Opinnäytetyö AMK

Tietojenkäsittely

2018

Lauri Pöyhönen

TIETOSUOJA-ASETUKSEN VAATIMUKSET JA HAASTEET ORGANISAATIOISSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2018 | 29 sivua

Lauri Pöyhönen

TIETOSUOJA-ASETUKSEN VAATIMUKSET JA HAASTEET ORGANISAATIOISSA

Click here to enter text.

Opinnäytetyö on tutkimus Euroopan unionin uuden tietosuoja-asetuksen (GDPR), 2016/679 tuomista haasteista ja muutoksista organisaatioiden toiminnassa. Lisäksi tutkimus sisältää selvityksen siitä, miten toimeksiantajana toimivan XCure Solutions Oy:n kehittämä Tietosuojatyökalu on vaikuttanut vaatimuksien täyttymiseen.

Tietosuoja-asetus on suuri muutos koko Euroopan Unionissa. Vaikka asetus on osa suoraan sovellettavaa lainsäädäntöä, jättää se silti paljon tulkinnan varaa. Asetus ei vain vaadi tietosuoja-asetuksen noudattamista, vaan myös asetuksen noudattamisen osoittamista.

Opinnäytetyön teoriaosuudessa käsitellään mitä tietosuoja-asetus tarkoittaa ja mitä haasteita se tuo yrityksille. Teoriaosuudessa myös määritellään vaatimukset, jotka yrityksen täytyy täyttää noudattaakseen uutta tietosuoja-asetusta.

Teoriaosuuden ja haastatteluiden pohjalta on laadittu yhteenveto, joka kertoo toimeksiantajan asiakasyritysten nykytilanteesta ja haasteista mitä on kohdattu tietosuoja-asetuksen tuomien vaatimusten täyttämisessä.

Opinnäytetyö sisältää sen, miten yritysten tilanne on muuttunut ennen toimeksiantajan tarjoaman tukipalvelun käyttöä, mitä haasteita prosessi pitää sisällään ja millaisia vaikutuksia uudistuksella on ollut yritysten toimintaan.

Yhteenvetona voidaan todeta, että osoitusvelvollisuuden täyttäminen, kaiken olemassa olevan tiedon kartoittaminen ja dokumentoinnin tärkeys vaatii organisaatioilta huomattavan määrän aikaa ja vaivaa. Tämän takia kiinnostus tietosuoja-asetukseen liittyvien toimenpiteiden ulkoistamiseen on suurta.

ASIASANAT:

tietosuoja, tietosuoja-asetus, Euroopan Unioni, osoitusvelvollisuus, rekisterinpitäjä, rekisteri, rekisteröity, organisaatio

BACHELOR´S / MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Data processing

2018 | 29 pages

Lauri Pöyhönen

DATA PROTECTION REGULATION'S CHALLENGES AND REQUIREMENTS IN ORGANIZATIONS

Click here to enter text.

The thesis is a study about the challenges and changes what the European Union's new Data Protection Regulation (GDPR) 2016/679 brings in the operation of organizations. In addition, the study includes an analysis of how the data protection solution called "Tietosuojatyökalu" developed by the XCure Solutions Oy has affected the fulfillment of these requirements.

The Data Protection Regulation is a major change throughout the whole European Union. Although the Regulation is part of the directly applicable legislation, it leaves a lot room for interpretation. The Regulation not only requires compliance with the privacy policy, but also to demonstrates compliance.

The theoretical part of the thesis deals with what the privacy setting means and what challenges it brings to organizations. The theory section also defines the requirements that an organization must meet to comply with the new privacy policy.

Based on the theoretical part and the interviews, a summary of the client's current client situation and the challenges faced by the client in fulfilling the requirements of the Data Protection Regulation has been compiled.

The thesis includes how the situation of companies has changed before using the support service offered by the client, what challenges the process entails, and what impact the reform has had on business.

In summary, the fulfillment of the assignment obligation, the identification of all existing information and the importance of documenting it require a considerable amount of time and effort from organizations. Therefore, the interest in outsourcing the data protection regulation measures is great.

KEYWORDS:

data protection, data protection regulation, European Union, assignment obligation, controller, register, registered, organization

SISÄLTÖ

SANASTO

GDPR	General Data Protection Regulation, eli EU:n uusi tietosuoja-asetus(Tietosuojatyökalu.fi)
Henkilötieto	Kaikki tieto millä voidaan tunnistaa ja yksilöidä henkilöitä. (Tietosuojatyökalu.fi)
Rekisteri	Henkilörekisteri eli rekisteri on henkilötietoja sisältävä tietojoukko, joka on järjestelty listaksi, luetteloksi tai muulla vastaavalla tavalla. (Tietosuojatyökalu.fi)
Rekisterinpitäjä	Taho, joka päättää mihin tarkoituksiin ja millä tavalla henkilötietoja kerätään ja käytetään. (Tietosuojatyökalu.fi)
Rekisterin käsittelijä/ henkilötietojen käsittelijä	Taho, jonka rekisterinpitäjä on valtuuttanut käsittelemään henkilötietoja. Käsittelijä siis käsittelee tietoja rekisterinpitäjän puolesta. (Tietosuojatyökalu.fi)
Rekisteröity	Rekisterissä oleva tunnistettavissa oleva luonnollinen henkilö. (Tietosuojatyökalu.fi)
Pseudonymisointi	Henkilötietojen käsittelemistä niin, että käytetään keinotekoisia tunnisteita, jotta tietoja ei voida enää yhdistää tiettyyn rekisteröityyn lisätietoja käyttämättä. (Tietosuojatyökalu.fi)

1 JOHDANTO

Opinnäytetyö käsittelee tietosuoja-asetuksen aiheuttamia haasteita ja vaikutuksia organisaatioissa. Opinnäytetyön aihe on valittu tietosuoja-asetuksen ajankohtaisuuden, sekä oman henkilökohtaisen kiinnostuksen pohjalta. Lisäksi olen aloittamassa työskentelyn tietosuojan parissa, joten uskon aiheen auttavan minua kehittymään tulevaan ammattiini.

Euroopan unionin tietosuoja-asetus on uudistunut. Uusi tietosuoja-asetus (General Data Protection Regulation), 2016/679 annettiin 27.4.2016. Asetus tuo mukanaan paljon uusia vaatimuksia, haasteita ja sanktiota Euroopan unionin jäsenmaissa toimiville yrityksille. Uudistus vaikuttaa suuresti henkilötietojen käsittelyyn, dokumentointiin ja luo vaatimuksia yritysten tietoturvalle. Asetusta alettiin soveltamaan 25.5.2018, josta lähtien kaikkien jäsenvaltioiden lainsäädännön on vastattava asetuksen ehtoihin. Uuden tietosuoja-asetuksen tarkoitus on suojata luonnollisten henkilöiden oikeuksia, yksityisyyden suojaa ja lisätä luottamusta henkilötietojen käsittelyssä. (Tietosuojavaltuutetun toimisto)

Uusi tietosuoja-asetus on todella ajankohtainen kaikille Euroopan unionin alueella toimiville yrityksille. Asetuksen noudattamatta jättämisestä voi organisaatiolle koitua sanktioita jopa 4 prosenttia organisaation globaalista liikevaihdosta. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 83 artikla.)

