Haaga-Helia
ammattikorkeakoulu Oy

EU:n tietosuoja-asetukseen valmistautuminen mikroyrityksessä

Vesa Rautio

Opinnäytetyö
Liiketalouden koulutusohjelma
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Vesa Rautio

Koulutusohjelma
Liiketalous

Raportin/Opinnäytetyön nimi
EU:n tietosuoja-asetukseen valmistautuminen mikroyrityksessä.

Sivu- ja liitesivumäärä
49 + 5

Tämän toiminnallisen opinnäytetyön tarkoituksena on toteuttaa pienyrityksessä projekti, jossa yrityksen asiakas- ja markkinointirekisterien henkilötietojen käsittely saatetaan vastaamaan EU:n yleisen tietosuoja-asetuksen vaatimuksia. Projekti sisältää yrityksen tietosuojaselosteiden sekä muiden dokumenttien ja henkilötietojen käsittelyprosessien ja järjestelmien päivittämisen tietosuoja-asetuksen mukaisiksi. Projektin tuotoksena syntyi järjestelmiin tehtyjen muutosten lisäksi asetuksen mukainen ohjeistus henkilötietojen käsittelyyn sekä dokumentaatio yrityksen asiakkaiden henkilötietojen käsittelystä.

Opinnäytetyön tietoperustassa selvitetään datan sekä asiakas- ja henkilörekisterien merkitys yritysten toiminnalle sekä käydään läpi organisaation kannalta oleelliset kohdat ja vaatimukset EU:n tietosuoja-asetuksesta. Tietosuoja-asetuksen yhtenä tarkoituksena on ohjata organisaatioita kohti entistä läpinäkyvämpään henkilötietojen käsittelyä. Tietosuoja-asetus tuokin organisaatioille osoitusvelvollisuuden, joka tarkoittaa, että henkilötietolaista poiketen organisaatiolla on nyt velvollisuus osoittaa noudattavansa tietosuoja-asetusta. Tämä tarkoittaa käytännössä organisaatioissa noudatettavien käytänteiden dokumentointia.

Empiriassa on kuvattu yrityksessä toteutettu projekti, jolla päivitettiin rekisterien henkilötietojen käsittely täyttämään EU:n tietosuoja-asetuksen vaatimukset. Empiriassa käydään ensimmäisenä läpi projektisuunnitelman laadinta, joka sisältää projektin tavoitteen, kohderyhmät sekä projektin onnistumista mahdollisesti uhkaavat riskit. Projektisuunnitelman jälkeen kuvataan projektin toteutusvaihe. Kuvauksessa tarkastellaan muun muassa kohdeyrityksen asiakkaiden henkilötietojen kulkua asiakas- ja markkinointirekisteriin sekä rekistereistä yhteistyökumppaneille. Rekisterien sisältämät tiedot muodostuvat rekisteröidyiltä kerätyistä tiedoista sekä tilaus-, toimitusprosessin aikana syntyvistä tiedoista. Rekisterien tietoja siirretään kolmansille osapuolille pääasiassa vain sopimuksesta syntyneiden velvoitteiden toteuttamiseksi. Tällaisia kolmansia osapuolia ovat järjestelmien toimittajat, logistiikkakumppanit sekä maksutapojen toimittajat.

Projektin toteutusvaiheeseen päästiin vasta melko lähellä asetuksen siirtymäajan päättymistä. Toteutusvaiheessa suoritettiin kartoitusvaiheessa määritetyt toimenpiteet, jonka jälkeen uudistukset testattiin kolmivaiheisesti. Yksikkövaiheessa tarkastuslomakkeen avulla testattiin yksittäisten osa-alueiden vastaavuus tietosuoja-asetuksen kanssa. Järjestelmätestauksessa testattiin järjestelmään lisättyjen ominaisuuksien toimivuus. Viimeisenä toteutettiin toimenpidetestaus, jossa testattiin yksiköiden ja järjestelmän kokonaistoimivuutta käymällä läpi erilaisia skenaarioita.

Opinnäytetyön viimeisenä osuutena on pohdinta, jossa analysoidaan ja arvioidaan projektin ja opinnäytetyön onnistumista sekä mietitään keinoja projektin parantamiseksi. Pohdinnassa kiinnitetään huomiota haasteisiin, joita tietosuoja-asetuksen tulkinnanvaraisuudesta aiheutui projektin toteutukselle. Opinnäytetyönä toteutettu projekti onnistui suunnitelmien mukaan vaikka viimeinen kokonaistoimivuutta mittaava toimenpidetestaus saatiinkin suoritettua vasta lomien jälkeen elokuussa. Tietosuoja-asetuksen kannalta oleelliset kokonaisuudet saatiin valmiiksi suunnitellussa aikataulussa ennen tietosuoja-asetuksen siirtymäajan päättymistä.

Asiasanat
Tietosuoja-asetus, GDPR, henkilörekisteri, asiakasrekisteri

Sisällys

1 Johdanto

Erilaisiin rekistereihin kerätty tieto on yritysten toiminnan kannalta tärkeä resurssi. Siitä lähtien kun ihminen on alkanut harjoittaa kaupallista toimintaa vaihtotalouden muodossa, on esimerkiksi asiakastuntemuksella ollut merkitystä vaihdannan onnistumiseen. Toisen kanssa vaihdannassa takaisin saatu tavara on voinut olla heikompilaatuista kuin toisen kanssa, jolloin on pitänyt tietää kenen kanssa ensisijaisesti vaihdantaa kannattaa harjoittaa. Nykymaailmassa yritysten asiakastiedot ja muutkaan rekisterit eivät sijaitse pelkästään myyjän päässä, vaan tietoa tallennetaan suuria määriä yritysten järjestelmiin, joista tieto on helposti saatavilla ja sitä voidaan käsitellä ja analysoida. Teknologian kehitys on mahdollistanut entistä sujuvamman tiedon käsittelyn ja keräämisen. Kaupan käynnin globalisoituminen on myös lisännyt kerättävän tiedon määrää. Kerätyt tiedot sijaitsevat yritysten tietokannoissa, ja ne voivat sijaita eri puolilla maailmaa, jolloin niihin sovelletaan eri maiden lainsäädäntöjä.

Vuonna 2012 Euroopan komissio teki ehdotuksen EU-maiden henkilötietojen käsittelyä koskevien direktiivien sekä lainsäädäntöjen uudistamisesta. Uudistuksen tarkoituksena oli ajantasaistaa ja yhtenäistää EU-maiden toisistaan eroavat henkilötietojen käsittelyyn liittyvät lait sekä pyrkiä parantamaan henkilön mahdollisuuksia valvoa omien tietojensa käsittelyä.

Valitsin opinnäytetyön aiheeksi EU:n tietosuoja-asetuksen käyttöönoton pienyrityksessä, koska opinnäytetyön tullessa ajankohtaiseksi olin jo työstämässä omalla työpaikallani EU:n tietosuoja-asetuksen dokumentointia työpaikkani rekisterien ylläpidon käytänteistä. Aihe on ajankohtainen sillä EU:n yleisen tietosuoja-asetuksen kahden vuoden siirtymäaika päättyi 24.5.2018, jonka jälkeen asetusta alettiin soveltamaan kaikissa EU:n jäsenmaissa ja monelle pienyritykselle asetuksen vaatimukset ovat vielä asetuksen voimaantultuakin epäselviä.

EU:n tietosuoja-asetus liittyy kaikkeen henkilötietojen käsittelyyn ja on näin ollen ajankohtainen kaikissa organisaatioissa, joissa käsitellään henkilötiedoiksi luokiteltavia tietoja. Uusi tietosuoja-asetus tuo yrityksille uusia velvollisuuksia ja antaa rekisteröidyille uusia oikeuksia omien tietojen käsittelyyn liittyen.

EU:n uusi tietosuoja-asetus on herättänyt paljon keskustelua, ja keskustelua on monesti hallinnut korvausvastuu ja sakkokäytännöt, joista on levinnyt myös liioiteltua ja ajoittain vääräkin tietoja. Keskusteluista ja erilaisista koulutuksista huolimatta monille on edelleen epäselvää mitä kenenkin pitää tehdä ja kuka on vastuussa mistäkin. Yritys saattaa kerätä

henkilötietoja verkkokaupan kautta, jonka ylläpidosta vastaa verkkokauppa-alustan toimittaja. Henkilörekisteri sijaitsee kuitenkin kolmannen osapuolen palvelimella, joka vastaa rekisterin toimivuudesta ja varmuuskopioinnista. Edellä mainitussa tilanteessa pienyrittäjä saattaakin ajatella vastuun kokonaan tai osittain olevan palveluiden toimittajilla. Todellisuudessa rekisterinpitäjän vastuulla on pystyä näyttämään, että yritys jolta tietojen säilytyspalvelu on ostettu, täyttää EU:n tietosuoja-asetuksessa määritetyt vaatimukset ja käsittelee tietoja rekisterinpitäjän ohjeiden mukaisesti.

1.1 Yrityksen esittely

Kohdeyritys XXX on pieni, tällä hetkellä kuusi henkilöä työllistävä ja mikroyritykseksi luokiteltava yritys, jonka toimialana on työkalu- ja tarviketukkukauppa. Yritys harjoittaa maahantuontia Kaukoidästä, Yhdysvalloista sekä useista Euroopan maista. Tuotteet myydään pääasiassa jälleenmyyjien kautta, joita ovat rakennus- ja turvallisuusalan tarvikkeita myyvät yksityiset liikkeet sekä kauppaketjut. Yritys toimittaa tuotteita myös kalusteteollisuuden asiakkaille sekä kuntasektorille. Yrityksen varasto- ja logistiikkatoiminnot sijaitsevat Itä-Uudellamaalla, josta tilaukset toimitetaan kaikkialle Suomeen. Yritys toimittaa jonkin verran tuotteita myös vientiin. Pääasiallisia vientimaita ovat Ruotsi, Venäjä, Yhdysvallat ja Viro.

Yritykselle tulevat tilaukset otetaan vastaan edelleen pääasiassa puhelimitse, jonka jälkeen työntekijät syöttävät tilaukset yrityksen toiminnanohjausjärjestelmään. Kasvavassa määrin tilauksia tulee myös sähköpostitse sekä verkkokaupan kautta. Kauppaketjujen on mahdollista tehdä tilaukset omasta järjestelmästään suoraan yrityksen järjestelmään EDI-yhteyden välityksellä. Yrityksellä on verkkokauppa, joka toimii yhtenä sopimusasiakkaiden tilauskanavana. Verkkokaupan kautta tuotteita myydään myös kuluttaja-asiakkaille sekä yritysasiakkaille, jotka eivät ole yrityksen sopimusasiakkaita.

Yritykselle muodostuu erityyppisiä rekistereitä kaupankäynnin, rekrytointien ja markkinointitoimenpiteiden seurauksena. Yritys ei osta tai hanki muuten osoitetietoja ulkopuolisilta toimijoilta, vaan yrityksen markkinointirekisteri muodostuu kaupankäynnin seurauksena tai asiakkaiden tilatessa yrityksen sähköisen uutiskirjeen. Rekistereihin kerättyjä tietoja hyödynnetään tilausten toimittamisessa, laskuttamisessa, markkinoinnissa sekä tuotteiden ja tuotevalikoiman kehittämisessä.

1.2 Toiminnallisen opinnäytetyön taustat ja rajaus

Kohdeyrityksellä on useita rekistereitä, joihin on kerätty erityyppisiä henkilötietoja, tästä syystä EU:n tietosuojauudistus käynnisti yrityksessä asetukseen liittyvien velvoitteiden

selvityksen sekä tietosuojaselosteiden täydentämisen ja tietosuojaan liittyvien käytänteiden dokumentoinnin. Asetuksen mukaan rekisterinpitäjän tulee tarvittaessa osoittaa käsittelevänsä henkilötietoja asetuksen vaatimalla tavalla. Myös toimeksiantosopimusten sisällöt eri toimijoiden kanssa, joille henkilötietojenkäsittely on ulkoistettu, jouduttiin tarkastamaan.

Päätin rajata opinnäytetyön käsittelemään mikroyrityksen asiakkaista koostettuja henkilörekistereitä, jotka eivät sisällä tietosuoja-asetuksen yhdeksännessä artiklassa määriteltyjä erityisiä henkilötietoryhmiä. Tällaisia ryhmiä ovat muun muassa etnistä alkuperää, poliittisia mielipiteitä, seksuaalista suuntautumista, uskonnollisia tai filosofisia mielipiteitä sisältävät tietoryhmät. Edellä mainittujen arkaluontoisten tietojen käsittely on pääsääntöisesti kiellettyä, mutta tietoja voidaan kuitenkin käsitellä, mikäli tietojen käsittelylle on jokin tietosuoja-asetuksessa määritetty erityinen peruste. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 40-41.)

Opinnäytetyön painopiste on pienen yrityksen henkilötietojen käsittelyn organisatorisissa toimissa, joita ovat ohjeistusten, sääntöjen ja käytänteiden laadinta, henkilökunnan koulutus ja opastustoimenpiteet. Työssä ei paneuduta tarkemmin erilaisiin teknisiin tietoturvaratkaisuihin kuten salauksiin, tiedon siirron tai varmuuskopioinnin teknisiin järjestelyihin.

1.3 Toiminnallisen opinnäytetyön tavoitteet ja rakenne

Tämän toiminnallisen opinnäytetyön päätavoitteena on saattaa kohdeyrityksen asiakas- ja markkinointirekisterien sisältämien henkilötietojen käsittely vastaamaan EU:n yleisen tietosuoja-asetuksen vaatimuksia. Opinnäytetyön toisena tavoitteena on luoda selkeä ja helposti ymmärrettävä kuvaus toimista, jotka tulee suorittaa kun pieni yritys aloittaa henkilötietojen keräämisen ja käsittelyn. Prosessin aikana yrityksen henkilötietojen käsittely muuttuu vastaamaan uuden tietosuoja-asetuksen vaatimuksia ja tuloksena syntyy ohjeistus sekä dokumentaatio vallitsevista käytänteistä.

Alatavoitteena on tuoda esiin ongelmakohtia, joita työn kohteena olevassa yrityksessä kohdataan sekä tarkastella kriittisesti mahdollisia ristiriitaisuuksia, joita tietosuoja-asetuksen vaatimusten ja käytännön välillä esiintyy.

Opinnäytetyöprosessissa syntyy kuvaus yrityksen käytännön prosessista, joka linkittyy vahvaan tietoperustaan. Opinnäytetyön tietoperusta sekä prosessin kuvaus on muille yrityksille hyödyllisempi tuotos, kuin prosessin tuloksena syntyvä dokumentaatio, sillä jokainen yritys joutuu luomaan dokumentaation omien rekistereidensä laadun ja laajuuden

sekä käyttötarkoitusten mukaan. Tietoperusta sekä prosessinkuvaus antavat yritykselle suuntaviivat miten prosessi tulisi hoitaa. Pyrin tuottamaan mahdollisimman selkeän toimintaohjeistuksen pienyrityksen tarpeisiin, jonka avulla henkilötietojen käsittely kohdeyrityksessä on mahdollisimman mutkatonta ja läpinäkyvää.

Opinnäytetyön raportti muodostuu viidestä osasta. Ensimmäisenä on johdanto, jossa käydään läpi opinnäytetyön taustat ja rajaukset sekä tavoitteet. Johdannossa esitellään myös työn kohteena oleva yrityksen toimintaa. Toisessa luvussa perehdytään erilaisiin yrityksissä oleviin rekistereihin ja niiden käyttötarkoituksiin. Kolmannessa luvussa käsitellään Euroopan unionin uutta tietosuoja-asetusta ja sen sisältöä. Tämän jälkeen neljännessä luvussa kuvataan produktin suunnittelu ja toteutus. Raportin viimeisessä osassa arvioidaan produktin toteutusta, kohdattuja haasteita sekä asetettujen tavoitteiden toteutumista. Pohdinnassa esitetään myös toimia, joilla prosessia on mahdollista kehittää.

2 Datan merkitys yritykselle

Tiedon kasvavaa merkitystä nyky-yhteiskunnassa kuvastaa sanonta ”tieto on uusi öljy”, jota on viljelty erilaisissa markkinointialan kirjoituksissa viime vuosina. Tiedon merkityksen kasvu näkyy myös yritysten eri osastojen tehtävissä. Taloushallinnon tehtävänä on perinteisesti ollut tarkastella yrityksen kiinteää omaisuutta ja määrittää tälle arvo. Nykyaikana kuitenkin suuri osa yritysten omaisuudesta voi olla aineetonta pääomaa, kuten brändejä, jakelukanavia, immateriaalioikeuksia, asiakkaita sekä tietoa, näille aineettomille pääomille taloushallinto joutuu nyt määrittämään arvon. Aineettoman pääoman arvon määrittäminen luotettavasti on vaikeaa, ja etenkin tiedon kohdalla arvon määrittäminen voi olla erityisen haasteellista, sillä kerätyn tiedon arvo on aika- ja kontekstisidonnaista. Se mikä on arvotonta tänään, voi olla arvokasta huomenna. Tiedon arvon ymmärtäminen on kuitenkin tärkeää, sillä yritysten keräämää dataa pidetään jo useasti toimialasta riippumatta yrityksen tärkeimpänä omaisuuseränä. (Hellman & Värilä 2009, 75; Alanko & Salo 2013, 4,10.)

Tiedon merkityksestä puhuttaessa esiin nousee Big data, joka on viime vuosien puhutuimpia businessmaailman termejä. Big data tarkoittaa käytännössä eri lähteistä kerättyä erittäin suurta ja nopeasti kasvavaa vaihtelevan muotoista tietomassaa. Big dataa voidaan kerätä monista eri paikoista käyttämällä elektronisia tai ei-elektronisia kanavia, kuten ostohistoriatietoja, verkkokaupan analytiikkaa, erilaisten sähköisten markkinointitoimenpiteiden onnistumistietoja, RFID-tunnistetietoja sekä asiakastyytyväisyyskyselyitä ja asiakaspalautteita (Rubanovitsch & Aminoff 2015, 44-45; Alanko & Salo 2013, 4.)

Sähköisten tiedonkeräysmenetelmien lisääntyminen tarkoittaa tiedon keräämisen helpottumista ja nopeutumista. Enää ei tarvitse jalkautua fyysisesti asiakkaiden pariin tekemään asiakastyytyväisyyskyselyä, vaan asiakkaiden tyytyväisyyttä voidaan tiedustella sähköpostilla, verkkosivuille sijoitettavilla lomakkeilla tai palvelupisteen läheisyyteen sijoitettavalla palautelaitteella. Kun tiedon kerääminen on muuttunut vaivattomammaksi ja vähemmän resursseja vaativaksi, yrityksille saattaa muodostua niin paljon tietoa, että yrityksen päätöksenteko halvaantuu. Yritys saattaa epäillä tiedon luotettavuutta eikä siksi uskalla käyttää sitä. Yritykselle on myös saattanut kertyä paljon monipuolista dataa monista eri lähteistä eikä yritys enää tiedä mitä tietoa sen pitäisi käyttää. Mikäli yritys onnistuu ylittämään kaksi edellä mainittua karikkoa, saattaa yrityksen datan hyödyntäminen vielä kaatua datan ylianalysointiin, jolloin yritys jatkaa tiedon analysoimista loputtomiin. (Pajunen 2016.)

Näkemykseni mukaan liiketalouden alalla työskentelevät ovat yhtä mielisiä tiedon suuresta merkityksestä yritysten ja organisaatioiden kilpailukyvylle. Tiedon määrä ei kuitenkaan korreloi suoraan arvon kanssa ja kaikki kerätty tieto ei välttämättä ole tärkeää. Tiedon arvo yritykselle tai organisaatiolle riippuu paljon yrityksen tai organisaation kyvystä jalostaa ja hyödyntää saatua tietoa omassa toiminnassaan (Laihonen 2013).

2.1 Yritysten rekisterit

Henkilötietolaissa henkilörekisteri on määritetty henkilötietoja sisältäväksi tietojoukoksi, joka muodostuu käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä. Tietojoukko on järjestetty kortistoksi, luetteloksi tai jotenkin muuten edellä mainittuihin verrattavilla tavoilla. Henkilötietolaissa määritettyä henkilörekisteriä voidaan käsitellä joko osittain tai kokonaan automaattista tietojenkäsittelyä käyttäen. (Henkilötietolaki 22.4.1999/523.)

Henkilötietolain määritettä henkilörekisteristä voidaan käyttää myös määritettäessä mitä tahansa rekisteriä. (Hanninen ym. 2017, 22) määrittelevät kirjassaan rekisterin yhtenäiseksi tietojoukoksi, jonka sisältämät tiedot on kerätty samaa käyttötarkoitusta varten. Tekninen tapa, jolla rekisteri on toteutettu, ei siis vaikuta siihen katsotaanko tietojoukko rekisteriksi.

Tiedon keräämiseen käytettävien lähteiden määrän kasvaminen tarkoittaa myös sitä, että yrityksille ja organisaatioille muodostuu eri paikkoihin ja –järjestelmiin erityyppisiä rekistereitä joihin tietoa kerätään. Yrityksellä voi olla käytössään oma järjestelmä tuotannonohjaukselle, taloushallinnolle, markkinoinnille ja asiakashallintaan. Pienellekin yritykselle voi

kertyä lähes huomaamatta useita erityyppisiä rekistereitä, etenkin jos yritys harjoittaa verkkokaupan kautta tavarakauppaa kuluttajille ja tuotteita ostetaan useilta toimittajilta.

