjän on suhteutettava henkilötiedon suojan toteuttaminen omiin tarpeisiin ottaen huomioon luonnollisen henkilön oikeuksille aiheutuva riski.

Työssä käsitellään tietosuoja-asetuksen vaatimuksia rekisterinpitäjän näkökulmasta. Rekisteröidyn oikeudet eivät suoranaisesti ole työssä tarkemman tarkastelun keskiössä, vaikka niiden toteutuminen onkin tietosuoja-asetuksen ydin. Pikemminkin keskitytään siihen, miten rekisterinpitäjä voi organisatorisin keinoin luoda edellytykset tietosuojan toteutumiselle. Tietosuoja edellyttää tietojärjestelmien suojaamista lukuisilla teknisillä toimenpiteillä. Tietojärjestelmät tulee lähtökohtaisesti suunnitella siten, että ne täyttävät kaikki tietosuoja-asetuksen vaatimukset rekisteröidyn oikeuksien toteuttamiseksi. Tässä työssä ei keskitytä tietoturvaan liittyviin kysymyksiin.

Kohdeyritys kuuluu kansainväliseen rakennustuotteita valmistavaan ja markkinoivaan konserniin. Konserni- ja maatasolla tietosuoja on hoidettu asianmukaisesti, mutta tutkimuksen kohteena olevassa yrityksessä käytännön tietoisuus ja osaaminen vaativat kehittämistä. Tutkija, joka toimii itse organisaatiossa, esitti opinnäytetyön aihetta juuri tämän puutteellisuuden korjaamiseksi. Koska kyseessä on B-to-B yritys, on oletettavaa, että henkilötietojen riskitaso ei ole korkea. Silti yrityksen on pystyttävä osoittamaan, että tarpeellinen riskikartoitus on tehty ja henkilötiedon käsittely täyttää lainsäädännön vaatimukset.

Opinnäytetyö kuuluu juridiikan alaan. Menetelmä sijoittuu oikeustieteellisessä kentässä oikeusdogmatiikan alaan, joka tutkii olemassa olevaa oikeutta laintulkinnan kautta. Työn teoreettinen viitekehys syntyy henkilötietoon ja tietosuojaan liittyvästä laista ja sen käsitteistöstä. Tietosuojaperiaatteet ovat tutkimuksen keskiössä muodostaen perustan käytännön kehitystyölle. Tutkimuksen voidaan katsoa kuuluvan oikeustieteen kentässä informaatio-oikeuden alaan, jossa tutkitaan henkilötiedon omistukseen ja hallintaan liittyvää problematiikkaa niin yksilön kuin yrityksen näkökulmasta (Voutilainen 2019, 21).

Koska tämän opinnäytetyön tavoitteena on luoda uusia välineitä ja parannuksia käytäntöihin sekä toteuttaa ne, valittiin menetelmälliseksi perustaksi toiminnallinen tutkimus. Siinä tutkimuksen tekijä toimii sekä tutkijana että jäsenenä kehitysprojektissa. Tuloksena syntyy raportin lisäksi valmiita tuotoksia, joilla parannetaan käytäntöjä. Tietosuojaan liittyvä lainsäädäntö on peruste

käytäntöjen parantamiselle. Tavoitteena on lainsäädännön tavoitteiden jalkauttaminen organisaatioon luomalla henkilötietojen nykytilan kartoitus sekä ohjeistus henkilötietojen käsittelylle. Kehitysprosessin aikana parannetaan prosesseja sekä varmistetaan yrityksen vaatimuksenmukaisuus laatimalla selkeät toimintaohjeet samalla varmistaen hyvien käytänteiden jatkuvuus yrityksessä. Tietosuojanormeja tutkitaan suhteessa käytäntöön eli miten yrityksessä tietosuoja tulee toteuttaa, jotta lain vaatimukset tulevat täytetyksi. Aluksi on konkretisoitava tietosuoja-asetuksen keskeiset periaatteet ja niiden tavoitteet. Lähdeaineisto koostuu tietosuoja-asetuksesta sekä sitä systematisoivasta ja tulkitsevasta aineistosta.

Aluksi työssä esitellään työn tavoite, konteksti ja tutkimusote. Keskeisenä lähtökohtana on kohdeyrityksen liiketoiminta B-to-B yrityksenä sekä sen toimintaympäristö, joiden perusteella asetuksen vaatimuksia tulkitaan riskiperusteisesti. Teoreettisessa osuudessa selvitetään EU:n tietosuoja-asetuksen tietosuojaperiaatteisiin liittyvää problematiikkaa. Keskeisinä käsitteinä ovat osoitusvelvollisuus sekä tietosuojaperiaatteet, jotka muodostavat empiirisen osuuden perustan. Työn raportointiosuudessa selvitetään kohdeyrityksen tietosuojan nykytila. Nykytilaa tarkastellaan tietosuojaperiaatteiden toteutumisen kannalta samalla sitoen teoreettinen osuus empiriaan. Tulosten raportoinnissa esitellään keinot osoitusvelvollisuuden toteuttamiseksi sekä tutkimuksen aikana jo toteutetut toimenpiteet. Tutkimustyön varsinainen tuotos koostuu erilaisista dokumenteista, joista tärkein on tietotilinpäätös.

2 TYÖN TAVOITE JA VIITEKEHYS

2.1 Tavoite, tutkimuskysymys ja konteksti

Tämän opinnäytetyön lähtökohtana on oikeudellisen kysymyksen tutkiminen käytännön tilanteessa. Tarkoituksena on tulkita voimassaolevaa oikeutta sekä kuvata, miten lain mukaan tulisi toimia. Tavoitteena on analysoida kohdeyrityksen tietosuojan nykytila, parantaa henkilötiedon käsittelyn käytäntöjä ja siten varmistaa henkilötiedon lainmukainen käsittely ja EU:n yleisessä tietosuoja-asetuksessa määritetty osoitusvelvollisuuden täyttyminen. Tietosuoja-asetuksen tietosuojaperiaatteet toimivat tutkimuksen teoreettisena viitekehyksenä. Tietosuojaperiaatteet ovat henkilötiedon käsittelyn lainmukaisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen ja

säilytysajan minimointi, täsmällisyys, eheys sekä luottamuksellisuus. Osoitusvelvollisuus merkitsee näiden periaatteiden noudattamista ja todentamista.

Tutkimustehtävänä on toiminnallisen tutkimuksen menetelmin

- kuvata kohdeyrityksen tietosuojan nykytila sekä
- selvittää miten tietosuoja-asetuksen osoitusvelvollisuus ja tietosuojan keskeiset periaatteet voidaan toteuttaa kohdeyrityksessä.

Tiedollisena motiivina tutkimukselle on tekijän halu selvittää, mitä osoitusvelvollisuus ja riskiperusteisuus tarkoittavat B-to-B yrityksessä yleensä ja miten tietosuojaperiaatteet voidaan toteuttaa käytännön tasolla välttäen mahdolliset valvontaviranomaisen langettamat sanktiot. Käytännön motiivina on ratkaista tietosuoja-asetuksen vaatimuksenmukaisuudessa olevat puutteet. Tekijä toimii itse yrityksessä ja omaa siten jo kokemusta ja tietoa yrityksen nykyisistä käytännöistä.

EU:n yleinen tietosuoja-asetus asettaa konkreettisia teknisiä vaatimuksia yrityksille, sillä rekisteröidyn tiedonsaantioikeudet edellyttävät järjestelmiltä uusia ominaisuuksia. Siksi monissa yrityksissä tietosuojakysymykset ovatkin IT-osaston vastuulla. Vaikka teknologia liittyy kiinteästi henkilötiedon suojaan, yhtä olennaisia ovat tietoja käsittelevät henkilöt ja käsittelyprosessit. Jos jossakin tiedonkäsittelyn elementissä on puutteita, tietosuoja ei voi toteutua. Siksi liiketoimintaprosessit, organisaatiokulttuuri ja teknologia on rakennettava saumattomaksi kokonaisuudeksi. Toisaalta kyse ei ole enää pelkästään lain vaatimusten täyttämisestä, vaan uudesta ajattelutavasta ja kyvystä ymmärtää yksityisyys, mikä puolestaan heijastuu organisaation käytäntöihin ja organisaatiokulttuuriin (Grundström, Väyrynen, Iivari & Isomursu 2019, 5044).

Tietosuojaa, henkilötietojen käsittelyä ja yksityisyyden suojaa on tutkittu erityisesti informaatio-oikeuden alalla. Informaatio-oikeuden tutkimuskohteena ovat informaatio ja tieto sekä niiden käsittelyn ja hallinnan oikeudellinen säätely (Voutilainen 2019, 15). Tietosuoja-asetusta, kuten mitä tahansa muutakin lainsäädäntöä, on tulkittava, sillä normit eivät anna käytännön toiminta-ohjeita. Tietosuojalainsäädäntöä edeltävä henkilötietodirektiivi sisälsi saman sisältöisiä periaatteita, mutta niiden noudattamista ei valvottu eikä seuraamuksista ollut säädetty yhdenmukaisesti jäsenvaltioissa (Yleinen tietosuoja-asetus 679/2016, resitaali 9-13.) Uuden asetuksen myötä yritykskenttää kohtasi paineet saada käytännön ohjeita vaatimuksenmukaisuuden toteuttamiseksi. Viime kädessä tulkintaa tekee EU-tuomioistuin. Virallisena instanssina asetuksen tulkintoja ja

lausuntoja antavana on toiminut EU:n tietosuojaryhmä, joka ennen toukokuuta 2018 toimi nimellä Working Party 29. Sittemmin toimintaa on jatkanut EU:n tietosuojavaltuutettu ja tietosuojaneuvosto (EDPB), joka toimii myös kansallisten valvontaviranomaisten ohjeistajana ja laintulkitsijana. Sen tehtävä on myös varmistaa jäsenvaltioiden yhdenmukainen asetuksen soveltaminen. (Tietosuojavaltuutetun toimiston www-sivut 2020; Euroopan tietosuojaneuvoston www-sivut 2020.)

Tietosuoja on ollut erityisesti vuoden 2017 jälkeen useiden AMK-opinnäytetöiden aiheena. Niitä on valmistunut Satakunnan ammattikorkeakoulussakin parikymmentä kappaletta. Varsinkin vuonna 2018, jolloin siirtymäaika loppui ja yritysten tuli täyttää asetuksen vaatimukset, opinnäytetöitä syntyi yritysten todelliseen tarpeeseen selvittää nykytilaa ja kartoittaa mahdollisia ongelmia. Useissa töissä tehdään tutkimusta siitä, mitä vaikutuksia uudella lainsäädännöllä on yrityksen toimintaan. Vertailukohtana on usein henkilötietolaki, jonka päivittäminen tapahtui uuden asetuksen myötä. (SAMK Finnan www-sivut 2020.) Osoitusvelvollisuutta, joka on tämän tutkimuksen keskeinen teema, on kattavasti tutkittu mm. Vainion pro gradu-tutkielmassa. Siitä käsitellään osoitusvelvollisuusperiaatteen käsitteellistä syntyhistoriaa ja sen käytännön toteutuksen haasteellisuutta rekisterinpitäjille. (Vainio 2018.) Lukuisissa oikeustieteellisissä artikkeleissa on kirjoitettu tietosuojaperiaatteiden tulkintaan liittyvistä kysymyksistä. Google Scholar löytää asiasanalla ”GDPR” vuosina 2018-2020 n. 21.000 julkaistua artikkelia ja sitaattia. Kahden vuoden voimassaolon jälkeen on alkanut muodostua myös oikeuskäytäntöä tuomioiden ja ennakkoratkaisujen muodossa (Euroopan Unionin tuomioistuimen www-sivut 2020).

Kohdeyritys kuuluu kansainväliseen monialakonserniin. Yritys on Suomessa toimiva maahantuoja ja myyntiorganisaatio, jonka asiakkaina ja muina sidosryhminä ovat mm. kaupungit, urakoitsija, tukkuliikkeet ja suunnittelijat. Osa toiminnoista kuten HR, palkkahallinto, taloushallinto ja IT ovat yhteisen palvelukeskuksen hoidossa. Kohdeyritys toimii itsenäisenä liiketoimintayksikkönä ja hoitaa operatiiviset toiminnot (myynti, osto, tuotanto, varastointi) itsenäisesti. Työntekijäitä yrityksessä on 24, heistä toimihenkilöitä on 17 ja 7 työntekijöitä. Tietosuojahallinto on organisoitu konsernin ja Suomen tasolla. Kohdeyrityksessä tietosuojan jalkauttaminen käytäntöihin on kuitenkin jäänyt kesken. Yhtenä syynä on oletettavasti se, että yrityksen sidosryhmät ovat ammattilaisia ja sen liiketoiminta perustuu kaupankäyntiin toisten yritysten kanssa. Yrityksessä ei ole myynnin- ja markkinoinnin yhtenäistä asiakas- tai markkinointirekisteriä, sillä aiemman toiminnanohjausjärjestelmään linkittynyt kontaktirekisteri on uuden järjestelmän myötä

poistunut. Henkilötietojen käsittely on siten suhteellisen suppeaa. Yritys on mukana emoyhtiövetoisessa asiakkuudenhallintajärjestelmän kehitysprojektissa ja voidaan odottaa, että järjestelmä otetaan käyttöön lähiaikoina.

Yritysten prosessit joutuvat uudelleenarvioinnin kohteeksi EU:n tietosuoja-asetuksen myötä. Prosesseja on kehitettävä, jotta asetuksen vaatimukset tulevat täytetyiksi. Kohdeyrityksessä tietosuoja-asetuksen organisaation prosesseihin kohdistamien vaatimusten motivoivana tekijänä ei ole liiketoiminnan tehostaminen sinänsä, vaan lain vaatimuksiin vastaaminen. Prosessien ja järjestelmien mukauttaminen uusiin vaatimuksiin on välttämätöntä, jotta vaatimuksenmukaisuuden puutteet eivät muodostuisi liiketoimintaa haittaavaksi tekijäksi ja mahdollisesti hallinnollisiin sakkoihin johtavaksi.

Eri toimialoilla henkilötietojen sensitiivisyys vaihtelee suuresti. Esimerkiksi sosiaali- ja terveysalalla, jossa voidaan käsitellä laajasti henkilöiden arkaluonteisia tietoja, henkilötietojen lainmukainen käsittely ja yksityisyyden suoja korostuvat. Kuluttajakaupassa yritykset keräävät asiakkaiden tietoja mm. ostokäyttäytymisestä, joka on hyvin arvokasta tietoa markkinoijille. Kohdeyrityksen käsittelemät henkilötiedot eivät riskitasoltaan ole korkeita, sillä liiketoiminnassa kerätään vain niitä tietoja, jotka ovat välttämättömiä asiakassuhteen ylläpitämiseksi ja yritysasiakkaiden lähestymiseen markkinointitarkoituksessa. Työntekijöiden henkilötietoja käsitellään jonkin verran, vaikka HR ja palkkahallinto on ulkoistettu palvelukeskukseen. Oletuksena on, että henkilötietojen käsittelyn vähäisestä riskistä johtuen B-to-B -yrityksessä ei henkilötiedon käsittelyssä ilmeen suuria ongelmia. Ongelma onkin dokumentoinnin ja käytänteiden puuttuminen.

