jamk.fi

Muutossuunnitelman laadinta EU:n tietosuoja-asetuksen pohjalta

Case: Kotimainen monialakonserni

Mikael Malste

Opinnäytetyö
Helmikuu 2018
Tekniikan ja liikenteen ala
Tietotekniikan koulutusohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Mikael Malste	Opinnäytetyö, AMK	Helmikuu 2018
	Sivumäärä 55	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: kyllä

Työn nimi

Muutossuunnitelman laadinta EU:n tietosuoja-asetuksen pohjalta

Case: Kotimainen monialakonserni

Tutkinto-ohjelma

Tietotekniikan koulutusohjelma

Työn ohjaaja(t)

Tero Kokkonen, Mika Rantonen

Toimeksiantaja(t)

Sparta Consulting Oy

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Sparta Consulting Oy, joka tarjoaa monipuolisesti ICT-alan konsulttipalveluita. Työn aiheena oli laatia muutossuunnitelma kotimaiselle monialakonsernille Euroopan tietosuoja-asetuksen pohjalta.

Opinnäytetyössä perehdyttiin Euroopan tietosuoja-asetuksen tuomiin haasteisiin asiakasyrityksessä. Toukokuun lopussa 2018 voimaan tuleva, uudistettu koko Euroopan talousaluetta koskeva asetus tuo mukanaan haasteita jokaiselle yritykselle. Suurimpina haasteina yrityksille on kerättävän henkilötiedon minimointi, oikeellisuus, tiedon käyttö alkuperäistä tarkoitusta varten sekä rekisteröidyn oikeus tulla unohdetuksi.

Työn tavoitteena oli tunnistaa asiakasyrityksessä käytössä olevissa prosesseissa sekä järjestelmissä olevat mahdolliset riskitekijät henkilötietojen käsittelyssä ja luoda löydösten pohjalta muutossuunnitelma, jossa huomioidaan Euroopan tietosuoja-asetuksen tuomat haasteet. Muutossuunnitelmassa on jouduttu ottamaan huomioon myös asiakasyrityksen yhteistyökumppanit.

Työ suoritettiin laadullisena haastattelututkimuksena, jossa asiakasyrityksestä haastateltiin avainasemassa olevia henkilöitä. Haastattelutulokset analysoitiin ja niistä luotiin toimenpidesuunnitelma asiakasyritykselle.

Tulosten perusteella kotimainen monialakonserni alkaa toteuttamaan prosessien ja järjestelmien muutostöitä. Tietosuoja-asetus ei suoraan ohjeista toimimaan jollain tietyllä tavalla, vaan asetusta täytyy tulkita parhaan ymmärryksen mukaisesti. Toimenpidesuunnitelma on toteutettu oman tulkinnan ja tiedon perusteella, eikä työssä ole pystytty hyödyntämään lainopillisia tahoja.

Avainsanat (asiasanat)

Euroopan tietosuoja-asetus, GDPR

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Mikael Malste	Bachelor's thesis	February 2018
		Language of publication: Finnish
	Number of pages: 55	Permission for web publication: yes

Title of publication

Drafting change plan based on EU Data Protection Regulation.

Case: Domestic multi-industry corporation

Degree programme

Information Technology

Supervisor(s)

Kokkonen Tero, Rantonen Mika

Assigned by

Sparta Consulting Oy

Abstract

The thesis was assigned by Sparta Consulting Oy, which offers a wide range of ICT consulting services. The objective was to prepare a change plan for a domestic multi-industry corporation based on the European Data Protection Regulation.

The thesis focuses on the challenges of the European Data Protection Regulation in the multi-industry corporation. The revision of the entire European Economic Area regulation, which came into effect at the end of May 2018, brings challenges for every company. The most significant challenge for businesses is to collect a minimum amount of personal data, ensure the correctness of the data, use the collected information for the correct purpose as well as to allow the right of the data subject to be forgotten.

The aim was to identify the potential risk factors in the company's processes and in the systems for the processing of personal data. Additionally, an Agenda was to be created for the change based on the findings-, in accordance with the European Data Protection Regulation, which caused challenges. The conversion plan also had to take the company's partners into account.

The research method was a qualitative interview, with the key persons of the company. The results were analyzed, resulting in an action plan for the company.

Based on the results, the company begins to implement processes and system changes. The regulation does not directly guide employees to work in a certain way. The regulation must be interpreted in accordance with the best understanding. The action plan has been implemented according to the researcher's interpretation and knowledge without any use of legal entities.

Keywords/tags (subjects)

General Data Protection Regulation, GDPR

Miscellaneous

Sisältö

Kuviot

Taulukot

Lyhenteet

CRM	Customer Relationship Management
DMZ	Demilitarized Zone
ERP	Enterprise Resource Planning
ETA	Euroopan talousalue
EU	Euroopan Unioni
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IOT	Internet of Things
IP	Internet Protocol
IT	Information Technology
MDM	Master Data Management
PIA	Privacy Impact Assessment
SLA	Service Level Agreement
URL	Uniform Resource Locator
VPN	Virtual Private Network

1 Työn lähtökohdat

1.1 Taustaa

Opinnäytetyön aihe löytyi harjoittelun aikana asiakasprojektin kautta. Olin mukana tiimissä, jonka tavoitteena oli tuottaa muutossuunnitelma asiakasyritykselle ennen uuden tietosuoja-asetuksen voimaantuloa. Opinnäytetyö sisältää paljon tutkimusta saatujen lähdetietojen perusteella. Näitä ennalta saatuja tietoja sovellettiin eri standardeihin ja asetuksiin, joiden perusteella luotiin asiakasyritykselle tarvittavia muutoksia varten suunnitelma. Euroopan Unionin (EU) tietosuoja-asetus koskettaa jokaista yritystä viimeistään keväällä 2018.

Opinnäytetyö täytyi rajata johonkin osa-alueeseen liian laajan aiheen takia. Lopulliseksi aihealueeksi valikoitui myyntiprosessiin kuluttaja-asiakkaalle liittyvien järjestelmien kartoittaminen, nykytilan selvitys ja nykykäytänteiden saattaminen EU:n tietosuoja-asetuksen mukaiseksi.

1.2 Tutkimus

Opinnäytetyön tutkimuksen pohjalta luotiin muutossuunnitelma asiakasyritykselle sekä dokumentoitiin tarvittavat toimenpiteet ennen tietosuoja-asetuksen astumista voimaan. Tärkeimpänä seikkana oli tutkia, kuinka ja miten yrityksen järjestelmät käsittelevät henkilötietoja. Tutkimuksen tuloksena syntyi suunnitelma, miten henkilötietoja käsitellään, tallennetaan, poistetaan ja siirretään järjestelmien sisällä. Myös henkilötietojen säilytysaikaan kiinnitetään huomiota. Yrityksellä täytyy olla tiedossa, kuinka järjestelmään tallennettu henkilö voi vaatia kaikkia omia tietojaan nähtäväksi tai vaikkapa poistettavaksi ja tulla ns. unohdetuksi.

Työ tehtiin laadullisena haastattelututkimuksena, joka toteutettiin haastattelemalla asiakasyrityksessä avainasemassa olevia henkilöitä. Aineisto kerättiin marras-joulukuun aikana 2017. Tämän jälkeen alkoi tulosten analysointi sekä muutossuunnitelman kehitys. Laadullisesta haastattelututkimuksesta on kerrottu lisää luvussa 5.1.

1.3 Opinnäytetyön toimeksiantaja

Sparta Consulting Oy (myöh. Sparta) on konsulttiyritys, jolla on toimipisteet Helsingissä ja Jyväskylässä. Spartassa työskentelee tällä hetkellä 28 työntekijää. Spartalla on vahva kokemus muutosjohtamisesta, kyberturvallisuudesta, liiketoiminta- ja informaatioarkkitehtuurien konsultoinnista. Yrityksen johto, hallinto ja myynti sekä konsulttitoiminta ovat painottuneet pääkaupunkiseudulle. Jyväskylän toimipisteessä toimii ohjelmistotuotteen tuotekehitysorganisaatio. Sparta on kasvuyritys, joka investoi voimakkaasti tuotekehitykseen. Kuviossa 1 on Sparta Consulting Oy logo. (Sparta Consulting 2017.)

Kuvio 1. Sparta Consulting Oy

1.4 Asiakasyritys

Asiakasyritys toimii usealla eri tuote- ja palvelusegmentillä. Yrityksen asiakkaita ovat sekä kuluttaja- että erilaiset yhteisöasiakkaat. Yrityksellä on liiketoimintaa Itämeren alueella ja se on tietyissä segmenteissä tämän alueen suurin toimija. Yrityksessä työskentelee yli 400 henkilöä ja se teki tilikaudella liikevaihtoa yli 300 MEUR. Yritys on organisoitu konsernirakenteeksi. Maayhtiöt ovat itsenäisiä juridisia yhtiötä. Yhtiön valmistamilla tuotteilla ja tuottamilla palveluilla on päivittäin huomattava määrä loppuhyödyntäjiä. Yrityksen sidosryhminä toimii yhteisöjä, yksinyrittäjiä sekä monitoimipaikkaisia suuryrityksiä. Yrityksen asiakkaiden rooleissa on yrityksiä, talonyhtiöitä ja yksityisasiakkaita.

2 Muutossuunnitelma Euroopan Unionin tietosuoja-asetuksen valossa

2.1 Euroopan Unionin tietosuoja-asetus

Euroopan Unionin tietosuoja-asetuksen, (General Data Protection Regulation, GDPR) tarkoituksena on taata samat säännöt kaikille EU:n alueella toimiville yrityksille ja organisaatioille, jotka käsittelevät EU-kansalaisten henkilötietoja. Henkilötiedoilla tarkoitetaan kaikkia niitä tietoja, joista henkilö tai hänen perheenjäsenensä voidaan tunnistaa. Henkilötiedoiksi luetaan esimerkiksi nimi, osoite, valokuva, henkilötunnus, sijaintipaikka, Internet Protocol (IP)-osoite, työnantajan nimi, tulot ja kulttuurillinen profiili. (EU:n tietosuoja-asetus GDPR 2016.)

Lainsäädäntöuudistuksen takana on kaksi tunnistettua pääsyytä. Ensimmäisenä syynä on tunnistettu internetin valtavaksi korostunut asema ja entistä monimutkaisemmat henkilötietoja sisältävät tietojärjestelmät. Toisena syynä on tunnistettu eri EU-maiden vaihtelevat käytännöt aiemman direktiivin tulkinnassa ja noudattamisessa. (Lloyd 2017.)

Kaikilla yrityksillä on velvollisuus suojella niiden ihmisten oikeuksia, jotka luovuttavat yritykselle omia henkilötietojaan. Suojelemisen varmistamiseksi on määrätty joukko sääntöjä, joita yritysten on pakko noudattaa. Mikäli sääntöjä jätetään noudattamatta, siitä seuraa sanktio. Sanktiot voivat olla huomautus, varoitus, tietojenkäsittelyn keskeyttäminen tai pahimmillaan sakko. Sakko voi olla jopa 20 miljoonaa euroa tai 4 % yrityksen vuosittaisesta liikevaihdosta. (Miinalainen 2017, 6-7.)

Yhtenä suurimmista tunnetuista riskeistä on liian henkilötiedon kerääminen suhteessa käyttötarkoitukseen. Yritysten tulisi kerätä vain se määrä tietoa, joka riittää palvelun tai hyödykkeen toimittamiseksi. Yrityksissä täytyy varmistaa, ettei tietoihin pääse käsiksi liian suuri määrä työntekijöitä. Tietosuoja-asetuksen mukaan kerättyihin tietoihin pääsyä täytyy rajoittaa tietojärjestelmien oikeuksia rajaamalla. Näin varmistutaan, että vain asianmukaisilla henkilöillä on pääsy henkilötietoihin. (Heiskanen 2017, 8-9.)

Tähän asti kussakin maassa on toimittu maan omien lakien ja säännösten mukaan. Lakien ja säännösten noudattaminen yli maan rajojen tapahtuvassa liiketoiminnassa on ollut hankalaa. EU:n tietosuoja-asetus tuli voimaan 24.5.2016, ja siirtymäaika päättyy 25.5.2018. Samat, kaikkia EU-maita koskevat säännöt helpottavat liiketoimintaa ja antavat yksityishenkilölle mahdollisuuden hallita hänestä kerättyjä tietoja. (Miinalainen 2017, 6-7.)

Tietosuoja-asetuksen myötä henkilötietojen käsittelyssä pyritään EU:n tasolla yhteiseen säännöstöön, jossa pyritään turvaamaan rekisteröityjen yksityisyys, itsemääräämisoikeudet, syrjimättömyys sekä henkilötietojen säilytyksen ja käsittelyn läpinäkyvyys. (McDermott 2017.)

EU:n tietosuoja-asetuksessa olennaisessa osassa ovat tiedonhallinnan ja käsittelyn vaatimukset rekisteröidylle henkilölle. Näitä vaatimuksia ovat mm:

- kerättävän tiedon minimointi (vain tarvittava tieto kerätään ja varastoidaan)
- rekisteröidyn oikeus nähdä omat tietonsa ja mahdollisuus omien tietojensa korjaamiseen
- oikeus tulla unohdetuksi
- oikeus omien tietojen siirrettävyyteen sähköisesti luettavassa muodossa

(Sallinen 2017, 4.)

Vielä nykypäivänäkin erittäin harva ihminen tuntee hallitsevansa antamiaan tietoja verkossa. EU:n tietosuoja-asetus antaa henkilölle mahdollisuuden nähdä ja muokata kerättyjä tietoja, tai tulla unohdetuksi kokonaan. Näillä keinoilla henkilötietojen käsittelystä saadaan läpinäkyvää ja luotettavaa. (Kysymyksiä ja vastauksia tietosuojauudistuksesta 2016.)

Tietosuoja-asetus asettaa vaatimuksia ja velvoitteita, joihin tiedon tallentajien ja käsittelijöiden on vastattava määräajassa. Rekisterinpitäjillä on velvollisuus vastata rekisteröidyn tekemään tietopyyntöön ilman aiheetonta viivytystä ja viimeistään kuukauden kuluttua tehdystä tietopyynnöstä. Rekisteröidyn tekemä tietopyyntö pitäisi käynnistää rekisterinpitäjän järjestelmissä prosessin, joka on etukäteen suunniteltu, toteutettu ja todettu toimivaksi. Tiedon tallentajalla/käsittelijällä on toteennäyttämisvelvollisuus, eli hänen on kyettävä todistamaan mistä ja millä tavalla rekisteröidyn

tiedot on poistettu. Kaikki tiedon poistossa toteutetut vaiheet on suoritettava jäljitettävällä tavalla, jolloin jokainen tehty vaihe voidaan todentaa rekisteröidylle. (Sallinen 2017, 4.)

Yrityksillä on myös velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta tietosuojaviranomaiselle 72 tunnin kuluessa loukkauksen havaitsemisesta. Rekisteröidylle henkilölle on kyettävä ilmoittamaan viiveettä, mikäli loukkaus todennäköisesti aiheuttaa hänelle haittaa. Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. (Talus, Autio, Hänninen, Pihamaa & Kantonen 2017.)

Yritykset eivät pysty ratkaisemaan EU:n yleisen tietosuoja-asetuksen vaatimuksia yksistään valmiilla tuotteella. Yritysten on mietittävä asetusta koko yritystä koskevana kokonaisuutena. Jokainen yritys joutuu toteuttamaan oman räätälöidyn muutosprosessinsa. Valmista ulkopuoliselta toimijalta ostettavaa ratkaisua ei tule missään vaiheessa tarjoille, vaan ratkaisussa tulee kytkeä yhteen yrityksen prosessit sekä henkilötietoja käsittelevät järjestelmät. Jokaisen rekisterinpitäjän on laadittava asiakirja, josta tulee ilmetä mm. henkilötietojen käsittelyn tarkoitus, mihin tietoja luovutetaan ja kuvaus rekisterin suojauksesta. Mikäli henkilötietoja ei enää tarvita, tulee ne hävittää järjestelmästä, ellei niiden säilyttämiselle ole laillista perustetta. Yritysten täytyy pystyä perustellusti todentamaan, miksi henkilötietoja kerätään, mihin niitä käytetään ja kuinka pitkään tietoja säilytetään. (EU:n tietosuoja-asetus GDPR 2016.)

Henkilötietoja voidaan rekisteröidyn poistopyynnöstä huolimatta säilyttää, mikäli säilytykseen on lakisääteinen peruste. Perusteena voi olla mm. kirjanpidollinen säilytystarve tai sopimuksien säilytystarve. Kirjanpidon lakisääteinen säilytystarve on kuusi vuotta, jonka aikana rekisteröity ei voi tulla unohdetuksi. (EU:n tietosuoja-asetus GDPR 2016.)

Tietosuojaviranomaisten asema tulevassa uudistuksessa on myös herättänyt keskustelua kansainvälisesti. Euroopan-Unionin tietosuojaviranomaiset ovat itsenäisiä toimijoita, joille on myönnetty omat valtuudet. Tietosuojaviranomaiset valvovat tietosuojaa EU:ssa ja valvontaviranomaisten yhteistyö alueella on lisääntynyt huomatta-

vasti. Tietosuojaviranomaiset ovat ilmaisseet olevansa huolestuneita heihin kohdistuvasta paineesta tietosuoja-asetuksen astuessa voimaan. Uudistus tulee lisäämään viranomaisten yhteistyötä entisestään, mutta epäselvää on, kuinka paljon asetus tulee yhdentämään eri maiden käytäntöjä ja kuinka paljon viranomaisille jää kansallista liikkumavaraa. (Barnard-Wills, Chulvi, De Hert 2016, 587-598.)