Tässä opinnäytetyössä käsitellään omasta mielestäni tietosuoja-asetuksen tärkeimmät ja keskeisimmät kohdat. Koko asetuksen läpikäyminen ei asetuksen laajuuden vuoksi ollut mahdollista. Opinnäytetyössä sivutaan myös ajankohtaisia tietoturvaratkaisuja, jotka auttavat vastaamaan asetuksen osoitusvelvollisuuteen.

Tämän tutkimuksen tavoitteena on kartoittaa mitä vaatimuksia ja haasteita uudistus luo organisaatioille ja miten ne vaikuttavat yrityksen toimintaan. Tutkimus selvittää, myös kuinka toimeksiantajan tarjoama tukipalvelu vaikuttaa yritysten kykyyn vastata uuden tietosuoja-asetuksen vaatimuksiin ja haasteisiin. Tämä tutkimus on tarpeellinen, sillä toimeksiantaja XCure Solutions tarvitsi tietoa tarjoamansa tukipalvelun ja työkalun hyödyllisyydestä.

2 TIETOSUOJA-ASETUKSEN PERUSTEET

Tässä kappaleessa kerrotaan tietosuoja-asetuksesta perustasolla. Kappale kertoo tietosuoja-asetuksesta ja käsittelee asetuksen tuomia muutoksia aikaisempiin tietosuojakäytäntöihin

EU:n uusi yleinen tietosuoja-asetus, eli GDPR (General Data Protection Regulation) hyväksyttiin Euroopan komissiossa 26.4.2016 ja sitä alettiin soveltamaan 25.5.2018. Asetus määrittelee miten henkilötietoja saa käsitellä EU:ssa. Asetus on viralliselta nimeltään 2016/679. (findwise.com)

Kyseessä on suoraan jäsenvaltiossa sovellettava asetus ja se tulee yhdenmukaistamaan tietojenkäsittelyn säännökset EU:n alueella. (Ylipartanen, A, Andreasson, A 2015)

Uusi tietosuoja-asetus korvaa vuonna 1995 voimaan tulleen direktiivin. Vanha direktiivi oli julkaistu digiajan ulkopuolella, ja on nykyisten verkkopalveluiden ja jatkuvan teknologian kehityksen takia pahasti vanhentunut. Lukuisat verkkopalvelut luovat uusia tietosuojahaasteita. Uusi asetus pyrkii lisäämään rekisteröityjen luottamusta erilaisiin verkkopalveluihin ja henkilötietojen käsittelyyn. Tämän takia tietosuoja-asetus on tarpeellinen ja ajanmukainen. (Aalto-Setälä 2017)

2.1 Mitä uusi tietosuoja-asetus tarkoittaa?

Jatkuva teknologian kehitys ja tiedon digitalisoituminen luovat uusia haasteita henkilötietojen käsittelyn suojaamiselle. EU:n uusi tietosuoja-asetus on säädetty vastaamaan edellä mainittuihin haasteisiin. Uusi asetus parantaa EU:n kansalaisten henkilötietojen suojaamiseen liittyviä oikeuksia, yksityisyyden suojaa sekä lisää luottamusta tietojen käsittelyssä.

Uuden asetuksen myötä EU:ssa toimivat yritykset saavat yhteiset kaikkia koskevat säännöt, nykyisen voimassa olevan valtiokohtaisesti sovellettavissa olevan direktiivin sijaan. Uusi asetus helpottaa kansainvälisesti toimivien yritysten toimintaa, kun tietosuojaan liittyvän asioinnin voi jatkossa hoitaa vain yhden valtion tietosuojaviranomaisen kanssa. Asetuksen suurin tavoite on lisätä ja vahvistaa rekisteröityjen oikeuksia tietää miten heidän tietojaan käsitellään. Uuden asetuksen myötä henkilötietojen käsittely

muuttuu avoimemmaksi ja läpinäkyvämmäksi. Asetusta sovelletaan kaikkeen henkilötietojen käsittelyyn EU:n alueella. (Tietosuojavaltuutetun toimisto)

2.2 Tietosuojaperiaatteet henkilötietojen käsittelyssä

Tietosuoja-asetuksessa on säädetty lainmukaiset periaatteet henkilötietojen käsittelylle. Säädetyt periaatteet pitävät huolen, että tietoja käsitellään rekisteröidyn oikeuksia kunnioittaen. Rekisterinpitäjän on pystyttävä dokumentein todistamaan, että se noudattaa seuraavia periaatteita tietojenkäsittelyssä:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen, eheys ja luottamuksellisuus (tietosuojatyökalu.fi 2018, Tietosuojavaltuutetun toimisto)

2.3 Henkilötietojen käsittelyn lainmukaisuus

Henkilötietojen käsittely vaatii aina lainmukaista käsittelyperustetta. Perusteita on useita, joista vähintään yhden tulee toteutua, jotta käsittely täyttäisi lainmukaisuuden vaatimukset. Käsittely perustuu aina johonkin perusteeseen, eikä perustetta voi enää sen jälkeen vaihtaa kyseisten käsiteltävien tietojen osalta. Käsittelyperuste vaikuttaa suuresti siihen, millaisia oikeuksia rekisteröidyllä on. Tietosuoja asetus määrittelee kuusi eri perustetta henkilötietojen käsittelylle. Perusteet ovat:

- suostumus
- sopimus
- rekisterinpitäjän lakisääteinen velvoite
- elintärkeiden etujen suojaaminen
- yleistä etua koskeva tehtävä tai julkinen valta
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu (Tietosuojavaltuutetun toimisto)

Suostumus

Rekisteröity voi antaa suostumuksensa henkilötietojensa käsittelylle. Suostumuksen tulee olla vapaaehtoinen ja selkeä rekisteröidyn oma tahdonilmaisu. Suostumuksellaan rekisteröity hyväksyy tietojensa käsittelyn sovittuja tarkoituksia varten. Suostumus voi olla suullinen, kirjallinen, tai muu selkeä ja helppo tapa. Suostumus on voitava myös peruuttaa yhtä helposti ja vaivattomasti, kun se on annettu. Rekisterinpitäjällä on velvollisuus osoittaa, että pitävä ja lain mukainen suostumus henkilötietojen käsittelyyn on annettu. (Tietosuojavaltuutetun toimisto)

Sopimus

Rekisteröity ja rekisterinpitäjä voivat tehdä sopimuksen henkilötietojen käsittelystä. Sopimus määrittelee mihin tarkoitukseen ja miksi tietoja käsitellään. Sopimuksen ehdot tulee olla selkeästi määritelty, koska ne määrittävät tietojen käsittelyn tarpeellisuuden ja rajat. (Tietosuojavaltuutetun toimisto)

