Haverinen Jenna ja Juvonen Salla

EU:n tietosuoja-asetuksen mukainen henkilötietojen käsittely yrityksessä - Case yritys X

Liiketalous

Taloushallinto & juridiikka

Kevät 2018

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tiivistelmä

Tekijä(t): Haverinen Jenna & Juvonen Salla

Työn nimi: EU:n tietosuoja-asetuksen mukainen henkilötietojen käsittely yrityksessä - Case yritys X

Tutkintonimike: Tradenomi (AMK), taloushallinto ja juridiikka

Asiasanat: EU:n tietosuoja-asetus, arkistointisuunnitelma, tietosuoja, tietoturva, henkilötietojen käsittely

Opinnäytetyössä tarkasteltiin yritys X:n arkistointia ja henkilötietojen käsittelyä sekä sitä, kuinka niitä voidaan parantaa. Käytetty teoria-aineisto pohjautui pääasiallisesti tietosuoja-asetukseen ja arkistointikirjallisuuteen. Työn teoriaosuudessa esiteltiin tietosuojan ja tietoturvan peruskäsitteitä, suurimmat EU:n tietosuoja-asetuksen henkilötietojen käsittelyyn tuomat muutokset ja arkistointisuunnitelman osa-alueet. Opinnäytetyö oli kehittämistyö, jonka tarkoituksena oli tuottaa yritykselle arkistointisuunnitelma, nykytila-analyysi henkilötietojen käsittelystä sekä dokumentaatio, joka toimii todisteena EU-tietosuoja-asetuksen mukaisesta henkilötietojen käsittelystä. Nykytila-analyysissa kartoitettiin yrityksen tietosuojariskejä ja laadittiin raportti tarvittavista muutoksista henkilötietojen käsittelyyn. Arkistointisuunnitelman tarkoituksena oli antaa yrityksen työntekijöille ohjeistus arkistointitoimenpiteistä ja paperisten asiakirjojen säilytysajoista.

Nykytila-analyysin pohjalta yritykselle laadittiin Word-muotoinen dokumentaatio EU:n tietosuoja-asetuksen mukaisesta henkilötietojen käsittelystä. Dokumentaation laadinnan yhteydessä täytettiin myös erilliset lomakemuotoiset tietosuojaselosteet yrityksessä olevista rekistereistä. Dokumentaatiosta ilmenee, mitä rekistereitä yrityksellä on käytössään ja mitä henkilötietoja niihin on kerätty. Lisäksi siinä kerrotaan, miksi yritys kerää henkilötietoja ja mihin se niitä käyttää. Dokumentaatiolla yritys voi todistaa viranomaisille, että se käsittelee henkilötietoja EU:n tietosuoja-asetuksen asettamien vaatimusten mukaisesti.

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Abstract

Author(s): Haverinen Jenna & Juvonen Salla

Title of the Publication: Processing of personal data according to the EU Data Protection Regulation – Case Company X

Degree Title: Bachelor of Business Administration

Keywords: EU's Data Protection Regulation, archiving plan, data protection, data security, processing of personal data

The thesis investigated archiving and processing of personal data at company X as well as methods to improve them. The theoretical part of the thesis is based mainly on the EU Data Protection Regulation and archiving literature. It introduces the basic concepts of data protection and security, the biggest changes brought in personal data processing by the EU Privacy Policy as well as components of an archiving plan. The thesis was development work and its purpose was to create an archiving plan, a current-state analysis of personal data processing and a documentation that would serve as evidence of personal data processing being done in accordance with the EU Data Protection Regulation. The current-state analysis surveyed the company's data protection risks and prepared a report on the changes necessary in processing of personal data. The objective of the archiving plan was to provide the employees of the company with instructions on archiving measures and preservation of paper documents.

Based on the results of the current-state analysis, a Word document was prepared for the company for processing personal data in accordance with the EU Data Protection Regulation. When the documentation was compiled, separate privacy policy forms were also filled in of the company registers. The documentation shows the records the company has and the personal information it has collected. It also explains why the company collects personal data and where it uses the collected personal data. With the documentation, the company can prove to the authorities that it processes personal data in accordance with the requirements of the EU Privacy Policy.

Sisällys

1 Johdanto

Euroopan unionin tietosuojalainsäädäntö uudistui vuonna 2016 voimaan tulleen yleisen tietosuoja-asetuksen myötä. Jokaisen EU-alueen yrityksen täytyy muuttaa henkilötietojen käsittely tietosuoja-asetuksen mukaiseksi 25.5.2018 mennessä, jolloin kahden vuoden siirtymäaika umpeutuu. Asetus tuo yrityksille uusia velvoitteita henkilötietojen käsittelyn suhteen sekä uusia oikeuksia luonnollisille henkilöille. Koska asetuksen myötä yritykset ovat velvollisia tarvittaessa osoittamaan viranomaiselle noudattavansa tietosuoja-asetusta, on yritysten tärkeää päivittää henkilötietojen käsittelynsä ennen siirtymäajan umpeutumista. Osassa yrityksissä tietosuoja-asetuksen huolehtimisesta vastaa jo tietosuojavastaava, jonka yritys onkin asetuksessa mainittujen ehtojen täyttyessä velvollinen nimeämään. Toimeksiantajayritys X ei ole velvollinen hankkimaan tietosuojavastaavaa, joten he päättivät hyödyntää opiskelijoita tietosuoja-asetuksen mukaisen toiminnan saavuttamisessa. Opinnäytetyön aihe saatiin täten koulun kautta.

Opinnäytetyö on toiminnallinen opinnäytetyö, jossa tarkastellaan sekä henkilötietojen käsittelyä että arkistointia. Tavoitteena on toimeksiantajayrityksen EU:n tietosuoja-asetuksen mukainen henkilötietojen käsittely ja tarkoituksena tehdä nykytila-analyysi toimeksiantajan henkilötietojen käsittelystä, tietosuoja-asetuksen vaatima dokumentaatio sekä arkistointisuunnitelma. Nykytila-analyysissa kartoitetaan mahdolliset tietosuojariskit toimeksiantajan toiminnassa ja laaditaan raportti henkilötietojen käsittelyyn tehtävistä muutoksista. Toiminnallisessa osuudessa tehdään myös dokumentaatio, jolla yritys voi todistaa tarvittaessa viranomaisille noudattavansa tietosuoja-asetuksen vaatimuksia. Dokumentaation liitteeksi täytetään lomakemuotoiset tietosuojaselosteet yrityksen rekistereistä. Henkilötietojen käsittely on voimakkaasti yhteydessä arkistointiin ja täten yritykselle tehdään myös arkistointisuunnitelma, jossa otetaan huomioon uudistunut lainsäädäntö. Opinnäytetyön toiminnallisessa osuudessa kuvataan, kuinka edellä mainitut tuotokset on laadittu ja millaiset niistä tuli.

Opinnäytetyön toimeksiantaja on 1950-luvulla perustettu suomalainen puualan yritys. Yritys aloitti sahatoiminnan harjoittamisen vuonna 1959 ja sen asiakkaita ovat yritykset sekä satunnaiset luonnolliset henkilöt. Yritys valmistaa melkein kaikkia sahateollisuuden tuotteita, jotka ovat tarpeen vaatiessa mahdollista räätälöidä asiakkaan tarpeiden mukaisiksi. Yrityksen sahatavaran tuotantokapasiteetti on 400 000 m3 vuodessa.

Sahatavaratuotannon yhteydessä syntyy myös sivutuotteita, joita ovat muun muassa sahanpuru, kuituhake, kuivamurske ja kuori. Sahatoiminnan lisäksi yrityksen toimenkuvaan

kuuluu keskeisesti sahatavarakaupan käyminen kansainvälisesti; yritys toimittaa sahatavaraa 30 vientimaahan. Yrityksen suurin vientimaa on Egypti. Viime vuosina myös vienti Kaukoitään on kasvanut, mutta suurimmat markkinat ovat kuitenkin edelleen kotimaassa. Yritys hoitaa itse henkilöstö- ja palkkahallinnon tehtävät, joten yrityksessä toimii henkilökuntaa myös palkkahallinnossa, kirjanpidossa sekä reskontrassa. Täten henkilötietojen käsittely on osalle yrityksen henkilöstöstä jokapäiväistä toimintaa, joten EU:n tietosuoja-asetuksen noudattaminen on tärkeää.

2 Tietosuoja

Tietosuojalla (data protection) tarkoitetaan vakiintunutta ilmaisua, jota käytetään puhuttaessa henkilötietojen suojan oikeudellisesta säätelystä. Ilmaisua käytetään kansainvälisesti ja se on laajalti käytössä myös Suomessa. Tietosuoja ei suojaa vain tietoja, vaan se turvaa itse tiedon kohteen (data subject). Se turvaa myös luonnollisen henkilön oikeuksia, etuja ja yksityisyyttä. Tietosuoja-termi ei erikseen ota huomioon yksilöä, vaan sillä tarkoitetaan vain keinoa, jonka avulla suojataan henkilötietoja. Tietosuojalainsäädännön päätarkoituksena on laaja yksityisyyden suojaaminen. Tietosuoja-käsite on ollut käytössä jo kauan ja sen suuresta merkityksestä kertovat useat säädökset ja erityislait, jotka ovat astuneet voimaan vuoden 1988 jälkeen, jolloin hyväksyttiin henkilörekisterilaki. (Alapuranen, Heino, Koskinen & Lehtonen 2012, 40.)

Tietosuojaperiaatteisiin kuuluu, että yksilöstä voidaan kerätä tietoja vain, jos hän on antanut suostumuksensa. Tietojen keräämisen tulee olla myös rekisterinpitäjän toiminnan kannalta tarpeellista ja tietojen täytyy olla virheettömiä. Yksilöllä on oikeus vaatia virheellisten tietojen korjaamista. Kerättyjä tietoja ei saa käyttää muuhun tarkoitukseen, kuin mihin ne on tarkoitettu. Tietosuojaperiaatteiden mukaan ihmisten tietoja ei myöskään saa luovuttaa ulkopuolisille ilman suostumusta. (Tietosuojavaltuutetun toimisto 2013.) Kuitenkaan pelkät henkilötiedot, kuten henkilön osoite ja nimi, eivät aina ole salaisia, mutta tietosuojalait suojaavat ihmisiä heidän henkilötietojensa aiheettomalta keräämiseltä. Tarpeeton henkilötietojen rekisteröinti ja kerääminen sekä näiden tietojen yhdistely eri lähteistä saattavat aiheuttaa vahinkoa. (Järvinen 2002, 30.)

2.1 Tietoturva

Tietosuoja ja tietoturva liittyvät läheisesti toisiinsa. Tietoturva-termillä tarkoitetaan sitä perustaa, jolle luottamuksellisten tietojen käsittely rakentuu. Yrityksille tärkeinä tietoina voidaan pitää muun muassa palkkoihin, henkilöstöön sekä myyntilukuihin liittyviä tietoja. Laajasti ajateltuna tietoturvaan voidaan katsoa kuuluvaksi kaikki sellaiset asiat, mitkä liittyvät tietojen oikeellisuuteen ja saatavuuteen. Tietoturva pyrkii kattamaan myös tietojen luottamuksellisuuden säilymisen säilytyksen, käsittelyn sekä tiedonsiirron aikana. (Järvinen 2002, 21.) Tietoturva pyrkii suojaamaan tietojärjestelmiä ja niiden sisältämiä tietoja sekä takaamaan järjestelmien toiminnan olosuhteista riippumatta (Järvinen 2012, 12).

Tietoturvan tavoitteina ovat tietojen eheys, luottamuksellisuus, kiistämättömyys, vastuullisuus, todennus sekä saatavuus. Eheydellä (integrity) tarkoitetaan tietojen luotettavuuden ja virheettömyyden turvaamista. Sen avulla varmistetaan, että tiedot eivät ole päässeet muuttumaan tai tuhoutumaan ihmisen toiminnan tai muiden ulkoisten tapahtumien aikaansaannoksena. Luottamuksellisuuden (confidentiality) tavoitteena on pitää tiedot kaikissa käsittelyn vaiheissa salaisina niin, että ne ovat vain oikeutettujen henkilöiden käytettävissä. Kiistämättömyyden (non-repudiation) tavoitteena on, että kaikki tietoihin liittyvät tapahtumat on mahdollista jälkeenpäin todistaa luotettavasti. Tämä myös estää sen, ettei osapuolilla ole jälkikäteen mahdollisuutta kiistää osuuttaan tietojenkäsittelyyn. Vastuullisuudella (accountability) tarkoitetaan, että tietojen muuttamisesta ja käyttämisestä jää jäljet, joiden avulla voidaan jälkikäteen selvittää ketkä ovat käsitelleet tietoja. Todennuksen (authenticity) tavoitteena on varmistaa käyttäjien ja osapuolten luotettava tunnistaminen. Saatavuudella (availability) tarkoitetaan, että tiedot ovat kaikkien niiden käyttöön oikeutettujen henkilöiden käytettävissä. (Pitkänen, Tiilikka & Warma 2013, 215–216.)

Teknisiä järjestelmiä sekä koneita ei ole vaikea hallita ja ne on helppo saada toimimaan halutulla tavalla. Asiat muuttuvat vaikeasti hallittaviksi silloin, kun järjestelmien käyttäjinä on ihmisiä. Ihmiset eivät aina noudata ohjeita, tekevät virheitä ja voivat tahallaan aiheuttaa vahinkoa. Tietosuojan sekä tietoturvan ongelmissa olisi kannattavampaa kohdistaa ratkaisut henkilöstöön teknisten laitteiden sijasta. (Järvinen 2002, 47.) Tietoturvan tulee olla yhtenä osana organisaation toiminnan suunnittelua ja johtamista. Tämän saavuttamiseen tarvitaan johdon tukea. Organisaation täytyy varata tietoturvan toteuttamista varten tarpeeksi suuret resurssit sekä ohjausmekanismit. Tietoturvan tavoitteet voidaan saavuttaa ottamalla tarvittavat toimenpiteet mukaan organisaation riskienhallintaan. (Pitkänen ym. 2013, 220.)

2.2 Uhat ja riskit

Tietoturvaan kohdistuu jatkuvasti erilaisia uhkia, joilta yrityksen tulee pyrkiä suojautumaan. Uhat voivat olla yrityksen sisäisiä tai tulla sen ulkopuolelta. Suurin tietoturvauhka on yrityksen henkilöstö. Jokainen työntekijä tekee joskus inhimillisiä virheitä, joiden seurauksena saattaa pahimmassa tapauksessa olla tietovuoto. (Jyväskylän yliopisto 2010.) Niin uudet kuin vanhatkin työntekijät voivat välittää salassa pidettäviä tietoja yrityksen ulkopuolelle, tarkoituksenmukaisesti tai huolimattomuuttaan. Tältä uhalta voidaan suojautua parhaiten kouluttamalla ja opastamalla henkilökuntaa asiaan liittyen, jotta heillä on ajantasaista tietoa oikeaoppisista toimintatavoista. (Viestintävirasto 2017.)