Asetuksen epäselvyys ja ongelmat kieliasioissa yhteistyötä tehdessä ovat nousseet myös esiin tietosuojaviranomaisten taholta. Tietosuojaviranomaiset pitävät tärkeänä viranomaisten välistä yhteistyötä, mutta asetuksen epäillään tuovan mukanaan huomattavia rahallisia kustannuksia, tarvetta lisätä työvoimaa ja perustaa uusia hallinnollisia tehtäviä. Uuden tietosuoja-asetuksen haasteet eivät siis ole vielä selvillä edes avainasemassa toimiville tietosuojaviranomaisille. (Barnard-Wills, Chulvi, De Hert 2016, 587-598.)

2.2 Tietosuojavastaava

Yrityksiin on nimettävä tietosuojavastaava, mikäli henkilötietoja käsitellään laajamittaisesti tai yrityksessä käsitellään arkaluontoiseksi luokiteltua tietoa. Tietosuojavastaavan tehtävänä on laatia, ohjeistaa ja ylläpitää tietosuojaa organisaatiossa sekä valvoa henkilötietojen käsittelyä ja niiden suojausmenetelmiä. Hän on myös vastuussa henkilökunnan tietosuojakoulutuksesta sekä sen toteuttamisesta. Yrityksen tietosuojavastaava vastaa mahdollisista henkilökuntaa tai rekisteröityjä koskevista tietosuojakysymyksistä ja hänet on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn. (Tietosuojavastaavan asema 2017.)

Rekisterinpitäjän, eli henkilötietoja keräävän yrityksen on taattava tietosuojavastaavalle riittävät resurssit, jotka ovat tarpeen tehtävän täyttämiseksi sekä riittävät oikeudet päästäkseen käsiksi henkilötietoihin. Hänellä pitää olla mahdollisuus ylläpitää asiantuntemustaan ja kouluttautua tarvittaessa. Hän toimii myös yhdyshenkilönä valvontaviranomaisten suuntaan mahdollisen tietosuojaloukkauksen tapahtuessa. Tietosuojavastaava raportoi suoraan organisaation johdolle tietosuojan ja tietoturvan tilasta, kehityksestä ja mahdollisista tarpeista. Tietosuojavastaavaa ei saa erottaa tai rangaista hoitamiensa tehtävien vuoksi. (Tietosuojavastaavan asema 2017.)

Tietosuojavastaavaa sitoo salassapitovelvollisuus Euroopan unionin ja maan lainsäädännön mukaisesti. Hän voi suorittaa myös muita tehtäviä tietosuojavastaavan velvollisuuksien ohessa. Rekisterinpitäjän on varmistuttava, ettei muut tehtävät aiheuta eturistiriitoja tietosuojavastaavan velvollisuuksien kanssa. (Tietosuojavastaavan asema 2017.)

2.3 Privacy Impact Assessment

Privacy Impact Assessment (PIA) on haastattelutilaisuus, jossa käydään läpi tietojärjestelmän henkilötietojen käsittelyyn liittyvää teknologiaa, toimitapoja ja turvallisuutta. Taustalla tässä on toukokuussa 2018 sovellettavaksi alkava EU-laajuinen tietosuoja-asetus, sen paikallinen lainsäädäntö, näiden asettamien vaatimusten arviointi ja jatkon kehitystoimet, joilla asetuksenmukaisuutta voitaisiin nostaa. (Shroff 2007.)

Haastattelu ei auditoi tai etsi nykykäytänteistä virheitä. Tavoite on löytää osa-alueita, joilla yrityksen tietosuoja-asetuksen-mukaisuutta voitaisiin tehokkaimmin kehittää ja joista olisi hyötyä tulevaisuudessa myös kehittämään niin järjestelmiä kuin esim. tiedonhallintaa laadukkaamman henkilö-/asiakastiedon suuntaan. (Shroff 2007.)

Haastattelussa on yhdeksän teemaa, joita selvitetään kysymysten keinoin. Nämä ovat: Alustan turvallisuus, fyysinen turvallisuus, kolmannet osapuolet, koulutus, liiketoiminnan jatkuvuus, pääsynhallinta, tiedon luokittelu, tietosuoja ja verkon turvallisuus. Haastateltavat ovat valittu niin, että heillä on ymmärrys järjestelmän liiketoimintakäytöstä, näitä tukevista ja mahdollistavista tekniikoista ja tietovirroista. (Shroff 2007.)

2.4 Service Level Agreement

Service Level Agreement (SLA), eli palvelutasosopimus neuvotellaan asiakkaan ja palveluntarjoajan kesken. Sopimus tarjoaa keinot palveluntarjoajan lupausten todentamiseksi. Sopimus on yhteinen ymmärrys palvelusta, sen sisällöstä ja toteutuksesta. Palvelutasosopimus sisältää kuvauksen palvelusta, palvelun käytettävyyden ja kapasiteetin, vasteajan, ongelmien hallinnan, takuut, palvelukeskeytyksistä toipumisen, so-

pimuksen voimassaoloajan ja mahdolliset sanktiot. Sopimuksen eri osa-alueet voidaan kuvata palvelutason mukaan esimerkiksi Taso 1, Taso 2 ja Taso 3. Yksinkertaisimmillaan SLA-sopimus määritellään dokumentiksi, jossa luetellaan asiakkaan odotukset, näiden mittaustavat sekä ongelmien ratkaisutavat ja mikäli sovituista tavoitteista jäädään, mitkä ovat myyjälle tästä aiheutuvat seuraamukset. (Overby, Greiner & Gibbons 2017.)

2.5 Prosessihaastattelut

Haastattelussa on tarkoitus käydä läpi tietosuoja-asetuksen osalta keskeisiä kysymyksiä: mitä henkilötietoa käsitellään, luovutetaan kolmansille osapuolille, tallennetaan, mihin tietoa käytetään, mitä tietosuojakäytänteitä on käytössä ja esim. miten tiedonlaatua varmistetaan. Prosessihaastattelu on keskusteleva, ei auditointia tai virheiden etsintää. Tarkoitus on löytää henkilötiedon hallintaan ja tietosuojan kehittämiseen keinoja, joilla päästään 2018 toukokuusta alkaen sovellettavan EU:n tietosuoja-asetuksen ja paikallisen lainsäädännön osalta riittävälle tasolle. (Sparta Consulting N.d.)

Haastateltavien ei tarvitse valmistautua erityisesti aiheen läpikäyntiin. Riittää, että haastateltavat tuovat oman tietämyksensä keskusteluun. Mikäli joitain haastattelussa kysyttyjä kysymyksiä jää avoimiksi, niitä voidaan selvittää haastattelun jälkeen. Tarkoituksena on, että näillä haastatteluilla saataisiin myös tarjottua haastateltaville neuvoja ja ohjeita päivittäiseen työhön. (Sparta Consulting N.d.)

2.6 Customer Relationship Management

Asiakkuudenhallintajärjestelmä, eli Customer Relationship Management (CRM) on termi, joka viittaa käytäntöihin, strategioihin ja tekniikoihin, joita yritykset käyttävät hallitakseen ja analysoidakseen asiakasvuorovaikutusta ja -tietoja koko asiakkuuden elinkaaren ajan. Asiakkuudenhallintajärjestelmät on suunniteltu kokoamaan tietoa kaikissa kanavissa, joissa asiakas ja palveluntarjoaja kommunikoivat. Kanavia voi olla esimerkiksi yrityksen internetsivut, puhelinkeskustelut, suoramainonta- ja markkinointimateriaalit sekä sosiaalisen median palvelut. (Bain & Company 2017.)

CRM-järjestelmiin voidaan sisällyttää tietoa asiakkaiden henkilötiedoista, kulutushistoriasta ja ostomieltymyksistä. Järjestelmät yhdistävät asiakastiedot ja kaikki asiakkaisiin liittyvät asiakirjat yhdeksi yhtenäiseksi tietokannaksi. Tämä helpottaa järjestelmän käyttäjiä ja kaikki olennainen asiakkaaseen liittyvä tieto löytyy yhdestä keskitetystä paikasta. Järjestelmiin voi tallentua mm. asiakkaan kanssa vaihdetut sähköpostit, puhelut ja sosiaalisen median viestit ja työnkulun prosessien automatisointi. (Schiff 2011.)

2.7 Master Data Management

Master Data Management (MDM), tarkoittaa yrityksen ydintiedon hallintaa, tai liiketoimintakriittisen perustiedon hallintaa, jossa avain on tiedon omistajuudessa. Järjestelmän tarkoitus on luoda yritykselle luotettava ydintiedon lähde. MDM sisältää tiedonhallinnan prosessit, linjaukset, standardit ja välineet, joiden avulla organisaatio varmistaa tiedon yhdenmukaisuuden, hallinnan, oikeellisuuden sekä vastuunjaon. Järjestelmää voidaan käyttää poistamaan päällekkäisyyksiä, standardoimalla dataa ja yhtenäistämällä sääntöjä virheellisen tiedon järjestelmään pääsyn estämiseksi. (Laatikainen 2015.)

2.8 Enterprise Resource Planning

Toiminnanohjausjärjestelmä eli Enterprise Resource Planning (ERP) on toiminnan ja resurssien suunnitteluun ja hallintaan kehitetty tietojärjestelmä. Järjestelmä voi sisältää kirjanpidon, laskutuksen, varastonhallinnan, tuotannonohjauksen, sekä prosessien, materiaalien että resurssien hallinnan. Nykyaikaisissa järjestelmissä yrityksen tarvitsemat osat voidaan valita käyttötarpeen mukaan moduuleina. Usein ERP- järjestelmä on kytkettynä yrityksessä käytettävään CRM-järjestelmään. (Klinge 2017.)

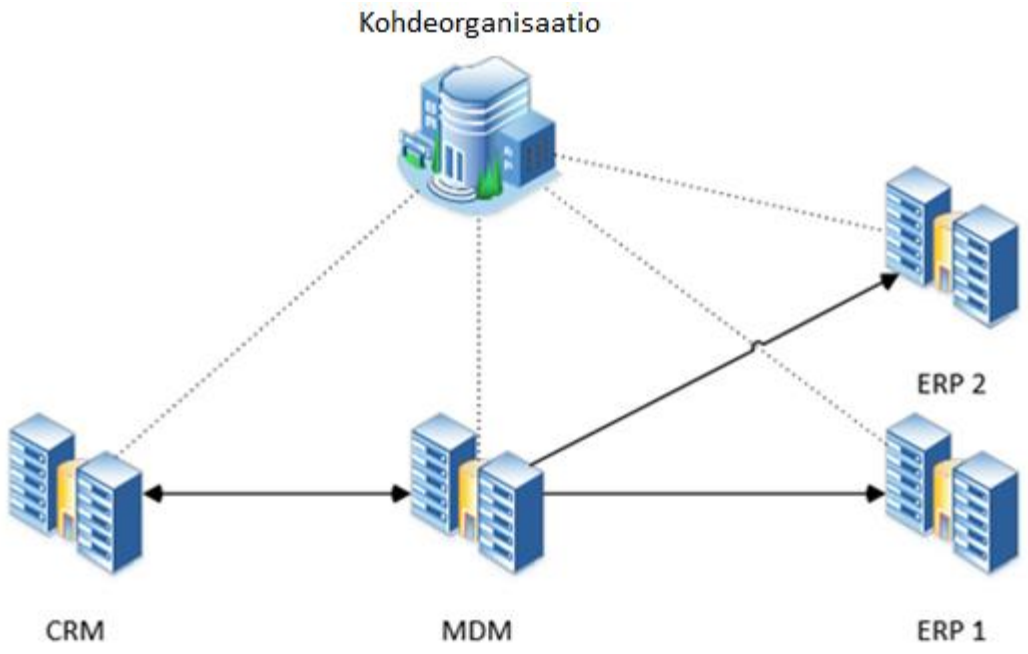
ERP-järjestelmässä tiedot eri toimintojen välillä voidaan tallentaa yhteen ja samaan paikkaan, jolloin saadaan reaaliaikaista tietoa. Keskitettyä tietoa voidaan hyödyntää kaikkien yritysten osastojen kesken samanaikaisesti. Järjestelmästä saadaan tietoa missä resursseja tarvitaan lisää ja mistä niitä voidaan vähentää. Päätöksenteosta saadaan nopeampaa tiedon ollessa heti saatavilla. (Klinge 2017.)

Yrityksen kaikkien osastojen tiedot ovat saatavilla reaaliajassa järjestelmästä, joten yrityksen kehittäminen ja osastokohtainen suunnittelu helpottuu. Järjestelmän tiedot ovat aina ajan tasalla ja päätöksentekoa ei tarvitse lykätä tarkastelukauden raporttia odotellessa. ERP-järjestelmät ovat vähentäneet paljon manuaalista työtä, joten toiminta tehostuu ja yrityksen resursseja voidaan keskittää muihin tehtäviin. (Klinge 2017.)

3 Muutossuunnitelman kohdejärjestelmät ja -alustat

3.1 Yleistä kohdejärjestelmistä ja -alustoista

Myyntiprosessiin liittyvät järjestelmät ja myyntiprosessin läpivienti on kuvattu tarkemmin liitteessä 1. Myyntitapahtuman aikana henkilötietojen käsittelyyn osallistuu neljä eri järjestelmää, joita havainnollistettu kuviossa 2. Luvussa kuvataan järjestelmien käyttötarkoitukset ja keskeiset ominaisuudet. Järjestelmien ylläpitoa hoitavat useat eri yhteistyökumppanit ja ne toimivat pilvipalveluna Euroopan talousalueen (ETA) sisällä tai yhteistyökumppanien omissa konesaleissa Suomessa.



Kuvio 2. Myyntiprosessin järjestelmät

Luvuissa 3.2 – 3.5 kerrotaan, millaisella alustalla järjestelmät toimivat, kuka on vastuussa kehitystyöstä, järjestelmän saatavuus, kuka vastaa alustan ja järjestelmien ylläpidosta ja kuinka tietoturva on otettu huomioon.

3.2 CRM-järjestelmä ja alusta

CRM-järjestelmä sisältää yli 20000 asiakkaan tiedot. Järjestelmään kirjaudutaan ulkopuolisen ohjelmistotalon internetsivujen kautta. Järjestelmä on auki internetiin, ja käyttäjän todennus tapahtuu henkilökohtaisia käyttäjätunnuksia käyttämällä. Myynti asiakkaalle voi tapahtua verkkokaupan, sähköpostin tai puhelimen välityksellä. Järjestelmä pitää kirjaa asiakassopimuksista ja kaikesta muusta dokumentaatiosta, mitä asiakassuhteen hoitamiseen tarvitaan. CRM-järjestelmään tuodaan asiakastietoa yrityksen Master Data Management (MDM)-järjestelmästä. Järjestelmällä on siis melko suuri strateginen merkitys liiketoiminnan kannalta. Järjestelmän sisältämä tieto luokitellaan sisäiseksi, luottamukselliseksi ja salaiseksi. Myyntitapahtuman jälkeiset asiakkaan yhteydenotot tallentuvat suoraan CRM-järjestelmään, josta niitä päästään tarvittaessa lukemaan. Järjestelmä toimii pilvipalveluna ulkoisen palveluntarjoajan konesalissa ETA-alueen sisällä. Järjestelmän sisältävä tieto säilytetään myös ETA-alueen sisäpuolella.

Yrityksen käyttämä CRM-järjestelmä toimii kokonaisuudessaan ulkoisen palveluntarjoajan ylläpitämänä pilvipalveluna. Järjestelmä on kehitetty omana tuotantona ja teknisestä konsultaatiosta vastaa ulkopuolinen yritys. Teknistä konsultointia tekevällä yrityksellä on pääkäyttäjän oikeudet järjestelmään. Pääkäyttäjät pääsevät tarvittaessa tekemään pyydettyjä muutoksia järjestelmään. Järjestelmään liittyvät osapuolet on kuvattu taulukossa 1. Palveluntarjoajalla on palvelimia ympäri maailmaa, ja asiakasyritys voi päättää, millä talousalueella haluaa tietojansa säilytettävän. Järjestelmä vaatii ympärivuorokautista saatavuutta, joka on otettu huomioon palvelutasosopimusta (Service Level Agreement, SLA) tehtäessä. Etäkäyttö ja järjestelmien välinen tiedonvälitys on toteutettu Transport Layer Security (TLS) -protokollaa käyttäen. Mikäli järjestelmään haluaa kirjautua tuotantoympäristön ulkopuolisen hallintayhteyden kautta, vaaditaan käyttäjältä kaksivaiheinen tunnistus yhteyden saamiseksi.

Taulukko 1. CRM-järjestelmään liittyvät osapuolet

Järjestelmän kehittäjä:	Oma kehitys
Järjestelmän ylläpito:	Pilvipalvelu
Alustan ylläpito:	Järjestelmän toimittaja
Järjestelmätyyppi:	Avoinna internettiin

Varmuuskopiointi hoidetaan viikoittain ottamalla täysi kopio järjestelmän sisältämästä tiedosta. Kopiosta voidaan tarvittaessa palauttaa kaikki tieto tai haluttuja osia täydestä kopiosta. Varmuuskopio on saatavilla palveluntarjoajan pilvipalvelusta ennalta määritellyn ajan. Tämän jälkeen varmuuskopio poistuu automaattisesti roskakoriin, josta se on vielä mahdollista palauttaa tietyn ajan sisällä. Roskakorista on siis mahdollista palauttaa määritellyn aikavälin varmuuskopiot tarvittaessa.

3.3 MDM-järjestelmä ja alusta

Asiakasyrityksen MDM-järjestelmä sisältää kaiken yrityksen liiketoimintakriittisen materiaalin. Järjestelmä sisältää mm. asiakas- ja toimittajatiedot. MDM:sta on integraatioita useisiin eri järjestelmiin ja järjestelmä on yrityksen sisäinen. Myyntiprosessissa käytettävä asiakkuudenhallintajärjestelmä on yksi näistä integraatioista. Järjestelmä pitää sisällään yli 20000 asiakkaan henkilötiedot. MDM-järjestelmä toimii ulkoisen palveluntarjoajan konesalissa Suomessa. MDM:n sisältämä tieto säilytetään myös ETA-alueen sisäpuolella.