Lakisääteinen velvoite

Rekisterinpitäjällä on velvollisuus noudattaa lakia. Lakisääteinen velvoite tarkoittaa, että rekisteröidyn henkilötietoja voidaan käsitellä ilman erillistä suostumusta, tai sopimusta. Esimerkiksi kun työnantajan on annettava työntekijän palkkatiedot veroviranomaiselle, täyttyy tällöin lakisääteisen velvoitteen tunnusmerkit. (Tietosuojavaltuutetun toimisto)

Elintärkeiden etujen suojaaminen

Henkilötietoja saadaan käsitellä, jos henkilön elintärkeät edut vaativat suojaamista. Esimerkiksi jos kyse on hengenvarasta, mikä voi johtaa kuolemaan tai loukkaantumiseen. Elintärkeää etua voi henkilötietojen käsittelyllä palvella esim. epidemian puhjetessa, kun halutaan saada tietoa epidemian leviämisestä. (tietosuojavaltuutetun toimisto)

Yleinen etu ja julkinen valta

Henkilötietoja voidaan käsitellä, kun yleinen etu tai rekisterinpitäjän julkisen vallan käyttö sitä vaatii. Esimerkki tällaisesta käsittelyperusteesta voi olla tieteellisen tutkimuksen tekeminen. (Tietosuojavaltuutetun toimisto)

Rekisterinpitäjän oikeutettu etu

Jos rekisterinpitäjän etu vaatii henkilötietojen käsittelyä, tai rekisteröidyn ja rekisterinpitäjän välillä on joku suhde, on käsittely silloin sallittua. Esimerkiksi asiakas tai työsuhde on tilanne, missä rekisterinpitäjän etu vaatii tietojenkäsittelyä. (Tietosuojavaltuutetun toimisto)

2.4 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennetulla tietosuojalla tarkoitetaan, että organisaatioiden tulisi huomioida tietojenkäsittelyn- ja yksityisyyden turvallisuus jo alkuvaiheessa suunnitellessaan tietojenkäsittelytoimintoja. Organisaation toiminta tulisi siis olla suunniteltu myös tietosuojan mukaisesti. Esimerkki sisäänrakennetusta tietosuojasta on pseudonymisointi. Pseudonymisoinnissa käsiteltävät henkilötiedot korvataan muilla tunnisteilla, siten että vain valtuutetut henkilötietojen käsittelijät voivat lukea niitä ja yhdistää tiedot rekisteröityihin. (Euroopan komissio)

Oletusarvoinen tietosuoja tarkoittaa, että organisaatiossa on oletusarvoisesti varmistettu tietojenkäsittely korkeaa tietosuojaa noudattaen. Esimerkiksi käsiteltävien tietojen säilytysaika tulisi pitää mahdollisimman lyhyenä ja vain välttämättömiä tietoja tulisi käsitellä. (Euroopan komissio)

2.5 Asetuksen noudattaminen ja sanktiot

Tietosuoja-asetuksen noudattaminen pitää pystyä todistamaan. Tämä tarkoittaa, että dokumentoinnin tärkeys korostuu entisestään. Valvontaviranomainen voi tarvittaessa vaatia dokumentteja todentamaan, että organisaatio on noudattanut tietosuoja-asetuksen vaatimuksia henkilötietojen käsittelyssä. Organisaatiolla on myös velvollisuuksia itse ilmoittaa viranomaiselle, esimerkiksi jos tapahtuu tietoturvaloukkaus. Asetus vaatii, että tietoturvaloukkauksen tapahtuessa, tulee siitä ilmoittaa viranomaiselle 72 tunnin kuluessa. Mikäli organisaatio ei onnistu noudattamaan tai todistamaan että asetusta on noudatettu, tulee organisaatiolle sanktioita. Tietosuoja-asetuksen sanktiot voivat ulottua jopa 20 miljoonaan euroon tai 4% globaalista liikevaihdosta. Sanktiot voivat olla myös

rajoitteita, kuten kielto toimia jatkossa rekisterinpitäjänä. Asetus ja sen sisältämät sanktiot tulee siis ottaa vakavasti ja huomioida henkilötietojen käsittelyssä ja dokumentoinnissa. (Lukander Ruohola HTO)

2.6 Tietosuojavastaava

Tietosuoja-asetuksessa velvoitetaan, että osalle rekisterinpitäjistä täytyy nimetä tietosuojavastaava. Tietosuojavastaava on organisaation itse nimittämä oma sisäinen asiantuntija, joka valvoo henkilötietojen käsittelyn oikeellisuutta ja antaa tarvittaessa tukea organisaatiolle tietosuojaa koskevissa asioissa. Tietosuojavastaava toimii rekisteröityjen ja organisaation välisenä yhteyshenkilönä henkilötietoja koskevissa asioissa. Nimitettäessä tietosuojavastaavaa tulee huomioida, että vastaavalla on tarpeeksi aikaa ja osaamista hoitaa velvollisuutensa sekä mahdollisuus tietosuoja koulutukseen. Tietosuojavastaava tulee ottaa mukaan tietosuojakysymysten käsittelyihin. Lisäksi tietosuojavastaavan mielipiteille tulisi antaa riittävä painoarvo ja vastaavalla pitäisi olla mahdollisuus raportoida suoraan organisaation johdolle tietosuoja-asetukseen liittyvissä asioissa. Tietosuojavastaava ei ole itse henkilökohtaisesti vastuussa, jos organisaatio rikkoo tietosuoja-asetusta. Vastuu on aina organisaatiolla ja sen johdolla. (Tietosuojavaltuutetun toimisto)

Organisaatioon tulee nimetä tietosuojavastaava, mikäli joku seuraavista kohdista täyttyy:

- Rekisterinpitäjä on viranomainen tai julkisen hallinon elin-
- Rekisterinpitäjän tehtävät muodostuvat tietojenkäsittelystä, jotka jostain syystä vaativat laajamittaista henkilötietojen käsittelyä.
- Rekisterinpitäjän tehtävät edellyttävät erityisten henkilötietoryhmien käsittelyä.

Tietosuoja-asetus jättää tulkinnan varaa siihen miten julkishallinon elin tai laajamittainen käsittely tarkoittaa. Velvollisuus nimetä tietosuojavastaava ei siis koske kaikkia rekisterinpitäjiä. (Yrittäjät 2017)

3 REKISTERÖIDYN OIKEUDET

Tietosuoja-asetuksen suurin tavoite on lisätä ja laajentaa huomattavasti rekisteröityjen oikeuksia tietojenkäsittelyssä. Tämä luo rekisterinpitäjille paljon uusia velvollisuuksia. Rekisteröidyllä on tilanteesta riippuen mahdollisuus oikeuteen saada lisätietoa tietojensa käsittelystä, oikaista, siirtää, rajoittaa tietojensa käsittelyä, tai poistaa tietonsa kokonaan rekisteristä. (Valtiovarainministeriö 2016)

3.1 Oikeus saada tietoa henkilötietojensa käsittelystä

Tietosuoja-asetus antaa rekisteröidylle oikeuden saada tietää käsitteleekö rekisterinpitäjä hänen tietojaan. Mikäli rekisterinpitäjä käsittelee hänen tietojaan on rekisteröidyllä oikeus saada tietää mitä henkilötietoryhmiä käsitellään ja mahdolliset vastaanottajat joille rekisterinpitäjä on hänen tietojaan luovuttanut tai on aikeissa luovuttaa. Rekisteröidyllä on myös oikeus saada tietää, kuinka kauan hänen tietojaan on suunniteltu säilytettävän ja hänen tietojensa alkuperä, mikäli tietoja ei ole saatu rekisteröidyltä itseltään. (Yrittäjät 2018)

