LAPIN AMK
Lapland University of Applied Sciences

VALMISTAUTUMINEN EU: N YLEISEEN TIETOSUOJA-ASETUKSEEN

Case: Profin Oy

Terhi Keränen

Opinnäytetyö
Kauppa, hallinto ja oikeustieteet
Liiketalouden koulutusohjelma
Tradenomi (AMK)

2018

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Kauppa, hallinto ja oikeustieteet
Liiketalouden koulutusohjelma
Tradenomi (AMK)

Tekijä Terhi Keränen Vuosi 2018
Ohjaaja(t) Satu Valli
Toimeksiantaja Profin Oy
Työn nimi Valmistautuminen EU:n yleiseen tietosuoja-asetukseen
Sivu- ja liitesivumäärä 42 + 4

EU:n yleistä tietosuoja-asetusta sovelletaan 25.5.2018 alkaen kaikissa EU:n jäsenmaissa ja sen tavoitteena on vahvistaa yksilön oikeuksia ja vapauksia sekä lujittaa Euroopan sisämarkkinoita. Samalla tietosuojaan liittyvää valvontaa vahvistetaan ja huomioidaan myös tietosuojan globaalinen kehitys. Tietosuoja-asetus koskee lähtökohtaisesti kaikkea henkilötietojen käsittelyä ja se tuo mukanaan myös uusia velvollisuuksia organisaatioille.

Opinnäytetyön tavoitteena oli tutkia EU:n tietosuoja-asetuksen sisältöä ja sen perusteella auttaa toimeksiantaja yritystä valmistautumaan asetuksen voimaantuloon. Kerätyn tiedon pohjalta tavoitteena oli luoda tarvittavia dokumentteja koskien henkilötietojen käsittelyä yrityksessä. Opinnäytetyö on tehty kehittämistutkimuksena, jossa on käytetty laadullista tutkimusotetta sekä käytännön havainnointia yrityksen henkilötietojen käsittelystä.

Teoriaosuudessa käsitellään EU:n tietosuoja-asetuksen keskeistä sisältöä. Tutkimusaineisto on koottu monipuolisesti useista eri lähteistä ja tiedon keruussa on huomioitu tutkimuksen tekeminen toimeksiantona yritykselle. Tutkimuksen tuloksena toimeksiantaja yritykselle luotiin useita dokumentteja, joista suurin osa jää vain yrityksen yksityiseen käyttöön, eivätkä ne näin ole julkistettavia.

Avainsanat EU-oikeus, tietosuoja, yksilönsuoja, henkilötiedot

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

School of Business and Culture
Degree Programme in Business Administration
Bachelor of Business Administration

Author	Terhi Keränen	Year	2018
Supervisor	Satu Valli		
Commissioned by	Profin Oy		
Subject of thesis	Preparing for the EU's General Data Protection Regulation		
Number of pages	42 + 4		

The EU's general data protection regulation will be enforced from 25 May 2018 in all EU member states with the aim of strengthening individual rights and freedoms and strengthening the European internal market. At the same time, data protection control is strengthened and also took into account the global development of data protection. The Data Protection Regulation applies, in principle, to all processing of personal data and also entails new responsibilities for organizations.

The purpose of the thesis was to examine the content of the EU Privacy Regulation and help the commissioner to prepare for the enforcement into force of the regulation. Based on the collected data, the aim was to create the necessary documents regarding the processing of personal data in the company. The thesis has been developed as a development study using qualitative research material and practical observation on the processing of company's personal data.

The theoretical part looks at the core content of the EU Data Protection Regulation. The research material has been compiled from a wide range of sources and the research has considered the commissioning of this research as an assignment for the company. As a result of the research, several documents were created for the client company, most of which remained only for the private use of the company and were not publicly available

Key words EU law, data protection, personal data

SISÄLLYS

1 JOHDANTO

Tietosuojan historian voidaan katsoa ulottuvan 2500 vuoden taakse Hippokrateen valaan, jonka tarkoituksena on velvoittaa potilassuhteen suojaaminen. Tähän päivään mennessä kehitys on käynyt läpi monia vaiheita niin 1700- luvun suurista vallankumouksista joukkotiedotusvälineiden kehittymiseen 1800-luvun loppupuolella kuin myös II-maailmansodan henkilörekisterien väärinkäytön kautta 1960-luvulla tapahtuneeseen IT-teknologian kehittymiseen. Suomessa ensimmäinen henkilötietojen käsittelyn yleislaki tuli voimaan 1. tammikuuta 1988. EU:n henkilötietodirektiivi (95/46/95) vuodelta 1995, saatettiin voimaan myös Suomessa tälläkin hetkellä käytössä olevalla henkilötietolailla (523/1999) 1. kesäkuuta 1999. (Andreasson, Koivisto & Ylipartanen 2014, 47–49.)

Tänä päivänä yhä nopeampaan kehittyvä teknologia ja globalisaatio tuovat mukanaan uusia haasteita henkilötietojen käsittelyn suojelemiseen. Uutisvirrasta saamme lukea harva se viikko palvelunestohyökkäyksistä, haittaohjelmista, internetiin vuotaneista henkilötiedoista, kadulta löytyneistä henkilötietoja sisältävistä papereista sekä monista muista tietosuojaan liittyvistä epäkohdista. Annamme henkilötietoja itse tietoisesti muun muassa käyttämällä sosiaalista mediaa, tilaamalla tuotteita niin internetistä kuin myös ostamalla niin sanotuista kivijalkakaupoista. Meistä voidaan myös kerätä tietämättämme tietoja ja niitä voidaan myös myydä eteenpäin esimerkiksi suoramarkkinointia varten.

EU:n yleinen tietosuoja-asetus, josta käytetään myös lyhennettä GDPR (General Data Protection Regulation) hyväksyttiin keväällä 2016 ja se on velvoittava 25.5.2018 alkaen kaikissa EU-maissa. Tapahtuneen kehityksen myötä Euroopan unionissa tarvitaan entistä vahvemmat ja johdonmukaisemmat raamit tietosuojalle. Uudistuksen tavoitteena on vahvistaa yksilön oikeuksia ja vapauksia mutta myös lujittaa Euroopan sisämarkkinoita, huomioida tietosuojan globaali ulottuvuus sekä myös tehostaa tietosuojaan liittyvää valvontaa. Monet asetuksen mukaiset vaatimukset ovat jo olemassa nykyisessä lainsäädännössä, mutta mukana on myös tarkennuksia ja uudistuksia sekä velvollisuuksia, jotka tulee huomioida kaikilla henkilötietoja käsittelevillä organisaatioilla (Opi tietosuojaa 2018a; Tietosuojavaltuutetun toimisto 2018a.) Tämä tuo väistämättä myös lisätyötä kaikkiin

näihin organisaatioihin, jotta asetuksen voimaantullessa sen velvoitteet olisivat täyttyneet.

1.1 Toimeksiantajan esittely

Opinnäytetyön toimeksiantaja on Pohjois-Pohjanmaalla toimiva lasiliukuovia valmistava Profin Oy. Kyseessä on pohjoissuomalainen perheyritys, jonka tarina on alkanut vuonna 1977. Yrityksessä tehtiin omistajanvaihdos vuonna 2012, jolloin Profin Oy:n perustajat Pirjo ja Martti Haapala siirsivät yrityksen omistajuuden Martin veljenpojalle Mikko Haapalalle. Yrityksen tuotanto sekä tehtaan toimisto sijaitsevat Pudasjärvellä ja hallinnon ja markkinoinnin toimisto Oulussa. Moderni teknologia ja perinteiset puusepäntaidot yhdistyvät Profinin tuotteissa, joita menee sekä talotehtaille että rakennusteollisuuden projektikohteisiin. Profin Oy:n tytäryhtiö, Sydänpuu ikkunat ja ovet Oy, on erikoistunut yksilöllisten ikkunoiden ja ovien suunnitteluun ja valmistukseen, joita tarvitaan vaativissa rakennuskohteissa ja arvorakennuksissa. Tuotannon työntekijöitä Profin Oy:ssä on tällä hetkellä 24 ja vakituisia toimihenkilöitä 13. (Lantto 2018; Lehtola 2018; Rakennuslehti 7.11.2013; Profin Oy 2017; Profin Oy 2018.)

1.2 Tutkimuksen tavoitteet ja rajaus

Tutkimuksen tavoitteena on selvittää yrityksen nykyiset käytännöt henkilötietojen käsittelystä sekä perehtyä EU:n tietosuoja-asetukseen. Tämän kerätyn tietopohjan perusteella päätavoitteena opinnäytetyössä on auttaa yritystä valmistautumaan EU:n tietosuojauudistuksen voimaantuloon sekä tehdä yritykselle tarvittavaa dokumentaatiota tietosuojaan liittyen. Tietosuoja huomioidaan myös opinnäytetyötä tehdessä ja julkaistaessa, sillä osa dokumentaatiosta on tarkoitettu vain yrityksen omaan sisäiseen käyttöön, joten niitä käsitellään tässä työssä mahdollisimman yleisellä tasolla eikä kaikkia yksityiskohtia aineistosta tuoda julki. Opinnäytetyön yhteydessä yritykselle luotavaa aineistoa ovat tietosuojaopas, tietosuojasuunnitelma, rekisteri- ja tietosuojaselosteet, taulukko tietoturvaloukkausten kirjaamiseksi sekä seloste käsittelytoimista. Vaikka tutkimus tehdään toimeksiantona yhdelle yritykselle ja käsiteltävät henkilötiedot sekä tavat vaihtelevat yrityksissä, niin opinnäytetyön ajatuksena on myös tuottaa sellaista pohjatietoa,

joka auttaa ymmärtämään tietosuojauudistusta kokonaisuutena ja sen vaikutuksia yrityksen käytänteisiin. Opinnäytetyöstä on toivottavasti hyötyä myös opiskelijoille, jotka mahdollisesti tulevassa työssään asian kanssa ovat tekemisissä sekä jo työelämässä oleville ammattilaisille, jotka kaipaavat tiivistettyä tietoa asiasta.

Työ rajattiin koskemaan Profin Oy:n henkilötietojen käsittelyä, eli yrityksen tytäryhtiössä valmistautuminen tietosuoja-asetukseen tehdään omana itsenäisenä työnään. Tietosuoja-asetus on varsin laaja kokonaisuus, ja työstä rajattiin pois yrityksen sopimukset henkilötietojen käsittelijöiden kanssa niin, että työssäni tuon esille vain teoriatasolla yleisesti asetuksen mukanaan tuomia muutoksia koskien tietojenkäsittelyn huomioimista yritysten välisissä sopimuksissa. Profin Oy on ulkoistanut yrityksen IT-tuen, jonka tehtäviin kuuluu muun muassa teknisen suojauksen hoitaminen koskien myös henkilötietojen käsittelyä, ja tietotekninen puoli ei myöskään suoranaisesti liity liiketalouden koulutusohjelmaan, joten senkin vuoksi teknisen puolen käsittely on pitkälti rajattu pois työstä.

Toimeksiantoyrityksen tarpeiden ja tutkimuksen rajausten myötä tutkimuskysymyksiä ovat:

- Mitä EU:n tietosuoja-asetuksen voimaantulo käytännössä tarkoittaa toimeksiantajayrityksen toiminnassa?
- Millainen nykykäytäntö yrityksen henkilötietojen käsittelyssä on?
- Kuinka tietosuoja huomioidaan yrityksessä tällä hetkellä?
- Mitkä ovat EU:n tietosuoja-asetuksen keskeisimmät mukanaan tuomat muutokset?
- Mitkä ovat yrityksen velvollisuudet asetuksen voimaantulon jälkeen?

1.3 Tutkimusmenetelmä

Kvalitatiivisen eli laadullisen tutkimuksen tavoitteena on tutkittavan ilmiön kuvaaminen, ymmärtäminen ja tulkinnan antaminen, eli tarkoituksena on pyrkiä ymmärtämään ilmiö perusteellisesti, eikä asioita pyritä myöskään yleistämään

kuten kvantitatiivisella eli määrällisellä tutkimuksella. Laadullisella tutkimusmenetelmällä myös tutkitaan ennemmin yksittäistä tapausta kuin suurempaa joukkoa, kuten määrällisellä tutkimuksella tehdään. Laadullisessa menetelmässä tutkimusprosessi ei ole suinkaan suoraviivainen vaan aineistoa kerätään jaksottaisesti eikä tutkimuksen alussa voida määritellä tarkasti etukäteen kerättävän aineiston määrää ja sitä, mitä tietoa tullaan keräämään vaan aineistoa tulee kerätä riittävästi niin, että tutkija ymmärtää ilmiön sekä tutkimusongelma ratkeaa. Kerättyä aineistoa on syytä analysoida koko ajan, jolloin tutkijan ymmärrys ilmiöön kasvaa ja samalla teemahaastattelujen myötä esille voi nousta uusia kysymyksiä, joita on hyvä huomioida seuraavia haastatteluja tehdessä tai palata aiheeseen jo haastatellun kanssa. Aineisto on hyvä käydä läpi useamman kerran ja sitä pitäisi pyrkiä katsomaan tutkimusongelman kannalta niin, että lopputuloksena on mahdollisimman hyvä tulkinta, jonka avulla luodaan kuvaus ilmiöstä. (Kananen 2013, 106–107; 2014, 16–19.)