MDM pitää myös huolta asiakaskontaktien tallennuksesta, jotka tuodaan asiakkuudenhallintajärjestelmästä. Järjestelmän strateginen merkitys on erittäin suuri ja sen sisältämä tieto luokitellaan luottamukselliseksi.

MDM-järjestelmä toimii kokonaisuudessaan ulkoisen palveluntarjoajan konesalissa Suomessa. Konesalin palveluntarjoaja hoitaa palvelinten huollot ylläpidon. Heillä on pääkäyttäjän oikeudet hallitsemiinsa palvelimiin, mutta palvelinten sisältämiin tietoihin he eivät pääse käsiksi. Itse MDM-järjestelmää ylläpitää eräs ulkopuolinen taho. Nimetyillä pääkäyttäjillä on pääsy järjestelmän sisältämään tietoon. Järjestelmän kehityksen taustalla on useita eri tahoja. Taulukossa on 2 esitetty MDM-järjestelmään liittyvät osapuolet.

Taulukko 2. MDM-järjestelmään liittyvät osapuolet

Järjestelmän kehittäjä:	Useita
Järjestelmän ylläpito:	Yritys 1
Alustan ylläpito:	Ulkoinen palveluntarjoaja 1
Järjestelmätyyppi:	Sisäinen järjestelmä

Alustaan on tehty kovennus yrityksen oman ohjeistuksen mukaisesti. Käytössä on myös monipuolinen uhkia analysoiva -ohjelmisto. Järjestelmän alusta toimii virtuaalisena, joka on kahdennettu palveluntarjoajan toimesta. Järjestelmä pystytään ajamaan ylös levykuvaa käyttäen toisessa virtuaalikoneessa laiterikon sattuessa. Palautusaika laiterikon sattuessa on muutamia tunteja.

Käyttäjät tunnistetaan henkilökohtaisilla käyttäjätunnuksilla, jotka ovat riittävin käyttäjäoikeuksin varustettuja. Järjestelmään on mahdollista kirjautua myös ulkoverkon kautta, mutta kirjautuminen vaatii Virtual Private Network (VPN) -yhteyden yrityksen sisäverkkoon. VPN-yhteyden muodostaminen vaatii kirjautumisen yrityksen myöntämillä käyttäjätunnuksilla.

3.4 ERP-järjestelmä 1 ja alusta

Yrityksen ERP-järjestelmä sisältää keskitetysti koko konsernin taloushallinnon ja toiminnanohjauksen. Taloushallinnon komponentit sisältävät mm. myynti- ja ostotoiminnot, tuotannonohjauksen, varaston- ja projektien hallinnan ja tuotetiedonhallinnan. ERP-järjestelmällä on myös useita integraatioita yrityksen muihin järjestelmiin. Kyseessä on yrityksen sisäisesti käytettävä järjestelmä, johon on tarvittaessa mahdollista päästä käsiksi erillisen Client-ohjelmiston kautta etänä. Toiminnanohjausjärjestelmän strateginen merkitys yrityksessä on erittäin suuri ja vaatii ympärivuorokautista saatavuutta. Järjestelmä pitää sisällään yli 20000 asiakkaan henkilötiedot. Tiedot ovat luokiteltu sisäiseksi sekä luottamuksellisiksi. Järjestelmä toimii ulkoisen palveluntarjoajan konesalissa Suomessa ja tiedot säilytetään ETA-alueen sisäpuolella.

Myös ERP-järjestelmä toimii ulkoisen palveluntarjoajan konesalissa Suomessa. Erona edelliseen on, ettei konesalin palveluntarjoaja hoida alustan ylläpitoa. Ylläpidon hoitaa ulkopuolinen taho Yritys 2. ERP-järjestelmää ylläpidetään yhteistyönä Yritys 3:n kanssa. Taulukossa on 3 esitetty MDM-järjestelmään liittyvät osapuolet.

Taulukko 3. ERP-järjestelmään liittyvät osapuolet

Järjestelmän kehittäjä:	Yhteistyönä Yritys 3:n kanssa
Järjestelmän ylläpito:	Yhteistyönä Yritys 3:n kanssa
Alustan ylläpito:	Ulkoinen palveluntarjoaja 2
Järjestelmätyyppi:	Sisäinen järjestelmä

ERP-järjestelmä toiminta on erittäin kriittistä myyntipalvelun kannalta, joten järjestelmältä vaaditaan ympärivuorokautista saatavuutta. Myyntiprosessi ei onnistu, mikäli järjestelmä on hetkenkin poissa käytöstä. Vaikka kyseessä on sisäisesti toimiva järjestelmä, siihen on mahdollista kirjautua tarvittaessa ulkoverkosta. Kirjautuminen vaatii VPN-yhteyden ottamisen yrityksen sisäverkkoon. Käyttäjätunnukset myönnetään yrityksen toimesta ja käyttäjätunnusten ajantasaisuuden katselmointiin on olemassa oma prosessinsa.

3.5 ERP-järjestelmä 2 ja alusta

Asiakasyritys rajasi tästä työstä pois prosessi- ja PIA-haastattelut ERP-järjestelmän 2 osalta. Järjestelmä on osana myyntikokonaisuutta ja siksi esitettynä tämän työn prosessikuvissa sekä järjestelmäkuvauksissa.

4 Prosessit

4.1 Prosessit yleisesti

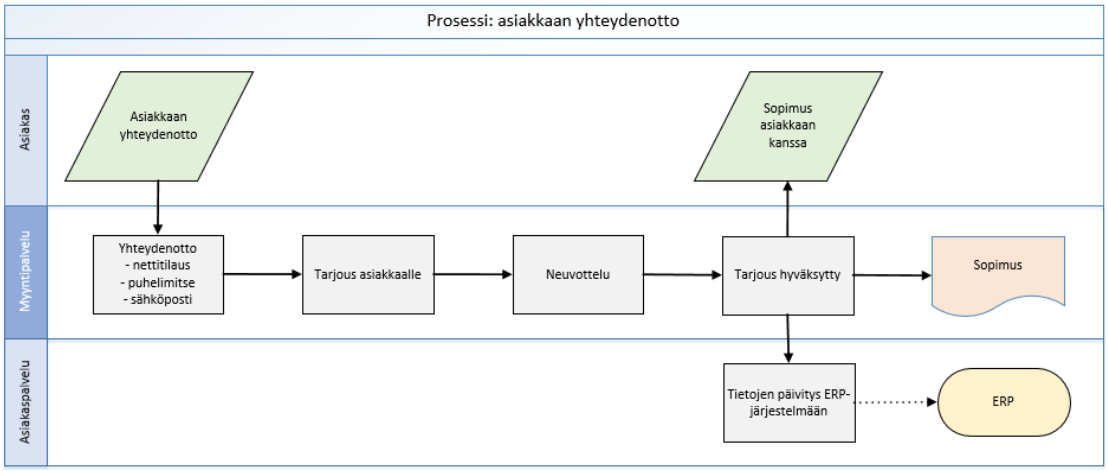
Yrityksessä on lähes kaikki mahdollinen toiminta saatu kuvattua prosessien kautta. Valmiita prosessikuvia on saatavilla koko organisaation laajuudella omasta intranetistä. Hankinnoille, myynneille, henkilökunnan palkkaamiselle, -ylentämiselle ja jopa työntekijän menehtymisen jälkeisille toimenpiteille löytyy oma prosessinsa. Prosessien tarkat kuvaukset eivät sinänsä auta selviämään tietosuoja-asetuksen tuomista haasteista. Lähtökohtaisesti jokainen prosessi on käytävä läpi ja mietittävä, onko jossain prosessin vaiheessa käsitelty henkilötietoja. Mikäli ongelmakohtia löytyy, on niitä muutettava vastaamaan asetuksen vaatimuksia. Yrityksen järjestelmistä yli 20 osallistuu jollain tapaa henkilötietojen käsittelyyn. Järjestelmiä on erittäin vaikeaa ja kallista lähteä muokkaamaan, jotta ne vastaisivat asetuksen vaatimuksia. Osa

järjestelmistä on elinkaarensa loppupuolella ja niiden saattaminen tarvittuun tilaan vaatisi lähes koko järjestelmän tekemistä uudelleen. Huomattavasti helpompaa on ottaa riskikohdat huomioon prosesseja laatiessa. Tiedostetaan ne kohdat, joissa henkilötietoja joudutaan käsittelemään ja varastoimaan. Suunnitellaan ennalta, kuinka tiedon määrä voidaan minimoida jo sen keräysvaiheessa ja poistaa ne tiedon elinkaaren päättyessä. Nämä vaiheet olisi myös kyettävä tekemään niin, että ne pystytään tarvittaessa todentamaan.

Rekisteröidyn unohduspyynnön saapuessa rekisterinpitäjälle tämän tulisi käynnistää prosessi, joka jäljittää kaiken rekisteröidyn tiedon järjestelmistä ja kykenee poistamaan ne todennetusti. Yrityksessä käytettävien järjestelmien lukumäärä huomioon ottaen automatisoitua prosessia ei ole mahdollista toteuttaa. Asiakasprojektin pohjalta yrityksessä mietitään, kuinka prosessien avulla rekisteröityjen tiedot saadaan jäljitettyä eri järjestelmistä.

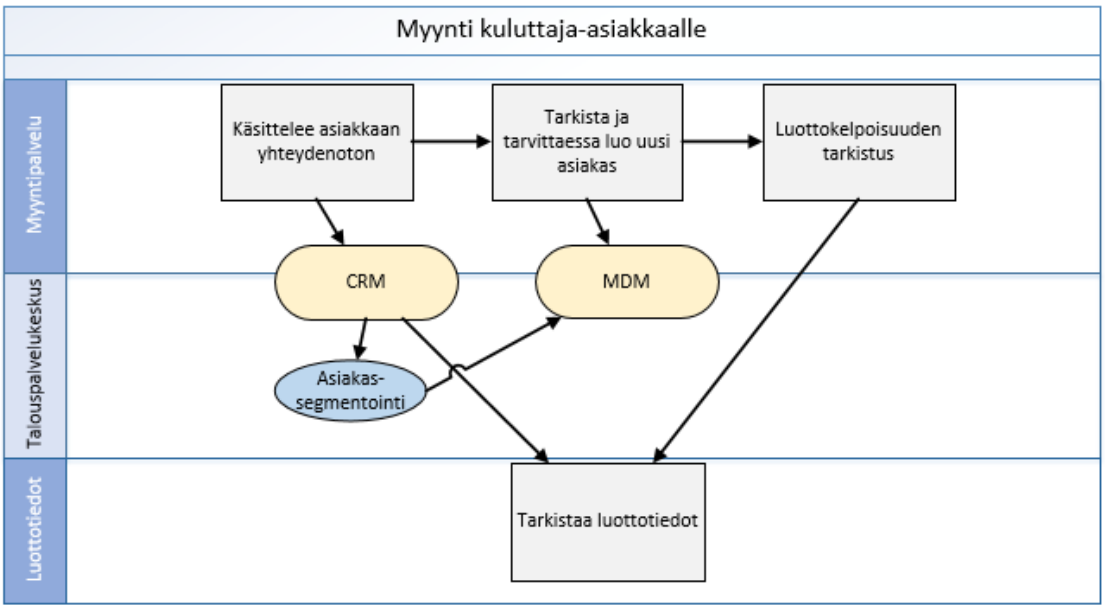
4.2 Kuvaus asiakasyrityksen myyntiprosessista

Myyntiprosessi käynnistyy herätteestä, jossa asiakkaalla on tarve yrityksen tarjoamalle hyödykkeelle. Asiakas voi lähestyä yritystä puhelimitse, sähköpostitse tai internetsivujen kautta. Yhteydenoton jälkeen asiakkaan yhteystiedot ja yhteydenoton syy tallentuvat yrityksen CRM-järjestelmään. Prosessi jatkuu tarjouksen tekemisellä asiakkaalle. Tarjouksen jättämisen jälkeen asiakkaan kanssa järjestetään neuvottelu, jossa asiakas hyväksyy tai hylkää tarjouksen ja toimitusehdot. Tarvittaessa tarjousta muutetaan. Mikäli asiakas on ostanut kiinteähintaisen tuotteen, tarjousta sekä neuvottelua ei tehdä. Asiakkaan hyväksyessä tarjouksen, hänen kanssaan syntyy sopimus. Tilaus päivittyy yrityksen ERP-järjestelmään, ja prosessi lähtee etenemään. Asiakkaan yhteydenotto on havainnollistettu kuviossa 3.



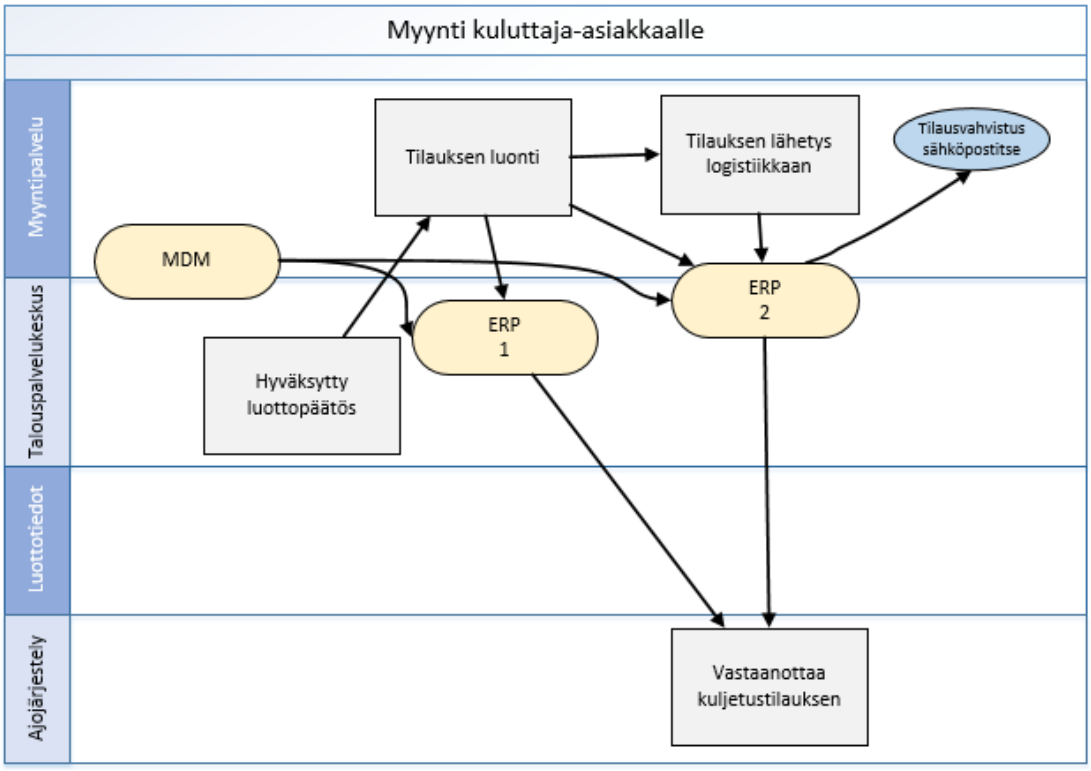
Kuvio 3. Asiakkaan yhteydenotto

Luottokauppaa tehdessä asiakkaan luottokelpoisuus tarkistetaan luotonhallinnasta. Mahdollinen asiakkaan luottohäiriö keskeyttää prosessin, ja asiakasta informoidaan asiasta. Tilausta tehdessään asiakas ilmoittaa, mikäli hänellä on käyttökohteita, joiden käyttöön tilausta ollaan tekemässä. Käyttökohteen perusteella asiakkaat segmentoidaan ja heille tarjotaan jatkossa juuri heidän käyttökohteeseensa sopivia tuotteita. Tämän jälkeen asiakkaan tiedot ja mahdolliset käyttökohteet tallennetaan MDM-järjestelmään. Luottotietojen tarkistusta ja segmentointia havainnollistettu kuviossa 4.