3.2 Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus vaatia organisaatiota poistamaan omat tietonsa järjestelmistään. Tähän on oikeus, jos rekisteröidyn tietoja ei tarvita tai käsitellä niihin tarkoituksiin mihin ne on alun perin kerätty. Rekisteröity voi myös vaatia tietojaan poistettavaksi, jos tiedot on annettu suostumuksella ja rekisteröity peruu antamansa suostumuksen tai jos rekisterinpitäjä on käsitellyt tietoja lainvastaisesti. Rekisteröidyn tiedot voidaan myös poistaa, mikäli lakisääteinen velvoite sitä vaatii. Tietyissä tilanteissa rekisterinpitäjän etu voi voi vaatia, että rekisteröidyn tietoja ei voida poistaa. Esimerkiksi tilanteessa jossa rekisteröity on työntekijä ja rekisterinpitäjä toimii työnantajana ei rekisteröidyn tietoja voida poistaa. (Yrittäjät 2018)

3.3 Oikeus siirtää omat tiedot toiseen järjestelmään

Mikäli rekisteröidyn tietoja käsitellään suostumuksella tai sopimuksella, ja tietojenkäsittely tapahtuu jonkinlaisella automatisoidulla ohjelmalla. On rekisteröidyllä tällöin oikeus siirtää häntä koskevat tiedot toisen rekisterinpitäjän järjestelmään. Tämä lisää rekisterinpitäjän velvollisuuksia. Järjestelmä missä tietoja käsitellään tulisi suunnitella siten, että tietojen siirto toiselle rekisterinpitäjälle on mahdollista. Oikeus tietojen siirtoon ei koske paperisia tietoja. (Yrittäjät 2018)

3.4 Oikeus rajoittaa tietojen käsittelyä

Rekisteröity voi vaatia tietojensa poistamisen sijaan myös tietojensa käsittelyn rajoittamista. Tällöin tietoja saa käsitellä vain rekisteröidyn erillisellä suostumuksella tai jos toisen henkilön etu sitä vaatii.

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää rajoittamaan tietojensa käsittelyä seuraavissa tilanteissa:

- Henkilötietojen käsittely on lainvastaista ja rekisteröity ei halua tietojaan poistettavan, vaan vaati käsittelyn rajoittamista.
- Rekisterinpitäjällä ei ole enää syytä käsitellä tietoja, mutta rekisteröidyn etu vaatii tietojen säilyttämistä.
- Rekisteröidyn ja rekisterinpitäjän välillä on erimielisyys tietojen käsittelyn tarpeellisuudesta. Päätöstä odottaessa rekisteröity voi vaatia tietojensa käsittelyn rajoittamista. (Yrittäjät 2018)

3.5 Oikeus vastustaa tietojensa käsittelyä.

rekisteröity voi milloin vaan vastustaa häntä koskevien tietojen käsittelyä, mikäli hän on antanut suostumuksensa tietojen käsittelylle. Rekisteröity voi myös vastustaa tietojensa käsittelyä, jos käsittely perustuu rekisterinpitäjän oikeutettuun etuun tai profilointiin.

Vastustamisen jälkeen rekisterinpitäjä ei saa käsitellä tietoja, ellei se pysty osoittamaan, että käsittelyn syynä on huomattava tärkeä ja perusteltu syy. Syyn tulee olla niin tärkeä ja hyvin perusteltu, että rekisteröidyn etu ja oikeus ei riitä tietojen käsittelyn vastustamiseen. (Yrittäjät 2018)

4 OSOITUSVELVOLLISUUS

Tässä kappaleessa käydään läpi rekisterinpitäjän osoitusvelvollisuutta. Tietosuoja-asetus velvoittaa rekisterinpitäjän paitsi noudattamaan, myös osoittamaan noudattavansa asetusta. Kappale kertoo tärkeimmät dokumentoitavat asiat, jotka rekisterinpitäjällä tulee olla selkeästi kirjattuna.

Henkilötietoja käsittelevällä organisaatiolla, eli rekisterinpitäjällä, on velvollisuus osoittaa konkreettisesti dokumentein noudattavansa tietosuoja-asetuksen vaatimuksia. Aikaisemman lakiasetuksen mukaan riitti, että rekisterinpitäjä noudatti lakia. Mitään velvollisuuksia lain noudattamisen osoittamisen suhteen ei ollut. Osoitusvelvollisuus on keskeinen osa tietosuoja-asetusta ja sen noudattaminen on yhtä tärkeää kuin itse asetuksen noudattaminen. Rekisterinpitäjän tulee todistaa pyrkineensä tunnistamaan tietosuojaan liittyvät riskit ja ottaneensa käyttöön tarvittavat tietosuojatoimenpiteet. Lisäksi osoitusvelvollisuus velvoittaa rekisterinpitäjän suorittamaan ja kirjaamaan erilaisia toimenpiteitä. Täyttääkseen osoitusvelvollisuuden rekisterinpitäjällä tulee olla selkeä dokumentaatio ainakin siitä mihin käyttötarkoitukseen tietoja käsitellään, miten henkilötietoja käsitellään, mihin henkilötietojen käsittely perustuu, mitä tietoryhmiä käsitellään ja tietosuojavastaavan tiedoista. Jos henkilötietoja käsitellään rekisteröidyn suostumuksella, tulee rekisterinpitäjän pystyä tämä dokumentein osoittamaan. Myös tietoturvaloukkaukset tulee dokumentoida ja niistä ilmoittaa viimeistään 72 tunnin kuluessa tietomurron havaitsemisesta tietosuojaviranomaiselle (Tietosuojavaltuutetun toimisto)

.

4.1 Seloste käsittelytoimista

Rekisterinpitäjällä tulee olla kirjallinen seloste siitä, kuinka henkilötietoja käsitellään. Selosteen tulee kattaa kaikki henkilötietojen käsittelyyn liittyvä toiminta. Seloste toimii rekisterinpitäjän omana apuvälineenä tietojen käsittelyn kokonaiskuvan hahmottamisessa ja samalla sen avulla voidaan osittain täyttää rekisterinpitäjän osoitusvelvollisuutta. Seloste on rekisterinpitäjälle pakollinen, mikäli organisaatiossa työskentelee

enemmän kun 250 työntekijää. Käsittelyseloste tulee tehdä myös tietyissä tilanteissa, vaikka organisaatiossa olisi alle 250 työntekijää. Tällaisia tilanteita ovat:

- Rekisterinpitäjän käsittelemät henkilötiedot sisältävät erityisiä henkilötietoja, tai rikostuomioihin liittyviä tietoja.
- Henkilötietojen käsittely on kohdistettua ja järjestelmällistä.
- Henkilötietojen käsittely luo todennäköisiä riskejä rekisteröidyn edulle ja vapaudelle. (Tietosuojavaltuutetun toimisto)