Kanasen (2012, 13, 35–38, 42–43) mukaan kehittämistutkimuksen taustalla on jokin ilmiö, prosessi tai asiantila, jonka halutaan olevan paremmin kehittämisen tai muutoksen jälkeen, ja näin kehittämisen kohteesta voidaan muodostaa ongelma, josta saadaan tutkimuskysymys. Tiedonkeruumenetelmät ovat kehittämistutkimuksessa monipuolisia. ja tutkimusaineistona toimivat muun muassa arkistot, haastattelut ja havainnot. Sekä laadullinen että määrällinen tutkimus ovat toteavia, eli asiat ovat niin kuin tutkimuksessa on tulokseksi saatu ja sellaiseksi tutkimus myös jää. Sen sijaan toiminta- ja kehittämistutkimuksissa pyrkimyksenä on asiantilojen muutos, eli yksistään toteaminen ei riitä, vaan niihin liittyy muutos tai kehittäminen ja sen läpivieminen. Syy-seurausyhteyksien ymmärtäminen on tutkijalle tärkeää, jotta muutos saadaan aikaiseksi, ja tämä voi olla myös haastava tehtävä. Kehittämistutkimuksen tarkoituksena ei ole tuottaa pelkästään tekstiä vaan käytännössä toimivia ratkaisuja, ja toimintatutkimuksessa tutkija itse on mukana kokeilemassa sitä, kuinka ratkaisu toimii. Tutkimustulosta ei voida suoranaisesti sellaisenaan siirtää vastaavaan asiayhteyteen koska tulos edellyttää muutosprosessia. Muutoksen vaatimien toimenpiteiden ja asiayhteyksien huomioimisella tuloksia voidaan kuitenkin hyödyntää myös toisaalla vastaavanlaisissa tapauksissa, jolloin jo tehtyjä virheitä voi olla helpompi välttää.

Case-tutkimuksella ei ole varsinaisesti omia analyysimenetelmiä, koska se pohjautuu pitkälti laadulliseen tutkimusmenetelmään. Sisältöanalyysissä aineisto ensin hajotetaan ja luokitellaan omiksi asiasisällöikseen, jonka jälkeen tutkija muodostaa näistä johtopäätöksiä, joiden pohjalta luodaan ilmiöstä hyvä kuvaus. Luokittelussa voidaan käyttää teoria- tai aineistolähtöistä luokittelua tai niiden yhdistelmää. Luokittelulla pyritään helpottamaan tulkintaa, jotta ilmiöstä saataisiin hyvä ja systemaattinen kuvaus käytettävissä olevan aineiston perusteella. Tarkoituksena sisältöanalyysillä on löytää käytettävissä olevan materiaalin ydin ja tehdä sen pohjalta tiivistetty kuvaus. Kerätty aineisto, josta analyysi on tehtävä, voi koostua esimerkiksi teemahaastatteluista, raporteista ja keskusteluista. (Kananen 2012, 116; 2013, 103–105.)

Yrityksen henkilötietoja käsitteleviä henkilöitä toimii eri paikoissa, joten kasvokkain haastattelu ei onnistu kaikkien kanssa, ja näin ollen sähköpostilla tehdyt kyselyt ovat aineiston keruun kannalta tärkeitä. Haastateltava voi vastata kyselyyn sellaisena ajankohtana, mikä hänen työaikaansa parhaiten sopii, ja samalla vastaukset tulevat myös kirjattua kirjalliseen muotoon, jolloin se helpottaa omaa työskentelyäni eikä esimerkiksi nauhoitteiden litterointia tarvitse näin tehdä, ja samalla annetut tiedot on helppo tarkistaa sähköpostista sekä tallettaa tai tulostaa mahdollista myöhempää tarkastelua varten. Tarvittaessa ja mahdollisuuksien mukaan keskusteluja käydään myös kasvokkain. Koska yrityksessä työskentelevät toimihenkilöt tekevät eri työtehtäviä ja voivat näin käsitellä eri henkilötietoja eri tavalla tai eri järjestelmien kautta, ei yhden yhtenäisen kyselylomakkeen luominen kaikille ole mahdollista vaan kysymykset tulee soveltaa kulloisenkin käsiteltävän aineiston mukaisesti. Tutkimuksen edetessä voi esille tulla myös seikkoja, joihin on tarvetta tehdä lisäkysymyksiä tai tarkennuksia. Opinnäytetyö sopii hyvin juurikin kehittämistutkimukseksi, sillä työn avulla on tarkoitus kehittää toimeksiantoyrityksen tietosuojaa henkilötietojen käsittelyn osalta vastaamaan EU:n tietosuoja-asetuksen mukanaan tuomia vaatimuksia. Menetelmänä työssä on lähinnä kvalitatiivinen eli laadullinen tutkimusote, sillä se sopii parhaiten tiedonkeruuseen ja analysointiin, mutta mukana on paljon myös omaan havainnointiin, arkistoihin tutustumiseen ja muihin mahdollisiin dokumentteihin liittyvä käytännön tutkimusta.

1.4 Luotettavuus

Kehittämistutkimuksessa on haasteellista tehdä luotettavuustutkimusta, sillä se ei ole oma tutkimusotteensa. Kehittämistutkimuksessa on tarpeen mukaan koottu sekä laadullista että määrällistä tutkimusta sopivana kokonaisuutena niin, että tutkimusongelma saadaan ratkaistua. Mikäli työssä käytetään laadullista tutkimusotetta, tulee siinä silloin käytännössä myös soveltaa kriteeristöä, jota laadullisessa tutkimuksessa käytetään. (Kananen 2015, 111.)

Tutkimuksen uskottavuutta ja reliabiliteettia vahvistetaan sillä, että tutkimuksessa esitetty aineisto on esitetty sellaisessa muodossa, jonka päättelyketju on myös muiden tarkistettavissa (Kananen 2012, 35). Laadullisen tutkimuksen luotettavuuden arviointi edellyttää riittävää dokumentaatiota opinnäytetyöllä. Perustelut tehdyistä valinnoista ovat tärkeitä, sillä niiden avulla kirjoittaja voi näyttää harkinneensa eri vaihtoehtoja ja päätyneensä esittämäänsä, samalla perustelut tuovat tehdylle työlle myös uskottavuutta. Dokumentaatio on myös edellytyksenä ratkaisun ja tulosten jäljentämiseen ja aineisto on syytä säilyttää tarvittavaa todentamista varten. Aineiston ja tutkimuksen tulosten paikkansapitävyyden vahvistamiseksi on yksinkertaisinta luetuttaa aineisto ja siitä tehty tulkinta henkilöllä tai henkilöillä, jotka ovat olleet tietolähteinä ja joita tutkimus koskee. (Kananen 2015, 112–113.)

2 TIETOSUOJA

Tietosuojalla tarkoitetaan yksinkertaisimmillaan luonnollisen henkilön yksityisyyden, oikeuksien ja vapauksien turvaamista. Käytännössä henkilötietoja tulee siis käsitellä oikein, ja niitä on suojattava luvattomalta käytöltä sekä sellaiselta käsittelyltä, johon niitä ei alun perin ole tarkoitettu. Tietosuoja voidaan joskus sekoittaa osin tietoturvaan, jolla tarkoitetaan sellaisia teknisiä ja hallinnollisia toimenpiteitä, joiden tarkoituksena on turvata tietosuojan tarkoittamat rekisteröidyn oikeudet ja vapaudet. (Opi Tietosuojaa 2018b.)

Suomessa tietosuojan yleissääntely perustuu tällä hetkellä henkilötietolakiin (523/1999) (Andreasson, Koivisto & Ylipartanen 2014, 17). Henkilötietojen käsittelyyn ja tietojen säilytysaikoihin vaikuttavat myös monet muut lait kuten muun muassa kirjanpitolaki, arkistolaki, työaikalaki ja laki yksityisyyden suojasta työelämässä. Henkilötietojen käsittelyyn liittyvää lainsäädäntöä on myös Suomen perustuslaissa (731/1999), jonka 2. luvussa käsitellään yksityiselämän suojaa ja luottamuksellisen viestin salaisuutta sekä viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuutta. (Opi Tietosuojaa 2018b.)

EU:n yleisen tietosuoja-asetuksen lopullinen sisältö hyväksyttiin keväällä 2016, ja sen jälkeen alkoi kahden vuoden siirtymävaihe, jonka aikana organisaatioiden tulee saattaa henkilötietojensa käsittely asetuksen vaatimusten mukaiseksi 25.5.2018 mennessä. EU:n yleinen tietosuoja-asetus oli yksi Euroopan parlamentin istuntokauden tärkeimmistä lainsäädäntöhankkeista, ja lähtökohtaisesti se koskee kaikkea henkilötietojen käsittelyä EU:n jäsenvaltioissa, ja samalla sen myötä eri maiden käytännöt tietosuojasäännöksissä yhdenmukaistuvat. Asetus mahdollistaa kuitenkin joiltain osin niin sanotun kansallisen liikkumavaran, eli jäsenvaltioissa voidaan säätää tarkennuksia kansallisella lainsäädännöllä. (Opi Tietosuojaa 2018a.)

Oikeusministeriön (2018) tiedotteen mukaan hallitus esittää uuden tietosuojalain säätämistä, joka olisi Suomessa henkilötietojen käsittelyä koskeva yleislaki. Tietosuojalaki tulisi voimaan yhtä aikaa EU:n tietosuoja-asetuksen soveltamisen kanssa, ja samalla kumottaisiin sekä nykyinen henkilötietolaki että laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Tietosuojalain mukaisesti Suomessa

esimerkiksi tietoyhteiskunnan palvelujen ikäraja olisi 13 vuotta, kun se yleisessä tietosuoja-asetuksessa on säädetty 16 ikävuoteen. Tällä kansallisella lainsäädännöllä tulisi säädettäväksi myös muita poikkeuksia tai vapauksia silloin, kun kyseessä on tietojen käsittely sananvapauden, tutkimuksen ja arkistoinnin turvaamiseksi.

2.1 Henkilötietojen käsittely

Tietosuoja-asetusta sovelletaan käytännössä aina, kun henkilötietoja käsitellään yrityksen tietojärjestelmissä, ja myös manuaalisen aineiston käsittely kuuluu asetuksen piiriin, kun kyse on esimerkiksi asiakaskortistosta tai sen osasta. Lähtökohtaisesti yrityksen tiedot eivät ole henkilötietoja eli yrityksen nimi, osoite ja vaikka vaihteen puhelinnumero eivät ole henkilötietoja, eikä tietosuoja-asetusta näin sovelleta niihin. Sen sijaan, jos tiedoissa mainitaan yrityksen yhteyshenkilön nimi ja muita mahdollisia henkilötietoja, kuten puhelinnumero, niin ne ovat asetuksen tarkoittamia henkilötietoja ja niiden käsittelyyn on silloin asetusta sovellettava. Lyhyesti sanottuna kaikki tiedot, joiden perusteella voidaan tietää tai saada selville kenestä on kyse, ovat henkilötietoja, ja niihin tulee tietosuoja-asetusta soveltaa. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 18–19.)

Tietosuoja-asetuksen mukaan rekistereissä saa olla vain sellaista tietoa, joka on etukäteen tehdyn suunnitelman eli tietosuojaselosteen, mukaista. Tietojen käsittelyyn on oltava aina laillinen peruste, esimerkiksi asiakassuhteen tai työsuhteen hoitaminen, ja vain kulloinkin tarpeellisia tietoja saa käsitellä. Tietojen määrän tulee siis näin olla riittävä, mutta samalla rajoitettu sisältämään vain välttämättömän tiedon kulloisenkin käsittelyn tarkoituksen kannalta. Käsittelyn perusteena voi olla myös rekisteröidyn antama suostumus tietojensa käsittelyyn joko yhtä tai useampaa tarkoitusta varten. Suostumuksen on oltava vapaaehtoinen, sen voi antaa selkeällä tavalla kirjallisena tai suullisena ja se täytyy myös pystyä peruuttamaan yhtä helposti kuin sen on voinut antaa. Arkaluonteisten henkilötietojen, kuten terveyttä koskevien tietojen, ammattiliiton jäsenyyden, uskonnollisen tai filosofisen vakaumuksen, käsittelyn perusteena voidaan käsitellä esi-

merkiksi nimenomaisen suostumuksen perusteella tai kun kyseisten tietojen käsittely voi olla tarpeen elintärkeiden etujen suojaamiseksi. (Hanninen ym. 2017, 16, 49–51; Tietosuojavaltuutetun toimisto 2018b.)

Tietosuojaperiaatteisiin kuuluu lisäksi, että käsittely on läpinäkyvää eli rekisteröidyillä tulee saada tieto siitä, mihin henkilötietoja käytetään sekä kuka on rekisterinpitäjä. Samoin rekisteröidyille olisi tiedotettava muun muassa heidän oikeuksistaan sekä henkilötietojen käsittelyyn liittyvistä riskeistä ja suojatoimista. Tietojen käsittelyssä on huomioitava asianmukainen luottamuksellisuus ja turvallisuus sekä säilytyksen rajoittaminen. (Article 29 Data Protection Working Party 2018b 6–8; Hanninen ym. 2017, 16, 47–48.)

