Tampereen ammattikorkeakoulu

GDPR-asetuksen vaikutus ulkoistetussa taloushallinnossa

Toni Tähkä

OPINNÄYTETYÖ
Huhtikuu 2019

Liiketalouden koulutus

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalouden koulutus

TÄHKÄ, TONI:
GDPR-asetuksen vaikutus ulkoistetussa taloushallinnossa

Opinnäytetyö 55 sivua, joista liitteitä 2 sivua
Huhtikuu 2019

Euroopan Unionin uuden tietosuoja-asetuksen 2016/679 voimaan astumisen myötä kaikki EU:n alueella toimivat yritykset ja yhdistykset ovat joutuneet tekemään paljon muutoksia henkilötietojen käsittelyyn. Tietosuoja-asetus vaikutti myös tämän opinnäytetyön toimeksiantajaan, josta käytetään työssä nimeä Yritys X. Opinnäytetyön tavoitteena oli selvittää GDPR:n vaikutuksia Yritys X:n toimintaan. Toimeksiantaja on Suomessa toimiva kirjanpidon ja taloushallinnon palvelukokonaisuus, jonka asiakkaat koostuvat toiminimellä toimivista yhtiöistä aina suurin pörssiyhtiöihin ja heidän kansainvälisiin tytäryhtiöihin. Asiakkaita Yritys X:llä on yhteensä noin 450. Työn tarkoituksena oli selventää, minkälaisia vaikutuksia asetuksella oli Yritys X:n liiketoiminnan ja asiakkuuksien johtamisen kannalta katsottuna ja mitä muutoksia asetuksen takia jouduttiin tekemään. Tietosuoja-asetuksen voimaan astumisen ja soveltamisen välissä oli noin kahden vuoden siirtymä aika, jolloin on valmisteltu yrityksen toimintatapojen muutosta tietosuoja-asetuksen mukaisiksi. Henkilötietojen käsittelyä tarkasteltiin ulkoistetussa taloushallinnossa Yritys X:n toimiessa henkilötietojen käsittelijänä ja rekisterinpitäjänä. Työssä tuotiin esille keskeisimpiä termejä ja tietosuoja-asetusta kuvailtiin esimerkkien ja kuvioiden avulla.

Opinnäytetyön tavoitteet saavutettiin, eli työssä saatiin selvitettyä GDPR:n vaikuttaneen Yritys X:n toimintatapoihin niin, että jouduttiin pitämään henkilökunnalle koulutuksia ja muuttamaan henkilötietojen käsittelytapoja, jotta ne vastasivat tietosuoja-asetuksen vaatimuksia. Näillä muutoksilla pystytään välttämään tietoturvaloukkauksen riskiä. GDPR vaikutti myös asiakkuuksiin ja ohjelmistoihin, sillä tietosuojasopimukset jouduttiin tekemään niin asiakkaiden kuin toimeksiantajan käyttämien ohjelmistojen toimittajien kanssa. Suuren asiakasmäärän ja useiden eri ohjelmistojen vuoksi Yritys X:llä oli paljon tekemistä uusien tietosuojasopimusten kanssa. Tuloksien pohjalta pystytään kehittämään henkilötietojen käsittelyä yhä paremmaksi asiakkuuksien johtamisen ja yrityksen liiketoiminnan kannalta tarkasteltuna osana yrityksen strategiaa. Työhön on tehty liitteiksi tietoturvaloukkauksesta ilmoituskaavake ja muistilista. Liitteitä voidaan käyttää apuna uusia asiakkaita neuvottaessa tietosuoja-asetukseen liittyen tai työntekijät voivat tarvittaessa käyttää apuna työssään. Tärkeinä kehitysideoina ovat tietosuoja-asetuksen korostaminen asiakkuuksien johtamisessa ja yrityksen strategiassa.

Asiasanat: tietosuoja-asetus, taloushallinto, henkilötieto, asiakkuuksien johtaminen

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Business Administration

TÄHKÄ, TONI:
How GDPR Impacts on Outsourced Financial Management

Bachelor's thesis 55 pages, appendices 2 pages
April 2019

The new General Data Protection Regulation established by the European Union affects all companies operating in the European Union. GDPR also affects the principal of this thesis which is referred to as Company X. Company X is an accounting and financial management service aggregate. The customers of Company X include companies from sole traders to publicly traded companies and their international subcompanies.

The purpose of this thesis was to get more information about GDPR and how it effects on the everyday operations of Company X in business. The changes included new rules how to operate personal data.

The results of this thesis showed that Company X needed to train all the employers and employees to work according to the new regulation terms and it also to make new contracts with the clients and software suppliers. However, having a big number of clients and software suppliers Company X had a lot of work with the contracts.

Based on the results it’s possible to notice the effects of the new General Data Protection Regulation and improve the processing of personal data in customer relationship management and as part of the strategy of Company X. This thesis includes two attachments which have information that can be useful to the employers in their job.

Key words: GDPR, financial management, personal data, customer relationship management

SISÄLLYS

LYHENTEET JA TERMIT

Anonymisointi	Anonymisointi tarkoittaa henkilötiedon tunnistettavuuden poistamista siten, että sitä ei voida enää yhdistää rekisteröityyn, jolloin tiedot eivät ole enää henkilötietoja (Holopainen 2018, 6).
Henkilötietojen käsittelijä	(Data processor) Luonnollinen henkilö, viranomainen, virasto tai jokin muu, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (GDPR.fi n.d.).
Pseudonymisointi	Pseudonymisoinnilla tarkoitetaan henkilötietojen käsittelyä niin, ettei henkilötietoja pystytä enää yhdistämään suoraan tiettyyn rekisteröityyn. Lisätietojen avulla yhdistäminen voi kuitenkin olla vielä mahdollista, mutta tiedot on säilytettävä erillään itse reksiteristä. Teknisillä ja organisatorisilla keinoilla täytyy varmistaa, ettei rekisterin tietoja pystytä yhdistämään tunnistettuun tai tunnistettavissa olevaan henkilöön. (Holopainen 2018, 6.)
Pilvipalvelut	Pilvipohjaisilla IT-palveluilla tarkoitetaan internetissä käytettäviä tietotekniikkaratkaisuja eli ohjelmistoja, palveluja, tallennuskapasiteettia tai laskentatehoa. Yleisiä palvelumalleja ovat SaaS, PaaS ja IaaS. (Heikinmäki 2017.)
Rekisteröity	Henkilö, josta kerätty tietoa rekisteriin ja on henkilötietojen perusteella tunnistettava tai tunnistettavissa (Maunu 2018).

1 JOHDANTO

Euroopan parlamentin ja neuvoston hyväksymän uuden tietosuoja-asetuksen soveltaminen aloitettiin 25. toukokuuta 2018, jolloin sen hyväksymisestä oli kulunut kaksi vuotta. Asetuksella korvattiin aikaisempi EU:n direktiivi 95/46/EY. (2016/679.) Asetuksen tarkoituksena on vahvistaa luonnollisten henkilöiden oikeuksia omiin henkilötietoihinsa. Luonnollisten henkilöiden oikeuksien kasvaminen henkilötietoihinsa vaikutti myös ulkoistetun taloushallinnon toimintaan. Opinnäytetyön tavoitteena on selventää GDPR:n vaikutuksia Yritys X:ään. Tietosuoja-asetusta tarkastellaan ulkoistetun taloushallinnon toimiessa henkilötietojen käsittelijänä ja rekisterinpitäjänä. Työn tarkoituksena on tarkentaa, mitä vaikutuksia asetuksella oli Yritys X:n liiketoiminnan ja asiakkuuksien johtamisen kannalta katsottuna sekä mitä toimia GDPR vaatii ja miten se muutti toimintatapoja Yritys X:llä. Opinnäytetyössä selvennetään kuvioiden ja esimerkkien avulla siihen liittyviä termejä ja GDPR:n vaikutuksia ulkoistetussa taloushallinnossa.

Monet GDPR:ään sisältyvistä ehdoista vaikuttavat enemmän suoraan henkilötietoja kerääviin ja luonnollisille henkilöille markkinoiviin yrityksiin, mutta tässä työssä tarkastellaan henkilötietojen käsittelijänä ja rekisterinpitäjänä toimimista tilitoimiston näkökulmasta. Yritys X:n asiakkaat ovat yrityksiä, jolloin käsiteltävinä henkilötietoina ovat pääasiassa toimeksiantajan asiakkaan työntekijät ja Yritys X:n omat työntekijät.

Rakenteeltaan työn alku sisältää enemmän teoriaa GDPR:stä. Luvussa 2 käsitellään GDPR:n määritelmä ja tärkeät käsitteet. Luvut 3, 4 ja 5 sisältävät teoriaosuuden, jossa tarkastellaan GDPR:n vaikutuksia tarkemmin. Luvussa 3 tarkastellaan henkilötietojen käsittelyä ulkoistetussa taloushallinnossa niin henkilötietojen käsittelijän kuin rekisterinpitäjän näkökulmasta. Luvussa 4 käsitellään GDPR-asetuksen vaikutuksia ulkoistetussa taloushallinnossa tiedonhallinnan kannalta katsottuna. Luvussa 5 tarkastellaan kuinka GDPR vaikutti asiakkuuksien johtamiseen. Luku 6 sisältää huomioitavia asioita mitä ilmeni työtä tehdessä ja luvussa 7 pohdinta työn onnistumisesta ja sen tuomista haasteista. Työ sisältää kaksi liitettä, jotka ovat tehty auttamaan Yritys X:ää konsultoidessa uusia asiakkaita GDPR:n liittyen sekä työntekijöille avuksi jokapäiväiseen työhönsä.

2 TIETOSUOJA-ASETUS

2.1 Mikä on GDPR?

GDPR eli General Data Protection Regulation on uusi EU:n tietosuoja-asetus, joka korvaa vuoden 1995 henkilötietodirektiivin 95/46/EY (Bergström, Karhula & Kipinoinen 2018). Asetuksen tehtävänä on vahvistaa luonnollisten henkilöiden tietosuojaa ja oikeuksia heistä kerättävään tietoon ja varmentaa EU:n sisämarkkinoita sekä saada sujuvammaksi henkilötietojen kansainvälisiä siirtoja. Hyvänä esimerkkinä oikeuksien parantumisesta, voidaan pitää sitä, että asetuksen astuttua voimaan rekisteröidyn pyytäessä rekisterinpitäjää kertomaan hänestä kerätyt henkilötiedot, täytyy rekisterinpitäjän toimittaa hänelle nämä tiedot. Tietojen täytyy olla helposti luettavassa muodossa ja toimitettuna mahdollisimman pian ilman turhia viivästyksiä. (Holopainen 2018, 14-17.)

Rekisteröidyillä on nykyään myös oikeus pyytää rekisterinpitäjää poistamaan hänestä kaiken kerätyn tiedon, eli ’’tulla unohdetuksi’’ paitsi silloin, kun tietojenkäsittely on tarpeen (Tietosuojavaltuutetun toimisto: Rekisteröidyn oikeudet n.d.). Käytännössä Yritys X:n käsittelemistä henkilötiedoista voidaan pyytää luovuttamaan tiedot rekisteröidylle, poistamaan tai siirtämään muualle. On olemassa toki myös poikkeuksia, jolloin näitä toimenpiteitä ei Yritys X:n tarvitse tehdä.

Vaikka GDPR astui voimaan 25.5.2018 ei se silloin vielä ollut Suomessa kansallisesti täytäntöön pantu. Tietosuoja-asetuksessa on EU:n jäsenvaltioilla direktiivinomaista kansallista liikkumavaraa, eli jokaisessa jäsenmaassa asetuksessa on hieman omia kansallisia muutoksia. Perusratkaisu on kuitenkin sama kuin asetuksessa EU 2016/679. Hallitus teki 1.3.2018 eduskunnalle esityksen HE 9/2018, joka täydentäisi GDPR asetusta EU 2016/679. Hallituksen esitys sai eduskunnan hyväksynnän 13.11.2018 (Bergström, Karhula & Kipinoinen 2018). GDPR asetusta täydentävä tietosuojalaki tuli voimaan 1.1.2019 ja sillä korvattiin aiemmat henkilötietolaki 22.4.1999/523 ja laki tietosuojalautakunnasta ja tietosuojavaltuutetusta 27.5.1994/389 (Henkilötietolaki 1999; Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta 1994).

2.2 Henkilötieto ja henkilörekisteri

Henkilötiedoilla rekisteröity pystytään tunnistamaan ja yksilöimään. Varatuomari Petri Holopainen kertoo Yrittäjän tietosuojaoppaassa (2018, 4), että henkilötieto voi olla esimerkiksi asiakkaiden, työntekijöiden tai yrityskontaktien tietoja, esimerkiksi nimi, osoite, puhelinnumero, IP-osoite tai mikä tahansa muu tieto, joka voidaan liittää tiettyyn luonnolliseen henkilöön. Henkilötiedoksi lasketaan siis kaikki, josta voidaan suoraan tai epäsuorasti tunnistaa luonnollinen henkilö.

Henkilötietorekisteri on jäsennelty tietojoukko, joka sisältää henkilötietoja. Siitä on saatavilla tiedot tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu, toiminnallisin tai maantieteellisin perustein jaettu. Tietojen ei siis tarvitse olla fyysisesti samassa paikassa. Ne ovat voitu hajauttaa eri maihin ja eri säilytyspaikkoihin, kuten paperille, pilvipalveluihin tai vain eri tiedostoihin. (Holopainen 2018, 5.) Yritys X:llä on käytössä omat ja asiakkaidensa henkilörekisterit, jotka sisältävät tarvittavia henkilötietoja yrityksen liiketoiminnalle. Perinteinen puhelinluettelo on hyvä esimerkki henkilötietorekisteristä.

Henkilörekisteri koostuu useamman rekisteröidyn henkilötiedoista ja sen kokoaa rekisterinpitäjä. Rekisterinpitäjä (Data controller) on luonnollinen henkilö, yritys, virasto tai joku muu, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä (Maunu 2018). Esimerkiksi Yritys X on työntekijöidensä henkilötietojen rekisterinpitäjä.

2.3 Tietoturvan ja tietosuojan ero

Tietoturvasta ja tietosuojasta puhutaan monesti samassa yhteydessä, mutta ne eivät silti tarkoita samaa asiaa. Olennaista on kuitenkin, että ne liittyvät vahvasti toisiinsa ja siksi myös arkikielessä helposti sekoitettavissa keskenään.

Tietosuoja tarkoitta yksilön suojaa eli henkilötietojen käsittelyä ja rekisteröidyn oikeutta henkilötietoihinsa. Tietosuoja on myös yksi tekijä, joka ohjaa tietoturvalle asetettavia vaatimuksia. Tietosuoja sisältää myös eräitä uusia velvoitteita, joita tietoturvalta ei edellytetä, esimerkiksi velvollisuus osoittaa, että tietojen käsittely

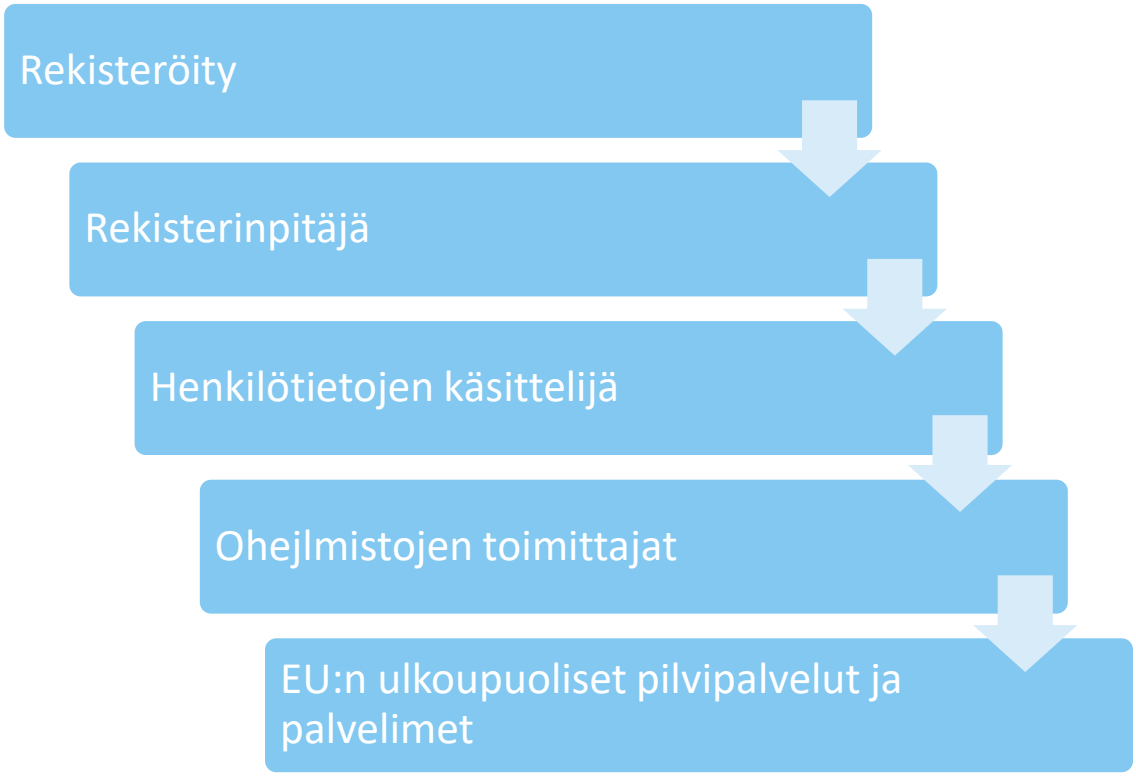
on turvallista ja kertoa, miten tämä turvallisuus on toteutettu. (Yritys X:n edustaja 2019.)