2.2 Teoreettinen ja menetelmällinen viitekehys

Ammattikorkeakoulun opinnäytetyön tarkoituksena on osoittaa opiskelijan oman alansa oppineisuus ja samalla hyödyttää jollakin tavalla työelämää. Teoreettinen tutkimus pitäytyy tiedollisessa tutkimusongelman ratkaisussa mahdollisesti uutta teoreettista tietoa lisäten. Käytännön työelämään suuntautuva tutkimus pyrkii soveltamaan teoreettista tietoa käytäntöön ja saamaan erilaisten tiedonkeruumenetelmien avulla tietoa tutkittavasta kohteesta. Teoreettinen viitekehys ja käsitteet antavat tutkimukselle näkökulman, josta käsin ja joiden läpi tutkittavaa kohdetta ja tutkimusaineistoa tarkastellaan johdonmukaisesti. Niiden avulla voidaan myös rakentaa tutkimusongelmia ja empiirisiä tutkimuskysymyksiä sekä kuvata tutkittavaa kohdetta. (Vilkka 2015.)

Oikeustieteessä perinteinen lähestymistapa tutkittavaan kohteeseen on lainoppi eli oikeusdogmatiikka, jossa tiedonintressinä on kuvata voimassaolevan oikeuden sisältöä oikeudellisten normien ja niiden ajatussisältöjen tulkinnan ja systematisoinnin kautta (Kolehmainen 2016, 107). Lainopin tärkeä tehtävä on jäsentää eri oikeudenalojen käsitteitä ja oikeusperiaatteita. Tulkinta merkitsee merkityssisällön antamista eikä vain sen toteamista. (Hirvonen 2011, 25, 37.) Tämän tutkimuksen lähtökohta on EU:n yleisen tietosuoja-asetuksen normien tulkinta ja niiden muuttaminen käytännön toimintaohjeiksi. Koska kyse on ammattikorkeakoulun opinnäytteestä eikä oikeustieteellisestä tutkimuksesta, työssä kerätään oikeusoppineiden ja viranomaisten tulkintaohjeita ja sovelletaan niitä omaan tutkimustehtävään.

Tutkimustulokseen pääsemiseksi tutkija tarvitsee jonkin metodin, jolla hän saa vastaukset tutkimuskysymyksiinsä. Metodin avulla tutkija määrittää miten tutkimuskohteesta saadaan tietoa, miten saatua tietoa analysoidaan ja millaisiin johtopäätöksiin tietojen perusteella voidaan päätyä (Hirvonen 2011, 9). Tämän tutkimuksen keskeinen lähtökohta on käsite, jonka merkityssisältöä pyritään selkeyttämään. Käsitteiden abstraktiotaso vaihtelee suuresti. Abstraktiotasoltaan korkeat teoreettiset käsitteet voivat sisältää monimutkaisia oletuksia todellisuuden luonteesta ja niiden sisällöstä käydään usein jatkuvaa debattia. Konkreettiset käsitteet liittyvät kiinteästi johonkin ajallisesti tai paikallisesti olemassa olevaan ilmiöön ja niiden ymmärtäminen tuntematta teoreettista lähtökohtaa on helpompaa. (Hirsjärvi, Remes & Sajavaara 2007, 143-146.)

Lainopillisessa tutkimuksessa käsitteet voivat olla joko normatiivisia tai systemaattisia. Normatiivinen käsite on oikeuslähteessä käytetty käsite kuten lakitermi, kun taas systemaattinen käsite on oikeustieteen luoma ja käyttämä käsite. (Voutilainen 2019, 40.) Käsitteiden määrittelyn tarkoitus on rajata ja täsmentää sitä, antaa sille merkitys ja luoda ohje käsitteen käytölle (Hirsjärvi ym. 2007, 148). Tietosuoja-asetukseen liittyvät käsitteet ja periaatteiksi muotoillut normit ovat normatiivisia ja myös melko konkreettisia. Asetus sisältää 173 johdantokappaletta (resitaalia), joissa selvitetään asetuksen tavoitteita, selvennetään sen soveltamisalaa ja annetaan tulkintaohjeita eli määritellään lain tulkintakehys. Käsite määritellään normatiivisin keinoin kirjottamalla termin määritelmä asetustekstiin. Esimerkiksi suostumuksen pääasiallinen merkitys omassa kontekstissaan esitettynä voi vaikuttaa selkeältä, mutta mitä se tarkoittaa konkreettisesti, onkin tulkinnanvaraisempaa. Sana ”nimenomainen” toistuu asetuksessa usein ja sen merkitystä on jouduttu purkamaan selkeiksi ohjeiksi (esim. Working Party 29 2016).

Tietosuoja-asetuksen käsitekokonaisuudet muodostuvat tietosuojaperiaatteista, henkilötiedon käsittelyn säännöistä ja rekisteröidyn oikeuksista. Tietosuojaperiaatteet voidaan nähdä käsitehierarkian ylimpänä tasona, josta kaikki rekisteröidyn oikeudet ja toisaalta rekisterinpitäjän ja käsittelijän velvollisuudet voidaan johtaa. (Bartolini, Muthuri & Santos 2015). Tietosuojalainsäädäntö tukeutuu juuri näiden periaatteiden varaan. Ne kertovat toisaalta lainsäädännön pääasiallisen sisällön, mutta samalla ne ovat normatiivisia eli toimintaa ohjaavia. (Alapuranen, Lehtonen, Koskinen & Wiberg 2020, 50.) Siksi tietosuojaperiaatteiden nostaminen tutkimuksen keskiöön on perusteltua.

2.3 Informaatio-oikeus ja sen keskeiset käsitteet

Oikeustieteellisessä kentässä tutkimus kuuluu informaatio-oikeuden oikeudenalaan. Sen tutkimuskohteena on oikeus tietoon, tiedollinen itsemääräämisoikeus, informaatiovapaus, viestintä ja tietoturva. Tiedosta on muodostunut merkittävä yhteiskunnan eri rakenteisiin vaikuttava strateginen väline ja markkinahyödyke, jolla tehdään kauppaa ja jolla on arvo sinänsä. Informaatio-oikeus keskittyy tietoon liittyvien informaatioprosessien sääntelyyn, tiedonsaantioikeuteen ja tietoon liittyviin velvollisuuksiin. Informaatioprosessissa on kyse tiedon hankinnasta, käytöstä, luovuttamisesta, säilyttämisestä ja hävittämisestän eli kaikenlaisesta tiedon käsittelystä. Informaatio-oikeuden yksi lainopillinen tehtävä on muotoilla, systematisoida ja tulkita niitä säätelyperiaatteita ja oikeusnormeja, jotka ohjaavat informaation käsittelyä. (Voutilainen 2019, 22-23.)

Informaatio-oikeuden keskeinen periaate on oikeus tietoturvaan ja yksilön oikeudesta määrätä itseään koskevista tiedoista, ns. tiedollinen itsemääräämisoikeus (Neuvonen 2019, 37). Oikeus tietoon on informaatio-oikeuden keskeinen perusperiaate. Yksilöllä on oikeus saada itseään koskevat tiedot, mutta myös oikeus määrätä omien tietojensa käytöstä. Tämä puolestaan rajoittaa muiden oikeutta saada henkilön tietoja käyttöönsä. (Voutilainen 2019, 33-34.)

Informaatio-oikeuden keskeisiä käsitteitä ovat tieto, hyvä henkilötietojen käsittelytapa ja tietojenkäsittely. *Tieto* voidaan määritellä monella tavalla, mutta informaatio-oikeudellisessa viitekehyksessä se on ”tiettyä kohdetta tai asiaa koskeva, käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa yhdistelmä” (Voutilainen 2019, 39). *Tietojenkäsittely* koskee toimenpiteitä, jotka kohdistuvat tietoon sen elinkaaren eri vaiheissa aina keräämisestä sen hävittämiseen saakka. *Tietosuojalla* tarkoitetaan yksilön perusoikeuksien toteutumista henkilötietojen

käsittelyn turvaamisella ja oikeutta omiin henkilötietoihin. Se ei ota kantaa tietojen julkisuuteen tai salattavuuteen. (Voutilainen 2019, 60.) Tietosuojakäsitettä ei ole tietosuoja-asetuksessa eikä myöskään Suomessa lainsäädännön tasolla määritelty normatiivisesti. Tietosuoja on kuitenkin kansainvälisesti käytetty termi, jolla viitataan henkilötietojen suojan oikeudelliseen sääntelyyn. Säätelyn kohteena ei ole vain tieto, vaan myös luonnollisen henkilön yksityisyys ja oikeudet. (Alapuranen ym. 2020, 37-38.) *Tietoturva* merkitsee tietojen ja järjestelmien suojaamista teknisin ja hallinnollisin toimenpitein siten, että tieto on saatavilla käyttöön ja hyödynnettävissä tarvittaessa tietoon oikeutetuilla henkilöillä. Tietoturvan keskeiset periaatteet ovat eheys, luottamuksellisuus sekä saatavuus. (Voutilainen 2019, 197.)

2.4 Toiminnallinen tutkimus tutkimusotteena

Tutkimus suoritetaan toiminnallisena tutkimuksena. Sille on tyypillistä sekä tutkia että hakea käytännön ongelmiin ratkaisuja konkreettisilla kehitystoimilla. Tutkija ei ole prosessissa ulkopuolinen, vaan osallistuu itse kehitystoimintaan yhteistyössä muun organisaation kanssa. Tämä erottaa toiminallisen tutkimuksen muista laadullisista tutkimusmenetelmistä. Tapaustutkimuksesta tämän tutkimuslaji eroaa siinä, että ongelmaan tai kysymykseen ei vain haeta vastausta, vaan pyritään myös muuttamaan vallitsevaa olosuhdetta. (Saaranen-Kauppinen & Puusniekka 2006.) Toimintatutkimuksessa kehitetään yksilöityä kohdetta, eikä tuloksia voi laajentaa tai yleistää muihin tapauksiin. Muutoksen edellytys on muutettavan ilmiön ja siihen vaikuttavien tekijöiden tunteminen. Muutos saadaan aikaiseksi yhteistyössä kehitettävän organisaation kanssa tutkimalla ja kehittämällä toimintoja prosessissa. Kun laadullinen tutkimus yleensä päätyy analysoimaan ja ratkaisemaan tutkittavaa ongelmaa tiedollisesti, toimintatutkimuksessa edetään itse toiminnan parantamiseen ja kehittämiseen käytännön tasolla. (Kananen 2014, 14-15.)

Toiminnallinen opinnäytetyö ja toimintatutkimus pyrkivät käytännönläheiseen ja käytäntöä hyödyttävään lopputulokseen erotuksena tutkimuksellisesta opinnäytetyöstä, jonka pääasiallisena tiedonintressinä on uuden tiedon löytäminen. Tavoitteena ei ole vain tietää, miten asiat ovat, vaan myös ratkaista, miten asiat voisi tehdä paremmin. Tutkimuksen varsinainen kohde ei ole toiminta sinänsä, vaan toiminnan kehittäminen. Tutkimuksessa tutkijan rooli on kaksinainen, sillä hän toimii sekä tutkijana että itse muutokseen osallistuvana. Tutkijan interventio on siis olennainen osa toimintatutkimusta. Toimintatutkimus on sosiaalista toimintaa, jossa tutkittava kohde samalla oppii ja kehittyy. (Heikkinen 2018.)

Vaikka toimintatutkimuksessa pääpaino on käytännön toiminnan parantamisessa, se ei kuitenkaan sulje pois uuden tiedon tuottamista käytännöistä ja uuden ammatillisen tiedon luomista. Teoria toimii käytännöllisten tavoitteiden saavuttamisen tukena, mutta ei tutkimuksen keskiössä. Tulosten arvioinnissa on keskeisintä juuri niiden hyödyllisyys ja käytettävyys toiminnan kehittämisessä ja ongelmien ratkaisussa. Tutkimuksellisuus tulee esiin järjestelmällisyytenä, kriittisenä suhtautumisena sekä analyyttisena otteena erotuksena arkiajatteluun pohjautuvasta kehittämisestä. Siinä ratkaisuja ei juurikaan perustella teoreettisilla tai menetelmällisillä valinnoilla. (Ojasalo, Moilanen & Ritalahti 2014,18-22.)

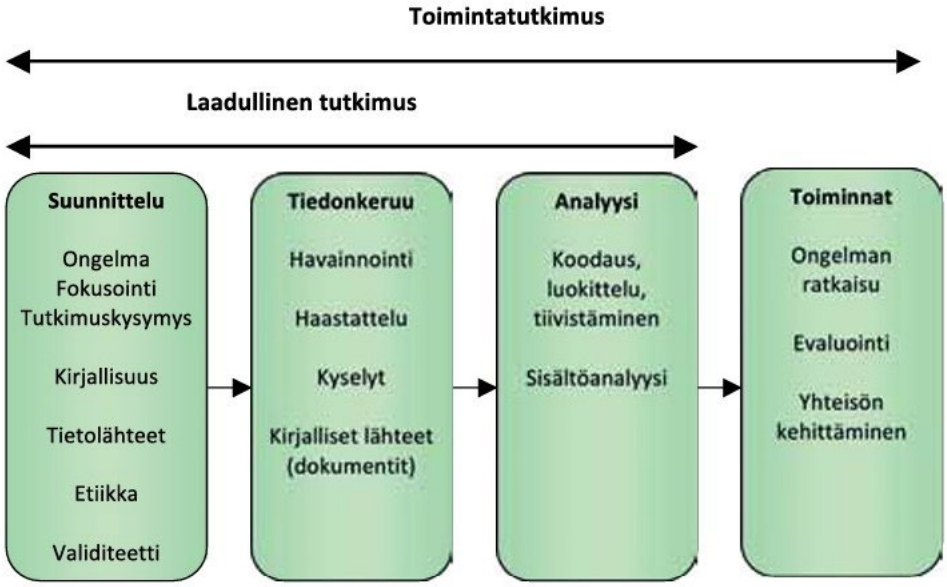
Erilaisista painotuksista huolimatta erilaisten toimintaa painottavien tutkimusotteiden pääasiallinen intressi on toiminnan ja tutkimuksen yhdistäminen. Toiminnan ja tutkimuksen yhdistäviä tutkimussuuntauksia on lukuisia, ja toimintatutkimuksella onkin yhteiskuntatieteissä pitkät perinteet. Jo 1920-luvulla John Dewey arvosteli tiedon ja toiminnan erottamista toisistaan yhteiskuntatieteissä. (Heikkinen 2018.) Paljon siteerattu toimintatutkimuksen uranuurtaja Kurt Lewin toi esiin todellisuuden muuttamisen olennaisena osana tutkimusprosessia. Toimintatutkimus ei ole vain yksi tutkimussuuntaus, vaan esimerkiksi tutkijan roolissa voi olla olennaisia eroja. Perinteinen lewiniläinen suuntaus pitää tutkijan havainnoijan asemassa, kun taas osallistavassa toimintatutkimuksessa tutkittava yhteisö on aktiivisesti mukana tutkijoina. (Toikko & Rantanen 2009, 29-30.) Toimintatutkimuksessa tutkijan osallisuus tutkittavan yhteisön kehittämisessä on olennaisesti tutkimustulosta määrittävä tekijä. Tutkija tekee aloitteita ja vaikuttaa yhteisöön, jolloin tutkija on itse osa tutkittavaa kohdetta. (Heikkinen 2018.)