Tietosuoja-asetuksen mukaisesti henkilötietoja tulisi säilyttää ainoastaan sen ajan, mikä on tarpeen tietojen käsittelyn kannalta, ja sen vuoksi rekisterinpitäjän tulisi käydä läpi tietojen tarpeellisuus ajoittain ja poistaa tarpeettomat tiedot. Samalla varmistetaan tietojen täsmällisyys, eli käydään läpi henkilötietojen oikeellisuus ja laatu, sekä tarvittaessa tehdään tietoihin tarvittavat korjaukset ja poistot. Esimerkiksi asiakassuhteen päättyessä tietojen säilyttäminen voi olla tarpeellista rajoitetun ajan laskutuksen, takuun tai muun syyn vuoksi, jonka jälkeen henkilötiedot tulisi poistaa. Mikäli asiakassuhteeseen liittyviä tietoja on tarvetta säilyttää kauemmin, esimerkiksi tilastollisen syyn vuoksi, tulisi tietoja pystyä muokkaamaan niin, ettei rekisteröity olisi enää tunnistettavissa, eli anonymisoida tieto. Tietosuoja-asetuksen myötä tulevalla uudella käsitteellä, pseudonymisoinnilla, puolestaan tarkoitetaan henkilötietojen käsittelyä niin, että niitä ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja ja jotka tulee myös säilyttää erillään. (Hanninen ym. 2017,21, 50.)

2.2 Osoitusvelvollisuus

Monet tietosuoja-asetuksen seikat ovat olemassa jo nykyisessä lainsäädännössä, ja sen mukaisesti on ollut riittävää, että säännöksiä noudatetaan. Yksi olennaisimpia muutoksia organisaatioille tietosuoja-asetuksen voimaan tullessa on se, että asetuksen noudattaminen ei yksistään riitä, vaan organisaation on kyettävä osoittamaan tietosuojasäännösten huomioiminen rekisterinpitäjän toiminnassa. Jotta osoitusvelvollisuus täyttyy, on

rekisterinpitäjän arvioitava, mitä tietosuojaperiaatteet tarkoittavat ja kuinka ne toteutuvat rekisterinpitäjän omassa toiminnassa. Yritysten tulee siis asetuksen voimaantulon jälkeen pystyä näyttämään dokumenttien avulla se, kuinka tietosuojaperiaatteita yrityksessä käytännössä toteutetaan. (Hanninen ym. 2017, 47, 50–55.)

Dokumentointia on syytä päivittää aina, kun siihen on tarvetta. Dokumentointia voi olla esimerkiksi tietotilinpäätös, tietoturvan ja tietosuojan omavalvonta-suunnitelma, käytännesäännöt ja sertifioinnit. Rekisteri- ja tietosuojaselosteet ovat osa tätä dokumentointia, joista ilmenee muun muassa se, mitä tietoja rekistereihin kerätään, mihin tietoja käytetään sekä miten niitä käsitellään, ja samalla niiden avulla täytetään myös rekisteröidyille tehtävää informointivelvollisuutta. Henkilötietojen suojaamista koskeva kuvaus olisi myös hyvä liittää dokumentaatioon. Teknisestä tietojen suojauksesta voisi olla kirjattuna paitsi tietotekninen suojaus, kuten viruksentorjunta ja palomuurit, niin myös fyysisten tilojen suojaus, johon kuuluu muun muassa kulkuoikeudet ja tilojen lukitseminen sekä työpisteiden sijoittelu. Samoin yhtiön salassapito- ja salasanakäytännöt on hyvä kuvata sekä samalla huomioida missä työtehtävissä on tarve käsitellä henkilötietoja ja minkä tasoisiin käyttöoikeuksiin missäkin tehtävissä on tarve. (Hanninen ym. 2017, 47, 50–55; Opi tietosuojaa 2018a.)

Kaikilla yli 250 työntekijän organisaatioilla on laadittava seloste käsittelytoimista, ja sitä pienemmillä organisaatioilla seloste on laadittava, mikäli henkilötietojen käsittely ei ole organisaatiossa satunnaista, henkilötietojen käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille tai organisaatiossa käsiteltävät henkilötiedot kuuluvat erityisiin tietoryhmiin taikka käsiteltävissä henkilötiedoissa on tietoja, jotka koskevat rikostuomioita tai rikkomuksia. Tietosuojavaltuutetun toimiston (2018b) maaliskuussa päivittämän tiedon mukaan tietosuojatyöryhmä WP29 valmistelee ohjausta siitä, kuinka näitä kriteereitä on sovellettava.

Tietosuojavaltuutetun toimisto on julkaissut mallipohjan rekisterinpitäjän selosteen käsittelytoimista, jota yritykset ja organisaatiot voivat halutessaan käyttää. Selosteen tarkoituksena on toimia yrityksen sisäisenä asiakirjana, sekä samalla sen avulla voidaan hahmottaa henkilötietojen käsittelyä yrityksessä, ja

seloste käsittelytoimista on osaltaan osoittamassa tietosuojalainsäädännön noudattamista. Seloste on pyydettäessä toimitettava valvontaviranomaiselle, sillä sen avulla viranomainen voi tarvittaessa arvioida yrityksen tietojenkäsittelytoimien lainmukaisuutta. Kun jokin muu organisaatio suorittaa henkilötietojen käsittelyä rekisterinpitäjän lukuun, on kyseisen henkilötietojen käsittelijän kuvattava käsittelytoimet omalta osaltaan. Rekisterinpitäjä voi liittää tämän selosteen omaan selosteeseensa niiltä osin kuin se koskee rekisterinpitäjän vastuulla olevien tietojen käsittelyä. (Tietosuojavaltuutetun toimisto 2018b.)

Selosteen voi laatia myös muulla tavoin kuin tietosuojavaltuutetun toimiston mallin mukaisena, mutta siitä on käytävä ilmi tarvittavat tiedot. Rekisterinpitäjän sekä mahdollisten yhteisrekisterinpitäjän, rekisterinpitäjän edustajan sekä tietosuojavaltuutetun nimi ja yhteistiedot on tultava ilmi selosteessa. Henkilötietoryhmistä ja rekisteröityjen ryhmistä on oltava kuvaus kuten esimerkiksi asiakkaat ja työntekijät. Kaikista tiedoista, joita yritys käsittelee, on oltava määriteltynä laillinen peruste niiden käsittelyyn, ja tämä puolestaan määrittelee jatkossa sen mitä tietoja ja mihin tarkoitukseen sekä kuinka pitkäksi ajaksi voidaan kerätä ja käsitellä. Selosteesta on käytävä ilmi myös ryhmät, joille henkilötietoja on luovutettu tai luovutetaan, mukaan lukien myös yhteisrekisterinpitäjät sekä henkilötietojen käsittelijät. Sen sijaan viranomaisten ei katsota olevan asetuksen määritelmän mukaisia vastaanottajia, mikäli henkilötietoja luovutetaan määrätyn, unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan selvitystyön tekemiseksi. Tietojen siirtämisestä niin sanottuihin kolmansiin maihin eli EU- tai ETA- alueiden ulkopuolelle tai kansainvälisille järjestöille on selosteessa oltava maininta, ja mikäli tietoa siirtyy, on myös tarkemmin kuvattava, mitkä tietosuoja-asetuksen kohta tai kohdat mahdollistavat kyseisen tiedonsiirron. (Tietosuojavaltuutetun toimisto 2018b.)

2.3 Rekisteröityjen oikeudet ja informointi

Rekisterinpitäjällä on velvollisuus avoimeen informointiin henkilötietojen käsittelystä rekisteröidyille jo ennen kuin käsittelyä on aloitettu. Informoitavien tietojen määrä kasvaa ja tarkentuu nykylainsäädännöstä tietosuoja-asetuksen myötä. Tietosuoja-asetuksen mukaisesti määrättyjä tietoja on toimitettava tiiviisti esitettynä, läpinäkyvästi, helposti ymmärrettävässä ja saatavilla olevassa

muodossa sekä selkeällä ja yksinkertaisella kielellä. Informointivelvollisuuden täyttämällä yritys voi myös paremmin hahmottaa, mitä henkilötietoja käsitellään ja mihin tarkoituksiin niitä käytetään. Samalla tulee selvitettyä myös tarpeelliset säilytysajat henkilötiedoille eivätkä tarpeettomat tiedot rasita arkistointia. Yrityksen on myös hyvä valmistautua mahdollisiin rekisteröityjen kysymyksiin koskien heidän oikeuksiaan. Rekisteröityjen informointi ja muut toimenpiteet ovat lähtökohtaisesti maksuttomia. Mikäli pyynnöt ovat ilmeisen kohtuuttomia tai perusteettomia, esimerkiksi pyyntöjen esittäminen on toistuvaa, voi yritys periä kohtuullisen maksun tai kieltäytyä tietojen toimittamisesta. (Hanninen ym. 2017, 73–74; EU:n tietosuoja-asetus 679/2016/EU, 12 artikla.)

Tietosuoja-asetuksen mukaan selitys henkilötietojen käsittelystä tulisi toimittaa rekisteröidyille kirjallisesti tai muulla tavoin ja tapauksen mukaan sähköisessä muodossa ja olla näin rekisteröityjen helposti saatavilla. Tiedot tulisi ilmaista mahdollisimman yksinkertaisella tavalla ja pyrkiä välttämään monimutkaisia lauseita. Mikäli tiedot on käännettävä yhdeksi tai useammaksi kieleksi, on rekisterinpitäjän huolehdittava, että käännökset olisivat mahdollisimman tarkkoja. Yhdistetyn rekisteri- ja tietosuojaselosteen laatiminen voi olla ainakin alkuun helpoin tapa informointivelvollisuuden täyttämiseksi. (Article 29 Data Protection Working Party 2018a, 8-9; Hanninen ym. 2017, 73–75.)

Rekisteröidyn oikeuksia tietosuoja-asetuksen mukaan on läpinäkyvän informoinnin lisäksi myös rekisteröidyn oikeus pyytää yritykseltä pääsy häntä itseään koskeviin tietoihin, joka käytännössä tarkoittaa sitä, että yrityksen on pystyttävä kokoamaan rekisteröidyn tiedot omista järjestelmistään niin, että ne voidaan esittää rekisteröidyn nähtäväksi jäljennöksenä käsiteltävistä tiedoista, ja mikäli pyyntö on tehty sähköisesti, tulee myös tiedot toimittaa yleisesti käytetyssä sähköisessä muodossa, jollei rekisteröity toisin pyydä. Oikeus henkilötietojen siirtämisestä järjestelmästä toiseen tarkoittaa, että rekisteröidyn tulisi saada häntä itseään koskevat ja hänen itsensä rekisterinpitäjälle toimittamat tiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa. (Hanninen ym. 2017, 56, 60; EU:n tietosuoja-asetus 679/2016/EU, 15 artikla, 20 artikla.)

Rekisteröidyllä on oikeus pyytää omien tietojensa oikaisemista sekä myös poistamista eli oikeus tulla unohdetuksi. Tietojen poistamista on kuitenkin rajoitettu

niin, että oikeutta tulla unohdetuksi ei sovelleta esimerkiksi silloin, kun henkilötietojen käsittely on tarpeen oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Myöskään varmuuskopioinnin osalta ei ole tarkempaa ohjeistusta olemassa. Rekisteröidyllä on myös oikeus saada tietoonsa sellaiset henkilötietojen vastaanottajat, joille rekisterinpitäjän on ilmoitettava henkilötietojen oikaisuista, poistoista ja käsittelyn rajoituksista. Rekisteröidyllä on oikeus pyytää henkilötietojensa käsittelyn rajoittamista tietyissä tilanteissa, joka käytännössä tulisi pystyä teknisesti toteuttamaan niin, että tietoihin pääsy voitaisiin estää tai tiedot tulisi siirtää eri järjestelmään. Yritys saisi siis säilyttää tiedot, mutta niiden käsittely olisi sallittua vain rajatuin ehdoin. (Hanninen ym. 2017, 56, 62–64; EU:n tietosuoja-asetus 679/2016/EU, 16 artikla, 17 artikla, 18 artikla.)

Oikeuksiin kuuluu myös saada tietää, tehdäänkö henkilötietojen perusteella profilointia sekä kohdistuuko niihin pelkästään automaattista päätöksentekoa. Rekisteröidyllä on myös oikeus vastustaa häntä koskevien henkilötietojen käsittelyä ja rekisterinpitäjä ei saa tämän jälkeen tietoja käsitellä, jollei voi osoittaa käsittelyyn olevan jonkin huomattavan tärkeän ja perustellun syyn, joka syrjäyttää rekisteröidyn oikeudet ja vapaudet. Käsittelyn jatkaminen on sallittua myös, mikäli se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Henkilötietojen käsittelyn vastustaminen suoramarkkinointia varten tarkoittaa, ettei henkilötietoja saa enää kyseiseen tarkoitukseen käyttää, ja sähköpostimarkkinoinnissa tulisi markkinointiviestiin sisällyttää selkeä ohjeistus siitä, kuinka vastaavien viestien vastaanottamisen voi estää. Mikäli rekisteröity katsoo tietosuoja-asetukseen perustuvia oikeuksiaan loukatun, on hänellä oikeus tehdä valitus valvontaviranomaiselle. (Hanninen ym. 2017, 56, 68–69, 79; EU:n tietosuoja-asetus 679/2016/EU, 21 artikla.)

