Opinnäytetyö AMK

Liiketalous

2019

Ville Mäenranta

FYYSINEN TIETOTURVA KULKUNEUVOALAN YRITYKSESSÄ

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalous

2019 | 32 sivua

Ville Mäenranta

FYYSINEN TIETOTURVA KULKUNEUVOALAN YRITYKSESSÄ

Tämän opinnäytetyön tarkoituksena oli käsitellä ja kehittää tietyn kulkuneuvoalan yrityksen fyysisen tietoturvan kipupisteitä sekä pohtia miten uusi EU:n yleinen tietosuoja-asetus GDPR on vaikuttanut yrityksen toimintaan. Kävin läpi autoliikkeen fyysisen tietoturvan keinoja omien kokemuksieni perusteella ja kehittämishankkeessa keskityimme toisen kulkuneuvoalan yritykseen. Fyysinen tietoturva on erityisen tärkeä osa-alue yrityksessä, jossa käsitellään arkaluonteisia henkilötietoja päivittäin. Analysoin miten fyysisen tietoturvan toimenpiteet toteutuvat erikoisliikkeessä, sillä asenteet fyysistä tietoturvaa kohtaan eivät ole halutulla tasolla. Keskityin opinnäytetyössä erityisesti myymälätiloissa sijaitsevien henkilötietojen käsittelyyn ja niiden säilömiseen. Kävin läpi prosesseja ja käytäntöjä, jotka vaikuttavat turvalliseen asiakastietojen käsittelyyn myymälätiloissa sekä analysoin, toteutuuko turvallisen tietoturvan menettely yrityksessä. Tilannekatsauksen avulla löydämme epäkohtia fyysisestä tietoturvasta, joiden avulla asiakasyritys pystyy kehittämään toimintaansa entistä turvallisemmaksi. Ajantasainen fyysisen tietoturva on yrityksen sekä asiakkaan etu. Turvallisen tietoturvan käytännöt tulee ottaa yrityksessä huomioon yleisesti sekä sisäistää toimialakohtaiset erityispiirteet.

ASIASANAT:

Tietosuoja, GDPR, fyysinen tietoturva, henkilötieto, kulkuneuvoala

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business

2019 | 32 pages

Ville Mäenranta

PHYSICAL DATA PROTECTION IN VEHICLE INDUSTRY COMPANY

The purpose of this thesis was to process and develop the full range of physical security points for a vehicle dealership company and to consider how the new EU general data protection regulation has affected GDPR's operations. I went through the physical security means of the car dealership because of my own experiences, and in the development project we focus on a vehicle industry company in another field. Physical security is a particularly important part of a company that deals with sensitive personal data daily. I analyzed how physical security measures take place in vehicle dealership, as attitudes towards physical security are not at the desired level. We focused on the processing and preservation of personal data in store premises. I reviewed the processes and practices that promote the safe handling of customer data in the store premises and found out whether a secure data security procedure is being implemented in the company. Through my data collection, I found flaws in physical information security that enable a client company to develop its operations more safely. Up to date physical security is the interest of the company and the customer. Safe data security practices should be taken into account in the company and internalized by industry-specific features.

KEYWORDS:

Data protection, GDPR, physical information security, personal data, vehicle dealership

SISÄLTÖ

KUVIOT

SANASTO

Henkilötieto

Henkilötiedolla tarkoitetaan informaatiota, josta henkilö, hänen perheenjäsen tai samassa taloudessa asuva voidaan tunnistaa suorasti tai epäsuorasti. Henkilötietoja ovat esimerkiksi nimi, sähköposti, kotiosoite tai auton rekisterinumero. (Hanninen ym. 2017, 19 20) Jokaisella kansalaisella on oikeus, että hänen henkilötietojaan käsitellään turvallisesti ja tietosuojaperiaatteiden mukaisesti. Vain yritystä koskevat tiedot eivät ole henkilötietoja. Henkilötiedon määritelmää voidaan pitää laajana, mutta tiivistettynä kaikki tieto mistä tietty henkilö voidaan tunnistaa, on henkilötietoa. Yrityksessä on tärkeä miettiä henkilötietojen elinkaari mihin sisältyy prosessien luonti muun muassa henkilötietojen keräämiseen, käsittelyyn, luovutukseen ja säilytykseen. (Korpisaari ym. 2018, 49 50)

Kuvio 1. Henkilötiedon elinkaari (toimeksiantajayrityksen GDPR-koulutusmateriaali 2018).