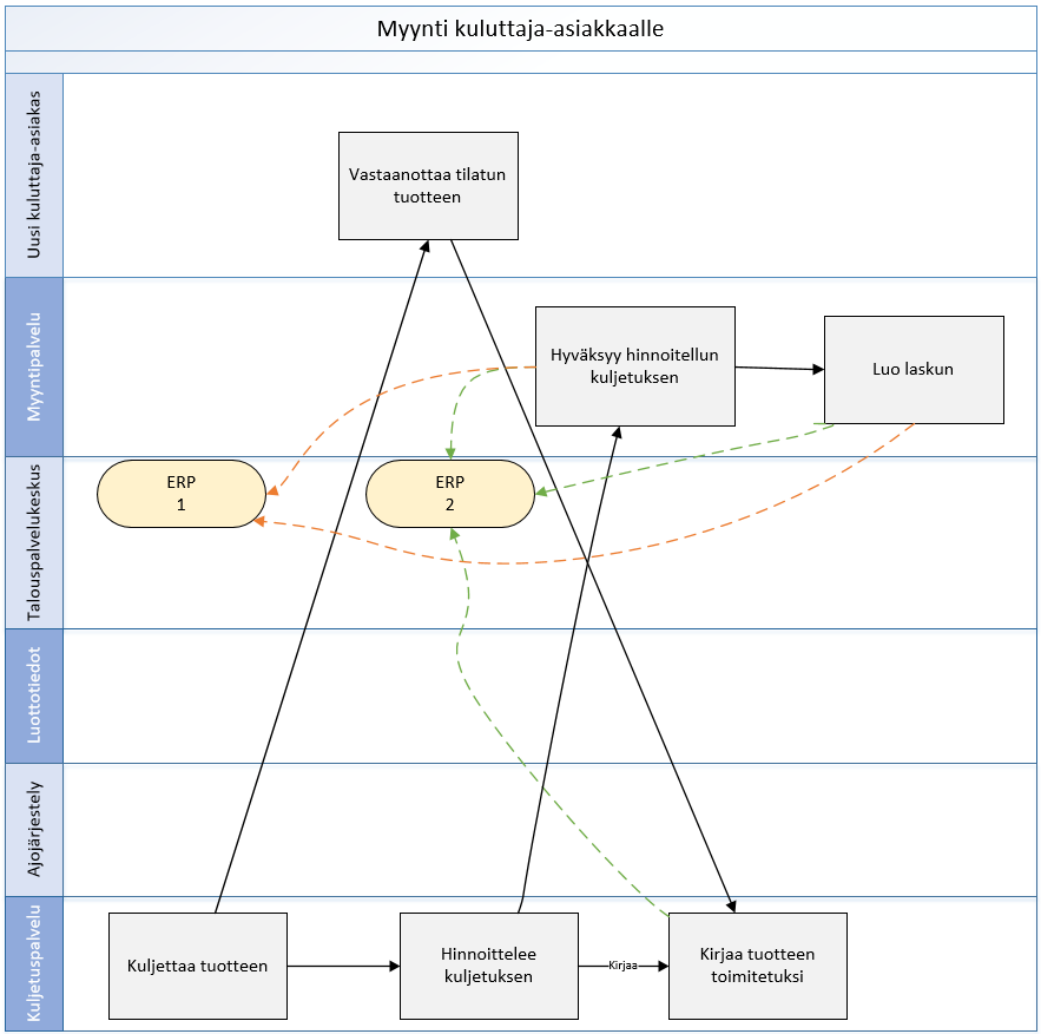
Kuvio 4. Luottotietojen tarkistus ja segmentointi

Onnistuneen tilauksen luonnin ja asiakassegmentoinnin jälkeen tilaus välitetään logistiikan käsiteltäväksi. MDM tallentaa asiakas- ja tilaustiedot molempiin ERP-järjestelmiin. ERP-järjestelmä 2 lähettää tilausvahvistuksen asiakkaan antamaan sähköpostiosoitteeseen. Molemmat ERP-järjestelmät välittävät toimitustiedot ajojärjestelyyn. Kuviossa 5 esitetty tilauksen välitys ajojärjestelyyn.



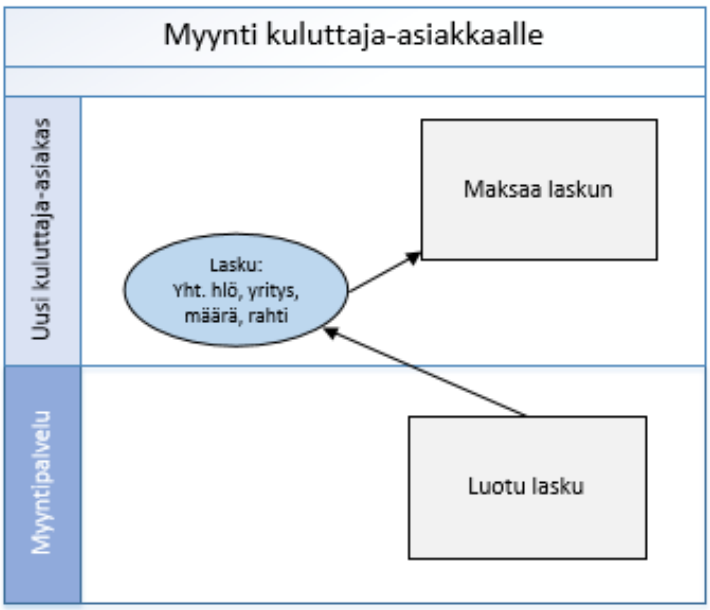
Kuvio 5. Tilauksen välitys ajojärjestelyyn

Tilattu tuote siirtyy ajonjärjestelyn toimesta keräilyyn ja tarvittava määrä tuotetta lastataan kuljetusliikkeen kuljetettavaksi. Rahdin hinta määräytyy lastatun kuorman painon mukaan. Ajojärjestely välittää rahdin hinnan myyntipalveluun, joka kuittaa rahdin hinnan hyväksytyksi. Hyväksyntä tallentuu molempiin ERP-järjestelmiin. Hyväksytystä rahdista muodostuu automaattisesti loppulasku asiakkaalle, jonka tiedot tallentuvat samalla ERP-järjestelmä 1een. Kuljetusliike toimittaa tilauksen asiakkaalle, jonka jälkeen kuljettaja kuittaa tilauksen toimitetuksi ajoneuvopäätteelle. Ajoneuvopääte välittää tiedon toimitetusta tilauksesta ajojärjestelyyn kuvion 6 mukaisesti.



Kuvio 6. Asiakkaan tilaaman tuotteen kuljetus

Rahdin hinnoittelun jälkeen myyntipalvelu lähettää asiakkaalle laskun. Asiakasmaksaa laskun, mikäli tuotteessa ei ole reklamoitavaa. Maksettu tilaus kuittaantuu ERP-järjestelmä 1een. Kuviossa 7 esitetty tilatun tuotteen laskutus asiakkaalle.



Kuvio 7. Asiakkaan laskutus

4.3 Prosessikuvauksen ongelmat

Monissa pitkään toimineissa yrityksissä on vuosien varrella muotoutunut toimivat ja hyväksi havaitut prosessit. Organisaatioissa saattaa olla pitkään talossa olleita työntekijöitä, jotka ovat osallistuneet nykyisten prosessien ja käytänteiden laatimiseen. Hyvin usein ongelmana on, ettei vanhoja ja toimivia toimintatapoja haluta muuttaa. Toimintatapojen ja prosessien muuttaminen saattaa parhaassa tapauksessa tehostaa toimintaa, vähentää kuluja ja kasvattaa tuottavuutta huomattavasti. Tietosuoja-asetus tuo omat haasteensa prosessien uudelleensuunnitteluun. Yritysten eri osastot joutuvat tekemään yhteistyötä, jotta asetuksen tuomat vaatimukset saadaan täytettyä. Organisaatioiden sisällä joudutaan ensimmäisenä miettimään, kuinka saada eri liiketoimintayksiköiden työntekijät ja esimiehet ymmärtämään tietosuoja-asetuksen asettamat haasteet. Asetus ei koske vain tiettyä osaa organisaatiosta, vaan yhteisesti koko yrityksen toimintaa.

Asetuksen myötä esimerkiksi markkinointiosastot eivät saa enää lähestyä jo olemassa olevia asiakkaita markkinointiviesteillä. Asiakkailta on saatava erikseen markkinointilupa, jonka jälkeen heitä saa lähestyä puhelimitse, sähköpostitse tai kirjeitse. Tätä varten on mietittävä, kuinka olemassa olevaa prosessia saadaan muutettua niin,

että tietosuoja-asetusta noudatetaan. Henkilöstöosastojen on myös mietittävä sellaisten työntekijöiden tietojen säilyttämistä, jotka eivät enää syystä tai toisesta työskentele yrityksessä. Onko henkilötietojen säilytykselle riittävät perusteet ja vastaako tallennettu henkilötiedon määrä käyttötarkoitusta. Yrityksen aulapalveluun saattaa tulla sähköpostitse yhteydenottoja, jotka sisältävät henkilötietoa. Prosesseissa joudutaan huomioimaan sähköpostilaatikoiden tyhjennys ja esimerkiksi puhelutallenteiden hallinta, mikäli ne tallennetaan.

Haasteena muutosprosessissa on oman henkilökunnan vastahakoisuus uudistuksia kohtaan. Uudistukset saatetaan kokea epämiellyttävinä, turhina ja liian työläinä. Yrityksessä on toimittu vuosikaudet tietyn mallin mukaan, johon henkilökunta on tottunut. Vanhat toimintamallit koetaan toimivaksi eikä niitä haluta lähteä muuttamaan. Muutosprosessi vaatii projektin vetäjältä määrätietoista toimintaa, jotta henkilökunta ja organisaation kaikki osastot saadaan ymmärtämään muutoksen tarve ja tässä tapauksessa pakollisuus. Tietosuoja-asetusta täytyy katsoa koko organisaatiota koskettavana asiana ja ymmärrettävä, ettei siirtymäajan jälkeen voida enää toimia vanhojen toimintamallien mukaan.

5 Toteutus

5.1 Tutkimusmetodologia

Laadullisella haastattelututkimuksella tutkitaan haastateltavien kokemuksia ja näkemyksiä tutkittavaan aiheeseen liittyen. Sen avulla pyritään ymmärtämään tutkittavaa ilmiötä tai asiaa. Laadullinen haastattelututkimus pyritään yleensä tekemään harkinnanvaraisella otannalla haastateltavia. Teoria on mukana haastatteluissa kahdella tavalla: keinona tutkimuksen tekemisessä ja päämääränä, jolloin tutkimuksella pyritään kehittämään teoriaa edelleen. Tutkimuksessa tarvitaan taustatietoa, jota vasten aineistoa arvioidaan sekä tulkintateoriaa, joka auttaa muodostamaan haastateltaville esitettävät kysymykset. (Kustula 2015.)

Laadullisen ja määrällisen tutkimuksen erona on, että määrällisessä tutkimuksessa tutkimusongelmat muotoillaan tarkasti etukäteen ja laadullisessa tutkimuksessa tutkimustehtävä voi muuttua tutkimuksen aikana. Tulkinnan ja ongelman ratkaisemisen

avulla luodaan tutkimuksen aikana malleja, ohjeita toimintaperiaatteita ja kuvauksia tutkittavasta asiasta. (Vilkka 2007.)

Tutkimuksen haastattelu voidaan suorittaa kirjallisena lomakehaastatteluna tai avoimena haastatteluna. Haastateltavat tulee valita sen mukaan, mitä ollaan tutkimassa. Haastateltavilla tulee olla omakohtaista kokemusta tai asiantuntemusta tutkittavasta aiheesta. Heidät tulee valita riittävän laaja-alaisesti, eri osastoilta ja vastuualueilta. Haastattelutilanteessa on syytä kiinnittää huomiota kysymysten asetteluun, esitystapaan ja esitysjärjestykseen. Kysymysten asettelussa on vältettävä kysymyksiä, joihin haastateltava kykenee vastaamaan muutamalla sanalla tai vastaamalla kyllä tai ei. (Vilkka 2007.)

Riittävän laajalla taustateorialla ja oikeiden haastateltavien valinnalla, tutkimuksesta saadaan erittäin kattava ja vastaamaan alkuperäistä tarkoitustaan. Mikäli haastateltavat ovat liian samanlaisia tai eivät edusta monipuolisesti yrityksen eri osastoja, haastattelutulokset ovat liian suppeita. Tulokset eivät muodostu koko organisaation laajuisiksi ja voivat edustaa vain yhden osaston näkökulmaa. (Vilkka 2007.)

5.2 Haastattelut

Prosessi- sekä PIA-haastatteluihin kutsuttiin organisaation henkilökuntaa monipuolisesti. Tavoitteena oli saada haastateltua järjestelmän omistajat, pääkäyttäjät ja vähintään yksi järjestelmää aktiivisesti käyttävä henkilö. Haastatteluissa oli myös mukana henkilöstöjohtajia, projektipäälliköitä, osastojen vastaavia ja Information Technology (IT)-osaston vastaavia henkilöitä. Haastattelut etenivät ennalta laaditun rakenteen mukaisesti. Niissä nostettiin esiin kriittisimpiä tietosuoja-asetuksen tuomia kohtia ja tavoitteena oli saada kokonaiskuva yrityksen nykytilasta. Haastateltavia pyrittiin saamaan mahdollisimman monipuolisesti eri osastoilta. Näin saadaan kattava kokonaiskuva järjestelmien käyttäjistä ja heidän tietotaidostaan.

Järjestelmiä ylläpitävät ulkoiset yhteistyökumppanit ovat auditoitu jo yritysten tehdessä sopimuksia keskenään. Auditointeja suoritetaan ennen vuoden 2018 toukokuuta, mikäli niihin on tarvetta. SLA-sopimukset, rekisteriselosteet ja prosessikuvat tarkastellaan muutosprosessin aikana ja myös niitä päivitetään tarvittaessa.

6 Tulokset

6.1 Kuvaukset löydöksistä: CRM

CRM-järjestelmän PIA-haastatteluun osallistui asiakasyrityksestä tieto- ja Information and Communications Technology (ICT)-osastolta järjestelmän omistaja, -vara- omistaja, järjestelmän pääkäyttäjä ja markkinointiosastolta järjestelmän pääkäyttäjä. Tässä kappaleessa kerrotaan CRM-järjestelmässä havaitut puutteet ja huomiot. Löydösten perään on kirjattu tietosuoja-asetuksen kohta, johon se viittaa. Kappaleen loppuun on kirjattu lyhyt yhteenveto tutkimuksen löydöksistä.

Tietosuoja-asetuksen artiklojen 25 ja 30 mukaan järjestelmien dokumentaation täytyy sisältää erittelyn, miten henkilötietoja käsitellään, kuvaukset tietovirroista, selvityksen tietovarantojen omistajista, ohjeet tiedon luokittelusta, selvityksen tiedon fyysisestä ja loogisesta sijainnista sekä ohjeet henkilötiedon turvallisesta käsittelystä. Tutkimushaastattelussa havaittiin, ettei tietoa ole luokiteltu ja tietoon pääsee käsiksi yrityksen sisältä, eikä tarkkaa ohjeistusta ole olemassa. Järjestelmän osalta ei ole dokumentoitu mikä rekisteri- ja tietosuojaseloste ovat kytkettyinä mihinkin järjestelmän tuotantoversioon ja sitä varten kerättyyn henkilötietoon. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 50-51.)

Asetuksen 5. artiklassa vaaditaan, että täytyisi kyetä varmistamaan henkilötietojen käyttötarkoitussidonnaisuus sekä tietojen minimoinnin toteutuvuus. Prosessi täytyisi myös automatisoida. Tutkimuksessa havaittiin, että tietojen siivousta ja minimointia toteutetaan vain tarpeen mukaan. Yrityksessä ei ole olemassa tiettyä aikaväliä jolloin henkilötietojen siivousta suoritetaan. MDM-järjestelmästä tiedonsiirto toimii vielä manuaalisesti, mutta automatisointi on tulossa. (EU:n tietosuoja-asetus (GDPR) 2016, 117-118.)

Tietosuoja-asetuksen 5 artiklassa ohjeistetaan anonymisoimaan tai poistamaan henkilötiedot käyttötarpeen poistumisen jälkeen. Tutkimuksessa havaittiin, että vaikka anonymisointi tai poisto tapahtuisi, MDM-järjestelmän kautta on mahdollista palauttaa poistetut tiedot ja ajaa ne takaisin CRM-järjestelmään. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Viidennessä artiklassa myös vaaditaan ohjeistus, miten kyetään varmistamaan, ettei kerättyjä tietoja käytetä alkuperäisesti määritellyn ja rekisteröidylle informoidun käyttötarkoituksen vastaisesti. Tutkimuksessa havaittiin, ettei yrityksessä ole olemassa ohjeistusta tietojen käyttötarkoituksen määrityksistä. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Rekisteröitävien henkilötietojen käytön oikeusperusteet sekä ohjeistus vaaditaan myös asetuksen viidennessä artiklassa. Yrityksessä järjestelmän sekä rekisteröitävien henkilötietojen käytön oikeusperusteet ovat sopimukset, laskutus, markkinointi ja toimitus. Tähän ei ole vielä olemassa ohjeistusta. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Viidennen sekä 28. artiklan mukaan vaaditaan tarkka kuvaus, mikäli tietoja siirretään tai luovutetaan järjestelmistä. Tiedonsiirtoprosessien tulisi myös olla automatisoituja. Järjestelmien oikeus- tai käyttöperuste tulisi olla sama, eli onko rekisteröity antanut suostumuksen juuri tähän tiettyyn käyttöön. Tutkimuksessa selvisi, että asiakasyrityksessä CRM-järjestelmään siirretään tietoa MDM- ja ERP 1-järjestelmistä. Tietoja luovutetaan markkinointitarkoituksessa ja asiakastyytyväisyyskyselyyn. Markkinointikiellot päivitetään manuaalisesti asiakkaan pyynnöstä. Järjestelmän tiedonsiirtoprosessit ovat automatisoituja ja niistä kerätään ulkoisen integraation kautta asiakkaiden sähköpostiosoitteet markkinointiviestintää varten. Asiakastietoja lähetetään myös ulkopuoliselle yhteistyökumppanille, joka suorittaa asiakastyytyväisyyskyselyt. Yritysten välillä tiedot kulkevat salatun sähköpostin kautta Excel-tiedostona. Asiakastyytyväisyyskyselyn suorittamisen jälkeen yhteistyökumppani lähettää anonymisoidun raportin asiakastyytyväisyydestä. Yritysten välisessä sopimuksessa on mainittu tietojen hävitysvelvollisuus, mutta sen toteutumista ei valvota. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36, 49-50.)

Asetuksen 13:sta ja 30:ssä artiklassa kuvataan tiedonantovelvoitetta rekisteröidylle. Hänelle tulisi ilmoittaa selkeästi henkilötietojen säilytysaika, käyttötarkoitus, tietosuojavastaavan yhteystiedot ja hyväksyntä henkilötietojen käyttöön. Tutkimuksessa kävi ilmi, että yrityksessä rekisterinpitäjän tiedonantovelvoite toteutetaan verkkosivuilta löytyvällä rekisteri- ja evästeselosteella, josta selviää käyttötarkoitus ja tietosuojavastaavan yhteystiedot. Henkilötietojen käsittelystä pyydetään asiakkaan hy-

väksyntä ruksi ruutuun- periaatteella nettisivujen kautta. Mahdollisissa messukyselyissä henkilötietojen käsittelylupa kerätään erillisellä paperilla. Messuilla kerättyjen henkilötietojen hävityksestä ei ole ohjeistusta olemassa. Rekisteröidylle ei myöskään ilmoiteta henkilötietojen säilytysaikaa. Verkkosivujen kautta tehtävissä tilauksissa markkinointilupaa ei kysytä erikseen, hän on automaattisesti markkinointilistalla ostettuaan yrityksen tuotteen. (EU:n tietosuoja-asetus (GDPR) 2016, 40-41, 50-51.)