Toimittajarekisteri yritykselle muodostuu kun yritys ostaa myytäviä tuotteitaan toimittajilta ja kerää toimittajien tietoja yhteen. Yritys tarvitsee todennäköisesti toiminnan harjoittamiseen myös erilaisia laitteita, järjestelmiä sekä muiden yritysten tarjoamia palveluita. Näiden hankintaan tarvittavat yhteystiedot voidaan kerätä yhteistyökumppanirekisteriin. Toimittaja ja yhteistyökumppanirekisterin lisäksi yrityksellä voi olla erikseen alihankkijoista koostettu rekisteri.

Yrittäjän palkatessa ensimmäisen työntekijänsä muodostuu työntekijän tiedoista työntekijärekisteri. Suuressa organisaatiossa voi olla olemassa olevien työntekijöiden tiedoista koostuvan rekisterin lisäksi rekisteri työnhakijoista. Rekrytoinnin aikana kerätyistä henkilötiedoista ja testien tuloksista muodostuu henkilötietorekisteri, mikäli työnantaja tallentaa ja säilyttää tietoja myöhempää käyttöä varten. (Fondia-VirtuaaliLakimies 2018).

Nykyaikana yrityksellä voi olla asiakasrekisterin lisäksi erillinen markkinointirekisteri, johon on kerätty olemassa olevien asiakkaiden sekä potentiaalisten asiakkaiden tietoja. Yritys tai organisaatio voi kerätä tietoa myös yrityksen verkkosivujen ja verkkokaupan vierailijoista erillisellä kävijäseurantatyökalulla. Seurantatyökalu käyttää seurantatiedon keräämiseen käyttäjän päätelaitteelle tallennettavaa pientä tekstitiedostoa, evästettä (engl. Cookie). Evästeiden välityksellä kerätystä tiedosta muodostuu rekisteri, jonka sisältöä voidaan suodattaa ja analysoida kävijäseurantaohjelman avulla.

Edellä mainitut esimerkit on helppo mieltää rekistereiksi, koska rekisteriin kirjattu tieto on luettavassa muodossa ja rekisterin tiedot ovat helposti selattavissa ja tarvittaessa tiedot voidaan myös tulostaa paperille. Vaikeammin rekistereiksi hahmotettavia ovat kamera- ja kulunvalvonnan seurannasta muodostuvat tallenteet. Kameravalvonnan tallenteista muodostuu henkilörekisteri, sillä kameravalvonnan tallentamasta kuvasta luonnollinen henkilö on tunnistettavissa esimerkiksi fyysisen ja geneettisen ominaisuuden perusteella. Näin ollen tallenne täyttää tietosuoja-asetuksen neljännessä artiklassa määritetyn henkilötiedon kriteerit. (Yleinen tietosuoja-asetus 2016/679, 4 artikla.)

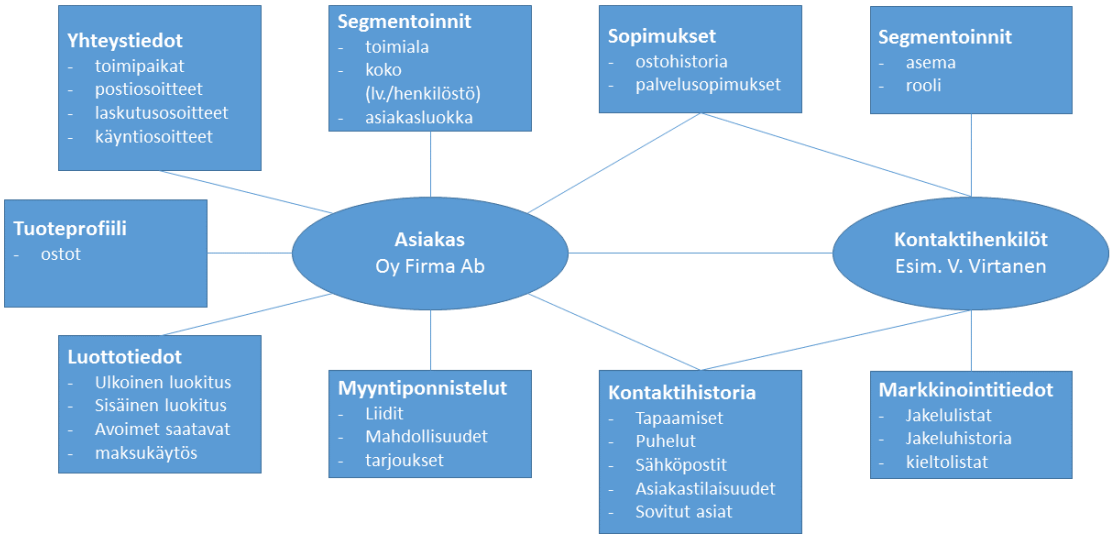
2.2 Rekistereihin kerättävä tieto

Yrityksissä oleva tieto voidaan jakaa kahteen eri kategoriaan; hiljaiseen tietoon ja näkyvään tietoon. Hiljaista tietoa syntyy yrityksen toiminnassa esimerkiksi tilaus- toimituspro-

sessin aikana. Prosessin kulusta vastaavat tuntevat asiakkaat ja osaavat toimia asiakkaiden toiveiden ja suosimien käytäntöjen mukaan. Hiljanen tieto on siis yrityksen jokapäiväisessä toiminnassa syntyvää kokemusperäistä tietoa. Näkyvää tietoa puolestaan on kirjoitettu tai muuten dokumentoitu tieto. Hiljainen tieto voidaankin dokumentoida esimerkiksi CRM-järjestelmään, jolloin se muuttuu näkyväksi tiedoksi. Yleensä asiakkaisiin liittyvää näkyvää tietoa ovat muun muassa nimet, osoitteet, muut yhteystiedot, historiatiedot, jakelu- ja kieltolistat, sopimukset, reklamaatiot ja tarjoukset. (Oksanen 2010, 150-153.)

Yritysten asiakkaistaan keräämä tieto voi koostua hyvinkin erityyppisistä asioista. Kerättävien tietojen laajuuteen ja määrään vaikuttaa muun muassa yrityksen toimiala ja kilpailutilanne, kohderyhmät sekä yrityksen toiminnan taso. Suuryritys, joka toimii useassa myynti- ja markkinakanavassa, voi kerätä tietoa asiakkaiden käyttäytymisestä hyvinkin laajasti, hyödyntäen käyttämiään sähköisiä- ja ei-sähköisiä-kanaviaan. Vastaavasti pienen b2b-sektorilla toimivan palveluyrityksen asiakasrekisteri voi muodostua hyvin suppeasta tietomäärästä, joka sisältää yhteystietojen lisäksi vain ostohistoriatiedot.

Asiakastietojen ajatellaankin monesti olevan pelkät kontaktitiedot, mutta ne muodostavat vain pienen osan asiakkaasta kerättävästä tiedosta. Tärkeämpinä osina asiakkuuden hoitamisen kannalta voidaan pitää segmentointi- ja historiatietoja, sillä näistä tiedoista muodostuu yrityksen asiakkuuden kuva. On myös huomioitava, että CRM-järjestelmiin ei kerätä pelkästään asiakkaisiin liittyvää tietoa, vaan myös muihin sidosryhmiin, kuten toimittajiin, kumppaneihin ja kilpailijoihin liittyvää tietoa. Näihin tietoihin tulee suhtautua vastaavalla tarkkuudella, ja tietojen ylläpitämisessä ja kartuttamisessa tulee käyttää samanlaista logiikkaa kuin asiakastietojen hallinnassa. (Oksanen 2010, 148.)



Kuvio 1. Yksinkertaistettu esimerkki B2B-asiakastiedosta (Oksanen 2010, 149)

Tiedon keräystavat ja käsittelytavat ovat mullistuneet kaksituhattaluvulla teknologian kehityksen myötä. Yritykset ovat alkaneet kerätä asiakkaalta saatujen perustietojen lisäksi tietoa asiakkaiden käyttäytymisestä mitä erilaisimmalla tavoilla. Tietoja asiakkaista voidaan kerätä muun muassa navigointipalveluista, sosiaalisesta mediasta, kanta-asiakaskorteista, video- ja kuvatallenteista. Kerätyn tiedon kautta yritykset pyrkivät analysoimaan asiakkaan ostokäyttäytymistä ja ennakoimaan tulevaa. (Rubanovitsch & Aminoff 2015, 117.)

Vielä muutama vuosi sitten yritysten ajattelua internetissä leimasi asiakasmääriin keskittyminen. Yritykset pyrkivät haalimaan suuria määriä asiakaskontakteja vaikka suurinta osaa näistä ei pystytty hyödyntämään (Hellman & Värilä, 2009, 38). Nykyään verkkomarkkinoinnissa alaa valtaa inbound-markkinointi, jossa verkkoon tuotetun sisällön kautta pyritään hankkimaan yrityksen tuotteista ja palveluista oikeasti kiinnostuneiden kontaktitietoja. Inbound-markkinoinnin onnistumiseen vaikuttaa merkittävästi valitun kohderyhmän tunteminen. Kohderyhmästä tarvitaan riittävästi oikeanlaista tietoa, jotta kohderyhmä opitaan tuntemaan riittävän hyvin ja heille pystytään luomaan merkityksellistä sisältöä. (Salescommunications 2018.)

Teknologian kehittyminen on mahdollistanut entistä tarkemman mittaamisen ja markkinointitoimenpiteiden kohdentamisen. Evästeitä käyttämällä voidaan kerätä hyvinkin monipuolista ja yksityiskohtaista tietoa asiakkaan toiminnasta verkkosivuilla tai verkkokaupassa. Evästeillä saadaan tietoja muun muassa vierailijan IP-osoitteesta sekä mistä verk-

kotunnuksesta vierailija on tullut tai mitä hakusanoja käyttämällä vierailija on päätynyt yrityksen sivuille. Evästeet mahdollistavat myös tiedon keräämisen vierailijan käyttämästä selaimesta ja päätelaitteesta sekä tarkan seurannan vierailijan selausreitistä yrityksen sivuilla; millä sivuilla vierailija on käynyt sekä miten kauan mitäkin sivua on katseltu. (Viestintävirasto 2017.)

Yritysmarkkinoilla ostopäätöksen tekevät yksilöt tai yksilöistä muodostuvat ryhmät, joiden ostokäyttäytymiseen vaikuttaa yleisesti organisaatioiden ominaispiirteet ja tarpeet, suhteet yrityksen sisällä sekä yrityksen ulkopuolella (Wood 2017, 58.) Yritys saattaakin kerätä omaan CRM-järjestelmäänsä (Customer Relationship Management) tietoja edellä mainituista asiakasyritysten ostokäyttäytymiseen vaikuttavista tekijöistä sekä sisäisiin valtasuhteisiin liittyvistä huomioista. Klingen mukaan myös asiakkaan kanssa käydyt keskustelut olisi hyvä kirjata CRM-järjestelmään, jotta asiakaspalvelijan vaihtuessa asiakkaalle voidaan tarjota joustavaa ja yhtenäistä palvelua. (Klinge 2017).

2.3 Rekistereissä olevan tiedon hyödyntäminen

Rekistereihin kerätyn tiedon määrä kasvaa jatkuvasti ja joillakin yrityksillä onkin hallussaan kattava tietomäärä asiakkaistaan. Pelkkä laaja tietomäärä ei kuitenkaan takaa tehokkaasti hyödynnettävää tietoa. Tiedon laadukas analysointi edellyttää, että kerätty tieto on laadukasta. (Oksanen 2010, 176-177.)

Laadukaskin tieto on hyödytöntä, mikäli ei tiedetä mihin sitä käytetään tai sitä ei osata jalostaa tarkoitukseen sopivaksi. Jotta yrityksen keräämän tiedon analysoinnista olisi yritykselle liiketoiminnallista hyötyä, yrityksen pitääkin ensin selvittää itselleen mitä se aikoo analytiikan avulla saavuttaa. (Nahkala 2015.)

Nykyään yritykset panostavat entistä enemmän resursseja sähköisiin tilausjärjestelmiin sekä sähköiseen kaupankäyntiin. Asiakkaiden tunnistaminen sekä interaktiivinen viestintä ja mainonta ovat sähköisten järjestelmien ohella yritysten investointien kohteina. Näihin kohteisiin tehtyjen investointien tuloksellisuutta on monesti mitattu tuotteiden kautta. Investointien kasvaessa ja niiden ollessa pidempiaikaisia sekä vaatiessa laajennuksia ja ylläpitoa, investointien onnistuminen on muodostunut yritysten toiminnan kannalta kriittiseksi. Myös näiden investointien onnistumisten mittaamisessa sekä yrityksen asiakkuusraporttien ja analyysien tehokkaassa hyödyntämisessä tärkeäksi tekijäksi muodostuu kerätyn tiedon oikeanlainen mittaaminen sekä saatujen analyysien oikea tulkinta. (Hellman & Värilä 2009, 36-40, 99-100.)

Rekistereihin kerätyn datan käsittely erilaisilla analyysityökaluilla sekä markkinointiautomaatiota ja luottamuksellista vuoropuhelua hyödyntämällä pystytään tietomassasta erottamaan potentiaaliset ostajat (Rubanovitsch & Aminoff 2015, 125). Asiakkaista kerätyn tiedon avulla asiakkaat voidaan jaotella segmentteihin. Segmentointi voidaan suorittaa kahdella tavalla, staattisesti tai dynaamisesti. Staattisessa segmentoinnissa asiakkaat jaetaan määriteltyihin segmentteihin. Asiakkaat pysyvät määritetyissä segmenteissä kunnes niitä muutetaan. Dynaamisessa segmentoinnissa asiakkaat jaotellaan staattisen segmentoinnin tapaan soveltuviin segmentteihin. Mutta toisin kuin staattisessa segmentoinnissa asiakkaiden luokittelu on jatkuva prosessi. Dynaamisessa segmentoinnissa luokittelukriteerit poikkeavat myös staattisessa segmentoinnissa käytetyistä kriteereistä. Dynaamisessa segmentoinnissa segmentit valitaan asiakassuhteen kehitysvaiheesta, asiakkaan liiketoimintaan liittyvistä asioista tai asiakkaan ympäristössä tapahtuvista muutoksista. Luokittelua voidaan tehdä myös asiakkaan omaan toimintaan liittyvistä asioista, kuten asiakkaan reagoinnista uutiskirjeeseen tai keskusteluun chat-palvelussa. (Oksanen 2010, 178-179; Lemminki, 2016.)

Yrityksen evästeillä keräämää tietoa voidaan analysoida ja tutkia web-analytiikkatyökaluilla kuten Googlen Analyticsilla, Snoobi Analyticsilla tai Pikwik-kävijäseurantaohjelmistolla. Tietojen avulla verkkosivun sisältöä voidaan kehittää vastaamaan paremmin vierailijoiden ja asiakkaiden tarpeita. Digitaalisissa kanavissa toteutetun verkkomainonnan tehokkuutta pystytään mittaamaan paljon tarkemmin kuin perinteisissä mainoskanavissa toteutettua mainontaa. Yhdistämällä verkkomainonnasta saadut tiedot kävijäseurannasta saatuihin tietoihin, yritys pystyy kohdistamaan markkinoinnin jatkotoimenpiteet potentiaalisille asiakkaille. Seurantatietoja analysoimalla yritys pystyy rakentamaan markkinointiviestin sisällön kohderyhmän kiinnostuksen mukaiseksi ja pyrkiä näin vahvistamaan asiakkaan ostopäätöstä. (Asml 2012, 5.)

Yritysten keräämää tietoa voidaan siis hyödyntää tehokkaasti ja monipuolisesti ja moniin eri tarkoituksiin, kunhan ensi on varmistettu tiedon laadukkuus ja selvitetty mihin tietoa halutaan käyttää.

3 EU:n tietosuoja-asetus 2016/679

Teknologian kehittyessä ja yritysten toiminnan siirtyessä entistä enemmän kansallisten rajojen yli, Euroopan unionissa haluttiin yhtenäistää jäsenvaltioiden henkilötietojen käsittelyä ja tietosuojaa koskevat säännökset sekä vahvistaa rekisteröityjen oikeuksia omien tietojensa käsittelyn valvontaan ja parantaa henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä. EU:n tietosuoja-asetus (GDPR=General Data Protection Regulation) tuli voimaan

24.5.2016. Asetuksen siirtymäaika oli kaksi vuotta ja asetusta alettiin soveltamaan Euroopan unionin alueella 25.5.2018. Siirtymäajan päättymisen jälkeen henkilötietojen käsittelyn tuli viimeistään täyttää tietosuoja-asetuksen vaatimukset. (Talus, Autio, Hänninen, Pihamaa & Kantonen 2017, 9.)

3.1 Tietosuoja-asetuksen soveltaminen henkilötietojen käsittelyyn

Tietosuoja-asetusta sovelletaan lähes kaikkeen Euroopan unionin alueella tapahtuvaan henkilötietojen käsittelyyn. Tietosuoja-asetuksessa henkilötiedoilla tarkoitetaan kaikkea sellaista tietoa, jonka avulla luonnollinen henkilö voidaan tunnistaa suoraan tai epäsuorasti rekisterissä olevan tiedon perusteella. Tällaisia tietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitieto. Tunnistetietoina pidetään myös luonnollisen henkilön fyysisiä, fysiologisia tai geneettisiä ominaisuuksia, joista henkilö voidaan tunnistaa. Vaikka rekisterinpitäjä tai henkilötietojen käsittelijä sijaitsisivat Euroopan unionin ulkopuolella, mutta henkilötietoja käsitellään heidän EU:n alueella sijaitsevassa toimipaikassaan, joutuvat he käsittelemään henkilötietoja asetuksen velvoittamalla tavalla. (Hanninen ym. 2017, 19-20.)

Tietyissä tilanteissa asetusta sovelletaan myös henkilötietojen käsittelyyn, jossa unionin alueella olevan rekisteröidyn henkilötietoja käsitellään unionin ulkopuolella. Tällaisia tilanteita ovat rekisterinpitäjän tai henkilötietojen käsittelijän suorittama henkilötietojen käsittely, joka perustuu palvelun tai tavaran tarjoamiseen tai myymiseen unionin alueella olevalle rekisteröidylle. Myös näiden rekisteröityjen käyttäytymisen seurannasta kerättyjen tietojen käsittelyyn sovelletaan tietosuoja-asetusta. Esimerkiksi, mikäli Euroopan unionin ulkopuolella toimiva verkkokauppa haluaa myydä tuotteitaan Suomeen, joutuu verkkokauppa huomioimaan henkilötietojen käsittelyssään tietosuoja-asetuksen vaatimukset. (Hanninen ym. 2017, 18-20.)

Kaikki markkinat muodostuvat ihmisistä. Markkinat voidaan kuitenkin jakaa karkeasti kahteen osaan; kuluttajamarkkinoihin ja yritys/organisatorisiin markkinoihin. Kuluttajamarkkinoilla luonnolliset henkilöt ostavat tuotteita ja palveluita omaan käyttöönsä. Yritysmarkkinat taas muodostuvat oikeudellisista henkilöistä, kuten yhdistykset ja säätiöt sekä eri yhtiömuotoiset yritykset, joiden luonnollisista henkilöistä koostuva henkilökunta, ostavat tuotteita tai palveluita organisaationsa lukuun. (Wood 2017, 48.)

B2b-sektorilla toimivan yrityksen asiakasrekisteriin keräämä tieto on oikeushenkilöön kohdistuvaa tietoa, johon EU:n tietosuoja-asetusta ei sovelleta. Kuitenkin asiakasyrityksen päättäjistä ja yhteyshenkilöistä on saatettu kerätä henkilötiedoiksi luokiteltavia tietoja, ku-

ten nimi, puhelinnumero tai sähköpostiosoite. Näistä luonnollista henkilöä koskevista tiedoista yritykselle muodostuu asiakasrekisterin lisäksi henkilötietorekisteri, johon sovelletaan tietosuoja-asetusta. (Hanninen ym. 2017, 15, 20.)

Yrityksen koolla ei ole merkitystä velvollisuuteen noudattaa tietosuoja-asetusta, sillä myös yksityisen elinkeinonharjoittajan, jolla ei ole palkattua työvoimaa tulee huomioida tietosuoja-asetuksen vaatimukset, mikäli yritys myy tai markkinoi palveluitaan tai tuotteitaan kuluttajille ja on kerännyt kuluttajien henkilötietoja asiakasrekisteriinsä. Yritys on velvoitettu toimimaan tietosuoja-asetuksen vaatimusten mukaisesti myös silloin kun sillä on yksikin työntekijä palveluksessaan. Vaikka yritys olisi ulkoistanut palkanlaskennan esimerkiksi tilitoimistolle, on yrityksen rooli edelleen rekisterinpitäjä ja näin ollen velvoitettu toimimaan tietosuoja-asetuksen mukaisesti. (Hanninen ym. 2017, 15, 25.)

Tietosuoja asetus koskee siis kaikkia organisaatioita, jotka käsittelevät henkilötietoja. Käsittelyn laajuus, luonne tai käsittelyyn käytetyt menetelmät ja teknologiat eivät vaikuta yrityksen velvollisuuteen noudattaa tietosuoja-asetusta. Asetuksessa määritetyt velvoitteet kuitenkin riippuvat organisaation rekisterin sisältämien henkilötietojen laadusta sekä laajuudesta. Organisaatioon kohdistuviin velvoitteisiin vaikuttavat myös henkilötietojen käsittelyyn liittyvät riskit sekä yrityksen henkilötietojen käsittelyn nykyiset käytännöt. (Talus ym. 2017, 9,11.)