Tietoturva	Tietoturvalla eli tietoturvallisuudella tarkoitetaan muun muassa henkilötietojen lainmukaista käsittelyä sekä haluttujen henkilöiden pääsyä haluttuihin tietoihin. Tietojärjestelmät, tietoaineistot ja palvelut tulee suojata materiaalien eheyttä ja luottamuksellisuutta ajatellen. Virus- ja salasanasuojaukset ovat muun muassa osa tietoturvaa. (Tietosuoja.fi 2019)
Henkilörekisteri	Samaan käyttötarkoitukseen kerättyjä henkilötietoja sisältävä tietojoukko. Tietynlaiset tiedot on kerätty joukoksi, josta tarvittavat tieto voidaan tarvittaessa helposti löytää. Rekisteriä tehdessä tulee miettiä mitkä tiedot ovat tarpeellisia yritystoiminnalle ja mitkä välttämättömiä tietoja. Rekisteri sisältää samaa käyttötarkoitusta varten olevia tietoja. Tulee myös tietää mitä varten henkilötietoja käytetään. Henkilörekisteri voi olla sähköisessä muodossa tai esimerkiksi paperilla. (AKL 2018)
Rekisterinpitäjä	Rekisterin pitäjä käsittelee ja on vastuussa henkilötietojen oikeellisuudesta sekä laillisuudesta. Rekisterinpitäjä voi olla yksityishenkilö, yritys tai jokin muu taho, jonka nimiin henkilörekisteri on perustettu. Rekisterinpitäjä päättää henkilötietojen käsittelyn tarkoitukset sekä keinot. (AKL 2018)
Rekisteröity	Tarkoitetaan henkilöä, kenen henkilö- tai asiakastiedot ovat henkilörekisterissä tai muussa sellaisessa. Rekisteröity on henkilö, kenen tietoja käsitellään. (AKL 2018)
Tietovuoto	Tiedon tarkoittamaton pääsy oman suojatun järjestelmän ulkopuolella. Arkaluontoisen tiedon vuotamisella tarkoitetaan minkä tahansa suojatun tiedon pääsemistä väärille osapuolille. Suojattu materiaalia voi olla esimerkiksi asiakas- tai henkilötietoja. (Hanninen ym. 2017, 23)
Suostumus	Kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Rekisterinpitäjällä tulee olla asiakkaan suostumus käsitellä hänen henkilötietojaan. Tälläinen syy henkilötietojen

käsittelylle voi olla muun muassa suullinen toimeksianto tai monien yritysten tapauksessa esimerkiksi kauppasopimuksen allekirjoittaminen. Tietosuojalaissa kerrotaan kuusi erilaista suostumusta, joiden myötä rekisterinpitäjällä on oikeus henkilötietojen käsittelyyn. Nämä käsittelyperusteet oikeuttavat lailliseen henkilötietojen käsittelyyn. (Tietosuojavaltuutetun toimisto, GDPR 2018)

- Rekisteröidyn suostumus
- Sopimus
- Rekisterinpitäjän lakisääteinen velvoite
- Elintärkeiden etujen suojaaminen
- Yleinen etu ja julkinen valta
- Rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

1 JOHDANTO

Tietosuojan tehtävä on suojella yksityishenkilöiden tietoja. Jokaisella on oikeus henkilötietojensa suojaan ja yksityisyyteen. Tämä tarkoittaa käytännössä sitä, että yrityksellä on velvollisuus käsitellä henkilötietoja suojatusti, joten yksityishenkilön on turvallista luovuttaa henkilötietoja yrityksen käyttöön ilman pelkoa niiden väärinkäytöstä. Tämän vuoksi laissa on määritetty tietosuojalaki, jonka tarkoituksena on tukea turvallista ja nykyaikaista tietosuojaa. Haasteena on luoda täysin aukottomia tietosuojaprosesseja- ja toimintoja, jotka toimivat käytännön tasollakin ilman ongelmia. Henkilötietojen säilyttäminen oikeiden tahojen hallussa on elintärkeää yrityksien sekä yksityishenkilöiden edun kannalta.