Tutkimuksellinen kehittämistoiminta etenee spiraalimaisesti suunnittelusta toimintaan, havainnointiin ja reflektointiin jatkuvana prosessina. Ajatuksena on, että jokainen kierros kehittää toimintaa. Arvioimalla saatuja tuloksia voidaan tehdä uusia suunnitelmia ja toteuttamisen kautta todeta niiden toimivuus ja korjata toimintaa. (Toikko ym. 2009, 66-67; Salonen 2013, 14.) Käsillä olevassa toimintatutkimuksessa korostuu tämän kaltainen eteneminen, sillä tietosuoja on organisaatiossa opittava ja sisäistettävä asia, ja ymmärrys lisääntyy jatkuvasti työn edetessä. Työstettävät materiaalit ovat jatkuvan parannuksen kohteena. Tietoturva organisaatiossa on jo lähtökohdiltaan ja asetuksessakin mainittuna jatkuvan parannuksen ja kehittämisen kohde.

Spiraalimaisessa kehittämistoiminnassa suunnitteluvaihe käsittää kuvauksen tutkimuksen tavoitteista, kontekstista, toimijoista, menetelmistä, aineistoista ja dokumentointitavoista. Varsinaisessa toteutusvaiheessa suunnitelma toimeenpannaan ja siinä tapahtuu varsinainen oppiminen. Arviointivaiheessa syntynyttä tuotosta tarkastellaan suhteessa tavoitteisiin ja tehdään korjauksia ja täsmennyksiä. Viimeistelyvaiheessa valmistellaan lopullinen tuotos. Siinä voidaan myös esitellä virallisesti tuotos kohderyhmälle. (Salonen 2013, 17-19.) Tässä työssä koulutusmateriaalin esittäminen ja koulutusten järjestäminen sekä tietotilinpäätöksen ja muun materiaalin julkaiseminen edustavat työn lopputulosta.

Toiminnallisessa tutkimuksessa käytetään perinteisiä tutkimusmenetelmiä. Tiedonhankinta poikkeaa kuitenkin perinteisen laadullisen tutkimuksen menetelmistä, sillä tietoa saavutetaan parhaiten toiminnan kautta. Tieto on usein sisällä prosesseissa ja siihen pääsee käsiksi vain osallistumalla toimintaan. (Kananen 2014, 13.) Toiminnallisessa opinnäytetyössä tutkimusmenetelmien käyttö on vapaampaa kuin tutkimuksellisessa työssä. Toiminnallisessa tutkimuksessa on riittävää saada suuntaa antavaa tietoa, riippuen toki tutkimustehtävästä. Tällöin esimerkiksi haastattelu voi toimia yhtenä tiedonlähteenä, ei varsinaisena analyysin kohteena. Tiedon analysointi ei ole yhtä tarkkaa ja jäsentynyttä kuin tutkimuksellisessa työssä. Esimerkiksi haastattelun litterointi tai puhtaaksi kirjoittaminen ei ole välttämätöntä. (Vilkka & Airaksinen 2003, 57, 53.)

Toiminnallinen tutkimus koostuu kahdesta osasta, raportista ja tuotoksesta eli produktista. Raportissa kuvataan tutkimuksen ja tutkimuksenteon perusasiat. Sen perusteella voidaan arvioida, miten tutkija on tavoitteessaan onnistunut asiallisesti, viestinnällisesti ja muodollisesti. Itse tuotos on suunnattu työn tilanneelle taholle, joten sen muoto määräytyy käytännön tarpeiden mukaisesti. (Vilkka ym. 2003, 65.)



Kuva 1. Toimintatutkimus suhteessa laadulliseen tutkimukseen. (Kananen 2014, 26)

Kohdeyrityksessä käytännön tietosuojan jalkauttaminen käytäntöihin ei ole täysin toteutunut. Siksi pelkästään tutkiminen ja tutkimustuloksen raportointi eivät ole riittäviä keinoja ongelman ratkaisemiseksi. Toimintatutkimus valikoitui tutkimusmenetelmäksi juuri sen toimintaan ulottuvan otteensa vuoksi. Kohdeorganisaatiossa on tarve tuottaa dokumentointia, mutta myös ohjeistaa ja lisätä tietosuojan tietoperustaa. Dokumentointi on olennainen osa ongelman ratkaisua eli osoitusvelvollisuuden täyttämistä. Tutkija toimii osana prosessia asiantuntijan roolissa samalla ratkaisten tietosuoja-asetuksen käytännön soveltamisen ongelmakohtia.

Tässä tutkimuksessa tutkimustehtävään pyritään saamaan taustatietoa henkilöstölle suunnatun kyselylomakkeen (liite 1) ja täydentävän teemahaastattelun (liite 2) keinoin. Kysely suoritetaan kyselytyökalun avulla. Lomakkeessa esitetään monivalintakysymyksiä, joilla kerätään tietoa henkilötiedon käsittelystä käytännön työtehtävissä. Käytettävät käsitteet määritellään lomakkeessa ja se testataan ennen laajempaa jakelua. Siten voidaan varmistua siitä, että kysymykset ovat ymmärrettäviä ja yksiselitteisiä. Lomake- ja avoimessa haastattelussa ei voi kysyä mitä tahansa, vaan kysymysten on oltava kiinteässä yhteydessä tutkimuksen tarkoitukseen ja ongelmanasetteluun (Tuomi & Sarajärvi 2018). Tässä työssä kysymykset johdetaan tietosuoja-asetuksen käsitteistä, tarkemmin tietosuojaperiaatteista, sillä juuri niiden saattaminen osaksi käytäntöjä on kehitystyön tavoite.

Teemahaastattelussa käsiteltävät teemat on ennakolta mietitty, mutta varsinainen haastattelu on vapaamuotoinen. Haastateltavasta riippuen eri teemoja voidaan painottaa ja joitain käsitellä suppeammin. (Eskola, Lätti & Vastamäki 2018.) Teemahaastattelu suoritetaan myynnin, oston ja hallinnon edustajille. Haastattelu toimii samalla työn tavoitteen saavuttamisessa antamalla uusia ajatuksia kehittää henkilötiedon käsittelyä omassa työssä. Vilkkaan mukaan yksi haastattelun tavoitteista voikin olla emansipatorinen antaen haastateltavalle mahdollisuuden oivaltaa uusia asioita. Tutkijan toimiminen tutkittavassa organisaatiossa luo edellytykset ymmärtää toimintaympäristöä ja organisaatiokulttuuria. Siten haastattelija ja haastateltava jakavat saman käsitteellisen ympäristön ja auttavat tulkintojen tekemisessä. (Vilkka 2015.)

Haastatteluilla saadaan selville nykytila – miten ja mitä henkilötietoja henkilöstö käsittelee tietoja ja mikä on yleinen tietotaso tietosuoja-asetuksen vaatimuksista. Laadulliselle tutkimukselle tyypillisellä tavalla aineistoa tarkastellaan teoreettisen viitekehyksen läpi etsien ongelman kannalta olennaiset ainekset (Alasuutari 2011). Toimintatutkimuksen tavoite on saada aikaan muutosta. Tässä työssä muutosta edustaa henkilökunnan tietoisuuden lisääntyminen tietosuojasta sekä tietosuojan dokumentointi ja menetelmien kehittäminen sekä tietosuojan nivominen osaksi prosesseja ja johtamista.

Toiminnallisen tutkimuksen validiteettia ja reliabiliteettia ei voida arvioida yhtä helposti kuin määrällisessä tai perinteisessä laadullisessa tutkimuksessa. Tämä johtuu siitä, että toiminnan muutoksen mittaamiseksi ei ole kunnollisia mittareita eikä sen tavoitteena ole yleistettävyys. Toiminnallisen tutkimuksen luotettavuuden keskeinen mittari on asianmukainen dokumentointi prosessin jokaisessa vaiheessa. Lisäksi tutkimukseen osallistuvat toimijat voivat vahvistaa tulosten oikeellisuuden ja sen, että tutkimuksessa on saavutettu suunnitellut tulokset. Myös tutkijan on oltava tarkkana, jotta omat mielipiteet eivät sekoitu saatuihin tutkimustuloksiin. (Kananen 2014, 138.)

2.5 Lähdeaineisto

Oikeustieteellinen tutkimus on keskittynyt tietosuoja-asetuksen lainopilliseen analyysiin ja erityisesti sen tulkintaan, miten yritykset voivat varmistaa tietosuojan toteutumisen. Oikeustieteellisen tutkimuksen lähdeaineistoja voidaan jakaa monella tapaa, mutta yksi tyypillinen on Aulis Aarnion jako vahvasti velvoittaviin kuten lainsäädäntöön ja tuomioistuinten ennakkoratkaisut,

heikosti velvoittaviin kuten lainvalmisteluaineisto ja tuomioistuinten ratkaisut sekä sallittuihin lähteisiin kuten oikeustieteellinen kirjallisuus. Jaottelun perusteena on kysymys siitä, mitä tapahtuu, mikäli lakia tulkitseva sivuuttaa ratkaisussaan tietyn oikeuslähteen. Tähän staattiseksi kutsutun jaottelun rinnalla on dynaaminen oikeuslähdeoppi, jossa oikeuslähteiden painoarvoa tulkitaan tilannekohtaisesti. Esimerkiksi Eurooppa oikeuden kysymyksissä on huomattava, että kansallinen lainsäädäntö on alemman arvoista ja EU-tuomioistuimen ratkaisut voivat olla sitovia. (Kolehmainen 2016, 116-117.)

Tutkimuksen lähdeaineisto muodostuu lainsäädännöstä ja muista virallislähteistä sekä erilaisista viranomaisohjeistuksista ja tulkinnoista. Oikeusnormin sisältö muotoutuu konkreettisessa elämäntilanteessa, jossa normi esiintyy. Siksi erilaisia abstrakteja normeja ja periaatteita tulee tarkastella siinä yhteydessä, jossa niitä käytetään. (Hirvonen 2011, 47.) Tietosuoja-asetuksen ja yleensä henkilötiedon suojan oikeustieteellinen tutkimus keskittyy pääosin asetuksen normien tulkintaan, sillä artiklojen sisältö ei ole yksiselitteistä. Yrityksille asetetaan suoria velvoitteita, joiden täyttämättä jättämisestä voidaan asettaa huomattavia hallinnollisia sakkoja. Asetuksen normien kirjoittaminen periaatteiden muotoon ei lievennä tulkinnanvaraisuutta ja epävarmuutta, joskin se lisää liikkumavaraa. (Lindroos-Hovinheimo 2018, 53, 61.) Käytännön laintulkinnassa lähtökohtana on lain kielellinen ilmaisu. Mikäli se on selkeä ja yksiselitteinen, lisäperusteita ei tarvita. Mikäli lisäperusteita tarvitaan, niitä haetaan mm. lainsäädännön tarkoituksesta, oikeudenalakohtaisesta systematiikasta, perusoikeusargumenteista, oikeuskäytännöstä ja lainopista. (Kolehmainen 2016, 10.)

EU:n tietosuoja-asetuksen keskeiset periaatteet on pyritty määrittelemään jo asetuksen tekstissä antamalla myös esimerkkejä niiden sisällöstä. Tietosuojaan liittyvän sääntelyn periaatteet ja tavoitteet on asetuksessa määritelty hyvin laajasti. Silti käytännön toteutuksen tasolla esiintyy paljon epäselvyyttä konkreettisesta tarkoituksesta ja siksi erityisesti EU:n tietosuojaryhmä WP29 on antanut tulkintaohjeita asetuksen siirtymäajan päättymiseen saakka 25.5.2018. Sen jälkeen toimintaa on jatkanut Euroopan tietosuojaneuvosto, European Data Protection Board EDPB (Euroopan tietosuojaneuvoston www-sivut 2018). Vaikka tietosuoja-asetuksessa suosituksille ja mielipiteille ei myönnetä sitovuutta, käytännössä mm. jäsenvaltioiden tietosuojavaltuutetuista koostuvan elimen kannanotot ovat tärkeitä ohjenuoria niin kansallisille viranomaisille kuin rekisterinpitäjille (Eriksson 2019, 21-22). EU:n tuomioistuinten ratkaisut ja ennakkoratkaisut ohjaavat viime kädessä tietosuoja-asetuksen tulkintaa. Vuoteen 2020 mennessä on tuomioistuin antanut tuomionsa kaikkiaan 54 tapauksessa. (EUR-Lex www-sivut 2020.)

Tämän työn empiirisessä osiossa henkilötietojen käsittelyprosessia tutkitaan kohdeyrityksen dokumenttien, pääasiassa prosessikuvausten ja ohjeistusten kautta. Tarkoituksena on selvittää, millaisia henkilötietoja, missä järjestelmissä ja millaisissa prosesseissa niitä käsitellään. Prosessien ja käytänteiden selvittämisessä käytetään tukena haastatteluja, joiden avulla selvitetään nykyinen prosessinjohtamismalli sekä se, minkälaisia vaatimuksia ja haasteita EU-tietosuoja-asetus tuo prosessien hallintaan organisaation näkökulmasta. Keskeinen kysymys toimintojen kehittämisen kannalta on se, miten tällä hetkellä henkilötieto tunnistetaan prosessissa, millaisia käytäntöjä siihen liittyy ja miten viestintä prosessissa on hoidettu.

Tietosuoja-asetuksen normeja tutkittaessa tutkitaan käytännössä sitä, mitä se tarkoittaa tietosuojan ja rekisteröidyn osalta. Viimekädessä tulkintaa tekee Euroopan Unionin tuomioistuin (European Court of Justice). Tulkintaa tekevät ja kannanottoja antavat niin ikään Euroopan tietosuojaneuvosto (European Data Protection Board) sekä eri kansalliset tietosuojaviranomaiset esim. Iso-Britannian ICO (Information Commissioner's Office) tai Suomen Tietosuojavaltuutetun toimisto (Tietosuojavaltuutetun www-sivut 2020). Suomessa tietosuojaviranomainen on langettanut ensimmäisiä hallinnollisia seuraamusmaksuja ja antanut ohjeita ja määräyksiä useissa tapauksissa. Tapaukset ovat koskeneet puutteita rekisteröidyn informoinnissa, käsittelyn dokumentoinnissa ja vaikutustenarvioinnissa sekä tarpeettomien tietojen keräämistä työnhakijoilta. (Tietosuojavaltuutetun www-sivut 2020.) Viranomaisen päätökset antavat henkilötiedon käsittelijöille konkreettisesti vinkkejä siitä, missä menee sallittavuuden raja.

3 EU:N YLEINEN TIETOSUOJA-ASETUS JA TIETOSUOJAPERIAATTEET

3.1 Yleistä tietosuoja-asetuksesta

Yksityisyys ja henkilötietojen suoja on ihmisen perusoikeus, joka on kirjattu niin EU:n perusoikeuksiin (EU:n perusoikeuskirja 2012/C 326/02, 8) kuin Suomen perustuslakiin (PerL 731/1999 10 §). Suomessa ensimmäinen henkilörekisterilaki (471/1987) astui voimaan 1988. Se kumottiin uudella henkilötietolailla (523/1999). Euroopan laajuinen sääntely syntyi vuonna 1995, jolloin säädettiin tietosuojadirektiivi (95/46/EY) ja Suomessa henkilötietolaki (523/1999). EU:n yleinen

tietosuoja-asetus astui voimaan 24.5.2016 ja sen soveltaminen alkoi 25.5.2018. Asetuksella kumotaan aikaisempi tietosuojadirektiivi 95/46/EC. Tietosuoja-asetus on suoraan sovellettavaa oikeutta. Asetukseen on kirjattu kuitenkin myös kansallista liikkumavaraa mm. tietosuojaviranomaiseen liittyen ja siten siihen liittyy myös asetukselle epätyypillisiä, mutta direktiiville tyypillisiä elementtejä. Suomessa asetusta täydentävä ja täsmentävä tietosuojalaki (5.12.2018/1050) on astunut voimaan 1.1.2019. Uuden lainsäädännön tärkeä tavoite on vahvistaa rekisteröidyn oikeuksia., mutta samalla turvata yritysten liiketoimintamahdollisuudet. Euroopan Unioni pyrkii uudella tietosuoja-asetuksella myös varmistamaan sisämarkkinoiden tehokkaan toiminnan yhtenäistämällä jäsenvaltioiden henkilötietoja koskevaa lainsäädäntöä. (Yleinen tietosuoja-asetus 679/2016).