Henkilöstön lisäksi yleisimpiä yritysten uhkia ovat päivitysten laiminlyönti, tietomurrot ja varkaudet, huijaukset, roskapostit sekä tietoturva-aukot. Jos yritys ei päivitä tasaisin väliajoin käyttämiään ohjelmia ja järjestelmiä, on erilaisten haittaohjelmien sekä virusten helpompi päästä käsiksi sen tietojärjestelmään. Haittaohjelmat ja virukset tulevat useimmiten tietokoneelle erilaisten tiedostojen, Internetin tai sähköpostin välityksellä. Tietomurtojen ja varkauksien estämiseksi tietoturvan suojatoimenpiteiden tulee olla hyvässä kunnossa, sillä koko ajan kehittyvä teknologia on lisännyt hakkereiden mahdollisuuksia päästä salaisiin tietoihin. Jos henkilö murtautuu suojaamattomalle tai suojatulle tietokoneelle ja käyttää sitä sekä sen sisältämiä tietoja luvatta, on kyseessä tietomurto. Yrityksen sähköpostien kautta voidaan pyrkiä pääsemään käsiksi yrityksen tietoihin erilaisten huijaus- ja roskapostien avulla. Asiantuntijoiden käyttäminen yrityksen tietoturvan luomisessa sekä ylläpitämisessä on tärkeää, erityisesti tietoturva-aukoilta välttymisen kannalta. Tietoturva-aukko syntyy, jos tietojärjestelmän osassa tai sen suojauksessa on heikkous, joka mahdollistaa murtautumisen järjestelmään. (Jyväskylän yliopisto 2010.)

Tietojen suojaamiseen ja turvaamiseen liittyy aina riski. Tapahtuessaan riski voi haitata tai estää tietojen käytön. Pahimmillaan ne saattavat myös uhata tietojen olemassaoloa. Riskit voivat johtaa esimerkiksi tietojen väärentämiseen, katoamiseen tai tuhoutumiseen. Lisäksi ne voivat johtaa tietojen vääränlaiseen tulkintaan sekä inhimillisiin virheisiin. Tietojen turvaamisen päätavoitteena on riskien tunnistaminen ja niihin varautuminen. Kaikkiin riskeihin ei ole mahdollista varautua eikä epätodennäköisiin riskeihin varautuminen ole kustannukset huomioon ottaen kannattavaa. (Tammisalo 2005, 10.)

Sähköisten arkistojen ja rekisterien käyttöönotto on tuonut mukanaan uusia mahdollisuuksia, mutta se on myös lisännyt riskejä. Valtakunnalliset arkistot ja rekisterit ovat tehneet tiedon varastoimisen helpommaksi. Esimerkiksi potilastietojen sähköinen käsittely on helpottanut tietojen siirtämistä sinne, missä potilas saa hoitoa. (Andreasson, Koivisto & Ylipartanen 2014, 51.)

Rekisterinpito ja tietojen käsittely on hajaannutettu. Rekisterinpitäjä voi antaa työntekijöilleen käyttöoikeudet arkistoihin ja rekistereihin. Työntekijä kuitenkin itse tekee päätöksen siitä, kuinka hän käyttää rekisterinpitäjältä saamiaan käyttöoikeuksia. Käyttöoikeuksien väärinkäyttö on tietosuojariski. Käyttöoikeuksien väärinkäytön tapahtuessa on valvonnan tehtävänä etsiä, kuka on tietojen urkinnan takana ja saada henkilö vastaamaan teoistaan. Tietosuojaloukkauksen tehneen henkilön kiinnijäämisriski on kuitenkin valitettavan pieni. (Andreasson ym. 2014, 51.)

2.3 Suojausmenetelmät

Riskien aikaansaamat vaikutukset voivat olla samat, vaikka sen aiheuttajat ovat erilaiset. Tämän seurauksena riskeiltä suojautumisessa käytetään useita erilaisia menetelmiä. Uhat ja riskit on tärkeää tuntea mahdollisimman hyvin ja yksityiskohtaisesti. Tämä helpottaa niiden seurauksien selvittämistä ja mahdollistaa varatoimenpiteiden suunnittelun. Tällöin suojaustoimenpiteet kohdistuvat suoraan riskiin. Tietyt suojaustoimenpiteet suojaavat eri tietoja useilta riskeiltä. (Tammisalo 2005, 10.)

Rekisterinpitäjällä on velvollisuus pitää huolta henkilötietojen suojaamisesta. Tämä sama velvollisuus koskee sellaisia elinkeinonharjoittajia, jotka toimivat rekisterinpitäjän lukuun. Velvollisuus koskee myös sitä henkilöä, jolle rekisterinpitäjä mahdollisesti luovuttaa tietoja teknisen käyttöyhteyden kautta. Rekisterinpitäjän tulee sekä suunnitella että toteuttaa tarvittavat organisatoriset eli hallinnolliset ja tekniset toimenpiteet henkilötietojen suojelemiseksi. Toimenpiteet suojelevat henkilötietoja vahingossa tai tahallisesti tapahtuvalta tuhoamiselta, muuttamiselta, häviämiseltä ja luvattomalta luovuttamiselta. (Pitkänen ym. 2013, 220.)

Organisaation suojauksen vaatimustasossa tulee ottaa huomioon suojaukseen käytettävissä olevat tekniset keinot, sekä niihin liittyvät kustannukset. Näitä verrataan tietojenkäsittelyn aiheuttamiin riskeihin ja suojeltavaan tietoon. (Pitkänen ym. 2013, 222.) Organisatoriset ja tekniset toimenpiteet täytyy myös muistaa päivittää säännöllisesti (Vanto

2011, 139). Tarvittavaan suojauksen tasoon vaikuttaa se, millaisia henkilötietoja käsitellään. Esimerkiksi arkaluonteisia tietoja sisältävän rekisterin suojaamiseen tulee kiinnittää huomiota. Tällaisten tietojen joutuminen ulkopuolisten käsiin saattaa aiheuttaa suuren vahingon. Arkaluontoisten tietojen suojaamiseksi edellytetään normaalia suurempia toimenpiteitä. (Pitkänen ym. 2013, 222.)

Tietoturvan suojausmenetelmät voidaan jakaa kolmeen eri ryhmään; tekniset, fyysiset sekä hallinnolliset menetelmät. Tekniset menetelmät pohjautuvat ohjelmistojen ja laitteistojen tietoturvaratkaisuihin. Niiden avulla pyritään poistamaan mahdolliset tietoturvapuutteet laitteistoista ja ohjelmistoista. Teknisiä suojautumismenetelmiä ovat esimerkiksi palomuurit, automaattiset virustarkistukset, erilaiset tunnistamismenetelmät sekä salatut tiedonsiirtoyhteydet. Fyysisillä menetelmillä pyritään, nimen mukaisesti, estämään tunkeilijan pääsy fyysisesti käytettäville tietokoneille tai lähiverkkoon. Näitä keinoja ovat muun muassa kulunvalvonta, tilojen lukitseminen, tarvittavien tietojen ja ohjelmistojen varmuuskopiointi sekä kaapeleiden sijoittaminen turvalliseen ja eristettyyn tilaan. Kolmas ryhmä, hallinnolliset menetelmät, tarkoittaa käyttäjien toimitapoja sekä heille myönnettyjä oikeuksia. Siihen sisältyy myös tietojärjestelmiä hallinnoivien henkilöiden tietoturvaratkaisujen oikeanlainen, huolellinen ja suunniteltu toteuttaminen. Hallinnollisia suojauskeinoja ovat esimerkiksi käyttäjien tietoturvaosaamisen lisääminen, salasanojen ja käyttäjätunnusten asianmukainen säilytys sekä sovittujen tietoturvaratkaisujen noudattaminen. (Jyväskylän yliopisto 2010.)

Suojaamistoimenpiteitä ja niiden tarvetta arvioidessa täytyy ottaa huomioon tiedon laadun lisäksi myös tietojen ikä. Lisäksi tulee kiinnittää huomiota käsiteltävien tietojen määrään. Jos tietoja on paljon, tarvitaan tavallista kalliimpia toimenpiteitä niiden suojaamiseksi. Käsiteltävien tietojen pieni määrä ei ole kuitenkaan pätevä syy huolellisuus- tai suojaamisvelvollisuuden lieventämiseksi. (Pitkänen ym. 2013, 220.)

Rekisterinpitäjän tehtävänä on määritellä tietojen käyttöoikeudet sekä käsittelyyn liittyvät tavat, kuten haku, tuhoaminen ja tallennus. Tietojärjestelmät voivat antaa mahdollisuuden siihen, että eri henkilöille luovutetaan erilaiset oikeudet tietojen käsittelyyn. Työntekijän tunnistamiseen voidaan käyttää salasanoja, käyttäjätunnuksia sekä muita turvajärjestelyitä. Tämä takaa sen, että tietoihin ei pääse käsiksi kukaan ulkopuolinen henkilö. Järjestelmässä voidaan myös rajoittaa annettuja oikeuksia. Käyttäjällä voi olla oikeus katsoa tietoja, mutta ei muuttaa niitä. Organisaatiossa tulee huolehtia, että järjestelmän käyttäjän oikeudet vastaavat hänen vastuitaan ja asemaansa. Lisäksi tulee varmistaa, että käyttäjä pääsee käsiksi vain sellaisiin tietoihin, joiden käsittely on tarpeellista hänen työtehtäviensä suorittamisen kannalta. Suojauksen parantamiseksi voidaan ottaa käyttöön myös sellaisia

toimenpiteitä, joiden avulla voidaan seurata kuka on käsitellyt tietoja sekä millaisia toimenpiteitä hän on suorittanut. (Pitkänen ym. 2013, 220- 221.)

Tietosuojavastaava toimii organisaation erityisasiantuntijana, jonka toimenkuvaan kuuluu auttaa rekisterinpitäjää saavuttamaan mahdollisimman hyvä henkilötietojen käsittelytapa sekä korkea tietosuojan taso. Niiden avulla pystytään säilyttämään luottamus rekisterinpitäjän ja rekisteröidyn välillä. Tietosuojavastaavan päätehtävänä on neuvoa etenkin organisaation johtoa ja henkilöstöä. Vastuu henkilötietojen käsittelystä rekisterinpitäjänä kuuluu johdolle eikä tietosuojavaltuutetun nimeäminen täten poista rekisterinpitäjän vastuita. (Tietosuojavaltuutetun toimisto 2010, 2.)

Organisaation tietojärjestelmä tulee suojata niin, että laittomat yritykset päästä sellaiseen laitteistoon, jossa käsitellään henkilötietoja saavat aikaan hälytyksen rekisterinpitäjälle. Suojaus pitää toteuttaa käyttäen toimenpiteitä, jotka mahdollisesti antavat tarpeellisia tietoja laittoman yrityksen alkuperästä. Organisaation tulee myös käyttää toimenpiteitä tietojen siirron varmistamiseksi. Tämä estää muutoksien tapahtumisen tietojen sisällöstä sekä estää niiden häviämisen. (Pitkänen ym. 2013, 223.)

Suojautumisessa voi käyttää apuna myös erilaisia säännöllisiä tarkastuksia sekä auditointeja. Näiden toimeenpanojen avulla on tarkoitus varmistaa, että rekisterinpitäjän työntekijät noudattavat henkilötietojen käsittelyä koskevia lakeja ja tietosuojaa. Lisäksi työntekijöiden täytyy työskennellä rekisterinpitäjän tietoturvaa koskevien toimintaperiaatteiden mukaisesti. (Vanto 2011, 139.) Auditoinnin avulla voidaan myös tunnistaa organisaation sisäiseen ohjeistukseen liittyviä puutteita sekä ehkäistä vahingonkorvauksien ja sanktioiden mahdollisuutta (Vanto 2011, 191).

3 Euroopan unionin tietosuoja-asetus

Euroopan parlamentti ja neuvosto antoivat 27.4.2016 uuden tietosuoja-asetuksen, joka tuli voimaan 24.5.2016. Tietosuoja-asetusta koettiin tarpeelliseksi uudistaa jatkuvan teknologian kehittymisen sekä globalisaation vuoksi. Asetuksella halutaan varmistaa henkilötietojen vapaa liikkuvuus jäsenmaasta toiseen. Pyrkimyksenä on myös yhdenmukaistaa luonnollisten henkilöiden henkilötietojen käsittelyä koskevien perusoikeuksien ja -vapauksien suojelua. Kahden vuoden siirtymäaika päättyy 25.5.2018, johon mennessä yritysten on täytynyt tehdä tarvittavat muutokset toimintatapoihinsa. Asetus koskee kaikkea henkilötietojen käsittelyä, joka tapahtuu unioniin sijoittautuneen rekisterinpitäjän tai henkilötietojen käsittelijän toiminnan yhteydessä. Asetusta on noudatettava, vaikka itse henkilötietojen käsittely tapahtuisikin unionin ulkopuolella. (EU:n tietosuoja-asetus 2016/679, momentit 1-3 ja 22.)

Henkilötietosuoja kuuluu jokaisen ihmisen perusoikeuksiin. Jatkuva teknologian kehitys sekä yritysten kansainvälistyminen ovat tehneet tietosuojan säilyttämisestä entistä vaikeampaa. Esimerkiksi kaupankäynnin yhteydessä henkilötietoja siirretään usein EU:n sisäisesti valtiolta toiselle sekä kolmansiin maihin ja kansainvälisille järjestöille. Henkilötietojen käsittelyn laajentuessa ja lisääntyessä on tärkeää, että EU:n alueen kaikkien valtioiden kohdalla täyttyy henkilötietojen korkeatasoinen suoja. Eroavaisuudet henkilötietojen käsittelyssä jäsenvaltioiden välillä voivat estää henkilötietojen vapaan liikkuvuuden Euroopan unionin alueella. Vapaan liikkuvuuden estyminen voi hankaloittaa unionin taloudellista toimintaa sekä viranomaisten velvollisuuksien suorittamista. Lisäksi riskinä on kilpailun vääristyminen, joka vaikuttaa negatiivisesti taloudelliseen tilanteeseen. Henkilötietoja siirrettäessä yli rajojen luonnollisten henkilöiden mahdollisuus käyttää oikeuttaan tietosuojaan voi vaikeutua ja täten henkilötietojen suojaaminen laittomalta käytöltä tai luovuttamiselta jää olemattomaksi tai puutteelliseksi. (EU:n tietosuoja-asetus 2016/679, momentit 5-9.)

Luonnolliset henkilöt saavat laitettua itsekin aiempaa helpommin omia tietojaan julkisesti muiden nähtäville. Erityisesti sosiaalinen media on lisännyt luonnollisten henkilöiden yleisesti nähtävillä olevien henkilötietojen määrää. Omien henkilötietojen laittamista erilaisiin sovelluksiin sekä muualle verkkoon pidetään normaalina arkipäiväisenä asiana eikä tietosuojaan kiinnitetä välttämättä lainkaan huomiota. Tällöin riski henkilötietojen varastamiseen tai väärinkäyttämiseen on suuri. Jotta tiedot eivät päädy kolmansille osapuolille ilman rekisteröidyn tietämistä, rekisterinpitäjien oikeutta käyttää henkilötietoja suoramarkkinointiin tai profilointiin on rajattu uuden asetuksen avulla. Suurimpia EU:n tietosuoja-

asetuksen tuomia muutoksia ovat todentamisvelvoite, tietosuojavastaavan nimeäminen, rekisteröidyn oikeudet sekä rikkomuksista aiheutuvat sanktiot. Näitä muutoksia käsitellään jäljempänä. (EU:n tietosuoja-asetus 2016/679, momentti 70–71; Oikeusministeriö 2017.)

3.1 Keskeiset käsitteet

Rekisteröity: henkilö, jota henkilötiedot koskevat (Tietosuojavaltuutetun toimisto 2013).

Rekisterinpitäjä: yksi tai useampi henkilö, laitos, säätiö tai yhdistys. Rekisteri perustetaan rekisterinpitäjää varten. Rekisterinpitäjä määrää henkilörekisterin käytöstä sekä toimii sen ylläpitäjänä. (Tietosuojavaltuutetun toimisto 2013.)

Henkilötietojen käsittelijä: Henkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (Yrittäjät n.d.).