Fyysisellä tietoturvalla tarkoitetaan toimitilojen sekä niissä olevien arkaluontoisten materiaalien suojaamista ulkopuolisilta uhilta. Uhkana voi olla muun muassa varkaus, tulipalo tai lukitsemattomat säilytystilat. Opinnäytetyössä käyn läpi tietosuojaperiaatteita fyysisen tietoturvan näkökulmasta ja luomme kehitysideoita turvallisemman tietosuojan puolesta. Opinnäyte on tehty yhteistyössä kulkuneuvoalan yrityksen kanssa, jonka myötä kartoittamaan tietoa yleisemmistä fyysisen tietoturvan kehityskohdista ja mitkä osa-alueet ovat tärkeitä turvallisen toimintaympäristön kannalta. Tavoitteena on luoda tietoturvan mittareita, joita voi testata missä tahansa vastaavan alan yrityksessä ja niiden avulla toteuttaa entistä turvallisempaa liiketoimintaa niin yrityksen kuin asiakkaan näkökulmasta.

Henkilötietojen kanssa tekemisissä olevia tahoja säätelee lainsäädäntö. EU:n laajuinen tietosuoja-asetus eli General Data Protection Regulation (GDPR) astui voimaan 25.05.2018. Asetus on jo säädetty 2016, mutta siirtymäaikaa oli 2 vuotta yritysten valmistautuessa nykyisiin velvoitteisiin. Tämän säädöksen on tarkoitus yhtenäistää tietosuojalainsäädäntöä eri maiden välillä ja luoda selvät sekä yhteiset pelisäännöt. Tarkoituksena on myös turvata yksityishenkilöiden oikeus turvalliseen henkilötietojen käsittelyyn. Uusi asetus koskee kaikkia EU:n alueella palveluja tarjoavia yrityksiä ja pyrkii päivittämään tietosuojalain vastaamaan nykyajan tarpeita sekä odotuksia. Säädöksen myötä voimaan astui erilaisia oikeuksia ja velvoitteita. Tietosuojalaki pyrkii vaalimaan turvallista tietosuojakäytäntöä ja turvaamaan jokaisen henkilötiedot.

Henkilötiedot ovat keskeisiä tekijöitä jokapäiväisessä toiminnassa monessa eri yrityksessä. Henkilötietojen käsittelyprosessien tulee olla turvallista ja tukea

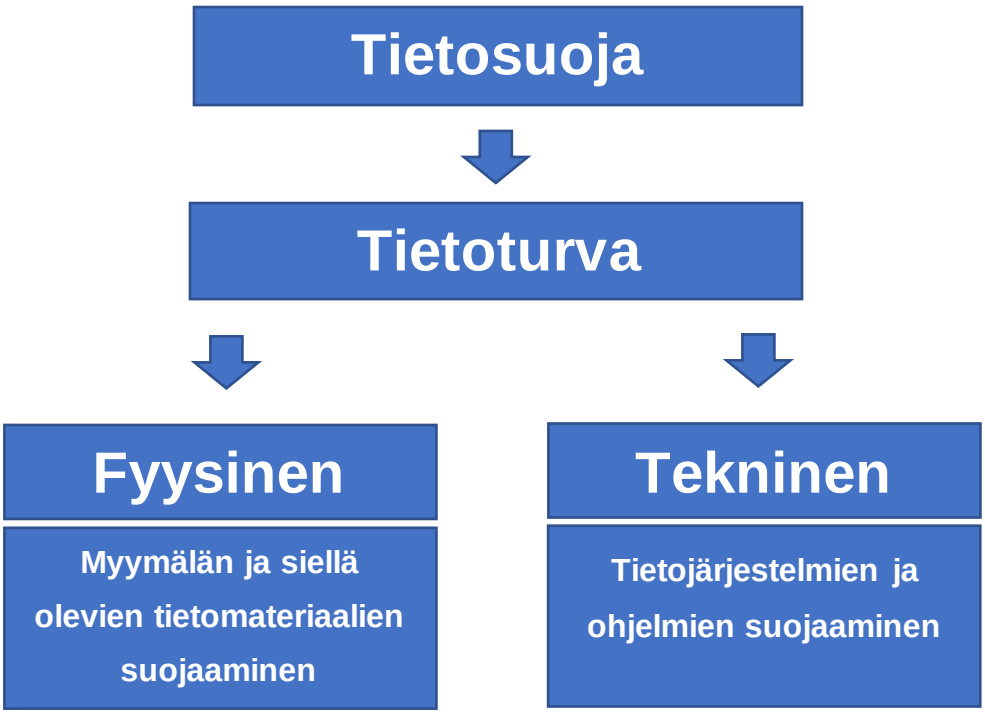
tietosuojalakia. Tietosuoja voidaan jakaa tekniseen sekä fyysiseen suojaamiseen. Fyysisellä suojaamisella tarkoitetaan, että erityisesti asiakkaiden henkilötiedot tai muu arkaluonteinen materiaali ei ole ulkopuolisten ulottuvilla autoliikkeessä liikkuessa. Tämä tarkoittaa, että kuka tahansa myymälätiloissa liikkuu, fyysisen tietotietoturvan prosessit ovat ajan tasalla ja muun muassa asiakkaiden henkilötiedot ovat suojassa ulkopuolisilta ja muilta uhilta. Henkilötietoja sisältäviä materiaaleja voivat olla huolto- ja tai rahoitussopimukset.