Jos seloste on tehty jostain edellä mainitusta syystä, tulee sen kattaa vain kyseiseen syyhyn liittyvät käsittelytoimet. (Tietosuojavaltuutetun toimisto)

Täyttääkseen osoitusvelvollisuuden rekisterinpitäjän laatimassa selosteessa tulee olla selkeästi dokumentoituna ainakin seuraavat asiat:

- Rekisterinpitäjä ja tietosuojavastaava.
- Käsittelyn tarkoitukset.
- Kuvaus henkilötietoryhmistä.
- Ryhmät tai tahot joille henkilötietoja luovutetaan tai on luovutettu.
- Tiedot tietojen siirrosta kolmanteen maahan tai kansainväliselle järjestölle.
- tietojen säilytysajat.
- Kuvaus teknisistä ja organisatorisista turvatoimista. (Tietosuojavaltuutetun toimisto)

Rekisterinpitäjä ja tietosuojavastaava

Rekisterinpitäjällä tulee olla dokumentoituna itsensä ja tietosuojavastaavan yhteystiedot. Rekisterinpitäjällä tarkoitetaan luonnollista henkilö tai organisaatiota, joka päättää miten ja mihin tarkoituksiin tietoja kerätään ja käsitellään. Tietosuojavastaavalla taas tarkoitetaan henkilöä, joka avustaa rekisterin pitäjää tietosuojaan liittyvissä asioissa ja valvoo, että organisaatiossa noudatetaan tietosuoja-asetusta. Tietosuojavastaavalla tulee olla tietosuojaan liittyvää asiantuntemusta. (Tietosuojavaltuutetun toimisto)

Käsittelyn tarkoitukset

Rekisterinpitäjällä tulee olla määriteltynä tarkat lailliset käyttötarkoitukset niille tiedoille, joita se toiminnassaan käsittelee. Kaikki käyttötarkoitukset tulee olla erikseen dokumentoitu. Käyttötarkoitus määrittelee mihin tarkoituksiin tietoja käsitellään ja mitä tietoja on tarpeen kerätä. Tietojenkäsittely tarkoittaa toimia, jotka kohdistuvat henkilötietoihin.

Dokumentoinnissa tulisi myös ilmetä millä perusteella tietoja käsitellään, sillä se vaikuttaa tietosuoja-asetuksen mukaisiin rekisteröidyn oikeuksiin. (Tietosuojavaltuutetun toimisto)

Kuvaus henkilötietoryhmistä

Rekisterinpitäjän tulee dokumentoida ryhmäkohtaisesti, keitä rekisteröidyt, joiden tietoja käsitellään ovat ja millaisia tietoja heistä on. Henkilöryhmällä tarkoitetaan esimerkiksi asiakkaita tai työntekijöitä. Tietoryhmä voi olla esimerkiksi yksilöintitiedot, kuten nimi tai syntymäaika. Henkilötiedoiksi luetaan kaikki tieto minkä avulla rekisteröity voidaan tunnistaa. (Tietosuojavaltuutetun toimisto)

Ryhmät tai tahot joille henkilötietoja luovutetaan tai on luovutettu

Mikäli henkilötietoja lähetetään jollekin toiselle taholle, tulee sekin olla selkeästi dokumentoituna. Tietojen vastaanottajalla tarkoitetaan luonnollista henkilöä tai muuta tahoa jolle on luovutettu henkilötietoja. Dokumentaatiossa tulee näkyä kaikki henkilötietojen vastaanottajat. Vastaanottajalla tulee olla laillinen peruste, tai oikeus henkilötietojen käsittelyyn. Dokumentaatiossa tulee kuvata vastaanottaja niin tarkasti kuin mahdollista. Viranomaisia, joille luovutetaan tietoja EU:n tai jäsenvaltion lainsäädäntöön perustavan syyn takia ei tarvitse erikseen dokumentoida. (Tietosuojavaltuutetun toimisto)

Tiedot tietojen siirrosta kolmanteen maahan tai kansainvälisesti

Dokumentaatiossa tulee näkyä myös mahdolliset tietojen siirrot kolmansiin maihin, tai kansainvälisille järjestöille. Siirrosta tulee kirjata mihin ja kenelle siirretään. Rekisterinpitäjän tulee pystyä osoittamaan tietosuoja-asetuksen kohta, joka mahdollistaa tietojen siirron. (Tietosuojavaltuutetun toimisto)

Tietojen säilytysajat

Rekisterinpitäjän tulee dokumentoida arviot siitä kauan mitäkin tietoryhmiä tullaan säilyttämään. Tämä liittyy tietojenkäsittelyn minimointiin ja säilytyksen rajoittamiseen. Säilytysaika voi määräytyä lain tai eri toimialojen käytäntöjen mukaan. Aika-arvioiden perusteella tulee pystyä arvioimaan, myös kauanko henkilötietoja tullaan käsittelemään. Tietojen säilytysajan arvion tulee olla jokin konkreettinen aika - ei tilanne tai sen muuttuminen. Esimerkki tietojen säilytysajasta voi olla, että tietoja käsitellään niin kauan kun tarpeen on. (Tietosuojavaltuutetun toimisto)

Kuvaus teknisistä ja organisatorisista turvatoimista

Dokumentoinnista tulisi käydä ilmi mitä suojausmenetelmiä on käytössä tietojenkäsittelyn suojaamiseksi. Käsiteltävät tiedot tulisi suojata ainakin organisaation ulkopuolisilta. Myös käyttöoikeuksia tulisi rajata siten, että vain valtuutetut henkilötietojen käsittelijät pystyvät tietoja käsittelemään. Tietosuoja-asetus velvoittaa rekisterinpitäjän suojaamaan käsiteltävät tiedot riittävän tehokkaasti. Lisätietoa tietoturvaratkaisuista kappaleessa 5. (Tietosuojavaltuutetun toimisto)

5 TEKNISET TIETOTURVATOIMET

Tässä kappaleessa käydään läpi teknisiä tietoturvaratkaisuja, jotka tulee huomioida ja toteuttaa uuden tietosuoja-asetuksen myötä. Tietoturvalla tarkoitetaan tietojen suojausta ja salausta. Tietoturvan tavoite on tietojen pysyminen vain niiden käytössä, joilla on tietoihin oikeus. Tietoturvallisuudella tähdätään tietojen riittävään eheyteen, käytettävyyteen ja luottamuksellisuuteen. On hyvä muistaa, että ilman hyvää tietoturvaa, ei voi olla toimivaa tietosuojaa. Oikein hoidettu tietoturva on myös välttämätön osa rekisterinpitäjän osoitusvelvollisuutta. Tietosuoja-asetuksessa on vaatimus, joka velvoittaa rekisterinpitäjän toteuttamaan teknisiä ratkaisuja henkilötietojen käsittelyssä. Näillä ratkaisuilla pyritään takaamaan käsiteltävien tietojen riittävä turvallisuus. Seuraavassa on kuvattu tietoturvaratkaisuja, jotka kannattaisi ottaa huomioon henkilötietojen suojaamisessa. (Tirronen, 2003)