Sertifiointi: tietosuojaan liittyvät sinetit, mekanismit sekä merkit, joiden avulla pyritään osoittamaan, että rekisterinpitäjät sekä henkilötietojen käsittelijät noudattavat tietosuoja-asetusta (EU:n tietosuoja-asetus 2016/679, artikla 42).

Tietosuojavastaava: henkilö, joka toimii organisaation erityisasiantuntijana. Tietosuojavastaava auttaa rekisterinpitäjää korkean tietosuojan tason sekä hyvän henkilötietojen käsittelytavan saavuttamisessa. (Tietosuojavaltuutetun toimisto 2010.)

Valvontaviranomainen: jäsenvaltion perustama riippumaton viranomainen, jonka tehtävänä on valvoa luonnollisten henkilöiden perusvapauksia sekä -oikeuksia henkilötietojen käsittelyssä. (EU:n tietosuoja-asetus 2016/679, artikla 51.)

Euroopan komissio: Euroopan unionin toimielin, joka ei edusta poliittisia puolueita tai kansallista hallitusta. Sen tehtävänä on valvoa EU:n etua, ehdottaa uusia toimintapoliitikoita sekä lakeja ja valvoa niiden täytäntöönpanoa. (Euroopan komissio n.d.)

Kolmannet maat: Euroopan unionin ulkopuoliset maat. (Finto 2016)

3.2 Henkilötietojen käsittelyn periaatteet

Tietosuoja-asetuksessa säädetyt periaatteet opastavat henkilötietojen käsittelijöitä sekä rekisterinpitäjiä käsittelemään henkilötietoja rekisteröidyn vapauksia ja oikeuksia kunnioittavalla tavalla. Rekisterinpitäjän on pystyttävä todistamaan, että hän noudattaa periaatteita. Periaatteet ovat pitkälti samat kuin henkilötietolaissa, mutta osaa niistä on täsmennetty. (Oikeusministeriö 2017, 12.)

Ensinnäkin henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti sekä rekisteröidyn kannalta läpinäkyvästi. Tietojen läpinäkyvyys tarkoittaa, että käsittelyyn liittyvät tiedot ovat yksinkertaisesti ja selkeästi esille tuotuina helposti saatavilla ja ymmärrettävissä. Toisen periaatteen mukaan tiedot täytyy kerätä tiettyä, nimenomaista ja laillista tarkoitusta varten, niitä ei saa käsitellä myöhemmin tavalla joka ei ole yhteensopiva edellä mainittujen tarkoitusten kanssa. Tätä periaatetta kutsutaan käyttötarkoitussidonnaisuudeksi. Tietojen minimoinnissa, kolmannessa periaatteessa, on kyse henkilötietojen määrän rajoittamisesta vain tarpeelliseen. Käsiteltävien henkilötietojen on oltava asianmukaisia sekä olennaisia suhteessa käsittelyn tarkoituksiin. Neljäntenä periaatteena voidaan pitää henkilötietojen täsmällisyyttä. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava tarvittavilla toimenpiteillä, jotta tiedot ovat täsmällisiä ja päivitettyjä.

Viidennen periaatteen, säilyttämisen rajoittaminen, mukaan henkilötietoja on säilytettävä muodossa, josta rekisteröity voidaan tunnistaa vain niin kauan kuin on tarpeellista tietojenkäsittelyn tarkoituksen toteutumiseksi. Tietojen eheyden ja luottamuksellisuuden takaamiseksi henkilötietoja on käsiteltävä varmistaen niiden asianmukainen turvallisuus. Oikeanlaisia teknisiä ja organisatorisia toimia käyttäen on varmistettava tietojen suojaus luvattomalta ja lainvastaiselta käsittelyltä sekä häviämiseltä, tuhoutumiselta tai vahingoittumiselta. (Oikeusministeriö 2017, 12.)

3.3 Todentamisvelvoite

Uuden asetuksen myötä rekisterinpitäjien täytyy kyetä todistamaan tarvittaessa viranomaisille noudattavansa uutta tietosuoja-asetusta. Rekisterinpitäjällä täytyy olla dokumentaatio, jossa kuvataan henkilötietojen käsittelyyn liittyvien prosessien ja tietosuojaperiaatteiden käytännön toteuttamista. Myös tietosuoja-asetuksen mukaisia tietosuojaa koskevia sertifikaatteja sekä käytännesääntöjä voidaan käyttää asetuksen noudattamisen osoittamiskeinona. Sertifikaattien avulla rekisteröidyt voivat helposti ja nopeasti arvioida

palveluiden ja tuotteiden tietosuojan laatua. Alakohtaisten käytännesääntöjen avulla voidaan helpottaa asetuksen noudattamista ottamalla huomioon alalla suoritettavan käsittelyn erityispiirteet. (Oikeusministeriö 2017, 14.)

Rekisterinpitäjiä kannustetaan ottamaan käyttöönsä sertifiointimenetelmiä sekä tietosuojasinettejä ja -merkkejä tietosuojaa koskien. Sertifiointi ei kuitenkaan vähennä rekisterinpitäjän vastuuta tietosuoja-asetuksen noudattamisesta, eikä se saa rajoittaa toimivaltaisten valvontaviranomaisten tehtäviä ja valtuuksia. Sertifioinnin tulee aina olla vapaaehtoista sekä helposti saatavilla läpinäkyvällä menettelyllä. Sertifioinnin myöntää toimivaltainen valvontaviranomainen ja/tai nimetty akkreditointielin. Rekisterinpitäjän on luovutettava sertifiointielimelle tai valvontaviranomaiselle kaikki tarvittavat tiedot sekä pääsy käsittelytoimintaan, joita tarvitaan sertifiointimenettelyssä. Sertifiointi voidaan myöntää rekisterinpitäjälle tai henkilötietojen käsittelijälle enintään kolmeksi vuodeksi. Se voidaan kuitenkin uusia, jos vaatimukset täyttyvät edelleen. Jos vaatimukset eivät täyty, sertifiointi voidaan peruuttaa. Sertifioinnin helpottamiseksi kaikki sertifiointimekanismit ja tietosuojasinetit sekä -merkit löytyvät rekisteristä, jonka tietosuojaneuvosto laatii ja asettaa julkisesti saataville. (EU:n tietosuoja-asetus 2016/679, 42 artikla.)

3.4 Tietosuojavastaava

Jos jokin seuraavista kolmesta ehdosta täyttyy yrityksen kohdalla, tulee sen nimetä itselleen tietosuojavastaava:

-Tietojenkäsittelijänä on jokin muu julkisen sektorin toimija kuin tuomioistuin.

- Ydintehtävät muodostuvat käsittelytoimista, jotka vaativat laajamittaista säännöllistä ja järjestelmällistä rekisteröityjen seuraamista.

-Ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu rikostuomioita tai rikkomuksia koskeviin tietoihin tai erityisiin henkilötietoryhmiin.

Tietosuojavastaavia voidaan nimittää vain yksi, jos kaikista toimipaikoista voidaan ottaa häneen helposti yhteyttä. Tietosuojavastaava voi hoitaa tehtäviään palvelusopimuksen perusteella tai hän voi olla rekisterinpitäjän tai tietojenkäsittelijän henkilöstön jäsen. Tietosuojavastaavan valinnassa kiinnitetään huomiota tietosuojalainsäädännön ammattipätevyyteen, ja alankäytänteiden asiantuntemukseen sekä tietosuojavastaavan tehtävien

hoitamisvalmiuteen. Kun tietosuojavastaava on nimetty tehtäväänsä, tulee hänen yhteystietonsa julkistaa sekä ilmoittaa viranomaisille rekisterinpitäjän tai henkilötietojen käsittelijän toimesta. Tietosuojavastaava neuvoo rekisterinpitäjää sekä henkilötietojen käsittelijää tietosuoja-asetuksen noudattamisessa sekä samalla valvoo sen toteutumista. Tietosuojavastaava toimii myös rekisteröityjen ja valvontaviranomaisen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä ongelmissa. Hän ei ole kuitenkaan vastuussa henkilötietojen käsittelyn lainmukaisuudesta vaan vastuu kuuluu rekisterinpitäjälle tai henkilötietojen käsittelijälle. (Oikeusministeriö 2017, 34–35; EU:n tietosuoja-asetus 2016/679, 37–39 artikla.) Suomessa valvontaviranomaisena toimii uusimman hallituksen esityksen mukaan tietosuojavaltuutetun toimisto (HE 9/2018 vp).

3.5 Rekisteröidyn oikeudet

Uuden tietosuoja-asetuksen myötä rekisteröityjen oikeudet vaikuttaa heidän omien tietojensa käsittelyyn kasvavat. Rekisterinpitäjän on toimitettava rekisteröidylle kaikki hänen henkilötietojen käsittelyä koskevat tiedot. Tiedot voi ilmoittaa tapauksesta riippuen sähköisenä, pääasiallisesti kirjallisesti tai muulla tavoin. Rekisteröidyn toiveesta tiedot voidaan antaa suullisesti, mutta tällöin rekisteröidyn henkilöllisyys tulee vahvistaa. Rekisterinpitäjän on toimitettava tiedot rekisteröidylle viipymättä ja perusteltava syy, jos hän ei noudata pyyntöä. Tietojen saaminen on ilmaista rekisteröidylle. Kuitenkin pyyntöjen ollessa kohtuuttomia tai perusteettomia, rekisterinpitäjä voi periä tietojen ilmoittamisesta kohtuullisen maksun tai kieltäytyä suorittamasta pyydettyä toimea lainkaan.

Kaikille rekisteröidyille on heiltä itseltään henkilötietoja kerättäessä ilmoitettava rekisterinpitäjän yhteystiedot ja identiteetti, mahdollisen tietosuojavastaavan yhteystiedot, käsittelyn tarkoitus sekä oikeusperusteet, rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, henkilötietojen vastaanottaja tai -ryhmät sekä tieto mahdollisesta henkilötietojen siirrosta kolmanteen maahan. Näiden lisäksi rekisterinpitäjän on ilmoitettava rekisteröidylle henkilötietojen säilytysaika, rekisteröidyn oikeudesta päästä häntä koskeviin tietoihin, oikeudesta pyytää tietojen oikaisemista tai poistamista ja oikeudesta rajata tai estää henkilötietojen käsittelyä sekä siirtää tiedot järjestelmästä toiseen. Rekisteröidyn tietoon on saatettava myös, että hänellä on oikeus peruuttaa suostumuksensa henkilötietojen käsittelyyn milloin tahansa. Lisätiedoissa on kerrottava myös rekisteröidyn oikeudesta tehdä valitus viranomaisille, automaattisen päätöksenteon olemassaolo sekä mihin henkilötietojen antaminen perustuu. Edellä mainitut tiedot on ilmoitettava rekisteröidyllä ainoastaan kerran. Kun tietoja kerätään muualta kuin rekisteröidyltä itseltään, on edellä mainittujen

tietojen lisäksi kerrottava mistä henkilötiedot on saatu. (EU:n tietosuoja-asetus 2016/679, 12–14 artikla.)

Oikeus omien henkilötietojen oikaisemiseen tai niiden poistamiseen on määrätty myös henkilötietolaissa, mutta tietosuoja-asetuksesta siitä käytetään nimeä Oikeus tulla unohdetuksi. Rekisteröity voi siis vaatia rekisterinpitäjää korjaamaan virheelliset tai epätarkat henkilötiedot ja hänen täytyy myös saada täydentää puutteelliset tiedot. Rekisterinpitäjän velvollisuus poistaa henkilötiedot rekisteröidyn pyynnöstä on kuitenkin osittain tapauskohtaista. Henkilötiedot voidaan poistaa, jos ne ovat merkityksettömiä alkuperäisen keräystarkoituksen kannalta. Tiedot tulee poistaa myös, jos rekisteröity peruuttaa suostumuksen niiden käsittelyyn eikä käsittelylle ole muuta laillista perustetta tai rekisteröity vastustaa niiden käsittelyä perustellusti. Rekisterinpitäjän poistaessa tietoja, tulee hänen ilmoittaa poistopyynnöstä muillekin kyseisiä henkilötietoja käsitteleville rekisterinpitäjille, jotta he toimisivat samoin. (EU:n tietosuoja-asetus 2016/679, 16–17 artiklat.) Henkilötiedot voidaan myös pseudonymisoida. Tällöin henkilötietoja käsitellään niin, että tietoja ei ole enää mahdollista yhdistää rekisteröityyn ilman lisätietoja. (Tietosuojavaltuutetun toimisto 2016.)

Asetuksessa on säädetty neljästä eri tapauksesta, jolloin rekisteröity voi rajoittaa henkilötietojensa käsittelyä. Jos rekisteröity kiistää, että häntä koskevat henkilötiedot eivät ole totuudenmukaisia, voidaan käsittelyä rajoittaa kunnes rekisterinpitäjä on varmistanut tietojen paikkansapitävyyden. Rekisteröidyn kieltäessä tietojensa poiston kun käsittely on lainvastaista, voidaan niiden käyttöä rajoittaa. Kun tiedot eivät ole enää tarpeellisia niiden alkuperäistä tarkoitusta varten, niitä voidaan kuitenkin tarvittaessa käyttää rajoitetusti oikeudellisen vaateeseen liittyen. Kun rekisteröity on vastustanut henkilötietojensa käsittelyä, hänen tietojensa käsittelyä voidaan rajoittaa siksi aikaa, kunnes päätös tehdään. Jos käsittelyä on rajoitettu, saa tietoja säilyttämisen lisäksi käyttää pääasiallisesti vain rekisteröidyn suostumuksesta. Kuten henkilötietojen poistosta, niin myös niiden oikaisusta tai rajoituksista rekisterinpitäjän tulee ilmoittaa jokaiselle, jolle henkilötiedot on luovutettu. Rekisteröity voi halutessaan siirtää henkilötietonsa toiselle rekisterinpitäjälle, jos käsittely perustuu sopimukseen ja se suoritetaan automaattisesti. (EU:n tietosuoja-asetus 2016/679, 18–20 artikla.)

Henkilötietojen ollessa käsiteltävinä suoramarkkinointia varten, rekisteröidyllä on oikeus vastustaa kyseistä käsittelyä milloin tahansa. Rekisteröity voi vastustaa tietojensa käsittelyä myös muulloin, jos hänellä on sitä varten henkilökohtaiseen erityiseen tilanteeseen perustuva selitys. Rekisteröidyn tulee voida välttää joutumasta päätöksen kohteeksi, joka

perustuu pelkästään automaattiseen käsittelyyn. Asetus kieltää automatisoitujen päätösten tekemisen, joilla on rekisteröityä koskevia oikeusvaikutuksia tai jotka vaikuttavat häneen muulla tapaa merkittävästä. (EU:n tietosuoja-asetus 2016/679, 21–22 artikla.)

3.6 Asetuksen rikkominen

Rekisteröity voi tarvittaessa tehdä viranomaisille valituksen, jos hän kokee, että hänen henkilötietojensa käsittelyssä ei noudateta EU:n tietosuoja-asetusta. Valituksen vastaanottanut viranomainen on velvollinen ilmoittamaan valituksen tekijälle valituksen etenemisestä ja ratkaisusta. Jos kyseinen valvontaviranomainen ei ole kolmen kuukauden sisällä käsitellyt valitusta tai ilmoittanut siitä rekisteröidylle, rekisteröidyllä on oikeus nostaa kanne valvontaviranomaista vastaan. Rekisteröity voi nostaa kanteen myös rekisterinpitäjää tai tietojen käsittelijää vastaan, jos hänen tietosuoja-asetukseen perustuvia oikeuksiaan on loukattu asetuksen vastaisella henkilötietojen käsittelyllä. Rekisteröity voi valtuuttaa voittoa tavoittelemattoman elimen tekemään valituksen puolestaan. (EU:n tietosuoja-asetus 2016/679, 77–80 artikla.)