2 TIETOSUOJA

2.1 Tietosuojan määritelmä

Ihmisellä on aina ollut tarve yksityisyyteen jollain tasolla. Yksityisyyden tarve on tullut ilmi eri tavoilla ajan saatossa. Viime vuosikymmeninä tieto- ja viestintäteknologia on kehittynyt hurjin harppauksin ja jotta edelleen ihmisille voidaan tarjota turvallista yksityisyyden suojaa, on luotava erilaisia lakeja ja asetuksia ajamaan turvallisia tietosuojaperiaatteita. (Korpisaari ym. 2018, 1) Tietosuoja on ollut viime aikoina pinnalla yhteiskunnallisesti entistä enemmän kuin ennen. Tähän on vaikuttavat muun muassa uusi tietosuoja-asetus eli GDPR (General Data Protection Regulation) sekä suurten yritysten virheet henkilötietojen kanssa. Ihmiset ovat entistä enemmän huolissaan, että käsitelläänkö heidän henkilötietojaan oikein ja millä perustein. Jokaisella meistä on oikeus tietosuojaan perusoikeuden mukaisesti, minkä tarkoituksena on turvata meitä henkilötietoja käsitellessä. Tietosuoja tarkoittaa pääsääntöisesti oikeutta omiin henkilötietoihin sekä rekisterinpitäjien huolellisia asetusten mukaisia käsittelyperiaatteita niiden suhteen. (Autoliikkeen tietoturvamateriaali 2018) Tietoturva on kuitenkin eri termi kuin tietosuoja ja näiden kahden termin eroavaisuudet on tärkeä tiedostaa; tietoturvalla tarkoitetaan prosesseja tietoaineistojen ja -järjestelmien suojaamiseksi kun taas tietosuojalla enemmän henkilökohtaisia oikeuksia henkilötietoihin ja käsittelyperiaatteita. (Tietosuoja.fi 2018)

Kuvio 2. Tietosuojan ja tietoturvan yhteys (Mäenranta 2019)



Tietototurva voidaan jakaa karkeasti kahteen eri osa-alueeseen: tekniseen sekä fyysiseen tietoturvaan. Tekninen tietoturva käsittää, ettei laitteissa tai järjestelmissä ole tietoturvallisia puutteita eli henkilötiedot ja muu arkaluontoinen materiaali pysyy haluttujen tahojen hallussa. Ohjelmistot ja laitteet tulee pitää ajan tasalla päivityksistä sekä suojata ulkopuoliselta väärinkäytöltä ajantasaisilla keinolla. Suojakeinoja teknisessä tietoturvassa on muun muassa käyttäjätunnuksilla pääsy järjestelmiin, virustorjunta sekä palomuurit.