Oikeuksien lisäksi rekisterinpitäjän on tiedotettava rekisteröidyille myös muita asioita kuten rekisterinpitäjän yhteystiedot sekä mahdollisen tietosuojavastaavan yhteystiedot. Rekisteröidyille on myös kerrottava, mihin tarkoitukseen rekisteriin kerättävää tietoa käytetään ja mitkä ovat käsittelyn oikeusperusteet. Tietojen mahdollisesta luovuttamisesta EU:n tai ETA:n ulkopuolelle on myös informoitava, ja mikäli tietoja luovutetaan näiden alueiden ulkopuolelle tai kansainvälisille järjestöille, on kerrottava myös se, kuinka tietosuojan riittävyydestä on huolehdittu

ja mistä rekisteröity halutessaan voi saada lisätietoa asiasta. Henkilötietojen säilyttämisaika taikka määrittämiskriteerit, joiden perusteella säilyttämisaika määräytyy rekisterissä, on tuotava rekisteröityjen tietoon. (Hanninen ym. 2017, 78–80; Valtiovarainministeriö 2016, 14.)

Henkilötietoja kerättäessä muualta kuin rekisteröidyltä itseltään tulee edellä mainittujen tietojen lisäksi kertoa, mitä tietoja kerätään sekä mistä tiedot on saatu ja ovatko saadut tiedot peräisin yleisesti saatavilla olevista lähteistä kuten yritykseltä, joka myy henkilötietoja suoramarkkinointiin. Nämä tiedot voidaan sisällyttää jo suoraan tietosuojaselosteeseen, jolloin niitä ei tarvitse erikseen ilmoittaa. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 80–81.)

2.4 Tietosuojavastaava

Tietosuojavastavastaavan nimittäminen on pakollista pienelle tai keskisuurelle yritykselle, kun sen ydintehtävät muodostuvat sellaisesta henkilötietojen käsittelytoimista, jotka edellyttäisivät laajamittaista järjestelmällistä ja säännöllistä seurantaa. Myös silloin kun yrityksen ydintehtävät muodostuvat laajamittaisesta, arkaluontoisten henkilötietojen käsittelystä, on tietosuojavastaava palkattava. Tietosuoja-asetuksella pyritään kannustamaan myös vapaaehtoiseen tietosuojavastaavan nimittämiseen. Tietosuojavastaava voidaan nimittää joko yrityksen omasta henkilökunnasta tai hänet voidaan ottaa töihin palvelusopimuksen perusteella. Tietosuojavastaava voi olla myös yhteinen useammalle organisaatiolle. Huomioitavaa nimittämisessä on, että tietosuojavastaavalta odotetaan riippumattomuutta, jolloin nimitettävä henkilö ei voi olla sellainen henkilö, joka vastaa yrityksen tietosuojajärjestelmistä tai työssään päättää henkilötietojen käyttötarkoituksista. Tietosuojavastaavan koulutuksesta ja kokemuksen määrästä ei ole varsinaisia vaatimuksia, mutta nimittämisessä on huomioitava henkilön tietämys tietosuojalainsäädännön tuntemuksesta sekä siihen liittyvistä käytänteistä ja huomioitava myös muuten kyseisen henkilön edellytykset tehtävän hoitamiseen. Tietosuojavastaavan nimittämiseen, tehtäviin ja asemaan liittyvät vaatimukset ovat samat siitä huolimatta, nimitetäänkö tietosuojavastaava vapaaehtoisesti vai pakollisesti. (Hanninen ym. 2017,121; Tietosuojavaltuutetun toimisto 2017b.)

Tietosuojatyöryhmä suosittelee rekisterinpitäjiä ja henkilötietojen käsittelijöitä tekemään sisäisen analyysin tietosuojavastaavan tarpeesta, mikäli ei ole selvää tulisiko tietosuojavastaava nimittää. Tämä analyysi tulisi dokumentoida ja liittää se osaksi muuta tietosuojadokumentointia sekä tarvittaessa myös päivittää, sillä viranomainen voi edellyttää analyysin tekemistä. (Tietosuojatyöryhmä 2017a, 5–6.)

Sellaisella yrityksellä joka ei ole velvoitettu tietosuojavastaavan nimittämiseen tai ei halua tehdä sitä vapaaehtoisesti, on mahdollisuus vapaasti palkata joko ulkopuolisia konsulentteja tai henkilöstöä hoitamaan yrityksen henkilötietojen käsittelyä. Tehtävänimike ei tällöin voi kuitenkaan olla tietosuojavastaava, ja tämä tulee selventää niin sisäisessä kuin julkisessa yrityksen viestinnässä esimerkiksi asiakkaille. (Hanninen ym. 2017, 121; Tietosuojatyöryhmä 2017a, 7.)

2.5 Vaikutusten arviointi

Vaikutusten arviointi auttaa rekisterinpitäjän osoitusvelvollisuuden täyttämistä, sillä se auttaa noudattamaan tietosuoja-asetuksen vaatimuksia sekä sen avulla voidaan myös osoittaa, että rekisterinpitäjä noudattaa asetusta asianmukaisin toimenpitein. Tietosuojan vaikutuksen arvioinnin tarkoituksena on luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvien henkilötietojen käsittelyn kuvaaminen sekä arvioida tietojen käsittelyn tarpeellisuutta ja oikeasuhteisuutta. Samalla sen tekeminen tukee henkilötietojen käsittelystä aiheutuvien riskien hallintaa, koska sen avulla voidaan määritellä mahdolliset riskit sekä myös toimenpiteet näiden riskien vähentämiseksi. (Hanninen ym. 2017, 115; Tietosuojatyöryhmä 2017b, 4.)

Vaikutusten arviointi on tehtävä, jos henkilötietojen käsittely todennäköisesti aiheuttaa luonnollisen henkilön kannalta korkean riskin käsittelyn laajuuden, luonteen, asiayhteyden sekä tarkoituksen huomioon ottaen. Kaikkien rekisterinpitäjien on siis ainakin arvioitava käsittelemiinsä henkilötietoihin kohdistuva riski ja sen mukaan perusteltava vaikutusten arvioinnin tarve. Lisäksi on huomioitava rekisterinpitäjän yleinen velvollisuus huolehtia sellaisista toimenpiteistä, joilla pyritään hallitsemaan rekisteröidyn oikeuksiin ja vapauksiin kohdistuvia riskejä, eli käytännössä käsittelytoimien mahdollisesti aiheuttamia

riskejä on arvioitava jatkuvasti. Erityisesti on huomioitava tilanteet, jolloin käytetään automaattista käsittelyä henkilökohtaisten ominaisuuksien arviointiin ja jonka seurauksena on päätöksiä, joilla on oikeusvaikutuksia tai muita merkittäviä vaikutuksia ihmiseen. Samoin pitkäaikaisesti tai laajasti arkaluontoisia henkilötietoja käsitellessä on vaikutuksen arviointi aina pakollinen. Kansallisen tietosuojaviranomaisten tulee laatia tietosuoja-asetuksen mukaisesti lista sellaisista käsittelytoimien tyypeistä, jolloin vaikutusten arviointi ainakin vaaditaan, ja tämä lista tulee myös julkaista. (Hanninen ym. 2017, 115–118; Tietosuojatyöryhmä 2017b, 4, 7.)

2.6 Tietoturvaloukkaus

Rekisterinpitäjän tulee huolehtia, että henkilötietojen suojaustoimissa on huomioitu niiden käsittelyyn liittyvä riski, sekä valmistautua mahdollisiin tietoturvaloukkauksiin laatimalla toimintaohjeet niitä varten. Toimintaohjeita varten on arvioitava, minkä tasoinen riski rekisteröidylle voi tietoturvaloukkauksesta koitua, ja sen perusteella määritellään toimenpiteet kuten esimerkiksi tietoturvaloukkauksen dokumentointi, ilmoitus rekisteröidylle tai ilmoitus valvontaviranomaiselle. (Article 29 Data Protection Working Party 2018a, 6; Hanninen ym. 2017, 106–107.)

Henkilötietojen tietoturvaloukkauksella tarkoitetaan sellaista loukkausta, jonka seurauksena henkilötietoja tuhoutuu, häviää tai muuttuu, tietoja luovutetaan luvattomasti tai niitä pääsee käsittelemään taho, jolla ei ole käsittelyoikeutta. Tietoturvaloukkaus voi olla esimerkiksi hakkerointi, varastettu tietokone, kadonnut USB-tikku, tulipalo tai haittaohjelma. Tietoturvaloukkaus voi siis näin olla esimerkiksi paitsi tahaton tai tahallinen tekninen vika niin myös inhimillisen erehdyksen seurauksena tapahtunut tietojen häviäminen. Tietoturvaloukkauksen seurauksena voi olla fyysisiä, aineellisia tai aineettomia vahinkoja, kuten rahallisia menetyksiä, identiteettivarkauksia, petoksia ja maineen vahingoittuminen, lisäksi rekisterinpitäjä voi olla estynyt käsittelemään henkilötietoja ja rekisteröityjen oikeudet voivat olla rajoittuneet tai estyneet. (Article 29 Data Protection Working Party 2018a, 7; Hanninen ym. 2017, 108; Tietosuojavaltuutetun toimisto 2017a.)

Tietoturvaloukkauksesta tulee rekisterinpitäjällä tehdä ilmoitus tietosuojaviranomaiselle, paitsi jos loukkaus ei aiheuta todennäköisesti riskiä rekisteröityjen oikeuksille ja vapauksille. Esimerkiksi tilanne, jolloin henkilötietojen käsittely ei ole mahdollista maksuliikenteen keskeytyksen vuoksi voi aiheuttaa riskin rekisteröidyn oikeuksille ja näin ollen on mahdollisesti ilmoitus tehtävä. Sen sijaan jos yritys ei tilapäisesti voi lähettää markkinointiviestejä, ei loukkaus todennäköisesti aiheuta riskiä, ja näin ollen ilmoitusta ei ole tarvetta tehdä. Tietoturvaloukkauksen kaikki mahdolliset seuraukset on siis arvioitava tapauskohtaisesti ja sen mukaisesti on harkittava ilmoituksen tekemisen tarpeellisuus. Rekisterinpitäjän vastuulla on ilmoituksen tekeminen siitä riippumatta, onko tietoturvaloukkauksen havainnut rekisterinpitäjä tai henkilötietojen käsittelijä. Henkilötietojen käsittelijän tulisikin ilmoittaa tietoonsa tulleesta tietoturvaloukkauksetta ilman aiheetonta viivytystä rekisterinpitäjälle. (Article 29 Data Protection Working Party 2018a, 10–11; Hanninen ym. 2017,108–109; Tietosuojavaltuutetun toimisto 2017a.)

Valvontaviranomaiselle tehtävä ilmoitus tietoturvaloukkauksesta tulee tehdä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta. Tietosuoja-asetuksessa ei huomioida pyhäpäiviä, joten tietoturvaloukkauksiin tulisi reagoida yhtä nopeasti, vaikka se tulisi ilmi joulun pyhinä. Mikäli ilmoitusta ei tehdä 72 tunnin kuluessa, tulee rekisterinpitäjällä toimittaa perusteltu selvitys viivästymisen syistä valvontaviranomaiselle. Rekisterinpitäjällä on dokumentointivelvollisuus kaikkiin henkilötietojen tietoturvaloukkauksiin ja niiden vaikutuksiin sekä tehtyihin toimenpiteisiin tilanteen korjaamiseksi riippumatta siitä, mitä toimenpiteitä loukkauksesta lopulta seuraa. Mikäli rekisterinpitäjä laiminlyö ilmoituksen tekemisen tai dokumentointivelvollisuuden, se voi johtaa tietosuoja-asetuksessa määriteltyihin seuraamuksiin. (Hanninen ym. 2017, 109; Tietosuojavaltuutetun toimisto 2017a.)

Tietoturvaloukkauksen aiheuttaessa todennäköisesti korkean riskin rekisteröityjen oikeuksille ja vapauksille on rekisterinpitäjän velvollisuus ilmoittaa heille tapahtuneesta tietoturvaloukkauksesta. Esimerkiksi luottokorttitietojen joutuminen ulkopuolisten haltuun ja mahdollisuus niiden väärinkäyttöön olisi tilanne, jolloin rekisteröityä olisi informoitava, ja näin rekisteröidyllä olisi mahdollisuus suojata itseään sulkemalla luottokortti. Henkilötietojen

tietoturvaloukkauksesta tulisi rekisteröidyille ilmoitettava ilman aiheetonta viivytystä. (Hanninen ym. 2017, 111; Tietosuojavaltuutetun toimisto 2017a.)