3.2 Tietosuoja-asetuksen ulkopuolelle jäävä henkilötietojen käsittely

Tietosuoja-asetusta ei sovelleta luonnollisen henkilön omaan tarkoitukseen suorittamaa henkilötietojen käsittelyä, joka ei ole sidoksissa kaupalliseen tai ammatilliseksi luokiteltavaan toimintaan. Tällaista toimintaa voi olla esimerkiksi henkilön oman osoitteiston pitäminen kirjeenvaihtoa tai muuta sosiaalista yhteydenpitoa ja verkostoitumista varten. Asetusta ei myöskään sovelleta anonyymeihin tietoihin, joissa rekisteröidyn tunnistettavuus on poistettu niin, ettei henkilöä enää voida tunnistaa. Tällaisia anonyymeja rekistereitä voivat olla erilaiset tilasto- ja tutkimustarkoituksia varten kerätyt rekisterit. Tietosuoja-asetus ei koske kuolleiden henkilöiden henkilötietojen käsittelyä, vaan kuolleiden henkilöiden kohdalla jäsenvaltioille on annettu mahdollisuus säätää kuolleita koskevista säädöksistä. (Yleinen tietosuoja-asetus 2016/679, (18), (26), (27).)

3.3 Rekisterinpitäjän ja henkilötietojen käsittelijän vastuut ja velvollisuudet

Harva yritys hoitaa nykypäivänä kaikki yrityksen hallinnoimat rekisterit itse. Etenkin pienyrityksissä on järkevää käyttää toisia yrityksiä hoitamaan oman ydintoiminnan ulkopuolelle jäävät toiminnot. Tällaisia useasti ulkoistettuja toimintoja ovat muun muassa kirjanpito,

palkanmaksu, markkinointi, vartiointi sekä verkkokaupan ja toiminnanohjausjärjestelmän tekninen ylläpito.

Tietosuoja-asetuksessa rekisterinpitäjäksi katsotaan yritys, virasto, viranomainen tai muu taho, joka päättää mitä tietoja kerätään ja miten niitä käytetään. Henkilötietojen käsittelijä on vastaavanlainen luonnollinen henkilö tai oikeushenkilö, mutta rekisterinpitäjästä poiketen henkilötietojen käsittelijä ei päätä tietojen keräämis- tai käsittelytavoista, vaan käsittelee henkilötietoja rekisterinpitäjän ohjeiden mukaisesti rekisterinpitäjän lukuun. (Yleinen tietosuoja-asetus 2016/679, 4 artikla.)

Tietosuoja-asetuksessa on määritetty rekisterinpitäjälle ja henkilötietojen käsittelijälle velvollisuudet. Yrityksen on tärkeää selvittää, kummassa roolissa se missäkin tilanteessa toimii. Rekisterinpitäjän sekä henkilötietojen käsittelijän pitää arvioida omaan henkilötietojen käsittelyynsä liittyviä riskejä sekä määritellä riskien perusteella riskitaso, jonka mukaan valitaan suoritettavat toimenpiteet. Tietosuoja-asetuksen myötä rekisterinpitäjällä on myös osoitusvelvollisuus, joka velvoittaa rekisterinpitäjän osoittamaan tarvittaessa myös jälkikäteen, että henkilötietoja on käsitelty asetuksen mukaisesti. Rekisterinpitäjä vastaa viime kädessä henkilötietojen käsittelyn lainmukaisuudesta. Tietosuoja-asetuksen osoitusvelvollisuuden myötä rekisterinpitäjän tulee pystyä osoittamaan, että henkilötietoja on käsitelty tietosuoja-asetuksen vaatimalla tavalla sekä huolehtia ja varmistaa henkilötietojen käsittelyssä tarvittavat tekniset ja organisatoriset toimenpiteet. (Hanninen ym. 2017, 16-17, 24-28.)

Henkilötietojen käsittelijän on toimittava oman roolinsa rajojen sisällä. Henkilötietojen käsittelijä ei saa määritellä henkilötietojen käsittelyn tarkoituksia, koska tällöin käsittelijä tulkitaan rekisterinpitäjäksi ja käsittelijän katsotaan tehneen sopimusrikkomuksen. Henkilötietojen käsittelijällä on oikeus käyttää alihankkijoita vain, jos rekisterinpitäjältä on saatu siihen lupa. Henkilötietojen käsittelijä on vastuussa käyttämiensä alihankkijoiden toimista täysimääräisesti. (Hanninen ym. 2017, 27-28.)

Ulkoistaessaan toimintoja, joiden hoitaminen vaatii henkilötietorekisterin käsittelyä, on toimintojaan ulkoistavan yrityksen rekisterinpitäjänä laadittava ohjeet henkilötietojen käsittelystä toimintoja hoitamaan ryhtyvälle yritykselle. Mikäli rekisterinpitäjä on ulkoistanut keräämiensä henkilötietojen käsittelyn, on rekisterinpitäjän varmistuttava siitä, että henkilötietojen käsittelijällä on tarvittavat resurssit ja valmiudet suorittaa henkilötietojen käsittely tietosuoja-asetuksen vaatimusten mukaisesti. Rekisterinpitäjä ja henkilötietojen käsittelijä

joutuivat uusimaan kahdenkeskisen sopimuksensa viimeistään tietosuoja-asetuksen siirtymäajan päättyessä. Sopimuksessa vahvistetaan muun muassa henkilötietojen käsittelyn kohde, kesto, tarkoitus ja luonne. (Yleinen tietosuoja-asetus 2016/679, (81).)

Pienyritysten taakkaa sopimusten uusimisprosessissa helpottaa esimerkiksi uudistetut IT2018-ehdot, joihin on lisätty henkilötietojen käsittelyä koskevat erityisehdot sekä sopimusmallipohjat, jotka yritys voi räätälöidä omiin tarpeisiinsa sopiviksi (Korhonen, 2018).

Rekisterinpitäjä sekä henkilötietojen käsittelijä ovat molemmat pyydettäessä velvoitettuja tekemään yhteistyötä valvontaviranomaisten kanssa, ja luovuttamaan henkilötietojen käsittelyä koskevat dokumentit sekä rekisterit viranomaisille (Yleinen tietosuoja-asetus 2016/679, (82).

3.4 Korvausvastuu ja hallinnolliset sakot

Tietosuoja-asetuksen 82 ja 83 artikloissa käsitellään rekisterinpitäjän ja henkilötietojen käsittelijän korvausvastuuta rekisteröidylle aiheutuneesta vahingosta sekä hallinnollisten sakkojen määräämiseen vaikuttavista yleisistä edellytyksistä.

Asetuksen 82 artiklan mukaan (Yleinen tietosuoja-asetus 2016/679) rekisterinpitäjä ja/tai henkilötietojen käsittelijä ovat velvollisia maksamaan aineellisen tai aineettoman vahingon kärsineelle rekisteröidylle/rekisteröidyille korvausta aiheutetusta vahingosta. Jokainen henkilötietojen käsittelyyn osallistunut taho (rekisterinpitäjä tai henkilötietojen käsittelijä), joka on käsitellyt henkilötietoja asetuksen vastaisesti, on korvausvastuussa. Henkilötietojen käsittelijä on kuitenkin vastuussa rikkomuksesta vain jos se on toiminut rekisterinpitäjän antamien lainmukaisten ohjeiden vastaisesti.

Kaikki vahingon aiheuttaneeseen tietojenkäsittelyyn osallistuneet toimijat ovat kokonaisvastuussa aiheutuneesta vahingosta. Tällä pyritään varmistamaan, että vahingon kärsinyt rekisteröity todella saa korvauksen. Täyden korvauksen rekisteröidylle maksanut toimija voi periä jokaiselta muulta vahingon aiheuttaneeseen henkilötietojen käsittelyyn osallistuneelta toimijalta korvausta, joka vastaa niiden osuutta vahingosta. (Yleinen tietosuoja-asetus 2016/679, 82 artikla.)

Korvausvastuusta vapautuakseen rekisterinpitäjän ja/tai henkilötietojen käsittelijän pitää pystyä osoittamaan, ettei se ole vastuussa vahingon aiheuttaneesta tapahtumasta ja että se on toiminut asetuksen mukaisesti. (Yleinen tietosuoja-asetus 2016/679, 82 artikla.)

Tietosuoja-asetuksen 83 artiklassa (Yleinen tietosuoja-asetus 2016/679) määritetään yleiset edellytykset valvontaviranomaisen määräämille hallinnollisille sakoille. Hallinnollisten sakkojen määräämiseen ja määrään vaikuttavat useat asiat. Sakkoja määriteltäessä viranomainen ottaa muun muassa huomioon rikkomisen luonteen, keston, vakavuuden ja tahallisuuden. Merkityksellistä on myös se, miten rikkomus on tullut viranomaisen tietoon, onko rikkomuksen tehnyt toimija ollut aloitteellinen ja tehnyt itse ilmoituksen viranomaiselle vai onko tieto rikkomuksesta tullut viranomaiselle muuta kautta.

Rikkomukseen osallistuneen toimijan oma toiminta rikkomuksen tultua julki vaikuttaa myös sakon määräytymiseen. Toimijan yhteistyö viranomaisen kanssa rikkomuksen korjaamiseksi sekä haittavaikutusten lieventämiseksi sekä toimijan toimet rekisteröidylle aiheutettujen vahinkojen lieventämiseksi ovat sakon määräytymisen vaikuttavia tekijöitä mutta myös asioita, joilla rikkomuksen tehnyt toimija voi yrittää vaikuttaa sakon määrään. (Yleinen tietosuoja-asetus 2016/679, 83 artikla.)

3.5 Tietosuojavastaavan nimittäminen

Yrityksen tulee tietyissä tilanteissa nimetä tietosuojavastaava. Tietosuojavastaavan nimi ja yhteystiedot pitää julkistaa sekä ilmoittaa valvontaviranomaiselle. Yhteystiedoiksi riittää nimi, osoite, puhelinnumero ja/tai sähköpostiosoite. Oleellista on, että tietosuojavastaava on helposti tavoitettavissa. Tietosuojavastaavan nimittämisvelvollisuus koskee myös pieniä ja keskisuuria yrityksiä mikäli niiden ydintehtäviä ovat laajamittaiset rekisteröityjen henkilötietojen käsittelyt, jotka edellyttävät säännöllistä ja järjestelmällistä rekisteröityjen seurantaa. (Hanninen ym. 2017, 120-122.)

Yritysten tulee nimittää tietosuojavastaava myös siinä tapauksessa jos niiden ydintehtävänä on laajamittainen rekisteröityjen arkaluontoisiksi luokiteltavien henkilötietojen käsittely. Tällaisia henkilötietoja ovat muun muassa terveystiedot, rotuun tai etniseen alkuperään, uskonnolliseen tai filosofiseen vakaumukseen, poliittisiin mielipiteisiin sekä seksuaaliseen käyttäytymiseen ja suuntautumiseen liittyvät tiedot. (Hanninen ym. 2017, 120-122.)

Asetus jättää tulkinnanvaraiseksi mitä tarkoitetaan käsitteellä ”laajamittainen”. WP29-työryhmän linjauksen mukaan toiminnan laajuutta arvioitaessa tulee ottaa huomioon rekisteröityjen täsmällinen lukumäärä tai rekisteröityjen suhde tarkasteltavaan väestön osaan. Määrittelyyn vaikuttaa myös käsiteltävä tietomäärä, käsittelytoiminnan kesto sekä maantieteellinen laajuus. WP29-työryhmä on linjannut, että esimerkiksi sairaalassa suoritettava potilastietojen käsittely on laajamittaista tietojen käsittelyä, mutta yksittäisen lääkärin suo-

rittama potilastietojen käsittely ei ole asetuksessa tarkoitettua laajamittaista tietojen käsittelyä, joka edellyttäisi tietosuojavastaavan nimittämistä. Myöskään yksittäisen asianajajan suorittama henkilötietojen käsittely ei ole laajamittaiseksi luokiteltavaa henkilötietojen käsittelyä, eikä edellytä tietosuojavastaavan nimittämistä vaikka käsittely koskee rikkomuksia ja rikostuomioita. (Tietosuojavaltuutetun toimisto, 1-2.)

Yritys voi nimittää tietosuojavastaavan myös vapaaehtoisesti vaikka yrityksen toiminta ei tietosuoja-asetuksen mukaan velvoittaisi yritystä nimittämään tietosuojavastaavaa. Tietosuojavastaava voidaan valita yrityksen oman henkilökunnan keskuudesta tai tehtävä voidaan ulkoistaa toiselle yritykselle. Tietosuoja-asetuksessa ei ole määritetty erityisiä vaatimuksia tietosuojavastaavan pätevyydestä tai koulutuksesta. Tehtävän monimutkaisuuden vuoksi, on tietosuojavastaavaksi suositeltavaa valita henkilö, jolla on useamman vuoden kokemusta tietosuoja-asioista. Tietosuojavastaavaa nimettäessä yrityksen omasta henkilökunnasta, tulee ottaa huomioon, että tietosuojavastaavalta edellytetään riippumattomuutta, joten henkilöt jotka päättävät esimerkiksi henkilötietojen käyttötarkoituksista tai vastaavat yrityksen IT-järjestelmistä eivät voi toimia tietosuojavastaavan tehtävissä. (Hanninen ym. 2017, 121-123.)

Tietosuojavastaavaa nimettäessä yrityksen johdon pitää ymmärtää, että tietosuojavastaavan nimittäminen ei vie vastuuta toiminnan lainmukaisuuden järjestämisestä yrityksen johdolta, vaan tehtävän luonne on konsultoiva. Tietosuojavastaava toimii myös yhteyshenkilönä rekisteröityjen, yrityksen työntekijöiden ja johdon sekä viranomaisten suuntaan. Tietosuojavastaava toimii itsenäisesti eikä saa ottaa vastaan ohjeita keneltäkään tehtävän hoitamista varten. Tietosuojavastaava raportoi suoraan yrityksen johdolle ja hänen tulisi olla läsnä tai häntä tulisi kuulla ennen tietosuoja-asioita koskevaa päätöksentekoa, vaikkei hän osallistukaan varsinaiseen päätöksentekoon. (Hanninen ym. 2017, 121-123.)

3.6 Henkilötietojen käsittelyn periaatteet

Henkilötietoja tulee lähtökohtaisesti aina käsitellä laillisesti ja asianmukaisesti. Tietosuoja-asetuksessa on lueteltu kuusi oikeusperustetta, joista vähintään yhteen käsittelyn tulee perustua. Lainmukaisen henkilötietojen käsittelyn kuusi oikeusperustetta ovat; suostumus, sopimus, lakisääteiset velvoitteet, elintärkeä etu, yleinen etu tai julkisen vallan käyttö ja oikeutettu etu. Pienyrityksen asiakas- ja markkinointirekisterien käsittelyperusteiksi soveltuu useimmiten suostumus, sopimus tai oikeutettu etu. Samaan rekisteriin saattaa soveltua useampikin oikeusperuste (Yleinen tietosuoja-asetus 2016/679, (39), 6 artikla; Hanninen ym. 2017, 29.)

Rekistereihin tulee kerätä vain toiminnan toteuttamisen kannalta tarpeellista tietoa, josta on ilmoitettu rekisteröitävälle. Ylimääräisen tai tarpeettoman tiedon kerääminen sekä tiedon kerääminen niin sanotusti varastoon on kielletty. Rekisterinpitäjän pitää ilmoittaa mihin tarkoitukseen tietoja kerätään, eikä tietoja pääsääntöisesti saa käyttää muihin tarkoituksiin. Asetuksessa on kuitenkin mainittu, että kerättyjä tietoja voidaan käyttää myös muihin tarkoituksiin, mutta vain jos käsittely sopii yhteen alkuperäisen tarkoituksen kanssa. Rekisterinpitäjän on kohtuullisia toimenpiteitä käyttäen varmistettava, että rekisteriin kerätyt tiedot ovat virheettömiä ja paikkansapitäviä. (Yleinen tietosuoja-asetus 2016/679, (39), (40), (50).)

Tietosuoja-asetuksen yleisenä periaatteena on läpinäkyvyys, jonka mukaan rekisterinpitäjän tulee informoida henkilötietojen keräyksestä avoimesti ja selkeästi. Henkilötietojen käsittelyn läpinäkyvyyden lisäämisellä pyritään parantamaan rekisteröidyn oikeuksia tietää mitä tietoja hänestä kerätään ja miten niitä käsitellään. (Hanninen ym. 2017, 73.)

Rekisterinpitäjän tulee asettaa henkilötietojen käsittelyyn liittyvät tiedot helposti rekisteröitävän saataville. Tiedot tulee toimittaa rekisteröidylle kirjallisesti ja tarvittaessa tiedot voidaan toimittaa sähköisessä muodossa. Tietosuoja-asetuksessa ei ole tarkkaan ilmoitettu missä formaatissa tiedot tulee toimittaa rekisteröidylle. Rekisterinpitäjän tulee kuitenkin viestiä rekisteröitävälle selkeästi, ja viestinnässä pitää käyttää yksinkertaista kieltä, jota lukijan on helppo ymmärtää. Helpoiten tiedot saatetaan rekisteröitävälle esimerkiksi asettamalla tietosuojaseloste verkkokauppaan rekisteröitymisen yhteyteen. (Yleinen tietosuoja-asetus 2016/679, (39), (50); Hanninen ym. 2017, 16, 73-74, 76.)

Mikäli rekisterinpitäjä saa tiedot muuta kautta kuin rekisteröitävältä itseltään, pitää rekisteröitävälle toimittaa tietosuoja-asetuksen 14 artiklassa vaaditut tiedot kohtuullisessa ajassa ilman aiheetonta viivytystä. Asetuksen 12 artiklassa on määritetty yhden kuukauden määräaika tietojen antamiselle sekä rekisteröidyn pyytämien toimenpiteiden suorittamiselle. Tarvittaessa määräaikaa voidaan jatkaa enintään kahdella kuukaudella. Oleellista rekisteröidyn tai viranomaisen pyyntöihin vastaamisessa on reagoida niihin viivytyksettä. (Hanninen ym. 2017, 77; Talus ym. 2017, 24.)

Tietosuoja-asetus on paikoitellen hyvinkin tulkinnan varainen ja asetusta onkin tarkoitus täsmentää kansallisella lainsäädännöllä. Asetuksen lopullinen tulkinta tarkentuu vasta oikeuskäytännön kautta, ja tätä kautta tehtävät tulkintalinjaukset koskevat myös joitain käsitteitä (Talus ym. 2017, 36; Hanninen ym. 2017, 14).

3.7 Rekisteröidyn oikeudet

Tietosuoja-asetuksen yhtenä tarkoituksena on parantaa rekisteröidyn oikeuksia saada tietoa omien henkilötietojensa käsittelystä. Rekisterinpitäjän velvollisuus on varmistaa omalla toiminnallaan, että rekisteröidyn oikeudet toteutuvat. Uudessa tietosuoja-asetuksessa rekisteröidyn oikeuksista on säädetty aiemmin voimassa ollutta henkilötietolakia yksityiskohtaisemmin. Rekisteröidylle on asetuksessa myös säädetty uusia oikeuksia. (Hanninen ym. 2017, 56.)

Rekisteröidyn esittämiin pyyntöihin tulee vastata viivyttelemättä. Pyyntöjä koskee kuukauden määräaika, jonka aikana pyyntöihin on reagoitava. Määräaikaa voidaan jatkaa enintään kahdella kuukaudella, mikäli pyynnöt ovat monimutkaisia ja niitä on paljon. Rekisteröidylle on tiedotettava määräajan jatkamisesta sekä kerrottava miksi henkilötietojen toimittaminen viivästyy. Pyyntöjen toteuttamisesta ei lähtökohtaisesti voi kieltäytyä eikä niistä saa periä maksua. (Talus ym. 2017, 25.)

Tietosuoja-asetuksen 12 artiklassa todetaan, että rekisterinpitäjä voi kuitenkin periä kohtuullisen maksun rekisteröidyn pyynnön toteuttamisesta aiheutuneista hallinnollisista kustannuksista tai kieltäytyä toteuttamasta rekisteröidyn pyyntöä, mikäli rekisteröity esittää pyyntöjä toistuvasti tai ne ovat ilmeisen perusteettomia tai kohtuuttomia. Käyttäessään edellä mainittuja vaihtoehtoja, rekisterinpitäjän pitää pystyä osoittamaan pyynnön ilmeinen perusteettomuus tai kohtuuttomuus. Rekisteröidylle tulee ilmoittaa päätöksestä viipymättä sekä syyt miksi pyyntöä ei toteuteta. Ilmoituksessa tulee myös kertoa, että rekisteröidyllä on mahdollisuus valittaa päätöksestä valvontaviranomaiselle sekä käyttää muita oikeussuojakeinoja (Yleinen tietosuoja-asetus 2016/679, 12 artikla.)

Oikeus saada läpinäkyvästi tietoa omien henkilötietojen käsittelystä

Rekisterinpitäjän pitää tiedottaa henkilötietojen käsittelystä jo ennen käsittelyn aloittamista. Rekisteröidylle tulee tiedottaa avoimesti toteutettavista käsittelytoimista sekä siitä mitä tietoja kerätään ja miten ja mihin tarkoituksiin niitä käytetään. Tiedottamisen selkeyteen pitää kiinnittää erityistä huomiota, mikäli toimijoiden määrä on suuri ja toteuttavat käytänteet sisältävät teknisesti monimutkaisia toimintoja. Informoinnin ymmärrettävyys ja selkeys korostuu myös niissä tilanteissa kun tiedottamisen kohteena on lapsi. (Hanninen ym. 2017, 73-74.)