Tietoturva on laaja-alaista perustoimintaa, jonka tarkoituksena on, että Yritys X:ssä käsiteltävät tiedot pysyvät luottamuksellisina, eheinä ja saatavilla. Hyvä tietoturva toteuttaa monta tietosuojaan sisältyvää asiaa, mutta ei kaikkia. GDPR ja tietosuojalaki 1050/2018 määräävät, miten henkilötietoja täytyy käsitellä. Tärkeintä kuitenkin on tietojen luottamuksellisuus. (Yritys X:n edustaja 2019.) Tietoturvalla tarkoitetaan teknisten toimenpiteiden lisäksi myös hallinnollisia toimenpiteitä, joiden tehtävänä on toteuttaa tietosuojaa. Näitä hallinnollisia toimia ovat muun muassa tietosuojavastaavan nimeäminen, henkilöstön kouluttaminen, omavalvonta suunnitelma, tilojen turvaaminen ja vakuutukset. Teknisiä toimenpiteitä ovat esimerkiksi palomuurit ja virustorjuntaohjelmistot. (OpiTietosuojaa.fi 2016.)

2.4 Ketä GDPR koskettaa?

Asetus koskee kaikkia niitä EU:ssa ja EU:n ulkopuolella toimivia tai palveluitaan tarjoavia organisaatioita, jotka keräävät, säilyttävät ja käsittelevät henkilötietoja EU:n alueella kuluttajille ja yrityksille. Asetuksen soveltaminen on todella laaja alue, sillä lähes jokaisessa yrityksessä ja yhdistyksessä on käytössä esimerkiksi asiakas- tai jäsenrekisteri, johon asetusta sovelletaan. EU:n ulkopuolelle henkilötietoja siirrettäessä täytyy yrityksen tai maan, johon tietoja siirretään, täyttää tarkat kriteerit. Tietojen siirtyessä EU:n ulkopuolella sijaitsevalle, esimerkiksi pilvipalvelulle, koskee GDPR myös silloin näitä palveluntarjoajia. (Euroopan parlamentin ja neuvoston asetus 2016/679.)

Koska GDPR vaikuttaa oikeastaan kaikkiin yrityksiin ja yhdistyksiin, täyttyivät toukokuussa sähköpostit eri yhdistysten ja yritysten lähettämistä GDPR sähköposteista. Yritys X:ää EU:n tietosuoja-asetus koskee rekisterinpitäjänä ja henkilötietojen käsittelijänä. Kuviossa 1 on kuvattu, keitä tietosuoja-asetus koskettaa ja missä järjestyksessä.



KUVIO 1. GDPR – asetuksen vaikutus

3 HENKILÖTIETOJEN KÄSITTELY ULKOISTETUSSA TALOUSHALLINNOSSA

3.1 Yritys X

Toimeksiantajana tälle opinnäytetyölle on yritys, joka on koko Suomessa toimiva kirjanpidon ja taloushallinnon palvelukokonaisuus. Toimeksiantajasta puhutaan opinnäytetyössä nimellä Yritys X, sen tunnistettavuuden ja kilpailijoiden mahdollisesti saaman hyödyn vuoksi. Yritys X on keskisuuri yritys, joka työllistää noin 100 henkilöä ja jonka liikevaihto oli 6,6 miljoona euroa tilikaudella 2017 (Yritys X:n kotisivut 2018).

Yritys X:n toiminta-alue on koko Suomi ja asiakkaita on noin 450, joista kymmenen on suomalaisten konsernien kansainvälisiä tytäryhtiöinä tai sivuliikkeenä listattuja ulkomaisia yhtiöitä. Asiakkaissa on yhden hengen toiminimiä, pien-, pk- ja suuryrityksiä, joille jokaiselle on tarjolla kohdistettuja omia palveluita. Asiakkaan yrityksen koko vaikuttaa myös siihen, mitä kaikkia palveluja asiakas tarvitsee ja mitä GDPR:ssä täytyy palvelun osalta ottaa erityisesti huomioon. (Yritys X:n kotisivut 2018.) Kuviossa 2 olen luetellut esimerkkejä, mitä palveluita Yritys X tarjoaa asiakkailleen.

KUVIO 2. Yritys X:n tarjoamia palveluita

3.2 Ulkoistettu taloushallinto henkilötietojen käsittelijänä

Henkilötietojen käsittelijä tarkastelee tiettyjä tietosuojasopimuksessa sovittuja henkilötietoja rekisterinpitäjän puolesta. Rekisterinpitäjän ulkoistaessaan palvelun, kuten Yritys X:lle, on rekisterinpitäjä vastuussa siitä, että valitsee henkilötietojen käsittelijäksi sellaisen yrityksen, joka käsittelee tietoja oikeaoppisesti ja täyttää GDPR:n vaatimukset. Ulkoistettu taloushallinto, kuten Yritys X, toimii asiakkailleen eli rekisterinpitäjille henkilötietojen käsittelijänä taloushallinnon tehtävissä, esimerkiksi palkanlaskennassa. Yritys X on näin ollen myös vastuussa henkilötiedoista ja niiden oikeanlaisesta käsittelystä. Varmistaakseen henkilötietojen oikeaoppisen käsittelyn, noudattaa Yritys X asiakkaidensa kanssa tekemiään tietosuojasopimuksia ja heiltä saatuja täsmennettyjä ohjeistuksia.

Henkilötietojen käsittelylle on määritelty kuusi syytä, joista ainakin yhden pitää täyttyä, jotta henkilötietoja saadaan käsitellä. Nämä kuusi syytä ovat suostumus, oikeutettu etu, sopimus, lakisääteinen velvoite, elintärkeä tai yleinen etu ja julkinen tehtävä. (Euroopan parlamentin ja neuvoston asetus 2016/679.) Myöskin henkilötietojen käsittelijälle täytyy olla määritelty tarkalleen, mitä oikeuksia hänellä on henkilötietojen käsittelijänä rekisterinpitäjän puolesta. Nämä oikeudet on määritelty tietosuojasopimuksessa.

Suostumukseksi henkilötietojen käsittelyyn ei ole enää sallittua käyttää opt-out mallia, joka oli suosittu ennen tietosuoja-asetuksen voimaanastumista. Opt-out lupa tarkoittaa esimerkiksi, että kohdassa, jossa kysytään lupaa henkilötietojen keräämiselle, on valmiina rasti ruudussa merkitsemässä suostumusta tietojen keräämisestä. Tällöin rekisteröity ei välttämättä edes huomaa antavansa suostumusta tietojen keräämiseen. Rekisteröidyn täytyy siis itse poistaa rasti ruudusta, jos ei ole halukas antamaan lupaa tietojen keräämiseen. Opt-in on taas parempi vaihtoehto suostumuksen hankkimiseksi, sillä rekisteröity huomaa siinä selkeästi antaneensa suostumuksen. Opt-in mallissa henkilö itse esimerkiksi laittaa rastin ruutuun merkiksi, kun kysytään suostumusta henkilötietojen keräämiselle. Opt-in mallissa henkilö siis huomaa antavansa suostumuksen, mutta koska opt-out vaihtoehdossa rekisteröity ei välttämättä huomaa valmiiksi täytettyä suostumusta, voidaan tulkita, ettei suostumusta ole annettu vapaaehtoisesti. (Call To Action 2017.) Yritys X:llä opt-in suostumuksen pyytämistä tietojen keräämiseen

käytetään esimerkiksi asiakkaiden ja rekrytoitavien uusien mahdollisten työntekijöiden yhteystietojen keräämistä varten. Edellä mainittujen vaihtoehtojen lisäksi myös suullisesti annettu lupa käy, mutta sitä kannattaa miettiä aina tilanteen mukaan.

Oikeutettuna etuna tietojen keräämiselle voidaan pitää esimerkiksi sitä, kun rekisteröidylle lasketaan palkkaa. Henkilötietojen käsittelijällä ja rekisteröidyllä on tällöin asianmukainen ja merkityksellinen suhde, koska rekisteröity on työsuhteessa rekisterinpitäjän kanssa. (Holopainen 2018,10.) Yritys X on oikeutettu käsittelemään asiakasyritystensä työntekijöiden henkilötietoja, joita se tarvitsee välittömästi palkanmaksussa ja muussa taloushallinnon tehtävissä, joihin Yritys X:n asiakkaat ovat siltä palvelut ostaneet. Vaikka Yritys X saakin asiakkaidensa työntekijöiden henkilötietoja käyttöönsä, ei heillä ole kuitenkaan oikeutta käyttää tietoja mihinkään muuhun kuin hoitaakseen heille uskotut tehtävät.

Lakisääteinen velvoite on myös yksi syy Yritys X:llä tietojen keräämiseen, sillä palkkahallinto ilmoittaa rekisteröityjen palkkatiedot tulorekisteriin. Lakisääteisen velvoitteen takia henkilötietojen käsittelyyn ei tarvita rekisteröidyn suostumusta (Holopainen 2018,11). Lasten henkilötietojen käsittelyyn GDPR tuo lisää suojaa alle 16-vuotiaille. Alle 16-vuotiaat eivät saa itse antaa suostumusta henkilötietojen käsittelyyn, vaan rekisterinpitäjän täytyy pyytää tässä tapauksessa lapsen huoltajilta lupa henkilötietojen käsittelyyn. Lapsen ollessa vähintään 16-vuotias saa hänelle tarjota suoraan tietoyhteiskunnan palveluita. (Holopainen 2018, 10.) Yritys X:ää lapsen tietojen käsittely saattaa koskea silloin, jos asiakkaalla on töissä alle 16-vuotiaita, joiden henkilötietoja joudutaan käsittelemään. Elintärkeä tai yleinen etu ja julkinen tehtävä ovat myös syitä henkilötietojen käsittelyyn ilman rekisteröidyn suostumusta, mutta Yritys X ei voi käyttää näitä syitä.

Kuviossa 3 on kuvattu Yritys X:n asiakkaan työntekijöiden henkilötietojen käsittelijät. Työntekijä on rekisteröity ja hänestä löytyy henkilötietoja henkilörekisteristä. Hänen työnantajansa (Yritys X:n asiakas) on rekisterinpitäjä, joka on ostanut ulkoistetun taloushallinnon palvelun, kuten palkanlaskennan tai matkalaskujen käsittelyn Yritys X:ltä. Rekisterinpitäjän ostaessa taloushallinnon palvelun Yritys

X:ltä tulee Yritys X:stä henkilötietojen käsittelijä, jolla on tietyt oikeudet rekisteröidyn henkilötietoihin. Yritys X on siis henkilötietojen käsittelijä ja hallinnoi rekisteröidyn tietoja rekisterinpitäjän puolesta.

KUVIO 3. Henkilötietojen käsittely henkilötietojen käsittelijänä

Palkanlaskenta ja Matkareskontra

Nykyään on hyvin yleistä, että yritykset päättävät ulkoistaa palkanlaskentansa tilitoimistoille. Ulkoistetusta taloushallinnosta tulee henkilötietojen käsittelijä käsitellessään asiakkaansa (rekisterinpitäjän) työntekijöiden henkilötietoja palkkahallinnossa. Yritys X:n hoitaessa asiakkaidensa palkanlaskentaa käsittele se henkilötietojen lisäksi myös erityisten henkilötietoryhmien tietoja. Näitä ovat arkaluontoiset tiedot, kuten ammattiliiton jäsenyys. Palkanlaskennassa voidaan tarkastella myös rekisteröityjen työajanseuranta tietoja, jos rekisterinpitäjä on tämän palvelun ostanut Yritys X:ltä. Näistä tiedoista saadaan tarkkaa tietoa siitä, miten rekisteröidyt liikkuvat eli saapuvat ja lähtevät työpaikalta. Palkanlaskenta ja Matkareskontra ovat myös Yritys X:n palveluista niitä, joita GDPR asetus koskettaa eniten. Molemmissa käsitellään paljon asiakkaiden henkilötietoja ja siksi on tärkeää, että GDPR asetuksen ohjeistusta noudatetaan oikein.

Matkareskontra on myös yleinen ulkoistetusta taloushallinnosta ostettu palvelu, jossa henkilötietojen käsittelijät hallinnoivat paljon henkilötietoja rekisterinpitäjän puolesta. Yritys X tarjoaa matkareskontran hoitopalveluita niin pienille-, pk- ja suuryrityksille. Matkareskontrassa käsiteltäviä henkilötietoja ovat muun muassa

matkasuunnitelmat, päivärahat ja kilometrikorvaukset sekä luottokortti- ja matkatoimistotapahtumat. Nämä tiedot ovat myös palkkahallinnon käytössä, jotta ne pystyvät maksamaan kulukorvaukset ja päivärahat oikeille henkilöille. Henkilötietojen suojaamisen varmistamiseksi täytyy henkilötiedot suojata niin, etteivät ne joudu ulkopuolisten tietoon. Anonymisointia ei kuitenkaan voida käyttää henkilötietojen suojaamiseksi, koska palkanmaksussa tarvitaan näitä tietoja ja palkkahallinnon on tunnistettava rekisteröidyt, joille korvauksia, kuten päivärahoja maksetaan.

Matkareskontran käsittelemissä matkalaskuissa ja matkasuunnitelmissa olevia henkilötietoja ei haluta kaikkien tietoon. Näitä henkilötietoja ovat esimerkiksi rekisteröidyn yhteystiedot. Henkilötietojen käsittelijän täytyy siis käyttää luotettavia järjestelmiä. Matkalaskujen käsittelyssä käytetään monessa yrityksessä M2-matkalaskutusjärjestelmää, joka on GDPR:n mukainen palvelu ja on näin ollen käytössä myös Yritys X:llä (Yritys X edustaja 2019).

Palkanlaskentaa ja matkareskontraa koskettaa myös 1.1.2019 voimaan astunut tulorekisteri. Maksetut palkat ja etuudet on ilmoitettava palvelussa 5 päivän kuluttua maksupäivästä. Tulorekisterin tavoitteena on tehdä palkanmaksajien arjesta helpompaa, sillä sen avulla ei enää tarvitse ilmoittaa usealle eri viranomaiselle maksetuista palkoista ja etuuksista, vaan kaikki ilmoitukset tehdään yhteen paikkaan. (Räty 2018.) Kuviossa 4 on kuvattu, kuinka tulorekisteriin ilmoitetaan maksetut palkat ja etuudet. Palkat ja etuudet voidaan ilmoittaa kahdella tapaa, joko käyttäen teknistä rajapintaa tai manuaalisesti käyttäen sähköistä asiointipalvelua.

KUVIO 4. Tulorekisteriin ilmoittamisen kanavat (Verohallinto 2018)

Tulorekisteriin voidaan kirjata ilmoituksia usealla eri tavalla, mutta tulorekisterin sivulla suositellaan käyttämään teknistä rajapintaa, jos sen käyttö on vain yrityksellä mahdollista. Teknisen rajapinnan käyttämiselle edellytyksenä on, että yrityksellä käytössä oleviin matkareskontran ja palkanlaskenta järjestelmiin on tehty sähköinen yhteys tulorekisteriin. (Verohallinto 2018.) Teknistä rajapintaa käyttäessä tiedot siirtyvät siis suoraan tulorekisteriin Yritys X:n käyttämistä taloushallinnon järjestelmistä.

Yritys X:n ilmoittaessa työntekijänsä tai asiakasyrityksensä työntekijöiden, eli rekisteröityjen palkkatietoja tulorekisteriin, on heidän myös mietittävä tietojensiirtotoimenpidettä GDPR:n vaatimusten kannalta. Rekisterinpitäjän tai henkilötietojen käsittelijän, joka ilmoittaa rekisteröidyn palkkatiedot tulorekisteriin, on GDPR:n mukaan arvioitava tulorekisteripalvelu ja sen riskit. Eli palkanmaksaja on vastuussa maksettujen palkkojen tiedoista ja niiden oikeaoppisesta suojaamisesta. Tämän vuoksi yritysten on täytynyt tehdä arviointi, aiheuttaako tulorekisteri korkean riskin. Erityisesti GDPR:n mukainen riskien arviointi on tehtävä tietojensyöttämisestä. Sähköistä asiointipalvelua ja teknistä rajapintaa käyttäessä, liittyy molempiin omat riskinsä. Arvioidessa näitä palveluun liittyviä riskejä täytyy ottaa huomioon, mitä vahinkoja palvelusta voi aiheutua rekisteröidylle. (Aitta & Matinpalo 2019.)