2.7 Tietojenkäsittelysopimukset

Tietotosuoja-asetus tulisi huomioida myös silloin, kun yritys esimerkiksi antaa ulkoiselle IT-tuelle pääsyn henkilöstöhallinnan järjestelmäänsä tai siirtää työntekijöiden tietoja palkanmaksusta vastaavalle palveluntarjoajalle. Tällöin tiedon katsotaan siirtyvän henkilötietojen käsittelijälle, joka käsittelee henkilötietoja yrityksen eli rekisterinpitäjän puolesta. Asetuksen mukaisesti näissä tilanteissa tulee laatia kirjallinen tietojenkäsittelysopimus tai muu vastaava oikeudellinen asiakirja, jonka voi sisällyttää varsinaiseen sopimukseen. tai tehdä erillinen liite, jolloin asiakirja on helppo sisällyttää jo olemassa olevaan sopimukseen. (Hanninen ym. 2017, 82–83.)

Sopimuksia laadittaessa on hyvä huomioida molempien osapuolten tarpeet ja vastuut. Tietojenkäsittelysopimukseen ei ole olemassa minkäänlaista valmista mallipohjaa, joten eri yrityksillä voi olla käytössään erilaisia variaatioita. Mahdollisia mallipohjia tai komission hyväksymiä vakiosopimuslausekkeita voidaan julkaista ja ottaa käyttöön myöhemmin, joten olisi hyvä seurata tietosuojaviranomaisen uutisointia ja ohjeistuksia asiasta. Sopimuksen olisi hyvä olla mahdollisimman selkeä ja jossa ei olisi yllättäviä ehtoa tai epämääräisiä velvoitteita. (Hanninen ym. 2017, 82–83; Yrittäjät 2018, 27.)

2.8 Käytännesäännöt ja sertifiointi

EU:n jäsenvaltioita ja viranomaisilta vaaditaan tietosuoja-asetuksessa edistämään sellaisten käytännesääntöjen laatimista, joiden avulla tuetaan asetuksen soveltamista asianmukaisesti. Näitä sääntöjä voivat laatia esimerkiksi alaa edustavat työnantaja- ja toimialaliitot toimialakohtaisesti ja ne voivat asetuksen mukaisesti koskea esimerkiksi henkilötietojen keräämistä, niiden käsittelyn asianmukaisuutta ja läpinäkyvyyttä. Käytännesääntöjen luonnos tulee hyväksyttää valvontaviranomaisella, että ne vastaavat asetuksen sisältövaatimuksia. Käytännesääntöjä noudattamalla yritys toimii samalla myös

lain edellyttämällä tavalla, joten käytännesäännöistä on näin hyötyä yrityksen toiminnalle. (Hanninen ym.2017,113–114.)

Tietosuojaa koskevien sertifiointimekanismien, tietosuojasinettien ja merkkien käyttö tulee myös asetuksen myötä mahdolliseksi. Niiden tarkoituksena on osoittaa se, että rekisterinpitäjä tai henkilötietojen käsittelijä noudattaa tietosuoja-asetusta omissa käsittelytoimissaan, mutta niiden käyttö ei kuitenkaan vähennä vastuuta asetuksen noudattamisesta. Sertifiointi on vapaaehtoista ja se myönnetään enintään kolmeksi vuodeksi kerrallaan. Se on uusittavissa samoilla edellytyksillä millä on myönnettykin mutta voidaan myös peruuttaa, mikäli vaatimukset eivät täyty. (Hanninen ym. 2017, 114.)

2.9 Valvonta ja sanktiot

Oikeusministeriön 1.3.2018 julkaiseman tiedotteen mukaan yleisen tietosuoja-asetuksen viranomaistehtävät keskitettäisiin tietosuojavaltuutetulle ja lisäksi tietosuojavaltuutetun toimistoon perustettaisiin asiantuntijalautakunta, jonka tehtäviin kuuluisi antaa lausuntoja lainsäädännön soveltamiseen liittyvistä asioista. Yrityksen tulee olla valvontaviranomaiseen tarvittaessa yhteydessä esimerkiksi tietoturvaloukkauksen yhteydessä tai kun henkilötietoja siirtyisi EU- tai ETA-maiden ulkopuolelle. Tietosuojavaltuutetulla olisi oikeus määrätä rekisterinpitäjä ja henkilötietojen käsittelijä antamaan tarvittavat tiedot sekä myös valtuudet antaa erilaisia varoituksia, huomautuksia tai määräyksiä. (Hanninen ym. 2017, 109–110, 128; Oikeusministeriö 2018.)

Tietosuojasäännösten rikkomisesta voisi lievimmillään seurata esimerkiksi huomautus. Rekisterinpitäjän oikeutta käsitellä henkilötietoja voitaisiin myös rajoittaa joko määräaikaisesti tai pysyväksi. Säännösten rikkomuksista voitaisiin määrätä myös hallinnollisia sakkoja, jotka lievemmissä tapauksissa voisivat olla enintään 10 miljoonaa euroa tai 2 % yrityksen kokonaisliikevaihdossa. Vakavammissa rikkomuksissa sakkojen määrä nousisi ja voisi olla enintään 20 miljoonaa tai 4 % yrityksen kokonaisliikevaihdosta. Tietosuojalaissa esitetään kansallisen liikkumavaran perusteella, ettei hallinnollista seuraamusmaksua sovellettaisi julkisella sektorilla tapahtuvaan henkilötietojen käsittelyyn ja perusteena tähän esitetään

hallintoa jo sitovan lainmukaisuusvaatimuksen, virkavastuun sekä vahingonkorvausvastuun. (Hanninen ym. 2017, 129–130; Oikeusministeriö 2018.)

Yritys voi joutua myös maksamaan vahingonkorvausta rekisteröidylle, mikäli tietosuoja-asetuksen rikkomisesta aiheutuu tälle aineetonta tai aineellista vahinkoa. Maksuvelvollinen on vahingon aiheuttaneesta tapahtumasta vastuussa oleva yritys. Henkilötietojen käsittelijä on vastuussa vain silloin, jos se ei ole noudattanut nimenomaisesti sille osoitettuja velvoitteita tai se on toiminut rekisterinpitäjän lainmukaisen ohjeistuksen ulkopuolella tai vastaisesti. (Hanninen ym. 2017, 130–131.)

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mukaan rikosoikeudellinen vastuu tulisi jatkossa kyseeseen vain sellaisissa tilanteissa, joissa lainvastainen henkilötietojen käsittely ei olisi hallinnollisten sakkojen piirissä. Kyseessä olisi sen sijaan tietosuojarikos, jonka seurauksena voisi olla sakkoja tai enintään vuosi vankeutta. Tietosuojarikoksesta voisi olla kyse esimerkiksi silloin, kun työntekijä urkkii rekisteröidyn tietoja, vaikkei hänellä työtehtäviensä mukaisesti olisi oikeutta niitä käsitellä, tai henkilörekisteristä tulostettuja asiakirjoja heitetään pois huolehtimatta niiden tietoturvallisesta hävittämisestä. Rangaistussäännökseen ei ole ehdotettu sovellettavan oikeushenkilön rangaistusvastuuta eli yritys ei voi syyllistyä tietosuojarikokseen. (Hanninen ym. 2017,131–132; Oikeusministeriö 2018.)

3 YRITYKSEN DOKUMENTOINTI

Yritystä varten koottu aineisto on kerätty sähköisenä versiona yhteen kansioon, jonne henkilöstöllä on pääsy etätyöpöytäyhteyden kautta omilta työpisteiltään. Lisäksi aineisto on tulostettu kansioon, jossa on lisänä myös Henkilötietojen käsittely -kirja. Tietosuoja-aineistossa on yritykselle laaditun dokumentaation lisäksi myös muuta tietosuojaan liittyvää aineistoa, kuten informaatiota tietosuojavaltuutetun toimiston sivulta, josta voi mahdollisesti olla hyötyä jatkossa.

3.1 Henkilöstön informointi

Henkilötietoja yrityksessä käsittelevien toimihenkilöiden, ja tuotannon työntekijöiden osalta käsittely rajoittuu lähinnä lähetteisiin ja tuotannon papereihin, joissa voi mahdollisesti olla esimerkiksi asiakkaan tai yrityksen yhteyshenkilön nimi. Lähetteen mukaisesti toimituksille laaditaan rahtikirjat, joten kyseiset tiedot ovat oleellisia, jotta tilattu tuote voidaan asiakkaalle toimittaa, ja näin ollen peruste niiden käsittelyyn lähetteessä on olemassa. EU:n tietosuoja-asetusta koskevan lyhyen koulutuksen yrityksessä olivat käyneet tehdaspäällikkö ja toimistopäällikkö, joten heillä oli jo tietoa asetuksen sisällöstä ja sen mukanaan tuomista vaatimuksista ja muutoksista. Kaikkien henkilötietoja käsittelevien on kuitenkin oltava tietoisia asetuksen voimaantulosta ja sen perusasioista, jotta asetuksen vaatimukset ja muutokset pystyttäisiin huomioimaan myös käytännössä.

Henkilöstön infromointia varten laadin yrityksen käyttöön tietosuojaoppaan, johon pyrin tiivistämään mahdollisimman hyvin keskeisimpiä asioita tietosuojauudistuksesta. Oppaan sisältämä tieto on hyvin pitkälti samankaltaista kuin tämän opinnäytetyön sisältämä teoriatieto asetuksen sisällöstä. Lisäksi korostin oppaassa tekstiä punaisella värillä niiltä osin, kun katsoin sen sisältävän tärkeimpiä tietoja. Oppaassa on käytetty lähteitä ja ne ovat merkittyinä tekstiin sekä tehty myös lähdeluettelo, jonka avulla henkilöstö voi tarvittaessa etsiä tarkempaa lisätietoa asioista.

3.2 Tietosuojasuunnitelma

Tietosuojasuunnitelma on yrityksen sisäiseen käyttöön tehtyä dokumentaatiota, jossa käydään läpi nimenomaan kyseisen yrityksen tietosuojaan liittyviä seikkoja. Arkistointi-osiossa käydään läpi yrityksessä käytössä olevia arkistointijärjestelmiä ja -tapoja. Osioon on myös kirjattuna yrityksessä arkistoitavien mahdollisesti henkilötietoja sisältävien asiakirjojen säilytysajat. Ohjeistuksena käytetään Kauppakamari Tieto liitettä A15 Eräitä asiakirjojen säilytysaikoja, joka on julkaistu 19.2.2016. Liitteen lähteenä on käytetty Liikearkistoyhdistys ry:n julkaisemaa kirjaa Vuodesta sataan – sähköisten asiakirjojen hallinta ja säilyttäminen, joka on julkaistu vuonna 2009. Kirjassa olevassa asiakirjaluettelossa määritellyt säilytysajat ovat vähimmäissäilytysaikoja, ja niiltä osin kuin ne eivät perustu lakeihin, asetuksiin tai viranomaisten määräyksiin, kyseessä on suositusluonteiset ja ohjeelliset säilytysajat. Arkiston säilytyksessä on huomioitavaa myös se, että alle 10 vuotta säilytettävät aineistot voidaan säilyttää sähköisesti ja yli 10 vuotta säilytettävä aineisto olisi hyvä tallentaa mikrofilmille tai tulostaa paperille. Pysyvästi tai pitkäaikaisesti säilytettävä aineisto tulisi aina tulostaa paperille. (Vuodesta Sataan -sähköisten asiakirjojen hallinta ja säilyttäminen 2009, 60–61.)

Nykyinen toiminnanohjausjärjestelmä on otettu käyttöön vaiheittain niin, että täydessä käytössä järjestelmä on ollut vuonna 2015. Edellisessä järjestelmässä on kuitenkin edelleen tietoja, jotka on syytä säilyttää muun muassa takuuaikojen vuoksi (Riekki 2018). Sähköisissä järjestelmissä jokaisella on omat salasanansa järjestelmiin, kuten myös koneet on suojattu henkilökohtaisilla tunnuksilla, näin henkilötietojen käsittelyä on rajoitettu työtehtävien mukaisesti vain niille henkilöille, joilla kulloinkin on tarve kyseisiä tietoja käsitellä.

Yrityksessä on olemassa myös paperista arkistoa, joista iso osa on ajalta ennen omistajanvaihdosta. Näiden tietojen läpikäyminen on aloitettu, jotta tietosuoja-asetuksen voimaantullessa yrityksellä olisi varmistettuna ja tallessa vain sellainen paperinen henkilötietoja sisältävä materiaali, jolle on laillinen peruste säilytykseen. Osassa aineistossa, kuten palkkakorteissa, arkistointiaika on niinkin pitkä kuin 50 vuotta, joten paperista aineistoa tulee jatkossakin olemaan säilytettävänä. Pienemmän paperisen aineiston tuhoamiseen tietoturvallisesti voidaan käyttää hyvää silppuria, mutta suuremman määrän tietoturvalliseen tuhoamiseen

on järkevämpää käyttää tietoturvapalvelua, jota Suomessa tarjoaa muutama yritys. Tietoturvapalvelua käyttämällä toimeksiantaja yritys saa myös todistuksen tietojen hävittämisestä, ja tämä todistus voidaan liittää osaksi dokumentaatiota.