Oikeus saada pääsy omiin tietoihin

Rekisteröidyllä on oikeus saada rekisterinpitäjältä tieto siitä, mitä tietoja hänestä on kerätty. Tietosuoja-asetuksessa ei ole säädetty missä muodossa rekisteröity voi pyytää pääsyä omiin tietoihinsa. Tietosuojavaltuutetun toimiston ja oikeusministeriön laatimassa ohjeistuksessa (Talus ym. 2017, 25) ohjeistetaan toimittamaan pyydetyt tiedot sähköisessä muodossa, jos pyyntö tietojen saamiseen on esitetty sähköisesti, ellei rekisteröity pyydä niitä jossain muussa muodossa. Henkilötiedot voidaan toimittaa myös suullisesti, mikäli pyynnön esittäjän henkilöllisyys on vahvistettu asianmukaisesti. (Yleinen tietosuoja-asetus 2016/679, (39), 12 artikla.)

Rekisteröidyn oikeus päästä tietoihin tarkoittaa käytännössä sitä, että rekisteröidylle toimitetaan jäljennös käsittelyn kohteena olevista rekisteröidystä kerätyistä henkilötiedoista sekä tietosuojaseloste tai muu vastaava henkilötietojen käsittelyä varten laadittu seloste, josta käy ilmi tietosuoja-asetuksessa määritetyt rekisteröitävälle tiedotettavat asiat (Hanninen ym. 2017, 60).

Oikeus omien henkilötietojen oikaisuun

Rekisteröidyllä on oikeus vaatia, että häntä koskevat epätarkat tai virheelliset tiedot korjataan. Mikäli rekisteröidyn henkilötiedot ovat puutteelliset, pitää hänen toimittaa rekisterinpitäjälle lisäselvitys tiedoista, jotta ne voidaan täydentää (Hanninen ym. 2017, 61).

Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus tulla unohdetuksi, eli hänellä on oikeus vaatia omien henkilötietojensa poistamista rekisteristä. Pyynnön toteuttaminen edellyttää kuitenkin, että vähintään yksi alla mainituista perusteista täyttyy:

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin. Jos esimerkiksi kokoustila on varattu ja asiakkaan tiedot on kerätty vain tätä varten, tulee tiedot poistaa asiakkaan pyynnöstä kokouksen jälkeen (olettaen, että tietoja ei enää tarvita muun lainsäädännön tai edun nojalla).
- Henkilötietojen käsittely perustuu suostumukseen ja rekisteröity peruuttaa antamansa suostumuksen. Jos rekisteröity vastustaa muuta käsittelyä kuin käsittelyä suoramarkkinointia varten, on lisäedellytyksenä se, että käsittelyyn ei ole olemassa perusteltua syytä. rekisteröidyn suostumukseen ja rekisteröity peruuttaa suostumuksensa. Lisäedellytyksenä pyynnön toteuttamiselle on, ettei käsittelyyn ole olemassa muuta perusteltua syytä.

- Rekisteröity vastustaa käsittelyä. Jos rekisteröity vastustaa muuta käsittelyä kuin käsittelyä suoramarkkinointia varten, on lisäedellytyksenä se, että käsittelyyn ei ole olemassa perusteltua syytä.
- Henkilötietoja on käsitelty lainvastaisesti.
- Henkilötiedot on poistettava lakisääteisen velvoitteen noudattamiseksi.
- Henkilötiedot on kerätty tarjottaessa sähköisiä palveluja suoraan lapselle. (Holopainen 2018, 16.)

Rekisteröidyn oikeus tulla unohdetuksi on hyvin rajallinen. Oikeutta tulla unohdetuksi ei voida soveltaa mikäli rekisterinpitäjän käsittelyperusteena on oikeutettujen etujen toteuttaminen ja peruste on voimassa. Esimerkiksi kun työnantaja käsittelee oikeutetun edun perusteella työntekijän henkilötietoja, ei työntekijällä ole oikeutta vaatia tietojen poistamista. Oikeutta vaatia tietojen poistamista ei ole myöskään silloin, jos tietoja joudutaan käsittelemään oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi. (Hanninen ym. 2017, 62-63.)

Oikeus rajoittaa omien henkilötietojen käsittelyä

Rekisteröity voi vaatia henkilötietojensa käsittelyn rajoittamista seuraavissa tilanteissa:

- Rekisteröity kiistää henkilötietojen paikkansa pitävyyden, jolloin henkilötietojen käsittelyä rajoitetaan, kunnes rekisteripitäjä on varmistanut henkilötietojen paikkansapitävyyden.
- Organisaatio käsittelee henkilötietoja lainvastaisesti ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii poistamisen sijaan tietojen käsittelyn rajoittamista.
- Rekisteröidyn henkilötiedot eivät enää ole tarpeellisia rekisterinpitäjälle, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.
- Rekisteröity ja rekisterinpitäjä ovat erimielisiä siitä, onko rekisterinpitäjällä huomattavan tärkeä ja perusteltu syy henkilötietojen käsittelyyn, joka syrjäyttää rekisteröidyn edut ja oikeudet. Selvityksen ajaksi rekisteröity voi vaatia henkilötietojen käsittelyn rajoittamista. (Yleinen tietosuoja-asetus 2016/679, 18 artikla.)

Mikäli rekisteröidyllä on oikeus rajoittaa henkilötietojensa käsittelyä jollakin edellä mainituista syistä, rekisterinpitäjä voi säilyttää tiedot mutta se saa käsitellä tietoja vain rekisteröidyn suostumuksella tai oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Rekisterinpitäjä voi käsitellä tietoja myös omien tai toisen henkilön oikeuksien

suojaamiseksi. Yrityksen on varmistettava, että henkilötietojen käsittelyyn käytetyssä järjestelmässä on mahdollista ilmaista selkeästi, että tiettyjen henkilötietojen käsittely on rajoitettu. (Hanninen ym. 2017, 64.)

Oikeus pyytää tieto niistä henkilötietojen vastaanottajista, joille rekisterinpitäjän tulee ilmoittaa rekisteröidyn henkilötietojen oikaisuista, käsittelyn rajoituksista sekä henkilötietojen poistoista.

Mikäli rekisteröity on vaatinut omien henkilötietojensa oikaisua, poistoa tai käsittelyn rajoitusta, pitää rekisterinpitäjän ilmoittaa näistä toimenpiteistä kaikille niille tahoille, joille kyseisiä henkilötietoja on luovutettu. Rekisterinpitäjän on ilmoitettava edellä mainituista tahoista rekisteröidylle jos tämä näitä tietoja pyytää. (Yleinen tietosuoja-asetus 2016/679, 19 artikla.)

Oikeus siirtää omat henkilötiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada vain ne itseään koskevat henkilötiedot, jotka rekisteröity on luovuttanut rekisterinpitäjälle. Henkilötiedot tulee toimittaa rekisteröidylle jäsennellyssä, yleisesti käytetyssä koneellisesti luettavassa muodossa. Rekisteröidyllä on oikeus siirtää saamansa tiedot toiselle rekisterinpitäjälle, jos henkilötietojen käsittely on perustunut rekisteröidyn suostumukseen tai sopimukseen ja henkilötietojen käsittely toteutetaan automaattisesti. (Yleinen tietosuoja-asetus 2016/679, 20 artikla.)

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää siirtämään omat henkilötietonsa toiselle rekisterinpitäjälle, jos tämä on teknisesti mahdollista. Siirto-oikeus koskee vain automaattisesti käsiteltäviä tietoja, joten paperille kerättyä rekisteriä ei tarvitse siirtää rekisterinpitäjältä toiselle. Rekisterinpitäjän ei tarvitse suostua henkilötietojen siirtoon, mikäli tietojen käsittelylle on joku muu peruste kuin suostumus tai sopimus. Mikäli henkilötietojen käsittelyn oikeusperusteena on käytetty yrityksen oikeutettua etua ja sopimusta, kuten silloin kun työnantaja käsittelee työntekijän henkilötietoja, koskee siirto-oikeus työsopimuksen täyttämistä varten käsiteltyjä tietoja, kuten palkkatietoja. (Hanninen ym. 2017, 65.)

Oikeus vastustaa omien henkilötietojen käsittelyä

Rekisteröity voi vastustaa häntä koskevien henkilötietojen käsittelyä erityiseen tilanteeseensa liittyvällä perusteella, jos tietojen käsittelyn oikeusperusteena on yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen tai

käsittely perustuu rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Pyynnön esittämisen jälkeen rekisterinpitäjä ei saa enää käsitellä rekisteröidyn henkilötietoja, ellei se pysty osoittamaan, ”että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet. Käsittelyä voidaan jatkaa myös jos se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.” (Yleinen tietosuoja-asetus 2016/679, 21 artikla.)

Asetuksessa ei selvennetä määritettä ”henkilökohtaiseen erityiseen tilanteeseen liittyvällä perusteella”, joten rekisterinpitäjän tulisi pyynnön saatuaan arvioida käsitelläänkö henkilötietoja laissa säädetyn velvollisuuden nojalla vai onko käsittelylle olemassa joku muu huomattavan tärkeä ja perusteltu syy. Mikäli rekisteripitäjä lopettaa rekisteröidyn henkilötietojen käsittelyn, tietoja ei välttämättä tarvitse poistaa kokonaan, vaan ne voidaan poistaa aktiivisesta käytöstä, niin ettei tietoihin enää ole pääsyä (Hanninen, ym., 2017, 68.)

Oikeus olla joutumatta pelkästään automaattiseen käsittelyyn perustuvan päätöksen kohteeksi

Yleisen tietosuoja-asetuksen 22 artiklassa säädetään automatisoiduista päätöksistä sekä profiloinnista. Tietosuoja-asetuksessa automaattisella päätöksenteolla tarkoitetaan sellaista päätöksenteko prosessia, jossa ihminen ei ole osallisena, vaan päätös syntyy puhtaasti automatisoidun käsittelyprosessin tuloksena. Tietosuoja-asetuksen mukaan ”Rekisteröidyllä oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi” (Yleinen tietosuoja-asetus 2016/679, 22 artikla).

Tietosuoja-asetuksessa on käytetty esimerkkinä internetissä tehtävän luottohakemuksen automaattista hylkäämistä sekä täysin sähköiseen prosessiin perustuvaa rekrytointia. Pitkälle vietyä automaattista tietojen käsittelyä ei ole kuitenkaan kielletty, kunhan prosessiin osallistuu myös ihminen. Ihmisellä tulee myös olla oikeus kumota automatisoidun käsittelyn seurauksena syntynyt päätös. (Yleinen tietosuoja-asetus 2016/679, (71).)

Automatisoitu käsittely on kuitenkin sallittu niissä tapauksissa, joissa käsittelyyn on annettu lupa jäsenvaltion lainsäädännössä tai rekisterinpitäjään sovellettavassa unionin oikeudessa. Automaattista käsittelyä voidaan hyödyntää myös jos rekisteröity on antanut siihen luvan tai käsittely on tarpeen rekisterinpitäjän ja rekisteröidyn välisen sopimuksen tekemistä varten. Kaikissa edellä mainituissa tapauksissa rekisteröidylle pitää tiedottaa hänen tietojen joutumisesta automaattisen käsittelyn kohteeksi, mahdollisuudesta vaatia

ihmisen osallistumista käsittelyyn sekä oikeus saada selvitys käsittelyn jälkeen tehdystä päätöksestä ja mahdollisuudesta riitauttaa tehty päätös. Lapseen kohdistuvat automaattiseen päätöksen tekoon perustuvat käsittelyt ovat kiellettyjä. (Yleinen tietosuoja-asetus 2016/679, (71).)

4 Tietosuojaprosessiin valmistautuminen ja toteutus

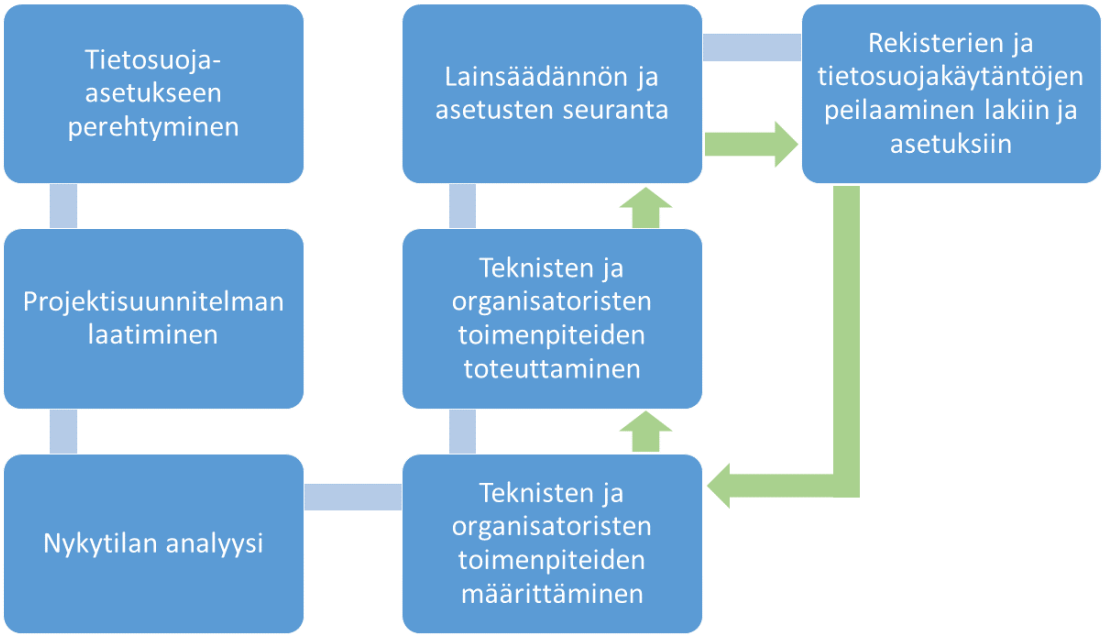
Projektiin valmistautuminen jouduttiin aloittamaan kohdeyrityksessä lähes täysin puhtaalta pöydältä. Pienessä yrityksessä ei ollut valmiiksi laadittuja tietoturvaan ja henkilötietojen käsittelyyn liittyviä kirjallisia ohjeistuksia. Verkkosivuilla oli henkilötietolain vaatimat rekisteriselosteet ja yrityksessä noudatettiin henkilötietolakia rekistereiden tietojen käsittelyssä, mutta toteutettuja käytänteitä ei ollut dokumentoitu.

Pienten yritysten ongelmana isoissa ja yrityksen ydintoimintaan liittymättömissä projekteissa on usein resurssien puute. Resurssien puute koskee aikaa, rahaa ja osaamista. Tietosuoja-asetukseen valmistautuessa yritys joutui punnitsemaan missä määrin prosessiin oli järkevää budjetoida rahaa ja mihin rahaa oli järkevä kohdentaa. Yrityksessä jouduttiin miettimään käytettäisiinkö budjettia henkilökunnan kouluttamiseen vai asianajajan tai konsulttitoimiston palkkaamiseen.

Ulkopuolisen tahon palkkaamista miettiessä tuli huomioida, että yrityksen henkilökunta joutuisi joka tapauksessa suunnittelemaan yritykselle sopivat prosessit rekisterien tietojen eheyden varmistamiseksi. Tämän lisäksi rekisterien tiedot pitäisi läpikäydä ja tarkistaa tietojen oikeellisuus sekä poistaa vanhentuneet ja tarpeettomat tiedot. Ulkopuolisen tahon mahdollisesta palkkaamisesta huolimatta yrityksen johdon tuli ymmärtää, että vähintään he joutuisivat perehtymään tietosuoja-asetukseen, sillä organisaation johto vastaa siitä, että henkilötietoja käsitellään lainmukaisesti (Talus ym. 2017, 34).

Tietosuoja-asetukseen valmistautumisprosessi jakautui käytännössä kahteen osaan; yrityksen toiminnan ja sen dokumentoinnin päivittämisestä vastaamaan tietosuoja-asetusta niissä määrin kun se projektisuunnitelmaa laadittaessa oli mahdollista sekä jatkuvaan osaan, joka muodosti kiertävän, loppumattoman kehän.

Prosessiin ryhdyttäessä tuli siis ymmärtää, ettei tietosuojaan liittyvä prosessi ole kertaluontoinen projekti, vaan tietosuojaan liittyviä käytänteitä ja dokumentteja pitää päivittää lainsäädännön ja yrityksen rekistereiden sekä käytänteiden muuttuessa.



Kuvio 2. Tietosuoja-asetus prosessin kulku kohdeyrityksessä

Ennen kuin yrityksessä voitiin aloittaa varsinaisen projektisuunnitelman laadinta, projektipäällikön piti ensin selvittää mitä tietosuoja-asetus tarkalleen ottaen piti sisällään ja miten se erosi edelleen voimassa olleesta henkilötietolaista.

Prosessi aloitettiin tutustumalla saatavilla olevaan materiaaliin tietosuoja-asetuksesta. Materiaalia löytyi muun muassa oikeusministeriön ja tietosuojavaltuutetun verkkosivuilta. Näiden lisäksi hyödynnettiin eri palveluntarjoajien sivuille kerättyä tietoa sekä YouTube-videopalveluun ladattuja verkkoseminaareja ja luentoja. Samaan aikaan tarkasteltiin EU:n tietosuoja-asetusta, jotta pystyttiin vertaamaan eri tahojen esittämiä tulkintoja asetuksesta omiin tulkintoihin.

4.1 Projektisuunnitelman laadinta

Tietosuoja-asetuksen vaatimusten hieman selkeydyttyä voitiin laatia projektisuunnitelma. Prosessin jatkuvasta luonteesta huolimatta, projektisuunnitelmaan päätettiin kirjata loppupiste teknisten ja organisatoristen toimenpiteiden toteuttamisen jälkeen. Projektin päättymispäiväksi määritettiin siirtymäajan päättymispäivä 24.5.2018. Projektin olisi ollut mahdollista laittaa päättymään aiemminkin, mutta asetuksen tulkintojen ja ohjeiden jatkuvan päivittymisen takia projektin päättymispäiväksi kirjattiin viimeinen mahdollinen päivä. Jatkuvalle prosessille, jossa seurataan lainsäädäntöä ja peilataan sitä yrityksen käytäntöihin, päätettiin laatia toimintaohje, jonka mukaan toimiessa käytänteet pysyvät lainsäädännön ja asetusten vaatimusten mukaisina.

Ensimmäiseksi projektisuunnitelmaan tehtiin selvitys projektin tarpeesta, josta kävi ilmi syyt sille, miksi projekti toteutettiin. Yrityksen perusperiaatteisiin kuuluu lakien ja asetusten noudattaminen, joten projektiin ryhdyttiin jo pelkästään tämän takia. Asiaa tarkasteltiin kuitenkin myös laajemmin ja projektille haettiin myös muita perusteita.

Projektin ensisijaisena syynä nähtiin toiminnan jatkamisen mahdollistaminen. EU:n tietosuoja-asetuksen siirtymäajan päätyttyä yrityksen tietosuojakäytännöt tuli olla asetuksen vaatimusten mukaiset, mikäli yritys ei toimisi asetusten mukaisesti, riskinä olisi toiminnan jatkuvuuden vaarantuminen. Viranomainen voisi keskeyttää rekisterien tietojen käsittelyn, joka käytännössä tarkoittaisi toiminnan keskeytymistä. Toiminnan keskeytyminen aiheuttaisi merkittävän uhan toiminnalle kassavirran häiriintymisen takia. Myös mainehaitta yhteistyökumppanien suuntaan voisi katkaista asiakkuus- ja toimittajasuhteita. Rekisterien tietojen käsittelyn keskeyttämisen lisäksi pahimmassa tapauksessa riskinä olisi lisäksi viranomaisen määräämä sakko, joka laiminlyönnin törkeydestä riippuen voisi enimmillään olla merkittävä riski yrityksen maksukyvylle.

Sanktioriskien lisäksi projektin toteuttamisen syynä oli huolehtia asiakas- ja yhteistyökumppanisuhteiden jatkuvuudesta. Osa yhteistyökumppaneista toimii yrityksen henkilötietojen käsittelijöinä, joten he odottivat asetuksen mukaisia henkilötietojen käsittelyohjeita rekisterinpitäjältä. Yhteistyö näiden kumppaneiden kanssa ei jatkuisi ilman ohjeistusten ja sopimusten tarkastuksia. Osa asiakkaiden kanssa solmituista toimittajasopimuksista myös velvoittaa noudattamaan voimassa olevia lakeja ja asetuksia, näiden laiminlyönti olisi sopimusten purkamiseen oikeuttava syy. Yritys halusi myös pitää huolen maineestaan vastuullisena toimijana sekä tuoda esiin sen, että asiakkaiden oikeuksia kunnioitetaan, jotta asiakkaat voisivat jatkaa huoletta kaupankäyntiä yrityksen kanssa.

Projektin tavoite pyrittiin määrittämään mahdollisimman lyhyesti ja ytimekkäästi, jotta tavoitteen saavuttaminen olisi mahdollisimman helppo todentaa. Projektin tavoitteena oli saattaa yrityksen asiakas-, toimittaja- ja markkinointirekisterien henkilötietojen käsittely vastaamaan EU:n uuden tietosuoja-asetuksen(GDPR) vaatimuksia.