Tulorekisteriin liittyviä riskejä ovat muun muassa palkkatietojen oikeellisuus. Palkkatietojen virheellinen ilmoittaminen voi aiheuttaa rekisteröidylle taloudellisia ongelmia, sillä tulorekisteriin ilmoitetut tiedot koskettavat suoraan rekisteröidyn muita etuja, kuten asumis- ja toimeentulotukea. Palkkatietoja ilmoittaessa tulorekisteriin sähköistä asiointipalvelua käyttäen on virheellisesti ilmoitettujen tietojen riski korkeampi kuin teknistä rajapintaa käyttäen. Ihmisten tehdessä manuaalisesti ilmoituksia voi tapahtua huolimattomuusvirheitä, jotka eivät ole mahdollisia, kun hyödynnetään automaattista kirjausta. (Aitta & Matinpalo 2019.) Tietoja ilmoittaessa on otettava huomioon käsittelyn tietoturva, kuten muulloinkin Yritys X:n työskennellessä henkilötietojen kanssa.

Tulorekisteriin kirjautuminen tehdään Suomi.fi palvelussa, kuten kuviossa 4 on kuvattu. Suomi.fi palvelussa tunnistautumisen voi tehdä esimerkiksi henkilökohtaisilla verkkopankkitunnuksilla tai mobiilivarmenteella (Verohallinto 2018). Koska palveluun kirjaudutaan omilla henkilökohtaisilla tunnuksilla, on työntekijän varmistettava niiden turvallinen säilyttäminen työpäivän aikana.

3.3 Yritys X rekisterinpitäjänä

Rekisterinpitäjänä Yritys X:llä on kokonaan vastuu siitä, mitä ohjelmistoja ja ulkoistettuja palveluita ne käyttävät ja täyttävätkö ne GDPR:n vaatimukset. Yritys X vastaa myös oman hallinnon käyttämistä henkilötietorekistereistä, joissa ne eivät käytä ulkopuolisia palveluita vaan ainoastaan omia. Hallinto käyttää muun muassa yrityksen asiakas-, palkanlaskenta-, rekrytointi- ja kulunvalvontarekistereitä sekä työajanseurantaa. Osaan rekistereistä Yritys X käyttää muiden yritysten tarjoamia palveluita, jolloin palveluntarjoaja toimii henkilötietojen käsittelijänä. Asiakasrekisterin sisältäessä henkilötietoja, kuten nimiä ja yhteystietoja, kuuluu se myös GDPR:ään, vaikka asiakkaat ovat yleensä yritysasiakkaita ja yrityksiä.

Hallinnon rekistereistä työajanseurantaa tarvitaan, jotta palkkahallinnossa saadaan laskettua työntekijöille kuuluvat palkat oikein. Työntekijät kirjaavat itsensä töihin ja ulos sekä merkitsevät mahdolliset poissaolot, jolloin tapahtumat kirjautuvat suoraan järjestelmään. Sieltä Yritys X:n palkkahallinto saa tarvittavat tiedot palkanmaksuun. Työajanseurannassa Yritys X käyttää samaa palvelua, joka on myös heidän asiakkailleen tarjolla.

Yritys X käyttää myös kulunvalvontaa, joka on hyvä keino varmistaa, että yrityksen tiloissa pääsevät kulkemaan vain ne, joilla on työn kannalta tärkeää päästä eri osastoille. Tämän avulla voidaan varmistaa myös henkilötietojen turvallinen käsittely ilman, että ulkopuolisia henkilöitä pääsee huomaamatta niitä näkemään. Kulunvalvonta on myös tärkeää turvallisuuden kannalta, sen avulla tiedetään, keitä on rakennuksessa sisällä ja missä päin kukin henkilö on. Kulkutiedot voidaan tarvittaessa myös pseudonymisoida, jolloin niistä ei heti selviä kenestä rekisteröidystä on kyse. Rekisteröidyn henkilöllisyys pystytään kuitenkin selvittämään ja tämän vuoksi se lasketaan edelleen henkilötiedoksi tehdystä toimenpiteestä huolimatta. Kulunvalvonta voidaan esimerkiksi pseudonymisoida tekemällä työntekijöille omat henkilönumerot. Kulunvalvontalokiin kirjattaisiin vain tämä numerosarja henkilön nimen sijaan. Henkilön nimi ja henkilönumero olisivat kirjattuna ylös taas toisella listalla, jolloin kulunvalvontaa voidaan seurata henkilönumeron avulla ja tarkastaa toisesta erillisestä listasta kuka henkilö on kyseessä.

Kuviossa 5 on selvennetty Yritys X:n asema henkilötietojen käsittelyssä heidän ollessaan rekisterinpitäjiä. Kuviossa näkyy kuka on rekisteröity, rekisterinpitäjä ja henkilötietojen käsittelijä.

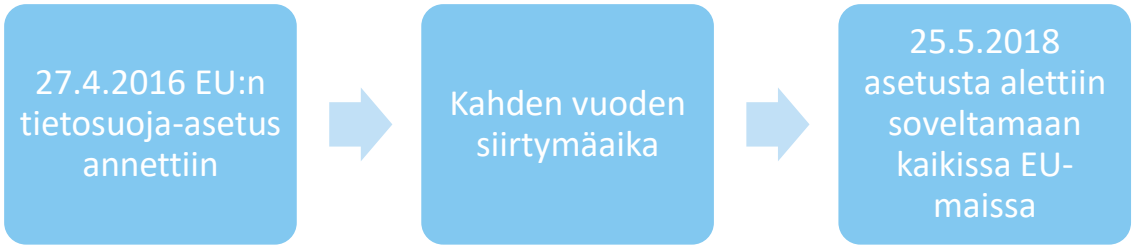
KUVIO 5. Henkilötietojen käsittely rekisterinpitäjänä

HR-rekisteri sisältää henkilötietoja työntekijöistä; dokumenteissa ovat muun muassa, yhteystiedot, työsuhdemuutokset ja lomat sekä palkat. Asiakirjoissa on myös ammatillisia tietoja henkilöistä, kuten työntekijöiden suorittamat ja tulevat kurssit ja tietoja osaamisista. Myöskin työntekijöiden kanssa käydyt kehityskeskustelut ja niistä saadut tiedot ja lomakkeet ovat yrityksen HR-rekisterissä henkilötietoja. Yritys X:llä on myös käytössä verkossa toimiva ohjelma, josta työntekijät näkevät omia henkilötiedot. Ohjelmasta työntekijät pystyvät tarkastelemaan esimerkiksi henkilötietonsa, työsuhde- etunsa (esimerkiksi liikuntaraha), lomasaldonsa ja palkkalaskelmansa sekä poissaolonsa. (Yritys X:n edustaja 2018.)

4 GDPR:N VAIKUTUS ULKOISTETUSSA TALOUSHALLINNOSSA

4.1 GDPR:ään valmistautuminen

EU:n yleisen tietosuoja-asetuksen uudistamista otettiin esille ensimmäisen kerran vuonna 2012 maaliskuussa. Asetuksen uudistamisesta keskusteltiin ja neuvoteltiin neljä vuotta, ennen kuin se lopulta Euroopan parlamentin ja neuvoston päätöksellä annettiin 27.4.2016. Tietosuoja-asetuksen hyväksymisen jälkeen annettiin noin kahden vuoden siirtymäaika, jolloin yritysten piti saada toimintansa EU:n tietosuoja-asetuksen mukaiseksi 25.5.2018 mennessä. (Euroopan parlamentin ja neuvoston asetus 2016/679.) Kuviossa 6 on kuvattu tärkeät ajankohdat asetuksen hyväksymisestä voimaan astumiseen saakka.



KUVIO 6. EU:n tietosuoja-asetuksen aikataulu

GDPR:ään valmistauduttiin Yritys X:ssä muun muassa pitämällä sisäinen koulutus koko henkilökunnalle. Myös prosesseja on jouduttu muuttamaan, jotta voidaan varmistaa asetuksen noudattaminen. Näitä muutoksia ovat muun muassa aineiston saapuminen asiakkaalta Yritys X:lle, turvasähköpostin käyttöön ottaminen ja turvatulostus mahdollisuus tulostimille. Näillä edellä mainituilla muutoksilla Yritys X pystyi vahvistamaan GDPR:n toteutumista paremmin heidän jokapäiväisessä työssään ja pienentämään tietosuojaloukkauksien mahdollisuutta.

GDPR:n voimaanastumisen jälkeen Yritys X:ään töihin tulleet on myös tärkeää perehdyttää siihen, miten GDPR vaikuttaa heidän jokapäiväisessä työssään.

Yritys X:ltä oli jo ennen GDPR:n voimaanastumista vaadittu hyvää tietoturvaa ja luotettavuutta, kuten muiltakin tilitoimistoilta. Työntekijät ovat aikaisemminkin joutuneet allekirjoittamaan salassapitosopimukset, joita nyt myös vaaditaan tietosuoja-asetuksen myötä tietosuojalta. GDPR voimaanastumisen jälkeen päivittäisessä työssään työntekijöiden on oltava vielä varovaisempia työskennellessään henkilötietojen kanssa. Eri asiakkailla on erilaisia vaatimuksia mitä pitää tehdä, jotta varmistetaan ettei tietosuojaloukkauksia pääse tapahtumaan. Kaikkien asiakkaiden kanssa tärkeitä muistettavia asioita ovat muun muassa pitää salasanat piilossa ja vain omassa tiedossa, pitää työpiste siistinä ja varmistaa ettei työpisteeltä poistuessa jää näkyville henkilötietoja sisältäviä asiakirjoja, varmistaa ettei kukaan ulkopuolinen tai henkilö, joka ei tietoja tarvitse työssään näe niitä ja työntekijät käsittelevät vain niitä henkilötietoja, joita töissään tarvitsevat.

Yritys X on rajannut pääsyn yrityksen eri osastoille vain niille henkilöille, joilla on näille osastoille tarvetta päästä töiden takia, pienentääkseen tietosuojaloukkausten mahdollisuutta. Näin varmistetaan, ettei osastoille pääse ulkopuolisia henkilöitä ilman lupaa. Rajaamalla pääsyn eri kerroksiin, Yritys X:n hallinto on pienentänyt tietosuojaloukkauksien riskiä, mutta käyttäen tietokoneen näytöllä tietoturvasuoja kalvoa voidaan estää vieressä olevia henkilöitä näkemästä näytölle. Pelkästään suojakalvoon ei aina kannata luottaa esimerkiksi siivoojan työskennellessä työpisteen luona. Tällöin näyttö kannattaa sulkea siivoojan työskentelyn ajaksi, varmistaakseen, ettei ulkopuolinen näe käsiteltäviä henkilötietoja. Sähköposteja lähetettäessä on henkilökuntaa opastettu lähettämään henkilötietoja sisältäviä arkaluonteisia viestejä turvasähköpostin kautta. Arkaluonteisia tietoja tulostettaessa on hyvä käyttää turvatulostusta. Näiden ohjeiden käyttöönotto tietosuoja-asetukseen valmistautuessa on ollut hyvä tapa varmistaa tietosuoja-asetuksen vaatimusten täyttyminen työntekijöiden päivittäisessä työskentelyssä.

4.1.1 Tietosuojavastaava

Tietosuojavastaava eli Data Protection Officer on nimitettävä aina, kun henkilötietojen käsittelijän tehtävät sisältävät laaja-alaista henkilötietojen käsittelyä, kuten erityisiin tietoryhmiin kohdistuvia tietoja (Holopainen 2018, 31). Yritys X käsittelee asiakkaidensa ja työntekijöidensä palkkoja säännöllisesti ja järjestelmällisesti, jonka vuoksi ne ovat tekemisissä erityisten henkilöryhmien tietojen kanssa, joihin muun muassa ammattiliittojen jäsenyys kuuluu. Henkilötietojen käsittelyn laaja-alaisuuden ja erityisiin tietoryhmiin kohdistuvien tietojen vuoksi Yritys X:ssä on pitänyt nimittää tietosuojavastaava.

Tietosuojavastaavan tehtävä voidaan ulkoistaa esimerkiksi konsultille tai se voi olla rekisterinpitäjän tai henkilötietojen käsittelijän omaa henkilökuntaa. Tietosuojavastaava ei kuitenkaan voi olla yrittäjä itse eikä myöskään esimerkiksi yrityksen IT-johtaja tai talousjohtaja. Eturistiriitojen välttämiseksi on hyvä, ettei tietosuojavastaava ole edellä mainituissa vai vastaavassa asemassa, vaikka hänellä voi olla muitakin tehtäviä tietosuojavastaavan tehtävän lisäksi. (Holopainen 2018, 31.)

Tietosuojavastaavan nimittämisessä on otettava huomioon hänen pätevyytensä tehtävään. Henkilön ammattipätevyys ja asiantuntemus tietosuojalainsäädännöstä ja valmiudet hoitaa tietosuojavastaavan työtä ovat tärkeitä huomioon otettavia kriteereitä valittaessa henkilöä tehtävään. (Holopainen 2018, 32.) Lainsäädännössä ei kuitenkaan ole tarkalleen määritelty vaatimusta siitä mikä koulutus tai ammattinimike hänellä täytyisi olla, mutta koulutuksen tulisi olla riittävä. Tultuaan valituksi tietosuojavastaavan tehtävään, täytyy hänellä olla myös mahdollisuus ylläpitää ja kehittää ammattitaitoaan. (Andreasson, Koivisto & Ylipartanen 2013, 17.)

Tietosuojavastaavalla täytyy olla riittävät resurssit, jotta hän pystyy hoitamaan tehtäväänsä. Hänen tehtävänsä on raportoida suoraan asiakkaan eli rekisterinpitäjän tai henkilötietojen käsittelijän ylimmille johdoille. (Holopainen 2018, 32.) Yritys X:n tietosuojavastaava raportoi suoraan asiakkaan ylimmälle johdolle (Yritys X:n edustaja). Tietosuojavastaavalla on salassapitosopimus, mutta tilitoimistossa

työskentelevillä salassapitosopimukset ovat yleisiä ja lähes aina solmittu työantajan ja työntekijän välille (Taloushallintoliitto n.d.).

Yritys X on ottanut nämä edellä mainitut asiat huomioon tietosuojavastaavansa valinnassa. Tietosuojavastaava on sama kaikille asiakkaille ja hän ei ole työsuhteessa Yritys X:n kanssa, vaan Yritys X:n emoyhtiöllä. Tietosuojavastaavalla on pääsy henkilötietoihin ja hän myös vastaa henkilötietojen kyselyihin. Hänen tehtäviään ovat myös rekisterinpitäjän ja henkilötietojen käsittelijän neuvominen. Tarvittaessa tietosuojavastaava antaa myös neuvoa GDPR:ää koskevasta vaikutuksenarvioinnista. (Yritys X:n edustaja 2018.)

Yritys X:n ja rekisterinpitäjien on varmistettava, ettei tietosuojavastaavan työhön puututa. Tietosuojavastaavaa ei saa johdattaa tekemään työtänsä esimerkiksi rekisterinpitäjän tai henkilötietojen käsittelijän tahdon mukaisesti. Koska tietosuojavastaavan on tehtävä työnsä asetuksen mukaisesti ja oltava ottamatta vastaan ohjeita, kuinka hänen pitää työnsä tehdä, ei häntä myöskään saa rangaista tai erottaa sen takia, että hän on hoitanut tehtäviään asetuksen mukaisesti. (Holopainen 2018, 32.) Tietosuojavastaavan tehtäviä neuvomisen ja vaikutuksenarvioinnin lisäksi ovat muun muassa katsoa, että asetusta noudatetaan yrityksessä, tarkkailla henkilötietojen käsittelijän tai rekisterinpitäjän toimia ja että, ne kouluttavat työntekijöitä, jotka käsittelevät työssään henkilötietoja. Yrityksen tietosuojavastaava toimii myös mahdollisissa käsittelyissä valvontaviranomaisen eli tietosuojavastaavan toimiston yhteyshenkilönä. (Tietosuojavaltuutetun toimisto: Tietosuojavastaavat n.d.)