Asetuksen 13:sta artiklassa määritetään informointivelvollisuus rekisteri- tai tietosuojaselosteen sisällöstä rekisteröidylle, mikäli henkilötietoja kerätään muuten kuin sähköisesti. Tutkimuksessa havaittiin, ettei rekisteröityä informoida henkilötietojen keräämisestä puhelinkeskusteluissa tai henkilökohtaisen kanssakäynnin aikana. (EU:n tietosuoja-asetus (GDPR) 2016, 40-41.)

Viides artikla määrittelee paikka- ja teletunnistetiedot anonymisoitaviksi tai pseudonymisoitaviksi, mikäli niitä kerätään. Täytyy myös kyetä varmistamaan, ettei tietojen yhdistämistä tapahdu. Paikkatietojen elinkaaresta on myös huolehdittava lainmukaisen käsittelyperusteen päätyttyä. Havaittiin, että CRM-järjestelmää käyttävien henkilöiden henkilökohtaiset Uniform Resource Locator (URL)-osoitteet ovat näkyvissä pääkäyttäjälle. Tarvittaessa järjestelmän kirjautumistiedoista saadaan tulostettua erillinen raportti. Anonymisointia tai pseudonymisointia ei tehdä erikseen järjestelmän käyttäjille. Järjestelmän käyttäjä tietää seurannasta ja hän pystyy myös itse seuraamaan omia kirjautumistietojaan. Seurannasta ei informoida käyttäjää erikseen. Myös tiedon elinkaaren hallintaa ei ole määritetty. Tietojen poiston tai anonymisoinnin suorittaminen ei ole täysin varmaa lainmukaisen käsittelyperusteen päätyttyä. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Asetuksen kahdeksas artikla rajaa alle 16-vuotiaiden tietojen käsittelyn tapahtuvan vain huoltajan suostumuksella tai valtuutuksella. Tutkimuksessa havaittiin, että järjestelmässä saattaa olla alle 16-vuotiaiden henkilöiden henkilötietoja, ilman asianmukaista suostumusta tai valtuutusta. He ovat voineet esimerkiksi osallistua arvontoihin messuilla ja antaneet kirjallisesti henkilötietonsa. (EU:n tietosuoja-asetus (GDPR) 2016, 37-38.)

Viidennen artiklan mukaan rekisterinpitäjän täytyisi varmistaa, ettei asiakkaan tai kuluttajan viestintätietoihin ole pääsyä muilla, kuin järjestelmän omistajilla tai käyttäjillä. Tutkimuksessa kävi ilmi, ettei asiakkaiden puhelut tallennu mihinkään järjestelmään. Vain asiakkaiden yhteydenottopuheluiden kellonaika ja päivämäärä tallentuvat järjestelmään. Mikäli järjestelmän käyttäjä yrittää selata puhelutietoja ulkoverkosta, häneltä vaaditaan vahva kaksivaiheinen tunnistautuminen. Asiakastietojen näkyvyyttä on myös rajoitettu käyttöoikeuksin. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Asetuksen 22. artiklan mukaan rekisteröidylle täytyy kertoa, millainen käsittelylogiikkaa käytetään, mikäli henkilötietojen käsittelyyn liittyy automaattista päätöksentekoa tai profilointia ja mitä seurauksia siitä on rekisteröidylle. Tulosten perusteella havaittiin, että järjestelmässä tapahtuu automaattista käyttäjätilien profilointia. Järjestelmä profiloi käyttäjänsä annettujen käyttäjäoikeuksien perusteella. Markkinointitarkoituksessa kerättyjä henkilötietoja käytetään vain kohdennettua markkinointia varten. Kohdennettua markkinointia suoritetaan aktiivisille asiakkaille, joiden kanssa on tehty kauppaa viimeisen kahden vuoden sisällä. Passiivisen asiakkaan kohdalla voidaan katsoa, onko markkinointilupa annettu ja otetaan yhteyttä, mikäli lupa on annettu. (EU:n tietosuoja-asetus (GDPR) 2016, 46.)

Tietosuoja-asetuksen 32. artikla määrittää järjestelmän palauttamisen sovitun ajan puitteissa, mikäli järjestelmä/alusta kaatuu tai vioittuu. Tutkimustuloksista käy ilmi, että järjestelmästä on saatavilla raportti viikon aikaisista tiedoista. Valittavissa on kaikki tieto, tai jotain haluttuja osia siitä. Halutun tiedon sisältävä raportti on tulostettavissa ja tallennettavissa pilvipalvelusta ennalta määritellyn ajan. Tämän ajanjakson jälkeen tiedot siirtyvät automaattisesti roskakoriin, jossa ne säilyvät tietyn ajan. Tietojen palautusprosessia ei ole vielä testattu ja siitä ei ole ohjeistusta olemassa. (EU:n tietosuoja-asetus (GDPR) 2016, 51-52.)

Artiklat 25 ja 32 määrittävät tietoliikenneverkon vyöhykkeistämisen ja suodatussääntöjen toteutuksen vähimpien oikeuksien ja monitasoisen suojaamisen periaatteiden mukaisiksi. Tutkimuksessa saatiin selville, että järjestelmä toimii pilvipalveluna, joten tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt, monitasoinen suojaa-

minen ja Demilitarized Zone (DMZ)- vyöhykkeistäminen on toimittajan vastuulla. Dokumentaatio näistä edellä mainituista määrityksistä puuttuu. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Artiklat 25 ja 32 määrittävät myös järjestelmäympäristön kolmansien osapuolten kuvauksen sekä roolituksen. Palveluntarjoajan valinnassa tulisi huomioida konsernin ohjeet ja käytännöt sekä valintaprosessi tulisi dokumentoida. Tulosten perusteella järjestelmäympäristön Integraatioihin liittyy kolmansina osapulina kaksi ulkoista yritystä, sekä pääkäyttäjän roolissa kolmas yritys. Verkkokaupan, järjestelmän vianselvityksen ja loppukäyttäjien tuen hoitavat myös ulkopuoliset yritykset. Kyseessä on melko vanha järjestelmä, joten dokumentoinnin puutteiden takia ei ole varmuutta onko palveluntuottajan valinnassa huomioitu konsernin ohjeet ja käytäntö. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

VAHTI-raportin 1/2016 mukaan kolmansille osapuolille tulisi luovuttaa vain ja ainoastaan niitä tietoja, jotka ovat tarpeen palveluntuottajan tehtävien suorittamiseksi. Tämä selvitys tulisi myös dokumentoida. Tuloksista selvisi, että kolmannen osapuolen järjestelmän ylläpitäjälle lähetetään Excel-muotoisena sähköpostiliitteenä järjestelmän päivitettävät tiedot. Tiedon elinkaarta ei pystytä myöskään luotettavasti varmentamaan, eikä prosessista ole olemassa dokumentaatiota. (VAHTI-raportti 2016, 32)

6.2 Yhteenveto

Järjestelmästä tehtiin yhteensä 21 eri havaintoa. Pääsääntöisesti järjestelmän osalta voidaan sanoa, ettei siitä löydy kriittisiä puutteita henkilötietojen käsittelyn kannalta. Suurimmat puutteet havaittiin ohjeistuksessa, dokumentoinnissa ja markkinointiluvan keräämisessä. Tutkimuksessa havaittiin järjestelmien välisen synkronoinnin palauttavan jo kertaalleen poistetut henkilötiedot takaisin CRM-järjestelmään. Tähän on myös kiinnitettävä huomiota.

Haastattelututkimuksessa saatiin nostettua esiin asioita, joita täytyy ottaa huomioon muutossuunnitelmaa tehdessä ja prosesseja uudistettaessa. Löydöksistä suurin osa on painoarvoltaan pieniä, mutta ne on hyvä ottaa huomioon. Osa löydöksistä on helposti saatettavissa tietosuoja-asetuksen vaatimaan tilaan, mutta osa vaatii yritykseltä

enemmän toimenpiteitä. Haastateltavat henkilöt oli valittu riittävän monipuolisesti eri osastoilta ja tutkimustulokset olivat luotettavia.

6.3 Kuvaukset löydöksistä: MDM

MDM-järjestelmän PIA-haastatteluun osallistui asiakasyrityksestä tieto- ja viestintätekniikka- osaston esimies sekä järjestelmän omistajana toimiva pääkäyttäjä. Tässä kappaleessa kerrotaan MDM-järjestelmässä havaitut puutteet ja huomiot. Löydösten perään on kirjattu tietosuoja-asetuksen kohta, johon se viittaa. Kappaleen loppuun on kirjattu lyhyt yhteenveto tutkimuksen löydöksistä.

Järjestelmän dokumentaatio ei sisällä riittävää ohjeistusta tietojen käsittelystä ja tietovirtojen kuvauksista, jotka ovat tietosuoja-asetuksen artikloissa 25 ja 30 kuvattuna. Järjestelmän dokumentaatiosta ei käy ilmi mikä rekisteri- ja tietosuojaseloste on kytkettyinä mihinkin järjestelmän tuotantoversioon ja sitä varten kerättyyn henkilötietoon. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 50-51.)

Henkilötietojen käyttötarkoitussidonnaisuudessa ja tietojen minimoinnissa tavoitteena on vuoden välein tarkistaa asiakastiedot ja putsata tarpeettomat tiedot järjestelmästä. Kaupallista toimintaa varten olennaista tietoa tarvitaan, huomioiden tiedon elinkaari. Asiakkailla ei ole mahdollisuutta muokata omia tietoa MDM-järjestelmään. Asiakaan tekemät muutospyynnöt joudutaan tekemään erillisen portaalin kautta. Erään organisaatioyksikön verkkokauppa ei vaadi asiakkaan kirjautumista tilausta tehdessä tällä hetkellä. Yrityksen sisällä oma henkilökunta voi tarkastella omia tietojaan ja tarvittaessa pyytää muutosta tietoihinsa henkilöstöhallinnan kautta. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Suuremmissa tietojen minimoimisissa on katsottu mitkä asiakkaat ovat olleet aktiivisia tietyn ajanjakson aikana ja heidän tiedot säilytetään aktiivisina asiakkaina. Loput asiakkaat siirtyvät passiivisiksi, mutta tietoja ei kuitenkaan poisteta järjestelmästä. Vuoden 2018 alusta alkaen aloitetaan yhden vuoden syklillä tekemään tarpeettoman tiedon siivousta. Kirjanpitolaki kuitenkin edellyttää, että tiedot voidaan säilyttää järjestelmässä perustellusti kaupan teon jälkeen kuusi vuotta. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Henkilötietojen elinkaarta suunniteltaessa yrityksessä on otettu huomioon liiketoiminnan tarpeet. ERP-järjestelmän siivouksien yhteydessä on poistettu tarpeettomat henkilötiedot manuaalisesti myös MDM-järjestelmästä. Varsinaisen tiedon käyttötarpeen päätyttyä tietoja ei kuitenkaan anonymisoida, vaan osa tiedoista poistetaan ja henkilö pyritään piilottamaan tarvittaessa. Tällä hetkellä henkilötietoja ei myöskään arkistoida mitenkään. Arkistointi pyritään toteuttamaan henkilötiedon piilottamisella. Henkilötiedon elinkaaritila on aktiivinen/passiivinen tai muu virhe. Varsinaista prosessia ei ole olemassa, jotta rekisteröity pystyisi itse ylläpitämään omia henkilötietojaan. Kaikissa liiketoimintayksiköissä ei ole sähköisiä järjestelmiä, joissa henkilö voisi pitää tietojaan ajan tasalla. Tällä hetkellä asia hoituu soittamalla myyntipalveluun ja pyytämään heitä tekemään tarvittavat muutokset järjestelmään. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Järjestelmän sisältävän henkilötiedon käyttöä alkuperäiseen käyttötarkoitukseen on varmistettu käyttäjäryhmiä rajaamalla. Lisäksi järjestelmän vienti- toiminnon käyttöä on rajoitettu, ettei tietoja voitaisi kopioida muualle. Ohjeistusta tiedon alkuperäisen käyttötarkoituksen käytöstä ei tällä hetkellä ole ollenkaan. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

CRM-järjestelmästä siirretään tietoa tällä hetkellä manuaalisesti muihin järjestelmiin, mutta siirron automatisointi on tulossa. Järjestelmästä ei kuitenkaan siirretä mitään henkilötietoja ulkopuolisten tahojen käyttöön. Järjestelmään ajetaan kerran vuodessa arvolisäverovelvollisuusrekisterin tarkistus. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36, 49-50.)

Rekisterinpitäjän tiedonantovelvoite on hoidettu yrityksen internetsivuilta löytyvällä rekisteriselosteella. Ulkomailla toimivien tytäryhtiöiden rekisteriselosteet eivät vastaa kattavuudeltaan Suomessa käytössä olevaa selostetta. (EU:n tietosuoja-asetus (GDPR) 2016, 40-41, 50-51.)

Rekisteriseloste on myös tulostettavissa ja luettavissa mobiililaitteilla pl. yhden tytäryhtiön verkkosivut, josta tulostus ei onnistu. Rekisteri- tai tietosuojaselosteessa ei ole kuvattu riittävän selkeästi henkilötietojen käyttötarkoitusta ja käsittelyperusteita. (EU:n tietosuoja-asetus (GDPR) 2016, 39-40, 50-51.)

Järjestelmä seuraa muutamien työkalujen avulla käyttäjämääriä ja mahdollisia ongelmatilanteita. Yksittäisten käyttäjien toimintaa sivuilla ei seurata ja seurannasta informoidaan käyttäjää heti verkkosivulle saavuttua. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Yrityksessä ei ole testattu onko rekisterinpitäjällä kyky ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisteröidyille ja valvontaviranomaiselle 72 tunnin kuluessa. Tämän arvioidaan onnistuvan annetussa aikamääreessä. Järjestelmän osalta ei ole myöskään käytössä minkäänlaista lokienhallintajärjestelmää. (EU:n tietosuoja-asetus (GDPR) 2016, 52, 52-53.)

Mikäli rekisteröity haluaa henkilötietonsa poistettavaksi tai nähtäväksi, pyynnön toteuttamista varten on tekniset valmiudet olemassa. Prosessin perustaminen tietojen toimittamiseksi on vielä suunnitteilla. Henkilötietojen poistaminen tai passivointi voidaan toteuttaa, mikäli poistamispyyntö tulee. Poistosta huolimatta järjestelmän pääkäyttäjä saa tarkistettua historiatiedoista mitkä tiedot ovat ennen poistoa olleet. (EU:n tietosuoja-asetus (GDPR) 2016, 43-44, 44-45, 45.)

Yrityksessä ei ole olemassa ohjeistusta tai prosessia, jossa pidetään huolta, että järjestelmän kehitys- ja ylläpitohenkilöstö osallistuu turvallisuuskoulutukseen, jossa on huomioitu yrityksen turvallisuuspolitiikka ja -käytänteet sekä tietosuojavaatimukset. (EU:n tietosuoja-asetus (GDPR) 2016, 62-64.)

Järjestelmäasennus on dokumentoitu ja kovennettu yrityksen ohjeistuksen mukaisesti, mutta teknistä turvallisuustestausta ei ole tehty ennen käyttöönottoa. Järjestelmästä on olemassa dokumentoitu jatkuvuussuunnitelma, jota ei ole ylläpidetty. Järjestelmää ei ole myöskään jouduttu vielä palauttamaan varmuuskopiosta, mutta yritys arvelee pääsevänsä tarvittaessa muutaman tunnin palautusaikaan. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Järjestelmän alusta on kahdennettu ja toimii virtuaalisena asennuksena. Se on mahdollista tarpeen tullen siirtää laiterikon sattuessa toiseen virtuaalikoneeseen. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Järjestelmään on annettu käyttöoikeuksia vain tarpeen mukaan ja käyttötarve on ennalta varmistettu. Jälkikäteen oikeuksien käyttötarpeen tarkistusta varten on prosessi määrittelemättä. Käyttäjän järjestelmätunnukset tunnistetaan kirjautumisvaiheessa ja kaikista tehdyistä muutoksista jää järjestelmän lokiin merkintä. Kaikki järjestelmän käyttäjät tunnistetaan ja pääkäyttäjillä on henkilökohtaiset käyttäjätunnukset. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52, VAHTI-raportti 2016, 33.)

Yrityksessä on arvioitu, ettei tämän järjestelmien sisältämiä tietoja tarvitse luokitella. Järjestelmän tietoturvapolitiikka on päivitetty joitakin vuosia sitten vastaan sen hetkistä politiikkaa. Järjestelmässä on käytössä suojaamaton http-yhteys, mutta päivitys https-yhteyksiin on tulossa. Järjestelmän osalta kriittisiä toimia valvotaan aktiivisesti. Verkon vyöhykkeistäminen on myös parhaillaan työn alla. Internet of Things (IOT)-laitteiden käyttämä verkko on suljettu täysin erilleen yrityksen sisäverkosta. Pääyhteistyökumppaneiden osalta tietoturva- ja tietosuoja- asiat on otettu huomioon palvelu- tai ylläpitosopimuksesta tehdessä, mutta on muutamia yhteistyökumppaneita, joiden sopimukset tulee tarkistaa ovatko ne kunnossa. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Kolmansille osapulille pyritään luovuttamaan ainoastaan niitä tietoja, jotka ovat tarpeen palveluntuottajan tehtävien suorittamiseksi, mutta sen on arvioitu olevan teknisesti hankala toteuttaa vastaamaan vaatimuksia. (VAHTI-raportti 2016, 32.)

6.4 Yhteenveto

Järjestelmästä kirjattiin tutkimuksen aikana yhteensä 29 eri havaintoa tai puutetta. Myyntiprosessiin liittyvistä järjestelmistä MDM:stä löytyi eniten huomioita. Kriittisiä puutteita ei tästäkään järjestelmästä löytynyt. Järjestelmän dokumentaatiossa on tämänkin järjestelmän osalta kehitettävää. Tiedon elinkaaren päätyttyä tiedot tulisi myös poistaa mielellään automatisoidusti tai vähintään anonymisoida. Prosessi täytyisi myös pystyä suorittamaan siten, että se on jäljitettävissä.