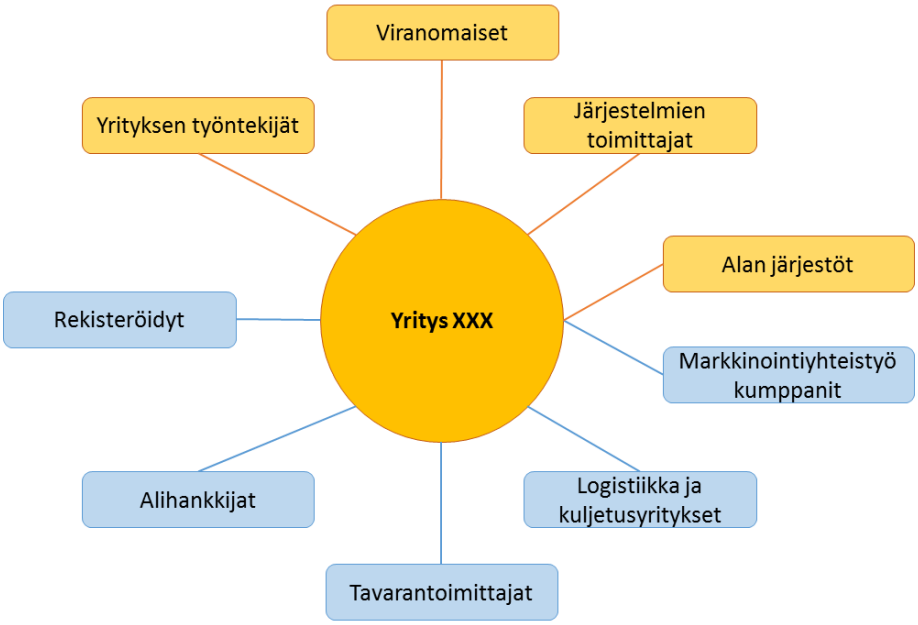
Asetetun tavoitteen saavuttamisen todentaminen oli haastavaa, sillä aivan viime kädessä yrityksen tietosuoja käytänteiden lain mukaisuuden voisi varmistaa vain valvovaviranomainen, sillä yrityksellä oli tiedossa, että asetuksen lopullinen tulkinta tarkentuisi vasta oikeuskäytännön kautta.

Tavoitteen saavuttamisen todentamiseksi, yrityksessä päätettiin laatia tarkistuslista, joka käytäisiin läpi projektin lopussa, ja jonka avulla varmistettaisiin rekisteröityjen henkilötietojen käsittelyn lainmukaisuus. Tarkistuslistan laatimisessa käytettäisiin apuna muun muassa yrittäjat.fi- sivustolla olevaa yrittäjän tietosuoja-opasta.

Tavoitteen määrityksen jälkeen määritettiin projektin välittömät ja välilliset kohderyhmät. Välittömiä kohderyhmiä olivat yritys ja yrityksen työntekijät. Yritys saisi projektin myötä tietosuojadokumentit asetuksen vaatimuksia vastaaviksi sekä yritys saisi dokumentoitua tietosuojakäytännöt asetusten vaatimusten mukaisesti. Samalla yrityksen työntekijät saisivat varmuuden yrityksen käytäntöjen lainmukaisuudesta sekä ajantasaisen ohjeistuksen käytännön toimenpiteistä erilaisissa tietosuojaan ja rekisteröityjen oikeuksia koskevissa tilanteissa.

Välillisiä kohderyhmiä olivat rekisteröidyt, jotka saisivat varmuuden omien tietojensa asianmukaisesta käytöstä ja käsittelystä sekä hyötyisivät toimivasta asiakaspalvelusta, mikäli haluaisivat käyttää omia oikeuksiaan. Välillisenä kohderyhmänä olisivat myös viranomaiset, jotka voisivat tarvittaessa todentaa yrityksen toimivan lain ja asetusten mukaisesti.

Kohderyhmien selvityksen jälkeen laadittiin sidosryhmäanalyysi, jolla selvitettiin eri sidosryhmien roolit ja odotukset kohdeyritystä kohtaan sekä sidosryhmien merkitys projektin onnistumiseen. Merkittävimmät sidosryhmät projektin onnistumisen kannalta olivat yrityksen työntekijät, joiden työpanoksen laatu ja sitoutumisen aste vaikuttivat kaikkein merkittävimmin projektin suunniteltuun läpivientiin. Viranomaisilta odotettiin tarkkoja ja selkeitä ohjeistuksia sekä ajantasaista tiedottamista tietosuoja-asetuksesta. Toimialan järjestöiltä odotettiin viranomaisten tavoin laadukkaiden koulutus- ja infotilaisuuksien järjestämistä sekä erilaisten ohje- ja infomateriaalien toimittamista. Yrityksen työntekijöiden ohella tärkein sidosryhmä sujuvan projektin läpiviennin sekä asetettuun tavoitteeseen pääsemisen kannalta olivat järjestelmien toimittajat. Heidän vastuullaan oli sellaisten projektiin liittyvien osa-alueiden toteuttaminen, joita ei käytännössä kukaan muu voinut toteuttaa.



Kuvio 3. Sidosryhmäkaavio

Kohderyhmien ja sidosryhmien määrittelyn jälkeen käytiin läpi projektin eteneminen, eli projektin osa-alueet ja aikataulu. Projektin osa-alueita oli määrittely, suunnittelu, toteutus, testaus ja päättäminen. Määrittely suoritettiin projektisuunnitelman alussa. Suunnitteluosaan sisältyi projektin tehtävien määritys ja aikataulutus, kustannusarvio, työnjako ja vastuu sekä nykytila-analyysi, joka piti sisällään käytössä olevien rekisterien määrityksen ja näiden tietoturvan tason kartoituksen sekä riskianalyysin.

Projektin etenemisen seuranta käsiteltiin toimenpiteiden jälkeen. Projektin seuranta suoritettaisiin kerran viikossa tapahtuvalla seurantakatsauksella, joka ajoitettaisiin maanantaihin. Maanantaina tarkasteltaisiin mitä edellisellä viikolla on saatu aikaiseksi ja mitä tehtäviä tulisi saada sillä viikolla suoritettua. Tavoitteiden ja aikarajojen saavuttamista seurattaisiin Gantt-kaaviolla.

Taulukko 1. Projektin alustava aikataulu

Toimenpide	**Toteuttaja/Vastuutaho**	**Aikataulu vko**
Projektisuunnitelma	X	42-43
Perehtyminen tietosuoja-asetukseen	X, Y, Z	44-20
Nykytila-analyysi	X	49-50
Vaadittavien toimenpiteiden kartoitus	X	2-4
Dokumentit (tietosuojaselosteet)	X	13-16
Käytänteiden dokumentointi	X	5-19
Sopimusten uusiminen	X, Z	9-13
Henkilötietojen käsittelyn ohjeistukset	X	5-19

Järjestelmän päivitykset	X, W	13-16
Käyttäjien oikeuksien tarkistus	X	13-16
Testaus	X, W	18-21
Projektin päättäminen	X, Y, Z	21

Pienessä yrityksessä ja pienessä projektiryhmässä, jossa henkilöt työskentelevät vierekkäisissä huoneissa, ajantasainen viestintä on suhteellisen helppo järjestää. Viestintä projektiryhmän henkilöiden välillä suunniteltiin tapahtuvaksi pääasiassa yhteisissä palavereissa sekä suullisena viestintänä. Projektin toteutuksen laatua suunniteltiin tarkkailtavan lähinnä aikataulussa ja budjetissa pysymisen kautta.

Projektin riskit luokiteltiin neljään eri luokkaan; aikatauluriski, laaturiski, henkilöriski sekä kustannusriski. Taulukkoon kirjattiin sanallinen kuvaus riskistä, riskin konkretisoitumisen vaikutus projektiin sekä miten riskiin oli tarkoitus varautua. Riskille arvioitiin vakavuusaste taulukolla 1-5 sekä todennäköisyysprosentti riskin konkretisoitumiselle.

Taulukko 2. Esimerkki projektin riskitaulukosta

Riski2 Laaturiski	Vakavuus (1-5)	Todennäköisyys %
	4	40
Kuvaus Projektin tuotosten heikkolaatu. Laatu ei vastaa tietosuoja-asetuksen vaatimuksia.		
Vaikutus Heikkolaatu tai tietosuoja-asetuksen vaatimuksia vastaamaton laatu heikentää yrityksen uskottavuutta ja voi tuottaa lisää kustannuksia sanktioiden tai ulkopuolisen tahon palkkaamisen kautta. Tuotosten heikkolaatu voi aiheuttaa lisää työtä, mikäli materiaaleja joudutaan uusimaan tai ohjeet ovat epäselviä.		
Varautuminen Aktiivinen perehtyminen tietosuoja-asetukseen webinaarien, luentojen ja yhteistyökumppanien kanssa.		

Aikatauluriski käsitti projektin toimenpiteiden venymisen määritettyjen aikarajojen yli tai koko projektin myöhästymisen määritellystä. Projektin päätöspäivän ylittämisen vakavuusasteeksi määritettiin kolmoseksi ja riskin todennäköisyyttä pidettiin keskisuurena (45 - 60 %). Aikatauluriskin suurimpana mahdollisena tekijänä pidettiin osaamattomuudesta johtuvia syitä. Tietosuoja-asetuksen laajuus ja tulkinnanvaraisuus sekä puutteelliset ohjeet viranomaisten taholta nähtiin projektin läpiviennin kannalta hidastavana tekijänä. Eri toimenpiteiden aikarajojen ylittyminen todennäköisesti viivästyttäisi koko projektin läpivientiä, sillä aikataulujen kurominen projektiryhmäläisten muiden ”normaali” töiden lisäksi uskottiin olevan vaikeaa. Aikatauluriskiin aiottiin varautua huolellisella perehtymisellä tietosuoja-asetukseen sekä järjestämällä työnjako tasaisesti ja hoitamalla viestintä työn etenemisestä täsmällisesti.

Projektin tuotosten heikkolaatu nähtiin laaturiskinä. Laaturiskissä projektin tuotosten laatu ei vastaa tietosuoja-asetuksen vaatimuksia tai henkilötietojen käsittelyohjeistus on puutteellista. Laaturiskiä pidettiin melko vakavana ja vakavuusasteeksi määritettiin neljä. Laaturiskin todennäköisyyttä pidettiin keskisuurena (40 %). Tietosuoja-asetuksen vaatimuksia vastaamattoman laadun uskottiin heikentävän yrityksen mainetta ja uskottavuutta. Huonolaatuiset tai epäselvät ohjeet voivat kasvattaa työmäärää, mikäli ohjeista huolimatta työntekijät joutuvat selvittämään oikeita toimintamalleja käytänteitä. Epäselvät ohjeet joudutaan myös todennäköisesti uusimaan, jolloin työ joudutaan tekemään kahteen kertaan. Tietosuoja-asetuksen vaatimuksia vastaamattomat dokumentit ja ohjeistukset voivat myös pahimmillaan aiheuttaa yritykselle rahallisia sanktioita. Laaturiskiin pyrittiin varautumaan huolellisella perehtymisellä tietosuoja-asetukseen. Perehtymiseen oli tarkoitus hyödyntää saatavilla olevaa kirjallisuutta ja eri tahojen järjestämiä webinaareja ja luentoja sekä konsultoimalla yhteistyökumppaneita.

Kolmantena riskinä pidettiin henkilöriskiä. Henkilöriskejä pääteltiin olevan kaksi; projektiin osallistuvien henkilöiden sairastuminen tai muu poissaolo sekä töiden epätasaisesta jakautumisesta syntyvä kuormittavuus.

Poissaoloista aiheutuva henkilöriski luokiteltiin laaturiskin kanssa kriittiseksi tasolle neljä. Henkilöriskin todennäköisyyttä pidettiin suhteellisen pienenä ja se arvioitiin 25 prosentiksi. Avainhenkilöiden poissaolon uskottiin vaikuttavan ensisijaisesti projektin aikatauluun ja mikäli poissaolo olisi pitkä, voisi se vaikuttaa myös kiireen kautta projektin tuotosten laatuun. Henkilöriskiin pyrittiin varautumaan aktiivisella projektin seurannalla sekä tasaisella työnjaolla, jolloin vältettäisiin tilanne, jossa henkilön vastuulle kuuluvat tehtävät ensin viivästyisivät ja sen jälkeen siirtyisivät muiden hoidettavaksi nopealla aikataululla. Henkilöriskiin varauduttaisiin myös huolellisella perehtymisellä tietosuoja-asetukseen, jolloin kaikilla projektiryhmän jäsenillä olisi yhtäläiset tiedot ja töitä pystyttäisiin tarvittaessa jakamaan tasaisesti kaikille ryhmän jäsenille sujuvasti.

Toisena henkilöriskinä pidettiin töiden epätasaisesta jakautumisesta aiheutuvaa ylikuormittumista, joka voisi johtaa aikatauluriskiin, laaturiskiin sekä poissaoloista aiheutuvaan henkilöriskiin. Riskiä pidettiin melko vakavana ja se arvioitiin tasolle neljä. Riskin todennäköisyyttä pidettiin keskisuurena (50 - 60 %), sillä pienessä yrityksessä normaalit toiminnot vievät suuren osan työajasta ja paljon selvitystä vaativille ylimääräisille töille on vaikea löytää aikaa. Vaikka töitä oli tarkoitus jakaa tasaisesti, uskottiin suuren osan työmäärästä kuitenkin kohdistuvan projektipäällikölle. Riskin todennäköisyys oli hyvin tiedostettu ja siihen pyrittiin varautumaan aktiivisella projektin seurannalla ja tasaisella työnjaolla.

Viimeisenä riskinä oli kustannusriski, joka tarkoitti projektiin budjetoitujen kustannusten kasvamista. Riskin vakavuutta pidettiin melko pienenä, sillä projektista ei katsottu muodostuvan paljon kustannuksia, ja budjettiin oli varattu myös huomattava ylitysvara suhteessa odotettuihin kustannuksiin. Näistä syistä myös todennäköisyyttä budjetin ylittymisestä ja siitä aiheutuvista ongelmista pidettiin hyvin epätodennäköisenä.

4.2 Projektin toteutusvaihe

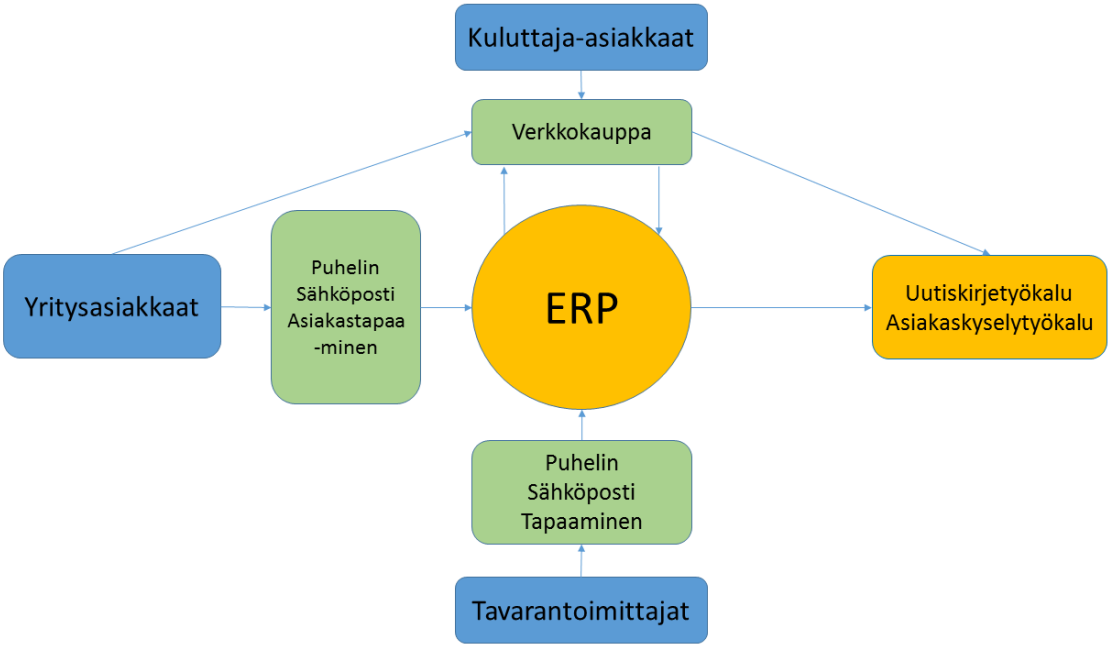
Projektin toteutus aloitettiin nykytilan kuvauksella. Nykytilan eli projektin lähtötilanteen kuvauksella oli tarkoitus saada mahdollisimman selkeä kuva yrityksen sen hetkisestä asiakkaiden henkilötietojen käsittelyn tilasta. Nykytilan analyysi sisälsi käytössä olevien rekistereiden kartoituksen, niiden tietosuojan ja –turvan kartoituksen sekä riskianalyysin.

Kun yrityksen lähtötilanne oli selvillä, siirryttiin kartoittamaan tarvittavia toimenpiteitä, jotka täytyi suorittaa, jotta yrityksen henkilötietojen käsittely saataisiin vastaamaan prosessien osalta sekä teknisesti tietosuoja-asetuksen vaatimuksia. Toimenpiteiden kartoituksen jälkeen ryhdyttiin toteuttamaan suunniteltuja toimenpiteitä, joihin liittyi selosteiden ja ohjeiden laatiminen ja päivittäminen, sopimusten uusiminen sekä toiminnanohjausjärjestelmään liittyvät uudistukset.

Toimenpiteiden suorittamisen jälkeen prosessit ja järjestelmän toiminnot testattiin yksitellen sekä kokonaisuutena, suorittamalla asiakaspolku vaihevaiheelta läpi. Testauksessa käytettiin hyväksi tarkistuslistaa, johon oli kirjattu tietosuoja-asetuksen vaatimukset rekisterinpitäjälle.

4.2.1 Lähtötilanteen kuvaus

Lähtötilanteen kuvaus aloitettiin selvittämällä mitä kautta henkilötietoja kerättiin, mitä tietoja asiakkaista oli kerätty sekä mihin rekistereihin tietoja oli tallennettu. Tämän jälkeen kartoitettiin järjestelmien toimittajat ja kuvattiin tietojen liikkuminen eri järjestelmien välillä.



Kuvio 4. Henkilötietojen kulku yrityksen asiakas- ja uutiskirjerekisteriin

Yritys ei kerää tai osta henkilötietoja kolmansilta osapuolilta vaan kaikki yrityksen käyttämät henkilötiedot kerätään rekisteröidyiltä itseltään. Kuluttaja-asiakkaita palvellaan pääasiassa verkkokaupan kautta, jolloin kuluttaja-asiakas syöttää verkkokauppaan toivomansa palvelun toimittamiseen tarvittavat tiedot. Asiakas voi tilata tuotteita verkkokaupan kautta, jolloin asiakkaasta kerätään tilauksen toimittamista ja maksamista varten tarvittavat tiedot.

Asiakas voi tilata verkkokaupan kautta myös pelkän uutiskirjeen, jolloin asiakkaalta kerätään vain sähköpostiosoite ja tieto siitä, onko hän yritys vai kuluttaja-asiakas. Kuluttaja-asiakkaan sähköpostiosoite voidaan myös siirtää yrityksen toiminnanohjausjärjestelmästä uutiskirjerekisteriin jos asiakas on antanut rekisteröityessään verkkokaupan asiakkaaksi suostumuksensa suoramarkkinointiin.

Yritysasiakkaiden tietoja kerätään asiakkaan tilatessa puhelimitse, sähköpostilla tai asiakastapaamisessa yrityksen edustajan kanssa. Yrityksen työntekijät syöttävät kerätyt tiedot toiminnanohjausjärjestelmään. Järjestelmästä voidaan siirtää asiakkaan sähköpostiosoite yrityksen uutiskirjerekisteriin, jos yritysasiakkaan yhteyshenkilö on antanut siihen suostumuksen.

Tavarantoimittajien yhteystietoja kerätään samalla tavalla kuin yritysasiakkaiden tietoja, eli puhelimitse, sähköpostitse tai tapaamisessa yrityksen edustajan kanssa. Tavarantoimittajien tietoja ei siirretä uutiskirjerekisteriin.

Taulukko 3. Asiakas- ja uutiskirjerekisterien tietosisältö

Asiakasrekisterin tietosisältö
Yhteystiedot Etunimi, sukunimi, katuosoite, postinumero, postitoimipaikka, puhelinnumero, sähköpostiosoite, käyttäjätunnus, salasana, markkinointilupa/-kielto.
Toimitustiedot Vaihtoehtoinen toimitusosoite, noutopiste, toimitustapa
Yritysasiakkaan yhteystiedot Organisaation nimi, postiosoite, postinumero, postitoimipaikka, yhteyshenkilön etunimi, yhteyshenkilön sukunimi, sähköposti, puhelin, gsm, asema, käyttäjätunnus, salasana.
Ostohistoriatiedot Tilatut tuotteet, määrät ja hinnat
Maksutiedot Maksutapa
Uutiskirjerekisterin tietosisältö
Sähköpostiosoite, tieto siitä onko asiakas yritysasiakas vai kuluttaja-asiakas, etunimi, sukunimi, yrityksen nimi.

Rekisteröityjen henkilötietojen luovutukset kolmansille osapuolille on hyvä kuvata visuaalisesti, jotta yrityksessä hahmotetaan kaikki ne tahot joille tietoja luovutetaan perustoimintojen toteuttamiseksi. Yrityksen työntekijöillä voi olla harhaluulo, ettei yrityksen hallinnoimia rekisteröityjen henkilötietoja pääse näkemään tai käsittelemään muut kuin yrityksen oma henkilökunta.

Kohde yritys ei luovuta keräämiään rekisteröityjen henkilötietoja kolmansille osapuolille muutoin kuin tilausten toimitusten ja maksutoimintojen järjestämiseksi sekä teknisille yhteistyökumppaneille järjestelmien toimivuuden varmistamiseksi.