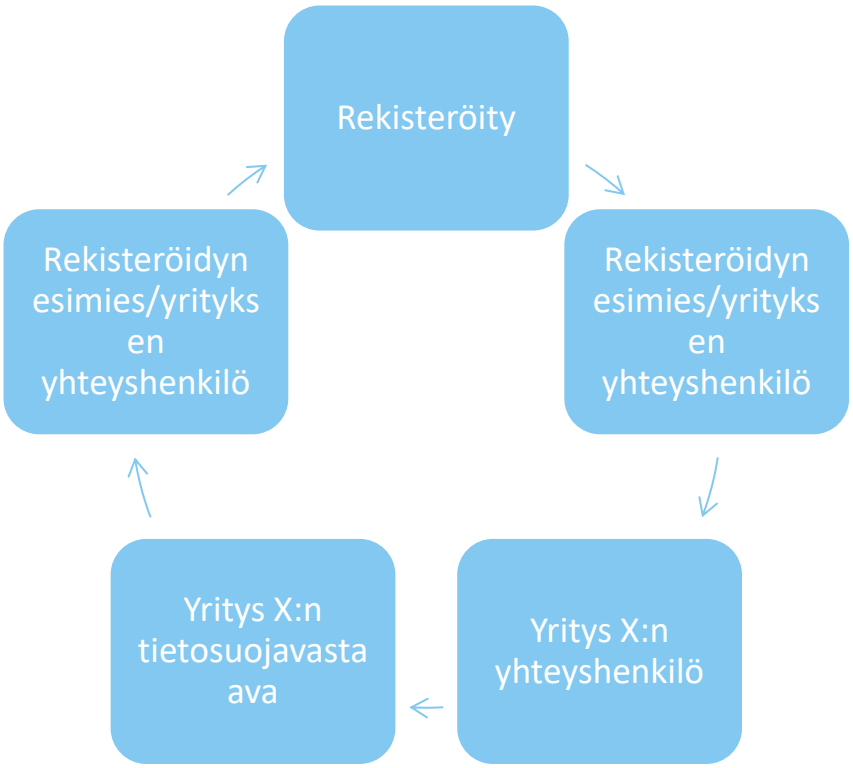
4.1.2 Rekisteröidyn oikeus henkilötietoihinsa

GDPR:n tarkoitus on parantaa EU:n alueella asuvien henkilösuojaa. Näin ollen EU:n alueella asuvilla luonnollisilla henkilöillä on oikeus saada tietää mitä tietoa heistä on kerätty. Kun Yritys X:n asiakas eli rekisteröity haluaa selvittää mitä tietoja Yritys X:llä on hänestä ja mahdollisesti niiden siirto- tai poistopyyntö, on se rekisteröidyn oikeus. Tietojen kysely ei tapahdu ottamalla suoraan yhteyttä tietosuojavastaavaan, vaan asiakkaan työntekijän tulee olla yhteydessä omaan esimieheensä, joka toimittaa kyselyn joko omalle yhteyshenkilölleen Yritys X:ssä tai

suoraan tietosuojavastaavalle. Yritys X:n edustaja kertoo, ettei heille ole tullut vielä yhtään tietopyyntöä tähän mennessä. (Yritys X:n edustaja 2018.)

Rekisteröidyn kysyessä hänestä kerättyjä henkilötietoja, voi henkilötietojen käsittelijä laskuttaa asiakastaan eli rekisterinpitäjää tästä tehtävästä. Myös Yritys X:llä nämä tietopyynnöt ovat aina sopimuksissa rajattu erillislaskutettaviksi, sillä nämä pyynnöt ovat heille sopimukseen kuulumatonta lisätyötä. Rekisteröidyn halutessa saada tietoja itsestään, joutuu rekisterinpitäjä silloin ostamaan Yritys X:ltä erikseen laskutettavana työnä nämä rekisteröidyn henkilötiedot. (Yritys X:n edustaja 2018.) Rekisteröidyn oikeuksia ovat siis saada henkilötietojen käsittelystä läpinäkyvästi tietoa, pääsyn omiin tietoihinsa, oikaista tietoja, tulla unohdetuksi, tietojen siirto toiseen järjestelmään, rajoittaa kerättyjen tietojen käsittelyä, vastustaa käsittelyä ja automatisoituja yksittäispäätöksiä, kuten profilointia. On myös mahdollista, että yrityksellä on oikeutettu etu henkilötietojen käsittelyyn, kuten esimerkiksi palkanlaskennan myötä. Tällöin yrityksen ei tarvitse poistaa rekisteröidyn henkilötietoja, vaikka hän sitä pyytäisi tai vastustaisi tietojen keräämistä. Rekisteröidyllä ei myöskään ole siirto-oikeutta henkilötietoihinsa, jos niiden siirto aiheuttaa vahinkoa muiden oikeuksiin ja vapauksiin. (Holopainen 2018, 14-17.)

Kuviossa 7 on havainnollistettu, missä järjestyksessä rekisteröidyn tekemä kysely henkilötiedoistaan etenee ja kuinka vastaus kulkee Yritys X:n tietosuojavastaavalta rekisteröidylle. Rekisteröity tekee kyselyn esimiehelleen, ellei hän itse ole esimies. Esimieheltä kysely menee Yritys X:n edustajalle ja hän toimittaa sen tietosuojavastaavalle, joka lopulta vastaa kyselyyn.



KUVIO 7. Henkilötietojen kysely

4.1.3 Tietosuojasopimukset ja osoitusvelvollisuus

Henkilötietojen käsittelijän ja rekisterinpitäjien täytyi tehdä tietosuojasopimukset jokaisen asiakkaan kanssa. Sopimuksissa todetaan mitä, miten, kuinka pitkään tietoja käsitellään. Lisäksi todetaan käsittelyn tarkoitus, henkilötietojen tyyppi, rekisteröityjen ryhmät ja rekisterinpitäjän velvollisuudet sekä oikeudet (Euroopan parlamentin ja neuvoston asetus 2016/679). Yritys X:n täytyi henkilötietojen käsittelijänä tehdä tietosuojasopimukset rekisterinpitäjien kanssa. Asiakkaiden suuren lukumäärän vuoksi on uusien sopimusten laatiminen vaatinut Yritys X:n hallinnolta paljon työtunteja (Yritys X:n edustaja 2018).

Sopimuksissa on tietyt velvoitteet mitä niissä täytyy olla, mutta jokainen asiakas voi neuvotella lisää ehtoja omiin sopimuksiinsa ja tämän vuoksi Yritys X:llä on lähes jokaisessa sopimuksessa erittäin paljon eroavaisuuksia. Lähes kaikki isot yritykset toimittivat heille oman versionsa, joihin ne tekivät muutosehdotuksia.

Nämä muutokset koskivat lähinnä mahdollisia korvaustilanteita tietosuojaloukkauksiin liittyen. Yritys X:llä on itsellään kybervakuutus, jossa korvauksen enimmäismäärä on todella suuri. Tämän huomioon ottaen, on kuitenkin asiakaskohtaisesti rajattu korvaukset tyypillisesti maksimissaan kolmen kuukauden palveluveloitusta vastaavaksi. Välillisiä kustannuksia, kuten maineen menetys, ei hyväksytty tietosuojasopimuksissa kertoo Yritys X:n edustaja. (2018.)

Rekisterinpitäjän ja henkilötietojen käsittelijän täytyy pystyä osoittamaan, että ne noudattavat GDPR asetuksen artikla 5 luvun 2 mukaista periaatteita, joita ovat muun muassa lain mukaisuus, läpinäkyvyys ja tietojen minimointi sekä säilytyksen rajoittaminen (Euroopan parlamentin ja neuvoston asetus 2016/679). Tämän takia on tarpeen dokumentoida kaikki tehdyt toimenpiteet, joilla voidaan todistaa yrityksen noudattavan GDPR asetusta. Yritys X:n on siis tarvittaessa pystyttävä todistamaan, että ne ovat noudattaneet artikla 5 luvun 2 periaatteita.

4.1.4 Ohjelmistot

Ohjelmistoja kaiken kaikkiaan Yritys X:llä on noin 50 yrityksen edustajan arvion mukaan. Tosin näistä kaikki eivät ole henkilötietojen käsittelyyn liittyviä. Palkkahallinnossa lasketaan palkkoja neljässä eri järjestelmässä. Kirjanpitoa ja taloushallintoa tehdään useammassa järjestelmässä, sillä niissä käytetään myös asiakkaiden omia järjestelmiä. Erityisesti GDPR koskettaa Yritys X:ssä palkkahallintoa ja matkareskontraa, mutta toki myös kirjanpidossa ja taloushallinnossa käsitellään henkilötietoja ainakin satunnaisesti. (Yritys X:n edustaja 2018.)

GDPR:n astuessa voimaan myös ohjelmistojen toimittajilta on vaadittu enemmän. Toimittajien pitää varmistaa, että henkilötietoja käsitellään oikein heidän ohjelmistoissaan ja tiedot säilytetään salattuna ja turvallisesti sekä tiedonsiirron että säilytyksen ajan. Henkilötiedot eivät saa olla saatavilla kuin niille, jotka tarvitsevat tietoja työssään, esimerkiksi matkareskontranhoitajan ei tarvitse tietää, kuuluuko rekisteröity ammattiliittoon, koska se ei ole oleellista hänen työssään. Koska nykyään rekisteröity voi pyytää tietojaan rekisterinpitäjältä ja tiedot täytyy toimittaa yksinkertaisessa ja helposti luettavassa muodossa rekisteröidylle, on hyvä varmistaa, että yrityksessä käytetyt ohjelmistot toimivat ja synkronoivat hyvin yhteen.

Tällöin tietojen toimittaminen helposti ja mahdollisimman pian on mahdollista. Sympan toimitusjohtaja ja perustaja Keijo Karjalainen kirjoittaa blogissaan, että monet HR- ja palkanlaskentajärjestelmät eivät pysty GDPR:n vaatimuksiin ja siirtämään tietoja järjestelmästä toiseen helposti ja yksinkertaisesti, jonka vuoksi yritykset joutuvat tekemään useita erilaisia Excel ja World tiedostoja tiedonsiirtoja varten (Karjalainen 2017.)

Tietojen siirtäminen järjestelmistä esimerkiksi erilaisiin Excel-tiedostoihin aiheuttaa sen, että henkilötietoja on monessa eri paikassa ja niiden hallinta voi vaikeutua. Tämän vuoksi on tärkeää tietää, minne tiedostoihin on siirretty mitäkin henkilötietoja. Lisäksi on varmistettava niiden asianmukainen säilyttäminen koko säilytysajan ja poistaa tiedot, kun säilytykselle ei ole enää edellytystä. Yritys X:n edustaja (2018) kertoo, että heillä on henkilötietoja sisältävien tietojen säilytys ja arkistointi sovittu asiakkaan kanssa tapauskohtaisesti, samoin säilytysajat, esimerkiksi osa Yritys X:n asiakkaista haluaa pidemmät säilytysajat kuin mitä laki vaatii.

4.1.5 Tietojen siirtäminen ulkomaille

Nykyään on yleistä, että yritykset saattavat säilyttää henkilötietoja erilaisissa pilvipalveluissa ja käytössä olevat ohjelmistot toimivat ulkomailla olevilla palvelimilla. Henkilötietoja joudutaan tällöin siirtämään ulkomaille, mahdollisesti myös EU:n ulkopuolelle. EU:n sisällä asetus koskee kaikkia yrityksiä samalla tavalla, mutta EU:n ulkopuolelle tietoja siirrettäessä on hyvä varmistaa, onko maa, johon henkilötiedot siirretään, komission kriteerien täyttävien maiden listalla. Yhdysvaltoihin henkilötietojen siirtäminen on rajattua ja sinne hyväksytään ainoastaan niihin yrityksiin tietojen siirtäminen, jotka kuuluvat Privacy Shield -järjestelmään. Tähän järjestelmään kuuluvat täyttävät ainoastaan henkilötietojen siirron kriteerit. Listaa siitä, mitkä yritykset kuuluvat Privacy Shield -järjestelmään ylläpitää Yhdysvaltojen kauppaministeriö. (European commission n.d.) Tällä hetkellä hyväksyttyjä maita ovat taulukossa 1 esitetyt maat.

TAULUKKO 1. Komission hyväksymät kriteerit täyttävät EU:n ulkopuoliset maat 26.3.2019 mennessä

Andorra	Guernsey	Japani	Liechten-stein	Sveitsi	Yhdysvallat (rajoitetusti)
Argen-tiina	Islanti	Jersey	Mansaari	Uruguay	
Färsaaret	Israel	Kanada	Norja	Uusi-Seelanti	

EU:n ulkopolisista maista kerrottaessa on myös huomioitava ajankohtainen Brexit eli Iso-Britannian eroaminen EU:sta. Iso-Britannian vielä kuuluessa EU:seen sovelletaan siellä GDPR asetusta, mutta jos Brexit toteutuu, lasketaan Iso-Britannia silloin myös EU:n ulkopuoliseksi maaksi. Kaikkien EU:n tai ETA:n ulkopuolella olevien maiden on täytettävä tietosuoja-asetuksen mukaiset suojatoimenpiteet tiedonsiirrossa tai tehtävä sopimus henkilötietojen siirrosta EU:n komissioin kanssa, eikä vielä ei ole tehty sopimuksia tiedonsiirrosta Iso-Britanniaan tai sieltä EU:n alueelle (Puustjärvi 2018).

Iso-Britannian oli tarkoitus erota EU:sta 12 huhtikuuta ilman sopimusta, mutta Iso-Britannia neuvotteli EU:n johtajien kanssa lisäajasta Brexitille. Neuvotteluiden tuloksena Iso-Britannia ja EU saivat 11 huhtikuuta sovittua lisäajasta 31 lokakuuta saakka. (Heikkilä ym. 2019.) Nyt Iso-Britannialla on lisäajalla aikaa tehdä sopimukset myös henkilötietojen siirrosta. Toisin kuin silloin, jos kova Brexit olisi tapahtunut ja Iso-Britannia eronnut ilman sopimusta.

Yrityksille kova Brexit olisi tarkoittanut GDPR:n kannalta katsottuna sitä, että henkilötiedot pitää siirtää joko EU:n alueelle tai jatkaa Isossa-Britanniassa henkilötietojen käsittelyä, mutta tästä vaihtoehdosta ei vielä osata sanoa varmaksi saadaanko tietoja siirrettyä EU:sta Isoon-Britanniaan ilman voimassaolevaa GDPR sopimusta. (Valo 2019.) Yritys X:ään Brexit voi vaikuttaa, jos he käyttävät Iso-Britanniassa sijaitsevia palvelimia tai heidän asiakkaiden kautta. Asiakkaiden

konsultoinnissa myös Brexitin vaikutukset GDPR:n kannalta katsottuna on ajankohtainen aihe.

4.2 Tietosuojaloukkaukset

Tietosuojaloukkauksella ja tietoturvaloukkauksella tarkoitetaan eri asioita ja siksi on tärkeätä, huomioida kummasta asiasta puhutaan. Tietosuojaloukkauksesta käytetään myös nimeä henkilötietojen tietoturvaloukkaus, joka kertoo, että kyseessä on tietosuojaloukkaus. (Tietosuojavaltuutetun toimisto: Tietoturvaloukkaukset 2018.) Tietoturva on laaja-alaista toimintaa, joka on osa henkilötietoja koskevaa tietosuojaa. Tietoturvaloukkaus ei siis aina kosketa tietosuoja-asetusta, tietoturvaloukkauksia ovat esimerkiksi palvelunestohyökkäys, tietokonevirukset ja tietomurrot. (Tietoturvaloukkaus.fi 2018.)

Asetuksessa tietosuojaaloukkauksella tarkoitetaan sitä, että siirrettyjä, tallennettuja tai muulla tavalla käsiteltyjä henkilötietoja lainvastaisesti tai vahingossa katoaa, muuttuu tai tuhoutuu. Myöskin tietojen luvaton luovuttaminen henkilöille, joilla ei ole oikeutta tai hyvää syytä käsitellä tietoja sekä luvaton pääsy tietoihin lasketaan tietosuojaloukkaukseksi. (Euroopan parlamentin ja neuvoston asetus 2016/679.)

Tietosuojaloukkaus voi tapahtua esimerkiksi, kun muistitikku tai muistikortti katoaa, tietokone varastetaan, tietokoneelle tulee virusohjelma tai palkkatosite toimitetaan väärälle henkilölle. Tietosuojaloukkaus voi aiheuttaa rekisteröidylle esimerkiksi riskin joutua identiteettivarkauden uhriksi. Yritykselle tietosuojaloukkauksesta voi aiheutua muun muassa maineen menetys yrityksen salassapitovelvollisuuden alaisten tietojen paljastuessa. (Tietosuojavaltuutetun toimisto: Tietoturvaloukkaukset 2018.)

Tietosuojavaltuutetun toimisto suosittelee yrityksiä dokumentoimaan jokaisen tietosuojaloukkauksen ja niistä aiheutuneet vaikutukset sekä tehdyt korjaavat toimenpiteet katsomatta sitä, mitä toimenpiteitä henkilötietojen tietoturvaloukkauk-

sesta lopulta seuraa. Jos yritys jättää tekemättä dokumentoinnin tietosuojaloukkauksesta, laiminlyövät he tietosuoja-asetusta. Laiminlyönnistä voi seurata yritykselle sanktioita. (Tietosuojavaltuutetun toimisto: Tietoturvaloukkaukset 2018.)

Tähän mennessä ei ole käynyt ilmi kovin monta tietosuojaloukkaustapausta, mutta Saksassa on tapahtunut ensimmäinen ennakkotapaus. Tapauksessa yhdysvaltalainen ICANN, joka vahtii rekisteröityjen domain-nimien tietokantaa, määräsi heidän saksalaisen yhteistyökumppaninsa EPAGin rikkomaan lakia. ICANN oli ostanut EPAGin keräämään henkilötietoja domaineja ostavilta ja ICANN määräsi EPAGin myöskin keräämään varmuuden vuoksi rekisteröinnin tehneen osapuolen teknisen ja hallintohenkilön nimet ja yhteystiedot. EPAG kieltäytyi määräyksestä ja vetosi GDPR:n artikla 5:een: ’’tietojen keräämiselle ei ole liiketoiminnan kannalta aitoa tarvetta’’. ICANN on valittanut Bonnin oikeusistuimelle, ettei EPAG ole noudattanut sopimusta, mutta oikeusistuin hylkäsi valituksen. Myöhemmin ICANN valitti Kölnin korkeimpaan oikeuteen saamastaan päätöksestä. (Virtanen Jori 2018.) Ennakkotapaus on hyvä esimerkki siitä, kuinka GDPR koskee myös EU:n ulkopuolisia toimijoita, jos ne keräävät tietoa EU:n kansalaisista.