Yksityisyyden suoja on kirjattu lukuisin lakeihin mm. lakiin yksityisyyden suojasta työelämässä (YksTL 759/2004). Suomessa henkilötietojen käsittelyä säätelevää lainsäädäntöä on olemassa muita EU-maita enemmän. Erityisesti työelämää ja potilaan oikeuksia on haluttu erityislainsäädännöllä turvata. (Alapuranen ym. 2020, 9.)

Uuden tietosuojalainsäädännön myötä vastuuta tietosuojasta on selkiytetty ja rekisterinpitäjältä edellytetään aktiivisempaa henkilötietojen hallintaa. Tietosuoja-asetuksen olennainen ero aiempaan lainsäädäntöön on rekisterinpitäjän kannalta riskiperusteinen, omaan arvioon, ennakoivuuteen ja osoitusvelvollisuuteen perustuva toiminnan sääntely. Riskiperusteisuus merkitsee osaltaan sitä, että riskialttiiden toimintojen sääntelyä kiristetään, mutta samalla vähäriskisten toimintojen osalta ylisäätelyä pyritään välttämään. Osoitusvelvollisuuden keskeinen ajatus on rekisterinpitäjän kyky osoittaa konkreettisesti tietosuojaperiaatteiden ja asetuksen velvoitteiden yleinen toteutuminen. (Aalto-Setälä & Honkasalo 2017.) Sen tulee pystyä osoittamaan, että tietosuoja-asetuksen artiklassa 5 säädettyjä tietosuojaperiaatteita noudatetaan (Yleinen tietosuoja-asetus 679/2016, 5).

Henkilötiedon käsittely on ennen uutta asetusta ollut lähinnä yrityksen sisäinen prosessi. Vaikka henkilötietolaki (523/1999) on jo entuudestaan asettanut velvoitteita henkilötietojen käsittelylle, on osoitusvelvollisuus pakottanut yritykset organisoimaan tietosuojan hallittavaksi kokonaisuudeksi osoitusvelvollisuuden mahdollistamiseksi. Uuden asetuksen myötä henkilötiedon käsittelyn läpinäkyvyys lisääntyy ja tiedonkäsittelyn prosesseihin liittyy myös ulkoiset prosessit rekisteröidyn vahvistettujen tiedonsaantioikeuksien sekä viranomaisten valvonnan myötä. Henkilötiedon käsittelyprosessit eivät siten ole enää organisaation sisäinen asia, vaan niissä on otettava

huomioon myös rekisteröidyn ja viranomaisten entistä laajemmat oikeudet. Uuden asetuksen tarkoituksena on vastata digitaalitalouden tietosuojaan ja –turvallisuuteen kohdistuneisiin haasteisiin lisäämällä henkilötiedon käsittelyn läpinäkyvyyttä, vahvistamalla rekisteröidyn oikeuksia ja mahdollisuuksia valvoa henkilötietojensa käyttöä ja velvoittamalla rekisterinpitäjiä huolehtimaan henkilötietojen suojaamisesta entistä paremmin ja aktiivisemmin. Yleisenä periaatteena tietosuoja-asetuksessa on oletusarvoinen ja sisäänrakennettu tietosuoja (privacy by design and default), jonka mukaan vaatimukset on otettava huomioon jo tietojärjestelmien suunnittelussa, toimintamalleissa sekä organisatorisissa järjestelyissä. (Henriksson 2017.)

Tietosuoja-asetuksen neljännessä artiklassa määritellään asetuksen keskeiset käsitteet. *Rekisterinpitäjä* on se taho, luonnollinen henkilö, oikeushenkilö, viranomainen tai muu sellainen elin, joka määrittelee henkilötiedon käsittelyn tarkoitukset ja keinot. *Henkilötietojen käsittelijä* on se taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. *Henkilötiedon käsittelyllä* tarkoitetaan niitä toimintoja, joita kohdistetaan henkilötietoihin kuten keräämistä, tallentamista, järjestämistä, säilyttämistä, muokkaamista, hakua, kyselyjä, tietojen käyttöä ja luovuttamista sekä tietojen yhdistämistä, poistamista, rajoittamista tai tuhoamista. Yrityksen työsuhteessa oleva työntekijä, joka käsittelee henkilötietoja, ei ole käsittelijä asetuksen mukaisessa merkityksessä. Työntekijä toteuttaa rekisterinpitäjälle asetettuja vaatimuksia. (Voutilainen 2019, 145.) Henkilötietoja käsittelevän henkilön on noudatettava käsittelyssä rekisterinpitäjän antamia ohjeistuksia (Yleinen tietosuoja-asetus 679/2016, 29).

Henkilötiedolla tarkoitetaan yleisen tietosuoja-asetuksen mukaan

> ”kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.” (Yleinen tietosuoja-asetus 679/2016, 4).

Henkilörekisteri puolestaan tarkoittaa ”mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa” (Yleinen tietosuoja-asetus 679/2016, 4), joka on käyttötarkoituksensa mukaan järjestetty ja jota käsitellään kokonaan tai osittain automaattisen tietojenkäsittely avulla ja josta tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia. Käyttötarkoitus on määräävä tekijä, jonka mukaan henkilötiedot muodostavat juuri tietyn henkilörekisterin. (Voutilainen 2012, 249.)

Henkilörekisteri on looginen rekisteri, jolloin määräävää ei ole miten ja missä fyysisessä paikassa henkilötieto on, vaan käyttötarkoitus määrittää sen kuulumisen tiettyyn rekisteriin. Siten myöskään tietojenkäsittelyssä syntyviä väliaikaisia tiedostoja ja tallenteita ei pidetä erillisenä henkilörekisterinä niin kauan kuin ne ovat rekisterinpitäjän hallussa niiden käyttötarkoituksen pysyessä muuttumattomana. (HE 96/1998; Voutilainen 2012, 250.) Rekisterin järjestämiselle ei ole erityisiä kriteerejä esim. kortiston tai luettelon muoto. Jos tarkoituksena on käyttää tietoja tiettyyn tarkoitukseen ja ne ovat helposti saatavilla, olkoonpa tiedot manuaalisessa tai sähköisessä muodossa, ne muodostavat henkilötietorekisterin (EUTI C25/17). Tietosuoja-asetus koskee vain sellaisten henkilötietojen käsittelyä, joka on kokonaan tai osittain automaattista taikka muuta kuin automaattista käsittelyä, jos henkilötiedot muodostavat rekisterin osan. Luonnollisen henkilön yksityisiin tarkoituksiin tapahtuva henkilötiedon käsittely ei kuulu asetuksen soveltamisalan piiriin. (Yleinen tietosuoja-asetus 679/2016, 2.)

3.2 Osoitusvelvollisuus

Osoitusvelvollisuus (accountability) on tietosuoja-asetuksen olennaisimmista muutoksista aikaisempaan lainsäädäntöön verrattuna. Olennainen ero johtuu, ei niinkään tietosuojavelvoitteiden sisällöstä, vaan siitä, että näiden velvoitteiden tehokas toteuttaminen pitää pystyä näyttämään toteen. Rekisterinpitäjän on toimeenpantava oikeanlaiset ja tehokkaat keinot tietosuojaperiaatteiden toteuttamiseksi ottaen huomioon ”käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit”(Article 29 Data protection working party 2010). Lisäksi sen pitää pystyä osoittamaan, että nämä toimenpiteet on tosiasiassa suoritettu. Osoitusvelvollisuus merkitsee, että yrityksen on teknisin ja organisatorisin toimin varmistettava, että tietosuojaperiaatteiden kirjain täytetään. Sen on dokumentoitava mm. mitä ja miten henkilötietoja käsitellään, mihin tarkoitukseen tietoja kerätään ja kuinka pitkään niitä säilytetään. Yrityksen on myös pystyttävä osoittamaan, miten se on varautunut mahdolliseen tietomurtoon. (Yleinen tietosuoja-asetus 679/2016, 24; European Data Protection Supervisor www-sivut 2018.)

Osoitusvelvollisuus terminä edellyttää, että on jokin taho, joka on tilivelvollinen jollekin jonkin asian suhteen ja tämä ulkopuolinen taho voi määrätä velvoitteen noudattamatta jättämisestä sanktion (Bennett 2010, 3). Osoitusvelvollisuuden periaatetta on pyritty systematisoimaan käytäntöä palvelevaksi. WP29 neuvoa antava elin on purkanut periaatteen kolmeen tasoon, jotka Bennet on

nimennyt periaatteiksi (policy), menettelyiksi (procedures) ja käytännöiksi (practice). Jotta osoitusvelvollisuus kokonaisuudessaan toteutuu, pitää nämä kolme eri ulottuvuutta olla huomioituna. Periaatteiden tasolla rekisterinpitäjä sitoo tietosuojaperiaatteet osaksi yrityksen sisäisiä käytännesääntöjä ja prosesseja. Menettelytasolla rekisterinpitäjä ilmentää organisatorisilla toimilla kuten ohjeistuksilla, tietosuojavaltuutetun nimeämisellä ja koulutuksella, osoitusvelvollisuutensa. Jotta se pystyy osoittamaan, että tietosuojaperiaatteita ei noudateta vain dokumentoinnilla, sen pitää toteuttaa periaatteet myös käytännössä. Käytännön toimien tehokkuus voidaan todentaa esimerkiksi auditointien kautta. Auditointi voisi olla esimerkiksi osa laatusertifikaattia ISO 9001. (Bennett 2010, 6-7.) Tietosuoja-asetuksessa todetaan sertifiointimekanismien noudattamisen olevan yksi tapa osoittaa rekisterinpitäjälle asetettujen vaatimusten noudattaminen (Yleinen tietosuoja-asetus 679/2016, 24).

Alla olevassa taulukossa Bennetin osoitusvelvollisuuden tasot on purettu käytännön toimiksi.

OSOITUSVELVOLLISUUDEN TASOT		
Periaatteet ja normit	Käytäntö	Todentaminen
Strategiat Tietosuojapolitiikka Periaatteet	Tietosuojaorganisaatio Tietotilinpäätös Prosessikuvaukset Toimintaohjeet Koulutus	Sisäiset ja ulkoiset auditoinnit Sertifikaatit Mittarit

Kuva 2. Bennettin (2010) osoitusvelvollisuuden tasot kuvattuna käytännössä

Rekisterinpitäjän on itse selvitettävä, mitä asetuksen vaatimus merkitsee sen oman toiminnan kannalta. Rekisterinpitäjän on otettava käyttöön sellaiset menetelmät ja käytänteet, jotka parhaiten palvelevat sen liiketoimintaa ja asiakkaiden vaatimuksia (Bennett 2010, 6).

WP29 ryhmä on osaltaan tarkastellut osoitusvelvollisuutta ja konkreettisia keinoja sen osoittamiseksi. Konkreettisia toimia voi olla esimerkiksi sisäiset toimintaohjeet ja prosessikuvaukset ja henkilöstön koulutus. Toimenpiteiden tehokkuus tulee pystyä osoittamaan esimerkiksi sisäisillä ja ulkoisilla auditoineilla tai erilaisilla valvontamekanismeilla. Tehokkuutta arvioitaessa lähtökohta on riskiperusteinen eli tarpeelliset toimet riippuvat siitä kuinka arkaluontoista tietoa ja

kuinka paljon tietoa käsitellään. (Article 29 Working Party 2010.) Osoitusvelvollisuuden liittäminen olennaiseksi osaksi tietosuoja-asetusta pyrkii kannustamaan rekisterinpitäjiä integroimaan henkilötietojen turvallisen käsittelyn osaksi yrityksen tietosuojakulttuuria (Vainio 2018, 19).

Seloste käsittelytoimista (records of processing activities) on yksi osa vaatimuksenmukaisuuden osoittamisessa. Se on pakollinen vain yli 250 työntekijän yrityksissä tai jos käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille. (Yleinen tietosuoja-asetus 679/2016, 30; Tietosuojavaltuutettu 2017.) Yhtenä mahdollisuutena on hyödyntää tietosuojasertifikaatteja tai alakohtaisia käytännesääntöjä (Oikeusministeriö 2017, 14). Nämä eivät kuitenkaan poista muun dokumentoinnin tärkeyttä. Jokaisen yrityksen on oman tietoturvakartoituksen perusteella määritettävä se taso, jolla dokumentointi tulee riittävällä tavalla suorittaa.

3.3 Tekniset ja organisatoriset edellytykset

Sisäänrakennetun ja oletusarvoisen tietosuojan periaate edellyttää teknisten ja organisatoristen seikkojen huomioimista aina uusia järjestelmiä kehitettäessä (Yleinen tietosuoja-asetus 679/2016, resitaali 78). Järjestelmässä on oltava valmiina mahdollisuudet täyttää rekisteröidyn oikeudet sekä osoitusvelvollisuus (Oikeusministeriö 2017, 13). Tietosuojaperiaatteet tulee ottaa oletusarvoisesti huomioon jo käsittelytapoja määritettäessä ja käsittelyn yhteydessä erityisesti uusia tietoteknisiä järjestelmiä kehitettäessä. Tällöin on otettava huomioon kohtuulliset toteuttamiskustannukset sekä riskikartoituksen myötä arvioitu käsittelyn aiheuttama riski henkilön oikeuksille ja tietosuojalle. Teknisillä ja organisatorisilla toimilla varmistetaan kerättävien henkilötietojen tarpeellinen laajuus ja laatu. (Yleinen tietosuoja-asetus 679/2016, 25).

Henkilötietoihin pääsyn tulee olla rajoitettu vain niille henkilöille, joilla on perusteltu oikeus käsitellä tietoja. Organisatorisia toimenpiteitä ovat mm. henkilöstön kouluttaminen, salassapitosäännökset, käsittelyn ohjeistukset ja menettelysäännöt tietoja käsitteleville henkilöille. Teknisiä toimenteitä ovat mm. tietojen salaus, tekniset rajoitukset, käytönvalvonta ja tietotilinpäätösprosessit. Niiden avulla yrityksen tulee ehkäistä tietomurrot, tietojen tuhoutuminen ja vahingoittuminen. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 51.) Tietotekniikka näyttelee suurta osaa silloin, kun rekisteröidyn oikeuksia käytännössä toteutetaan. Tietosuoja-asetuksen luvussa 3 luetellaan varsinaiset rekisteröidyn oikeudet. Tietojärjestelmissä on oltava valmiudet tiedon

nopeaan löytymisen, sen muokkaamiseen, käsittelyn rajoittamiseen ja poistamiseen. Myös tiedon siirto toiseen järjestelmän on oltava mahdollista. (Yleinen tietosuoja-asetus 679/2016, luku 3.)