Rekisteröidyllä on oikeus saada korvaus aiheutuneesta vahingosta, jos rekisterinpitäjä tai henkilötietojen käsittelijä aiheuttaa aineellista tai aineetonta vahinkoa rekisteröidylle rikkomalla tietosuoja-asetusta. Henkilötietojen käsittelijä on vastuussa vahingosta ainoastaan, jos hän ei ole noudattanut asetuksen velvoitteita tai rekisterinpitäjän lainmukaista ohjeistusta. Rekisterinpitäjä on sen sijaan aina vastuussa tapahtuneesta vahingosta, jos hän on osallistunut tietojenkäsittelyyn. Hänet voidaan kuitenkin vapauttaa vastuusta, jos hän pystyy osoittamaan osallistumattomuutensa vahingon aiheutumiseen. Useamman rekisterinpitäjän tai henkilötietojen käsittelijän ollessa osallisena samassa tietojenkäsittelyssä, jokainen heistä on vastuussa koko vahingosta. Rekisterinpitäjällä tai henkilötietojen käsittelijällä on kuitenkin oikeus, maksettuaan täyden korvauksen vahingosta, periä muilta samaan käsittelyyn osallistuneilta korvaus, joka vastaa heidän osallisuuttaan aiheutuneesta vahingosta. (EU:n tietosuoja-asetus 2016/679, 82 artikla.)

Kun asetuksen rikkomisesta määrätään hallinnollisia sakkoja, valvontaviranomaisen on varmistettava tapauskohtaisesti määräämisen tehokkuus, oikeasuhteisuus ja varoittavuus. Sakkojen suuruutta määritettäessä otetaan huomioon kaikki tapausta koskevat seikat. Rikkomisen luonne, vakavuus, kesto ja tahallisuus vaikuttavat rangaistukseen. Rekisterinpitäjä tai henkilötietojen käsittelijä voi mahdollisesti lieventää saamaansa rangaistusta, tekemällä tarvittavat toimenpiteet yksin sekä yhdessä valvontaviranomaisen kanssa

rekisteröidyn vahinkojen minimoimiseksi sekä ilmoittamalla rikkomisesta valvontaviranomaiselle itse ja kertomalla tapahtuneesta totuudenmukaisesti. Lisäksi vaikuttavia tekijöitä ovat mahdolliset aiemmat rikkomiset, käytännesääntöjen ja sertifiointimekanismien noudattaminen sekä vahingon kohteeksi joutunut henkilöryhmä. Sakkojen enimmäismäärä seuraavista tapauksista on 10 000 000 euroa tai kaksi prosenttia yrityksen edeltävän tilikauden vuotuisesta kokonaisliikevaihdosta, jos se on suurempi: asetuksessa mainittuihin rekisterinpitäjän, henkilötietojen käsittelijän, sertifiointielimen tai valvontaelimen velvollisuuksiin kohdistuva rikkominen. Enintään 20 000 000 euron sakot tai neljä prosenttia yrityksen edeltävän tilikauden vuotuisesta liikevaihdosta voidaan määrätä, kun kyseessä on henkilötietojen käsittelyn periaatteiden tai rekisteröidyn oikeuksien rikkominen, asetuksen vastainen tietojen siirto kolmanteen maahan tai valvontaviranomaisen määräyksen noudattamatta jättäminen. (EU:n tietosuoja-asetus 2016/679, 83 artikla.)

3.7 Riskien kartoitus

Tietosuoja-asetukseen kuuluu riskiperusteinen lähestymistapa. Se tarkoittaa, että tietosuoja-asetuksen velvoitteet sekä suojatoimet tulee määritellä henkilötietojen käsittelystä rekisteröidyn vapauksille ja oikeuksille aiheutuvien riskien perusteella. Näin voidaan ehkäistä matalariskisen toiminnan ylisääntelyä sekä määritellä tarvittavat suojaustoimenpiteet henkilötietojen käsittelyn aiheuttamien riskien perusteella. (Oikeusministeriön 2017, 16.)

Rekisterinpitäjän tulee arvioida huolellisesti henkilötietojen käsittelyyn liittyvät riskit eli tehdä riskikartoitus. Sen avulla rekisterinpitäjä voi toteuttaa oletuksellista ja sisäänrakennettua tietosuojaa sekä muita asetuksessa mahdollisesti säädettyjä velvollisuuksia. Riskeillä tarkoitetaan henkilötietojen käsittelyssä rekisteröidylle mahdollisesti aiheutuvia aineellisia, aineettomia tai fyysisiä vahinkoja. Näitä ovat muun muassa petokset, identiteettivarkaudet, syrjintä sekä sosiaaliset vahingot. Muita mahdollisia riskejä ovat taloudelliset menetykset ja pseudonymisoinnin kumoutuminen. (Oikeusministeriö 2017, 16.)

Rekisteröityjen vapauksiin ja oikeuksiin mahdollisesti kohdistuvien riskien vakavuus sekä todennäköisyys tulee arvioida tietojenkäsittelyn laajuuden, asiayhteyden, tarkoitusten ja luonteen perusteella. Riskien arvioinnissa tulee hyödyntää myös objektiivista arviointia, jonka avulla voidaan todeta, kuuluuko tietojenkäsittelytoimiin riski vai korkea riski. (EU:n tietosuoja-asetus 2016/679, 24 artikla.) Riski saattaa olla suurempi silloin, kun käsitellään

heikossa asemassa olevien tietoja, suuria määriä henkilötietoja, erityisiin henkilötietoryhmiin kuuluvien tietoja tai kun käsittely koskee suurta määrää rekisteröityjä. Myös henkilökohtaisia ominaisuuksia arvioitaessa riski on normaalia suurempi. (Oikeusministeriön julkaisu 2017, 16.)

Rekisterinpitäjän tulee tehdä tietosuojaa koskeva vaikutustenarviointi, etenkin silloin kun käyttöön otetaan uutta teknologiaa tai käsitellään henkilötietoryhmään kuuluvia tietoja. Se tulee tehdä myös käsiteltäessä rikkomuksia ja rikostuomioita sekä silloin kun on kyse automatisoituun päätöksentekoon liittyvästä arvioinnista. Vaikutustenarviointia voidaan hyödyntää myös tilanteessa, jossa valvotaan yleisölle avointa aluetta. Vaikutustenarviointia käytetään, jos käsitellään paljon henkilötietoja tai käsittelytoimet vaikuttavat suureen määrään rekisteröityjä. Arviointia on mahdollista hyödyntää samankaltaisten käsittelytoimien aiheuttamiin riskeihin. Tietosuojavastaavan tehtävänä on neuvoa rekisterinpitäjää vaikutustenarvioinnin teossa. (Oikeusministeriö 2017, 17.)

Vaikutustenarvioinnissa tarkastellaan erilaisia suojaustoimia, mekanismeja ja toimenpiteitä, joiden avulla pyritään takaamaan henkilötietojen suoja, pienentämään riskejä ja varmistamaan, että asetuksen vaatimukset toteutuvat rekisterinpitäjän toiminnassa. Rekisterinpitäjän tulee varmistaa, että henkilötietojen käsittely tehdään vaikutustenarvioinnin mukaisesti. (EU:n tietosuoja-asetus 2016/679, 35 artikla.)

Jos rekisterinpitäjä ei ole tehnyt tarvittavia toimenpiteitä riskin tason ollessa korkea, rekisterinpitäjän tulee kuulla valvontaviranomaista ennen kuin hän voi aloittaa käsittelyn. Tällöin rekisterinpitäjä toimittaa valvontaviranomaiselle ennen kuulemista vaikutuksenarvioinnin tietosuojasta sekä perustiedot rekisterinpitäjästä, suojaustoimista ja käsittelystä. (EU:n tietosuoja-asetus 2016/679, 35 artikla.)

3.8 Henkilötietojen siirto kolmansiin maihin ja kansainvälisiin järjestöihin

Tietosuoja-asetusta tulee noudattaa kaikenlaisessa henkilötietojen käsittelyssä, jos se suoritetaan unioniin sijoittautuneen henkilötietojen käsittelijän tai rekisterinpitäjän toiminnassa. Sillä ei ole vaikutusta asiaan, tapahtuuko käsittely unionin alueella vai ei. Asetusta sovelletaan unionissa olevien rekisteröityjen henkilötietojen käsittelyyn, vaikka henkilötietojen käsittelijä tai rekisterinpitäjä ei olisi sijoittautunut unioniin, jos käsittely liittyy palveluiden sekä tavaroiden tarjoamiseen rekisteröidyille tai heidän käyttäytymisensä seuraamiseen unionin alueella. (EU:n tietosuoja-asetus 2016/679, 3 artikla.)

Henkilötietojen siirtäminen Euroopan unionin ulkopuolisiin maihin, erilaisille kansainvälisille järjestöille ja niistä takaisin unioniin ovat tarpeellisia. Tämä mahdollistaa kansainvälisen yhteistyön ja kaupan kehittämisen. Lisääntyneet henkilötietojen siirrot ovat tuoneet ilmi uusia henkilötietojen suojaamiseen liittyviä huolenaiheita sekä haasteita. Henkilötietojen siirtäminen Euroopan unionista kansainvälisissä järjestöissä ja kolmansissa maissa toimiville henkilötietojen käsittelijöille, rekisterinpitäjille ja muille mahdollisille vastaanottajille ei saa aiheuttaa vaaraa luonnollisten henkilöiden henkilötietojen suojalle. Suoja ei saa vaarantua silloinkaan, jos joltain kansainväliseltä järjestöltä tai kolmannesta maasta saatuja henkilötietoja lähetetään eteenpäin samassa tai jossain muussa kolmannessa maassa tai toisessa kansainvälisessä järjestössä olevalle henkilötietojen käsittelijälle ja rekisterinpitäjälle. Henkilötietoja voi siirtää kansainvälisille järjestöille sekä kolmansiin maihin vain, jos henkilötietojen käsittelijät sekä rekisterinpitäjät noudattavat tietosuoja-asetusta. (EU:n tietosuoja-asetus 2016/679, 44 artikla.)

Tietosuoja-asetus ei vaikuta kolmansien maiden ja unionin välille luotuihin kansainvälisiin henkilötietojen siirtoa koskeviin sopimuksiin. Jäsenvaltioiden on siis mahdollista solmia kansainvälisiä sopimuksia, jotka sisältävät henkilötietojen siirtämistä kansainvälisille järjestöille ja kolmansiin maihin, mikäli näillä sopimuksilla ei ole vaikutusta unionin lainsäädäntöön. Sopimuksiin tulee lisäksi sisältyä rekisteröityjen perusoikeuksien mukainen suojataso. (EU:n tietosuoja-asetus 2016/679, 44 artikla.)

Henkilötietojen siirtämisen kansainvälisille järjestöille ja kolmanteen maahan mahdollistaa komissio. Komission tulee kuitenkin ennen siirron tekemistä varmistaa, että kolmas maa tai kansainvälinen järjestö pystyy takaamaan tarpeeksi hyvän tietosuojan. Kolmannen maan tulee kyetä tarjoamaan takeet, joiden avulla se varmistaa tarpeeksi korkean tietosuojan tason. Tietosuojan tason tulee vastata Euroopan unionin vaatimuksia. Kolmannen maan tulee huolehtia myös tietosuojavalvonnasta ja sen on pystyttävä takaamaan rekisteröidyn oikeudet sekä oikeudelliset ja hallinnolliset muutoksenhakukeinot. Komissio tutkii myös, miten kolmannessa maassa toteutetaan oikeussuojaa, valtioperiaatetta, kansainvälisiä ihmisoikeuksia, normeja sekä lainsäädäntöä. Jos edellä mainitut vaatimukset täyttyvät, niin tämän jälkeen henkilötietoja saa siirtää tiettyyn maahan ilman lupaa. (EU:n tietosuoja-asetus 2016/679, 45 artikla.)

Komissiolla on myös mahdollisuus kumota tekemänsä päätös. Se voi todeta, että kolmas maa tai kansainvälinen järjestö ei pysty enää takaamaan vaadittua tietosuojan tasoa. Tässä tilanteessa henkilötietojen siirto tulee kieltää, elleivät siirtoa koskevat säännöt ja erityistilanteiden poikkeukset toteudu. Tässä tilanteessa voidaan hyödyntää komission ja

kansainvälisen järjestön tai kolmannen maan välistä kuulemismenettelyä. Komission tulee kumminkin ilmoittaa päätöksestään sekä toimittaa perustelut kyseiselle kansainväliselle järjestölle tai kolmannelle maalle. Tämän jälkeen aloitetaan neuvottelut, jotta tilanne saadaan korjattua. (EU:n tietosuoja-asetus 2016/679, 45 artikla.)

Jos ei ole tehty päätöstä tietosuojan riittävyydestä, henkilötietojen käsittelijän tai rekisterinpitäjän tulee toteuttaa sellaisia toimenpiteitä, joiden avulla on mahdollista varmistaa rekisteröidylle tarvittavat suojaustoimet kompensoidakseen kolmannen maan puutteellista tietosuojaa. Suojaustoimina voi olla esimerkiksi valvontaviranomaisten tai komission hyväksymät tietosuojaa koskevat vakiolausekkeet sekä erilaiset säännöt yritykselle. Lisäksi voidaan hyödyntää valvontaviranomaisen hyväksymiä sopimuslausekkeita. Toimenpiteiden avulla varmistetaan rekisteröityjen oikeuksien kunnioittaminen sekä tietosuojavaatimusten noudattaminen. (EU:n tietosuoja-asetus 2016/679, 46 artikla.)

Kolmannen maan hallintoviranomainen tai tuomioistuin voi tehdä päätöksen, jossa henkilötietojen käsittelijältä tai rekisterinpitäjältä mahdollisesti vaaditaan henkilötietojen luovuttamista tai siirtämistä. Tällainen päätös on täytäntöönpanokelpoinen, jos se perustuu unionin, jäsenvaltion tai pyynnön tehneen kolmannen maan välillä olevaan kansainväliseen sopimuksen. Tästä esimerkkinä on keskinäinen oikeusapusopimus. Tämä ei saa kuitenkaan rajoittaa muita siirtoa koskevia perusteita tai niiden soveltamista. (EU:n tietosuoja-asetus 2016/679, 48 artikla.)

Valvontaviranomaiset ja komissio pyrkivät kehittämään kansainvälisten järjestöjen ja kolmansien maiden kanssa kansainvälisiä yhteistyökeinoja, joiden avulla on mahdollista edistää henkilötietojen suojaamista. Komissio ja valvontaviranomaiset tarjoavat apua henkilötietojen suojaan liittyvän lainsäädännön toteuttamisessa, esimerkiksi antamalla tutkinta-apua, vaihtamalla tietoja, lähettämällä valituksia käsiteltäväksi sekä ilmoitusten avulla. He haluavat edistää henkilötietojen suojaan liittyvien käytänteiden ja lainsäädännön dokumentointia sekä vaihtamista, ja pyrkivät lisäämään myös sidosryhmien välistä toimintaa ja keskustelua. (EU:n tietosuoja-asetus 2016/679, 50 artikla.)