Kuvio 5. Tietojen luovutukset yrityksen ERP-järjestelmästä

Nykytilan kartoitukseen liittyi olennaisesti myös riskianalyysi, joka tehtiin käyttämällä riskienarviointilomaketta. Riskiarviointilomakkeen mallina käytettiin valtionvarainministeriön laatiman riskiarviointityökalun ohjetta. Lomakkeelle kirjattiin kaikki tunnistetut riski. Riskeille määritettiin todennäköisyys asteikolla 1-4, jonka jälkeen arvioitiin riskin vaikutus yrityksen toimintaan. Riskille saatiin merkittävyysarvo kertomalla riskin todennäköisyydelle merkitty arvo riskin vaikutuksen arvolla. Arvojen määrityksen jälkeen taulukkoon kirjattiin sanalliset perustelut määritetyille riskitasoille sekä tarvittavat jatko- ja kehittämistoimenpiteet riskin minimoiseksi. Riskiarviointilomake laadittiin erikseen jokaiselle yrityksessä käytössä olevalle rekisterille.

Taulukko 4. Esimerkki riskien arviointiin käytetystä lomakkeesta

RISKIARVIOINTILOMAKE	Laatimispäivä	Päivitetty			
	25.4.2018	-			
Rekisterin nimi Yritys XXX:n asiakasrekisteri	**Järjestelmä** ERP	**Kartoituksen pvm:** 2.5.2018			
Kerätty henkilötieto Nimi, osoite, sähköposti, puhelinnumero Ostotapahtumaan liittyvät tiedot: Tilatut tuotteet, maksutapa, toimitustapa, noutopiste	**Riskin todennäköisyys** 1 = epätodennäköinen 2 = mahdollinen 3 = todennäköinen 4 = varma	**Riskin vaikutus** 1 = vähäinen 2 = kohtalainen 3 = merkittävä 4 = suuri	**Riskin merkittävyys** 1-4 = vähäinen 5-8 = kohtalainen 9-12 = merkittävä 13-16 = kriittinen		
Kuvaus riskistä Tiedot eivät ole ajan tasalla, tietojen päivittäminen epäonnistuu.	**3**	**2**		**6**	
Perustelut määritetyille riskitasoille Kuluttaja- ja verkkokauppa-asiakkaat voivat päivittää omat tietonsa kirjautumalla verkkokauppaan. Kuluttaja-asiakkaiden tietoja voidaan muuttaa ja päivittää rekisteriin kun asianomainen ottaa yhteyttä rekisterinpitäjään ja pyytää tietojensa päivittämistä.					

Yritysasiakkaiden tietoja päivitetään asiakkaiden tiedotettua tietojen muutoksesta tai yrityksen henkilökunnan tarkistaessa rekisterin tietojen ajantasaisuuden henkilökohtaisesti asianomaisen yrityksen edustajalta/yhteyshenkilöltä. Yritysasiakas rekisterin ollessa melko laaja sekä yritysten tietojen muuttuessa useasti, tietojen ajantasaisuudessa voi ilmetä puutteita.
Tarvittavat jatkotoimenpiteet Yrityksessä laaditaan asiakastietojen tarkastuslista, johon merkitään ne asiakastiedot, jotka pitää tarkastaa aina asiakkaan kanssa tekemisissä. Myyntiedustajat tarkistavat tiedot tarkastuslistaa laajemmin asiakastapaamisten yhteydessä ja asiakkaiden tilatessa puhelimitse yrityksen työntekijä käy läpi asiakkaan tiedot asiakastietojen tarkastuslistan mukaisesti. Yrityksessä jatketaan vuosittain asiakkaille uutiskirjeen mukana lähetettävää kehotusta tarkastaa omat tiedot verkkokaupan asiakastiedot-osiossa.

4.2.2 Tarvittavien toimenpiteiden kartoitus

Nykytila-analyysin jälkeen kartoitettiin tarvittavat toimenpiteet, jotta yrityksen toiminta saatiin vastaamaan tietosuoja-asetuksen vaatimuksia. Jonkin asteisia toimenpiteitä tarvittiin lähes koko henkilötietojen käsittelyprosessin matkalle.

Ensimmäinen kohtaamispiste kuluttaja-asiakkaan kanssa on verkkokauppa. Yritys käyttää verkkosivuillaan evästeitä, jolloin evästeistä tiedottamista oli tarpeellista muuttaa. Projektia toteutettaessa Suomessa ei vaadittu erillistä ponnahdusikkunaa tiedottamaan evästeistä, vaan käytettävistä evästeistä tuli tiedottaa sivustolla niin, että vierailija pystyi halutessaan lukemaan yrityksen evästekäytännöistä. Viestintävirasto myös tulkitsi silloin voimassa ollutta sähköisen viestinnän tietosuojadirektiiviä, niin että vierailijan tuli itse estää omasta selaimestaan evästeet, mikäli ei antanut verkkosivulle lupaa kerätä tietoja itsestään evästeillä. (Viestintävirasto 2017.) Yritys ei käyttänyt evästeistä ilmoittavaa ponnahdusikkunaa, koska piti sitä enemmän käyttäjää häiritsevänä ja oletti evästeiden käytön olevan yleisessä tiedossa ja piti näin ollen riittävänä evästeistä tiedottamista info-sivulla.

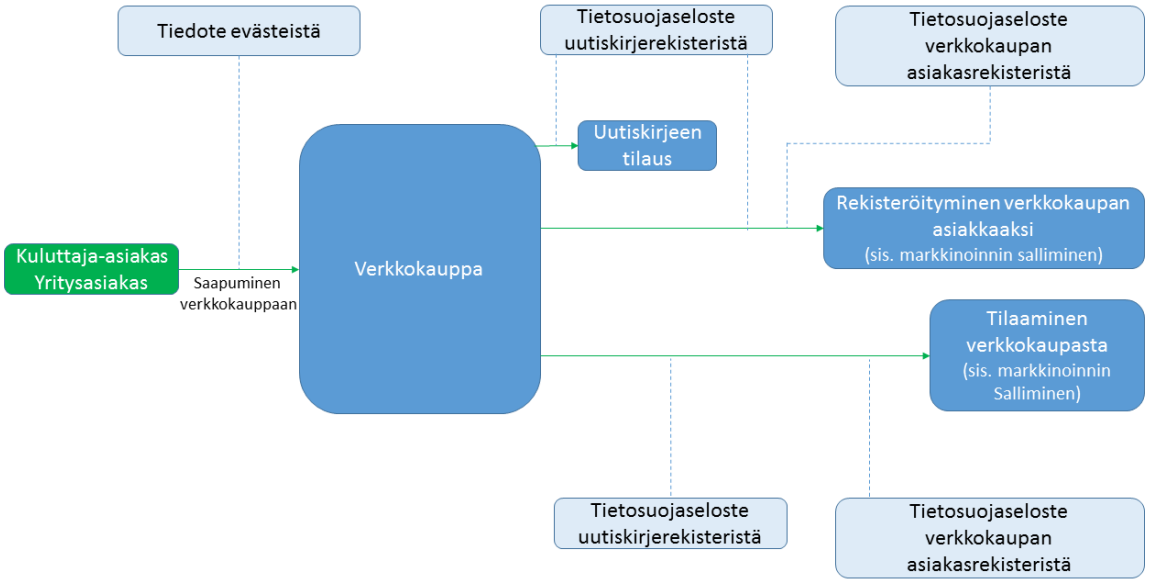
Tietosuoja-asetus ei suoraan tuonut muutosta evästeistä tieodottamiseen, vaikka suostumuksen edellytykset sen myötä muuttuivatkin. Suomessa Viestintävirasto ei ollut tätä kirjoittaessakaan vielä muuttanut evästekäytäntöjen tulkintaa, vaan odotti tulevaa sähköisen viestinnän tietosuoja-asetusta, ennen kuin uudelleen arvioi evästeisiin liittyviä käytäntöjä. (Viestintävirasto 2017.)

Yritys kuitenkin halusi valmistautua mahdolliseen tulevaan muutokseen tiedottamisessa, ja tiedusteli verkkokaupan tarjoajalta ponnahdusikkuna-ominaisuutta liitettäväksi verkkokauppaan. Ominaisuus oli olemassa ja se oli käyttäjän itse helposti lisättävissä verkkokauppaan tarvittaessa. Yritys päätti jättää ominaisuuden toistaiseksi käyttämättä, ja päätti seurata viestintäviraston ja tietosuojavaltuutetun tiedottamista asian tiimoilta. Myöskään

viestintävirasto ei käyttänyt tätä kirjoittaessa ponnahdusikkunoita evästeistä tiedottamiseen.

Verkkokauppaan siirtymisen jälkeen oli oletettavaa, että mikäli vierailija jatkaa sivuston selausta, seuraava vierailijan suorittama toimenpide sivustolla on joko uutiskirjeen tilaus, jolloin asiakasta pitää informoida uutiskirjettä varten kerättyjen tietojen käytöstä tai asiakas rekisteröityy verkkokauppaan tai tilaa tuotteita verkkokaupasta, jolloin asiakasta informoidaan näiden toimintojen toteuttamista varten kerättyjen tietojen käytöstä.

Yrityksellä oli jo käytössään henkilötietolain vaatimat rekisteriselosteet, jotka asiakkaan tuli lukea ja hyväksyä ruksittamalla kohta ”Olen lukenut ja hyväksyn Yritys XXX:n käyttöehdot ja rekisteriselosteen”. Käytössä olevat rekisteriselosteet tuli päivittää tietosuoja-asetuksen mukaisiin tietosuojaselosteisiin.



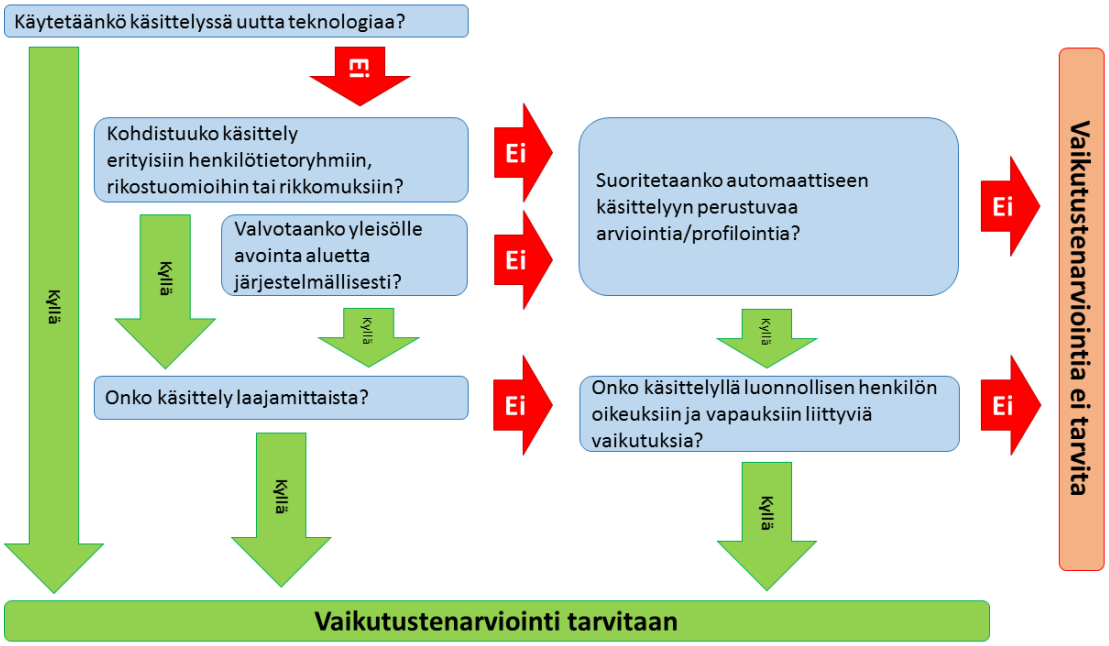
Kuvio 6. Verkkokaupan tietosuojaselosteet asiakaspolun eri vaiheissa.

Verkkosivuille lisättävien tietosuojaselosteiden lisäksi täytyi tehdä selosteet käsittelytoimista. Selosteet käsittelytoimista ovat yrityksen omaan käyttöön selventämään yrityksen tietojenkäsittelyprosessia ja luovutettaviksi viranomaisille mikäli nämä niitä pyytävät. Selosteet käsittelytoimista muodostavat tärkeän osan yrityksen osoitusvelvollisuudesta. (Tietosuojavaltuutetun toimisto 2018.)

Toiminnanohjausjärjestelmään tehtäviä toimenpiteitä varten selvitettiin ensin tietosuoja-asetuksen asettamia vaatimuksia ja velvollisuuksia rekisteripitäjää kohtaan, jonka jälkeen

tarkasteltiin asetuksen myötä rekisteröidylle tulevia oikeuksia. Selvityksen myötä todettiin, että yrityksen toiminnanohjausjärjestelmään tarvitaan raportti, jonka avulla voidaan tulostaa rekisteröidystä kerätyt tiedot. Samassa selvityksen yhteydessä huomattiin tarve tehdä rajoituksia työntekijöiden rekisterin muokkausoikeuksiin.

Tietosuoja-asetuksessa rekisterinpitäjä velvoitetaan tekemään vaikutustenarviointi, mikäli henkilötietojen käsittelyyn liittyy todennäköinen korkea riski luonnollisen henkilön oikeuksille tai vapauksille. (Yleinen tietosuoja-asetus 2016/679, (90).) Vaikka yrityksessä suoritettavasta henkilötietojen käsittelystä ei kohdistuisi merkittävää riskiä rekisteröidyn oikeuksille tai vapauksille tai henkilötietojen käsittely ei liittyisi erityisiin henkilötietoryhmiin, täytyy rekisterinpitäjän joka tapauksessa arvioida vaikutustenarvioinnin tarpeellisuutta. Kohdeyrityksessä tarkasteltiin eri rekisterien tietojen käsittelyä alla olevan kaavion mukaan ja päädyttiin johtopäätökseen, ettei yrityksen tarvitse tehdä asiakas- ja markkinointirekisterien osalta vaikutustenarviointia.



Kuvio 7. Vaikutustenarvioinnin tarpeen määritys

Kohdeyrityksen asiakas- ja markkinointirekistereissä ei käsitellä erityisiin henkilötietoryhmiin liittyviä tietoja eikä henkilötietojen käsittelyyn kohdistu luonnollisen henkilön oikeuksiin tai vapauksiin liittyviä riskejä. Henkilötietojen käsittelyn vaikutukset eivät ole merkittäviä eikä käsittelyyn liittyvien riskien realisoituminen ole todennäköistä. Vaikutustenarvioinnin tekemättä jättämispäätökseen vaikuttaneet asiat dokumentoitiin, ja dokumentit liitettiin muiden henkilötietojen käsittelyyn liittyvien selosteiden ja dokumenttien yhteyteen.

4.2.3 Selosteiden laatiminen ja käytänteiden dokumentointi

Uusien tietosuojaselosteiden runko oli pääpiirteittäin sama vanhan rekisteriselosteen kanssa, joten itse selosteen päivittäminen ei osoittautunut kovin suureksi työksi kun ensin oli selvitetty tietosuoja-asetuksen vaatimukset tietosuojaselosteelle. Tietosuoja-asetuksessa oli tarkat määritykset tietosuojaselosteen sisällölle. Yritys keräsi tietoja suoraan rekisteröidyiltä, joten yritys muodosti tietosuojaselosteet yleisen tietosuoja-asetuksen 13 artiklan mukaan.

Taulukko 5. Tietosuojaselosteeseen vaaditut tiedot Tietosuoja-asetuksen 13 artiklan mukaan (Yleinen tietosuoja-asetus 2016/679, 13 artikla).

1.	**Kerättäessä rekisteröidyltä häntä koskevia henkilötietoja rekisterinpitäjän on silloin, kun henkilötietoja saadaan, toimitettava rekisteröidylle kaikki seuraavat tiedot:**
a)	Rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot
b)	Tapauksen mukaan tietosuojavastaavan yhteystiedot *Tietosuojavastaavan nimittämisestä säädetään asetuksen 37 artiklassa*
c)	Henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste
d)	Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu 6 artiklan 1 kohdan f alakohtaan. *Tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohtaa voidaan käyttää käsittelyn oikeusperustana, jos käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Kohtaan käytetään oikeusperusteena esimerkiksi suoramarkkinoinnin ja uutiskirjeiden lähettämiseen.*
d)	Henkilötietojen vastaanottajat tai vastaanottajaryhmät
e)	Tapauksen mukaan tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, ja tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, tai jos kyseessä on 46 tai 47 artiklassa tai 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, tieto sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville. *Artiklassa 46 säädetään tiedonsiirtoon sovellettavista asianmukaisista suojatoimista.* *Artiklassa 47 säädetään yritystä sitovista säännöistä koskien tiedonsiirtoa yritysryhmän tai konsernin sisällä.* *Artiklan 49 kohdan 1 toisessa alakohdassa tarkoitettu siirto on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöönpanemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.*
2.	**Edellä 1 kohdassa tarkoitettujen tietojen lisäksi rekisterinpitäjän on silloin, kun henkilötietoja saadaan, toimitettava rekisteröidylle seuraavat lisätiedot, jotka ovat tarpeen asianmukaisen ja läpinäkyvän käsittelyn takaamiseksi:**
a)	henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;
b)	Rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen;

c)	Oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu 6 artiklan 1 kohdan a alakohtaan tai 9 artiklan 2 kohdan a alakohtaan; *6 artiklan 1 kohdan a alakohdassa käsittelyn perusteena on rekisteröidyn suostumus yhteen tai useampaa tarkoitusta varten.* *Artiklassa 9 kielletään erityisten henkilötietoryhmien käsittely. 9 artiklan 2 kohdan a alakohdassa määritetään, ettei 9 artiklan kieltoa sovelleta, jos rekisteröity on antanut suostumuksensa erityisten henkilötietojen käsittelyyn.*
d)	Oikeus tehdä valitus valvontaviranomaiselle
e)	Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset;
f)	Automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle. *22 artiklan 1 kohdassa säädetään rekisteröidyn oikeudesta olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn.* *22 artiklan 4 kohdassa säädetään poikkeuksista, jolloin automaattista päätöksentekoa voidaan käyttää myös silloin kun päätös perustuu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin henkilötietoryhmiin.*

Tietosuojaselosteiden laadinnassa kohdattiin haasteita, jotka liittyivät selosteiden sisällön ilmaisuun. Tietosuoja-asetuksessa määritetään, että kuluttajien saataville asetettavien selosteiden tulisi olla selkeitä ja helposti ymmärrettäviä (Yleinen tietosuoja-asetus 2016/679, (39)). Kuitenkin WP29-työryhmän julkaiseman tulkintaohjeistuksen mukaan selosteiden pitäisi olla kattavia ja tarkkoja ja esitetty tiiviissä muodossa. Pohdintaa aiheutti myös ohjeistuksessa oleva kohta, jossa rekisterinpitäjän pitäisi nimetä EU:n ulkopuoliset maat, joihin tietoja siirretään sekä ohjeistus olla käyttämättä sanoja ”mahdollisesti ja saatamme”. (European Commission 2018, 8, 38.)

Edellä mainittujen sanojen käyttämättä jättäminen sekä kolmansien maiden nimeäminen tarkoittaisi käytännössä sitä, että yrityksen pitäisi etukäteen tietää, aikooko se tulevaisuudessa siirtää tietoja kolmansiin maihin ja mihin maihin tietoja on tarkoitus siirtää. Suurin ongelma tässä oli se, että kohde yritys ei itse varsinaisesti voinut päättää minne tietoja tulevaisuudessa siirrettäisiin. Yritys käyttää sähköisten palveluiden tuottamiseen palvelun-tarjoajia, joiden kanssa tehdyissä sopimuksissa on maininta mahdollisuudesta tietojen siirtoon EU:n tai ETA:n ulkopuolisiin maihin palveluiden teknisen toteuttamisen mahdollistamiseksi.

Yritys päätti käyttää vähemmän suositeltua ilmaisua ja kertoa rekisteröidyille tietojen mahdollisesta siirrosta EU:n tai ETA:n ulkopuolelle palvelun toteuttamista varten, ja mikäli näin

tehdään, tietojen siirto toteutetaan voimassa olevan lain edellyttämällä tavalla. Edellä mainittu tapa näytti muodostuvan yleiseksi tavaksi yritysten tietosuojaselosteissa.

Yrityksessä tiedostettiin, että tietojen käsittelyn tarkkojen ja kattavien kuvausten esittäminen tiiviissä ja selkeässä muodossa voisi muodostua ongelmaksi, joten alkuun selosteita laatiessa täytyisi valita jompikumpi. Yritys päätyi laatimaan aluksi kattavan selostuksen, jota työstettäisiin myöhemmin kun tietosuojavaltuutetun omat verkkosivut uudistuisivat, joita voitaisiin peilata omiin selosteisiin. Yrityksessä myös todettiin, että tarkkojen ja kattavien kuvausten antaminen ilmentää paremmin tietosuoja-asetuksen henkeä läpinäkyvästä tietojen käsittelystä. Yritys myös käsitti määritelmät ”tiivis” ja ”selkeä”, jossain määrin subjektiivisiksi käsitteiksi, joista voitiin alkuun tinkiä. Yrityksessä kuitenkin tiedostettiin tietosuoja-asetuksen pyrkimys saada selosteista niin sanotusti kansantajuisia. Tätä puolta oli tarkoitus työstää myöhemmässä vaiheessa.

Yritys piti tärkeänä, että rekisteröidyille kerrotaan tarkasti ja avoimesti heidän tietojensa käytöstä. Tällä pyrittiin myös vähentämään rekisteröityjen tarvetta ottaa yritykseen yhteyttä tiedustellakseen omien tietojensa käytöstä ja käsittelystä.