Tietosuojasuunnitelmassa on osittain päällekkäistä tietoa myös muiden tehtyjen dokumenttien kanssa, sillä siinä käydään myös läpi rekisteri- ja tietosuojaselosteissa olevat tiedot. Suunnitelmassa on kuitenkin tarkemmin selitettynä yrityksen eri henkilötietojen käsittelijöitä ja yhteistyötahoja, joita ei rekisteri- ja tietosuojaselosteisiin voi suoraan laittaa, koska nämä tahot voivat vaihdella esimerkiksi asiakkaiden kohdalla tilauksen kuljetukseen liittyvien yksityiskohtien vuoksi. Rekisteröidyn mahdollisesti pyytäessä tietoja henkilötietojensa käsittelystä hänelle annetaan vastauksessa tiedoksi nimenomaan ne tahot, jotka käytännössä hänen tietojaan käsittelevät.

Kuvaus fyysisestä työympäristöstä tietosuojan näkökulmasta on myös osana suunnitelmaa. Yrityksessä on olemassa ajantasaiset luettelot avaimista ja niiden hallussapitäjistä, jotka tarvittaessa voidaan esittää osana tietosuojan dokumentteja. Osaan tiloista kuten arkistoon on pääsy vain niillä henkilöillä, jotka työnsä puolesta tarvitsevat kyseiseen lukittuun tilaan pääsyn. Työpisteiden sijoittelussa on myös pyritty huomioimaan mahdollisimman hyvin se, ettei sivullisen ole mahdollista nähdä näytöllä olevia tietoja.

Varsinaisen teknisen suojauksen käsittely rajattiin työni ulkopuolelle, mutta tekninen suojaus on yleisesti ottaen varsin tärkeää huomioida, sillä iso osa tiedoista on sähköisissä järjestelmissä. Teknisen suojauksen on oltava kunnossa ja myös siitä on hyvä olla olemassa dokumentaatiota, ja niinpä yrityksen IT-tuen hoitavalta yritykseltä on pyydetty selostetta teknisestä suojauksesta sekä heidän tiedossaan olevasta tarkemmasta listauksesta käyttöoikeuksista eri järjestelmiin. Tämä seloste tulee olemaan osana tietosuojasuunnitelmaa, ja IT-tuen hoitava yritys toimittaa sen suoraan toimeksiantoyrityksen edustajalle tietoihin lisättäväksi.

3.3 Rekisteri- ja tietosuojaselosteet

Tietosuojavaltuutetun toimiston (2018c) mukaan rekisterinpitäjä on voinut toteuttaa informaatiovelvoitteensa tietosuojaselostetta käyttämällä nykyisen

henkilötietolain aikana. Tietosuoja-asetuksen myötä rekisterinpitäjän tulee arvioida, täyttääkö käyttötarkoituksen mukaisesti tehdyt selosteet informaatiolta edellytettävät vaatimukset, mikäli rekisterinpitäjä aikoo jatkossa kyseisenkaltaisia selosteita käyttää. Tarkempia ohjeistuksia informointitapaan ei kuitenkaan ole olemassa, ja pohjatyönä tutustuin eri alojen erilaisiin rekisteriselosteisiin, joita oli hyvin monenlaisia mutta pääpiirteittäin ne vaikuttivat varsin selkeiltä keinolta tarvittavien tietojen esille tuomiseen. Yrityksellä ei ollut ennestään olemassa rekisteriselostetta, joten sen puolesta aloin rakentamaan selosteita alusta asti. Todennäköisesti tietosuoja-asetuksen voimaantulon jälkeen tulee esille erilaisia käytäntöjä, joista osa voi vakiintua yleisemmin käytetyiksi niin sanotuiksi mallipohjiksi, vaikkei virallisia malliohjeita informointitapaan sen tarkemmin julkaistaisi myöhemminkään.

Yrityksessä käsiteltävät henkilötiedot jakaantuvat varsin selkeästi kolmeen eri pääryhmään: asiakkaisiin, yhteistyötahoihin sekä henkilöstöön. Ryhmistä ei voi tehdä suoraan yhtä kaikkia kattavaa kokonaisuutta, koska mikäli kaikki tietosuoja-asetuksen mukaiset informoitavat asiat laitettaisiin niin sanotusti yksiin kansiin, tulisi selosteesta hyvin pitkä ja todennäköisetsi myös vaikeaselkoinen. Informaatio tulisi kuitenkin antaa rekisteröidyille tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa, joten kaikkien ryhmien tietojen kokoaminen yhteen ei tätä vaatimusta täyttäisi.

Yhteyshenkilöiden nimeäminen eri ryhmille on myös luontevaa tehdä yrityksen sisäisten työtehtävien mukaisesti niin, että rekisterin yhteyshenkilönä toimiva myös käsittelee nimenomaan kyseisessä rekisterissä olevia henkilötietoja työtehtävissään. Suunnittelin yritykselle rekisteri- ja tietosuojaselosteet asiakas- ja markkinointirekisterille (Liite 1), henkilöstölle ja yhteistyötahoille. Lisäksi tein työnhakijoita koskevan oman rekisteri- ja tietosuojaselosteen, vaikka hakijoiden määrä ja käsiteltävien henkilötietojen määrä on varsin pieniä, mutta hakijoista kuitenkin luodaan omanlaisensa rekisteri, koska sen käsittely kuitenkin eroaa henkilöstörekisterin käsittelystä, eikä sitä näin ollen ole järkevää laittaa senkään alle.

Kaikissa rekisteri- ja tietosuojaselosteissa on kirjattuna yrityksen ja kyseisen rekisterin yhteyshenkilön tai yhteyshenkilöiden tiedot. Niissä tuodaan ilmi myös perusteet henkilötietojen keräämiselle ja käsittelylle kuten asiakassuhteen tai työsuhteen hoitaminen. Samoin rekisteröidyn tietoon on selkeästi tuotava myös seuraukset, mikäli tietoja ei saa käsitellä, esimerkiksi mikäli asiakas kieltäytyy antamasta yhteystietojaan ei yritys vastaavasti pysty toimittamaan tilausta, joten tilauksen sopimusta ei voida solmia.

Rekisterin tietosisältö kohdassa käydään läpi se, mitä tietoja kuhunkin rekisteriin talletetaan, esimerkiksi työnhakijan kohdalta tallennetaan ainoastaan nimi, puhelinnumero sekä koulutus ja/tai mahdollinen aiempi työkokemus nimenomaan kyseisessä yrityksessä. Säännönmukaisina tietolähteinä rekistereissä on henkilötietojen osalta pääsääntöisesti rekisteröity itse, poikkeuksena asiakkaiden kohdalla mahdollisten työmaan yhteyshenkilöiden tiedot, jotka tulevat yleensä asiakkaan kautta eivätkä yhteyshenkilöltä itseltään suoraan.

Yrityksestä ei luovuteta tietoja EU:n tai ETA:n ulkopuolelle, ja tämä myös mainitaan rekistereissä samoin kuin ilmaistaan ne tahot, joille tietoja voidaan yrityksen puolelta luovuttaa. Rekisterin suojauksen periaatteet sekä manuaalisen eli paperisen että ATK:lla käsiteltävän aineiston suhteen käydään lyhyesti läpi jokaisessa selosteessa. Rekisteröidyn oikeudet tuodaan esille mahdollisimman selkeästi ja lyhyesti esitettynä kokonaisuutena, ja rekisteröidyn oikeus tehdä valitus valvontaviranomaiselle on omana kohtanaan selosteen lopussa.

Henkilöstön kohdalta tietojen säilytysajat vaihtelevat hyvinkin pitkiä aikoja, riippuen siitä mistä tiedosta on kyse, esimerkiksi verokorttia säilytetään verovuoden ajan tai lyhyemmänkin aikaa, mikäli palkanlaskentaan toimitetaan muutosverokortti, joka korvaa aiemmin käytetyn. Tapaturmia koskevat asiakirjat tulee puolestaan säilyttää 20 vuoden ajan, ja osa työsuojelun asiakirjoista on pysyvästi säilytettäviä. Henkilöstölle suunnatussa rekisteri- ja tietosuojaselosteessa on kirjattuna kaikki tämän hetkiset säilytysajat, ja mikäli niihin tulee muutoksia lainsäädännössä tai muussa ohjeistuksessa, päivitetään tiedot myös selosteeseen.

Yhteistyötahojen ja asiakkaiden kohdalla säilytysaikaan vaikuttaa luonnollisesti asiakassuhteen pituus mutta myös tuotteiden takuuajat sekä lisäksi myös hyvä asiakaspalvelu, sillä yritys haluaa mahdollisuuden asiakkaalle saada tietoonsa

esimerkiksi tilauksessa käytetyn värimallin mahdollista myöhempää tarvetta varten. Yhteistyötahojen henkilötietojen säilyttämisessä on huomioitavaa myös se, että joidenkin tahojen kanssa yhteistyö voi olla satunnaisempaa ja välillä voi olla pidempiäkin aikoja, jolloin yhteistyötä ei ole lainkaan, joten tietoja ei ole kuitenkaan järkevää poistaa kovin lyhyin aikavälein. Työnhakijoiden suhteen henkilötietojen säilytysaika on suhteellisen lyhyt, sillä tietoja säilytetään vain vuoden ajan tai hakijan pyynnöstä tiedot poistetaan jo aiemmin.

Rekisteri- ja tietosuojaselosteista asiakas- ja markkinointirekisteriä koskeva seloste (Liite 1) tulee olemaan esillä yrityksen internetsivuilla sekä saatavilla myös paperisena versiona toimipaikoissa. Henkilöstön rekisteriseloste pidetään nähtävillä toimipisteiden ilmoitustauluilla ja siitä informoidaan henkilöstöä myös tarkemmin ennen asetuksen voimaantuloa toukokuussa. Työnhakijoiden ja yhteistyötahojen osalta rekisterin ovat käytettävissä ja ilmi tuotavana niillä toimihenkilöillä, jotka kyseisten tahojen kanssa asioivat. Yhteistyötahojen osalta seloste voi myös mahdollisesti tulla esille yrityksen internetsivuille jossakin vaiheessa.

3.4 Tietoturvaloukkausten kirjaaminen

Tietoturvaloukkauksista puhuttaessa on hyvä ymmärtää, ettei se käsitä yksistään teknisiä loukkauksia kuten haittaohjelmia, palvelunestohyökkäyksiä ja tietomurtoja sähköisiin järjestelmiin, vaan loukkauksiksi katsotaan myös esimerkiksi kadonnut USB-tikku tai ulkopuolisen käsiin joutuneet paperit, jotka sisältävät henkilötietoja. Nämä seikat tulevat esille henkilöstölle kootussa tietosuojaoppaassa. Tietosuojasuunnitelma sisältää tarkemmat ohjeistukset siitä, kuinka toimia yrityksessä sisäisesti, mikäli tietoturvaloukkaus havaitaan, sekä myös tietosuojavaltuutetun toimiston ohjeet loukkauksen ilmoittamisesta tietosuojaviranomaiselle tai rekisteröidyille, mikäli näiden toimenpiteiden katsotaan yrityksessä olevan tarpeen.

Kaikki tietoturvaloukkaukset tulisi kuitenkin dokumentoida, vaikka niistä ei olisikaan tarvetta tehdä ilmoitusta eteenpäin rekisteröidyille tai tietosuojavaltuutetulle. Näin yrityksessä voidaan tältä osin täyttää osoitusvelvollisuutta ja tarvittaessa

näyttää tietosuojaviranomaiselle, mitä mahdollisia tietoturvaloukkauksia yrityksessä käsiteltäviin henkilötietoihin on kohdistunut ja mitä jatkotoimenpiteitä niiden seurauksena on tehty.

Tietoturvaloukkausten kirjaamiseksi laadin Excel-taulukon (Taulukko 1, Taulukko 2), johon on esimerkeiksi kirjattu kaksi erilaista keksittyä tietoturvaloukkausta malliksi tarvittavia kirjauksia varten. Taulukkoon on merkittynä viisi erilaista tapahtumatyyppiä: haittaohjelma, tietomurto, palvelunestohyökkäys, inhimillinen erehdys ja muu tietoturvaongelma. Erilaisia tapahtumatyyppejä voisi listata huomattavasti enemmänkin mutta pyrin erittelemään tapahtumatyypeiksi sellaiset, joita yleisen uutisoinnin perusteella voisi todennäköisimmin tapahtua ja lisänä on muu tietoturvaongelma, jonka sattuessa tapahtuman kuvaukseen voisi tarkemmin eritellä tarvittaessa tapahtumatyyppiä. Tarpeen mukaan itse taulukkoa sekä tapahtumatyyppejä on myös mahdollista muokata myöhemmin.