3.9 Mahdolliset poikkeukset ja erityistilanteet

Tietojen siirtoa, kolmansiin maihin sekä kansainvälisille järjestöille, koskien saatetaan tehdä muutamia lisäsäännöksiä vielä lähitulevaisuudessa. Tiedonsiirtoja tulisi pystyä tekemään silloin, kun rekisteröidyltä on saatu suostumus, siirto on tarpeellinen oikeudellisen vaateen tai sopimuksen kannalta tai siirto tapahtuu satunnaisesti. Tietoja tulee voida siirtää jäsenvaltion lainsäädäntöön sekä unionin oikeuteen perustuen, jos yleisen edun syyt sitä vaativat tai siirto tehdään lailla perustetusta rekisteristä, jota kaikki voivat käyttää. Tiedonsiirto rekisteristä ei kuitenkaan saa käsittää rekisterin sisältämää kokonaista tietoryhmää tai henkilötietoja kokonaisuudessaan. Siirto tulee tehdä ainoastaan tällaisten henkilöiden pyynnöstä tai heidän ollessaan henkilötietojen vastaanottajia, joiden oikeutettu etu edellyttää sitä. Lisäksi tulee ottaa huomioon myös rekisteröidyn perusoikeudet ja edut. (EU:n tietosuoja-asetus 2016/679, 49 artikla.)

Sellaiset tiedonsiirrot tulisi sallia, jotka koskevat vain pientä määrää rekisteröityneitä eivätkä ole toistuvia. Tällainen siirto voitaisiin sallia esimerkiksi, jotta rekisterinpitäjän pakottavat edut toteutuisivat eivätkö rekisteröidyn oikeudet, vapaudet tai edut syrjäytä kyseisiä etuja. Rekisterinpitäjän tulisi ottaa huomioon tiedonsiirtojen olosuhteet, henkilötietojen luonne, käsittelytoimien kesto ja tarkoitus. Lisäksi hänen tulee perehtyä tilanteeseen tietojen kolmannessa maassa, alkuperämaassa sekä kohdemaassa. Suojatoimista tulee myös huolehtia. Tämän tyyppisiä tiedonsiirtoja tulisi olla käytössä vain marginaalisissa tapauksissa, joissa ei voida soveltaa muuta siirtämisperustetta. Rekisterinpitäjän täytyisi ilmoittaa tiedonsiirrosta rekisteröidyille sekä valvontaviranomaisille. (EU:n tietosuoja-asetus 2016/679, 49 artikla.)

Erityistapauksiin lukeutuu myös tilanne, jossa komissio ei ole antanut myönteistä päätöstä kolmannen maan tietosuojan riittävyydestä. Tällöin henkilötietojen käsittelijän tai rekisterinpitäjän pitäisi tehdä ratkaisuja, joiden avulla rekisteröidylle annetaan tehokkaat sekä täytäntöönpanokelpoiset oikeudet, jotka liittyvät heidän tietojensa käsittelyyn unionissa näiden tietojen siirtämisen jälkeen. Näin pyritään takaamaan rekisteröityjen suojatoimet ja perusoikeudet. (EU:n tietosuoja-asetus 2016/679, 49 artikla.)

Joissain kolmansissa maissa saatetaan hyväksyä asetuksia, säädöksiä sekä lakeja, joiden avulla säännellään jäsenvaltioiden lainkäyttövallan alaisuuteen kuuluvien oikeushenkilöiden tai luonnollisten henkilöiden käsittelytoimia. Niitä voivat olla muun muassa kolmannen maan hallintoviranomaisten sekä tuomioistuinten tekemät päätökset. Päätöksissä saatetaan vaatia henkilötietojen käsittelijää tai rekisterinpitäjää luovuttamaan tai siirtämään henkilötietoja. Henkilötietojen siirtäminen tai luovuttaminen ei välttämättä perustu

pyynnön tehneen unionin, sen jäsenmaan tai kolmannen maan välillä olevaan kansainväliseen sopimukseen. Tämän tyyppisten asetusten, säädösten tai lakien käyttäminen kolmansien maiden alueiden ulkopuolella saattaa estää tietosuoja-asetukseen kuuluvan luonnollisten henkilöiden suojan. Tiedonsiirtoja tulisi saada tehdä tällaisessa tilanteessa vain silloin, jos tietyt edellytykset tietojen siirtämiseksi kolmansiin maihin pystytään takaamaan. (EU:n tietosuoja-asetus 2016/679, 49 artikla.)

4 Arkistointi

Yritys tarvitsee päätöksentekonsa tueksi kattavat ja ajan tasalla olevat tiedot. Tämän vuoksi yrityksen toiminnasta syntyvä ja toiminnassa tarvittava tieto talletetaan asiakirjoina arkistoon eli arkistoidaan. Arkistojen asiakirjat voivat olla vielä vuosienkin jälkeen tärkeitä, kun tarvitsee selvittää vanhoja asioita tai etsiä tietoja. (Itälä, Latva-Koivisto, Roos & Toivonen 2000, 5.) Asiakirjat ovat kirjallisia tai kuvallisia esityksiä taikka sähköisesti tai muulla vastaavalla tavalla aikaan saatuja esityksiä, jotka ovat luettavissa, kuunneltavissa tai muutoin ymmärrettävissä teknisin apuvälinein (Arkistolaki 831/1994, 6§). Asiakirja-aineistot voidaan jakaa kolmeen luokkaan niiden sijainnin ja käytön kannalta; käsiarkisto, lähiarkisto sekä päätearkisto. Käsiarkistoon kuuluu työtilojen yhteydessä säilytettävät asiakirjat, joita käsitellään päivittäin. Lähiarkistoon kuuluvat asiakirjat ovat myös työtilojen läheisyydessä, mutta niiden säilytysturvallisuudelle asetetaan suuremmat vaatimukset. Pysyvästi säilytettävät asiakirjat kuuluvat päätearkistoon. Päätearkistossa olevia asiakirjoja käytetään ja täydennetään suhteellisen harvoin. (Arkistolaitos 2013, 4.)

4.1 Asiakirjojen käsittely

Arkistoa järjestäessä tulee muistaa huomioida asiakirjojen käsittely. Asiakirjoja tulee aina käsitellä varoen mahdollisimman hyvä säilymisen varmistamiseksi. Asiakirjoihin ei saa käyttää teippiä eikä niitä tule yhdistää toisiinsa niiteillä tai klemmareilla. Reikien tekeminen asiakirjoihin ja kortistojen niputtaminen kumilenkeillä kuuluvat myös huonoihin tapoihin käsitellä asiakirjoja. Ajan kuluessa kuminauhat katkeilevat, ylimääräiset reiät paperissa voivat saada aikaan repeämiä, klemmarit ruostuvat sekä teipit voivat jättää asiakirjoihin ikäviä jälkiä. Asiakirjoihin saa tehdä merkintöjä vain tarpeen vaatiessa, silloinkin olisi hyvä käyttää lyijykynää. (Pohjola, Hakala & Harvilahti 2010, 33–34.)

Asiakirjojen ollessa käsiarkistossa yrityksen toimistotiloissa ja usein käsiteltävinä, säilytysvälineiden tulee olla mahdollisimman helppokäyttöisiä. Tämä parantaa asiakirjojen löydettävyyttä sekä pysymistä oikeassa järjestyksessä. Asiakirjojen säilytykseen käsiarkistossa voidaan käyttää muun muassa rengaskansioita, mappeja sekä kortistolaatikostoja. Asiakirjojen käytön määrän pienentyessä ne siirretään toimistotiloista yrityksen päätearkistoon. Tällöin asiakirjat säilötään vähän tilaa vieviin arkistokoteloihin, jotka suojaavat asiakirjoja pölyltä, kulumiselta sekä valolta.

Arkistokoteloiden tulee olla helppokäyttöisiä sekä sopivan kokoisia ja ne tulee muistaa pakata täyteen. Liian väljissä arkistokoteloissa on vaarana, että asiakirjojen reunat taipuvat ja vaurioituvat. Liian suuressa kotelossa taas asiakirjat eivät pysy paikoillaan. (Rastas 1994, 119.) Arkistokoteloihin ei saa jättää muovitaskuja tai muitakaan pieniä esineitä, sillä ne vähentävät tilaa kotelosta ja voivat tarttua kiinni papereihin ja vahingoittaa niitä (Pohjola ym. 2010, 34).

Kansioita pakattaessa on hyvä tarkistaa, että asiakirjojen selkien paksut kohdat eivät ole kaikki arkistointikotelon samalla puolella. Tämä tulee ottaa huomioon myös pakatessa niitattuja asiakirjoja. Asiakirjapino on hyvä kääntää puolesta välistä kerran kansion sisällä. Arkistointikotelon päällimmäisen ja alimmaisen asiakirjanipun suojaksi tulee käyttää suojalehteä, joka estää asiakirjojen vaurioitumista ja hankautumista. Arkistointikotelot tulee asettaa arkistointihyllylle pystyasentoon joko pitkän tai lyhyen sivunsa varaan. (Rastas 1994, 120–121.)

Asiakirjahallinnossa määritellään organisaation kaikki asiakirjat tehtäväalueittain, ohjeistetaan niiden säilyttämistä sekä käyttöä. Tällöin asiakirjojen oikeanlainen nimeäminen on erittäin tärkeää. Puutteellinen nimeäminen vaikeuttaa huomattavasti asiakirjojen löytymistä. Asiakirjojen sekä niiden kopioiden ja rinnakkaiskappaleiden määräaikainen hävittäminen ja käsittely järjestelmällisesti tulevat vaikeutumaan, ellei nimeämiseen ole panostettu. Järjestelmälliseen nimeämiseen kuuluu, että tiettyjä nimikkeitä käytetään asiakirjojen kaikissa käsittelyvaiheissa. Näihin vaiheisiin kuuluvat esimerkiksi asiakirjojen laatiminen, käyttäminen, tallettaminen, hävittäminen sekä siirtäminen. Asiakirjojen nimikkeet rakentuvat kahdesta osasta. Ensimmäinen osa kertoo asiakirjan luonteen, tyypin sekä tarkoituksen. Toinen osa kertoo yrityksen päätoiminnan tai siihen sisältyvän tehtävän, jota varten asiakirja on luotu. Samalla se voi myös kertoa asiakirjan sisällöstä. (Itälä ym. 2000, 8-9.)

4.2 Arkistointitilat

Yritys ei voi arkistoida asiakirjojaan mihin vain haluaa, vaan paikan valinnassa tulee ottaa huomioon asiakirjojen säilyvyyteen vaikuttavat tekijät. Asiakirjojen tulee olla turvassa tuhoutumiselta, vahingoittumiselta sekä asiattoman käsittelyn ulottumattomissa. Arkistotilat tulee valita niin, että ne suojaavat aineistoa mm. vedeltä ja kosteudelta, tulelta ja pakokaasuilta, liialliselta valolta ja lämpenemiseltä sekä vahingonteolta ja luvattomalta käytöltä. (Arkistolaitos 2013, 3.)

Arkistointitilojen sijoitusta päätettäessä tulee ottaa huomioon mahdolliset ulkopuoliset haittatekijät. Rautateiden, pääliikenneväylien tai teollisuuslaitoksien läheinen sijainti ei ole suositeltavaa arkistointitiloja suunniteltaessa. Rakennuksessa arkistointitilojen pitää sijaita paikassa, jossa ei ole lähellä palo- tai räjähdysvaarallisia tiloja eikä yläpuolella kosteita tiloja. Vesivahinkoriskin välttämiseksi tilan kautta ei saa kulkea muita kiinteistön vesi- ja viemäriputkia kuin vesipatterien putket. Arkistotilojen ollessa kellaritilassa, sen lattiat eivät saa olla pohjavesipinnan alapuolella. Kellarikerroksessa olevilla arkistointitiloilla on yleistä suurempi vesivahinkoriski, joten tällaisissa tapauksissa on tärkeää kartoittaa ja ottaa huomioon vesivahingon riskitekijät. Myös liikuntasaumat ja pihatasot lisäävät vesivahingon riskiä. Paras sijoituspaikka arkistoille olisikin rakennuksen ensimmäinen kerros tai ylimmät kellarikerrokset. Suosituksena on myös, että arkistotilat eivät rajoitu rakennuksen ulkoseiniin tilojen sisäilman tasapainottamiseksi. Toimitiloista on oltava hyvä yhteys päätearkistoon, täten aineiston siirtämisen helpottamiseksi hissien sijainti lähellä arkistotiloja on suositeltavaa. Väestönsuojan käyttäminen arkistotilana on kiellettyä, koska kriisitilanteessa se on kyettävä tyhjentämään ja kunnostamaan väestönsuojaksi 72 tunnissa. Määräajan säilytettävää arkistointiaineistoa voi kuitenkin vähäisessä määrin säilyttää väestönsuojassa, kunhan tyhjennystilannetta varten on tehty suunnitelma ja varattu asiakirjoille turvallinen sijoituspaikka. (Arkistolaitos 2013, 4-5.)

Kun suunnitellaan arkistotilojen mitoitusta, tulee ottaa huomioon asiakirja-aineiston kartunta sekä määräajan kuluttua hävitettävän aineiston osuus. Mitoitukseen vaikuttavat myös aineiston säilytysajat, koko sekä laatu. Säilytystavalla on iso merkitys tilojen tarpeeseen, sillä siirtohyllyköitä käyttämällä saadaan 80 % enemmän hyllytilaa asiakirjoille kuin kiinteiden hyllyköiden avulla. Arkistotiloissa ei saa käyttää palavia kalusteita tai sisusteita, esimerkiksi puuhyllyt ovat kielletty. Arkistotilat olisi suositeltavaa mitoittaa 20 vuoden tarvetta varten. Arkistotilojen yhteydessä tulee olla aputiloja aineistojen käsittelyä, puhdistamista ja vastaanottamista varten. Muista poiketen, pienet arkistonmuodostajat voivat säilyttää asiakirjojaan kokonaan lähiarkistossa arkistokaapissa tai -holvissa, joka on paloturvallinen. (Arkistolaitos 2013, 5-6.)

Toimiva ilmanvaihto arkistointitiloissa on tärkeää asiakirjojen alkuperäisen kunnon ylläpitämisen kannalta. Tilan ilman pitäisi vaihtua vähintään kahden tunnin välein, joten ilmanvaihtolaitteiston huollosta ja kanavien puhtaana pidosta on huolehdittava säännöllisesti. Päätearkistoissa tulee käyttää koneellista ilmanvaihtojärjestelmää, jolla saadaan suodatettua sekä ulkoa tuleva korvausilma että sisäkierrossa ennaltaan oleva ilma. Tasaisen ja sopivan lämpötilan ylläpitämiseksi, arkistointitiloihin voi hankkia lämmityslaitteita. Lämmi-

tystä voi hoitaa patteri- tai ilmalämmityksellä sekä lattialämmityksellä, kunhan lämpökaapelit eivät ole arkistohyllyjen kohdalla. Sähkölämmityslaitteita saa käyttää arkistotiloissa vain valvotusti ja virka-aikana, sillä niitä käytettäessä tulipaloriski kasvaa. Arkistotiloissa olevat sähkölaitteet tulee kyetä muuttamaan jännitteettömiksi tilan ulkopuolelta, lähelle sisääntulotietä asetetusta kytkimestä tai muusta vastaavasta. Tarvittaessa arkistotiloihin voidaan asentaa pistorasioita, mutta niiden tulee olla maadoitettuja ja roiskevedenpitäviä. Yleisin arkistotiloissa käytettävä valonlähde on mahdollisimman vähän UV-säteilyä sisältävät loistelamput. Turvallisuus syistä valaisimien tulee olla roiskevedenpitäviä sekä sijoitettuna vähintään 35 cm päähän säilytettävästä materiaalista. Kaikkein käytännöllisin valaistus olisi liiketunnistimin ohjautuva, sillä tällöin käsittelyn ulkopuoliset asiakirjat eivät altistuisi valolle. (Arkistolaitos 2013, 9-11.)