Tietosuojaselosteiden valmistuttua, laadittiin selosteet käsittelytoimista, joiden rakenne ja vaadittu tietosisältö saatiin suoraan tietosuoja-asetuksen 30 artiklasta. Selosteiden laatiminen viivästyi, koska yritys joutui odottamaan teknisten yhteistyökumppaneiden ja palveluntarjoajien selvityksiä käyttämistään teknisistä ja organisatorista toimista. Moni toimija viivytti omien selosteidensa julkaisua mahdollisimman pitkään ja toimitti suuntaa antavan selosteen kunnes palveluntarjoajan lakimies oli tarkastanut selosteen. Palvelun tarjoajat sanoivat selosteiden toimittamisen viivyttämisen syyksi tietosuoja-asetuksen tulkintojen jatkuvan tarkentumisen.

Taulukko 6. Vaaditut tiedot selosteisiin käsittelytoimista (Yleinen tietosuoja-asetus 2016/679, 30 artikla).

1.	**Jokaisen rekisterinpitäjän ja tarvittaessa rekisterinpitäjän edustajan on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista. Selosteen on käsitettävä kaikki seuraavat tiedot:**
a)	Rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot;
b)	käsittelyn tarkoitukset;
c)	kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä;
d)	henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan, mukaan lukien kolmansissa maissa tai kansainvälisissä järjestöissä olevat vastaanottajat;

e)	tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, mukaan lukien tieto siitä, mikä kolmas maa tai kansainvälinen järjestö on kyseessä, sekä asianmukaisia suojatoimia koskevat asiakirjat, jos kyseessä on 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto; *Artiklan 49 kohdan 1 toisessa alakohdassa tarkoitettu siirto on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöönpanemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.*
f)	mahdollisuuksien mukaan eri tietoryhmien poistamisen suunnitellut määräajat;
g)	mahdollisuuksien mukaan yleinen kuvaus 32 artiklan 1 kohdassa tarkoitetuista teknisistä ja organisatorisista turvatoimista. *32 artiklan 1 kohdassa määritettyjä toimenpiteitä ovat muun muassa henkilötietojen pseudonymisointi ja salaus, kyky taata käsittelyohjelmien ja palveluiden jatkuva luottamuksellisuus, käytettävyys, eheys ja vikasietoisuus. Kyky palauttaa pääsy tietoihin fyysisen ja teknisen vian sattuessa. Menettelyt, joilla testataan teknisten ja organisatoristen toimenpiteiden tehokkuutta.*

Selosteiden ja käytänteiden dokumentoinnin kanssa laadittiin kohdeyritykselle ohjeistus asetuksen mukaisesta henkilötietojen käsittelystä. Ohjeistukseen lisättiin liitteeksi lomake (liite 1), joka rekisteröidyn tulee täyttää, mikäli rekisteröity haluaa käyttää tietosuoja-asetuksessa hänelle määritettyjä oikeuksiaan. Käytännössä tämä tarkoittaa mahdollisuutta tehdä hänen omia henkilötietojaan koskevan pyynnön.

Viranomaisille ilmoittamista varten laadittiin lomake (liite 2), jonka sisällön määrittämisen apuna käytettiin Helsingin kauppakamari Oy:n kustantamaa kirjaa ”Henkilötietojen käsittely, EU-tietosuoja-asetuksen vaatimukset”. Toukokuun lopussa tietosuojavaltuutetun toimisto julkaisi uudet verkkosivut, joilla oli kattavat ohjeet tietoturvaloukkauksesta tehtävää viranomaisilmoitusta varten sekä sähköinen lomake, jolla kyseisen ilmoituksen voi kätevästi tehdä. Kohdeyrityksen ohjeistukseen lisättiin sähköisen ilmoituslomakkeen osoite, sekä suositeltiin käyttämään ensisijaisesti tietosuojavaltuutetun omaa lomaketta ilmoituksen tekemiseen.

4.2.4 Toiminnanohjausjärjestelmän päivitykset ja käyttöoikeuksien tarkistaminen

Järjestelmien osalta tuli varmistaa, että tietoturva ja tietojen suojaus oli asianmukaisesti hoidettu ja vastasi tietosuoja-asetuksen vaatimuksia. Yrityksen keräämät henkilötietorekisterit sijaitsevat palvelimilla, jotka on suojattu palomuurilla, ajantasaisella virusturvalla. Rekistereitä käytetään salatun yhteyden yli.

Yrityksen työntekijöiden käyttöoikeudet käytiin läpi ja niihin tehtiin tarvittavat muutokset. Käyttöoikeuksia ja tietojen muokkausoikeuksia kiristettiin, jotta vältettäisiin tietojen oikeellisuuteen ja eheyteen liittyvät ongelmat. Tietojen käyttö- ja muokkaus oikeudet jaettiin työntekijöille työtehtävien perusteella. Aiemmin työntekijät ovat päässeet käyttämään toimin-

nanohjausjärjestelmää syöttämällä etäyhteyden salasanan sekä myyjänumeron. Tietosuoja-asetuksen myötä edellä mainittujen toimien lisäksi jokaiselle työntekijälle määritettiin salasana, joka tulee syöttää ennen kuin järjestelmää pääsee käyttämään.

Toiminnanohjausjärjestelmään ladattiin raporttipohja, jonka avulla järjestelmästä voidaan tulostaa rekisteröidystä kerätyt tiedot, rekisteröidylle tiedottamista varten, mikäli rekisteröity käyttää oikeuttaan nähdä itsestään kerätyt tiedot. Samalla järjestelmään asennettiin aputyökalu, jolla voidaan poistaa ja anonymisoida tarvittaessa rekisteröidyn henkilötietoja.

Muihin käyttöliittymiin, joilla eri rekistereihin tallennettuja rekisteröityjen tietoja hallinnoitiin, ei tarvinnut tietosuoja-asetuksen myötä tehdä muutoksia. Myöskään muiden käyttöliittymien käyttäjien oikeuksiin ei ollut tarpeellista tehdä muutoksia tiedonkäsittelijöiden vähäisen määrän vuoksi.

4.3 Testaus ja projektin päättäminen

Vaadittujen toimenpiteiden toteuttamisen jälkeen muutosten toimivuutta testattiin. Testivaihe jaettiin kolmeen osaan; yksikkötestaukseen, järjestelmätestaukseen sekä toimenpidetestaukseen. Yksikkötestauksessa tarkasteltiin yksittäisten osa-alueiden toimivuutta ja tietosuoja-asetuksen vaatimusten mukaisuutta. Yksikkötestaus suoritettiin tarkastuslomakkeen avulla (liite 3). Järjestelmätestauksessa testattiin järjestelmään lisättyjen ominaisuuksien ja raporttien toimivuus.

Toimenpidetestauksessa testattiin yksiköiden ja järjestelmän kokonaistoimivuutta. Testauksessa hyödynnettiin lähtötilanteen kuvausvaiheessa tehtyä riskianalyysiä. Riskianalyysi tehtiin ennen testausta uudelleen ja katsottiin onko lähtötilanteen kuvausvaiheessa tehtyyn riskianalyysiin kirjattujen riskien todennäköisyysluokkaa saatu projektin myötä pudotettua ja onko riskejä tullut lisää.

Toimenpidetestauksessa käytiin myös läpi koko asiakaspolku verkkosivuille saapumisesta tuotteiden tilaamiseen sekä tilanteet, joissa rekisteröity käyttää tietosuoja-asetuksen hänelle suomia oikeuksiaan. Oikeuksien käyttötilanteissa testattiin rekisteröidyn pyyntö nähdä itseään koskevat tiedot, rekisteröidyn pyyntö siirtää itseään koskevat tiedot järjestelmästä toiseen sekä rekisteröidystä kerättyjen tietojen poisto, rekisteröidyn pyytäessä itse tietojen poistoa tai rekisterinpitäjän todetessa tietojen olevan tarpeettomia.

Projektin onnistumista testattiin käymällä riskikartoitukseen merkatut riskit läpi niin, että jokaisen riskin realisoituessa yrityksestä löytyy toimintaohje miten riskin vaikutukset minimoidaan ja miten tilanteessa toimitaan viranomaisten, rekisteröityjen ja teknisten yhteistyökumppaneiden kanssa.

Projektin päätös oli merkitty 24.5.2018, mutta projekti ei ollut tällöin vielä kaikilta osin valmis. Tietosuoja-asetuksen siirtymäajan päättymispäivänä 24.5. yritys latasi uudet tietosuoja-asetuksen mukaiset tietosuojaselosteet verkkosivuille. Selosteet käsittelytoimista sekä henkilötietojen käsittelyohjeet olivat myös valmiit siirtymäajan päättyessä.

Järjestelmään ladattavat raportit, joiden avulla voidaan tulostaa rekisteröityjen tiedot sekä tietojen poisto työkalu eivät olleet vielä käytettävissä tietosuoja-asetuksen voimaan tullessa. Edellä mainitut ominaisuudet olivat lisättävissä ja asennettavissa vasta lähellä tietosuoja-asetuksen siirtymäajan päättymistä, jolloin näitä ei ehditty asentaa. Asennus suoritettiin kesäkuun lopulla ja kesälomista johtuen uusien toimintojen testaus suoritettiin kokonaisuudessaan vasta elokuussa.

5 Pohdinta

Produkti onnistui mielestäni hyvin, vaikka se osoittautuikin ennakoitua haasteellisemmaksi. Kohdeyrityksen asiakas- ja markkinointirekisterien käsittely saatiin päivitettyä yleisen tietosuoja-asetuksen mukaiseksi suunnitellussa aikataulussa. Tietosuoja-asetukseen valmistautuminen oli yrityksen kannalta kaiken kaikkiaan hyödyllinen kokemus, ja kaikesta vaivasta huolimatta projektin tuoma hyöty on osoittautunut vaivaa suuremmaksi.

Produkti käynnisti rekisterien siivousprosessin, jonka seurauksena rekisterien sisältöjä alettiin yrityksessä käymään läpi tarkoituksena poistaa tarpeettomaksi käyneitä tietoja. Samalla rekisterien ja sisältöjen tarpeellisuudesta alettiin käymään keskusteluita, joiden seurauksena yrityksessä on tiedostettu mitä tietoja kannattaa kerätä ja mitä ei, tällöin resursseja kulu turhan tiedon keräämiseen ja taltioimiseen. Projektin myötä tietojen käsittelyyn ja eheyden varmistamiseen laadittiin ohjeistus, jolloin rekisterien tietojen ajantasaisuuteen voidaan luottaa, eikä aikaa kulu esimerkiksi yhteystietojen turhaan tarkisteluun.

Produktin ensisijaisena tavoitteena oli saattaa kohdeyrityksen henkilötietojen käsittely tietosuoja-asetuksen mukaiseksi ja luoda selkeä ja helposti ymmärrettävä kuvaus toimista, jotka yrityksen tulee suorittaa kun se aloittaa henkilötietojen keräämisen ja käsittelyn. Mielestäni onnistuin tässä kohtuullisen hyvin. Raportissa käydään loogisesti läpi henkilötietojen käsittelyyn valmistautuminen projektisuunnitelmasta, lähtötilanteen kuvauksen kautta tarvittavien toimenpiteiden kartoittamiseen. Alkutoimenpiteitä seuraa määritettyjen toimenpiteiden suorittaminen sekä toteutettujen toimenpiteiden testaus ja produktin päättäminen. Raporttiin on sisällytetty sanallisen kerronnan lisäksi kuvioita ja taulukoita helpottamaan suhteellisen monimutkaisen asiakokonaisuuden hahmottamista.

5.1 Opinnäytetyöprosessin arviointi

Valitsin opinnäytetyön aiheeksi EU:n tietosuoja-asetuksen sen ajankohtaisuuden vuoksi ja myös sen takia, että aihe liittyi vahvasti omaan työhöni. Ajattelin kirjoittavani opinnäytetyön jouhevasti samalla kun laadin työpaikalleni tietosuoja-asetuksen mukaisia dokumentteja ja ohjeistuksia. Opinnäytetyöprosessi osoittautui kuitenkin oletettua konstikkaammaksi, sillä ennen tietosuoja- ja opinnäytetyöprosessin aloitusta ilmeni tapahtumaketju, joka vaikutti työtä hankaloittavasti koko prosessin ajan.

Tietosuoja-asetukseen valmistautumista sekä opinnäytetyöprosessin sujuvaa läpivientiä haittasi yrityksessä yllättäen tapahtuneet henkilöstömuutokset, joihin en osannut varautua oikein projektisuunnitelmaa laatiessani. Seitsemän hengen yrityksessä työntekijämäärän

tiputtua suhteellisen lyhyessä ajassa neljään työntekijään, muutos oli merkittävä ja vaikutti suuresti kaikkien toimenkuviin. Riskianalyysissä otin huomioon työntekijöihin kohdistuvana riskinä sairastumiset, mutta jostain syystä jätin huomioimatta mahdolliset työsuhteiden päättymiset sekä uusien työntekijöiden rekrytointien viivästymiset.

Opinnäytetyön ja produktin tekoa hidasti myös luotettavan tiedon saanti. EU:n uusi tietosuoja-asetus oli astunut voimaan jo keväällä 2016, mutta vielä huhtikuun puolivälissä 2018 tietosuojavaltuutetun toimisto ei ottanut kantaa yksittäisten organisaatioiden kysymyksiin tietosuoja-asetuksen soveltamisesta tai tulkinnoista. Tietosuojavaltuutetun toimisto lisäsi ohjeistuksia sivuilleen sitä mukaan kun niitä valmistui. Osa ohjeistuksista tuli hyvinkin lähellä siirtymäajan päättymistä. Tietosuojavaltuutetun toimiston verkkosivujen oli tarkoitus uudistua kokonaisuudessaan toukokuun 2018 aikana, ja samassa esimerkkilomakkeiden piti olla tietosuoja-asetuksen mukaisia. Verkkosivut ja lomakkeet olivat vielä 16.5.2018 uudistumatta.

Prosessin haastavuutta pienyrityksen kannalta lisäsi se, että valmistautumista tietosuoja-asetukseen ei voinut jättää pelkästään 173 johdantokappaletta ja 99 artiklaa sisältävän tietosuoja-uudistuksen lukemisen varaan, vaan tämän lisäksi piti myös seurata EU:n kansallisista tietosuojaviranomaisista koostuvan WP29-työryhmän tasaisin väliajoin julkaisemia ohjeistuksia tietosuoja-asetuksen tulkinnoista. WP29-työryhmän ohjeistuksia tuli vielä lähellä tietosuoja-asetuksen siirtymäajan päättymistä. Haastavuutta lisäsi se, että ohjeistukset olivat monesti englanninkielisiä. Ongelmia tietosuoja-asetuksen aikarajan noudattamisessa tuotti myös seurantaevästeiden sääntelyyn liittyvän sähköisen viestinnän tietosuoja-asetuksen viivästyminen.

Tietosuoja-asetuksen tulkinnanvaraisuus sekä WP29-työryhmän tulkintojen ajoittainen ristiriitaisuus tietosuoja-asetuksen kanssa näytti antavan konsultti- ja asiantuntijaorganisaatioille tilaisuuden esittää blogikirjoituksissa omia tulkintoja viranomaisten julkaisuista. Tämä hankaloitti, ainakin alussa omaa selvitystyötä ja kokonaisuuden hahmottamista.

Tietosuoja-asetuksen ajatus ja perusperiaate on sinällään kunnioitettava ja yksinkertainen. Asetuksellahan pyritään ohjaamaan yritykset avoimempaan tiedottamiseen henkilötietojen käsittelystä sekä tarkastamaan, että omat toimintamallit ovat asianmukaiset ja, että henkilötietojen käsittelyssä kunnioitetaan rekisteröityä ja hänen tietojaan. Jarkko Reitun mukaan tietosuoja-asetus on tarkoituksellisesti jätetty tulkinnanvaraiseksi, jolloin rekisterinpitäjällä on mahdollisuus päättää tarvittavista toimenpiteistä (Reittu 2017, 3). Tätä tarkoituksen mukaista tulkinnanvaraisuutta ei ole viranomaisten taholta juurikaan mainostettu, tai se on jäänyt allekirjoittaneelta huomaamatta. Mahdollisuus päättää tarvittavista

oman yrityksen toimintaan soveltuvista toimenpiteistä on kaksiteräinen miekka, etenkin silloin kun pienessä yrityksessä ei ole riittävää asiantuntevuutta tunnistaa niitä toimenpiteitä, joilla asetuksen vaatimukset täytetään. Pienen yrityksen kannalta olisi ollut helpompaa, mikäli viranomaisilta olisi saanut ajoissa selkeät ohjeet tietosuoja-asetuksen suhteen. Asetuksen voimaan astuminen tulkinnanvaraisena ja edelleen muuttuvana asettaa suuren haasteen pienelle yritykselle pystyä noudattamaan asetusta.

Tietosuoja-asetuksen tuloa alettiin tiedottamaan noin vuosi ennen siirtymäajan päättymistä eri asiantuntijaorganisaatioiden toimesta, ja viestinnän kärkinä olivat suuret sanktiot sekä ”monimutkainen” uusi asetus. Tietosuojavaltuutetun toimiston joulukuisen blogi-kirjoituksen mukaan yritykset lähtivät kankeasti valmistautumaan tietosuoja-asetukseen ja sakoilla uhkailu oli yksi konsulttien tapa herättää yritysjohtajat toimimaan (Tietosuojavaltuutetun toimisto 2017).

Suurten sanktioiden pelko sekä tietämättömyys lainlaatijoiden tarkoituksen mukaisesta tulkinnanvaraisuudesta lisäsi tarvetta pyrkiä noudattamaan asetusta sekä WP29-työryhmän tulkintoja erityisen tarkasti. Jossain vaiheessa asiantuntijaorganisaatioiden viestinnässä ei enää tuotu esiin voimallisesti sanktioita, vaan sanktio politiikkaa käsiteltiin realistisemmin ja esimerkiksi blogikirjoituksissa tuotiin esiin, ettei sakko ole ensimmäinen vaihtoehto viranomaisen huomatessa puutteita yrityksen henkilötietojen käsittelyssä.

Sanktiokeskustelun laannuttua sekä kansallisen tietosuojalain ja sähköisen viestinnän tietosuoja-asetuksen viivästyttyä ilmapiiri muuttui jossain määrin toiseen ääripäähän. Kiire kaikkosi ja yritykset jäivät odottavalle kannalle. Odottava ilmapiiri oli havaittavissa myös tietosuojavaltuutetun sivustolla, jonka olisi luullut olevan uudistettu ja sisältävän tietosuoja-asetuksen mukaiset mallilomakkeet jo asetuksen astuttua voimaan 2016. Tiedustellessani yhteistyökumppaneilta uusia sopimuksia sain vastaukseksi lähes järjestään, että sopimukset ovat vielä lakimiehillä tarkastettavina.

Projektisuunnitelmaa laatiessani määrittelin, että tarkastelen tuotosten laatua muun muassa vertaamalla selosteita muiden yritysten selosteisiin, mutta saatuani tietosuojaselosteet valmiiksi huomasin, että vain harva yritys oli päivittänyt verkkosivuilleen tietosuoja-asetuksen mukaisen tietosuojaselosteen. Yritysten päivitetyt selosteet myös erosivat toisistaan paljon. Tietosuojavaltuutetun toimiston verkkosivujen luvattu uudistuminen tapahtui niin lähellä siirtymäajan päättymistä, ettei heidänkään malleihin voinut omia selosteita verrata.

Prosessin aikana en voinut välttyä ajatukselta, että tietosuoja-asetuksen tulkinnanvaraisuudella ja ajoittain julkaistavilla WP29-työryhmän tulkinnoilla pyrittiin lähinnä työllistämään lakitoimistoja sekä tietosuoja-asetukseen perehtyneitä asiantuntijaorganisaatioita. Pienen yrityksen on vaikea irrottaa resursseja ydintoiminnoista tulkintojen seuraamiseen. Sanktiot edellä toteutettu asetuksen ”markkinointi” asetti paineen pyrkiä mahdollisimman tarkkaan asetuksen noudattamiseen.

Uskon, että pienyrityksen valmistautuminen henkilötietojen käsittelyyn helpottuu tulevaisuudessa kun asetuksen tulkinta vakiintuu sekä kansallinen henkilötietolaki ja EU:n sähköisen viestinnän tietosuoja-asetus astuvat voimaan.

Rekisterien sähköistyminen ja tietojenkäsittelyn tehostuminen merkittävästi parinkymmenen viime vuoden aikana muodostivat perustellun syyn henkilötietojen käsittelyyn liittyvien lakien uudistamiselle. Ongelmana lakiuudistuksessa on mielestäni ollut se, että uudistuksen kohteena olevat asiat muodostavat monimutkaisen kokonaisuuden, jonka hallintaan on pyritty luomaan yksinkertainen asetus. Luulenkin, että tässä ristiriidassa on osa syy siihen, miksi asetus on jätetty tulkinnanvaraiseksi.

Portaittain etenevä tapa, jolla lainsäädäntö uudistuu, ei välttämättä ole pienyrityksenkään kannalta huono. Kun tietosuoja-asetus astui voimaan, yritykset joutuivat käymään läpi rekisterit ja henkilötietojen käsittelyprosessinsa. Vaikka asetuksen tulkinnanvaraisuus aiheutti epävarmuutta valittuja ratkaisuja kohtaan, oli yrityksissä kuitenkin viety henkilötietojen käsittelyyn liittyviä asioita rekisteröidyn kannalta rutkasti parempaan suuntaan.