Tutkimusta varten haastatellut henkilöt oli valittu onnistuneesti ja heillä oli riittävä tietotaito vastaamaan kattavasti haastattelun kysymyksiin. Vaikka järjestelmästä tehtiin paljon huomioita, niistä vain muutamat olivat korkean prioriteetin huomioita.

Haastattelussa tehtiin asiakasyrityksen kannalta tärkeitä huomioita, joiden perusteella pystytään tekemään monipuoliset toimenpidesuositukset.

6.5 Kuvaukset löydöksistä: ERP

ERP-järjestelmän PIA-haastatteluun osallistui asiakasyrityksestä järjestelmien infrastruktuurista vastaava, ERP-järjestelmän vastuuhenkilö, talousosaston pääkäyttäjä ja toimitusketjun hallinnasta vastaava henkilö. Tässä kappaleessa kerrotaan ERP-järjestelmässä havaitut puutteet ja huomiot. Löydösten perään on kirjattu tietosuoja-asetuksen kohta, johon se viittaa. Kappaleen loppuun on kirjattu lyhyt yhteenveto tutkimuksen löydöksistä.

Järjestelmän dokumentaatio ei sisällä ohjeistusta järjestelmän käyttäjälle, mitä tietoja sinne tulisi syöttää. Syötettävä tieto on käyttäjän vastuulla ja sisältö vaihtelee tiedon kirjaajan mukaan. Järjestelmän tietoja ei ole myöskään luokiteltu mitenkään. Rekisteriseloste on tehty yleisellä tasolla, mutta ei riittävän tarkasti ja kattavasti. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 50-51.)

Suuri osa järjestelmän sisältämästä tiedosta periytyy yrityksen jo käytöstä poistetuista järjestelmistä. Joukossa on hyvin paljon tietoa, joka ei ole enää tarpeellista. (EU:n tietosuoja-asetus (GDPR) 2016, 53-54.)

Järjestelmään pyritään keräämään juuri sen verran tietoa mitä tarvitaan. Kerättävälle tiedolle on käyttöperuste olemassa ja kirjanpidon lakisääteinen tiedon säilytystarve on kuusi vuotta. Tarpeettomien tietojen poistoa ei ole automatisoitu, vaan ne jäävät järjestelmään passiivinen-tilaan. Järjestelmä on integroitu MDM:n kanssa ja osa tiedoista siirtyy ERP-järjestelmään tätä kautta. Passiiviset asiakkaat voidaan poistaa MDM:n kautta, jonka jälkeen ne poistuvat myös ERP-järjestelmästä tietojen replikoinnin yhteydessä. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Tiedon elinkaaressa on huomioitu yrityksen verovelvollisuus sekä mahdollinen asiakkaiden reklamointien tarve. Käyttötarpeen päätyttyä tietoja ei suoraan poisteta järjestelmästä, eikä niitä edes anonymisoida. Tämän järjestelmän osalta ei myöskään kyetä varmistamaan, ettei tietoja käsitellä niille alkuperäisesti määritellyn ja rekiste-

röidylle informoidun käyttötarkoituksen vastaisesti, tietoja kopioida toisaalle tai käytetä ilman tarveperustetta muissa järjestelmissä. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Järjestelmästä viedään henkilö- ja tuotantotietoa testiympäristöön. Viennin perusteena on tekniset- ja kehityssyyt. Ympäristön vanhentuneet versiot säilytetään yhden tilikauden ajan. (EU:n tietosuoja-asetus (GDPR) 2016, 36-37, VAHTI-raportti 2016, 25.)

Yrityksen yleinen rekisteriseloste löytyy yrityksen verkkosivuilta, josta löytyy vain yhteyshenkilön tiedot ongelmatilanteita varten. Tietosuojavastaavan tietoja ei ole verkkosivujen kautta saatavilla, eikä henkilötietojen säilytysaikaa ilmoiteta rekisteröidylle. (EU:n tietosuoja-asetus (GDPR) 2016, 40-41, 50-51.)

Rekisteröity voi tarvittaessa tulostaa ja tallentaa rekisteri- ja tietosuojaselosteen verkkosivujen kautta. Ulkomailla toimivien tytäryhtiöiden kohdalla ei täyttä varmuutta onko seloste saatavilla ja onko se riittävän kattava. (EU:n tietosuoja-asetus (GDPR) 2016, 39-40.)

Emoyhtiön ja tytäryhtiöiden osalta on käytävä läpi rekisteri- tai tietosuojaselosteet, joissa on kuvattu kaikkien rekisteröitävien henkilötietojen käyttötarkoitus ja käsittelyperusteet. (EU:n tietosuoja-asetus (GDPR) 2016, 40-41.)

Rekisteröidylle ei ole täysin selvää se, että hyväksyykö hän rekisteri- tai tietosuojaselosteen verkkokaupassa vieraillessaan. (EU:n tietosuoja-asetus (GDPR) 2016, 37, 40-41.)

Järjestelmään kertyy rekisteröityjen paikkatietoja, jotka liittyvät suoraan liiketoimintatarpeeseen. Tietojen poisto ei ole automatisoitua käyttötarpeen päätyttyä. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Yrityksessä ei ole täyttä varmuutta, onko rekisterinpitäjällä kyky ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisteröidyille ja valvontaviranomaiselle 72 tunnin kuluessa. Tarve on tunnistettu ja se vaatii kuvauksen sekä riittävän toteutuksen. (EU:n tietosuoja-asetus (GDPR) 2016, 52, 52-53.)

Rekisteröidyn tehdessä tietojen päivityspyynnön, siihen pystytään vastaamaan onnistuneesti, mutta henkilön unohtaminen ei onnistu. Henkilön tietoja ei voi täysin poistaa, mutta teknisesti henkilötietojen anonymisointi onnistuu. Verojuridiikka estää tietojen poiston ensimmäisen kuuden vuoden aikana ja se on otettava huomioon unohduspyyntöjä käsitellessä. Tarvittaessa yhteystiedot voidaan poistaa välittömästi, eli tiedon minimointi onnistuu. Tiedon minimointi ja -poisto tapahtuu MDM:ssä, josta se replikoituu ERP-järjestelmään. (EU:n tietosuoja-asetus (GDPR) 2016, 43, 43-44, 44-45.)

Järjestelmässä ei kyetä tunnistamaan, mikäli sinne syötetään alle 16-vuotiaiden henkilöiden tietoja ja onko tätä varten huoltajan suostumus tai valtuutus saatu. (EU:n tietosuoja-asetus (GDPR) 2016, 37-38.)

Yrityksen oma henkilökunta on osallistunut turvallisuuskoulutukseen muutamia vuosia sitten. Järjestelmän kehitys- ja ylläpitohenkilöstön koulutuksesta ei ole tarkkaa tietoa. (EU:n tietosuoja-asetus (GDPR) 2016, 62-64.)

Järjestelmä vaatii jatkuvasti ympärivuorokautista saatavuutta. Järjestelmän toimittajan puolelta tehty SLA-sopimus ei kuitenkaan takaa täyttä ympärivuorokautista saatavuutta järjestelmälle. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Järjestelmän yhteiskäyttötunnuksia on käytössä omalla henkilökunnalla ja kolmansilla osapuolilla. Järjestelmän todellista käyttäjämäärää ei tiedetä, eikä kyetä identifioimaan luotettavasti johtuen käytössä olevista yhteiskäyttötunnuksista. (VAHTI-raportti 2016, 33.)

Järjestelmästä luovutetaan tietoa perintätoimistojen ja kuljetusyritysten käyttöön. Yritysten väliset sopimukset täytyy katselmoida läpi ja tarkistaa onko niissä mainittu asiakastietojen säilytyksestä sekä poistosta käyttötarpeen päätyttyä. (VAHTI-raportti 2016, 32.)

6.6 Yhteenveto

Tutkimuksen aikana kirjattiin 20 eri löydöstä järjestelmästä. Kriittisiä puutteita henkilötietojen käsittelyn osalta ei löytynyt. Dokumentaation ja ohjeistuksen päivittäminen oli tämänkin järjestelmän osalta esillä. Tiedon elinkaaren päätyttyä poisto tai

anonymisointi tulisi toteuttaa. Tällä hetkellä mitään tietoja ei poisteta järjestelmästä, vaan ne asetetaan passiivinen-tilaan, mikäli katsotaan tiedon elinkaaren olevan päätöksessä. Myös järjestelmän rekisteri- ja tietosuojaselosteessa havaittiin puutteita. Järjestelmän ympärivuorokautisessa saatavuudessa havaittiin myös puutteita, jotka otettava huomioon asiakasyrityksen ja palveluntarjoajan välisessä SLA-sopimuksessa. Järjestelmän käyttäjillä on käytössään yhteiskäyttötunnuksia ja niiden käytöstä on pyrittävä eroon.

Tutkimukseen osallistuneet henkilöt oli valittu monipuolisesti ja haastattelututkimuksen pohjalta saatiin luotettavat tulokset järjestelmän osalta. Järjestelmästä tehdyt havainnot olivat linjassa aiempien järjestelmien yhteydessä tehdyistä havainnoista. Kriittisiä kohteita ei löytynyt. Tutkimuksen tulokset tulevat auttamaan yritystä muutosprosessin aikana, joka tämänkin järjestelmän osalta tehdään.

6.7 Kuvaukset löydöksistä: Myyntipalvelut

Myyntipalvelun PIA-haastatteluun osallistui asiakasyrityksestä vastuuhenkilöitä myynti-, laskutus-, tilaus- ja toimitus- osastoilta. Tässä kappaleessa kerrotaan myyntipalvelun haastattelussa havaitut puutteet ja huomiot.

Myyntipalvelun oman henkilökunnan omia henkilökohtaisia muistiinpanoja asiakastiedoista säilytetään x-määrää aikaa, jonka jälkeen ne siirretään tuhottavien roskien joukkoon. Hävitysprosessista ei ole ohjeistusta olemassa, vaan jokainen vastaa omista muistiinpanoistaan ja niiden hävittämisestä. Asiakkaan tehdessä tilauksen, samassa yhteydessä häneltä ei kysytä markkinointilupaa tällä hetkellä.

Asiakkaiden luottokelpoisuus tarkistetaan aina luotonvalvonnasta. Luotonvalvonnan työntekijöillä on erilaisia käytänteitä omassa toiminnassaan. Asiakkaan henkilötunnus ja/tai y-tunnus saattaa kulkea sähköpostin välityksellä. Tiedot saattavat jäädä sähköpostin saapuneet-kansioon ja mahdollisesti lähetetyt-kansioon, mikäli viestiin vastataan tai se välitetään eteenpäin. Reklamaatiotilanteissa asiakas toimittaa tilinumeronsa kirjallisena luotonvalvontaan. Luotonvalvontaan jää sähköpostilaatikkoon asiakkaan tilinumero.

Asiakkaille ei ole olemassa portaalia missä he pystyisivät päivittämään omia henkilötietojaan. Projekti käynnissä yhteistyökumppanin kanssa, jolta saataisiin vahvistus

asiakkaan yhteystiedoista hänen ollessaan puhelimitse yhteydessä myyntipalveluun. Asiakas siirtyy passiiviseen-tilaan viiden vuoden jälkeen, mikäli hän ei tee ostoksia uudestaan. Asiakkaan tiedot eivät poistu automaattisesti missään vaiheessa, ellei tietoja poisteta manuaalisesti MDM:stä.

Kampanjoissa mainostusta osoitetaan asiakkaille, jotka eivät ole ostaneet tietyllä aikavälillä tuotteita uudestaan. Mainosviestintää tehdään, vaikka markkinointilupaa ei ole kysytty asiakkaalta erikseen. Tällä hetkellä kaikki tuotteita ostaneet asiakkaat ovat automaattisesti markkinointilistalla. Oletetaan heidän antavan luvan markkinointiviestinnästä, koska he ovat olleet kiinnostuneita yrityksestä ostaneet tuotteita.

6.8 Havaitut puutteet

Tutkimuksen tulosten perusteella voitiin havaita, että järjestelmissä havaitut puutteet ja huomiot kohdentuivat etupäässä samoihin aihealueisiin. Selkeimpänä puutteena havaitaan henkilökunnan ohjeistus ja kuinka tärkeää on toimia yhdenmukaisella ohjeistuksella koko organisaation laajuudella. Kaikissa myyntiprosessiin liittyvissä järjestelmissä havaittiin puutteita järjestelmien dokumentaatioissa. Järjestelmien rekisteri- ja tietosuojaselosteissa havaittiin puutteita, joiden korjaaminen oli jo tutkimusta tehdessä aloitettu.

Järjestelmien välisiä integraatiota tutkittaessa, havaittiin CRM-järjestelmästä poistettujen henkilötietojen replikoituvan takaisin poistosta huolimatta. Asiakkaat asioivat yrityksen kanssa ostotarkoituksessa yleensä noin vuoden välein. Ostotapahtumien uusimisväli on melko pitkä ja asiakassuhde passivoituu järjestelmiin vasta kahden vuoden jälkeen, mikäli asiakas ei osta tänä aikana yritykseltä tuotteita. Markkinointilupaa ei ole välttämättä saatu passiivisilta asiakkailta, mutta heitä lähestytään siitä huolimatta markkinointiviesteillä. Asiakas joutuu itse ottamaan yhteyttä asiakaspalveluun ja kieltämään markkinoinnin.

Tiedon elinkaaressa havaittiin myös puutteita. Asiakkaat passivoidaan järjestelmiin ja heidän henkilötietonsa säilyvät järjestelmissä. Yhtä järjestelmää lukuun ottamatta, asiakkaiden henkilötietoja ei kyetä jäljittämään ja poistamaan niin, että prosessi pystytään tarvittaessa todentamaan. Tutkimuksessa havaittiin myös asiakasyrityksen ja

heidän palveluntarjoajien välisien SLA-sopimuksien olevan osittain puutteellisia. Palveluntarjoajat eivät välttämättä kykene takaamaan tarvittavaa ympärivuorokautista saatavuutta tarjoamalleen palvelulle. Tutkimuksessa havaittiin myös, että järjestelmien käyttäjille oli jaettu yhteiskäyttötunnuksia.

6.9 CRM-järjestelmän toimenpidesuositukset

Järjestelmän dokumentaation havaittiin olevan puutteellinen, johtuen järjestelmän pilvipohjaisesta alustaratkaisusta. Tietosuoja-asetuksen artiklojen 25 ja 30 mukaan rekisterinpitäjän olisi dokumentoitava erittelyt henkilötietojen käsittelystä, tarkoista tietovirroista ja tiedon näkyvyyden luokittelusta. Myös tiedon fyysinen ja looginen sijainti tulisi olla kirjallisena järjestelmän toimittajan puolesta. Dokumentoinnin ohessa olisi kiinnitettävä huomiota organisaatiotasolla henkilökunnan ohjeistukseen, kuinka henkilötietoja käsitellään riittävän turvallisesti. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 50-51.)

CRM-järjestelmässä on paljon tiedon elinkaaren loppuvaiheessa olevaa tietoa. Tarpeetonta tietoa poistetaan muutaman vuoden välein tai tarvittaessa. Poistamista varten ei ole olemassa automaattista prosessia. Järjestelmien väliset integraatiot aiheuttavat tiedon palautumisen järjestelmään, vaikka se olisi jo kertaalleen poistettu. Asetuksen viidennen artiklan mukaan tiedon elinkaaren päätyttyä henkilötiedot tulisi poistaa tai anonymisoida järjestelmästä. Tätä varten tulisi olla valmis ja toimivaksi testattu prosessi, jonka tulisi mielellään toimia automaattisesti. Järjestelmien väliset integraatiot tulisi toteuttaa niin, etteivät ne aiheuta poistetun tiedon palaamista järjestelmään. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Järjestelmässä on tuhansia duplikaatteja sekä ei-aktiivisia asiakastietoja. Johtuen MDM-järjestelmän integraatiosta, jo kertaalleen poistetut tiedot palautuvat poistosta huolimatta. Tietosuoja-asetuksen viidennen artiklan mukaan tiedon elinkaaren päätyttyä tarpeettomat henkilötiedot tulisi poistaa järjestelmistä, mikäli niille ei löydy liiketoiminta- tai laillista käyttötarvetta. Järjestelmää varten tulisi kehittää prosessi, joka poistaa automaattisesti tarpeettomat henkilötiedot tiedon elinkaaren päätyttyä. Prosessissa tulisi ottaa huomioon MDM-järjestelmän integraatio. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Yrityksessä ei ole olemassa asetuksen viidennessä artiklassa mainittua ohjeistusta siitä, miten kyetään varmistamaan, ettei tietoja käsitellä niille alkuperäisesti määritellyn ja rekisteröidylle informoidun käyttötarkoituksen vastaisesti, tietoja kopioida toisaalle tai käytetä ilman tarveperustetta muissa järjestelmissä. Tätä varten tulisi tehdä koko organisaatiota koskeva ohjeistus siitä, miten rekisteröidyn tietoja käsitellään alkuperäisen tarkoituksen mukaisesti. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Rekisteröityjen tekemiä markkinointikieltoja päivitetään järjestelmään manuaalisesti. Asiakastyytyväisyyskyselyä ja markkinointikampanjoita varten lähetetään henkilötietoja kolmannelle osapuolelle sähköpostin välityksellä. Tietosuoja-asetuksen viidennen ja 28:n artiklan mukaan rekisteröidyllä tulisi olla mahdollisuus markkinointikieltoon erillisen portaalin kautta, jossa hän voi päivittää sekä katsella omia henkilötietojaan. Mikäli henkilötietoja välitetään kolmannelle osapuolelle, tulee varmistua siitä, että tiedon elinkaari ja anonymisointi on varmistettu sekä rekisteröidyltä on saatu lupa tietojen välittämiseen eteenpäin. Nämä asiat voidaan varmistaa yritysten välisillä sopimuksilla ja sähköpostilaatikoiden tyhjentämisellä tietyin väliajoin. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36, 49-50.)