TIETOTURVALOUKKAUKSEN KIRJAAMINEN

Tapahtumatyypit: 1. Haittaohjelma, 2. Tietomurto, 3. Palvelunestohyökkäys, 4. Inhimillinen erehdys, 5. Muu tietoturvaongelma

Tapahtuman havaitsemisaika (pvm + kellonaika)	Kuka havainnut	Kuvaus tapahtuneesta	Tapahtumatyyppi
ESIMERKKI 1.1.2018 klo 18.00	Matti Meikäläinen	Latasin asennuslistan USB-tikulle voidakseni käyttää tietoja työmatkalla myös junassa. Poikeuksellisesti työkoneen huollon vuoksi sovittiin erikseen kotikoneen käyttämisestä tällä matkalla, joten siksi tiedonsiirto tikun avulla. Kotona huomasin USB tikun kadonneen mutta löysin sen noin puolen tunnin etsimisen jälkeen tietokonelaukun vuorin ja päällisen välistä, jonne se oli mennyt laukun sisällä olevasta reiästä.	4. inhimillinen erehdys
ESIMERKKI 14.1.2018 klo 14.45	Pirkko Palkanlaskija	Yrityksen käyttämästä Jeesbox pankista tuli ilmoitus, että heitä kohtaan on tehty palvelunestohyökkäys ja tämä voi vaikuttaa rahansiirtoon seuraavien parin päivän ajan. Yrityksen palkanmaksupäivä on kuun 15. päivä, joten palvelunestohyökkäys voi viivästyttää palkan siirtymistä tilille.	3. palvelunestohyökkäys

Taulukko 1. Tietoturvaloukkauksen kirjaaminen, pohja ja esimerkki

Asiasta ilmoitettu rekisteröidyille	Asiasta ilmoitettu tietosuojaviranomaiselle	Toimenpiteet, joihin on ryhdytty tai aiotaan vielä ryhtyä vaikutusten pienentämiseksi ja poistamiseksi
Ei, tietojen katoaminen oli lyhytaikainen ja käytännössä tiedot eivät päässeet ulkopuolisten haltuun missään vaiheessa. Tiedot eivät myöskään sisältäneet arkaluonteisia tietoja lainkaan.	Ei, tietojen katoaminen oli lyhytaikainen ja käytännössä tiedot eivät päässeet ulkopuolisten haltuun missään vaiheessa. Tiedot eivät myöskään sisältäneet arkaluonteisia tietoja lainkaan.	Kiinnitetään huomiota tietojen käsittelyyn ja asianosainen korjauttaa kannettavan tietokoneen laukun tai mikäli korjaaminen ei ole mahdollista niin hankitaan uusi. Samalla kehotetaan myös muita työntekijöitä, jotka työssään käyttävät kannettavia ja kuljettavat niitä laukuissa, tarkistamaan laukkujensa kunnon.
Kyllä, henkilöstölle on ilmoitettu pankkiin kohdistuneesta palvelunestohyökkäyksestä, joka voi viivästyttää palkan siirtymistä tilille. Henkilöstön arkaluonteisest tiedot eivät ole olleet vaarassa hyökkäyksen vuoksi.	Kyllä, asiasta tehtiin ilmoitus, koska tapahtuneesta voi aiheutua riski koskien rekisteröityjen oikeuksia ja vapauksia, palkanmaksun viivästymisestä voi koitua esimerkiksi aineellista vahinkoa.	Tapahtuneesta ilmoitettiin henkilöstölle sähköpostitse sekä ilmoitustaulun avulla. Yrityksessä huolehditaan omalta osaltaan tietosuojan teknisestä toimivuudesta mahdollisimman hyvin.

Taulukko 2. Tietoturvaloukkauksen kirjaaminen, pohja ja esimerkki

3.5 Seloste käsittelytoimista

Tietosuojapaketin tekemisen alkuvaiheessa ei ollut olemassa valmista mallia, jota käsittelytoimien kirjaamiseksi voisi käyttää. Visma Suunta -sivustolta löytyi Riikka Lehtisen (2018) GDPR-esitys, taulukkopohja ja muistilistat, josta löytyi mallia tietoanalyysin tekemiseen. Laadin mallin pohjalta Wordiin yksinkertaisen tietoanalyysin muun muassa yrityksessä käsiteltävistä henkilötiedoista, käsittelyjärjestelmistä ja tietojen säilytysajoista. Koska yrityksellä on ainakin jollain tasolla arvioitava käsittelemiinsä henkilötietoihin kohdistuva riski ja sen perusteella arvioita riskinarvioinnin tarve, päädyin muokkaamaan myös tämän tiedon sisällyttämisen tietoanalyysiin. Tällä tavalla tietoja yhdistämällä pystyi vähentämään saman tiedon kirjaamista moneen otteeseen moneen eri paikkaan, jolloin tarvittava tieto löytyy helpommin sekä tiedon muuttuessa esimerkiksi rekisterin vastuuhenkilön vaihtumisen myötä myös tietojen päivittäminen on nopeampaa ja varmempaa.

Tietosuojavaltuutetun toimisto julkaisi maaliskuun 2018 lopussa mallipohjan rekisterinpitäjälle käsittelytoimien selosteesta. Taulukot 3, 4 ja 5 ovat Tietosuojavaltuutetun toimiston (2018d) sivulta ladatusta kyseisestä mallipohjasta, jossa on sekä otsikointia lukuun ottamatta tyhjä mallipohja että esimerkkipohja, josta kuvat on otettu. Omasta tietoanalyysistani puuttui mallipohjassa olevista kohdista kolmansista maista ja kansainvälisistä järjestöistä, joihin tietoa siirretään, tai tieto

siitä, että henkilötietoja ei näihin siirretä sekä mahdolliseen siirtoon liittyvä suojatoimia koskevan dokumentaation kohdat. Muuten sisältö oli pääsääntöisesti samankaltainen käsittelytoimien osalta.

Tehtävä, johon tietoja käsitellään	Käsittelyn tarkoitus	(Tarvittaessa) yhteisrekisterinpitäjä ja tämän yhteystiedot	Rekisteröityjen ryhmät
Taloushallinto	Palkanmaksu	N/A	Työntekijät
Taloushallinto	Palkanmaksu	N/A	Työntekijät
Taloushallinto	Palkanmaksu	N/A	Työntekijät
Taloushallinto	Palkanmaksu	N/A	Työntekijät
HR	Työsuhde	N/A	Työntekijät
HR	Työsuhde	N/A	Työntekijät
HR	Työsuhde	N/A	Työntekijät

Taulukko 3. Mallipohja rekisterinpitäjälle: seloste käsittelytoimista (Tietosuojavaltuutetun toimisto 2018d)

Henkilötietojen ryhmät	Vastaanottajaryhmät	Viittaus (mahdolliseen) henkilötietojen käsittelijän kanssa solmittuun henkilötietojen käsittelyä koskevaan sopimukseen	Kolmannet maat ja kansainväliset järjestöt, joihin tietoja siirretään tai tieto siitä, ettei henkilötietoja siirretä kolmansiin maihin tai kansainvälisiin järjestöihin
Yhteystiedot	HMRC	N/A	N/A
Pankkitiedot	HMRC	N/A	N/A
Eläketiedot	HMRC	N/A	N/A
Verotiedot	HMRC	N/A	N/A
Yhteystiedot	N/A	N/A	N/A
Palkkaustiedot	N/A	N/A	N/A
Vuosilomatiedot	N/A	N/A	N/A

Taulukko 4. Mallipohja rekisterinpitäjälle: seloste käsittelytoimista (Tietosuojavaltuutetun toimisto 2018d)

Asianmukaisia suojatoimia koskeva dokumentaatio, jos henkilötietoja siirretään kolmansiin maihin tai kansainvälisiin järjestöihin tietosuoja-asetuksen 49 artiklan 1 kohdan toisessa alakohdassa tarkoitetulla siirrolla	Tietojen säilytysajat, tai sen määrittämisen kriteerit	Kuvaus tietosuoja-asetuksen 32 artiklan 1 kohdan mukaisista teknisistä ja organisatorisista turvatoimista
N/A	X vuotta työsuhteen päättymisestä	Tietojen kryptaaminen
N/A	X vuotta työsuhteen päättymisestä	Tietojen kryptaaminen
N/A	X vuotta työsuhteen päättymisestä	Tietojen kryptaaminen
N/A	X vuotta työsuhteen päättymisestä	Tietojen kryptaaminen
N/A	X vuotta työsuhteen päättymisestä	Tietojen kryptaaminen
N/A	X vuotta työsuhteen päättymisestä	Tietojen kryptaaminen, pääsynvalvonta
N/A	X vuotta työsuhteen päättymisestä	Tietojen kryptaaminen, pääsynvalvonta

Taulukko 5. Mallipohja rekisterinpitäjälle: seloste käsittelytoimista (Tietosuojavaltuutetun toimisto 2018d)

Yrityksen ydintehtävänä on tuotteiden valmistaminen, ja henkilötietojen käsittely on tietyllä tavalla sivuosassa yrityksen toiminnassa, mutta niitä kuitenkin käsitellään päivittäin vähintäänkin tilauksiin liittyvien toimitusten yhteydessä. Seloste käsittelytoimista tulee kriteerien mukaan tehdä, kun muun muassa henkilötietojen käsittely ei ole satunnaista. Koska dokumentaatioita tehdessäni ei ollut tarkempaa ohjeistusta siitä, kuinka kriteereitä velvollisuudesta selosteen tekemiseksi käytännössä sovelletaan, niin päädyin siirtämään tietoanalyysin tiedot kyseiseen mallipohjaan. Muokkasin mallipohjaa niin, että mukaan tuli myös tietoanalyysiin tekemäni riskiluokitus. Tietojen siirto ei käynyt suoraan kopioimalla, sillä seloste käsittelytoimista pohjan mukaisesti tiedot eritellään hyvinkin tarkasti sen mukaan, mihin tehtävään tietoja käytetään, käsittelyn tarkoituksen sekä henkilötietojen ryhmän mukaan.

Riskiluokitus yrityksessä käsiteltävistä tiedoista on tehty kolmiportaiseksi niin, että luokkaan 1 kuuluviin tietoihin katsotaan kohdistuvan vähäinen tai ei riskiä lainkaan, luokkaan 2 huomioitava riski ja luokkaan 3 merkittävä riski. Suurin osa yrityksessä käsiteltävistä henkilötiedoista katsottiin kuuluvaksi luokkaan 1, sillä ne sisältävät lähinnä nimen ja yhteystiedon kuten puhelinnumeron ja mahdollisesti sähköpostiosoitteen sekä osoitteen. Osa tiedoista katsottiin kuuluvaksi luokkaan 2, sillä ne sisälsivät muun muassa pankkitietoja. Yrityksessä on huomioitu tietojen suojaaminen hyvin ja niiden käsittely on hyvin huolellista, joten tässä vai-

heessa mihinkään tietoihin ei katsottu kohdistuvan merkittävää riskiä, mutta mikäli yrityksessä esimerkiksi vaihdettaisiin sähköistä järjestelmää, tulisi tilannetta arvioida uudelleen, sillä käsiteltävien tietojen tulee pysyä turvattuna ja muuttumattomina myös tiedonsiirron ajan.

4 POHDINTA

EU:n yleinen tietosuoja-asetus on varsin laaja kokonaisuus, ja se tuo mukanaan monia uusia muutoksia ja velvollisuuksia. Valmistautuminen asetukseen teettää paljon työtä, sillä organisaatioilla on luotava iso joukko erilaisia dokumentteja henkilötietojen käsittelystään ja niiden toteuttaminen vaatii asioihin perehtymistä. Luettavaa materiaalia on paljon ja tiedon tiivistäminen tuo omat haasteensa sillä tavoitteena on pyrkiä tuomaan esille oleellisimmat seikat. Lisäohjeita ja tarkennuksia asetuksen eri kohtien soveltamiseen julkaistaan todennäköisesti tämän opinnäytetyön valmistumisen jälkeenkin ja lisäksi ajan myötä käytännöt tulevat myös muovautumaan sekä vakiintumaan.

Opinnäytetyön tiedonkeruussa keskeisessä osassa oli harjoittelun aikana tehty käytännön havainnointi sekä henkilöstöltä saatu hyvä ja kattava tieto henkilötietojen käsittelystä. Ilman tätä hyvää ja luottamuksellista tiedonsaantia ei dokumentaation ja opinnäytetyön tekeminen olisi ollut mahdollista. Tietosuoja-asiat olivat sinänsä yrityksessä jo hyvin huomioitu ja suurin työ olikin kerätä ja kirjata ylös näitä tietoja sekä koota niistä mahdollisimman johdonmukainen ja käytännöllinen kokonaisuus yrityksen käyttöön.

Laatimani asiakirjakokonaisuus ei laajuudestaan huolimatta sekään ole täydellinen kokonaisuus asetuksen täyttämiseksi, mutta se täyttää ne tavoitteet, jotka opinnäytetyölle asetettiin. Tietojenkäsittelysopimusten sekä teknisen suojauksen osalta tietoja lisätään dokumentaatioon yrityksen toimesta ja näin täydennetään asetuksen vaatimuksia. Tehdyt valinnat pohjautuvat tutkittuun teoriatietoon, tehtyihin havaintoihin sekä kyselyvastauksiin, ja ne on myös perusteltu, mikä osaltaan kasvattaa tehdyn työn luotettavuutta.