Suomessa paljon julkisuudessa ollut kohu Trafin ajokorttitietopalvelusta aiheutti myös paljon tietosuojaloukkauksista ilmoituksia tietosuojavaltuutetun toimistolle. Palvelussa oli tarkoitus pystyä tarkistamaan luonnollisten henkilöiden ajo-oikeuksia, mutta sieltä oli mahdollista myös selvittää luonnollisten henkilöiden henkilötunnukset, vaikka se ei ollut palvelun tarkoitus. Tietosuojavaltuutetun toimistolta lähetettiin Trafille selvityspyyntö heidän saamien palautteiden pohjalta. Tapauksen takia jouduttiin lopulta sulkemaan kokonaan Trafin sivut 9.12.2018 ja ne saatiin auki osittain vasta 21.12.2018. (Virtanen Jarmo 2018.)

4.2.1 Tietosuojaloukkauksesta ilmoittaminen valvontaviranomaiselle

Tietosuojaloukkauksen sattuessa on arvioitava, aiheutuuko loukkauksesta riskiä rekisteröidylle ja hänen henkilötiedoilleen, niin että se loukkaisi rekisteröidyn oikeuksia ja vapauksia. Ilmoitus tehdään valvontaviranomaiselle, joka on Suo-

messa tietosuojavaltuutetun toimisto. Tätä työtä kirjoittaessani Suomessa tietosuojavaltuutettuna toimi Reijo Aarnio. (Tietosuojavaltuutetun toimisto: Tietosuojavaltuutetun toimisto n.d.)

Henkilötietoja koskevan tietoturvaloukkauksen sattuessa on arvioitava tilanne. Jos todetaan loukkauksen vaikutusten olevan sellaiset, että ilmoitus on tehtävä, pitää se tehdä mahdollisimman pian ilman aiheetonta viivytystä. Rekisterinpitäjän huomatessa tietosuojaloukkauksen tapahtuneen, täytyy hänen ilmoittaa 72 tunnin sisällä tietosuojavaltuutetun toimistolle siitä. Tämä 72 tuntia alkaa siitä, kun rekisterinpitäjä on saanut tietää tietosuojaloukkauksesta. Henkilötietojen käsittelijän huomatessa tietosuojaloukkauksen, täytyy hänen ilmoittaa ensin rekisterinpitäjälle asiasta, elleivät rekisterinpitäjä ja henkilötietojen käsittelijä ole sopineet, että henkilötietojen käsittelijä voi tarvittaessa tehdä itse ilmoituksen suoraan tietosuojavaltuutetun toimistolle. Vaikka näin olisi sovittu, on vastuu ilmoituksen tekemisestä silti rekisterinpitäjällä. (Euroopan parlamentin ja neuvoston asetus 2016/679.) Yritys X:n työntekijän epäillessä henkilötietojen tietoturvaloukkausta, pitää hänen ilmoittaa asiasta esimiehelleen tai tietosuojavastaavalle, jotka arvioivat tilanteen ja tarvittaessa ilmoittavat siitä rekisterinpitäjälle ja tietosuojavaltuutetulle.

Jos ilmoitus joudutaan tekemään, on siinä kerrottava seuraavat asiat: kuvailtava tapahtunutta tietosuojaloukkausta, rekisteröityjen ryhmät ja henkilötietotyyppien ryhmät ja niiden määrät, todennäköiset seuraukset loukkauksesta, toimenpiteet, jotka on tehty tai ehdotettu sekä keinot, joilla pienennettäisiin haittavaikutuksia. (Euroopan parlamentin ja neuvoston asetus 2016/679.) Ilmoituksena voi käyttää esimerkiksi liitteenä 1 olevaa lomaketta tai täyttää tietosuojavastaavan kotisivuilla lomakkeen. Tietosuojaloukkauksista tehdyt ilmoitukset tietosuojavaltuutetun toimistolle tutkitaan aina.

4.2.2 Tietosuojaloukkauksesta rekisteröidylle ilmoittaminen

Tietosuojaloukkauksesta on ilmoitettava rekisteröidylle, loukkauksen aiheuttaessa hänelle korkean riskin. Ilmoitus täytyy tehdä ilman aiheetonta viivytystä. (Euroopan parlamentin ja neuvoston asetus 2016/679.) Yritys X:llä tietosuojaloukkaus on mahdollista tapahtua rekisterinpitäjänä ja henkilötietojenkäsittelijänä. Jos henkilötietojen tietoturvaloukkaus tapahtuisi ja Yritys X toteaisi sen aiheuttavan rekisteröidyille luonnollisille henkilöille korkean luokan riskin heidän oikeuksille ja vapauksille täytyisi rekisterinpitäjän tehdä ilmoitus rekisteröidyille, tapahtuneesta tietoturvaloukkauksesta mahdollisimman pian.

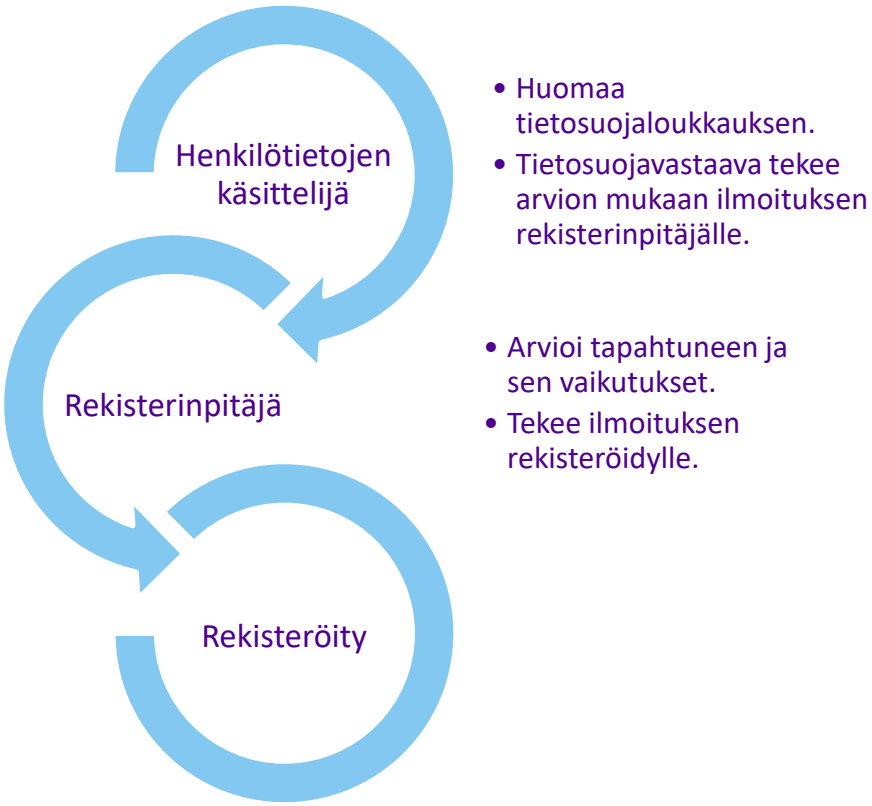
Rekisterinpitäjän tai mahdollisesti henkilötietojen käsittelijän tehdessä ilmoitusta rekisteröidylle on ilmoituksessa kerrottava selvästi ja helposti ymmärrettävästi, mitä on tapahtunut ja mitkä ovat mahdollisesti odotettavissa olevat seuraamukset. Tämän lisäksi on kerrottava tietosuojavastaavan nimi ja yhteystiedot tai muun vastaavan henkilön nimi ja yhteystiedot, jolta saa lisää tietoa, elleivät yhteystiedot jo olleet rekisteröidyllä tai rekisteröidyillä tiedossa. Rekisterinpitäjän jo tekemät tai ehdottamat toimenpiteet on myös kerrottava ilmoituksessa rekisteröidylle. (Euroopan parlamentin ja neuvoston asetus 2016/679.) Ilmoitusta rekisteröidylle tehtäessä pohjana voi käyttää samaa Liite 1 kaavaketta kuin millä ilmoitetaan tietosuojavaltuutetun toimistolle tietosuojaloukkauksesta.

Tietosuojaloukkauksen sattuessa täytyy tehdä selvitys aiheuttaako se korkean riskin rekisteröidylle. Ilmoitusta ei tarvitse tehdä loukkauksesta, jos yksi seuraavista kolmesta tietosuoja-asetuksen artiklan 34, ehdoista täyttyy: ensimmäinen ehto on se, että henkilötiedot on muutettu rekisterinpitäjän tai henkilötietojen käsittelijän toimesta muotoon, josta ulkopuolinen henkilö ei niitä pysty samaan ymmärrettäväksi. Tällöin tiedot ovat esimerkiksi anonymisoitu tai pseudonymisoitu. Toinen ehto on se, että rekisteröidyn henkilön oikeuksia ja vapauksia uhannut korkea riski ei tulevaisuudessa voi todennäköisesti tapahtua uudestaan rekisteröidyn ja henkilötietojen käsittelijän tekemien muutosten ja toimenpiteiden ansiosta. Kolmas ehto on se, että ilmoituksen tekeminen rekisteröidylle aiheuttaisi kohtuutonta vaivaa. Näin tapahtuessa on rekisterinpitäjän ilmoitettava apunaan käyttäen julkista tiedonantoa tai muuta samanveroista kanavaa käyttäen, millä

rekisteröidyille pystytään ilmoittamaan yhtä toimivalla tavalla. (Tietosuojamalli: Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle 2017.)

Jos rekisteripitäjä jättää tekemättä ilmoituksen tietosuojaloukkauksesta rekisteröidylle, voi tietosuojavaltuutetun toimisto vaatia rekisterinpitäjää tekemään ilmoituksen tai tehdä päätöksen, että yksi kolmesta edellä mainituista ehdoista täyttyy. Tapauksessa tarkastellaan, kuinka odotettavissa tietosuojaloukkauksesta aiheutuvat korkeat riskit ovat rekisteröidylle. (Euroopan parlamentin ja neuvoston asetus 2016/679.)

Kuviossa 8 on havainnollistettu, miten henkilötietojen tietoturvaloukkauksesta ilmoitetaan rekisteröidylle. Yritys X:n työntekijän havaitessa tietosuojaloukkauksen, tulee hänen ilmoittaa tietosuojavastaavalle, joka arvioi tapahtuneen ja ilmoittaa rekisterinpitäjälle. Rekisterinpitäjä arvioi yhdessä tietosuojavastaavan kanssa, täyttyykö jokin ehdoista miksi ilmoitusta ei tarvitsisi tehdä. Jos mikään näistä ehdoista ei täyty, ilmoittaa rekisterinpitäjä, silloin rekisteröidylle tapahtuneesta.



KUVIO 8. Henkilötietojen tietosuojaloukkauksesta rekisteröidylle ilmoittaminen

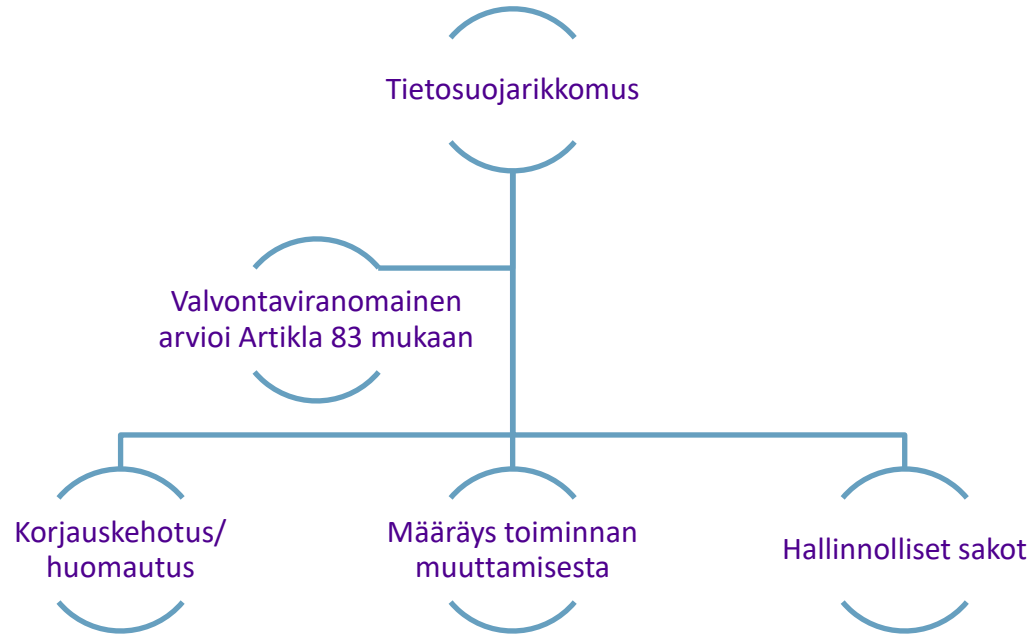
4.2.3 Sanktiot

Henkilötietojen käsittelyä koskeva rikos, rikkomus tai muu väärinkäyttö voi johtaa työoikeudellisiin sekä rikos- ja vahingonkorvausoikeudellisiin seuraamuksiin. Työoikeudellinen sanktio voi olla huomautus tai varoitus, mutta myös työsuhteen irtisanominen tai purkaminen on mahdollista. Henkilörekisteririkkomukseen voi syyllistyä, jos rikkoo rekisterinpitäjien antamia asiakastietojen käsittelyä koskevia suojausohjeita. (Euroopan parlamentin ja neuvoston asetus 2016/679.)

Tietosuoja-asetuksen rikkomisesta voidaan määrätä hallinnolliset sakot, jotka voivat olla suurimmillaan 20 miljoonaa euroa tai neljä prosenttia yrityksen maailmanlaajuisesta edellisen tilikauden liikevaihdosta, riippuen kumpi näistä on suurempi. Hallinnollinen sakko voi myös olla 10 miljoonaa euroa tai kaksi prosenttia yrityksen maailmanlaajuisesta liikevaihdosta, riippuen jälleen siitä, kumpi näistä on suurempi. Rikkomuksen täytyy tällöin olla todella vakava, jotta valvontaviranomainen määräisi ankarimmat sanktiot yritykselle. Rikkomuksessa vaikuttaa myös se mitä asetuksesta on rikottu, jonka mukaan katsotaan, onko enimmäissakko 20 miljoona/neljä prosenttia kansainvälisestä liikevaihdosta vai 10 miljoona/kaksi prosenttia kansainvälisestä liikevaihdosta. (Euroopan parlamentin ja neuvoston asetus 2016/679.) Tietosuoja-asetuksen rikkomisesta ei tietosuojaa valvova viranomainen, eli tietosuojavaltuutetun toimisto, voinut antaa Suomessa hallinnollista sanktiota ennen kuin kansallinen laki tuli voimaan 13.11.2018 (Mattila 2018).

Hallinnollisia sakkoja määrätessä katsotaan tapahtunut henkilötietojen tietoturvaloukkaus aina yksittäisenä tapauksena. Arvioitaessa sakkojen määräämistä ja sakon määrän suuruutta, otetaan huomioon artikla 83 EU yleisestä tietosuoja-asetuksesta. Ehtoja ovat muun muassa rikkomisen luonne, kesto ja vakavuus, moneenko tahoon rikkomus vaikuttaa, kuinka suuria aiheutuneet vahingot ovat, onko rikkomus ollut tahallinen, henkilötietojen käsittelijän tai rekisterinpitäjän tekemät toimet, jotta rekisteröidylle aiheutunutta vahinkoa on lievennetty, aiemmat rikkomukset henkilötietojen käsittelijällä tai rekisterinpitäjällä, yhteistyö valvontaviranomaisen kanssa rikkomisen korjaamiseksi ja sen aiheuttaneiden vahinkojen lieventämiseksi sekä vaikutus henkilötietoryhmiin. (Tietosuojamalli: Hallinnollisten sakkojen määräämisen yleiset edellytykset 2017.)

Kuviossa 9 on kuvailtu, kuinka tietosuoja-asetuksen rikkomisesta sanktioiden määrääminen menee. Ensin tapahtuu tietoturvarikkomus, josta tehdään ilmoitus valvontaviranomaiselle eli Suomessa ilmoitus tehdään tietosuojavaltuutetun toimistolle. Valvontaviranomainen arvio rikkomuksen ja sen vaikutukset artikla 83 mukaan. Tehtyään arvion tapahtuneesta rikkomuksesta valvontaviranomainen, eli tietosuojavaltuutetun toimisto, antaa korjauskehotuksen tai määräyksen toiminnan muuttamisesta, jos rikkomuksen huomautuksiin ei ole reagoitu. Tarvittaessa määrätään hallinnollinen sakko.