Suurimpia uhkia teknisessä tietoturvassa on ollut viime aikoina erilaiset tietomurrot sekä tietojen kalastelu yritykset. Erityisesti Office 365 -ohjelmiin liittyvät tietomurtoyritykset ovat kasvaneet vuonna 2019, joita voidaan sanoa kansainväliseksi trendiksi. Suuri suosio Office 365 -ohjelmien keskuudessa luo myös hakkereille mahdollisuuden tehokkaaseen vaihtoehtoon mahdollistaa tietojen kalastelu esimerkiksi väärennettyjen kirjautumissivujen avulla. Ulkopuoliset yrittävät päästä käsiksi yritysten järjestelmiin tai tietokantoihin muun muassa lähettämällä viruslinkkejä sähköpostin välityksellä ja teeskentelemällä muita tahoja. Tärkeimpiä keinoja tietojenkalastelulta suojautumiselle ovat kriittinen ajattelu, vahvat salasanat sekä kaksivaiheinen tunnistautuminen. Karkeasti voidaan sanoa, että kriittisellä ajattelulla pyritään arvioimaan, onko vieraista sähköpostiosoitteista tulleet salasana kyselyt tai miljoonaperintö onnittelut todenmukaisia vai yrittääkö toinen osapuoli mahdollisesti hyötyä sinun toiminnastasi jotenkin. Salasanan tulisi olla mahdollisimman vaikea ulkopuolisen tietää ja sen pitäisi olla mahdollisimman pitkä sekä sisältää isoja sekä pieniä kirjaimia, numeroita ja erikoismerkkejä. Lisäksi kaksivaiheinen tunnistautuminen tuo lisäturvaa, sillä sisäänkirjautuminen eri käyttöjärjestelmiin käyttäjätunnuksella ja salasanalla tulee lisäksi vahvistaa esimerkiksi omasta mobiililaitteesta. (Yrittäjät.fi 2019)

Fyysinen tietoturvan tarkoitus on taas katsastella ja turvata ettei kukaan pääse esimerkiksi varastamaan tai kopioimaan yrityksen henkilötietoja sisältäviä papereita myymälätiloissa. Fyysisyys tietoturvassa käsittää myös toimitilojen, henkilöiden sekä postiliikenteen suojaamisen mahdollisia uhkia vastaan. Fyysisen tietoturvan keinoja ovat muun muassa materiaalien säilyttäminen lukkojen takana sekä käsittelyn eheys lainmukaisesti. Pyritään myös minimoimaan mahdolliset palo- vesi- ja sähkövahingot sekä murtautumiset. Tarkoituksena on luoda yritykselle fyysisesti turvallinen toimiympäristö, joka on suojattu mahdollisilta sisäisiltä sekä ulkopuolisilta uhilta. (Vedenoja 2007, 8) Tässä opinnäytetyössä keskitymme asiakasyrityksen fyysiseen tietoturvaan ja tarkastelemme fyysisiä toimenpiteitä. Tarkkailun alla on esimerkiksi

säilytystilat, tietojen tuhoaminen sekä työpisteet. Asiakkaiden arat henkilötiedot tulisi olla myymälätiloissa täysin ulkopuolisten ulottumattomissa, joten fyysisessä tietoturvassa ei saisi olla aukkoja. Fyysisen tietoturvan ollessa heikko, muun muassa asiakkaiden henkilötiedot ovat jatkuvassa vaarassa joutua ulkopuolisten käsiin.

2.2 EU:n GDPR-asetus

Tietosuoja on tullut erityisen tutuksi aiheeksi monille uuden GDPR-tietosuoja-asetuksen tullessa voimaan. Euroopan komissio on laatinut tietosuoja-asetuksen (2016/679) vuonna 2016, joka siirtymä kauden jälkeen tuli voimaan 25.05.2018. Siirtymä kaudeksi asetettiin 2 vuotta, jotta kaikki yritykset pystyvät sopeutumaan uuteen direktiiviin. Tämän tietosuoja-asetuksen tehtävänä on ollut yhtenäistää valtioiden tietosuojakäytäntöjä sekä asettaa normit nykyaikaiselle tietosuojalle niin yritysten kuin yksityishenkilöiden kannalta. Tavoitteena on myös asettaa vahvistaa säännöt henkilötietojen käsittelylle sekä suojata henkilöiden perusoikeuksia tietosuojaan liittyen. Asetus lisää myös läpinäkyvyyttä yritysten ja yksityishenkilöiden välillä, sillä molemmille osapuolille tulee lisää oikeuksia turvallisen tietosuojan kannalta. (Korpisaari ym. 2018, 1 2)