Tiloissa, joihin arkistoidaan pysyvästi säilytettäviä asiakirjoja, tulee kiinnittää erityis-huomiota huoneen lämpötilaan sekä ilman kosteuteen ja puhtauteen. Ihanne lämpötila asiakirjojen säilytykseen on +16 ja +20 asteen välillä, sillä asiakirjat säilyvät parhaiten matalassa lämpötilassa. Tilojen lämpötilan ja kosteuden äkilliset vaihtelut huonontavat asiakirjojen kuntoa, joten ilman lämpötilaa ja kosteutta olisi hyvä mitata säännöllisin väliajoin sopivien olosuhteiden varmistamiseksi. Suurimmat vahingot asiakirjoille aiheutuu pitkäaikaisesta altistumisesta kostealle ilmalle. Tämä altistaa ne kosteusvaurioille, joista voi seurata homeitiöiden muodostumista aineistoon. Arkistotiloissa tai kiinteistössä mahdollisesti olevat kosteus- tai homevauriot eivät leviä asiakirjoihin, jos niitä säilytetään asianmukaisesti. (Arkistolaitos 2013, 13–14 ja 16.)

Palo- ja kosteusvaurioiden riskin pienentämiseksi on tärkeää, että arkistotiloissa käytettävät materiaalit ovat metallisia. Tiloissa ei saa säilyttää kalustoa, joka on tehty helposti palavasta tai asiakirjoille haitallisesta materiaalista, kuten esimerkiksi vinyylistä tai vanerista. Ilmankierron vuoksi hyllyjen ja seinän sekä lattian välille on jätettävä vähintään 10 cm väliä. Katon ja hyllyjen välissä tulee olla eroa enemmän, 20 cm. Hyllyjen kantavuus saa olla enintään 80 kg, tämä on otettava huomioon hyllyjen määrää mietittäessä. Huoneessa tulee olla ainakin yksi pöytä tai laskutaso asiakirjojen selaamista ja käsittelyä varten. Asiakirjat pitää säilöä arkistokelpoisiin ja umpinaisiin koteloihin tai laatikoihin. Niiden materiaalin tulee suojata aineistoa olosuhteiden vaihtelulta ja mahdollisuuksien mukaan myös joissain määrin vesivahingoilta. (Arkistolaitos 2013, 14–15.)

Arkistoaineistojen säilytykseen liittyy aina riskejä, joten on tärkeää tehdä hyvissä ajoin riskienkartoitus sekä pelastussuunnitelma mahdollista vahinkoa varten. Arkistotilojen lähettyvillä olisi hyvä olla pelastusvälineinä muun muassa suojamuoveja, vesi-imureita, kuljetuspusseja sekä pakkausmateriaaleja. Vesivahingon sattuessa kastuneet asiakirjat on kuivattava mahdollisimman pian, sillä homeen muodostuminen märkään paperiin kestää ainoastaan 1-2 päivää. Tulipalon varalta arkistotilaan tai sen lähettyville on hyvä sijoittaa käsisammutin. (Arkistolaitos 2013, 15–16 ja 12.)

4.3 Asiakirjojen säilytysajat

Asiakirjojen määrän kasvun hillitsemiseksi, yrityksen on hyvä asettaa asiakirjoilleen säilytysajat. Säilytysaikaohjeet varmistavat, että kaikki tarpeelliset tiedot sekä asiakirjat säilytetään riittävän kauan ja tarpeettomat hävitetään oikealla tavalla mahdollisimman nopeasti. Turhien asiakirjojen poistaminen helpottaa tarvittavan tiedon löytämistä, jolloin yrityksen toiminnasta tulee tehokkaampaa. Poistamalla turhat aineistot säästetään kalusto- ja tarvikekuluissa sekä henkilöstö- ja tilakustannuksissa. (Valtonen, Roos, Palonen, Toivonen & Järn 2009, 58.) Arkistointiin on tarpeellista laittaa asiakirjasta ainoastaan sen alkuperäinen versio, kopiot voidaan tuhota liiallisen paperin välttämiseksi. Täytyy kuitenkin ottaa huomioon, että oikaisu-, oikeudenkäynti- tai reklamaatiotapauksiin tarvittavia tai alkuperäistä tehtäväänsä täyttämättömiä asiakirjoja ei saa hävittää. (Rastas 1994, 141.)

Asiakirjojen säilytysaikoja määriteltäessä tulee ottaa useita eri tekijöitä huomioon. Yrityksen tulee ensinnäkin miettiä, kuinka kauan aineistoa tullaan tarvitsemaan yrityksen omassa toiminnassa. Yrityksellä tulee olla arkistoituna asiakirjat, joilla he voivat todistaa omistus-, hallinta- ja käyttöoikeutensa sekä asiakirjat, joita tarvitaan perusteeksi korvaus-, syyte- ja kanneoikeuksiin. Yrityksen taloushallintoon liittyvissä asiakirjoissa on paljon tietoa, joka täytyy arkistoida, sillä tietoja voidaan tarvita myöhemmin asioiden selvittämistä tai todentamista varten. Yksilön oikeusturvan tai muun edun kannalta tärkeitä papereita on pidettävä arkistossa niin kauan kuin niillä on oikeudellista merkitystä. Näitä asiakirjoja ovat muun muassa sosiaalisiin etuihin, omistukseen sekä sairaanhoitoon liittyvät tiedot. Joissain maissa saattaa olla erikseen säännös, jossa kielletään hävittämästä tiettyä ajankohtaa vanhemmat asiakirjat. Suomessa on tehty määräys, että vuotta 1920 vanhemmat julkisten viranomaisten asiakirjat on säilytettävä pysyvästi muutamaa poikkeusta lukuun ottamatta. (Itälä ym. 2000, 9-11.)

Jotta asiakirjat osataan hävittää oikeaan aikaan, tulee yrityksen tietää, mistä lähtien säilytysajan katsotaan alkaneen. Yleisesti ottaen asiakirjojen säilytysaika lasketaan asiakirjasta ilmi käyvän päivämäärän mukaan. Jos päiväystä ei ole, katsotaan säilytysaika alkaneeksi seuraavan vuoden alusta. Päätökseen johtavien asiakirjojen säilytysaika alkaa päätöksenteko päivästä. Täten useamman vuoden käsittelyssä olleiden asioiden säilytysaika alkaa lopullisen päätöksen jälkeen. Poikkeuksena ovat kirjanpitoasiakirjat, joiden säilytysajan katsotaan alkavan tilejä koskevan tilikauden lopusta. Kun asiakirjan säilytysaika päättyy, se tulee hävittää silppuamalla tai muulla luotettavalla tavalla. Asiakirjat eivät saa joutua missään vaiheessa ulkopuolisten saataville, joten erityisesti salaisten ja henkilötietoja sisältävien asiakirjojen hävittämisessä on oltava tarkkana. (Rastas 1994, 148.)

4.4 Arkistonmuodostussuunnitelma

Organisaation arkistonmuodostussuunnitelmalle ei ole vakiintunutta nimitystä. Erilaisia yleisesti käytettyjä nimityksiä ovat muun muassa arkistointisäännöt, asiakirjahallinnon suunnitelma ja tiedonohjausjärjestelmä. Arkistonmuodostussuunnitelma ja asiakirjahallinnan toimintaohje ovat nimityksistä yleisimmin käytetyt. (Valtonen ym. 2009, 31.) Arkistonmuodostussuunnitelman päätavoitteena on toteuttaa ja tuottaa yhtenä organisaation osana tiedonhallintaa, laadunvarmistamista ja tietojärjestelmäarkkitehtuuria. Asiakirjajärjestelmän tulee dokumentoida ja kuvata virheettömästi sekä huolellisesti kaikki asiakirjoihin tehtävät toimenpiteet. Lisäksi arkistointisuunnitelmassa kuvataan suunnitelmat ja ohjeistukset fyysisistä säilytysvälineistä. Asiakirjajärjestelmän tulee myös pystyä ohjeistamaan oikeanlainen toiminta riskitilanteissa. (Valtonen ym. 2009, 22.)

Arkistonmuodostussuunnitelman tarkoituksena on kertoa yksiselitteistä ja yksityiskohtaista tietoa organisaation liiketoimintoihin liittyvien asiakirjojen hallinnasta, säilyttämisestä ja tuottamisesta. Sen avulla myös varmistetaan, että organisaatiossa käytössä olevat asiakirjahallinnan menetelmät, toimintatavat sekä tietojärjestelmät tukevat liiketoiminnan tehtäviä, ohjaavat tietojen talteen ottamista ja varmistavat normien sekä säädösten noudattamista. Arkistonmuodostussuunnitelman olisi hyvä pystyä kattamaan asiakirjatiedon koko elinkaaren aikainen hallinnan sekä käsittelyn ohjeistus eikä vain luetella eri asiakirjaryhmien säilytysaikoja. Hyvin tehty arkistonmuodostussuunnitelma avustaa myös laadun- ja riskienhallintaa sekä toiminnan auditointia ja arviointia. (Valtonen ym. 2009, 30.)

Arkistonmuodostussuunnitelmassa kuvataan, ohjeistetaan ja määritetään asiakirjahallinnon keskeisiä asioita. Keskeisiin asioihin kuuluvat muun muassa organisaation asiakirja-

ja tietohallinnan tavoitteet sekä tarkoitus. Suunnitelmassa pitää pystyä kuvaamaan organisaation asiakirjajärjestelmä ja sähköpostien käsittely. Organisaation tulee suunnitelmassaan määritellä metatiedot ja asiakirjat sekä perehtyä metatietojen tallentamiseen ja asiakirjojen laatimiseen. Lisäksi arkistonmuodostussuunnitelmassa ohjeistetaan asiakirjahallinnon vastuista, periaatteista ja tietojärjestelmistä. Suunnitelmassa pitää tuoda ilmi, miten asiakirjat rekisteröidään ja talteen otetaan. Tärkeää on määritellä myös asiakirjojen käyttöoikeudet, hävittäminen sekä luokittelujärjestelmä. Arkistonmuodostussuunnitelman tulee sisältää tiedot asiakirjojen säilyttämistavoista, -ajoista ja välineistä. Lisäksi tulee perehtyä organisaation mahdollisiin tietosuoja- ja tietoturvakysymyksiin. (Valtonen ym. 2009, 31.)

Arkistonmuodostussuunnitelman on oltava oikeellinen, käytännöllinen, vastuullinen sekä hyvin tunnettu. Sen tulee olla helposti saatavilla ja muutoksista pitää tiedottaa hyvissä ajoin. Organisaation henkilöstöltä voidaan myös odottaa arkistonmuodostussuunnitelman käyttöön perehtymistä ja noudattamista. Arkistonmuodostussuunnitelman on tärkeää kattaa kaikki asiakirjahallinnon osa-alueet. Organisaation kannalta asiakirjahallinnon kokonaisuuden ymmärtäminen on välttämätöntä. (Valtonen ym. 2009, 30.)

Joissain tilanteissa organisaatiolaajuiset periaateohjeet voivat jäädä liian yleisiksi tiettyjen tehtäväkohtaisten asiakirjojen hallintaohjeina. Samalla tavalla myös koulutus voi antaa vain yleistä tietoa, joka ei välttämättä vastaa asiakirjahallinnon päivittäistarpeita. Henkilöstö tarvitsee tarkat tiedot siitä, millaisia asiakirjahallintavelvoitteita kullekin työntekijälle kuuluu. Jokaiselle työntekijälle erikseen tehdyssä yksinkertaisessa ohjeessa voidaan muun muassa määritellä ne asiakirjatyypit, jotka kukin työntekijä tallentaa. Lisäksi ohjeessa voidaan ilmoittaa, mitkä aineistot tulee tallentaa ja mitä ei. Periaateohjeisiin sisältyy myös yksinkertaiset tehtävä- ja työntekijäkohtaiset ohjeet, joiden avulla pyritään poistamaan epävarmuutta hävittämis-, tallentamis- sekä hakukäytännöissä. (Valtonen ym. 2009, 31.)

5 Nykytila-analyysi

Ensimmäinen vaihe opinnäytetyön toiminnallisessa osiossa oli tehdä nykytila-analyysi yrityksen käytännöistä henkilötietojen käsittelyssä. Analyysi tarvittiin, jotta saatiin selville, onko yrityksen tehtävä muutoksia toimintatapoihinsa vai käsittelevätkö he henkilötietoja EU:n tietosuoja-asetuksen mukaisesti. Analyysiin sisällytettiin myös raportti suositeltavista muutoksista, joita yrityksen olisi hyvä tehdä henkilötietojen käsittelyyn.

5.1 Toteuttaminen

Nykytilanteen selvittämiseksi ensimmäisenä oli hankittava tieto siitä, mitä rekistereitä yrityksellä on. Lisäksi oli otettava selvää, ketkä kaikki yrityksessä käsittelevät henkilötietoja, mitä tietoja he käsittelevät ja miten he niitä käsittelevät. Jotta edellä mainittuihin asioihin saatiin vastaukset, laadittiin haastattelulomake (liite nro 4), jota käytettiin haastateltaessa yrityksen henkilökuntaa. Haastattelukysymykset laadittiin opittua teoriaa soveltaen, miettien mitä kaikkea henkilötietojen käsittelyyn kuuluu sekä mitä tarvitsee tietää hahmottaakseen kokonaiskuvan yrityksen henkilötietojen käsittelystä. Toimeksiantoyrityksen yhteyshenkilö oli valinnut jo valmiiksi henkilöt, joita haastateltiin. Hän tiedotti haastattelusta etukäteen henkilökunnalle ja pyysi heitä valmistautumaan haastatteluun. Yrityksessä vierailtiin kaksi kertaa, ensimmäinen vierailu oli 14.12.2017 ja toinen vierailu 8.1.2018. Ensimmäisellä kerralla haastateltiin hallinnon sekä hankinnan työntekijöitä ja toisella kertaa myyntipuolen työntekijöitä, tuotantopäällikköä sekä työturvallisuuspäällikköä. Haastattelulomakkeen kysymysten lisäksi tiedusteltiin tilanteessa ilmi tulleita asioita ja työntekijät kertoivat myös itse oleellisina pitämiään tietoja. Suurin osa työntekijöistä ei ollut valmistautunut haastatteluun, poikkeuksena oli toimialalle erikoistunut kirjanpitäjä. Hän oli laatinut tiivistelmä oman osastonsa toiminnasta henkilötietojen käsittelyssä.

Haastattelemisen lisäksi kierrettiin myös yrityksen toimitilat. Ensimmäinen ja toinen haastattelu tapahtuivat eri toimipisteillä, joten molempiin tiloihin tutustuttiin paremman ja laajemman kuvan saamiseksi yrityksen toiminnasta. Kierrettäessä tiloja havainnoitiin mahdollisia tilojen aiheuttamia tietosuojariskejä. Näin saatiin selville asioita, joita ei haastattelun yhteydessä tullut esille tai ei kerrottu. Yhteyshenkilö laittoi myös ajankohtaista tietoa alaan ja henkilötietojen käsittelyyn liittyen, jos jotain tuli ilmi haastattelujen välissä tai jälkeen.