KUVIO 9. Tietosuojarikkomuksesta sanktion määräytyminen

Ensimmäinen suuri hallinnollinen sakko, jossa vedottiin GDPR:ään, määrättiin 21.1.2019 Ranskassa Googlelle. Ranskan tietosuojaviranomaiset (CNIL) määräsivät Googlelle 50 miljoonan euron sakot. Sakkoja perusteltiin GDPR:n vaatimusten toteuttamatta jättämisellä. CNIL kertoi, ettei Google tarjoa käyttöehdoistaan riittävän läpinäkyvää ja helposti saatavilla olevaa tietoa, vaan tiedot ovat vaikeasti ja monimutkaisesti löydettävissä. Googlen kohdennettua verkkomainontaa on erityisesti pidetty liian heikosti informoituna. Rekisteröidyille eli Googlen käyttäjille ei kerrota riittävän selkeäasti, mitä tietoa Google heistä kerää, mitä näillä tiedoilla

tehdään ja kauanko kerättyjä tietoja säilytetään. Google ei myöskään kerro riittävän selvästi, minkä tiedon avulla ne tekevät kohdennettua verkkomainontaa käyttäjilleen. (Alma Talent Pro 2019.)

Tietosuoja-asetuksen mukaan rekisterinpitäjän on ilmoitettava rekisteröidylle, muun muassa mitä tietoja kerätään ja niiden säilytyksestä sekä esittää ne rekisteröidylle mahdollisimman yksinkertaisesti. Googlella tiedot henkilötietojen käsittelystä ovat saatavilla, mutta CNIL:n mukaan niiden löytäminen on liian hankalaa, eikä näin ollen täytä GDPR:n vaatimuksia. (Laitila 2019).

Toisena perusteena määrätyille sakoille oli liian epäselvä käytäntö pyytää lupa rekisteröidyiltä käyttää henkilötietoja kohdennetussa mainonnassa. Googlen käyttöehdoissa ei kerrota tarpeeksi yksinkertaisesti henkilötietojen käytön laajamittaisuutta Googlen eri palveluissa, kuten esimerkiksi YouTubessa, Google Mapsissa ja Google Play kaupassa. (Laitila 2019.)

Ranskan tietosuojaviranomaisen CNIL:n päätökseen määrätä hallinnolliset sakot Googlelle sai alkunsa kahdesta valituksesta. Valitukset tekivät ranskalainen Quadrature du Net -ryhmä ja Noyb.eu. Quadrature du Net on ranskalainen digitaalisia oikeuksia ajava ryhmä, joka hankki myös 10 000 allekirjoitusta valituksensa tuekseen. Noyb.eu eli None Of Your Business on taas itävaltalaisen tietoturva-aktivistin Max Schremsin perustama ryhmä, joka on aikaisemminkin tehnyt valituksia suurista sosiaalisen median yrityksistä, kuten Facebook, Instagram ja WhatsApp, mutta näissä tapauksissa oli valitukset vielä kesken tätä työtä kirjoittaessani. Noyb.eu:n perustaja Schrems on muun muassa syyttänyt Googlea siitä, että käyttäjät saavat Googlen käyttämistä ponnahdusikkunoista vaikutuksen, että käyttöehdot on pakko hyväksyä, jos haluaa käyttää heidän palveluita. (HS-AFP 2019; Cyrus Farivar 2019.)

Kuvio 9 selventää, mitä Googlen tapauksessa on käynyt. Ensin on tapahtunut rikkomus, josta Googlea syytetään. Siitä on tehty ilmoitukset tietosuojarikkomuksesta valvontaviranomaiselle, joka tässä tapauksessa on Ranskan tietosuojaviranomainen eli CNIL. Ranskan tietosuojaviranomainen alkoi tutkimaan tapausta ja teki lopulta päätöksen määrätä hallinnolliset 50 miljoonan euron sakot Googlelle.

Kerroin aikaisemmin, että Yritys X:llä on käytössä kybervakuutus, jota myös osa asiakkaista vaati Yritys X:ltä. Asiakkuuksien johtamisen ja yrityksen strategian kannalta vakuutukset ovat merkittävässä osassa asiakassuhteen luottamuksen lisäämisessä.

Yrityksen oman strategian kannalta vakuuttamalla mahdollisesta tietosuojaloukkauksesta aiheutuvia kuluja pystytään hallitsemaan riskejä paremmin. Suomessa on mahdollista ottaa vakuutus tietosuojaloukkausta varten, vaikka jokaisessa maassa ei sakkoja kuitenkaan pystytä vakuuttamaan. Suomi ja Norja ovat ainoat maat Euroopassa, jossa sakot pystytään vielä vakuuttamaan. Osassa maissa katsotaan tapauskohtaisesti vakuutetun toimintaa. Vakuutuksissa aina katsotaan, onko toiminta ollut tahallisesti aiheutettua, jolloin ei vakuutetulle korvata mitään. Asioita, joita GDPR:n kannalta voi vakuuttaa ovat muun muassa tietoturvaloukkauksen tutkinta- ja puolustuskustannukset sekä esimerkiksi asiakkaalle aiheutuneet kustannukset. (Case & Heinonen n.d.)

5 GDPR:N VAIKUTUS ASIAKKUUKSIEN JOHTAMISEEN

Asiakkaat voidaan luokitella sisäisiin ja ulkoisiin asiakkaisiin. Sisäisiä asiakkaita ovat esimerkiksi Yritys X:n omat työntekijät ja ulkoisia heidän asiakkaansa. Asiakkuuksien johtamiseen vaikuttaa myös se, ovatko asiakkaat luonnollisia henkilöitä vai yrityksiä. Tässä työssä tarkastelen ulkoisia asiakkaita ja heidän asiakkuuksien johtamista, Yritys X:n ulkoiset asiakkaat ovat eri kokoisia yrityksiä.

5.1 Asiakaskokemus/palvelu

Palveluun perustuvassa työssä asiakaslähtöinen toiminta on tärkeää jokapäiväisessä työssä. Perustehtävistä eteneminen yhä enemmän asiakaslähtöisen toiminnan tukemiseen vaati yritykseltä asiakasajattelun osaamista, taidokasta taloustiedon yhdistämistä asiakkaisiin, taloushallinnon prosessien ja järjestelmien kehittämistä sekä muutoksia muiden yhteistyötä tekevien funktioiden kanssa (Hellman & Värilä 2009, 74).

Asiakkaan saama asiakaskokemus ei muodostu pelkästään kasvokkain ja muilla yhteydenpitotavoilla tapahtuvasta vuorovaikutuksesta, vaan siihen vaikuttaa koko asiakassuhteen kokonaisuus. Asiakaskokemukseen vaikuttaa siis asiakkaan mielikuva yrityksestä ja kuinka hyvin Yritys X onnistuu toteuttamaan asiakkaan odotukset ja onko palvelu sitä mitä toivottiin. Löytänän ja Kortesuon (2011, 62) mukaan asiakaskokemus jaetaan ydinkokemukseen, laajennettuun kokemukseen ja odotukset ylittävään kokemukseen. Ydinkokemuksella tarkoitetaan sitä, että asiakas saa Yritys X:n tapauksessa hyötyä ostamalleen palvelulle. Esimerkiksi palkanlaskennan ulkoistaminen Yritys X:lle tuo hyötyarvoa asiakkaalle.

Laajennetussa kokemuksessa lisätään ydinkokemukseen päälle vielä jotain, joka lisää palvelun arvoa. Laajennetussa kokonaisuudessa on kaksi osaa, jotka ovat edistäminen ja mahdollistaminen. Edistämisessä asiakaskokemukseen tuodaan osia, jotka suoraan tukevat asiakaskokemuksen levittäytymistä ydinkokemuksen ulkopuolelle. Mahdollistamisessa asiakkaalle tarjotaan välillisesti palveluja, joilla

parannetaan asiakaskokemusta, kuten itse käytettävät ohjelmat. (Löytänä & Kortesuo 2011, 62.) Edistämisestä esimerkkinä Yritys X tarjoaa asiakkailleen taloushallinnon tehtävien lisäksi konsultointipalveluja.

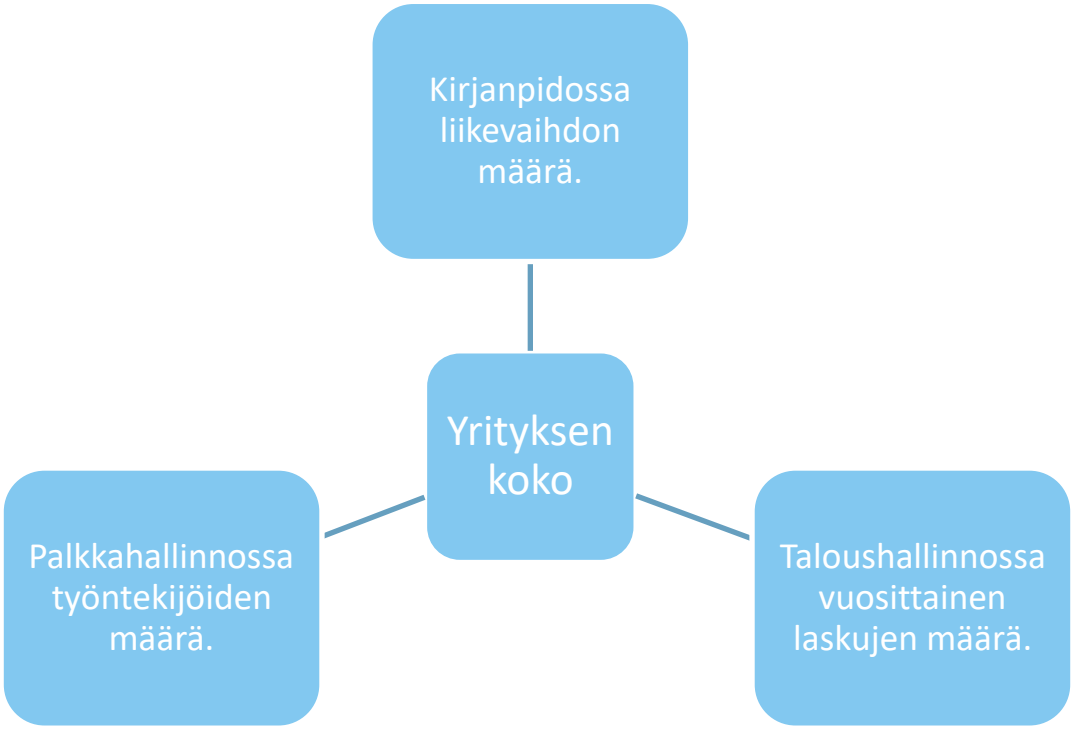
Ydinkokemuksen ja laajennetun kokemuksen jälkeen voi vasta syntyä odotukset ylittävä kokemus, joka muodostuu erilaisista elementeistä. Näitä elementtejä ovat muun muassa henkilökohtainen, olennainen, räätälöity, oikea-aikainen, kestävä, selkeä ja tuottava. (Löytänä & Kortesuo 2011, 64.) Odotukset ylittävässä asiakaskokemuksessa asiakkaalle pyritään tuomaan lisää arvoa asiakkaan tarpeiden mukaan edellä mainittujen elementtien avulla. Asiakaskeskeinen toimintatapa on myös oikein toteutettuna hyvä kilpailuetu.

Asiakaskokemuksen parantumisessa onnistumista kannattaa seurata erilaisten mittareiden avulla. Tässä tapauksessa asiakaskokemusta voidaan mitata esimerkiksi asiakkaille tehtävällä laadullisella eli kvalitatiivisella tutkimuksella, joka toteutettaisiin kyselyllä. Kyselyssä selvitettäisiin kuinka Yritys X on onnistunut asiakkaiden mielestä GDPR:ään liittyen. Kysymyksissä selvitettäisiin, tiedotettiinko GDPR:ään liittyvistä sopimuksista ja niiden muutoksista ajoissa, kuinka asiakkaat kokivat Yritys X:n onnistuneen tietosuojavaatimuksissa, toiko GDPR minkälaisia vaikutuksia asiakassuhteeseen, kuinka helpoksi koetaan tarvittaessa tietosuojavastaavan yhteyden saaminen ja mitä parannettavaa tietosuojaan liittyen olisi tehtävä. Yrityksen mitatessa GDPR:ssä onnistumista laadullisen tutkimuksen avulla, saa se arvokasta tietoa asiakkailtaan, mikä on hyvää palveluissa nyt ja mitä olisi mahdollista kehittää.

5.2 Erilaiset asiakkuudet

Tarkastelen asiakkuuksia työssä yrityksen koon mukaan. Näitä ovat suur-, pk- ja pienyritykset. Jako näihin luokkiin on tehty osittain kirjanpidon kokoluokituksen mukaan ja osittain Yritys X:n asiakkaan tarvitseman palvelukokonaisuuden mukaan. Osa asiakkaista on esimerkiksi pelkästään palkkahallinnon asiakas ja tällöin määräävää on työntekijöiden lukumäärä. Kirjanpidossa määräävää on yrityksen liikevaihto ja taloushallinnossa laskujen vuosittainen lukumäärä (Yritys X:n edustaja 2018). Kuviossa 10 on kuvailtu edellä mainittu yritysten jakoluokitus,

jonka mukaan Yritys X määrittelee asiakas yrityksensä koon. Jokaisella yrityksen kokoluokalla on erilaiset tarpeensa ulkoistetulta taloushallinnolta ja myös GDPR vaikuttaa näihin kaikkiin kokoihin, mutta yrityksille suunnatuissa palveluissa on eroja myös henkilötietojen käsittelyssä ja sen vaatimuksissa.



KUVIO 10. Asiakasyrityksen koon määritelmät Yritys X:llä

Suuret yritykset

Tähän luokkaan jaotellut yritykset ovat niitä yrityksiä, joilla on suuret liikevaihdot, palkkahallinnossa paljon työntekijöiden palkkoja laskettavana tai niillä on paljon laskuja vuosi tasolla mitattuna. Suurilla yrityksillä on nimetty omat asiakkuuspäälliköt, jotka toimivat yhteyshenkilönä asiakkaan ja Yritys X:n välillä. Suurilla yrityksillä on myös yleensä valmiina omat pohjansa GDPR sopimuksiin, joita Yritys X muokkasi aina jokaisen yrityksen kanssa yrityskohtaisesti. Suurien yritysten asiakkuuksien johtaminen eroaa muista yrityksistä siinä, että heillä on enemmän ehtoja, joita ne vaativat Yritys X:ltä sopimuksissa. Suurille yrityksille tarjottavista

palveluista muun muassa Palkkahallinto, HR-järjestelmät, M2-matkalaskujärjestelmä ja tietojärjestelmät ovat niitä palveluja, joissa GDPR erityisesti koskettaa Yritys X:ää henkilötietojen käsittelijänä. (Yritys X:n edustaja 2018.)

Suurilla yhtiöillä saattaa olla lisäksi omia ohjelmistojaan, joita Yritys X:n työntekijät käyttävät työssään. Yritys X:n käyttäessä asiakkaidensa ohjelmistoja, esimerkiksi asiakkaan intranetin kautta työssään henkilötietojen käsittelijänä, on ohjelmistojen tietoturvasta huolehtiminen asiakasyrityksen eli rekisteripitäjän vastuulla, mutta Yritys X:n täytyy pitää huolta, että heidän käyttämänsä yhteydet ovat suojattuja riittävällä tavalla. Jokainen työntekijä omassa jokapäiväisessä työssään huolehtii, ettei henkilötietoja ole näkyvissä niille, joilla ei ole oikeutta kyseisten henkilötietojen näkemiseen. Osa suurista asiakkaista saattavat haluta, että kaikki heidän kirjanpitonsa ovat samassa paikassa arkistoituna esimerkiksi rekisterinpitäjän omilla palvelimilla ja tiloissa. Tietojen arkistoinnista huolehtii tällöin rekisterinpitäjä. Tällöin Yritys X toimittaa ja tallettaa tiedot rekisterinpitäjän arkistoon, eikä henkilötietojen arkistointi ole enää Yritys X:n vastuulla.

Suuret yritykset ovat yleensä julkisesti tunnetumpia ja maailmanlaajuiset liikevaihdot ovat suurempia kuin pk- ja pienyrityksillä, jonka vuoksi nämä asiakkaat vaativat tiukempia sopimuksia GDPR:ään liittyen. Suurille yrityksille tietosuojaloukkaus voisi tuoda merkittäviä maineen menetyksiä ja sanktioiden suuruudet olisivat rahallisesti merkittävän suuria. Melkein jokainen suuri yritys toimitti Yritys X:lle omat versionsa GDPR-sopimuksista, joita muutettiin lähinnä juuri mahdollisten tietosuojaloukkausten korvausten osalta. Edellä mainittujen sanktioiden ja muiden seurausten vuoksi suuret yritykset vaativat tarkempia ohjeistuksia tietoturva-asetuksen noudattamiseen ja sitä voidaan seurata esimerkiksi auditointien avulla.