5.1 Pseudonymidointi

Pseudonymisointi tarkoittaa tapaa käsitellä henkilötietoja siten, että tietoihin liitetään keinotekoisia tunnisteita, joita ilman tietoja on mahdoton yhdistää rekisteröityyn. Pseudonymisointi on hyvä tapa turvata rekisteröityjen oikeuksia henkilötietojen käsittelyssä. (Tietosuojatyökalu.fi)

5.2 Palomuurit

Palomuuriksi kutsutaan järjestelmää, joka valvoo liikennettä verkkojen välillä. Palomuuri toimii tietoturvaratkaisuna verkon ulkopuolelta tuleville uhille. Valvottavan ja suojattavan liikenteen tulee kulkea palomuurin läpi. Palomuuri toimii eräänlaisena suodattimena, päästäen vain toivotun liikenteen läpi. Palomuuri yksin ei takaa riittävää suojausta tiedoille ja järjestelmille, mutta toimii hyvin osana toimivaa tietoturvaa. (Yksityisyydensuoja)

5.3 Suojattu ja salattu verkkoyhteys

Luottamuksellisen tiedon siirtoon kannattaa käyttää salattua yhteyttä. Tällainen yhteys voi olla vaikka SSL-salaus. SSL-salaus suojaa päätelaitteen ja palvelimen välisen yhteyden ja estää näin tiedon kaappaamisen yritykset. Myös sähköpostiliikenne kannattaa salata. Sähköpostin salaaminen onnistuu yleensä sähköpostipalvelun kautta. Itse sähköpostit, eli niiden sisältämät tiedot, kannattaa myös salata. Tätä varten on olemassa erilaisia palveluita. Käytettävästä salausmetodista tulee sopia sähköpostin vastaanottajan kanssa. (Viestintävirasto 2017)

5.4 Kulunvalvonta

Henkilötietoja- ja rekistereitä voi olla myös fyysisessä paperisessa muodossa, tai paikallisesti säilöttynä digitaalisessa muodossa. Tällöin tietojen fyysinen suojaus tulee myös olla kunnossa. Fyysisellä suojauksella tarkoitetaan säilytystilojen suojaamista lukituin ovin, kameravalvonnalla tai muulla kulunvalvontamenetelmällä. kulunvalvonnan tarkoitus on varmistaa, ettei tietoihin pääse käsiksi muut, kun tarkoitetut henkilötietojen käsittelijät. Kulunvalvonta mahdollistaa henkilöstön kulun seurannan ja antaa tietoa esimerkiksi siitä, kuka milloinkin käy suojatussa kohteessa tai tilassa. (Sähköala.fi)

5.5 Työasemien suojaus

Henkilökunnan käytössä olevat työasemat, joilla kytkeydytään organisaation verkkoon ja käsitellään tietoja tulisi suojata riittävällä tasolla. Suojaus lähtee laitteen fyysisestä suojauksesta. Varsinkin kannettavien työasemien kovalevyt tulisi salata ja suojata salasanalla. Laitteen käyttöoikeudet tulisi asettaa perustasolle, niin ettei käyttäjällä ole ylimääräisiä oikeuksia, tai ettei käyttäjä pääse liikkumaan verkossa saastuneille sivustoille. Kaikkien asemassa olevien ohjelmistojen tulisi olla aina päivitetty uusimpaan versioon, jotta niistä mahdollisesti jo löydettyjä haavoittuvuuksia ei voitaisi hyödyntää verkkohyökkäyksissä. lopuksi työasemat tulisi suojata viruksentorjuntaohjelmalla. Uusimissa ohjelmistoissa on mukana käyttöoikeuksien hallinta ja kovalevyn suojaus. (Valtiovarainministeriö 2009)

5.6 Tiedon salaus

Myös itse tiedot tulisi salata. Tietoa on nykyään tallennettuna paljon organisaation palvelimilla sekä erilaisissa pilvipalveluissa. Vaikka edellä mainitut olisikin suojattu, saattaa niihin silti kohdistua tietomurtoja. Salatut tiedostot ovat tällöinkin turvassa, sillä vaikka hyökkääjä saisi tiedostot itselleen, ei hän niitä voisi kuitenkaan avata.

6 TIETOSUOJA-ASETUS OSANA ORGANISAATION TOIMINTAA

Tähän opinnäytetyöhön liittyen on tutkittu kahden organisaation valmiutta ja kykyä vastata tietosuoja-asetuksen haasteisiin ja vaatimuksiin. Toinen organisaatio on kooltaan noin 3000 työntekijää ja toinen organisaatio noin 20 työntekijää. Molemmat organisaatiot ovat opinnäytetyön toimeksiantajan XCure Solutions Oy:n asiakkaita. Molempia organisaatiota on tutkittu ja haastateltu asiakasprojektien aikana. Organisaatiolta on haastattelussa kysytty:

- Miten koette tietosuoja-asetuksen vaikuttavan organisaationne toimintaan?
- Mitkä ovat mielestänne suurimmat haasteet tietosuoja-asetuksen noudattamisessa?
- Miten tietosuoja-asetus tulee näkymään toiminnassanne?
- Onko XCure Solutions oy:n Tietosuojatyökalu helpottanut tietosuoja-asetuksen osoitusvelvollisuuden noudattamista?
- Miten itse koette tietosuoja-asetuksen?

Projektit ovat liittyneet tietosuoja-asetukseen ja XCure Solutions Oy:n tarjoaman Tietosuojatyökalun käyttöön. Tietosuoja-asetus on suuri muutos ja vaikuttaa suuresti yritysten ja organisaatioiden toimintaan. Asetus luo uusia haasteita ja vaatimuksia, joihin vastaaminen vie paljon työtä ja aikaa. Organisaatioiden tulee nyt kartoittaa mitä ja minkä luonteista tietoa niillä on, missä tietoa säilytetään, ja miksi sitä kerätään tai on kerätty. Näitä kysymyksiä ei ole ennen jouduttu miettimään. Kaikki tämä liittyy suoraan organisaation osoitusvelvollisuuteen, mikä on tietosuoja-asetuksen ”näkyvä” osa. Tutkimuksessa selvisi, että kaiken tiedon kartoittaminen koettiin varsinkin isossa organisaatiossa haasteeksi. Tämä johtui siitä, että tietoa on paljon ja sitä on kerätty jatkuvasti vuosien ajan. Lisäksi kerätty tieto on säilötty hajautetusti ympäri organisaatiota. Henkilötietojen ja rekistereiden kartoittaminen koettiin siis suureksi haasteeksi. Toinen havaittu haaste liittyi suoraan tietosuoja-asetukseen ja sen ymmärtämiseen. Tietosuoja-asetus pitää sisällään paljon asiaa, uusia käsitteitä ja säännöksiä, joiden ymmärtäminen on haastavaa. Organisaatiossa henkilötietoja käsittelevän henkilöstön tulisi kuitenkin ymmärtää nämä asiat asetuksen noudattamisen ja osoitusvelvollisuuden täyttymisen vuoksi. Kolmas suurempi havaittu haaste liittyi tietosuoja-asetuksen mukaisiin tietosuojatapahtumiin. Tietosuojatapahtumia ovat rekisteröityjen pyynnöt, viranomaisten

yhteydenottopyynnöt ja ilmoitukset tietomurroista. Organisaatioilla ei ollut sovittuja toimintaohjeita- ja tapoja valmiina tietosuojatapahtumien varalle. Suurimpina haasteina ja vaikutuksina pidettiin siis asetuksen aiheuttamaa työmäärää, kaiken olemassa olevan tiedon näkemistä yhtenä isona kokonaisuutena ja asetuksen sisältämän tiedon ymmärtämistä ja sisäistämistä.