Jotta tietosuojasta huolehtiminen on yrityksessä organisoitua ja systemaattista, on sitä varten järkevää luoda tietosuojan hallintajärjestelmä, jota ohjaa ja valvoo tietosuojaorganisaatio. Tietosuojapolitiikassa luodaan yleiset suuntaviivat, menettelytavat ja strategiat yrityksen tietosuojan toteuttamisesta. Tietosuojasta vastaava henkilöstö määritellään ja vastuullistetaan organisoimaan tietosuojan vieminen käytänteisiin sekä valvomaan asetuksen noudattamista, suunnittelemaan tarvittavia toimenpiteitä ja raportoimaan tietosuojan toteutumisesta yrityksen johdolle. Tietosuojaorganisaation toiminta voidaan suunnitella vuosikellon muotoon, jolloin systemaattinen toiminnan kehittäminen ja toiminnan arviointi muodostuvat osaksi organisaation prosesseja. (Valtionvarainministeriö 2016.)

3.4 Käsittelyn laillinen peruste

Asetuksen 6:nnessa artiklassa luetellaan käsittelyn lainmukaisuuden kriteerit. Lainmukaisuus merkitsee, että henkilötietoja on käsiteltävä jonkin asetuksessa mainitun kuuden käsittelyperusteen mukaisesti. Näitä ovat rekisteröidyn suostumus, sopimus, rekisterinpitäjän lakisääteinen velvollisuus, elintärkeiden etujen turvaaminen, yleinen etu tai rekisterinpitäjän oikeutettu etu. (Yleinen tietosuoja-asetus 679/2016.) Kullekin käsittelytoimelle on määritettävä erikseen käsittelyn oikeusperuste, joka on määriteltävä ennen kuin henkilötietoja voidaan käsitellä. Mikään laillisista perusteista ei toteudu, mikäli tiedon kerääminen ei ole välttämätöntä sen käsittelylle asetetun tavoitteen saavuttamiseksi. Mikäli tavoite voidaan saavuttaa ilman henkilötiedon keräämistä, on käsittelystä luovuttava. (Information Comissioner’s Office www-sivut 2018.)

Yrityksen tärkeimmät perusteet henkilötietojen keräämiselle ovat sopimus, suostumus ja oikeutettu etu. Suostumukselle on asetuksessa mainittu erityiset vaatimukset. (Hanninen ym. 2017, 29-32.) Sen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Rekisterinpitäjän on pystyttävä osoittamaan suostumuksen saaminen ja annettava rekisteröidylle mahdollisuus peruuttaa suostumuksensa koska tahansa. (Yleinen tietosuoja-asetus 679/2016, resitaali 32, 42; 7 artikla.)

Sopimukseen perustuva henkilötietojen käsittely perustuu velvoitteiden täyttämiseen, joka ei olisi mahdollista ilman käsittelyä (Hanninen ym. 2017, 30). Sopimus voidaan tulkita sen valmisteluksi ja täytäntöönpanoksi niin suullisesti kuin kirjallisesti. Jotta sopimus voidaan katsoa solmitun, on se pystyttävä tosiallisesti osoittamaan. Siten esimerkiksi pelkän kiinnostuksen osoitus ei ole merkki sopimuksesta. (Voutilainen 2019, 161.) B-to-B yrityksessä asiakassuhde on tyypillisesti sopimussuhde, joten tätä perustetta voidaan käyttää yhtenä käsittelyperusteena.

Yleinen laillisen käsittelyn peruste B-to-B yritykselle on oikeutettu etu. Se on huomattavasti tulkinnanvaraisempi kuin sopimus ja suostumus ja siitä on esitetty erilaisia tulkintoja julkisissa keskusteluissa (esim. Tietosuojauutiset www-sivut 2018). Myös WP29 työryhmä on esittänyt seikkaperäisen analyysin oikeutetun edun sisällöstä. Oikeutettu etu ei ole peruste, joka voidaan ottaa käyttöön, kun muita perusteita ei ole olemassa. (Article 29 Working party 2014; Hanninen ym. 2017, 33.) Tietosuoja-asetuksen mukaan oikeutettu etu muodostuu rekisteröidyn ja rekisterinpitäjän välillä olevassa merkityksellisessä suhteessa mm. asiakassuhteessa, yhteisön jäsenyydessä tai työsuhteessa. Se ei kuitenkaan voi mennä rekisteröidyn oikeuksien ja perusoikeuksien edelle. Rekisteröidyn kohtuulliset odotukset käsittelystä on aina otettava huomioon. Myös konsernin sisällä voidaan siirtää niin asiakas- kuin työntekijätietoja oikeutettu etu perusteena. Huomioitavaa on, että asetuksen mukaan suoramarkkinointi voidaan katsoa oikeutetun edun toteuttamiseksi. (Yleinen tietosuoja-asetus 679/2016, resitaali 47-48.)

Oikeutettu etu on tosiasiassa vaikein näyttää toteen. Sen testaamiseen ja todentamiseen onkin kehitetty kuusiportainen tasapainotesti, jonka jokainen porras tulee läpäistä oikeutetun edun varmistamiseksi (Tietosuojavaltuutetun www-sivut 2020). Kaikissa tapauksissa on oltava seikkaperäinen perustelu oikeutetun edun käyttämiselle käsittelyperusteena jo osoitusvelvollisuuden täyttämiseksi (Hanninen ym. 2017, 33). Rekisterinpitäjän on pystyttävä osoittamaan, että on olemassa jokin asiallinen, sen toiminnassa perusteltavissa oleva yhteys rekisteröityyn sekä välitön tarve henkilötiedon käsittelylle rekisterinpitäjän etujen toteuttamiseksi. (Voutilainen 2019, 162–163.) Oikeutettu etu on joustavin kaikista laillisen käsittelyn perusteista, sillä se ei ole sidottu mihinkään tiettyyn tarkoitukseen. B-to-B liiketoiminnassa sen käyttö on perusteltua, sillä henkilön yksityisyydelle ei käsittelyllä useinkaan ole suurta vaikutusta, ja yhteistyökumppanin on perusteltua olettaa tietynlainen henkilötiedon käsittely. Lisäksi liiketoiminnassa voisi olla enemmän haittaa sillä, että kumppaneilta pyydetään suostumusta käsittelyyn, joka on muutoinkin välttämätöntä. Pitkäaikaisessa liikesuhteessa esimerkiksi suostumuksen pyytäminen ei enää ajaisi tarkoitustaan. (Information Commissioner’s Office www-sivut 2020.)

Oikeutetun edun olemassaolon näyttämiseksi yrityksellä pitää olla käsitys siitä, että käsittely tuo jotakin tiettyä ja selkeää etua liiketoiminnassa. Ei siis riitä pelkkä asiakassuhteen olemassaolo, vaan on pystyttävä seikkaperäisesti kuvaamaan esimerkiksi henkilötiedon käsittelyn välttämättömyys myynnin kehittämiseksi. Sen lisäksi käsittelyn tulee olla välttämätöntä tarkoituksen saavuttamiseksi, minkä selvittämiseksi pitää tutkia, onko olemassa jokin muu keino saavuttaa tarkoitus. (Information Commissioner's Office www-sivut 2020.) Oikeutetun edun lisäksi on yleensä suositeltavaa käyttää myös jotakin toista laillista käsittelyperustetta, joka edellä kuvatun mukaisesti B-to-B yritysten kyseessä ollessa on luontevaa olla sopimus.

3.5 Läpinäkyvyys ja asianmukaisuus

Asianmukaisuus merkitsee käsittelyä kohtuullisessa suhteessa käsittelyn tarkoitukseen. Asianmukainen käsittely edellyttää rekisteröidyn informoimista käsittelyn tarkoituksesta, käyttötarkoitussidonnaisuutta ja kaikenlaista rekisteröidyn oikeuksien huomioimista käsittelyn kaikissa vaiheissa. (Tietosuojavaltuutetun www-sivut 2020.)

Läpinäkyvyydellä tarkoitetaan helppoa pääsyä tietoihin ja rekisteröidylle annettavan informaation selkeyttä ja ymmärrettävyyttä (Blanchard 2016, 13). Rekisterinpitäjän on teknisin ja organisatorisin keinoin varmistettava, että kaikessa henkilötiedon käsittelyssä koko käsittelyn elinkaaren ajan toteutetaan tietosuoja-asetuksen kolmannessa luvussa säädettyjä rekisteröidyn oikeuksia. Henkilötietoja kerättäessä ja niitä käsiteltäessä rekisteröityä on informoitava käsittelyyn liittyvistä seikoista tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavissa olevalla tavalla kohderyhmä huomioiden. (Yleinen tietosuoja-asetus 679/2016, 12 artikla.)

Läpinäkyvyys tulee toteuttaa ennen käsittelyä, käsittelyn aikana sekä henkilötietojen käsittelyssä tapahtuneiden muutosten ja tietomurtojen yhteydessä. Läpinäkyvyys konkretisoituu tiedon antamisena käsittelytoimista, siinä miten käsittelyn aikana kommunikoidaan rekisteröidyn kanssa ja miten rekisterinpitäjä helpottaa rekisteröidyn oikeuksien käyttämistä ja toteuttamista. Olennaista on, että rekisteröity pystyy tiedon perusteella arvioimaan tietojen luovuttamiseen sisältyvän riskitason, jolloin käsittely ei tule yllätyksenä rekisteröidylle missään käsittelyn vaiheessa. (Article 29 Working Party 2018.) Kohtuullisuus ja asianmukaisuus merkitsevät rekisteröidyn etujen ja odotuksien huomioimista. Rekisteröidyn pitää voida luottaa siihen, että tietoja ei väärinkäytetä,

vaan niitä käytetään vain siihen tarkoitukseen, josta rekisteröityä on informoitu. (Korpisaari, Pitkänen & Warma-Lahtinen 2018, 89.)

Rekisterinpitäjän tiedot sekä käsittelyn tarkoitus ja oikeusperuste on mainittava aina tietoja kerättäessä. Lisäksi on ilmoitettava henkilötietojen vastaanottajat ja tietojen säilytysaika tai ajan määräytymiskriteerit. Rekisteröidylle on selkeästi ilmoitettava tämän oikeuksista sekä mahdollisuudesta peruuttaa suostumus ja tehdä valitus valvontaviranomaiselle käsittelytoimista. Riippuen siitä, onko tiedot kerätty suoraan rekisteröidyltä vai jostakin muusta lähteestä, tietojen antamiselle on erilaiset aikarajoitteet. (Yleinen tietosuoja-asetus 679/2016, 13-14 artikla.) Nämä tiedot on kätevintä ilmoittaa selosteessa käsittelytoimista.

Rekisteröidyllä on oikeus saada tietää, käsitteleekö yritys hänen henkilötietojaan ja mitä tietoja hänestä on kerätty. Henkilötietoja yritys ei ole velvollinen toimittamaan, jos sillä on haitallisia seuraamuksia muiden oikeuksiin tai vapauksiin, esimerkiksi jos tieto sisältää myös muiden henkilöiden henkilötietoja (Hanninen ym. 2017, 61). Rekisteröidyllä on oikeus oikaista tietojaan sekä poistaa tietonsa rekisteristä tietyin perustein. Tiedot tulee poistaa, mikäli henkilötietoja ei enää tarvita ilmoitettuun käyttötarkoitukseen tai rekisteröity peruuttaa suostumuksen käsittelyyn eikä muuta laillista perustetta käsittelylle ole. Tiedot on poistettava myös, mikäli henkilötietoja on käsitelty laittomasti tai rekisteröity vastustaa käsittelyä. (Yleinen tietosuoja-asetus 679/2016, 17 artikla.) Rekisteröityä ei saa johtaa harhaan väärällä tiedolla keräyksen tarkoituksesta, ja rekisterinpitäjän on otettava huomioon kaikki rekisteröidyn oikeuksille mahdollisesti aiheutuvat seuraukset (Information Comissioner’s Office www-sivut 2018

Muita rekisteröidyn oikeuksia ovat oikeus rajoittaa käsittelyä, siirtää omat tiedot toiseen järjestelmään, vastustamisoikeus sekä oikeus vastustaa automatisoitujen päätösten tekemistä esimerkiksi profiloinnin kautta. (Yleinen tietosuoja-asetus 679/2016, 18-22 artikla.)

3.6 Käyttötarkoitussidonnaisuus

Kun henkilötietoja suunnitellaan kerättäväksi, on aina ensin määritettävä tiedon käyttötarkoitus ja varmistuttava laillisen käsittelyperusteen olemassaolosta. Tietoja ei voi pääsääntöisesti käyttää myöhemmin muuhun käyttötarkoitukseen, ellei siihen ole saatu rekisteröidyn suostumusta tai

ellei siihen ole olemassa erikseen laissa määriteltyä perustetta. Käyttö muuhun kuin alkuperäiseen tarkoitukseen on mahdollista mm. silloin, jos toissijaisessa käsittelyssä toteutuu alkuperäisen keruun asiayhteys rekisteröidyn ja rekisterinpitäjän välisessä suhteessa tai käsittelyn tarkoitus. (Yleinen tietosuoja-asetus 679/2016, 5-6 artikla.) Asiakassuhde voi käsittää useita hyväksyttäviä käyttötarkoituksia kuten asiakassuhteen hoitaminen ja kehittäminen, tuotteiden markkinoiminen tai liiketoiminnan ja asiakaspalvelun kehittäminen (Elinkeinoelämän keskusliiton www-sivut 2020).

Kun yhteensopivia käyttötarkoituksia harkitaan riskiperusteisesti, ratkaisevaa on henkilötiedon arkaluonteisuus. Käsittely toiseen tarkoitukseen ei ole mahdollista, mikäli käyttötarkoitus muuttuu olennaisesti, jos käsittely on rekisteröidyn kannalta odottamatonta tai jos käsittelystä aiheutuu epäoikeudenmukaisia seurauksia rekisteröidylle. Uudesta käyttötarkoituksesta on ilmoitettava rekisteröidylle. Mikäli suostumus on vaadittu, on pyydettävä uusi suostumus ja rekisteröidylle on ilmoitettava uudesta käyttötarkoituksesta. (Tietosuojavaltuutetun www-sivut 2020.)

3.7 Tietojen ja säilytyksen minimointi sekä täsmällisyys

Rekisterinpitäjän määrittämä käyttötarkoitus rajaa käsiteltävän henkilötiedon laajuutta. Sellaista tietoa ei tule käsitellä, joka ei ole tarpeellista käyttötarkoituksen kannalta. Mitään henkilötietoa ei tule käsitellä vain varmuuden vuoksi. (Elinkeinoelämän keskusliiton www-sivut 2020.) Käsittelyn tarkoitus on pystyttävä siten täsmällisesti määrittelemään ja säilytysaika rajoitettava mahdollisimman lyhyeksi (Tietosuojavaltuutetun www-sivut 2020).

Minimointi liittyy säilytyksen rajoittamiseen. Kun henkilötietoa ei enää tarvita, se tulee poistaa. Yleinen sääntö on, että henkilötietoja tulee kerätä niin vähän kuin mahdollista, ja jokaiselle tiedolle tulee olla peruste. (Korpisasari ym. 2018, 94.) Esimerkiksi B-to-B yrityksen asiakasrekisterissä harvoin on tarvetta henkilön syntymäajalle. Sitä ei voida kerätä vain sen vuoksi, että muistaisi onnitella asiakasta syntymäpäivänä.