Pk-yritykset

Pk-yritykset eli pienet ja keskisuuret. Tätä termiä käytetään yrityksistä, joiden koko on isompi kuin pienillä yrityksillä, mutta pienempi kuin suurilla. Eli yrityksen liikevaihto ei ole yli 50 miljoonaa euroa tältä tilikaudelta, taseen loppusumma ei ylitä 43 miljoonaa euroa ja yrityksessä on alle 250 henkilöä töissä. Pk-yritykset

eivät kirjanpitolain mukaan ole varsinainen oma luokkansa, mutta se on yleisesti käytetty termi kuvaamaan yritystä, joka ei täytä suuryrityksen vaatimuksia, mutta on selvästi pienyritystä isompi. (Tilastokeskus n.d.) Näin ollen pk-yrityksillä on myös erilaiset tarpeet ulkoistetulta taloushallinnolta kuin suurilla ja pienyrityksillä. Pk-yrityksille tarjottavia palveluita, joita GDPR erityisesti koskettaa ovat henkilöstöhallinto, matkalaskujärjestelmät ja kirjanpito (Yritys X:n edustaja 2018).

Yritys X:n asiakkaana olevat pk-yritykset voivat myös olla julkisesti tunnettuja yrityksiä, jolloin myös tietosuojaloukkaus saattaa aiheuttaa huomattavan maineen menetyksen. Sanktiot eivät ole rahamääräisesti mitattuina yhtä suuria kuin isoimmilla pörssiyhtiöillä, mutta prosentuaalisesti suhteutettuna ne ovat vastaavia ja voivat vaikuttaa yritysten talouteen ratkaisevasti. Pk-yrityksien asiakkuuksien johtamisessa on GDPR:n osalta otettava huomioon juuri oikeaoppinen henkilötietojen käsittely, henkilöstöhallinnan palveluiden, matkalaskujärjestelmien ja kirjanpidon osalta. Muissa heille tarkoitetuissa palveluissa ei käsitellä henkilötietoja kuin satunnaisesti. Pk-yrityksien antamissa ohjeistuksissa rekisterinpitäjänä henkilötietojen käsittelijälle, eli Yritys X:lle, on yrityskohtaisia tapoja ja ehtoja henkilötietojen oikea oppiseen käsittelyyn. Ohjeistuksien noudattamista voidaan myös valvoa esimerkiksi auditointien avulla.

Pienyritykset

Kirjanpitolain mukaan pienyritykseksi luokitellaan yritys, joka on kirjanpitovelvollinen ja se ei ylitä kuin enintään yhden seuraavista raja-arvoista päättyneellä eikä sitä edeltäneellä tilikaudella. Raja-arvot ovat työntekijöitä on tilikaudella noin 50, yrityksen liikevaihto 12 miljoonaa euroa tai taseen loppusumma on 6 miljoonaa euroa. Näitä kriteereitä pienemmät yhtiöt ovat muun muassa mikro yritykset tai ammatin- tai liikkeenharjoittajia kirjanpitolain mukaan. (Kirjanpitolaki 1997.) Yritys X:n luokitellessa asiakkaita ryhmiin kuvion 10 mukaisilla kriteereillä, pienyritykseksi luokitellaan kaikki pienet yritykset, joilla on vähemmän laskuja tai henkilökuntaa, joille palkkoja lasketaan.

Pienyritykset eivät yleensä käsittele niin paljon henkilötietoja kuin pk- ja suuret yhtiöt, eivätkä ne siksi aina vaadi sopimuksiin lisäehtoja niin paljon kuin suuremmat yhtiöt. Samalla Yritys X:n edustajalla voi olla asiakkaana useampikin pieni yhtiö, jonka yhteyshenkilönä hän toimii. Pienyrityksille tarjottavia palveluja, joita GDPR erityisesti koskettaa ovat palkanlaskenta, sähköinen taloushallintojärjestelmä, ulkoistettu taloushallinto ja kirjanpito (Yritys X:n edustaja 2018).

Monelle pienelle yhtiölle taloushallinnon ulkoistaminen kokonaan Yritys X:lle on hyvä vaihtoehto, koska tällöin ne voivat keskittyä omaan liiketoimintaansa. Tällöin Yritys X on henkilötietojen käsittelijänä kaikissa asiakasyrityksensä taloudellisissa asioissa. Näin ollen myös taloushallintoa koskevat vaikutukset GDPR:stä ovat helpompia hallita ja varmistaa oikeaoppinen käsittely. Arkistoitaessa henkilötiedot ainoastaan Yritys X:lle, niiden hallinnointi tapahtuu yhdestä paikasta, eikä asiakkaan tarvitse kysellä usealta eri henkilötietojen käsittelijältä rekisteröityjen tietoja tarvittaessa.

Pienien yhtiöiden asiakkuuksien hallinnassa rekisterinpitäjille eli asiakkaille tarkoitetuissa GDPR:ää koskettavissa palveluissa on oltava tarkkoja samoissa asioissa kuin pk- ja suuryhtiöiden kanssa. Pienemmiksi luettaville yrityksille tarjotaan muun muassa taloushallinnon kokonaispalveluita ja konsultointia, joissa voidaan hyvin neuvoa rekisterinpitäjää, mitä pitää ottaa huomioon ja varmistaa GDPR ohjeistuksien osalta, jotta rekisterinpitäjä välttää ongelmat ja mahdolliset tietoturvaloukkaukset, varsinkin jos kyseessä on aloittava uusi yritys. Uutta yritystä konsultoidessa voidaan esimerkiksi käyttää liitteenä 2 olevaa tekemääni muistilistaa tai tietosuojavaltuutetun kotisivuilta löytyviä ohjeita varmistaakseen, että GDPR tulee huomioitua ilman ongelmia ja sanktioita.

5.3 Asiakkuuksien johtaminen

Asiakkuuksien johtaminen on tärkeä osa Yritys X:n liiketoimintaa, niin vanhoista asiakkaista huolehtiminen kuin myös uusien asiakkaiden hankkiminen. Huono asiakaskokemus leviää helposti ja sitä on vaikea korjata. Hyvä asiakaskokemus taas antaa asiakkaalle luotettavan kuvan yrityksestä ja luo pidempiä asiakassuhteita. Asiakkaan saama hyvä asiakaskokemus voi myös kantautua eteenpäin ja

luoda lisää uusia asiakkuuksia. Yritys X huolehtii jokaisesta vanhasta ja uudesta asiakkaastaan yrityskohtaisesti, jolloin asiakkaalla on tarvitsemansa palvelunsa yrityksen koosta riippumatta. (Yritys X:n edustaja 2018.)

Jotta asiakkuuksien johtamisessa onnistutaan hyvin, on yrityksen strategiassa tarkasteltava, kuinka asiakkuuksien johtaminen otetaan huomioon savuttaakseen yrityksen liiketoiminnan tavoitteet. Strategiassa asiakaskokemuksen parantaminen on hyvä osa asiakkuuksien johtamista. Kuten aikaisemmin mainitsin hyvän asiakaskokemukseen tuovan hyvän kuvan yrityksestä, vaikuttaa asiakaskokemukseen panostaminen positiivisesti yrityksen myyntiin ja uusien asiakkaiden hankintaan kertoo Sinisen Meteoriitin markkinointipäällikkö Jussi Vento kirjoituksessaan (2017, 10).

Yritys X:n hoitaessa asiakkaidensa taloushallintoa, pyörii sen toiminnasta suurin osa tilikausina. Hellman ja Värilä (2009, 80) kertovat kirjassaan ”Arvokas asiakas” taloushallintojen keräävän kulu- ja tulotapahtumia tilikaudelta ja sen loputtua kaikki nollataan ja aloitetaan uusi tilikausi. Asiakassuhteissa ei tilikauden jälkeen voida aloittaa asiakassuhdetta katsomalla alkutilanteesta uudestaan.

Koska asiakassuhteet jatkuvat myöskin tilikauden päättymisten jälkeen, on asiakkuuksien johtamisessa katsottava pitkällä tähtäimellä, eikä vain tilikausittain. GDPR koskee Yritys X:ää henkilötietojen käsittelijänä koko asiakassuhteen ajan ja myöhemmin vielä tarvittaessa. GDPR:n mukaan rekisteröityjen henkilötietoja on säilytettävä mahdollisimman vähän aikaa, ellei hyvästä syystä tietojen pidemmälle säilytykselle ole edellytystä, esimerkiksi kirjanpitolaki edellyttää kuuden vuoden säilytystä palkka tositteille. Säilytysajat voivat olla myös pidempiä, jos Yritys X sopii niin asiakkaan kanssa. Kirjanpidon arkistointi on Yritys X:llä aina erikseen asiakkaan kanssa sovittavissa. Osa yrityksistä haluaa itse arkistoida tositteensa, jolloin ne ovat vastuussa, että henkilötietoja ei loukata ja tietojen säilytys on oikeaoppisesti ja turvallisesti toteutettu. Laskujen, palkkalaskelmien ja tiliotteiden keskitetysti arkistointi sähköisesti säästää asiakkaiden ja tilitoimiston aikaa ja on myös turvallista GDPR kannalta katsottuna, kun tiedot eivät ole hajautetusti useammassa paikassa.

Asiakkuuksien johtamisessa GDPR:n huomioiminen on jokapäiväinen asia. Pelkästään työskentelytapojen ja työpisteen siisteyden pitäminen siinä kunnossa, että niistä ei paljastu ulkopuolisille rekisteröityjen tietoja, on tärkeää. Tietokoneen näytön suojaaminen ja varmistaminen, ettei työpisteessä ole näkyvissä tietoja ulkopuolisille, on hyvä keino estää mahdollisia tietoturvaloukkauksia. Näiden varmistamiseksi asiakasyritykset saattavat tehdä auditointeja, joissa heidän edustajansa käyvät tarkistamassa noudattaako yritys X heidän ohjeitaan henkilötietojen käsittelyssä. Asiakkuuksien johtamisessa on tärkeää pitää asiakaskeskeinen ajattelutapa ja muistaa, että asiakas on tärkein.

6 Tietosuoja-asetuksesta varmistettavat asiat

GDPR toi mukanaan monia tiukempia vaatimuksia henkilötietojen kaikenlaiseen käsittelyyn. Tietosuoja-asetuksen vaatimuksien täyttymistä tarkasteltaessa oli huomioitava siis mitä muutoksia tietosuoja-asetus toi Yritys X:n aikaisempiin henkilötietojen käsittelyperiaatteisiin. Muutosten tarkastelun jälkeen tehtiin tarvittavat muutokset, jotta Yritys X pystyy varmistamaan henkilötietojen oikeaoppisen käsittelyn. Jotta GDPR:n kanssa ei tulisi ongelmia ja pystyttäisiin välttämään asetuksen rikkomista ja siitä mahdollisesti tulevat sanktiot, on hyvä tehdä muistilista asioista, joita noudattamalla vältyttäisiin mahdollisilta ongelmilta. Jokaisen henkilötietoja käsittelevän yrityksen oli ennen tietosuoja-asetuksen voimaanastumista hyvä tehdä muistilista, jolla varmistaa kaikkien asetuksen henkilötietojen käsittelyä edellyttävien toimien täyttyminen.

Esimerkki muistilistasta on tekemäni liite 2. Listalta tärkeinä poimintoina pidän ensinnäkin sitä, yrityksen tietoturva on kunnossa, eli varmistetaan esimerkiksi riittävä virustorjunta ja salasanojen käyttö. Toinen muistettava asia on varmistaa, että henkilötietojen käsittelylle on oikea käsittelyperuste. Kolmas asia on selvittää, pitääkö yrityksen tehdä tietosuojaa koskeva vaikutusten arviointi. Vaikutusten arviointi on tehtävä muun muassa silloin, kun aluetta valvotaan kameroilla ja henkilötietojen käsittely koskee erityisiä henkilötietoryhmiä (Euroopan parlamentin ja neuvoston asetus 2016/679). Näiden asioiden selvittyä täytyi pohtia, pystytäänkö rekisteröityjen luonnollisten henkilöiden henkilötietoja luovuttamaan helposti ja ilman pitkää odotusta, asiakkaiden tietojaan pyytäessä. Onko tietojen poistaminen mahdollista, jos sitä pyydetään tai kun ei ole enää perusteltua syytä tietojen säilyttämiselle?

Tärkeintä kuitenkin on, että yrityksessä kaikki henkilötietoja käsittelevät henkilöt varmasti tietävät mikä luokitellaan henkilötiedoksi. Työntekijän on helppo miettiä itsestään mikä luokitellaan henkilötiedoksi, sillä kaikki tiedot, joiden avulla henkilö voidaan tunnistaa ovat henkilötietoa. Erityisesti palkanlaskennassa lähes kaikki tiedot, joita he rekisteröidystä käsittelevät ovat henkilötietoja muun muassa palkka, bonukset, tehtävä ja työsuhteen päättymissyy. Tietämällä mitkä tiedot ovat henkilötietoja on helpompaa käsitellä niin, ettei tietosuojarikkomusta tapahdu vahingossakaan.

Yritys X:llä otettiin GDPR:n myötä käyttöön muun muassa turvatulostus ja turvasähköposti arkaluontoisten tietojen tulostusta ja lähettämistä varten, esimerkiksi kun lähetään henkilötietoja sisältäviä viestejä. Näiden käyttö suojaa hyvin mahdollisilta tietoturvarikkomuksilta, mutta Yritys X:llä on hyvä varmistaa, että jokainen työntekijä tietää milloin täytyy sähköpostia lähettäessä käyttää turvasähköpostia ja milloin voi lähettää niin sanotusti normaalin sähköpostiviestin. Myös käytäntö, että tietokoneelta poistuttaessa kirjaudutaan aina ulos, vaikka tilassa olisi vain työkavereita tulisi olla käytössä jokaisella osastolla, jos ei vielä ollut. Vaikka nämä ovat yksinkertaisia asioita, ovat ne tärkeitä keinoja varmistaa henkilötietojen suojaaminen työntekijöiden jokapäiväisessä työssä. Yhteisten ohjeistusten noudattaminen on esimiehen vastuulla ja olisi myös hyvä muistuttaa henkilökuntaa näistä asioista aina tarvittaessa. Myös tietojen turhaa keräämistä ja säilyttämistä pitäisi välttää, eli jokaisen työntekijän täytyy tyhjentää tietokoneeltaan esimerkiksi työpöydältä kaikki henkilötietoja sisältävät tiedot, joille ei ole enää syytä säilytykseen.

Tietosuoja-asetuksen noudattamista voidaan parantaa jo tekemällä pieniä muutoksi kaikkien työntekijöiden jokapäiväisessä työssä. Tärkeätä on, että työntekijöille pidetään koulutuksia aiheista ja uudet työntekijät perehdytetään heti alussa toimimaan niin, että he noudattavat tietosuojaohjeistuksia henkilötietojen käsittelyssä. Jotta uudet työntekijät voivat noudattaa tietosuoja-asetusta oikein, on heidän muistettava ja ennen kaikkea tiedettävä mitkä tiedot ovat henkilötietoja. Tietosuoja-asetuksen vakavuutta ei voida korostaa liika, jonka vuoksi myös aiheesta on hyvä muistuttaa niin uusia kuin vanhoja työntekijöitä aina välillä.

7 POHDINTA

GDPR oli toukokuussa 2018 voimaanastuessaan hyvin pinnalla oleva aihe, josta ei voinut välttyä kuulemasta. Sähköpostit täyttyivät eri yritysten lähettämistä tietosuojaselosteista, joista suurin osa ei aiheuttanut erillisiä toimia vastaanottajalle. Monille nämä jokapäiväiset tiedotteet olivat ensimmäiset tiedot GDPR:stä. Vaikka usealle ihmiselle GDPR tuli tietoon vasta sähköpostiin saapuneiden viestien myötä oli yrityksissä työskennelty GDPR:n takia jo pidemmän aikaa ja mietitty saadaanko toiminta järjestettyä sellaiseksi, että voidaan todeta sen noudattavan GDPR:n vaatimuksia. Yritys X:ssä oltiin myös jo pitkään tehty paljon työtä, että 25.05.2018 kaikki olisi valmista asetuksen soveltamisen voimaan astuessa. Tilitoimistoissa tietojenkäsittely on aina ollut hyvin tarkkaa ja työntekijät ovat tehneet salassapitosopimukset, sillä he käsittelevät paljon arkaluonteisia materiaaleja, jotka eivät saa joutua ulkopuolisten saataville. Tämän vuoksi GDPR ei vaikuttanut Yritys X:n niin paljoa kuin esimerkiksi suoramarkkinointialan yritykseen, joka ei käsittele niin salaisia tietoja työssään. Nämäkin yritykset joutuvat nyt varmistamaan henkilötietojen käsittelyn olevan tietosuoja-asetuksen mukaista.

Työssä oli tavoitteena selvittää GDPR:n vaikutukset Yritys X:ään. Aiheen hyväksymisen jälkeen toimeksiantaja ei laatinut työlle tarkasti rajattuja ehtoja työn sisällöstä, vaan vastuu oli minulla. Lähdin aluksi tutustumaan toimeksiantajan suosituksesta artikkeleihin, jotka koskivat tietosuoja-asetusta, jonka jälkeen vasta siirryin lukemaan itse asetustekstiä. Työn tarkoitukseksi tuli tarkentaa, mitä vaikutuksia asetuksella oli Yritys X:n liiketoiminnan ja asiakkuuksien johtamisen kannalta katsottuna sekä mitä toimia GDPR vaatii ja miten se muutti toimintatapoja Yritys X:llä.