6.1 Vaikutukset organisaatioissa

Tietosuoja-asetus luo siis huomattavia haasteita organisaatioille, mutta millaisia vaikutuksia näillä haasteilla on käytännössä organisaation toimintaan? Ulospäin näkyvässä toiminnassa vaikutukset näkyvät lähinnä rekisteröityjen informointina oikeuksistaan. Organisaation sisäisen toiminnan vaikutukset ovat suuremmat. Tällaisia vaikutuksia ovat esimerkiksi tietoturvan huomioiminen ja kehittäminen. Tietoturvan tulee olla sellaisella tasolla, että käsiteltävät henkilötiedot ovat suojassa. Tietosuojavastaava tulee nimetä ja tietotilinpäätös tehdä. Henkilökunnalle tulee järjestää koulutus tietosuojaan liittyvissä asioissa. Henkilötietojen käsittelyä tulee dokumentoida jatkuvasti osoitusvelvollisuuden täyttämiseksi. Tämä tarkoittaa, että organisaation tietosuojaan- ja turvaan liittyvien sisäisten prosessien priorisointi on tärkeämpää kuin koskaan. Nämä tulokset saatiin haastatteluilla ja organisaatioiden toiminnan seuraamisella.

7 KOLMANNEN OSAPUOLEN TARJOAMAN TUKIPALVELUN KÄYTTÖ

Koska tietosuoja-asetus aiheuttaa paljon työtä ja velvollisuuksia, voi organisaatio halutessaan ulkoistaa tietosuojansa kolmannelle osapuolelle. Ulkoistaminen tapahtuu samalla tavalla kuin tietoturvankin ulkoistaminen. Tietosuojaan liittyvää vastuuta ei kuitenkaan voi ulkoistaa. Tässä kappaleessa kerrotaan opinnäytetyön toimeksiantajan XCure Solutions Oy:n tarjoamasta Tietosuojatyökalusta. Tietosuojatyökalu on organisaatioille suunniteltu työkalu, jonne organisaatiot voivat kirjata tietojärjestelmiä ja rekistereitään ja niihin kuuluvia tietoja, kuten henkilötietojen käsittelijöitä, rekisteröityjen oikeuksia ja käsittelyperusteita. Oikein täytettynä voi työkalulla helpottaa rekisterinpitäjän osoitusvelvollisuuden mukana tulevaa taakkaa ja näin ollen keventää tietosuoja-asetuksen aiheuttamaa työmäärää. Tietosuojatyökalu on ollut käytössä molemmilla tutkimukseen osallistuneilla organisaatioilla.

7.1 Tietosuojatyökalu osana organisaation toimintaa

Tietosuojatyökalu on suunniteltu jäsentämään monimutkainen tietosuoja-asetus helposti ymmärrettäviksi tehtäviksi. Työkalu helpottaa tietosuoja-asetuksen vaatimusten kartoittamista ja vastaa osoitusvelvollisuuden täyttämisen haasteisiin. Työkalua käyttämällä organisaation on siis helpompi vastata tietosuoja-asetuksen asettamiin haasteisiin. Tässä tutkimuksessa mukana olleet molemmat organisaatiot ovat käyttäneet Tietosuojatyökalua. Työkalun käyttö on koettu helpoksi ja sen avulla on ollut helppoa hahmottaa ja ymmärtää tietosuoja-asetuksen vaatimuksia. Työkalun käyttöönoton jälkeen 3000 työntekijän organisaatio on saanut kirjattua kaiken asetuksen vaatiman dokumentaation yhteen samaan paikkaan, josta tietosuojaviranomainen voi tarvittaessa tietoja lukea. Molemmissa organisaatioissa Tietosuojatyökalua on pidetty tarpeellisena osoitusvelvollisuuden täyttämisessä. Työkalun on todettu keventävän myös tietosuoja-asetuksen aiheuttamaa työtaakkaa. Kokonaisuudessa molemmat organisaatiot ovat olleet tyytyväisiä XCure Solutions Oy:n Tietosuojatyökalun käyttöön ja jatkavat työkalun käyttöä.

8 POHDINTA

Tässä viimeisessä luvussa kirjaan esille tulleita omia ajatuksiani ja havaintojani Organisaatioiden kohtaamista haasteista ja vaatimuksista, joita tietosuoja-asetuksen mukana on tullut. Käyn myös yhteenvetona läpi opinnäytetyön tavoitteiden ja päämäärien täyttymistä.

8.1 Yleisesti

Kuten tässä opinnäytetyössä on jo esille tullut, tietosuoja-asetus on suuri muutos koko Euroopan Unionin mittapuulla. Vaikka asetus on osa suoraan sovellettavaa lainsäädäntöä, jättää se silti paljon tulkinnan varaa esimerkiksi tietoturvaratkaisujen suhteen. Asetus ei vain vaadi tietosuoja-asetuksen noudattamista, vaan myös asetuksen noudattamisen osoittamista. Omien kokemuksieni kautta olen huomannut juurikin osoitusvelvollisuuden olevan suurin haaste ja kipupiste organisaatioille. Jotta organisaatiot pystyisivät osoittamaan noudattavansa asetusta. Tulee niiden käyttää paljon aikaa ja resursseja tämän tavoitteen saavuttamiseksi. On ymmärrettävää, että liiketoiminnan ulkopuoliseen asiaan ei haluttaisi käyttää resursseja, jotka ovat pois itse liiketoiminnasta ja sen kehittämisestä. Tämä heijastuu organisaatioiden haluna ulkoistaa tietosuoja-asetuksen osoitusvelvollisuus. Olen ollut opinnäytetyön kirjoittamiseen liittyen mukana asiakasprojekteissa, jotka ovat liittyneen asiakasorganisaation tietosuoja-asetuksen osoitusvelvollisuuden täyttämiseen, olemassa olevien tietojen ja rekistereiden kartoittamiseen sekä henkilökunnan ohjeistamiseen. Olen huomannut, että organisaatioilla on paljon motivaatiota hoitaa tietosuoja kuntoon, mutta aikaa siihen ei tunnu aina löytyvän. Tietosuoja-asetus on vielä uusi tulokas lainsäädännöissä, eikä varsinaisia ennakkotapauksia vielä ole. Tämä saattaa vaikuttaa vielä organisaatioiden ajatteluun tietosuojaan liittyvissä prosesseissa. Mielestäni organisaatioiden valmistautuminen tietosuoja-asetukseen on ollut korkeintaan kohtalaista, mutta asetuksen soveltaminen ja ottaminen osaksi omaa liiketoimintaa näyttää alkaneen hyvin. Matka on varmasti vielä monilla pitkä ja paljon työtä ja aikaa tarvitaan lopullisten tavoitteiden saavuttamiseksi. Osoitusvelvollisuuden noudattaminen on jatkuva prosessi, missä vaaditaan jatkuvaa tietojen ja dokumentoinnin päivittämistä normaalin päivittäisen liiketoiminnan yhteydessä.