Ennen tietojen keräämistä on hyvä olla selvillä myös henkilötiedon elinkaari ja sen määräytymisperuste. Lähtökohtana on henkilötiedon käyttötarkoitus. Tietoja ei tule säilyttää kauempaa kuin sen käyttöön on perusteltu tarve. Säilytysajat on myös pystyttävä dokumentoimaan. Säilytyksen rajoittaminen linkittyy kiinteästi tiedon täsmällisyyteen. Jos esimerkiksi perusteltu tarve

liittyy asiakassuhteen hoitamiseen, sen loppuminen merkitsee myös henkilötiedon tarpeen loppumista. Siten henkilötiedon säilyttäminen asiakasrekisterissä on rajoitettu asiakassuhteen kestoon. (Tietosuojavaltuutetun www-sivut 2020.)

Kun henkilötietoja ei enää tarvita, ne pitää poistaa tai anonymisoida. Anonymisointi tarkoittaa, että tieto muutetaan sellaiseen muotoon, jossa siitä ei voida enää tunnistaa henkilöä edes tietoja yhdistelemällä. Tietosuojalainsäädäntö ei koske anonymisoitua tietoa. (Korpisasari ym. 2018, 61.)

Tietojen on oltava täsmällisiä ja ajantasaisia. Yrityksen on suoritettava kohtuullisin toimenpitein virheellisten ja epätarkkojen tietojen korjaaminen tai poistaminen (Yleinen tietosuoja-asetus 679/2016, 5d artikla). Ennen käsittelyä henkilörekisterin ylläpitämiselle on siten määritettävä menettelytavat eli miten tiedot pidetään ajan tasalla. Arkaluonteisen tiedon kuten terveystiedon, täsmällisyys on ensiarvoisen tärkeää, kun taas yritysasiakkaiden yhteystiedot ovat usein julkisia eivätkä kovin kriittisiä. Tässäkin suhteessa riskiperusteinen lähestymistapa auttaa yritystä arvioimaan henkilörekisterin päivittämistiheyttä. Kaikissa tilanteissa rekisterinpitäjällä on kuitenkin oltava tekniset ja organisatoriset edellytykset henkilötiedon täsmällisyyden varmistamiseksi säännönmukaisesti. (Tietosuojavaltuutetun www-sivut 2020.)

3.8 Eheys ja luottamuksellisuus

Tiedon eheys ja luottamuksellisuus liittyvät olennaisena osana tietoturvaa. Organisaation tietotekninen ympäristö sekä henkilötiedon käsittelyn menettelykäytännöt ovat oltava sellaisia, että tieto ei vahingossa tai tahallisesti häviä, muutu tai vahingoitu. Riskiperusteinen lähestymistapa merkitsee, että arkaluonteisen tiedon suojaamiseksi on oltava vahvemmat varmistukset kuin ei-arkaluonteisen tiedon käsittelyssä. Eheyteen ja luottamuksellisuuteen vaikutetaan ennen kaikkea teknisillä ja organisatorisilla keinoilla, kuten salasanoilla, tiedonkäsittelylaitteiden oikeanlaisella käytöllä, ohjeistuksilla ja käyttöoikeuksien rajoittamisella. (Korpisasari ym. 2018, 95.)

4 TIETOSUOJAN TOTEUTTAMINEN KÄYTÄNNÖN PROSESSEISSA

4.1 Nykytilan analyysi

Tutkimusprosessi alkoi tutustumalla lainsäädäntöön ja aiheeseen liittyvään tutkimusaineistoon. Tekijällä oli olemassa jonkinlainen käsitys organisaation nykytilasta, jolloin tutkimusaihe voitiin rajata ottaen huomioon kohdeyritys ja sen akuutit tarpeet. Suunnitelma esiteltiin johtoryhmässä, jossa esitetty etenemistapa hyväksyttiin.

Tietosuoja-asetuksen riskilähtöisyys merkitsee sitä, että organisaation toimenpiteet tietosuojan toteuttamiseksi perustuvat riskikartoitukseen (Tietosuojavaltuutetun toimiston www-sivut 2020). Kehitystyön lähtökohta olikin selvittää, miten, kuka ja miksi henkilötietoja nykyisissä prosesseissa käsitellään. Sitä varten laadittiin kyselylomake, joka testattiin aluksi kolmella käyttäjällä. Lomakekyselyn avulla selvitettiin mitä henkilötietoja henkilö käsittelee, missä järjestelmissä ja sijainneissa niitä on, mitä tarkoitusta varten tietoja kerätään, mistä niitä hankitaan ja miten tietosuojasta varmistutaan.

Kysely suoritettiin Select Survey.NET palvelun avulla. Palvelu on konsernin tarjoama työkalu. Kysely lähetettiin kaikille organisaatiossa sähköpostin omaaville, joita on yhteensä 19 kpl. Kyselyyn vastasi määräaikaan mennessä 15 henkilöä. Kyselyn alussa selvitettiin kyselyn tarkoitus, määriteltiin käytettävät termit henkilötieto, henkilötietojen käsittely sekä henkilörekisteri. Lomakkeen alussa määriteltiin käsitteet henkilötieto, henkilötietojen käsittely sekä henkilörekisteri. Määrittelyillä pyrittiin varmistamaan, että vastaaja ymmärtää kysymykset oikein. Monivalintakysymykset koskivat tietosuojaperiaatteista käyttötarkoitussidonnaisuutta, tietojen minimointia, säilytysaikaa sekä täsmällisyyttä. (Liite 1.)

Suuri osa vastaajista ilmoitti tallentavansa henkilötietoja tietokoneelle, kannettaviin laitteisiin verkkosijaintiin sekä sähköpostin kontakteihin. Osa ilmoitti tallentavansa tietoja myös SAP toiminnanohjausjärjestelmään. Kahdeksan käyttäjää ilmoitti tallentavansa tietoja myös paperisiin arkistoihin. Tämä käytännössä tarkoittanee erilaisten muistikirjojen käyttöä myyntityössä. Myös työntekijöiden henkilötietoja säilytetään erilaisissa dokumenteissa kuten työsopimuskopioissa ja kehityskeskustelulomakkeissa. Henkilötietojen käyttötilanne liittyy esimiestyön lisäksi yleensä asiakkaiden kontaktointiin ja tilauskäsittelyyn sekä toimittajakontaktointiin.

Suurin osa vastaajista käsittelee ainoastaan nimeä, osoitetta, puhelinnumeroa ja sähköpostiosoitetta. Muutama vastaaja ilmoitti käsittelevänsä myös kotiosoitetta. Syntymäajan ja sosiaaliturvatunnuksen käsitteleminen liittyvät yleensä esimiesten työtehtäviin. Tosin myös myynnissä yksi vastaaja ilmoitti käsittelevänsä syntymäaikaa. Tämä vahvistaa olettamusta, että henkilötietojen laillinen käsittely ei ole täysin omaksuttu organisaatiossa.

B-to-B yritykselle tavanomainen tapa on kerätä henkilötietoja julkisista lähteistä kuten verkkosivuilta ja suunnata markkinointia ns. asemavaltuutuksen perusteella. Nykyinen lainsäädäntö mahdollistaa edelleen suoramarkkinoinnin oikeutetun edun turvin. Yhtä yleisesti henkilöstö kerää tietoja suoraan henkilöltä itseltään. Ostettuja henkilörekistereitä ei käytetä muutoin kuin satunnaisia markkinointikampanjoita varten.

Tietojen ajantasaisuus ja oikeellisuus tulee tarkistettua siinä yhteydessä, kun henkilöä kontaktoidaan. Yleisesti tämä tapahtuu asiakastietojen osalta hinnastojen postituksen yhteydessä kerran vuodessa. Tällöin jokainen myyjä tarkistaa omat yhteystietonsa. Kaksi vastaajaa ilmoitti, että tiedon oikeellisuudesta ei voi varmistua kovinkaan helposti. Tietoturvan edellytykset on organisaatiossa tiedostettu hyvin. Tietokoneen lukitus, päivitykset ja salasanojen käyttö ovat yleisimmät tavat suojata tietoja. Konsernin SFTP (SSH suojattu tiedonsiirto) palvelun käyttö henkilötietoja sisältävien aineistojen lähettämisessä on myös hyvin tiedostettu.

Syvempää analyysiä varten suoritettiin teemahaastattelu myynnin, oston ja hallinnon edustajille. Sen tarkoituksena oli keskustella syvemmin henkilötiedon käsittelyyn liittyvästä problematiikasta käytännön työssä sekä tunnustella, mitä erityisiä kehittämistarpeita organisaatiossa on. (Liite 2.)

Myyntihenkilöstö käsittelee myyntitilauksiin, asiakaspalautuksin, reklamaatioihin ja tiedusteluihin liittyviä työtehtäviä. Henkilötietoja käsitellään yhteydenottotarkoituksissa. Toiminnanohjausjärjestelmässä henkilötietoja ei systemaattisesti tallenneta sille erityisesti varattuun kenttään, vaan tiedot ovat hajallaan ja palvelevat lähinnä tavaran toimittamista. Asiakaspalvelija oli sitä mieltä, että SAPista ei tietoja saa helposti systemaattisesti edes ulos. Yhtenäinen ja jäsennelty asiakasrekisteri on olemassa ainoastaan excel-tiedostona ja se toimii lähinnä postitusrekisterinä hinnastojen ja asiakastiedotteiden lähettämistä varten niin kauan, kuin asiakkuudenhallintajärjestelmä (CRM, customer relationship management) ei ole käytössä.

Asiakaspalvelu- ja myyntityössä henkilötiedon käsittelytarkoitus on pääosin selkeä, sillä tietoja käsitellään myyntitapahtuman suorittamiseksi asianmukaisesti. Asiakastietoja ei ole tarpeen kerätä laajasti, eikä niitä säilytetä muutoin kuin asiakkuuden ajan. Markkinointirekisterin suhteen on ongelmallista sen hajautuneisuus. Tietoja on eri käyttäjien järjestelmissä ja excel-tiedostoissa. Kaikille ei myöskään ole täysin selvää, mitä tietoja asiakkaasta voidaan tallentaa. Toisaalta kun tiedot ovat julkisista lähteistä saatavia, niiden ei nähdä sisältävän yleensäkään suurta riskiä. Haastatteluissa kävi myös ilmi, että tietosuojaan liittyvien periaatteiden tuntemus on jokseenkin epäselvää. Esimerkiksi tietojen täsmällisyyden ei aina nähty liittyvän tietosuojaan.

Esimiehet käsittelevät alaistensa henkilötietoja HR-järjestelmässä. Työsopimuksien kopioita säilytetään organisaatiossa yhden henkilö toimesta. Kaikki henkilötietoja sisältävät digitaaliset aineistot sijaitsevat käyttäjän omalla tietokoneella tai verkkosijainnissa, johon ei ole muilla pääsyä.

Henkilöstö luottaa yrityksen tietoturvaan ja yleensä järjestelmien suojaukseen, eikä tietojen katoamista tai tietomurtoa nähty realistisena skenaariona. Myös omaan osaamiseen laitteiden ja järjestelmien tietoturvallisuuden mahdollistajana luotettiin yleisesti ottaen paljon.

Kyselyn ja haastattelujen perusteella voitiin todeta, että suurin riski henkilötietojen käsittelyssä muodostuu tällä hetkellä siitä, että oikeanlaista järjestelmää ylläpitää asiakas- ja markkinointirekisteriä ei ole. Tästä johtuen tietoja säilytetään hajanaisesti eri henkilöiden toimesta, eikä ajantasaisuudesta ole aina varmuutta. Lisäksi tiedostoista on olemassa useita kopioita, jolloin niitä ei pysty hallitsemaan vaatimusten mukaisesti. Myös säilytysaika on määrittämätön. Koska käsiteltävät henkilötiedot ovat suppeita ja ne ovat yleensä julkisista lähteistä saatavia yrityskohtaisia henkilötietoja, ei henkilötiedon tietosuojariskiä nähdä kovinkaan suurena.

4.2 Osoitusvelvollisuus dokumentoinnissa ja menettelyissä

Dokumentoinnin suunnittelua ja laatimista varten perustettiin Microsoft Teams-ryhmä, jonka tarkoituksena oli muokata yhteisiä dokumentteja, keskustella aiheesta sekä järjestää palavereja. Työkalu osoittautui tehokkaaksi, sillä henkilöt eivät istu samassa konttorissa ja lisäksi suuri osa työskenteli etänä. Projektiryhmään kuului controller, liiketoimintajohtaja, edustajat myynnistä sekä tuotannosta. Tuotantopäällikkö on myös paikallinen tietojärjestelmäasioiden yhteyshenkilö.

4.2.1 Oikeutetun edun tasapainotesti

Yrityksessä pääasiallinen laillinen käsittelyperuste on sopimus. Toisena käsittelyperusteena käytetään oikeutettua etua, jota sovelletaan markkinointitoimissa. Jotta oikeutettua etua voisi perustellusti käyttää, on suoritettava tasapainotesti, jossa arvioidaan seikkaperäisesti henkilötiedon käsittelyn tarpeellisuus ja rekisteröidylle aiheutuva riski. Tasapainotesti laadittiin varmistamaan perusteen olemassaolo. Kirjallinen dokumentointi liitettiin osaksi tietosuojadokumentointia tietotilinpäätöksen liitteeksi.

Dokumentin laatimiseen käytettiin Tietosuojavaltuutetun toimiston www-sivuilla olevaa testiä. Testin avulla voidaan varmistua siitä, että oikeutettu etu on oikea käsittelyperuste. Rekisterinpitäjän tulee varmistua mm. käsittelyn tosiallisista vaikutuksista rekisteröidyn oikeuksiin, käsittelyn välttämättömyydestä käsittelyn tavoitteen saavuttamiseksi sekä tarvittavien organisatoristen ja teknisten toimenpiteiden riittävyydestä henkilön oikeuksien suojaamiseksi. (Tietosuojavaltuutetun www-sivut 2020.) Dokumentissa kuvattiin yrityksen henkilötietorekistereiden sisällöllistä ja määrällistä laajuutta. Lisäksi kuvattiin henkilötiedon käyttöympäristöä ja rekisteröidyn oikeutettua oletusta käsittelyn laadusta.

4.2.2 Tietotilinpäätös

Tietotilinpäätöksen (liite 3) tarkoituksena on kuvata tietosuojan nykytila sekä tehdä tarvittavat suunnitelmat kehittämistoimenpiteille. Tietotilinpäätös on tärkeä osa osoitusvelvollisuuden toteuttamista sekä riskinhallintaa. Sen keskeinen tehtävä on tunnistaa organisaation tietovirrat sekä niiden riskitaso. Tietotilinpäätös asettuu aiemmin mainitussa kolmiportaisessa osoitusvelvollisuudessa menettelyjen tasolle. Siinä luodaan edellytykset käytännön toimille, joita puolestaan voidaan esimerkiksi sisäisten ja ulkoisten auditointien avulla seurata ja todentaa. Jotta menettelyohjeet ja käytänteet voidaan luoda, on yrityksen johdon sitouduttava tietosuojan edistämiseen. Siksi olisi hyvä kirjata tietosuoja yhdeksi yrityksen tavoitteista.