Vaikeuksia tuotti se että, tietosuoja-asetus oli vasta tullut voimaan, kun aloitin työn tekemisen ja siitä ei vielä ollut muuta tietoa saatavilla kuin asetusteksti ja muutamia asiantuntijakirjoituksia. Ajan kuluessa tietoa alkoi kuitenkin tulemaan lisää. Työn aloituksen aikaan ei ollut sattunut yhtäkään ennakkotapausta tietosuojaloukkauksesta, jota olisin voinut tutkia, mutta työn edetessä eräiden yhtiöiden harmiksi alkoi ennakkotapauksia tapahtumaan ja hallinnollisia sakkojakin jopa määrättiin. Työn kannalta tämä oli hyvä asia, sillä sain paremman perspek-

tiivin työhön, kun pystyin tutkimaan tapauksia tarkemmin ja kertomaan esimerkkien avulla sanktioista ja ennakkotapauksista. Ilman näitä tapauksia olisi tiedon hankkiminen ollut vielä hankalampaa.

Hain tietoa pääsääntöisesti internetistä, sillä GDPR:stä ei löytynyt juurikaan tietoa kirjoista. Internetistä käytin lähteinä tietosuoja-asetusta ja asiantuntijoiden kirjoituksia sekä lisäksi myös toimeksiantajalta ja heidän tietosuojavastaavalta saatua tietoa. Työssä haasteita toi myös aiheen rajaaminen ulkoistetun taloushallinnon asiakkaisiin. Tietoa oli tarjolla huomattavasti enemmän niille yrityksille, jotka suoramarkkinoivat ja myyvät kuluttajille, eivätkä yrityksille. Työssä on käytetty lähteinä paljon valvontaviranomaisten linjauksia ja asianajajien kirjoituksia, jonka vuoksi teoria on luotettavaa tietoa. Asetusteksti on kirjoitettu niin, että se ei ole helppolukuista, siksi tein opinnäytetyöhön paljon kuvioita ja esimerkkejä, jotta pystyin kertomaan käsittelemäni asiat lukijaystävällisesti.

Tammikuussa käyttöön tullut tulorekisteri toi työhön lisää pohdittavaa, sillä se kosketti palkkahallintoa merkittävästi, joka on myös Yritys X:n tarjoamista palveluista yksi eniten tietosuoja-asetusta koskettava. Koin siis tärkeäksi tarkastella työssä hieman, sitä miten tulorekisterin voimaanastumiseen myös GDPR vaikuttaa. Vaikka tulorekisteri on pakollinen valtion omistama palvelu, on yritysten määriteltävä sen käytön riskit GDPR:n kannalta, joka oli mielenkiintoinen asia.

Toinen paljon puhuttava aihe Brexit ja sen vaikutus GDPR:n kannalta katsottuna on hyvin ajankohtainen asia, jonka vaikutukset tulevat näkymään monissa EU:n alueella toimivissa yrityksissä. GDPR:n kannalta sopimukseton kova Brexit ja sen vaikutukset eivät ole vielä täysin tiedossa ja se voisi tuoda ongelmia datan vapaassa liikkumisessa ja henkilötietojen siirrosta Iso-Britanniasta EU:n alueelle. Iso-Britannian neuvoteltua lisäajasta Brexitille on sillä hyvät mahdollisuudet päästä sopimukseen ja välttää kova Brexit. Yrityksien kannalta sopimuksellinen ero EU:sta olisi parempi vaihtoehto ja pienentäisi myös GDPR:n kannalta tarkasteltuna riskejä henkilötietojen käsittelyssä.

Opinnäytetyössä päästiin tavoitteisiin ja ensimmäiset GDPR:n vaikutukset Yritys X:ään ulottuvat jo ennen GDPR:n soveltamisen voimaanastumiseen, sillä muun

muassa tietosuojasopimukset jouduttiin uusimaan niin asiakkaiden kuin ohjelmistojentoimittajien kanssa. Myös henkilökunnalle täytyi pitää koulutukset GDPR:stä ja henkilötietojen käsittelytapoja jouduttiin muuttamaan. Yritys X:n laajan henkilötietojen käsittelyn vuoksi täytyi tietosuojavastaava nimittää. Asiakkuuksien johtamisen kannalta tarkasteltuna GDPR:n toi mukanaan sen, että henkilötietojenkäsittelyjä auditointiin ja työntekijöiden työskentelytapoihin henkilötietojen kanssa ohjeistettiin tarkemmin asiakkaiden tietosuojasopimusten pohjalta. Isoja muutoksia muun muassa olivat turvatulostuksen ja turvasähköpostien käyttöönottaminen. GDPR:n soveltamisen voimaanastumisen myötä myös arkistointiin ja tietojen säilyttämiseen täytyy kiinnittää enemmän huomiota.

Työstä saatujen tulosten pohjalta pystytään todeta GDPR:n vaikuttaneen henkilötietojen käsittelyyn jokaisen Yritys X:n työntekijän työssä. Tietosuoja-asetus koskettaa yritystä monelta osalta ja siksi se on tärkeä osa strategiaa. GDPR pitää ottaa huomioon vakuutuksissa, jo pelkästään mahdollisten sakkojen vuoksi, mutta myös maineen kannalta katsottuna ja tietenkin myös asiakkuuksien johtamisessa. Yrityksen strategiassa GDPR:n huomioiminen näkyy vahvasti, kun mietitään riskien pienentämistä. Tärkeintä on, että tulosten pohjalta Yritys X pystyy kehittämään henkilötietojen käsittelyä yhä paremmaksi asiakkuuksien johtamisen ja yrityksen liiketoiminnan kannalta tarkasteltuna osana yrityksen strategiaa.

Tein myös liitteeksi kaksi kaavaketta, jotka ovat tietoturvaloukkauksesta ilmoittaminen ja muistilista GDPR:n vaatimista toimenpiteistä. Tietoturvaloukkauksesta ilmoittamisen kaavakkeesta on hyötyä työntekijöille, mutta sitä voidaan käyttää esimerkiksi Yritys X:n konsultoidessa uutta aloittavaa yritystä, kuten myös muistilistaa. Jatkotutkimusaiheena työlle ehdottaisin tietosuoja-asetuksen asiakassuhteisiin vaikutuksen mittaaminen. Tutkimuksesta saatujen tulosten pohjalta olisi mahdollista toteuttaa strategiassa uusia keinoja asiakastyytyväisyyden parantamiseen. Tutkimus olisi mahdollista toteuttaa opinnäytetyöni pohjalta, jolloin voitaisiin keskittyä ainoastaan vaikutusten mittaamiseen ja asiakastyytyväisyyden parantamiseen. Asiakastyytyväisyyttä halutaan aina parantaa ja sen vuoksi olisi sitä hyvä mitata myös uudelta näkökulmalta katsottuna.

LÄHTEET

Aitta & Matinpalo. 2019. Deloitte. Tulorekisteri + GDPR alle 5 minuutissa. Luettu 15.2.2019. https://www2.deloitte.com/fi/fi/pages/risk/articles/tulorekisteri-ja-gdpr-alle-viidessa-minuutissa.html

Alma Talent Pro. 2019. Ranskan tietosuojaviranomainen määräsi 50 miljoonan sakon Googlelle. Luettu 30.1.2019. https://pro.almatalent.fi/article/ranskan-tieto-suojaviranomainen-maarasi-50-miljoonan-sakon-googlelle/8484

Andreasson, Koivisto ja Ylipartanen. 2013. Tietosuojavastaavan käsikirja. Helsinki: Tietosanoma Oy.

Case & Heinonen. n.d. GDPR-sakot ovat vakuutettavissa ainoastaan Suomessa ja Norjassa kaikista Euroopan maista. Luettu 10.3.2019. https://www.aon.com/finland/kirjasto/suomessa-GDPR-sakot-vakuutetta-vissa.jsp

Bergström, Karhula & Kipinoinen. 2018. Eduskunta. EU:n tietosuojauudistuksen kansallinen täytäntöönpano. Luettu 26.10.2019. https://www.eduskunta.fi/FI/tie-toaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuo-jauudistus.aspx

Call To Action. n.d. Markkinoinnin automaatio ja EU:n tietosuoja-asetus (GDPR). Luettu 8.1.2019. https://calltoaction.fi/markkinoinnin-automaatio-ja-eun-tietosuoja-asetus-gdpr/

Cyrus Farivar. 2019. Ars Technica. Google must pay €50 million for GDPR violations, France says. Luettu 3.2.2019. https://arstechnica.com/tech-policy/2019/01/google-fined-57m-after-france-finds-violations-of-new-eu-privacy-law/

European commision. n.d. Adequacy of the protection of personal data in non-EU countries. Luettu 26.3.2019. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Euroopan parlamentin ja neuvoston asetus 2016/679. http://www.privacy-regulation.eu/fi/

GDPR.fi. n.d. EU:n Tietosuoja-asetus – sanasto. Luettu 10.10.2018. https://gdpr.fi/sanasto/

Heikinmäki A. 2017. Mikä on pilvipalvelu ja mitä hyötyä siitä on minulle? Luettu 10.10.2019. http://www.controla.fi/blogi/mika-on-pilvipalvelu-ja-mita-hyotya-siita-on-minulle

Heikkilä M. Karismo A. Kokkonen Y. STT-YLE. Töyrylä K. 2019. Brexitille jatkoaikaa lokakuun loppuun saakka, Tusk: "Älkää tuhlatko tätä aikaa" – Yle seurasi huippukokousta. Luettu 12.4.2019. https://yle.fi/uutiset/3-10731365

Hellman & Värilä. 2009. Arvokas asiakas. Talentum.

Henkilötietolaki 22.4.1999/523

HS-AFP. 2019. Ranska määräsi Googlelle 50 miljoonan euron sakot epämääräisten käyttöehtojen takia – perusteena ensi kertaa EU:n tietosuoja-asetus. Luettu 30.1.2019. https://www.hs.fi/ulkomaat/art-2000005973170.html

Holopainen P. 2018 Yrittäjän tietosuojaopas. Tulostettu 10.10.2018. www.yrittajat.fi/yrtittajan_tietosuojaopas

Karjalainen K. 2017. Mikä on GDPR – vinkit henkilöstöhallinnolle GDPR-vaatimusten täyttämiseen. Luettu 25.11.2018. https://www.sympa.com/fi/blogi/mika-on-gdpr/

Kirjanpitolaki 30.12.1997/1336

Laitila T. 2019. TIVI. Ranska läimäisi ensimmäisen kymmenien miljoonien gdpr-sakon – kyseenalainen kunnia osui Googlelle. Luettu 3.2.2019. https://www.tivi.fi/Kaikki_uutiset/ranska-laimaisi-ensimmaisen-kymmenien-miljoonien-gdpr-sakon-kyseenalainen-kunnia-osui-googlelle-6755819

Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta 27.5.1994/389.

Löytänä & Kortesuo. 2011. Asiakaskokemus – Palvelubisneksestä kokemusbisnekseen. Talentum.

Mattila J. 2018. Suomessa ryhdytään tekemään GDPR-tarkastuksia, kun Ruotsissa annetaan jo ensimmäisiä tuomioita. Luettu 27.12.2018. https://www.ts.fi/uutiset/kotimaa/4117122/Suomessa+ryhdytaan+tekemaan+GDPRtarkastuksia+kun+Ruotsissa+annetaan+jo+ensimmaisia+tuomioita

Maunu M. 2017. GDPR-muistilista ja peruskäsitteet: näin valmistaudut tulevaan EU:n tietosuoja-asetukseen. Luettu 14.11.2018. https://www.liana-tech.fi/blogi/gdpr-muistilista-ja-peruskasitteet-nain-valmistaudut-tulevaan-eun-tietosuoja-asetukseen.html

OpiTietosuojaa.fi. 2016. Yleistä Tietosuojasta. Luettu 16.4.2019. https://opitietosuojaa.fi/fi/aloitus/tietosuoja

Puustjärvi P. 2018. Brexit ja GDPR: Iso-Britanniako GDPR-mallioppilas? Luettu 3.4.2019. https://fondia.com/fi/blogsandnews/brexit-ja-gdpr-iso-britanniako-gdpr-mallioppilas

Räty J. 2018. Talousverkko. Yrittäjä, tulorekisteri tulee – mitä se tarkoittaa sinulle? Luettu 7.2.2019. https://www.talousverkko.fi/tulorekisteri-tulee-oletko-valmis/

Taloushallintoliitto. n.d. Tilitoimiston johtaminen ja henkilöstö. Luettu 4.12.2018. https://taloushallintoliitto.fi/laatu-tyokalut/tilitoimiston-ohjeet-ja-tyokalut/tilitoimiston-johtaminen-ja-henkilosto

Tietosuojamalli. 2017. Hallinnollisten sakkojen määräämisen yleiset edellytykset. Luettu 31.1.2019. https://fakta.tietosuojamalli.fi/gdpr-asetus/83-hallinnollisten-sakkojen-maaraamisen-yleiset-edellytykset

Tietosuojamalli. 2017. Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle. Luettu 10.1.2019. https://fakta.tietosuojamalli.fi/gdpr-asetus/34-henkilotietojen-tietoturvaloukkauksesta-ilmoittaminen-rekisteroidylle

Tietosuojavaltuutetun toimisto. n.d. Rekisteröidyn oikeudet. Luettu 22.10.2018. https://tietosuoja.fi/rekisteroidyn-oikeudet

Tietosuojavaltuutetun toimisto. n.d. Tietosuojavaltuutetun toimisto. Luettu 26.10.2018. https://tietosuoja.fi/tietosuojavaltuutetun-toimisto

Tietosuojavaltuutetun toimisto. n.d. Tietosuojavastaavat. Luettu 4.12.2019. https://tietosuoja.fi/tietosuojavastaavat

Tietosuojavaltuutetun toimisto. n.d. Tietoturvaloukkaukset. Luettu 03.01.2019. https://tietosuoja.fi/tietoturvaloukkaukset

Tilastokeskus. n.d. Käsitteet. Luettu 22.3.2019. https://www.stat.fi/meta/kas/pk_yritys.html

Tietoturvaloukkaus.fi. 2018. Tietoturvaloukkaus on usein vaikeasti havaittava tietomurto. Luettu 18.4.2019. https://www.tietoturvaloukkaus.fi/

Valo J. 2019. Brexit ja henkilötietojen siirto Iso-Britanniaan. Luettu 3.4.2019. https://www.secrays.com/tietosuojapalvelut/brexit-henkilotiedot/

Vento J. 2017 Erinomaisen asiakaskokemuksen kaksi kivijalkaa. Luettu 14.1.2019. https://www.meteoriitti.com/2017/10/20/asiakaskokemuksen-kaksi-kivijalkaa/

Verohallinto. 2018. Tulorekisteriin ilmoittamisen kanavat. Luettu 15.2.2019. https://www.vero.fi/tulorekisteri/yritykset-ja-organisaatiot/suorituksen-maksajat/ilmoittamisen-kanavat/

Virtanen Jarmo. 2018. Kohun silmässä ollut Trafi avaa osan asiointipalveluistaan lauantaina. Luettu 4.1.2019. https://yle.fi/uutiset/3-10555891

Virtanen Jori. 2018. Saksa ehti ensimmäisenä – gdpr-päätös napsahti, tärkeä ennakkotapaus. Luettu 28.12.2018. https://www.tivi.fi/Kaikki_uutiset/saksa-ehti-ensimmaisena-gdpr-paatos-napsahti-tarkea-ennakkotapaus-6732521

Yritys X:n edustaja. 2018. Sähköpostiviestit toni.tahka@tuni.fi

Yritys X:n kotisivut. 2018

LIITTEET

Liite 1. Tietosuojaloukkaus ilmoitus

Ilmoitus tietosuojaloukkauksesta Päivämäärä (pp.kk.vvvv) _____

Yrityksen nimi _____
Y-tunnus _____
Yrityksen osoite _____

Yhteyshenkilön tiedot (tietosuojavastaava)
Nimi _____
Puhelinnumero _____
Sähköposti _____
Postiosoite _____

Tietosuojaloukkauksen havaitsemisaika _____
Loukkaus alkanut _____
Loukkaus loppunut _____
Kuvaus miten tietosuojaloukkaus havaittiin

Kuvaus tietosuojaloukkauksesta (mitä tapahtunut ja loukkaus koskee)

Kuvaus tietosuojaloukkauksen todennäköisistä seurauksista

Toimenpiteet ennen tietosuojaloukkausta

Toimenpiteet loukkauksen tultua tietoon

Liite 2. Muistilista GDPR:n vaatimista toimenpiteistä

Muistilista	Kyllä	Ei
1. Tietosuoja-asetuksen mukainen oikeutettu käsittelyperuste henkilötietoja varten		
2. Seloste käsitttelytoimista tarvittaessa		
3. Dokumentointi rekisteröidyille tehdyistä ilmoituksista (henkilötietojen käsittelystä, keräilystä ja luovuttamisesta)		
4. Sopimukset henkilötietojen käsittelyn ulkoistamisesta ja tiedonsiirrosta		
5. Tarvitaanko tietosuojavastaava		
6. Täytyykö tehdä vaikutusten arviointi		
7.Tietoturvaloukkaukseta kertomiseen valmistautuminen tietosuojavaltuutetun toimistolle ja		
8. Rekisteröityjen oikeuksien toteuttamisen mahdollisuus (esim. tietojen kysely ja siirto)		