5.2 Haastattelun tulokset

Yrityksen asiakkaina on pääosin toisia yrityksiä, joten harvojen luonnollisten henkilöiden asiakkuuksien vuoksi yrityksen ulkopuolisten henkilötietoja käsitellään vähän. Yrityksellä on melko paljon omia työntekijöitä, joten luonnollisten henkilötietojen käsittelyä ilmenee talonsisäisesti. Jokainen työntekijä yrityksen toimistohenkilöstöstä käsittelee henkilötietoja jossain vaiheessa, mutta tällöin kyseessä on yleisimmin pelkästään henkilötunnus. Yrityksellä on kolme rekisteriä, jotka sisältävät henkilötietoja: palkkaohjelma Sonet, Savcor Mekawood -puunhankintajärjestelmä sekä Samet-toiminnanohjausjärjestelmä. Henkilötietoja käsitellään ohjelmien lisäksi arkistoinnissa ja niitä liikkuu myös sisäisessä postissa. Sisäisen postin kuljettaa yrityksen ATK-vastaava. Sisäisessä postissa kulkee työsopimuksia, verokortteja sekä sairauslomalappuja ja ne on suojattu asiaankuuluvalla tavalla.

5.3 Palkkaohjelma

Palkkaohjelma Sonet toimii yhtenä yrityksen rekistereistä. Toimistohenkilöstö pyytää tarvittaessa palkkaohjelmassa olevaa tietoa palkanlaskijalta. Palkkaohjelmaan on pääsy ainoastaan palkanlaskijalla ja tiettyinä aikoina häntä sijaistavalla kirjanpitäjällä. Palkanlaskija vaihtaa salasanansa aina jonkun toimittua hänen sijaisenaan tai kesätyöntekijän lähdettyä, turvatakseen henkilötietojen tietoturvan. Rekisterin ylläpito on palkanlaskijan vastuulla, joten hän poistaa, lisää ja muokkaa rekisterin tietoja tarvittaessa.

Rekisteri sisältää yrityksen työntekijöistä ainakin seuraavat tiedot: nimi, puhelinnumero, osoite, verotiedot, pankkitili, henkilötiedot sekä palvelussuhdetiedot kuten ammatti. Palkanlaskija välittää rekisteristä henkilötietoja niin yrityksen sisäisesti kuin ulkopuolellekin. Palkanlaskennassa ei voi välttää henkilötietojen siirtoa ulkopuolisille. Palkanlaskija lähettää henkilötietoja verottajalle, eläkevakuutusyhtiölle, vakuutusyhtiölle, ay-liitoille, EK:lle, Työttömyysvakuutusrahastoon, Kelalle ja Tilastokeskukselle. Ainoastaan tiedot verottajalle, eläkevakuutusyhtiölle, ay-liitoille, EK:lle, Kelalle ja Tilastokeskukselle lähetetään työntekijäkohtaisesti. Vakuutusyhtiöille tilastot lähetetään ammattinimikkeittäin ja Työttömyysvakuutusrahastoille lähetetään vuoden palkkasumma, joten ne eivät sisällä henkilötietoja. Yrityksen ulkopuolelle henkilötiedot lähtevät sähköisesti tietosuojaturvallisella tavalla ja niiden lähettäminen perustuu lakisääteisyyteen.

Yrityksen sisällä palkkaohjelmasta saatavia henkilötietoja käytetään yritysraportteihin ja työtodistuksiin. Palkanlaskija välittää paperillisena kirjanpitäjälle aineistoa, joka sisältää henkilötunnuksen. He ovat kuitenkin jo sopineet peittävänsä jatkossa henkilötunnuksen, sillä se ei ole kirjanpitäjän toimien kannalta välttämätöntä tietoa. Työntekijät saattavat tuoda palkanlaskijalle sairauslomalappuja, verokortteja ja työsopimuksia paperillisina, ne sisältävät luonnollisesti henkilötietoja.

5.4 Savcor Mekawood

Toisena rekisterinä yrityksessä toimii Savcor Mekawood -puunhankintajärjestelmä. Ohjelmaan kirjataan tietoja puiden myyjistä. Suurin osa myyjistä on elinkeinonharjoittajia tai yrityksiä. Y-tunnus ei ole henkilötieto, joten ainoastaan luonnollisten ihmisten henkilötiedot sisältyvät tietosuojan piiriin eikä niitä ole montaa. Uusia rekisteröitäviä tietoja syntyy puukaupoissa sekä tarjouksissa. Rekisterin ylläpitovastuu on metsäkirjanpidon vastaavalla, metsäpäälliköllä sekä alue-esimiehillä. Ohjelmaan pääsyä on rajattu salasanoilla, joten ainoastaan edellä mainituilla henkilöillä on oikeus muokata rekisterin tietoja. Rekisteristä löytyvät seuraavat henkilötiedot: nimi, puhelinnumero, osoite, henkilötunnus, sähköpostiosoite, kotikunta, maksunsaaja, tilatiedot, omistusmuoto sekä mahdollinen edustaja tai edunvalvoja. Rekisterin tietoja välitetään eteenpäin moto- ja autourakoitsijoille. Välitettäviä tietoja ovat nimi, puhelinnumero ja osoite.

5.5 Samet

Samet on yrityksen toiminnanohjausjärjestelmä. Järjestelmään on pääsy kaikilla toimistohenkilökunnasta, sillä se toimii yhdellä yhteisellä salasanalla. Koska yrityksellä ei ole paljoa luonnollisia henkilöitä asiakkaana, Sametin sisältämät henkilötiedot ovat vähäisiä. Laskutusta varten järjestelmään kerätään yritykseltä puuta ostavan luonnollisen henkilön nimi, osoite sekä tarvittaessa puhelinnumero.

Vientisihteerit kirjaavat laskun tiedot järjestelmään ja reskontra hakee ne sieltä varsinaista laskutusta varten. Laskutuksen lisäksi reskontra käsittelee henkilötietoja palkkapalautuksien kuten kelakorvauksien, verottajalle tekemien vuosi-ilmoitusten, osingonsaajien sekä pankista tulleiden tiliotteiden yhteydessä. Reskontra luovuttaa tietoja eteenpäin ainoastaan verottajalle. Toiminnanohjausjärjestelmää käytetään laskutuksen lisäksi tuotannon, lähetysten ja varastojen hoitamiseen.

5.6 Henkilötietojen käsittely urakoitsijoiden toiminnassa

Yritys tekee yhteistyötä moto- ja aliurakoitsijoiden kanssa puutavaran hankinnan yhteydessä. Tuodessaan puutavaraa puutavaranvastaanottoon sahalle, urakoitsija käyttää tiloissa sijaitsevan koneen avulla yrityksen Puuha-ohjelmaa, josta hän näkee myyjän nimen avulla kaupan kohteen. Ohjelmasta hän näkee siis vain metsänmyyjän nimen ja kaupan numeron, sillä henkilötietoja ja mahdollisesti arkaluonteista tietoa sisältävään kauppakirjaan pääsy on estetty. Vastaanottotodistukseen urakoitsija kirjoittaa yleensä edellä mainittujen lisäksi lisätietoja, jotka hän on saanut yritykseltä tai myyjältä. Jotta urakoitsijat käsittelevät henkilötietoja turvallisella tavalla, metsäosasto on laatinut yhtiön auto- ja korjuuyrittäjille yrittäjäsopimukseen henkilötietojen käsittelyä koskevan liitteen. Liitteessä on ohjeet EU:n tietosuoja-asetuksen mukaiseen henkilötietojen käsittelyyn ja siinä kerrotaan koneyrittäjää koskevat velvoitteet. Urakoitsijan on sitouduttava noudattamaan liitteen sisältöä ja allekirjoitettava se vakuudeksi.

5.7 Suositeltavat muutokset tietosuojan takaamiseksi

Tehdessämme nykytila-analyysia huomasimme, että yrityksessä oli muutamia tietosuojariskin aiheuttavia tekijöitä. Laadimme raportin, jossa kerroimme havainnoistamme ja suosittelimme muutamien muutoksien tekemistä toimintatapoihin henkilötietojen tietosuojan turvaamiseksi.

Yrityksellä ei ole arkistointisuunnitelmaa. Työntekijöillä ei ole virallista ohjeistusta siitä, kuinka kauan aineistoa tulee säilyttää tai miten ne tulee nimetä ja säilöä. Arkistossa on paljon henkilötietoja, sillä kaikki palkka-aineisto säilötään sinne. Palkka-aineistoa ei ole kertaakaan hävitetty yrityksen toiminnan aikana, joten arkistossa on paljon tarpeettomia henkilötietoja. Henkilötietojen minimoinnin toteutumiseksi turha ja hävittämiskelpoinen aineisto tulisi tuhota. Myös aineiston nimeäminen on jokaisen työntekijän omalla vastuulla eikä siitä ole annettu erillisiä ohjeita. Nimikkeessä lukee yleensä aineiston tyyppi sekä ajanjakso, jolta se on kerätty. Jos nimike on merkitty virheellisesti tai sitä ei ole ollenkaan, henkilötiedot voivat joutua väärään paikkaan ja niiden tietosuoja vaarantuu. Laadimme yritykselle arkistointisuunnitelman, jonka pohjalta he voivat toimia jatkossa. Ennen sen käyttöönottoa olisi kuitenkin suositeltavaa päivittää arkistot ajan tasalle ja tuhota kaikki hävityskelpoiset aineistot.

Yrityksen työntekijöillä on työasemiltaan yhteys palvelimella oleviin omiin henkilökohtaisiin kotihakemistoihin, joihin pääsee vain omilla toimialueen käyttäjätunnuksilla. Kotihakemiston kansioihin he keräävät tarpeellisia tietoja, jotka saattavat sisältää esimerkiksi palkkaohjelmasta saatuja henkilötietoja. Kansiot olisi hyvä käydä läpi ja poistaa tarpeettomat henkilötiedot, jotta niitä ei ole tallennettu muualle kuin rekistereihin.

Myös lukituksen kanssa on ongelmia, niin päätteiden kuin tilojenkin. Yrityksen toimistotiloissa vain muutamassa huoneessa on lukollinen ovi. Tälle asialle ei voida mitään, mutta huoneet joissa on lukot tulisi lukita aina paikalta pitemmäksi aikaa poistuttaessa. Jokainen työhuone sisältää kuitenkin asianmukaiset lukolliset kaapit, joihin henkilötietoja sisältävät tai muuten salassa pidettävät asiakirjat voidaan laittaa. Työntekijöiden tulisi täten pitää huolta, että kaikki henkilötietoja sisältävät aineistot laitetaan kyseisiin kaappeihin. Kaappien kanssa on kuitenkin sama ongelma kuin ovienkin kanssa: työntekijät eivät lukitse niitä työpaikalta lähtiessään. Tämä antaa vapaapääsyn ulkopuolisille työntekijöiden huoneisiin työaikaan, jos he eivät ole paikalla, sillä toimiston alaovi on auki päivisin. Asianosattomilla on pääsy myös toimistorakennuksessa olevaan lähiarkistoon, koska sen ovea ei pidetä lukossa, vaikka olisi mahdollista. Suurin osa henkilötiedoista, jotka ovat paperisessa aineistossa, sijaitsee arkistossa. Täten arkiston lukitsematta jättäminen aiheuttaa huomattavan tietosuojariskin. Toimistotyössä työnteko painottuu päätetyöskentelyyn ja suurin osa tiedoista on tietokoneella. Täten olisi tärkeää vaihtaa sopivin väliajoin salasanat ohjelmiin ja tietokoneelle. Salasanojen säännöllistä vaihtamista ehdotettaessa kävi ilmi, että yritys oli kokeillut sitä jo aikaisemmin, mutta he olivat kokeneet sen epäkäytännölliseksi. Tästä huolimatta olisi tietosuojan turvaamisen kannalta tärkeää, että salasanoja vaihdettaisiin. Päätteet tulee lukita aina paikalta poistuttaessa, muuten asianosattomat pääsevät helposti käsiksi koneen tietoihin. Päätteen ollessa auki myös ulkopuoliset voivat helposti lukea esimerkiksi auki jääneen sähköpostin, joka voi sisältää arkaluontoista tietoa kuten henkilötietoja.

6 Dokumentaatio

Euroopan parlamentin ja neuvoston antama tietosuoja-asetus, joka tuli voimaan 24.5.2016, vaatii yrityksiä laatimaan itselleen dokumentaation henkilötietojen käsittelystä yrityksessä. Kyseisen dokumentaation avulla yrityksen tulee kyetä tarvittaessa todistamaan viranomaisille noudattavansa tietosuoja-asetusta luonnollisten henkilöiden henkilötietojen käsittelyssä. Asetuksen kahden vuoden mittainen siirtymisaika umpeutuu 25.5.2018. Yritysten on tehtävä tarvittavat muutokset toimintatapoihinsa ennen kyseistä päivämäärää, toimiakseen asetuksen mukaisesti. (EU:n tietosuoja-asetus 2016/679, momentit 1-3) Kyseisen dokumentaation laatiminen oli opinnäytetyön toiminnallisen osuuden toinen vaihe.

Tietosuoja-asetuksessa ei ole annettu tarkkoja ohjeita sille, millainen dokumentaation tulisi ulkoisesti taikka sisällöllisesti olla. Toimeksiantajan kanssa sovittiin, että dokumentaatiota lähdetään tekemään aikaisemmin tehdyn nykytila-analyysin (liite nro 1) pohjalta. Dokumentaatiosta tulee käydä ilmi muun muassa, mitä henkilötietoja yritys kerää, minne henkilötietoja kerätään, miksi kyseisiä henkilötietoja kerätään sekä miten kerättyjä henkilötietoja käytetään. Kyseiset tiedot olivat koottuna jo nykytila-analyysiin. Virallisen dokumentaation tulee sisältää lisäksi myös toimintaohje tietoturvaloukkaustapauksia varten sekä selostus siitä, kuinka rekisteröityjen oikeuksien toteutuminen varmistetaan. Tietoturvaloukkaus osuuden dokumentaatioon teki yrityksen ATK-vastaava, sillä toimeksiannon alkuvaiheessa sovittiin, että hän hoitaa syvempää tietoteknistä osaamista vaativat osuudet. Rekisteröityjen oikeuksien toteuttamisen kuvaaminen kuului työn tekijöille, joten he lisäsivät nykytila-analyysipohjaan rekisteröityjen oikeuksia käsittelevän osuuden. Word-muotoisen dokumentaation liitteeksi täytettiin Tietosuojavaltuutetun toimiston tietosuojaselostelomakkeet (liite nro 3) jokaisesta yrityksen kolmesta rekisteristä sekä lisäksi yksi työturvallisuuteen kerättäviin henkilötietoihin liittyen. Valmis dokumentaatio tietosuojaselosteineen on opinnäytetyön liitteenä (liite nro 3).

7 Arkistointisuunnitelma

Toimivan asiakirjojen käsittelyn kannalta, jokaiselle yritykselle on tärkeää omistaa omaan toimintaansa sopiva arkistointisuunnitelma. Arkistointisuunnitelman avulla työntekijät tietävät kuinka toimia heidän käytössään olevan aineiston kanssa. Arkistointisuunnitelma sisältää ohjeistuksen asiakirjojen säilytysajasta, -tavasta sekä -paikasta.

7.1 Lähtötilanne

Yrityksellä ei ollut entuudestaan arkistointisuunnitelmaa, joten kehitystehtävää lähdettiin toteuttamaan puhtaalta pöydältä. Asiakirjojen arkistointi oli jokaisen työntekijän omalla vastuulla, koska yrityksellä ei ollut arkistointivastaavaa. Työntekijät nimesivät arkistointimapit itse päättämällään tavalla, sillä tähän ei ollut annettu ohjeistusta. Palkanlaskennasta tullut aineisto merkittiin esimerkiksi Palkanlaskenta, palkkakortit, 2016. Mappien nimiin merkittiin aineiston tyyppi sekä ajanjakso, jolta se oli kerätty ja mahdollisesti muuta yksilöivää tietoa. Mapit, joihin aineisto arkistoitiin, olivat asianmukaisia arkistointimappeja.