Tietotilinpäätöksen pohjana on käytetty tietosuojavaltuutetun toimiston www-sivuilla julkaistua ohjetta (Tietosuojavaltuutetun toimiston www-sivut 2020) ja sitä on mukailtu yrityksen tarpeisiin. Vinkkejä on haettu myös muiden organisaatioiden vastaavista dokumenteista. Tavoitteena oli luoda dokumentti, joka välittäisi olennaisen tiedon yrityksen tietovarannoista ja henkilötietojen organisatorisista perusteista. Tietojärjestelmien kuvaus haluttiin sisällyttää myös dokumenttiin, sillä tekniset järjestelmät ja niiden suojaus ovat olennainen osa tietosuojan toteutumista.

Tietotilinpäätöksessä kuvattiin organisaation tietojärjestelmäarkkitehtuuri ja tietosuojan nykytila. Tietoturvan kannalta tärkeää oli myös kuvata keskeisimmät tietovarannot eli loogisesti yhteen kuuluvat tietojoukot esimerkiksi asiakasrekisteri tai myyntitilaukset. Koska yrityksessä oli meneillään myös dokumentinhallintaprojekti, hyödytti tietovarantojen analysointi samalla erilaisten dokumenttien luokitteluja ja määrittelyjä. Dokumentissa kuvattiin jokainen henkilötietorekisteri ja niiden tietosisällöt. Olennaista oli kuvata kunkin rekisterin kohdalla tietosuojaperiaatteiden toteuttaminen eli mikä on henkilörekisterin laillinen käsittelyperuste, miten tietojen ja säilytyksen minimointi, läpinäkyvyys, täsmällisyys, eheys ja luottamuksellisuus on toteutettu.

Dokumenttiin oli myös kirjattu tiedot yhtiön tietosuojaorganisaatiosta yhteystietoineen. Tietotilinpäätöksen liitteenä on oikeutetun edun kuusiportainen tasapainotesti osoittamaan, että peruste on olemassa ja se on testattu. Liitteenä on myös tietosuojan koulutusrekisteri, johon kerätään henkilöstön käymät koulutukset yksityiskohtineen.

Omasta organisaatiosta nimettiin henkilö, joka toimii tietosuojakoordinaattorina. Hän ei ole asetuksessa mainittu tietosuojavastaava, koska sellainen on jo Suomen yhtiöiden tasolla. Koordinaattorin tehtävänään on hankkia itselleen tietoa ja kouluttaa muuta organisaatiota sekä neuvoa työntekijöitä yksittäisissä tietosuojaan liittyvissä kysymyksissä. Koordinaattori valittiin myynnin tiimistä, sillä tuleva CRM-projekti edellyttää panostusta juuri myynniltä. Koordinaattoriksi valittu henkilö on mukana CRM-projektissa, joten tehtävä nivoutui hyvin myös kyseiseen kehitysprojektiin.

4.2.3 Koulutukset

Organisaatiossa ei tietosuojaan ole kiinnitetty tarvittavaa huomiota ja tietämys oli ennakkokyselyjen perusteella puutteellista. Siksi jokainen tietojärjestelmiä käyttävä työntekijä edellytettiin

katsovan muistutukseksi Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) toteuttaman Arjen tietosuoja –videon ja tekemään siihen liittyvän nettitestin. Jokaisen piti myös kuitata video katsotuksi ja testi tehdyksi, jolloin saatiin ensimmäiset kirjaukset koulutusrekisteriin. Myyntihenkilökunnan säännöllisissä myyntipalavereissa otetaan yhdeksi kestoaiheeksi tietosuoja. Tietosuojakoordinaattori tuo esille käytännön asioita helposti ymmärrettävässä muodossa. Tarkoituksena on pitää aihetta säännöllisesti esillä.

Koulutukseen tartuttiin hyvin ja nettitestin suorittaneita oli jo koulutuksen lanseerausta seuranneena viikkona useita. Tietosuoja-asiaan suhtauduttiin positiivisesti ja sen tärkeys ymmärrettiin hyvin. Koulutuksen tueksi laadittiin PowerPoint esitys, jossa esitetään olennaiset lainsäädännölliset asiat sekä niiden merkitys käytännön työssä. (Liite 6)

4.2.4 Ohjeistukset ja menetelmäohjeet

Kyselyn, haastattelujen ja keskustelujen perusteella voitiin todeta, että tietosuojan toteuttamisessa pelkästään tiedon lisäämisellä voidaan saada parannusta aikaan. Useimmat puutteet koskivat tiedon epäsystemaattista ja sekavaa arkistointia ja käsittelyä. Prosessin aikana henkilöstö alkoi siivota omia tiedostojaan turhista ja vanhentuneista henkilötietorekistereistä. Niitä on kerääntynyt mm. erilaisten asiakaspostitusten yhteydessä.

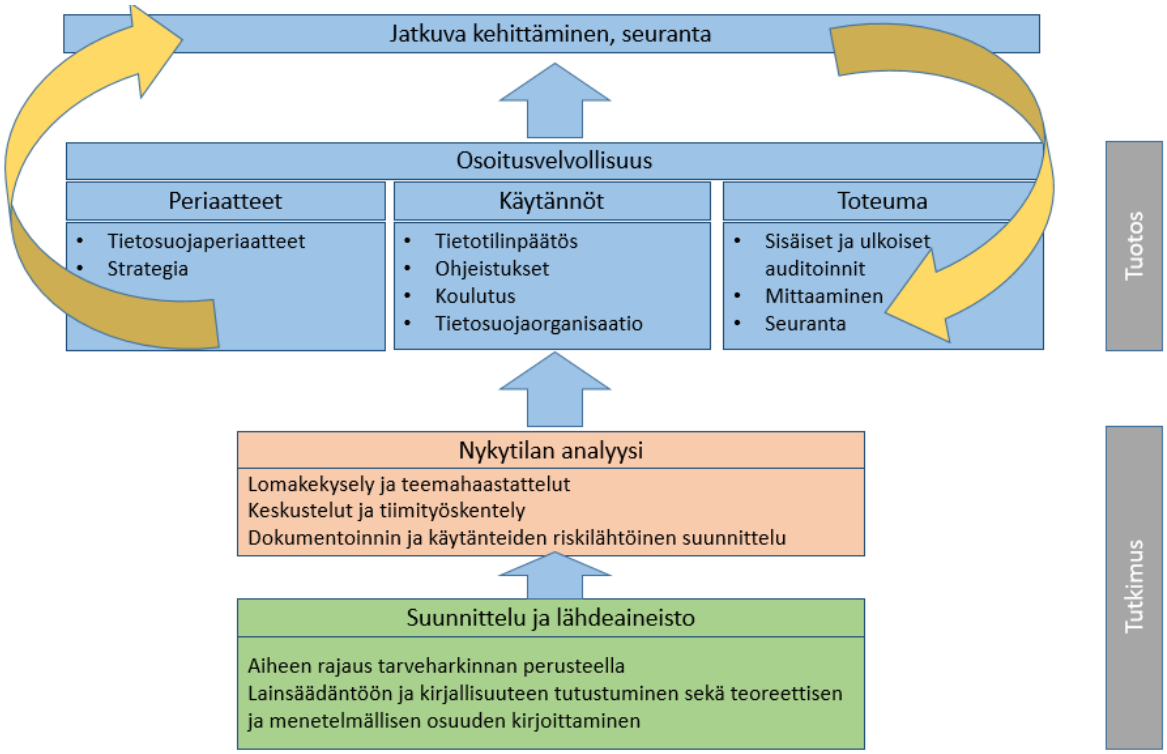
Myynnin, markkinoinnin ja oston henkilörekistereistä luotiin yksityiskohtainen ohje, jossa jokainen tietosuojaperiaate purettiin käytännön toimintaohjeeksi (liite 5). Ohjeen laatiminen osoittautui haastavaksi tehtäväksi, koska juuri siinä mitattiin normin ymmärtäminen ja soveltaminen käytäntöön. Eniten vaikeuksia aiheutti säilytysajan määrittäminen nykyisillä vajavaisilla hallintavälineillä. Henkilötietojen ajan tasalla pitäminen on myös tyypillinen ongelma. Henkilötiedon säilyttämisestä eri sijainneissa sekä niiden päivityksestä annettiin mahdollisimman tarkkoja ohjeita. Henkilötiedon laajuus on sidottu käyttötarkoitukseen. Lähinnä asiakkaiden ja muiden sidosryhmien kontaktoimiseen riittää yhteystiedot, eikä mitään muuta tietoa tule tallentaa. Ohjeeseen oli koottu lisäksi tiedot tietosuojaan ja -turvaan liittyvien oheismateriaalien sijainnista, tietosuojaorganisaatiosta sekä menettelystä tietoturvaloukkauksen sattuessa.

4.3 Osoitusvelvollisuus toimintaperiaatteissa ja toteumassa

Tietosuojan toteutuminen on johdon vastuulla. Ilman johdon sitoutumista ei tietosuoja voi toteutua organisaatiossa. Jotta johdon sitoutuminen voidaan osoittaa, tulisi se kirjata johdon dokumentaatioon. Parhaimmassa tapauksessa tietosuoja ja tietoturva olisi nostettu yrityksen yhdeksi strategiseksi tavoitteeksi. Johtoryhmässä päätettiin ottaa tietotilinpäätöksen käsittely agendalle. Se päivitetään vuosittain ja samalla käsitellään tarvittavat kehitystoimenpiteet. Lisäksi käsitellään edellisen vuoden tietosuojaan liittyvät tapahtumat esimerkiksi koulutukset ja muut olennaiset tietosuojaan liittyvät kysymykset.

Tietosuoja on jatkossa ”arkipäiväistettävä” yrityksen käytännöissä. Tätä termiä Yritys Akatemia käytti markkinoidessaan tietosuojakoulutusta kesäkuussa 2020. (YritysAkatemian www-sivut 2020.) Arkipäiväistäminen edellyttää johdolta johdonmukaista tietosuojan agendalla pitämistä ja jalkauttamista koko organisaatioon. Kun yrityksen sisäiset toimintatavat on juurrutettu sekä johdon että koko organisaation toimintaa ohjaaviksi käytännöiksi, voidaan ne ottaa mukaan sisäisen auditoinnin piiriin. Mittaamisella ja seurannalla voidaan todentaa tietosuojan toteutumista. Erilaisia tunnuslukuja voivat olla järjestetyt koulutukset, auditoinnit ja erilaiset logitiedot tietopyynnöistä.

Alla olevassa kuviossa on yhdistetty opinnäytetyöprosessin kulku sekä yrityksen tietosuojatyön kehittäminen. Dokumentaation ja käytänteiden luomisen jälkeen on luotava edellytykset jatkuvalle parantamiselle. Tietosuojan toteutuminen on pystyttävä todentamaan tunnusluvuin ja auditointien avulla.



Kuva 3. Opinnäytetyöprosessi ja organisaation tehtävät tietosuojan kehittämiseksi

5 YHTEENVETO JA POHDINNAT

Tässä toiminnallisessa opinnäytetyössä selvitettiin yrityksen tietosuojan nykytila taustaksi kehitystyölle. Koska tutkija on toiminut useita vuosia kohdeyrityksessä, oli jo ennen tutkimuksen alkua syntynyt käsitys siitä, että yleisen tietosuoja-asetuksen osoitusvelvollisuus ei täysin toteutunut. Siksi tavoitteena oli luoda menettelyt ja dokumentaatio, jolla nämä puutteet voitiin korjata.

Kyselylomakkeen avulla selvitettiin, mitä henkilötietoja, miten ja missä järjestelmissä henkilöstö niitä käsittelee. Voitiin todeta, että käsittely on melko suppeaa, sillä henkilötiedot koostuvat pääasiassa asiakkaiden ja muiden sidosryhmien julkisista yhteystiedoista. Yrityksen toiminta kunnallis- ja kiinteistöteknisten järjestelmien tavarantoimittajana oli perusteena riskiperusteiselle lähestymistavalle, koska henkilötiedon käsittelyn riskitaso on melko alhainen. Teemahaastattelujen avulla syvennettiin taustoittavaa tietoa henkilöstön henkilötiedon käsittelyn tietämystasosta. Haastattelut tukivat ennakko-oletusta siitä, että henkilötietojen käsittelyn problematiikka ei juurikaan ole tullut työssä vastaan.

Osoitusvelvollisuuden hahmottamisessa auttoi Bennetin hahmottelema kolmitasoinen malli, jossa osoitusvelvollisuus toteutuu periaatteiden, käytäntöjen sekä toteuman tasolla. Tämän työn varsinainen tuotos muodostui käytännön tasosta, johon kuuluvat tietotilinpäätös, menetelmäohjeet, koulutusmateriaali ja muu tukimateriaali. Osoitusvelvollisuus on yksi uusista tietosuojaperiaatteista, jota oikeusoppineet sekä tietosuojaviranomaiset ovat ohjeistaneet viime vuosina ahkerasti. Monille yrityksille juuri osoitusvelvollisuus on aiheuttanut päänvaivaa, sillä pelkkä muodollinen lain vaatimusten täyttäminen esimerkiksi tietosuojaselosteen muodossa ei enää riitä.

Työn keskeisin tuotos oli tietotilinpäätös. Se päätettiin luoda siksi, että yhteen dokumenttiin voitiin kerätä kaikki tietosuojaan ja –turvaan liittyvät keskeiset asiakokonaisuudet. Se toimi samalla nykytilan kuvauksena ja antoi pohjan jatkuvalle kehittämiselle. Dokumentti toimii myös sisäisenä ohjeistuksena ja tiedonlähteenä. Tietotilinpäätös on joka vuosi päivitettävä dokumentti tilinpäätökselle ominaiseen tapaan.

Tutkimustyölle asetetut vaatimukset toteutuivat tekijän näkökulmasta hyvin, sillä tarvittava dokumentaatio ja toimintasuunnitelmat jatkuvalle kehitykselle pystyttiin laatimaan. Kohdeyritys voi hyödyntää materiaalia suoraan tietosuojaperiaatteiden noudattamisen osoituksena ja ne toimivat hyvänä pohjana jatkokehitykselle. Lisäksi CRM-järjestelmän käyttöönotossa toteutettu materiaali toimii hyvänä perustana laatia yksityiskohtaiset ohjeistukset henkilötiedon käsittelylle. Prosessin aikana tapahtui ryhmän keskuudessa oppimista ja oivaltamista, joka oli yksi työn tavoite. Kehitysryhmän keskuudessa syntyi keskustelua konkreettisista toimista, joita uusi lainsäädäntö edellyttää. Prosessi täytti osallistavan toimintatutkimuksen periaatteen, jossa keskeinen osa kehitystyötä tapahtuu jo prosessin aikana.

Opinnäytetyön teoreettisen ja menetelmällisen osuuden koostaminen oli haasteellista, sillä oletuksena oli, että oikeudellinen aihe vaatisi oikeustieteellistä lähestymistapaa. Ammattikorkeakoulun käytännönläheisyyden vaatimus ei aluksi tuntunut olevan helppo liittää teoreettiseen viitekehykseen. Käytetty laintulkinta oikeustieteen metodina ei täytä tieteellisiä kriteereitä, mutta olennaista työssä olikin tutustua lainsäädäntöön ja tuottaa sen perusteella tarvittavaa dokumentointia ja käytänteitä. Tutkija onkin tyytyväinen lopputuloksen, jossa lainsäädännön vaatimukset pystyttiin taivuttamaan konkretiaksi. Tavoite kirjata yrityksen tietosuojan periaatteet, menettelyohjeet ja käytänteet saavutettiin. Kuten eräs myyntihenkilö totesi, kovinkaan paljon ei tarvitse

käytäntöjään muuttaa, vaan kyse on pikemminkin tietosuojan tärkeyden tiedostamisesta ja sisäistämisestä.