Epävarmuus valittujen ratkaisujen lainmukaisuudesta pitää yritykset oletettavasti hereillä ja pakottaa seuraamaan asetuksen tulkintojen kehittymistä sekä päivittämään omia käytänteitä näitä vastaaviksi. Prosessin myötä avoimeksi jääneisiin kysymyksiin, kuten evästeistä tiedottamiseen liittyviin kohtiin, saadaan todennäköisesti selvennystä asetuksen seuraavassa vaiheessa, kun EU:n sähköisen viestinnän asetus astuu voimaan.

Lisää selvyyttä asetukseen saadaan kun tietosuoja-asetukseen liittyviä tulkintoja tarkennetaan oikeuskäytäntöjen kautta. Tämä ei tietenkään lohduta niitä, jotka omalla esimerkillään selventävät oikeuskäsittelyn kautta oikeaa ja väärää tapaa käsitellä henkilötietoja.

Sakkoja pelätessä on kuitenkin hyvä muistaa, etteivät sakot ja rekisterien käyttökiellot ole kuitenkaan viranomaisen ensimmäinen vaihtoehto. Mikäli henkilötietojen käsittelyssä havaitaan puutteita, viranomaisten työkalupakissa on muun muassa varoitus, huomautus ja

määräys, joilla pyritään ohjaamaan rekisterinpitäjä tai henkilötietojen käsittelijä noudattamaan asetuksen mukaista henkilötietojen käsittelyä.

Uskon kuitenkin, että pienikin yritys pystyy saattamaan oman henkilötietojen käsittelynsä tietosuoja-asetuksen vaatimuksia vastaavaksi kunhan yritys malttaa tutkia huolella yleistä tietosuoja-asetusta ja tietosuojaviranomaisen sivuja sekä peilata omaa toimintaansa muiden toimintaan. Tärkeää on pitää mielessä tietosuoja-asetuksen perimmäinen päämäärä; avoin ja läpinäkyvä henkilötietojen käsittely.

Jatkossa kohdeyritykselle tuotettua materiaalia on tarkoitus kehittää tietosuoja-asetuksen periaatteen mukaiseen läpinäkyvään suuntaan. Tämä tarkoittaa, etenkin kuluttajille suunnattujen tietosuojaselosteiden selventämistä. Selosteita on tarkoitus havainnollistaa erilaisilla kuvioilla ja kuvakkeilla. Myös yrityksen työntekijöille suunnattua ohjeistusta henkilötietojen käsittelystä kehitetään jatkuvasti. Osittain materiaalien ja prosessien jatkuva tarkastelu liittyy tietosuoja-asetuksen vaatimuksiin, jotka velvoittavat yrityksen tarkastelemaan omaa henkilötietojen käsittelyprosessiaan aina kun kerättävissä tiedoissa, prosesseissa tai teknologioissa tapahtuu muutoksia.

5.2 Opinnäytetyön ja oman oppimisen arviointi

Tein opinnäytetyötäni pääasiassa vapaa-ajalla, sillä töissä tähän ei ollut kiireen takia mahdollisuutta. Olen aiemminkin joutunut työni puolesta tutustumaan laki- ja asetusteksteihin, joten tiesin suurin piirtein minkä tyyppinen projekti olisi odotettavissa.

Tietosuoja-asetusprosessin laajuus kuitenkin yllätti hieman. Mitä enemmän asiaan perehdyin, sitä enemmän löysin uusia asioita, jotka piti ottaa prosessissa huomioon tai joiden soveltuvuutta oman yrityksen toimintaan piti pohtia. Olin kuullut ja lukenut asiantuntijoiden kehottavan aloittamaan rekisterien kartoituksen ajoissa, sillä kerättävien tietojen laajuus ja rekisterien määrä saattaa yllättää. Tämä lukeutui asioihin, jonka kyllä ymmärtää kuulleessaan, mutta todella sisäistää vasta tehdessään.

Toinen yllätystekijä oli asetuksen tulkinnanvaraisuus. Ryhtyessäni perehtymään tietosuoja-asetukseen, huomasin melko nopeasti, että asetuksen tulkinnanvaraisuus tulee monimutkaistamaan työskentelyä. Pidin tietosuoja-asetusta runkona ja tutkin WP29-työryhmän julkaisuja. Näiden lisäksi kuuntelin webinaareja, katselin YouTubeen ladattuja luentoja sekä luin aiheeseen liittyvää kirjallisuutta ja blogi- ja lehtikirjoituksia sekä osallistuin tietosuojakoulutukseen. Vaikka aihe oli suhteellisen uusi, löysin yllättävän paljon materiaalia teoriaosuuden kirjoittamista varten.

Kattavan perehtymisprosessin aikana jouduin toteamaan, että tietosuoja-asetuksen kohdalla sanonta ”tieto lisää tuskaa” piti harmittavan hyvin paikkansa. Sain kuitenkin nivottua eri lähteistä keräämäni tiedon jossain määrin ymmärrettäväksi kokonaisuudeksi. Opin prosessin aikana olemaan vähemmän kriittinen tuottamaani materiaalia kohtaan. Tämä johtui pitkälti siitä, että huomasin jossain vaiheessa prosessia monen muun tahon kamppailevan samojen ongelmien kanssa. Huomasin myös, että joidenkin asiantuntijaorganisaatioiden luennoilla esiintyi epävarmuutta joistakin asetuksen vaatimuksista ja lainsäädännön kehittymisen suunnasta. Onnekseni löysin myös IT-juristi Panu Pökkylän blogi-kirjoituksen, jossa hän käsitteli WP29-työryhmän tulkintojen ja tietosuoja-asetuksen ristiriitaisuuksia (Pökkylä 2018). Edellä mainittujen huomioiden ja onnenkantamoisten johdosta ymmärsin, ettei asetuksen tulkinnoista ollut tässä vaiheessa lainsäädäntö-prosessia mahdollisuutta edes välttämättä päästä täyteen varmuuteen.

Sain vietyä projektin pääosin aikataulussa loppuun. Vaikka projektin viimeinen lopputestaus saatiinkin tehtyä vasta elokuussa, niin asetuksen noudattamisen kannalta tärkeimmät osa-alueet saatiin valmiiksi ajoissa toukokuussa. Seuraavissa projekteissa aikataulun pitämisen varmistamiseksi sekä ylikuormittumisen välttämiseksi tulen kiinnittämään enemmän huomiota riskianalyysin tekoon ja pyrin ottamaan paremmin huomioon myös epätodennäköiset riskit.

Lähteet

Alanko, M., Salo, I. 2013. Big data Suomessa. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/77955/Julkaisuja_25-2013.pdf?sequence=1. Luettu: 10.5.2018.

Asml. 2012. Digitaaliset asiakkuudet – mittaamalla menestykseen. Luettavissa: https://www.asml.fi/wp-content/uploads/Digitaalinen-Asiakkuus-ASML-11-20121.pdf. Luettu: 19.5.2018.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, Euroopan unionin virallinen lehti L119/1.

European Commission 2018. Guidelines on Transparency under Regulation 2016/679 (wp260rev.01). Luettavissa: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Luettu: 2.5.2018.

Fondia – VirtuaaliLakimies 2018. Työnhakijan henkilötietojen käsittely rekrytoinnin yhteydessä. Luettavissa: https://virtuallawyer.fondia.com/fi/articles/tyonhakijan-henkilotietojen-kasittely-rekrytoinnin. Luettu: 18.5.2018.

Hanninen, M., Laine, E., Rantala, K., Rusi, M., Varhela, M. 2017. Henkilötietojen käsittely - EU-tietosuoja-asetuksen vaatimukset. Helsingin Kamari Oy. Vantaa.

Hellman, K. & Värilä, S. 2009. Arvokas asiakas. Talentum Media Oy. Hämeenlinna.

Henkilötietolaki 22.4.1999/523

Holopainen, P. 2018. Suomen yrittäjät - Yrittäjän tietosuojaopas. Luettavissa: https://www.yrittajat.fi/sites/default/files/yrittajat_tietosuojaopas_2018_130418.pdf. Luettu: 15.4.2018.

Klinge, K. 2017. Mikä on CRM-järjestelmä? Luettavissa: https://www.accountorenterprise.fi/2017/08/02/mika-on-crm-jarjestelma/. Luettu: 15.8.2018.

Korhonen, S. 2018. It-sopimusehdot päivittyivät gdpr-aikaan. Luettavissa: https://www.tivi.fi/Kaikki_uutiset/it-sopimusehdot-paivittyivat-gdpr-aikaan-6706016. Luettu: 15.6.2018.

Laihonen, H. 2013. Tiedolla johtaminen tarkoittaa tiedon hyödyntämistä. Luettavissa: https://tietovirta.wordpress.com/2013/11/06/tiedolla-johtaminen-tarkoittaa-tiedon-hyodyntamista/. Luettu: 11.5.2018.

Lemminki, R-M. 2016, Aliarvostettu segmentointi. Luettavissa: https://www.linkedin.com/pulse/aliarvostettu-segmentointi-riikka-maria-lemminki. Luettu: 18.5.2018.

Nahkala, A. 2015. Onko analytiikka teillä renki vai isäntä? Luettavissa: https://digitalist.global/talks/onko-analytiikka-teilla-renki-vai-isanta/. Luettu: 19.5.2018.

Oksanen, T. 2010. CRM ja muutoksen tuska. Asiakkuudet haltuun. Talentum Media Oy. Helsinki.

Pajunen, J. 2016. Datasta tarinoihin. Luettavissa: https://blog.kauppalehti.fi/tiedosta/datasta-tarinoihin. Luettu: 11.5.2018.

Pökkylä, P. 2018. WP29:n tuore ohjeistus vaikuttaa merkittävästi kaikkiin tietosuojaselosteisiin. Luettavissa: https://jit2015.fi/2018/01/11/wp29n-tuore-ohjeistus-vaikuttaa-merkittavasti-kaikkiin-tietosuojaselosteisiin/. Luettu: 1.5.2018.

Reittu, J. 2017. Kuinka valmistautua yleiseen tietosuoja-asetukseen? Luettavissa: https://www.doria.fi/bitstream/handle/10024/144142/Jarkko_Reittu_Kuinka%20valmistautua%20tietosuoja-asetukseen.pdf?sequence=1&isAllowed=y. Luettu: 18.8.2018.

Rubanovitsch, M., Aminoff, J. 2015. Ostovallankumous – miten moderni myyjä vastaa asiakkaan muuttuvaan ostoprosessiin. OY Imperial Sales AB/Johtajatiimi. Helsinki.

Salescommunications. Mitä on Inbound-markkinointi? Luettavissa: https://www.salescommunications.fi/inbound-markkinointi. Luettu: 30.8.2018.

Talus, A., Autio, E., Hänninen, A., Pihamaa, H-T. & Kantonen, S. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf. Luettu: 14.4.2018.

Tietosuojavaltuutetun toimisto 2018. Seloste käsittelytoimista. Luettavissa: https://tietosuoja.fi/seloste-kasittelytoimista. Luettu: 20.6.2018.

Tietosuojavaltuutetun toimisto. Asiakirjan wp243 liite – usein kysytyt kysymykset. Luettavissa: https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavat+UKK+fi.pdf/006f8dcb-540a-403e-a29d-b8a4b7c4814f/Tietosuojavastaavat+UKK+fi.pdf.pdf. Luettu: 11.8.2018.

Tietosuojavaltuutetun toimisto. 2017. Konsultilta opittua- kuinka yritysjohtajat herätetään valmistautumaan tietosuoja-asetukseen. Luettavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/konsultilta-opittua-kuinka-yritysjohtajat-heratetaan-valmistautumaan-tietosuoja-asetukseen-. Luettu: 4.7.2018.

Viestintävirasto 2017. Evästeet. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/palveluidenturvallinenkaytto/evasteet.html. Luettu: 22.4.2018.

Wood, M. 2017. Essential guide to marketing planning. Pearson Education Limited. Harlow.

Liitteet

Liite 1. Lomake rekisteröidyn henkilötietoja koskevaa pyyntöä varten

(Liitteestä piilotettu yrityksen tunnistetiedot)

Tällä lomakkeella voitte tehdä EU:n tietosuoja-asetuksessa (2016/679) rekisteröidylle määriteltyjen oikeuksien mukaisen pyynnön. Täyttäkää lomake huolellisesti, sillä puutteellisesti täytettyjä lomakkeita ei käsitellä. **1 / 2**

Pyynnön lähetysohjeet lomakkeen toisella sivulla

Rekisteröidyn henkilötietoja koskeva pyyntö

Etunimi	**Sukunimi**		
Osoite		**Postinumero**	**Postitoimipaikka**
Puhelinnumero	**Sähköpostiosoite**		

Käyttäjätunnus Täytetään vain mikäli rekisteröity on rekisteröitynyt palveluun, johon kirjautumiseen tarvitaan käyttäjätunnus. (Huom! EI salasana)

Rekisterinnimi

Kuinka kauan aikaa on kulunut viimeisimmästä kontaktistanne [redacted].

☐ Vähemmän kuin ½ vuotta ☐ ½ - 1 vuosi ☐ 1-2 vuotta ☐ 2-5 vuotta

☐ Pyydän nähtäväksi rekisteriin tallennetut itseäni koskevat tiedot

☐ Pyydän poistamaan rekisteristä itseäni koskevat tiedot

☐ Pyydän korjaamaan rekisterissä olevat itseäni koskevat tiedot

Rekisteriin merkityt tiedot

Uudet, ajantasaiset tiedot

☐ Pyydän rajoittamaan rekisterissä olevien itseäni koskevien tietojen käyttöä

Perustelu pyynnön toteuttamiselle

☐ Pyydän siirtämään omat henkilötietoni toiselle rekisterinpitäjälle (Pyyntö koskee vain niitä henkilötietoja, jotka rekisteröity on itse luovuttanut rekisterinpitäjälle, jotka ovat tallennettu koneellisessa muodossa)

Rekisterinpitäjän yhteystiedot, jolle tiedot on tarkoitus siirtää

[redacted]

Tällä lomakkeella voitte tehdä EU:n tietosuoja-asetuksessa (2016/679) rekisteröidylle määriteltyjen oikeuksien mukaisen pyynnön. Täyttäkää lomake huolellisesti, sillä puutteellisesti täytettyjä lomakkeita ei käsitellä.

☐ Vastustan itseäni koskevien henkilötietojen käsittelyä **Perustelu pyynnön toteuttamiselle**	
Allekirjoitus ja nimen selvennys	**Paikka ja aika**

[redacted]**täyttää**

Pyynnön vastaanottaja	**Pyynnön saapumispäivämäärä** ____ / ____ / _____
Henkilöllisyyden todentaminen ☐ Passi ☐ Kuvallinen henkilökortti ☐ Ajokortti ☐ Tunnettu	

Lomakkeen täyttäminen
Täyttäkää lomake huolellisesti, sillä puutteellisesti täytettyjä lomakkeita ei käsitellä. Osa pyynnöistä vaatii rekisteröidyltä perustelun.

Pyynnön toimittaminen
Rekisteröity voi toimittaa omia tietojaan koskevan pyynnön henkilökohtaisesti [redacted] toimipisteeseen. Pyynnön voi toimittaa myös postitse, tällöin pyynnön yhteyteen tulee liittää kopio voimassa olevasta henkilötodistuksesta.

Käynti- ja postiosoite:
[redacted]

Henkilötietojen toimittaminen
Rekisteröity voi noutaa pyytämänsä tiedot [redacted] toimipisteestä, sen jälkeen kun rekisteröidylle on ilmoitettu tietojen olevan valmiina noudettaviksi. Noutaessaan tietoja rekisteröidyn on todistettava henkilöllisyytensä voimassaolevalla henkilötodistuksella.

Rekisteröity voi pyytää tietojen toimitusta postitse. Tällöin tiedot toimitetaan kirjattuna kirjeenä lähimpään Postin palvelupisteeseen.

Henkilöllisyyden todentaminen
Pyynnön esittäjän henkilöllisyys todennetaan voimassa olevalla henkilökortilla. Hyväksyttyjä henkilöllisyys todistuksia ovat passi, kuvallinen henkilökortti ja ajokortti.

Kulut
Henkilötietopyyntö on rekisteröidylle maksuton. Mikäli rekisteröidyn esittämä pyyntö on ilmeisen perusteeton tai kohtuuton, ja jos rekisteröity esittää pyyntöjä toistuvasti, voi rekisterinpitäjä periä kohtuullisen maksun pyynnön toteuttamisesta aiheutuvista kuluista tai kieltäytyä suorittamasta pyydettyä toimenpidettä. Edellä mainituista tilanteissa rekisterinpitäjän on osoitettava pyynnön ilmeinen kohtuuttomuus tai perusteettomuus.

[redacted]

Liite 2. Lomake viranomaisille tietoturvaloukkauksesta tehtävää ilmoitusta varten

(Liitteestä piilotettu yrityksen tunnistetiedot)

Tällä lomakkeella tehdään EU:n tietosuoja-asetuksessa (2016/679) määritetty ilmoitus valvovalle viranomaiselle havaitusta tietoturvaloukkauksesta. **1 / 2**

Ilmoitus viranomaisille tietoturvaloukkauksesta

Yrityksen nimi [redacted]	**Y:tunnus** [redacted]	**Alv-tunnus** [redacted]
Osoite [redacted]	**Postinumero** [redacted]	**Postitoimipaikka** [redacted]
Puhelinnumero [redacted]	**Sähköpostiosoite** [redacted]	
Rekisteriasioista vastaava yhteyshenkilö [redacted]	**Sähköpostiosoite** [redacted]	**Puhelinnumero** [redacted]
Rekisterinnimi	**Tietoturvaloukkauksen tapahtuma aika** _____ / _____ / _____	

Tietoturvaloukkauksen syy

Organisaation sisäinen tahaton	Organisaation sisäinen tahallinen	Organisaation ulkopuolinen tahaton	Organisaation ulkopuolinen tahallinen
☐	☐	☐	☐

Kuvaus tietoturvaloukkauksesta

Tietosuojaloukkauksen kohteena olevat rekisteröityjen ryhmät

Tietosuojaloukkauksen kohteena olevat tietosuojatyyppien ryhmät

Kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista

Tietoturvaloukkauksesta aiheutuvien seurausten vakavuus

☐ Vähäinen ☐ Kohtalainen ☐ Merkittävä ☐ Todella merkittävä

[redacted]

Tällä lomakkeella tehdään EU:n tietosuoja-asetuksessa (2016/679) määritetty ilmoitus valvovalle viranomaiselle havaitusta tietoturvaloukkauksesta.

Kuvaus rekisterinpitäjän toteuttamista toimenpiteistä loukkauksen jälkeen
Kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista
Kuvaus toimenpiteistä, joilla voidaan lieventää loukkauksen haittavaikutuksia

Ilmoituksen tekijä	**Paikka ja aika**

Valvova viranomainen
Tietosuojavaltuutetun toimisto
Käyntiosoite: Ratapihantie 9, 6. krs, 00520 Helsinki
Postiosoite: PL 800, 00521 Helsinki
Sähköposti: tietosuoja@om.fi

[redacted]

Liite 3. Tarkistuslomake

(Liitteestä piilotettu yrityksen tunnistetiedot)

[redacted]

Tarkistuslista **1 / 2**

4.6.2018

EU:n tietosuoja-asetus

X = tehty
O = kesken

Nro.	Tehtävä/suorite	Selvitys	Ei tarvita	Tehty
1	Asetuksen mukainen käsittelyperuste			
1.1	- [redacted]			
1.2	- [redacted]			
1.3	- [redacted]			
2	Tietosuojaselosteet			
2.1	- [redacted]			
2.2	- [redacted]			
2.3	- [redacted]			
3	Selosteet käsittelytoimista			
3.1	- [redacted]			
3.2	- [redacted]			
3.3	- [redacted]			
4	Rekisteröityjen informoinnin dokumentointi			
5	Henkilötietojen käsittelyn ulkoistamisen sopimukset			
5.1	- [redacted]			
5.2	- [redacted]			
5.3	- [redacted]			
6	Henkilötietojen käsittelyn turvallisuuden, virustorjunnan, palomuurien ja toimitilojen turvallisuuden varmistaminen ja dokumentointi			
7	Työntekijöiden käsittelyoikeuksien tarkistus (oikeudet, salasanat)			
7.1	- [redacted]			
7.2	- [redacted]			
7.3	- [redacted]			
8	Selvitys tietosuojavastaavan tarpeesta			
9	Selvitys salassapitosopimusten tarpeesta			
10	Selvitys vaikutusten arvioinnin tarpeesta			

4.6.2018

Nro.	Tehtävä/suorite	Selvitys	Ei tarvita	Kuittaus
11	Ohjeistus rekisteröityjen tiedottamista varten			
12	Ohjeistus viranomaisten tiedottamista varten			
13	Ohjeistus menettelystä kun rekisteröity haluaa käyttää oikeuksiaan			
14	Ohjeistus asetuksen mukaisesta henkilötietojen käsittelystä			
14.1	- Ohjeistus tietojen eheyden ja laadun varmistamiseksi (tietojen päivitys, poisto)			
14.2	- Ohjeistus kerättävistä tiedoista (mitä tietoja kerätään ja mitä tietoja ei kerätä)			
14.3	- Ohjeistus tietojen säilyttämisestä, tulostamisesta			
15	Ajantasainen virusturva sekä palomuuri (henkilökohtaiset päätelaitteet; tietokoneet, puhelimet, tabletit sekä palvelimet.)			
16	Henkilötietoja sisältävien tiedostojen ja tietokantojen varmuuskopiointi ja tietojen palautus menettely			
17	Tietoliikenteen salaus			
17.1	- [redacted]			
17.2	- [redacted]			
17.3	- [redacted]			
17.4	- [redacted]			

Kohta	Selitys

Tarkastuksen päivämäärä: ___ /___ / _____

Tarkastuksen tekijä: _____