8.2 Opinnäytetyön päämärät ja niiden saavuttaminen

Opinnäytetyön päämääränä on ollut listata ja kuvata tietosuoja-asetukseen kuuluvia vaatimuksia. Tämän jälkeen kartoittaa ja tutkia organisaatioiden kykyä, tilannetta ja kehitystä edellä mainittujen tietosuoja-asetuksen vaatimusten kannalta. Kun tietosuoja-asetusta alettiin soveltamaan 25.05.2018 olivat monet organisaatiot vielä vasta lähtökuopissa. Tässä osiossa keskitytään tutkimuksessa mukana olleiden organisaatioiden tilanteeseen ja kehitykseen tietosuoja-asetuksen noudattamisessa. opinnäytetyön päämäärät saavutettiin ja organisaatioiden tilanteista saatiin hyvä, realistinen ja selkeä kuva. Toivottavasti tätä opinnäytetyötä voivat käyttää myös muut organisaatiot apuna oman tietosuojansa kartoituksessa ja kehittämisessä.

8.3 Kohdatut haasteet

Opinnäytetyötä kirjoittaessani en kohdannut varsinaisia haasteita. Tietosuoja-asetuksesta aiheena löytyi hyvinkin paljon tietoa, eikä tiedonhaku näin ollen ollut vaikeaa. Lähteitä löytyi paljon - tosin kirjallisia teoksia aiheeseen liittyen oli vähän. Verkkojulkaisuja sen sijaan oli runsaasti ja niistä oli helppo löytää haluttu tieto. Pieniä haasteita aiheutti myös asetuksen tulkinnanvaraisuus. Esimerkiksi aikaisemmin mainittujen tietoturvatoimien kuvailu oli asetuksessa todella tulkinnanvaraista. Muita kohdattuja haasteita oli kaiken opitun, nähdyn ja koetun koostaminen järkeväksi kokonaisuudeksi. Viimeinen kohtaamani haaste liittyi opinnäytetyön sisältämän tiedon rajaamiseen. Opinnäytetyöstä tuli sellainen kuin olin sen suunnitellutkin, vaikka kirjoittamisen aikana joutuikin välillä miettimään työn rakennetta, jäsennyksiä ja luettavuutta uudella tavalla.

LÄHTEET

.

1. Aalto-Setälä, M. 2016. EU:n tietosuoja-asetus tulee – valmistaudu ajoissa. Viitattu 5.6.2018 https://kauppakamari.fi/2016/03/31/eun-tietosuoja-asetus-tulee-valmistaudu-ajoissa/

2. Euroopan komissio. Mitä tarkoittaa 'sisäänrakennettu' ja 'oletusarvoinen' tietosuoja? Viitattu 14.6.2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fi

3. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Viitattu 27.4.2016. Saatavilla http://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX:32016R0679

4. Findwise.com viitattu 1.6.2018 https://findwise.com/en/gdpr-fi#1

5. Lukander Ruohola HTO. Viitattu 14.6.218 https://tietosuoja.info/

6. Sähköala.fi. Kulunvalvonta- ja työajanseurantajärjestelmät. Viitattu 15.8.2018 http://www.sahkoala.fi/kiinteistoala/Turvallisuus/fi_FI/kulunvalvonta

7. Tietosuojatyökalu.fi. Sanasto. Viitattu 4.6.2018 https://tietosuojatyökalu.fi/ohjeet/sanasto/

8. Tietosuojatyökalu.fi. Sanasto. Viitattu 9.8.2018 https://tietosuojatyökalu.fi/ohjeet/sanasto/

9. Tietosuojavaltuutetun toimisto. Viitattu 14.6.2018 https://tietosuoja.fi/tietosuojavastaavat

10. Tietosuojavaltuutetun toimisto. Henkilötietojen käsittely. Viitattu 4.6.2018 https://tietosuoja.fi/henkilotietojen-kasittely

11. Tietosuojavaltuutetun toimisto. Milloin henkilötietoja saa käsitellä? Viitattu 5.6.2018 https://tietosuoja.fi/kasittelyperusteet

12. Tietosuojavaltuutetun toimisto. Osoita noudattavasi tietosuojasäädöksiä. Viitattu 27.6.2018 https://tietosuoja.fi/osoitusvelvollisuus

13. Tietosuojavaltuutetun toimisto. Seloste käsittelytoimista. Viitattu 27.6.2018 https://tietosuoja.fi/seloste-kasittelytoimista

14. Tietosuojavaltuutetun toimisto. Usein kysyttyä EU:n tietosuoja-asetuksesta. Viitattu 29.5.2018 https://tietosuoja.fi/gdpr

15. Tirronen, H 2003. Tietoturva ja tietosuoja. Viitattu 15.8.2018 http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva.html

16. Valtiovarainministeriö 2009. Vahtiohje: Kuinka välttää tartunta. Viitattu 22.08.2018 https://www.vahtiohje.fi/web/guest/kuinka-valttaa-tartunta?p_p_id=56_INSTANCE_L5jW&p_p_lifecycle=0&p_p_state=exclusive&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_56_INSTANCE_L5jW_struts_action=%2Fjournal_content%2Fview&_56_INSTANCE_L5jW_groupId=10128&_56_INSTANCE_L5jW_articleId=30400&_56_INSTANCE_L5jW_viewMode=print

17. Valtiovarainministeriö 2016. Rekisteröidyn oikeudet. Viitattu 17.12.2018 https://www.vahtiohje.fi/web/guest/rekisteroidyn-oikeudet

18. Viestintävirasto 2017. Viestinnän salaus. Viitattu 9.8.2018 https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/palveluidenturvallinenkaytto/viestinnansalaus.html

19. Yksityisyydensuoja. Virusturva ja palomuuri. Viitattu 9.8.2018 https://www.yksityisyydensuoja.fi/virusturva-ja-palomuuri

20. Ylipartanen, A, Andreasson, A. 2015. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. Viitattu 1.6.2018 https://opitietosuojaa.fi/fi/oikeus/lait/eu-n-tietosuoja-asetus

21. Yrittäjät. Viitattu 14.6.2018 https://www.yrittajat.fi/blogit/nakokulma/yrittaja-pitaako-yritykseesi-nimittaa-tietosuojavastaava

22. Yrittäjät. Yrittäjä – pitääkö yritykseesi nimittää tietosuojavastaava? Viitattu 18.6.2018 https://www.yrittajat.fi/yrittajan-abc/yritystoiminnan-abc/yrittajan-tietosuojaopas/rekisteroityjen-oikeudet-570909