Työn lähtökohtana oli aiheen tärkeys yrityksen kannalta. Näin selkeän puutteen yrityksen toimissa tietosuojan toteuttamiseksi ja siksi valitsin juuri tämän lähestymistavan. Ymmärsin, että tietosuojan merkitystä ei oltu juurikaan tiedostettu eikä toteutuksen puutetta pidetty merkittävänä haittana yrityksen toiminnalle. Siksi selkeän suunnitelman esittäminen perusteluineen oli tärkeää työn hyväksymisen ja toteuttamisen kannalta. Koska olin ainoa asiaan lähemmin perehtynyt henkilö, oli luonnollista, että suunnittelin tarvittavat dokumentit ja toimenpiteet. Niiden perusteella oli helpompaa lähteä hiomaan yksityiskohtia ja yleensä keskustelemaan aiheesta. Vaikka tietoperustan kokoaminen jäikin minun vastuulle, oli tärkeää, että projektiryhmä ymmärsi juridiset perusteet kehitystyölle ja oli valmis jalkauttamaan tietosuojaa käytänteisiin.

Haasteellisimmaksi tutkimuksen aikana osoittautui oman tutkijanroolin ylläpitäminen kehitystyön aikana. Pitkäaikainen työskentely organisaatiossa asetti niin ikään kehittämistyölle ennakko-odotuksia. Oli tärkeää muistaa, että omat ajatukset voivat olla pohjana tutkimukselle, mutta tiedon hankinta ja prosessointi on suoritettava tieteellisin menetelmin ja pystyttävä perustelemaan valinnat. Kohdeorganisaatiossa henkilötietojen käsittely on suppeaa ja melko riskitöntä varsinaisessa operatiivisessa toiminnassa. Tämä osoittautui ennakko-odotusteni mukaisesti yhdeksi motivaatiota heikentäväksi tekijäksi. Siksi tärkeäksi argumentiksi muodostuikin se, että huolimatta riskittömyydestä lainsäädännön vaatimukset tulee täyttää. Koulutusmateriaalin laadinnassa oli otettava huomioon käytännönläheisyys eli mitä konkreettisia asioita on otettava huomioon henkilötietoja käsiteltäessä.

Työssä toiminnallisuus toi esiin osoitusvelvollisuuden ja tietosuojaperiaatteiden käytännön toteuttamisen ja normin tulkinnan problematiikan. Mikäli olisi tyydytty vain asetuksen normien luettelemiseen ja kuvailemiseen, oltaisiin saatu vain pinnallinen kuva yritykselle muodostuvista haasteista, mutta niiden käytännön ratkaiseminen olisi jäänyt tekemättä.

Työ tietosuojan juurruttamiseksi jokapäiväiseen toimintakulttuuriin on nyt edessä. Kehitystyö tuki myös dokumentinhallintaprojektia, jossa dokumentteja luokitellaan ja järjestetään niiden luottamuksellisuuden mukaisesti. Tietosuojan merkitys tulee korostumaan, kun siirrytään uuteen CRM-järjestelmään. Silloin on etua nyt tehdystä perustyöstä ja huolellisesti tehdyistä määrittelyistä.

LÄHTEET

Aalto-Setälä, M. & Honkasalo, P. Uusi tietosuoja-asetus tulee – oletko valmis? Kauppakamarin koulutustilaisuus Raumalla 21.9.2017.

Alapuranen, L., Lehtonen, L., Koskinen, S. & Wiberg, M. 2020. Henkilötietojen käsittely työelämässä. 3., uud. p. Helsinki: Edita.

Alasuutari, P. 2011. Laadullinen tutkimus 2.0. 4. uud. p. Tampere: Vastapaino.

Article 29 Data protection working party. 2010. Opinion 3/2010 on the principle of accountability. Viitattu 8.5.2020. https://www.dataprotection.ro/servlet/ViewDocument?id=654

Article 29 Data protection Working Party. 2014. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Viitattu 2.6.2018. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Article 29 Data protection Working Party. 2018. Guidelines on transparency under Regulation 2016/679. Viitattu 31.5.2018. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Bartolini, C., Muthuri, R., & Santos, C. 2015. Using Ontologies to Model Data Protection Requirements in Workflows. Viitattu 4.3.2018. https://orbilu.uni.lu/bitstream/10993/22383/1/main.pdf

Bennett, C. 2010. International privacy standards: can accountability be adequate? Draft for Privacy Laws and Business International. University of Victoria. Viitattu 10.5.2020. https://www.colinbennett.ca/Recent%20publications/PrivacyLawsand%20BusinessAugust2010.pdf

Blanchard, S. 2016. The General Data Protection Regulation(GDPR). A practical guide for businesses. Viitattu 30.5.2018. https://cdn2.hubspot.net/hubfs/329382/_files/GDPR_eBook_-_Blue_Sheep.pdf

Elinkeinoelämän keskusliiton www-sivut 2020. Viitattu 3.5.2020. https://ek.fi/en/

Eriksson, D. 2019. The GDPR's lawful basis of legitimate interest. Advice and review regarding the balancing operation as of GDPR Article 6.1 (f). Master thesis in European Union Law 30 ECTS. Uppsala University. Viitattu 29.4.2020. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1319557&dswid=866

Eskola, J., Lätti, J. & Vastamäki, J. 2018. Teemahaastattelu: lyhyt selviytymisopas. Teoksessa Valli, R. & Aarnos, E. Ikkunoita tutkimusmetodeihin: 1, Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. 5.uud.p. Jyväskylä: PS-kustannus. Viitattu 23.5.2020. Ebrary-sovellus iPadissa.

EUR-Lex www-sivut 2020. Viitattu 22.5.2020. https://eur-lex.europa.eu/homepage.html

Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus), 27.4.2016, 2016/679/EU, EUVL L 119, 4.5.2016.

Euroopan tietosuojaneuvoston www-sivut 2020. Viitattu 4.5.2020. https://edpb.europa.eu/edpb_fi

Euroopan Unionin tuomioistuin. 2018. Ennakkoratkaisu asiassa C-25/17. Viitattu 20.5.2020. http://curia.europa.eu/juris/

Grundstrom, C, Väyrynen, K., Iivari, N. & Isomursu, M. 2019. Making sense of the general data protection regulation – Four categories of personal data access challenges. Viitattu 29.4.2020. https://scholarspace.manoa.hawaii.edu/handle/10125/59941

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

Heikkinen, H.L.T. 2018. Toimintatutkimus: kun käytäntö ja tutkimus kohtaavat. Teoksessa Valli, R. & Aarnos, E. Ikkunoita tutkimusmetodeihin: 1, Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. 5.uud.p. Jyväskylä: PS-kustannus. Viitattu 23.5.2020. Ebrary-sovellus iPadissa.

Henriksson, C. 2017. Tietosuojan perusteet haltuun. KPMG:n webinaari 28.9.2017.

Hirvonen, Ari. 2011. Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Helsinki. Helsingin yliopisto. Oikeustieteellinen tiedekunta. Viitattu 22.4.2020. https://www.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf

Hirsjärvi, S., Remes, P., & Sajavaara, P. 2007. Tutki ja kirjoita. Helsinki: Kustannusosakeyhtiö Tammi.

HE 9/2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

Information Comissioner's Office www-sivut 2020 Viitattu 22.4.2020. http://www.ico.org.uk

Kananen, J. 2014. Toimintatutkimus kehittämistutkimuksen muotona: Miten kirjoitan toimintatutkimuksen opinnäytetyönä? Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kolehmainen, A. 2016. Tutkimusongelma ja metodi lainopillisessa työssä. Teoksessa Miettinen T. (toim.). Oikeustieteellinen opinnäyte - Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvosteluista. Edilex Edita Publishing Oy. Viitattu 2.5.2020. http://www.edilex.fi/

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

Lindroos-Hovinheimo, S. 2018. Henkilötietojen suoja EU-oikeudessa – yksityisyyttä yhteisön kustannuksella. Lakimies 1/2018. 52-75.

Neuvonen, R. 2019. Viestintä- ja informaatio-oikeuden perusteet. Helsinki: Kauppakamari.

Oikeusministeriö. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Selvityksiä ja ohjeita 4/2017. Viitattu 24.9.2017. https://tietosuoja.fi/documents/6927448/9666681/Miten+valmistautua+tietosuoja-asetukseen/8c5b9a96-a8ce-4c91-ad06-6e36130bd0e5/Miten+valmistautua+tietosuoja-asetukseen.pdf

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

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV – Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 17.4.2020. https://www.fsd.tuni.fi/menetelmaopetus

Salonen, K. 2013. Näkökulmia tutkimukselliseen ja toiminnalliseen opinnäytetyöhön: Opas opiskelijoille, opettajille ja TKI-henkilöstölle. Turku: Turun ammattikorkeakoulu. Viitattu 10.5.2020. http://julkaisut.turkuamk.fi/isbn9789522163738.pdf

Samk Finna www-sivut 2020. Viitattu 8.5.2020. https://samk.finna.fi/

Tietosuojavaltuutetun toimiston www-sivut 2020. Viitattu 3.5.2020. http://www.tietosuoja.fi

Tietosuojavaltuutetun toimisto. 12.7.2017 1081/41/2017, Finlex

Toikko, T. & Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta. Näkökulmia kehittämisprosessiin, osallistamiseen ja tiedontuotantoon. Tampere: Tampereen Yliopistopaino Oy – Juvenes Print. Viitattu 25.5.2020. https://trepo.tuni.fi/bitstream/handle/10024/100802/Toikko_Rantanen_Tutkimuksellinen_kehittamistoiminta.pdf?sequence=1&isAllowed=y

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uud.p. Helsinki: Kustannusosakeyhtiö Tammi.

Vainio, S. 2018. Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa. Viestintä- ja informaatio-oikeuden pro gradu –tutkielma. Helsingin yliopisto. Oikeustieteellinen tiedekunta. Viitattu 8.5.2020. https://helda.helsinki.fi/bitstream/handle/10138/232856/Vainio%20Sonja%20pro%20gradu%20Rekisterinpit%C3%A4j%C3%A4n%20osoitusvelvollisuus%20EUn%20yleisess%C3%A4%20tietosuoja-asetuksessa.pdf?sequence=2&isAllowed=y

Valtionvarainministeriö. 2016. Vahti-ohje. Rekisterinpitäjän velvollisuudet. Viitattu 2.6.2018. https://www.vahtiohje.fi/web/guest/rekisterinpitajan-velvollisuudet

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

Vilkka, H. 2015. Tutki ja kehitä. 4. uud. p. Jyväskylä: PS-kustannus.

Voutilainen, T. 2012. Oikeus tietoon – informaatio-oikeuden perusteet. Helsinki: Edita.

Voutilainen, T. 2019. Oikeus tietoon – informaatio-oikeuden perusteet. Helsinki: Edita Publishing Oy.

LIITE 1

Kysely henkilötiedon käsittelystä työssä

Tämä kysely liittyy Satakunnan ammattikorkeakoululle tehtävään opinnäytetyöhön, jossa on tarkoituksena tutkia työntekijöiden henkilötietojen käsittelyn nykytilaa ja tehdä käytännönläheinen ohjeistus lainmukaisesta henkilötiedon käsittelystä.

EU:n yleinen tietosuoja-asetus astui voimaan toukokuussa 2018. Sen mukaan yrityksen on pystyttävä osoittamaan, että se noudattaa asetuksessa mainittuja tietosuojaperiaatteita henkilötiedon käsittelyssä.

Henkilötietoja ovat kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot mm. henkilön
- Nimi
- Henkilötunnus ja syntymäaika
- Verkkotunnistetieto
- Postiosoite
- Sähköpostiosoite (muotoa etunimi.sukunimi@yritys.fi)

Henkilötietojen käsittelyä ovat mm. kerääminen, järjestäminen, säilyttäminen, muokkaaminen, haku, käyttö, poistaminen eli kaikenlainen manuaalinen tai sähköisesti tapahtuva käsittely.

Henkilörekisteri on henkilötietoja sisältävä tietojoukko, jota käsitellään kokonaan tai osittain automaattisesti ja josta tiedot löytyvät helposti. Samaan käyttötarkoitukseen kuuluvat rekisterinosat kuuluvat samaan rekisteriin. Esim. asiakasrekisteri voi olla sähköpostiosoitteistossa, SAP:issa ja erillisessä excel-tiedostossa.

Tämä kysely on olennainen lähtökohta kehitystyölle ja siksi jokainen vastaus on tärkeä. Vastaathan 6.5. mennessä.

Kiitos vastauksestasi!

1. **Osasto**

- o Myynti
- o Markkinointi
- o Asiakaspalvelu
- o Osto ja -logistiikka
- o Tuotanto
- o Hallinto

2. **Missä järjestelmissä/laitteilla käsittelet työhön liittyviä henkilötietoja?**

- o PC
- o Kannettavat laitteet
- o Paperinen arkisto
- o Ulkoiset tallennusvälineet (esim. USB-tikut, CD-levyt)
- o Pilvipalvelut (esim. OneDrive, Google Drive)
- o Verkkolevy
- o Sähköposti (Outlook, Gmail)
- o SAP
- o Solu BS (verkkosivujen hallinta)
- o Muu, mikä?

3. **Mitä tarkoitusta varten käsittelet henkilötietoja?**

- o Asiakkaiden kontaktointi
- o Sopimusvelvoitteiden täyttäminen (esim. tilauskäsittely)

- Markkinointi
- Toimittajakontaktointi
- Työsuhteeseen liittyvä tarkoitus
- Muu, mikä?

4. Mitä henkilötietoja käsittelet?

- Etu- ja sukunimi
- Postiosoite (työ)
- Postiosoite (koti)
- Sähköpostiosoite
- Syntymäaika
- Sotu
- Henkilön käyttäjätunnus
- IP-osoite
- Muu, mikä?

5. Mistä hankit henkilötietoja?

- Julkisista lähteistä (esim. verkkosivut)
- Henkilöltä itseltään
- Ostamalla
- Muuta kautta, mistä?

6. Miten varmistut henkilötietojen ajantasaisuudesta ja oikeellisuudesta?

- Päivitän tietoja säännöllisesti
- Satunnaisesti, kun on tarve käyttää tietoja
- Satunnaisesti, kun saan tiedon muutoksesta
- En voi varmistua siitä kovinkaan helposti
- Muulla tavoin, miten?

7. Miten voit varmistua, että henkilötietoihin ei ole asiattomilta pääsyä?

8. Onko jotain muuta mitä haluaisit sanoa tästä aiheesta?

LIIITE 2

Teemahaastattelun runko

Kysymys 1. Mitä ymmärrät sanalla henkilötieto ja tietosuoja?
Kysymys 2. Millaisia tietoja sinulla on ennestään henkilötietojen käsittelystä?
Kysymys 3. Kerro miten käsittelet henkilötietoja työssäsi.
Kysymys 4. Kuvaile, miten ja mistä paikasta löydät tarvitsemasi henkilötiedot.
Kysymys 5. Mikäli henkilö, esim. asiakas, pyytää saada tarkistaa hänestä tallennetut henkilötiedot, miten toimit?
Kysymys 6. Mitkä seikat koet henkilötietojen käsittelyssä ja hallinnassa kaikkein haastavimmiksi käytännön työssäsi?

LIITTEET 3-6