Tutkimusta voisi laajentaa ja kehittää edelleen esimerkiksi koskemaan jonkin tietyn alueen tai toimialan yrityksiä ja selvittää, kuinka niissä on tietosuoja-asetuksen voimaantulo huomioitu. Myöhemmin tehtävässä tutkimuksessa voisi selvittää myös sitä, kuinka asetus on käytännössä näkynyt yrityksen tai yritysten toiminnassa: ovatko rekisteröidyt esittäneet pyyntöjä koskien henkilötietojensa käsittelyä tai tietojensa siirtoa järjestelmästä toiseen?

Perehtyminen tietosuoja-asetukseen toi lisää ammatillista tietoutta ja varmuutta omaan toimintaan. Saadusta tiedosta on hyötyä paitsi ammatillisesti niin myös henkilökohtaisessa elämässä, sillä hyvin monissa liiketalouden työtehtävissä käsitellään henkilötietoja ainakin jollakin tasolla ja myös omien henkilötietojen käsittelyyn ja tietojen luovuttamiseen on hyvä kiinnittää huomiota.

LÄHTEET

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Helsinki: Tietosanoma.

Article 29 Data Protection Working Party 2018a. Guidelines on Personal data breach notification under Regulation 2016/679. Päivitetty 6.2.2018. Viitattu 12.2.218 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimis-to/oppaat/zzKfe6Nbj/Guidelines_on_Personal_data_breach_notification_under_Regulation_2016679.pdf.

Article 29 Data Protection Working Party 2018b. Guidelines on transparency under Regulation 2016/679. Viitattu 10.4.2018. file:///C:/Users/Terhi/Downloads/wp260_enpdf.pdf.

EU:n tietosuoja-asetus 679/2016/EU. Viitattu 9.4.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL.

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

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkea-koulu.

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan opinnäytetyön vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2015. Kehittämistutkimuksen kirjoittamisen käytännön opas. Miten kirjoitan kehittämistutkimuksen vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Lantto, P. 2018. Profin Oy. Keskustelu tehdaspäällikön kanssa 30.1.2018.

Lehtinen, R. 2018. GDPR haltuun – 113 päivää aikaa toimia! Tiivistetty webinaarimateriaali, GDPR-taulukot ja tarkistuslista. Viitattu 13.4.2018. http://images.efficiency.visma.com/Web/Visma/%7B791de053-6bb9-4e80-b7ad-d3e71e725e3c%7D_GDPR-esitys_ja_taulukot.pdf.

Lehtola, S. 2018. Profin Oy. Toimistopäällikön haastattelu 7.2.2018.

Oikeusministeriö 2018. Tietosuojalaki täydentäisi EU:n tietosuoja-asetusta. Tiedote 1.3.20118. Viitattu 13.3.2018. http://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojalaki-taydentaisi-eu-n-tietosuoja-asetusta.

Opi Tietosuojaa 2018a. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. Viitattu 29.1.2018. https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus.

Opi Tietosuojaa 2018b. Yleistä tietosuojasta. Viitattu 13.4.2018. https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuoja.

Profin Oy 2017. Viitattu 9.4.2018. http://profin.fi/profin-oyssa-juhlittiin-40-vuotista-yritystaivalta/.

Profin Oy. 2018. Yritys. Viitattu 9.4.2018. http://profin.fi/yritys/.

Rakennuslehti 2013. Profin osti Sydänpuu Ikkunat & Ovet – liiketoiminnot. Viitattu 8.11.2017.https://www.rakennuslehti.fi/2013/11/profin-osti-sydanpuu-ikkunat-ovet-liiketoiminnot/.

Riekki, K. 2018. Profin Oy. Sähköposti toimistosihteeriltä 8.2.2018.

Tietosuojatyöryhmä 2017a. Tietosuojavastaavia koskevat ohjeet. Julkaistu 13.12.2013. Päivitetty 5.4.2017. Viitattu 10.4.2018. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimis-to/oppaat/UvreCmOiN/Tietosuojavastaavia_koskevat_ohjeet_wp243rev01_fi.pdf.

Tietosuojatyöryhmä 2017b. Ohjeet tietosuojaa koskevasta vaikutuksenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”. Viimeksi tarkastettu ja hyväksytty 4.10.2017. Viitattu 13.2.2018. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimis-to/oppaat/ibVehxmcp/Ohjeet_tietosuojaa_koskevasta_vaikutustenarvioinnista.pdf.

Tietosuojavaltuutetun toimisto 2017a. Henkilötietojen tietoturvaloukkaukset. Viitattu 12.2.2018. Julkaistu 5.12.2017. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/tietoturvaloukkaukset.html.

Tietosuojavaltuutetun toimisto 2017b. Tietosuojavastaavat. Julkaistu 5.12.2017. Viitattu 7.2.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/tietosuojavastaavat.html.

Tietosuojavaltuutetun toimisto 2018a. EU:n tietosuojauudistus. Julkaistu 15.6.2015. Päivitetty 21.2.2018. Viitattu 17.4.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html#miksitietosuojalaitmuuttuvat.

Tietosuojavaltuutetun toimisto 2018b. Erityisten henkilötietojen käsittely. Julkaistu 29.3.2018. Viitattu 12.4.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/erityistenhenkilotietoryhmienkasittely.html.

Tietosuojavaltuutetun toimisto 2018c. Informointikäytännöt. Julkaistu 13.4.2018. Viitattu 15.4.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/informointikaytannot.html.

Tietosuojavaltuutetun toimisto 2018d. Seloste käsittelytoimista. Julkaistu 23.3.2018. Päivitetty 26.3.2018. Viitattu 28.3.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/selostekasittelytoimista.html.

Valtiovarainministeriö 2016. EU-tietosuojan kokonaisuudistus. VAHTI-raportti – 1/2016. Viitattu 5.2.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128.

Vuodesta sataan – sähköisten asiakirjojen hallinta ja säilyttäminen 2009. Liikearkistoyhdistys ry. Julkaisu nro 18. Helsinki: Kirjapaino Laine Direct Oy.

Yrittäjät 2018. Yrittäjän tietosuojaopas. Viitattu 22.3.2018. https://www.yrittajat.fi/sites/default/files/yrittajat_tietosuojaopas_2018.pdf.

LIITTEET

Liite 1. Rekisteri- ja tietosuojaseloste: Asiakas- ja markkinointirekisteri

Liite 1 1(4)

Rekisteri- ja tietosuojaseloste – Asiakas- ja markkinointirekisteri

1. **Rekisterinpitäjä**

   Profin Oy
   Y-tunnus: xxxxxxx-x
   xxxxxxx
   xxxxx xxxxxxxxxx

2. **Yhteyshenkilö rekisteriä koskevissa asioissa**

   X X
   x.x @ xxxxxx.xx
   p. xxx xxx xxxx

3. **Rekisterin nimi**

   Asiakas- ja markkinointirekisteri

4. **Rekisteröidyt henkilöt**

   Profin Oy:n asiakkaat ja uusasiakkaat

5. **Henkilötietojen käsittelyn tarkoitus**

   Henkilötietojen käsittelyn tarkoituksena on rekisteröidyn ja Profin Oy:n väliseen asiakassuhteeseen liittyvien asioiden hoitaminen. Oikeusperusteena käsittelylle on asiakkaan ja Profin Oy:n välinen sopimus ja siitä johtuvat lakisääteiset velvoitteet.

   Keräämme ja käsittelemme ainoastaan sellaisia henkilötietoja, jotka ovat tarpeen tarjouksen ja sopimuksen tekemiselle Henkilötietojen antaminen on edellytys tarjouksen ja sopimuksen tekemiselle eli tarjousten ja tilausten toimittamista ei voida suorittaa ilman asiakkaan antamia henkilötietoja.

6. **Rekisterin tietosisältö**

   Rekisteriin talletetaan
   - yksityisasiakkaalta nimi ja yhteystiedot sekä tilauksen valmistumisen jälkeen työmaalla toimituksen vastaanottavan henkilön nimi ja puhelinnumero, mikäli eri kuin asiakas
   - yritysasiakkaalta yrityksen nimi, Y-tunnus, yhteyshenkilön nimi ja yhteystiedot sekä toimitusosoite
   - tilausta koskevat välttämättömät tiedot, kuten laskutusta koskevat tiedot

Uusasiakashankinnassa talletetaan

- uusasiakashankinnassa yksityisasiakkaan nimi ja yhteystiedot tai yritysasiakkaan ollessa kyseessä yrityksen nimi, yhteyshenkilön nimi ja yhteystiedot
- tarjousta koskevat välittömät tiedot kuten kohteen tarvittavat mitat

Uusasiakashankinnan eli tehtyjen tarjousten osalta tietoja säilytetään 5 vuoden ajan.

Toteutuneiden tilausten kohdalta tietoja säilytetään asiakassuhteen keston ajan sekä 10 vuotta sen jälkeen, kattaen näin sekä 5 vuoden takuuajan, että mahdolliset yrityksen sisäiset raportointitarpeet. Lisäksi asiakkaalla on tuona aikana myös tarvittaessa mahdollisuus saada tietoonsa esimerkiksi tilauksessa käytetyn värimallin numero tai muita mahdollisesti tarvittavia tietoja.

7. Säännönmukaiset tietolähteet

Rekisteriin tulevat henkilötiedot tulevat suoraan asiakkaalta ja rekisterissä oleva tilausta koskeva muu tieto kerätään asiakassuhteen eri vaiheissa. Työmaalla mahdollisesti toimivan yhteyshenkilön, joka on eri kuin asiakas, nimi ja yhteystiedot saadaan asiakkaalta.

Uusasiakashankinnassa henkilötiedot ja tarjouksen tekemistä varten tarvittava muu tieto tulevat asiakkaalta itseltään.

8. Tietojen säännönmukaiset luovutukset

Toteutuneissa tilauksissa tietoja voidaan luovuttaa yhteistyötahoille ja alihankkijoille seuraavia tehtäviä varten

- toimitusta ja laskutusta varten tarvittavat tiedot
- mahdollista asennusta varten tarvittavat tiedot
- tilaukseen mahdollisesti liittyvien välitystuotteiden valmistukseen ja toimittamiseen oleellisesti liittyvät tiedot

Uusasiakashankinnan tietoja voidaan luovuttaa vain Profin Oy:n sisällä.

9. Tietojen siirto EU:n tai ETA:n ulkopuolelle

Rekisterin tietoja ei luovuteta EU:n tai ETA:n ulkopuolelle.

10. Rekisterin suojauksen periaatteet

a. Manuaalinen aineisto
   Rekisteriin saatua manuaalista tietoaineistoa tai rekisteristä tulostettua aineistoa käsittelevät vain ne henkilöt ja siinä laajuudessa

kuin asiakassuhteeseen tai tehdyn tilauksen toimittamiseen liittyvän asian hoito edellyttää.

Tarpeeton aineisto poistetaan tietoturvallisesti noudattaen tietojen säilyttämisestä annettuja ohjeita ja päätöksiä.

b. ATK:lla käsiteltävät tiedot
Sähköinen aineisto kerätään tietokantoihin, jotka ovat suojattu salasanoin, palomuurein sekä muilla teknisillä toimilla. Pääsy rekisterin tietoihin on vain niillä henkilöillä ja siinä laajuudessa kuin tilattuun toimitukseen ja asiakassuhteeseen liittyvän asian hoito edellyttää.

Tarpeeton aineisto poistetaan tietoturvallisesti noudattaen tietojen säilyttämisestä annettuja ohjeita ja päätöksiä.

11. Rekisteröidyn oikeudet

- Rekisteröidyllä on oikeus saada tietoonsa ja tarkistaa rekisterissä hänestä olevat tiedot tai saada tietää, ettei rekisterissä ole häntä koskevia tietoja.

- Rekisteröidyllä on oikeus pyytää rekisterissä olemassa olevien itseään koskevien tietojen oikaisemista ja poistamista sekä täydentää olemassa olevia tietoja.

- Rekisteröidyllä on oikeus pyytää henkilötietojensa käytön rajoittamista.

- Rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä.

- Rekisteröidyllä on oikeus pyytää sellaisten henkilötietojen siirtämistä järjestelmästä toiseen, jotka perustuvat rekisteröidyn suostumukseen tai sopimukseen, jossa rekisteröity on osapuolena.

- Rekisteröidyllä on oikeus peruuttaa suostumuksena henkilötietojensa käsittelyyn, suostumuksen peruuttaminen ei vaikuta peruuttamista edeltävään lainmukaiseen käsittelyyn.

Rekisteröityjen oikeuksissa, kuten esimerkiksi tietojen oikaisemisessa, poistamisessa ja käytön rajoittamisessa huomioidaan yrityksen lakisääteiset velvollisuudet rekisterinpitäjänä.

Pyynnöt tulee esittää joko sähköpostilla tai kirjeenä kohdassa 2. olevalle yhteyshenkilölle**.**

12. Profilointi ja automaattinen päätöksenteko

Yritys ei tee asiakkaistaan profilointeja eikä automaattisia päätöksiä.

13. Valvontaviranomainen

Rekisteröidyllä on oikeus tehdä valitus tietosuojavaltuutetulle, jos hän katsoo tietosuoja-asetukseen perustuvien oikeuksiensa tulleen loukatuksi.