Yrityksen verkkosivuja käyttäessä rekisteröity saa ilmoituksen henkilötietojen käsittelystä, jonka hän hyväksyy, mikäli haluaa käyttää palvelua. Henkilötietojen säilytysaikaa ei ilmoiteta. Tietosuoja-asetuksen artiklojen 13 ja 30 mukaan rekisteröidylle tulee ilmoittaa häntä koskevien tietojen säilytysaika selkeästi ja riittävän kattavasti. Tiedot täytyy myös löytyä riittävän helposti yrityksen verkkosivuilta. (EU:n tietosuoja-asetus (GDPR) 2016, 40-41, 50-51.)

Rekisteröityä ei informoida esimerkiksi puhelinkeskustelun tai henkilökohtaisen kanssakäymisen aikana mitenkään siitä, että hänen tietoja kerätään asiakastietojärjestelmään. Tietosuoja-asetuksen 13 artiklan mukaan rekisteröidylle täytyy ilmoittaa, mikäli hänen tietojaan kerätään muuten, kuin sähköisesti. Tietojen keräämisen informoimisesta rekisteröidylle tulisi tehdä koko organisaatiota koskeva selkeä ohjeistus. (EU:n tietosuoja-asetus (GDPR) 2016, 40-41.)

Järjestelmän käyttäjiä pystytään seuraamaan epäsuorasti jokaiselle käyttäjälle kuuluvan URL-osoitteen johdosta. Järjestelmän pääkäyttäjä saa tarvittaessa raportin, josta

käyttäjät voidaan tunnistaa URL-osoitteen perusteella. Käyttäjät ovat tietoisia seurannasta. Tietosuoja-asetuksen viidennessä artiklassa mainitaan, että järjestelmän käyttäjien tunnistetiedot tulisi anonymisoida ja tietojen keräämisestä informoida käyttäjää. Käyttäjiä tulisi ohjeistaa siitä, mitä tietoja pääkäyttäjän raportissa näkyy. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Järjestelmässä saattaa olla alle 16-vuotiaiden henkilötietoja. Näitä on saattanut kirjautua järjestelmään esimerkiksi messuilla järjestettävien arvontojen johdosta. Tietosuoja-asetuksen artiklan kahdeksan mukaan alle 16-vuotiaiden henkilöiden tietojen käsittely täytyy tapahtua huoltajan suostumuksella tai valtuutuksella. Messuarvonnat tulisi suorittaa siten, että alle 16-vuotiaiden arvontakupongit poistetaan ennen tietojen järjestelmiin viemistä. Vaihtoehtoisesti arvontakupongeissa voidaan pyytää huoltajan suostumus tietojen tallentamiseen. (EU:n tietosuoja-asetus (GDPR) 2016, 37-38.)

Järjestelmässä tapahtuu automaattista asiakkaiden profilointia. Markkinointiluvan antaneille asiakkaille lähetetään markkinointimateriaalia tai suoramyyntiä ostohistorian perusteella. Asiakasta ei tiedoteta ennen ostotapahtumaa mahdollisesta tietojen automaattisesta profiloinnista tai suoramyynnistä. Tietosuoja-asetuksen 22 artiklassa mainitaan, että rekisteröidyllä täytyy olla tiedossa millainen käsittelylogiikka, käsittelyn merkitys ja seuraukset automaattisella profiloinnilla on. Rekisteröityä tulisi informoida, että hänelle voidaan lähettää markkinointimateriaalia tai tehdä suoramyyntiä ostohistorian perusteella, mikäli hän on antanut markkinointiluvan yritykselle. (EU:n tietosuoja-asetus (GDPR) 2016, 46.)

Laitevian tai järjestelmän kaatumisesta johtuvaa tiedon palautusta ei ole yrityksessä ohjeistettu tai harjoiteltu ollenkaan. Tietosuoja-asetuksen 32 artiklan mukaan järjestelmän tieto tai järjestelmä on kyettävä palauttamaan yhteisesti sovitun ajan puitteissa. Järjestelmän palauttamista tulisi harjoitella testiympäristössä ja palauttamisprosessista täytyy olla ohjeistus olemassa. (EU:n tietosuoja-asetus (GDPR) 2016, 51-52.)

Järjestelmän osalta ei ole olemassa dokumentaatiota, kuinka tietoliikenneverkko on jaettu vyöhykkeisiin, millaiset suodatussäännöt ovat käytössä ja onko verkko toteu-

tettu monitasoisen suojaamisen periaatteiden mukaisesti. Tietosuoja-asetuksen artiklojen 25 ja 32 mukaan järjestelmästä tulisi olla dokumentaatio olemassa, jossa on otettu edellä mainitut asiat huomioon, vaikka kyseessä onkin pilvipalvelu. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Palveluntuottajan valintaprosessia ei ole dokumentoitu vaatimuksien ja itse valinnan osalta. Tietosuoja-asetuksen artiklojen 25 ja 32 mukaan valintaprosessi tulisi dokumentoida sekä samanaikaisesti ottaa huomioon konsernin ohjeet ja käytännöt. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Järjestelmän päivittämistä varten luovutetaan tietoja sähköpostin välityksellä kolmannelle osapuolelle. VAHTI-ohjeistuksessa 1/2016 mainitaan, että järjestelmästä tulisi luovuttaa kolmannelle osapuolelle vain ja ainoastaan niitä tietoja, jotka ovat tarpeen palveluntuottajan tehtävien suorittamiseksi. Yritysten välisissä SLA-sopimuksissa tulisi olla maininta tiedon elinkaaresta. Kolmannen osapuolen tulisi poistaa saamansa tiedot säilytysajan umpeuduttua. Myös sähköpostilaatikot tulisi tyhjentää tietyin väliajoin. (VAHTI-raportti 2016, 32.)

6.10 MDM-järjestelmän toimenpidesuositukset

Järjestelmän dokumentaatiossa tulisi huomioida Tietosuoja-asetuksen artiklat 25 ja 30. Näiden mukaan dokumentaatiosta tulisi käydä ilmi järjestelmän rakenne ja integraatiot. Tietojen käsittelystä ja tietovarantojen omistajista tarvitaan myös kirjallinen ohjeistus ja dokumentaatio. Dokumentaatiossa täytyy ottaa myös huomioon yrityksen ulkopuoliset järjestelmän ylläpitäjät. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 50-51.)

Viidennen artiklan mukaan tulee huolehtia henkilötietojen käyttötarkoitussidonnaisuudesta sekä tietojen minimoimisesta. Järjestelmän tulisi automaattisesti poistaa tarpeettomat henkilötiedot. Rekisteröidyllä tulisi olla mahdollisuus päivittää omia tietojaan muuten, kuin erillisen muutospyynnön kautta. Tarpeettoman tiedon poistossa täytyy huomioida kirjanpitolain määrittämä kuuden vuoden säilytysaika. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Henkilötietojen elinkaari tulisi saattaa asetuksen viidennen artiklan mukaiseksi. Tiedon elinkaaressa tulee huomioida liiketoiminnan tarpeet ja käyttöperusteeton tieto

tulisi poistaa. Tarpeettomat tiedot tulisi vähintäänkin anonymisoida tai poistaa. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Tiedot tulisi arkistoida artiklan viisi mukaisesti kirjanpitolain määrittämäksi ajaksi ja tarvittaessa anonymisoida. Tällä hetkellä arkistointia pyritään toteuttamaan tiedon piilottamisella järjestelmässä, vaikka käyttöperustetta ei enää olisikaan. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Tiedon käsittelyä alkuperäisen tarkoituksen mukaisesti on rajattu järjestelmän käyttäjäoikeuksin. Järjestelmästä ulos otettavaa tietoa on myös rajoitettu. Käyttäjät tulisi ohjeistaa käyttämään järjestelmästä saatavaa tietoa vain ja ainoastaan artiklassa viisi mainitulla alkuperäisen käyttötarkoituksen tavalla. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Järjestelmien välillä siirretään tietoa manuaalisesti ja automatisoitu prosessi on suunnitteilla. Tietosuoja-asetuksen artikloissa viisi ja 28 mukaan arkkitehtuuri ja tiedonsiirtokuvaukset tulisi olla dokumentoituna, mikäli tietoa siirretään järjestelmien välillä. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36, 49-50.)

Yrityksen verkkosivuilla on ongelmia, mikäli rekisteriselostetta yrittää avata mobiililaitteella. Asetuksen 12 artikla ohjeistaa ilmoittamaan rekisteröidylle selkeästi henkilötietojen säilytysajan, tietosuojavastaavan yhteystiedot sekä rekisteri- ja tietosuojaselosteen. (EU:n tietosuoja-asetus (GDPR) 2016, 39-40.)

Yrityksen verkkosivuilla vierailevia käyttäjien käyttäytymistä seurataan ja analysoidaan usean eri ohjelman kautta. Artiklassa viisi mainitaan, että tämä tulisi suorittaa läpinäkyvästi ja rekisteröidylle täytyy ilmoittaa seurannasta ja käyttäytymistietojen analysoinnista. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Artiklat 33 ja 34 määrittävät rekisterinpitäjän ilmoittamaan 72 tunnin kuluessa tietoturvaloukkauksesta viranomaisille. Yrityksessä ei ole vielä olemassa prosessia tietoturvaloukkauksen tapahtumisesta ja sen jälkeisistä toimenpiteistä. Tietoturvaloukkauksesta ja sen jälkeisistä toimenpiteistä tulisi laatia prosessi ja testata sen toimivuus. Myös lokienhallintajärjestelmän käyttöönotto olisi viisasta. Näin pystytään paikantamaan mistä kautta ja/tai kenen toimesta loukkaus on tapahtunut. (EU:n tietosuoja-asetus (GDPR) 2016, 52, 52-53.)

Yrityksellä on olemassa valmiudet toimittaa rekisteröidyn tekemä henkilötietojen poistopyyntö. Artiklojen 16, 17, ja 18 mukaisesti rekisteröidyllä on oikeus tehdä omiin tietoihinsa oikaisu, käsittelyn rajoittaminen tai poisto. Tästä tulisi luoda toimiva prosessi, joka käynnistyy automaattisesti rekisteröidyn tehdessä poistopyyntö. Poiston yhteydessä on huomioitava järjestelmäintegraatiot ja varmistuttava ettei poistettu tieto palaa muista järjestelmistä. Myös tietojen kuuden vuoden säilytysvelvollisuus on huomioitava, mikäli rekisteröity on käynyt kauppaa yrityksen kanssa. (EU:n tietosuoja-asetus (GDPR) 2016, 43, 43-44, 44-45.)

Tietosuoja-asetuksen artiklan 47 mukaisesti järjestelmän kehitys- ja ylläpitohenkilöstön tulee osallistua turvallisuuskoulutuksiin, joissa on huomioitu yrityksen turvallisuuspolitiikka ja -käytänteet sekä tietosuojavaatimukset. Koulutuksien osalta tulisi laatia ohjeistus ja koulutuksia tulisi järjestää riittävän useasti sekä henkilökunnan osallistumisesta tulisi pitää kirjaa. (EU:n tietosuoja-asetus (GDPR) 2016, 62-64.)

Asetuksen 25 ja 32 artiklan mukaan järjestelmäasennukselle tulisi suorittaa tekninen turvallisuustestaus ennen käyttöönottoa. Järjestelmällä tulisi myös olla hyväksytty ja dokumentoitu ajan tasalla oleva jatkuvuussuunnitelma, jonka toimivuus testataan vuosittain. Tekninen turvallisuustestaus tulisi suorittaa sekä dokumentoida riittävän laajasti ja jatkuvuussuunnitelma päivittää vastaamaan tämänhetkistä tilannetta. Jatkuvuussuunnitelma tulisi päivittää vuosittain. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Tietosuoja-asetuksen 32 artiklan mukaan merkittävä tieto tai kriittinen järjestelmä on kyettävä palauttamaan yhteisesti sovitun ajan puitteissa. Varmuuskopioiden palautus olisi testattava ja dokumentoitava palautuksen vaiheet, sekä aika jonka palautus vaatii. (EU:n tietosuoja-asetus (GDPR) 2016, 51-52.)

Järjestelmän käyttäjille tulisi artiklan 25 ja 32 mukaisesti antaa vain ne oikeudet ja valtuudet, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä. Järjestelmän käyttäjäoikeudet ovat annettu vain tarvetta vastaan ja tarve on myös varmistettu todelliseksi ennen oikeuksien myöntämistä. Jälkikäteen käyttöoikeuksia ei tarkisteta, kuin satunnaisesti. Käyttöoikeuksien tarvetta tulisi tarkastella säännöllisin väliajoin. Joukossa voi olla käyttäjiä, joiden käyttötarve ei enää ole ajankohtainen. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Artiklan 25 ja 32 mukaan järjestelmän turvatoimet tulisi mitoittaa sen sisältämän tiedon suojaustarpeen perusteella sekä järjestelmien välinen tiedonvälitys tulisi toteuttaa salatuin yhteyksin. Järjestelmän sisältämä tieto tulisi luokitella ja suojauksen riittävyydelle tulisi tehdä riskipohjainen arviointi. Tietoturvapolitiikka tulisi myös päivittää vastaamaan nykyistä tilannetta. Järjestelmien välinen tiedonsiirto tulisi myös toteuttaa salattuja yhteyksiä pitkin nykyisten salaamattomien sijaan. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Verkkoa tulisi valvoa artiklan 25 ja 32 mukaan riittävän kattavasti ja käytössä tulisi olla palomuurit ja reitittimet sekä verkko tulisi vyöhykkeistää. Verkonvalvonnan hälytyksiin ja poikkeamiin täytyy myös reagoida riittävän nopeasti. Yrityksen liiketoimintayksiköissä rakennetaan parhaillaan kyvykkyyttä verkon valvomiselle ja vyöhykkeistämiselle. Palomuurisäännöt tulisi olla riittävän tiukat ja reitittimien konfiguraatiot ja dokumentoitu kattavasti. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Artikloissa 25 ja 32 mainitaan myös tietoturva- ja tietosuoja-asioiden ottaminen huomioon ylläpitosopimuksissa. Yrityksen pääyhteistyökumppanin osalta asiat on huomioitu, mutta muiden yhteistyökumppaneiden kohdalla asiasta ei täyttä varmuutta. Sopimukset tulisi käydä läpi ja tehdä tarvittavat korjaukset, mikäli tarvetta muutoksiin ja tiukennuksiin löytyy. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

VAHTI-ohjeistuksen 1/2016 mukaan järjestelmästä tulisi luovuttaa kolmansille osapuolille vain niitä tietoja, jotka ovat tarpeen palveluntuottajan tehtävien suorittamiseksi. Yrityksessä pyritään siihen, että vain ne tiedot luovutetaan, jotka on pakko. Tietojen luovutus tulisi ohjeistaa ja dokumentoida. On myös pidettävä huoli siitä, että kolmannen osapuolen edustajat pitävät huolen tiedon elinkaaren päättymisen jälkeisestä tiedon poistosta. (VAHTI-raportti 2016, 32.)

6.11 ERP-järjestelmän toimenpidesuositukset

Järjestelmän käyttäjiä ei ole ohjeistettu mitenkään siitä, mitä henkilötietoja järjestelmään tulee syöttää. Järjestelmästä voi siis löytyä käytännössä ihan mitä vaan tietoa, riippuen siitä kuka sitä on järjestelmään syöttänyt. Ohjeistus tiedon luokittelusta puuttuu ja rekisteriseloste on tehty yleisellä tasolla. Artiklojen 25 ja 30 mukaan jär-

jestelmän dokumentaation täytyy sisältää erittelyt henkilötietojen käsittelystä, tietovirtojen omistajista, tiedon luokittelusta ja ohjeet henkilötietojen turvallisesta käsittelystä. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 50-51.)

Järjestelmän osalta henkilötietojen käyttötarkoitussidonnaisuutta sekä tietojen minimointia ei tapahdu. Passiivisten asiakkaiden henkilötietojen poistoa ei tapahdu automaattisesti, mutta valmiudet siihen olisi olemassa. Henkilötietoja säilytetään verotuksellisista syistä kuusi vuotta. Järjestelmä on integroitu MDM-järjestelmään, joten se on otettava huomioon lopullisia muutoksia tehdessä. Artiklan viisi mukaisesti, tarpeettomat henkilötiedot tulisi poistaa tiedon elinkaaren päätyttyä. Tässä tapauksessa tiedon elinkaari on maksimissaan verotuksellisista ja mahdollisista reklamaatioista kuusi vuotta. Tätä varten olisi luotava automatisoitu prosessi, joka poistaa tai anonymisoi tiedot, mikäli asiakas pysyy passiivisena. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Artiklassa viisi mainittua arkistointia ei myöskään tapahdu tämän järjestelmän osalta. Tätä varten tulisi laatia tiedon arkistoinnin ohjeistus sekä automatisoitu tiedon poisto elinkaaren päätyttyä. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Tietosuoja-asetuksen artiklassa 5 mainitaan, että tietoja tulisi käsitellä sen alkuperäisen käyttötarkoituksen mukaisesti ja tästä tulisi olla tarkka ohjeistus olemassa. Yrityksen tulisi varmistaa, ettei tietoja käytetä alkuperäisen käyttötarkoituksen vastaisesti luomalla tarkat ohjeistukset koko konsernin laajuudelle. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Yrityksen testiympäristössä käytetään tietokantaa, joka sisältää tuotantojärjestelmästä otettuja henkilötietoja. Näitä säilytetään vähintään yhden tilikauden ajan ns. vanhoina versioina. Tietosuoja-asetuksen kuudennen artiklan ja VAHTI-ohje 1/2016 mukaan, testiympäristössä käytetty data tulisi vähintäänkin anonymisoida. Myös vanhemmat, kuin yhden tilikauden versiot tulisi poistaa. (EU:n tietosuoja-asetus (GDPR) 2016, 118-121, VAHTI-raportti 2016, 25.)