Arkistointisuunnitelman puuttumisen vuoksi yrityksellä ei ollut systemaattista aineiston hävittämisjärjestelmää. Aineistoa siirrettiin arkistosta toiseen, kun tila edellisessä loppui. Uusinta aineistoa työntekijät säilyttivät omissa työhuoneissaan käsiarkistossa. Kun käsiarkiston tilat kävivät vähäisiksi, aineistot siirrettiin toimistorakennuksen kellarikerroksessa sijaitsevaan lähiarkistoon. Vastaavasti lähiarkiston täytyttyä asiakirjat siirrettiin yrityksen toisen toimipaikan pommisuojassa sijaitsevaan päätearkistoon. Kun päätearkiston tilat täyttyivät, tilattiin ulkopuolinen asiakirjoja hävittävä yritys hakemaan liiallinen tuhoamiskelpoinen aineisto. Asiakirjoja hävitettiin noin kahden vuoden välein tai tarvittaessa useammin. Poikkeustapauksena oli palkanlaskennasta tulleet asiakirjat, joita ei siirretty lähiarkistosta eteenpäin. Palkkahallinnon asiakirjoja ei myöskään hävitetty missään vaiheessa vaan kaikki yrityksen alusta asti kertynyt palkanlaskentaan liittyvä aineisto on säilytetty. Pöytäkirjat, yrityksen perustamisasiakirjat ja kauppakirjat säilytetään arkistointitilojen sijasta paremman suojan takaamiseksi kassakaapissa tai pankkiholvissa.

7.2 Toteutus

Ensimmäinen vaihe oli perehtyä teoriapohjaan, jotta tiedettiin mitkä ovat arkistointiin liittyvät suositukset niin arkistointitilojen kuin aineistojenkin suhteen. Selvitettiin, millaisissa tiloissa arkiston tulee sijaita, kuinka asiakirjoja tulee käsitellä, miten ja milloin niiden hävittäminen tulee hoitaa, miten asiakirjat arkistoidaan ja tutustuttiin myös alustavasti eri asiakirjalajien arkistointiaikoihin. Hankitun teorian pohjalta kehitettiin haastattelulomake (liite nro 4), jonka avulla selvitettiin arkistoinnin nykytilanne. Myös arkistointiin liittyvät kysymykset laadittiin nykytila-analyysin kysymysten tavoin luetun teorian pohjalta. Haastattelu hoidettiin nykytila-analyysihaastattelun ohella, joten henkilökunta oli tietoinen haastattelusta. Haastattelun avulla saatiin tietää mitä kaikkia arkistoitavia asiakirjoja yrityksen toiminnassa liikkui sekä jokaisen työntekijän yksilölliset arkistointitavat. Tilannetta havainnoitiin myös yrityksen toimitiloja kiertäessä. Yritysvierailuiden yhteydessä käytiin tietysti sekä lähi- että päätearkistossa ja esitettiin näistä kysymyksiä yhteyshenkilölle. Yritysvierailuiden jälkeen koottiin ja analysoitiin kerätty tieto, jotta saatiin kokonaiskuvan yrityksen tämän hetkisestä arkistointijärjestelmästä.

Yritys ei ole kooltaan suuri eikä toimistohenkilöstöä taikka arkistoitavaa aineistoa ole kovinkaan paljon, joten ei lähdetty tekemään kokonaisvaltaista arkistointisuunnitelmaa, johon olisi merkitty esimerkiksi tarkka ohjeistus arkistointimappien nimeämisestä numerokoodien avulla. Yritys toivoi, että arkistointisuunnitelmasta tehtäisiin kuitenkin hieman yksilöity eikä siihen vain koottaisi asiakirjojen suositeltavia säilytysaikoja. Arkistointisuunnitelmaa lähdettiin tekemään siltä pohjalta, että se toimisi uudelle työntekijälle yksinkertaisena opastuksena yrityksen arkistoinnista. Alkuun kirjoitettiin tiivistelmä yrityksen arkistointitavoista. Ensimmäisestä luvusta käy ilmi, miten yrityksen arkistointi käytännössä toimii ja kuinka työntekijöiden tulee sitä toteuttaa. Yleiskatsauksen jälkeen koottiin suositellut asiakirjojen säilytysajat. Sisällysluetteloon lajiteltiin pääotsikoittain asiakirjalajit ja alaotsikoiden avulla asiakirjaryhmät. Täten työntekijällä ei kulu niin paljon aikaa yksittäisen asiakirjan säilytysajan etsimiseen. Esimerkkinä: ensimmäisenä asiakirjalajina on Yleishallinto, joka sisältää yhteisöasiakirjat, viranomaisasiakirjat, sopimustiedostot, yrityssuunnitteluasiakirjat ja hallintopalveluun liittyvät asiakirjat. Arkistointisuunnitelma tehtiin Word-tiedostona ja se löytyy opinnäytetyön liitteistä (liite nro 2).

8 Pohdinta

Opinnäytetyön tarkoituksena oli toimeksiantajalle tehtävien tuotosten lisäksi hankkia asiantuntemusta EU:n tietosuoja-asetuksesta sekä henkilötietojen käsittelystä. Aivan ensimmäisenä vaiheena opinnäytetyössämme perehdyimme laajasti työn teoriapohjaan, sillä teoriataustan hyvä tunteminen oli toiminnallisen osuuden kannalta välttämätöntä. EU:n tietosuoja-asetus oli opinnäytetyön tekovaiheessa todella ajankohtainen asia, joten siihen liittyen löytyi paljon materiaalia myös itse asetuksen lisäksi. Muihin osa-alueisiin, tietosuojaan ja arkistointiin, perehdyimme pääasiassa kirjallisuuden kautta, mutta hyödynsimme myös sähköisiä lähteitä sekä muuta aiheisiin liittyvää materiaalia. Saimme hankittua kattavan teoriapohjan heti alussa, mikä näkyi työn toiminnallisessa vaiheessa.

Toimeksiantomme muokkautui ja tarkentui opinnäytetyötä tehdessä. Vieraillessamme yrityksessä kävi ilmi, että emme laadi koko dokumentaatiota yksin. Osa-alueen haastavuuden ja erityisasiantuntemuksen tarpeen vuoksi yrityksen ATK-vastaava hoiti dokumentaation tietotekniikkaan pohjautuvan osuuden. Kun aloimme tehdä nykytila-analyysia ja sen jälkeen dokumentaatiota, huomasimme että ne olivatkin laajempia kuin olimme ajatelleet. Emme saaneet selkeää ohjeistusta minkään tuotoksen sisällöllisiin tai ulkoasullisiin vaatimuksiin, joten lähdimme tekemään niitä oman näkemyksen pohjalta. Palautettuamme ensimmäiset versiot toimeksiantajalle saimme kuitenkin palautetta tuotokseen liittyen ja samalla käsityksemme yrityksen toiveista parani. Yhteistyömme yrityksen kanssa sujui hyvin ja saimme tarvittaessa apua sekä neuvontaa opinnäytetyöhön liittyen.

Koska kyseessä oli toimeksiantajalle tehtävä toiminnallinen opinnäytetyö, työn tuotokset menevät suoraan yrityksen hyödynnettäväksi. Tuotokset olivat Word-muotoiset nykytila-analyysi, dokumentaatio tietosuojaseloste liitteineen sekä arkistointisuunnitelma. Yrityksen oli viisasta ulkoistaa osittain henkilötietojen käsittelyn päivittäminen EU:n tietosuoja-asetuksen mukaiseksi opiskelijoille, sillä he säästivät siinä omia henkilöstöresurssejaan. Suuremmissa yrityksissä muutokset hoitaa tietosuojavastaava, mutta yrityksellä ei ole nimetty virallista tietosuojavastaavaa sen pienen koon vuoksi. Nykytila-analyysia voitaisiin jatkossa hyödyntää tekemällä sen pohjalta vuosittainen analyysi henkilötietojen käsittelystä yrityksessä. Näin pidettäisiin nykytila-analyysi ajantasaisena ja voitaisiin varmistaa, että toiminta henkilötietojen kanssa on edelleen säännösten mukaista. Vuosittaisen analyysin avulla havainnoitaisiin myös mahdolliset virheet toiminnassa ja niihin voitaisiin puuttua hyvissä ajoin. Arkistointisuunnitelmaa voitaisiin jatkokehittää laajentamalla sen sisältöä. Laatimamme arkistointisuunnitelma sisältää vain asiakirjojen säilytysajat sekä lyhyen

opastuksen siitä, kuinka arkistointi yrityksessä hoidetaan. Siihen voisi lisätä tarkemmat säännökset arkistointikansioiden nimeämistä varten sekä arkistointitapoihin liittyen.

Itse olemme tyytyväisiä työn toteutumiseen. Pysyimme laatimassamme aikataulussa, jossa auttoi Excel-taulukkoon tehty tarkka suunnitelma. Teoriaosuutta saimme laadittua enemmän kuin olimme ensi alkuun ajatelleet. Toiminnallisen osuuden lopputulokset onnistuivat mielestämme hyvin, vaikka aloittaessa ei aina ollut selkeää käsitystä mitä lopputulokselta vaaditaan. Työnjako onnistui suhteellisen tasaisesti, loppuvaiheessa työmäärää saatiin tasattua työn tekijöiden välillä. Yhteistyö ohjaavan opettajan, toimeksiantajan sekä itse työn tekijöiden välillä onnistui hyvin. Nykytila-analyysin yritysvierailu vaiheessa käytimme haastatteluiden tukena laatimaamme haastattelulomaketta, jonka unohdimme hyväksyttää ohjaavalla opettajalla ennen sen käyttöä.

Opinnäytetyön aiheesta meillä ei ollut mitään tuntemusta ennalta, joten aloitimme tiedon keruun aivan perusteista. Ohjaavalta opettajalta olisimme voineet saada enemmän opastusta, jos aiheet olisivat olleet oppitunneilla käytyjä, mutta myöskään hänellä ei ollut syvempää tietämystä tietosuojasta taikka arkistoinnista. Yhteyshenkilömme toimeksiantoyrityksessä oli kuitenkin perehtynyt myös itse EU:n tietosuoja-asetukseen, joten häneltä saimme tärkeää apua työn teossa. Oli kuitenkin mielenkiintoista lähteä tekemään työtä, jossa kaikki eteen tuleva oli uutta. Erityisesti EU:n tietosuoja-asetus kiinnosti meitä, joten teoriapohjan kerääminen oli kiinnostavaa. Aihe oli melko haastava, sillä se pohjautuu pitkälti lakiin. Perehtymiseen kului aikaa ja tiedon ymmärtäminen vaati asioiden pohtimista käytännön kannalta. Haastavuuden ansiosta opinnäytetyö oli kuitenkin kiinnostava ja sen loppuun tekeminen palkitsevaa.

Lähteet

Alapuranen, L., Heino, A., Koskinen, S. & Lehtonen, L. 2012. Henkilötietojen käsittely työelämässä. Porvoo: Edita Publishing Oy.

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

Arkistolaitos. 2013. Määräys ja ohjeet arkistotiloista. Viitattu 25.11.2017. https://www.arkisto.fi/uploads/normit/valtionhallinto/maarayksetjaohjeet/maarays_ja_ohjeet_arkistotiloista01032013.pdf

Arkistolaki 831/1994. Helsinki. Opetusministeriö. 23.9.1994.

Eduskunta. 2018. Hallituksen esitys HE 9/2018 vp. Viitattu 16.4.2018. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx

Euroopan komissio. n.d. Perustietoa Euroopan unionista. Viitattu 29.11.2017. https://ec.europa.eu/info/about-european-union_fi

EU:n tietosuoja-asetus 2016/679. Bryssel. Euroopan parlamentti ja neuvosto. 27.4.2016

Finto. 2016. Kolmannet maat. Viitattu 29.11.2017. https://finto.fi/ysa/fi/page/Y144350

Heljaste, J-M., Korkiamäki, J., Laukkala, H., Mustonen, J., Peltonen, J. & Vesterinen P. 2008. Yrityksen turvallisuusopas. Helsinki: Helsingin seudun kauppakamari.

Itälä, R., Latva-Koivisto, P., Roos, C., & Toivonen, R. 2000. Pureeko ajan hammas: Arkistointi ja asiakirjojen säilytysajat. Helsinki: Liikearkistoyhdistys

Jyväskylän yliopisto. 2010. Suojautumismenetelmät. Viitattu 20.11.2017. https://koppa.jyu.fi/avoimet/mit/virtuaaliset-oppimisympaeristoet/oppimisympaeristoejen-tietoturva/suojautumismenetelmaet

Jyväskylän yliopisto. 2010. Tietoturvauhat. Viitattu 21.11.2017. https://koppa.jyu.fi/avoimet/mit/virtuaaliset-oppimisympaeristoet/oppimisympaeristoejen-tietoturva/tietoturvariskit

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo Finland Oy.

Järvinen, P. 2012. Arjen tietoturva. Jyväskylä: Docendo

Oikeusministeriö 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Viitattu 10.11.2017. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Pitkänen, O., Tiilikka, P. & Warma, E. 2013. Henkilötietojen suoja. Vantaa: Talentum Media Oy

Pixabay. 2018. Liiketoiminta gdpr sääntelyn. Viitattu 17.4.2018. https://pixabay.com/fi/liiketoiminta-gdpr-sääntelyn-3240283/

Pohjola, M., Hakala, P. & Harvilahti, L., 2010. Arkistot kuntoon. Vaasa: Waasa Graphics Oy

Rastas, P. 1994. Arkistotoimi ja asiakirjahallinto. Helsinki: Painatuskeskus Oy

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo Finland Oy.

Tammisalo, T. 2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Helsinki: Stakes

Tietosuojavaltuutetun toimisto. 2013. Tietosuoja-aiheista sanastoa. Viitattu 28.11.2017. http://www.tietosuoja.fi/fi/index/sanasto.html#o-s

Tietosuojavaltuutetun toimisto. 2010. Tietosuojavastaavan toimenkuva, tehtävät ja asema. Viitattu 28.11.2017. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqN4sf1/Tietosuojavastaavan_toimenkuva_tehtavat_ja_asema.pdf

Tietosuojavaltuutetun toimisto. n.d. Tietosuoja turvaa oikeutesi. Viitattu 12.11.2017. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuo-javaltuutetuntoimisto/oppaat/Uiznqahqj/Tietosuoja_turvaa_oikeutesi.pdf

Valtonen, M. R., Roos, C-M., Palonen, O., Toivonen, R. & Järn S. 2009. Vuodesta sataan: Sähköisten asiakirjojen hallinta ja säilyttäminen. Helsinki: Liikearkistoyhdistys

Vanto, J. 2011. Henkilötietolaki käytännössä. Helsinki: WSOYpro OY.

Viestintävirasto. 2017. Organisaatioiden 5 yleisintä tietoturvauhkaa ja 5 toimivaa ratkaisua. Viitattu 21.11.2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/01/ttn201701110903.html

Yrittäjät. n.d. Muista henkilötietojen suoja työelämässä. Viitattu 28.11.2017. https://www.yrittajat.fi/uudenmaan-yrittajat/jokelan-yrittajat-ry/a/yrittajan-abc/yritystoiminnan-abc/henkilotietojen-kasittely-ja-eun-tietosuojauudistus/muista

Liitteet

Liite 1: Nykytila-analyysi (salainen)

Liite 2: Arkistointisuunnitelma (salainen)

Liite 3: Dokumentaatio (salainen)

Liite 4: Haastattelulomake (salainen)