Yrityksen verkkosivuilta löytyvä yleinen rekisteriseloste ei ulotu ERP-järjestelmään asti ja se ei ole riittävän kattava kattaakseen myös verkkokaupan. Artiklojen 13 ja 30

mukaan rekisteriselosteesta tulisi löytyä selkeästi ja helposti löydettävästi tietosuojavastaavan yhteystiedot, tilatun tuotteen toimitusehdot sekä henkilötietojen säilytysaika. (EU:n tietosuoja-asetus (GDPR) 2016, 40-41, 50-51.)

Järjestelmään kerätään paikkatietoja perustellusti liiketoiminnan tarvetta varten. Tiedot jäävät järjestelmään ja poistoa ei tapahdu tiedon elinkaaren päätyttyä. Artiklan viisi mukaisesti paikkatiedot tulisi poistaa tiedon elinkaaren päätyttyä, tai anonymisoida niin, ettei henkilöitä kyetä saatavilla olevien tietojen perusteella tunnistamaan. Tätä varten olisi myös laadittava automatisoitu prosessi, joka poistaa tarpeettomat paikkatiedot elinkaaren päätyttyä. (EU:n tietosuoja-asetus (GDPR) 2016, 35-36.)

Yrityksessä ei olla täysin varmoja kyetäänkö mahdollisista tietoturvaloukkauksista raportoimaan viranomaisille tietosuoja-asetuksen artiklojen 33 ja 34 vaatimassa 72 tunnin ajassa. Tietoturvaloukkauksen riskin arvioidaan olevan hyvin pieni. Tätä varten tulisi laatia suunnitelma ja tunnistuskeinot tietoturvaloukkausten tunnistamiseksi. (EU:n tietosuoja-asetus (GDPR) 2016, 52, 52-53.)

Järjestelmään on mahdollista päivittää henkilötietoja, mikäli rekisteröity niin haluaa. Toistaiseksi poisto ei onnistu, mutta henkilötietojen anonymisointi on mahdollista. Tietojen anonymisointi täytyy tehdä MDM-järjestelmään, joka replikoi tietonsa ERP-järjestelmään. Tietosuoja-asetuksen artikloiden 16, 17 ja 18 mukaisesti rekisteröity tulisi kyetä unohtamaan, mikäli hän niin haluaa. On kuitenkin otettava huomioon verojuridiset seikat ja tietojen säilytysaika. Tapauksesta riippuen vähintäänkin henkilötietojen anonymisointi tulisi olla mahdollista. (EU:n tietosuoja-asetus (GDPR) 2016, 43, 43-44, 44-45.)

Järjestelmässä ei kyetä varmistamaan, ettei sinne syötetä alle 16-vuotiaiden henkilöiden tietoja. Tietosuoja-asetuksen 8 artiklan mukaan järjestelmään syötettävän alle 16 vuotiaan tiedoilla tulisi olla huoltajan suostumus tai valtuutus. Tätä varten tulisi luoda prosessi, joka tarkistaa onko huoltajan lupa olemassa. (EU:n tietosuoja-asetus (GDPR) 2016, 37-38.)

Järjestelmä toimii ulkopuolisen yhteistyökumppanin konesalissa ja järjestelmän kehityshenkilöstö on myös ulkopuolista. Tästä syystä ei ole varmaa tietoa ovatko he osallistuneet tarvittaviin tietoturva ja turvallisuuskoulutuksiin. Tietosuoja-asetuksen 47

artiklan mukaan järjestelmän kehitys- ja ylläpitohenkilöstön tulisi osallistua koulutuksiin jossa on huomioitu yrityksen turvallisuuspolitiikka ja -käytänteet sekä tietosuojavaatimukset. Koulutuksia tulisi järjestää myös riittävän usein. Yritysten väliset sopimukset tulisi tarkistaa ja tarvittaessa vaatia riittävää koulutusta henkilökunnalle. (EU:n tietosuoja-asetus (GDPR) 2016, 62-64.)

Järjestelmä vaatii ympärivuorokautista saatavuutta ja ajoja voi olla mihin kellonaikaan tahansa. Yrityksellä on tiedossa, ettei SLA-sopimuksissa ole mainintaa ympärivuorokautisesta saatavuudesta. Tietosuoja-asetuksen artikloiden 25 ja 32 mukaan palveluntarjoajan täytyy kyetä tarjoamaan riittävät resurssit ja vastaamaan hälytyksiin kaikkina vuorokauden aikoina. Ympärivuorokautinen saatavuus tulisi kirjata yritysten väliseen SLA-sopimukseen, jotta mahdollisiin hälytyksiin pystytään reagoimaan kaikkina vuorokauden aikoina. (EU:n tietosuoja-asetus (GDPR) 2016, 48, 51-52.)

Järjestelmään on olemassa yhteiskäyttötunnuksia omalla henkilökunnalla ja kolmannen osapuolen edustajilla. Järjestelmän todellisia käyttäjiä ei pystytä identifioimaan luotettavasti. VAHTI-raportin 1/2016 mukaisesti yhteiskäyttötunnuksia ei tulisi käyttää. Jokaisella järjestelmän käyttäjällä tulisi olla omat henkilökohtaiset käyttäjätunnukset, joiden tekemät muutokset voidaan jäljentää luotettavasti. Henkilökohtaisia tunnuksia käyttämällä saadaan myös seurattua todellista järjestelmän käyttäjämäärää. (VAHTI-raportti 2016, 33.)

VAHTI-raportin 1/2016 mukaisesti järjestelmästä tulisi luovuttaa kolmannelle osapuolelle vain ja ainoastaan niitä tietoja, jotka ovat tarpeen palveluntuottajan tehtävien suorittamiseksi. Tämä tulisi ottaa huomioon kolmansien osapuolien kanssa luoduissa sopimuksissa. Näissä täytyy olla maininta luovutettujen tietojen säilytysajasta ja poistosta. (VAHTI-raportti 2016, 32.)

6.12 Myyntipalvelun toimenpidesuositukset

Myyntipalvelun henkilökunnan tulisi kirjata omat muistiinpanonsa johonkin sellaiseen paikkaan, josta ne voidaan tiedon elinkaaren päätyttyä todennetusti poistaa. Omista muistiinpanoista muodostuu jossain vaiheessa henkilörekisteri, joka ei ole suotavaa, varsinkaan sen joutuessa syystä tai toisesta vääriin käsiin. Mikäli omien

muistiinpanojen käyttämistä jatketaan, tulisi niiden hävittämiselle olla valmiiksi mietitty prosessi. Asiakastilausten yhteydessä asiakkaalta tulisi saada markkinointilupa kirjallisena. Ilman lupaa häntä ei saa lähestyä markkinointiviesteillä.

Luotonvalvonnan henkilökunnalla tulisi olla käytössään samat prosessit henkilötietojen kirjaamisessa ja välittämisessä. Mikäli henkilötietoja välitetään sähköpostin välityksellä, tulisi sähköpostilaatikot tyhjentää tarvittavin väliajoin. Näin vältetään, ettei sähköpostista muodostu henkilörekisteriä.

Asiakkailla tulisi olla käytössään oma portaali, jonka kautta he pystyvät päivittämään omia tietojaan. Näin varmistutaan tietojen oikeellisuudesta ja ajantasaisuudesta. Tulevaisuudessa portaalin kautta rekisteröity voisi tehdä omien tietojensa poistopyynnön, joka käynnistäisi prosessin henkilön unohtamiseksi. Mikäli rekisteröity tekee unohtamispyynnön, tulisi hänen henkilöllisyys varmistaa jollain keinolla. Pahimmassa tapauksessa saatetaan syyllistyä tietosuojarikkomukseen, mikäli joku muu kuin rekisteröity pääsee muokkaamaan henkilötietoja tai tekemään unohduspyynnön.

Asiakkaiden yhteydenotoissa tulisi varmistua henkilön identiteetistä. Tätä varten käynnissä oleva projekti yhteistyökumppanin kanssa on erittäin hyvä asia. Puheluiden aikana henkilö pystytään tunnistamaan luotettavammin.

Asiakastietoja tulisi poistaa järjestelmistä tiedon elinkaaren päätteeksi. Prosessi tulisi automatisoida, eikä vain passivoida asiakkaita, jotka eivät ole enää ostaneet tuotteita. Manuaalisesti poistettavat tiedot lisäävät työmäärää ja näin ei myöskään kyetä todentamaan kaikkien tarpeettomien tietojen poistoa järjestelmistä.

Kampanjoissa tulisi lähestyä vain niitä asiakkaita, jotka ovat antaneet luvan markkinointiviestinnälle. Jokaiselta asiakkaalta tulisi kysyä lupa erikseen, eikä olettaa heidän antavan lupaa ostamalla yrityksen tuotteita.

7 Pohdinta

Työn tavoitteena oli luoda muutossuunnitelma asiakasyritykselle prosessi- sekä PIA-haastatteluiden pohjalta tehtyjen havaintojen pohjalta. Muutossuunnitelman pohjalta yritys aloittaa omien käytössä olevien prosessien ja järjestelmien saattamisen vastaamaan tietosuoja-asetuksen määritelmiä.

Haastatteluissa onnistuttiin havaitsemaan missä kohdissa yrityksen prosesseja ja järjestelmiä niin sanotut vaaran paikat ja puutteet sijaitsevat. Haastatteluiden tuloksia verrattiin tietosuoja-asetuksen artikloihin sekä VAHTI-ohjeistukseen. Tulosten analysoinnista syntyi toimenpidesuunnitelma asiakasyritykselle, jota he voivat käyttää prosessien ja järjestelmien päivittämisessä.

Asiakasyrityksen haastateltavat henkilöt oli valittu onnistuneesti ja se edesauttoi luotettavien tulosten saamista. Haastatteluihin oli onnistuttu valitsemaan juuri ne yrityksen avainhenkilöt, joilla oli vahvin tietämys, sillä hetkellä tarkasteltavasta järjestelmästä. Lähdin mukaan projektiin ns. pystymetsästä ja aiempaa tietämystä aiheesta ei ollut. Projekti oli juuri alkamassa ja aikaa valmistautumiseen ei ollut käytännössä ollenkaan. Alussa oma tietämättömyys aiheesta oli selkeästi läsnä ja uutta opeteltavaa oli todella paljon.

Aiheeseen liittyvää lähdemateriaalia on saatavilla hyvin rajoitetusti. Lähteiden vähyys ja riittävä luotettavuus aiheutti muutamaan otteeseen päänvaivaa. Tietosuoja-asetus on myös itsessään hyvin tulkinnanvarainen. Asetus tulee luultavasti tarkentumaan vielä kevään 2018 aikana EU:n ja tietosuojaviranomaisten toimesta. Moni tulkinnanvarainen kohta saattaa siis muuttua opinnäytetyön palautuksen jälkeen.

Toimenpidesuosituksia laatiessa en voinut käyttää hyväkseni minkäänlaista lainopillista apua tulkinnallisissa tilanteissa. Toimeksiantajan toimesta tehtävät erilliset toimenpidesuositukset eivät valmistuneet riittävän aikaisin, jotta niitä olisi voinut hyödyntää opinnäytetyötä tehdessä. Tästä syystä lainopilliset neuvot jäivät saamatta ja liian tulkinnanvaraiset huomiot on jätetty käsittelemättä, jotta opinnäytetyön uskottavuus säilyisi.

Toimenpidesuunnitelman pohjalta kävi selväksi, että verkkosivuilla vierailevaa käyttäjää ja hänen käyttäytymistään seuraavia ohjelmistoja tulisi tutkia lainoppineen kanssa tarkemmin. Seuranta ja siitä käyttäjälle tehtävä informointi jäi hieman epäselväksi ja se on syytä selvittää ennen kevättä 2018. Myyntiprosessissa mukana oli kaksi ERP-järjestelmää, mutta lähempi tarkastelu koski vain toista järjestelmistä. Molemmat ERP-järjestelmät tulisi tarkastella samalla tarkkuudella, jotta varmistutaan riittävän läpinäkyvästä henkilötietojen käsittelystä. Yrityksen yhteistyökumppanit ovat

merkittävässä osassa palveluiden tuottamista ja heidän henkilökuntansa koulutuksen taso ja yritysten välisten SLA-sopimusten ajantasaisuus tulisi tutkia.

Asiakasyritys voi käyttää opinnäytetyötä suuntaa antavana muutossuunnitelmana yhdessä toimeksiantajan omien suositusten kanssa. Toimeksiantajan muutossuunnitelma tulee sisältämään lainopillisen tulkinnan kohdista, jotka omaan opinnäytetyöhön olivat liian tulkinnanvaraisia ilman lakitekstin tulkintaa.

Opinnäytetyö oli kokonaisuudessaan erittäin työläs. Haastatteluosuus oli jaettu noin 1,5 kuukauden ajalle, jonka jälkeen pääsin vasta analysoimaan saatuja tuloksia. Työn laajuutta jouduttiin rajaamaan koskettamaan pelkkää myyntipalvelua, koska tarkasteltavia järjestelmiä oli yhtä opinnäytetyötä varten aivan liikaa. Haastattelutilanteissa lakia tuntevan ihmisen apu olisi myös ollut paikallaan.

Riittävän luotettavan ja ajan tasalla olevan lähdemateriaalin sekä lainopillisista puutteesta huolimatta sain kasattua hyvän muutossuunnitelman asiakasyritystä varten. Toimenpidesuunnitelma on täysin oman tulkinnan ja päättelyn tulosta, johtuen asetuksen tulkinnanvaraisuudesta. Opinnäytetyön aihe on erittäin ajankohtainen ja antaa varmasti hyvän pohjan työelämää varten.

Lähteet

Bain & Company. 2017. Customer Relationship Management. Viitattu 14.1.2018. http://www.bain.com/publications/articles/management-tools-customer-relationship-management.aspx

Barnard-Wills, D., Chulvi, C. P., De Hert, P. 2016. Data protection authority perspectives on the impact of data protection reform on cooperation in the EU, 587-598. Viitattu 29.1.2018. https://www.sciencedirect.com/science/article/pii/S026736491630084X

EU:n tietosuoja-asetus (GDPR). Viitattu 8.1.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=FI

Heiskanen, V-M. 2017. Tietotilinpäätös helpommanaan EU:n tietosuoja-asetukseen valmistautumista. Espoo: Tieto– ja Viestintätekniikan ammattilaiset TIVIA ry, 8-9. Viitattu 8.1.2018. http://view.24mags.com/mobilev/f96baa81f49bb6b0b88c11d535cda3ae

Klinge, K. 2017. Mikä on ERP-järjestelmä?. Viitattu 14.1.2018. https://www.accountorenterprise.fi/2017/08/08/mika-erp-jarjestelma/

Kustula, S. 2015. Laadullinen ja määrällinen tutkimus opinnäytetöissä. Viitattu 14.1.2018. http://esseepankki.proakatemia.fi/laadullinen-ja-maarallinen-tutkimus-opinnaytetyossa/

Kysymyksiä ja vastauksia tietosuojauudistuksesta. 2016. Tietosuojavaltuutetun toimisto. Viitattu 9.1.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymyksiajavastauksia.html

Laatikainen, T. 2015. Master Data on monisyistä, monista syistä. Viitattu 14.1.2018. http://www.arihovi.com/master-data-blogi/

Lloyd, I. 2017. Information Technology Law. Viitattu 24.1.2018. https://books.google.com/books?isbn=0198787553

McDermott, Y. 2017. Conceptualising the right to data protection in an era of Big Data. Viitattu 24.1.2017. http://journals.sagepub.com/doi/pdf/10.1177/2053951716686994

Miinalainen, P. 2017. Suojele henkilötietoja-suojele organisaatiotasi. Sytyke 3, 6-7. Espoo: Tieto– ja Viestintätekniikan ammattilaiset TIVIA ry. Viitattu 8.1.2018. http://view.24mags.com/mobilev/f96baa81f49bb6b0b88c11d535cda3ae

Overby, S. Greiner, L. Gibbons, L. 2017. What is an SLA? Viitattu 10.12.2017. https://www.cio.com/article/2438284/outsourcing/outsourcing-sla-definitions-and-solutions.html

Sallinen, J. 2017. EU:n yleinen tietosuoja-asetus prosessina. Sytyke 3, 4. Espoo: Tieto– ja Viestintätekniikan ammattilaiset TIVIA ry. Viitattu 8.1.2018. http://view.24mags.com/mobilev/f96baa81f49bb6b0b88c11d535cda3ae

Schiff, J. 2011. A Dozen Simple Ways to Improve Customer Relations. Viitattu 14.1.2018. http://www.enterpriseappstoday.com/crm/ways-to-improve-customer-relations-1.html

Shroff, M. 2007. Privacy Impact Assessment Handbook. Viitattu 8.1.2018. https://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf

Sparta Consulting. 2017. Sparta Consulting verkkosivut. Viitattu 14.1.2018. https://spartaconsulting.fi/

Sparta Consulting. N.d. Prosessihaastattelut. Yrityksen sisäinen materiaali.

Talus, A., Autio, E., Hänninen, A., Pihamaa, H-T. & Kantonen, S. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Viitattu 22.1.2018. http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuojavastaavan asema. 2017. Tietosuojatieto.fi. Viitattu 9.1.2018. https://www.tietosuojatieto.fi/gdpr-asetus/38-tietosuojavastaavan-asema

VAHTI-raportti – 1/2016. EU-tietosuojan kokonaisuudistus. Viitattu 24.1.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128#page=1

Vilkka, H. 2007. Tutki ja mittaa. Viitattu 14.1.2018. http://hanna.vilkka.fi/wp-content/uploads/2014/02/Tutki-ja-mittaa.pdf

Liitteet

Liite 1. Myyntiprosessin vaiheet