Ennen tämän asetuksen voimaan tuloa henkilötietolakia (Finlex 2019) on sovellettu käytännössä. Henkilötietolain tarkoituksena on ollut turvata yksityisyyden suojaa sekä henkilöiden perusoikeuksia. Myös henkilötietojen vapaata liikkuvuutta jäsenvaltioiden välillä on tuettu. Uuden tietosuoja-asetuksen tehtävänä on ollut kumota aiemmin voimassa ollut henkilötietolaki, vahvistaa henkilötietolain periaatteita sekä edistää Euroopan digitaloutta. Yhtenäisen tietosuoja-asetuksen myötä myös hallintokustannusten on katsottu vähentyvän yrityksillä tulevaisuudessa, vaikkakin kustannuksia on syntynyt siirtymävaiheessa uusista tietosuojainvestoinneista ja tarpeellisista koulutuksista henkilökunnan osalta. (Korpisaari ym. 2018, 35)

Suomessa ei ole vielä tutkitusti asetettu rangaistuksia uuden GDPR-asetukseen liittyen, mutta tulevaisuudessa tämä asia saattaa muuttua ja yrityksiä saatetaan laittaa tarkempaan valvontaan. Ruotsissa yli 60 toimijaa on listattu GDPR-vastaisesta toiminnasta, joiden joukossa on myös suuria kansainvälisiä toimijoita. Saksassa on myös annettu ensimmäinen tuomio liittyen uuteen tietosuoja-asetukseen, jossa yritys on kerännyt henkilötietoja mitkä eivät ole olleet liiketoiminnan kannalta tarpeellisia. (TS 2018) Voi olla, että Suomessa ei ole vielä täysin havahduttu tietoturvan kriteereihin tai tärkeyteen, sillä yrityksiä ei ole vielä rankaistu tai otettu erityisesti tarkkailun alle.

2.3 Tietosuoja-asetus käytännössä

Uusi tietosuojalaki asettaa uusia velvollisuuksia rekisterinpitäjälle sekä oikeuksia, jotka voidaan jakaa koskemaan rekisterinpitäjiä sekä rekisteröityjä EU:n jäsenvaltioissa. Rekisterinpitäjän eli yrityksen on pitänyt toteuttaa tarvittavat toimenpiteet, jotta yrityksen toiminta on uuden tietosuoja-asetuksen mukaista. Vaadittavat tekniset ja organisatoriset toimenpiteet tarkoittavat esimerkiksi henkilöstön kouluttamista, ohjeiden luomista, tietoturvan analysoimista, prosessien kehittämistä sekä valvontaa. Rekisterinpitäjällä on aina viimekädessä vastuu henkilötietojen oikeanmukaisesta käsittelemisestä. Tulee myös pystyä todistamaan, että tietosuojakäytännöt ovat lainmukaisia. Tämä osoitus velvollisuus voi olla esimerkiksi, että verkkosivuilla kerrotaan tietosuojavastaavasta, käsiteltävistä tietoryhmistä, käsittelyn perusteista, ja henkilötietojen käyttötarkoituksesta. Turhan tiedon keruuta tulee välttää, jos sille ei löydy perusteluja. GDPR-tietosuojalaki ottaa myös kantaa asetuksen rikkomuksiin ja tietovuotoihin. Tietosuojalain mukaan rekisterinpitäjän on ilmoitettava rekisteröidylle 72 tunnin kuluessa tietovuodon tapahtumisesta. Lisäksi jos rekisteröity rikkoo asetuksen säädöksiä, voidaan määrätä enintään 10 miljoonan euron sakko tai kaksi prosenttia edeltävän tilikauden maailmanlaajuisesta liikevaihdosta, kumpi onkaan suurempi. (Tietosuojamalli, 2018)

Rekisterinpitäjien valmistautumisen uuteen tietosuoja-asetukseen voidaan jakaa useampaan suurempaan aihealueeseen:

- Yrittäjän tulee tiedostaa missä järjestelmissä ja muodoissa henkilötietoja on. Tulee saada yleiskuva, mitä kaikkia henkilötietoja yritys käyttää ja missä tietojärjestelmissä tiedot sijaitsevat.
- Jokaiselle henkilötiedolle pitää olla oma käyttötarkoituksensa. On hyvä kategorioida mitä henkilötietoja tarvitaan mihinkin prosessiin tai käyttötarkoitukseen. Turhat tai vanhentuneet henkilötiedot pitää poistaa järjestelmistä.
- Tulee tiedostaa riskit liittyen henkilötietoihin liittyen niin teknisesti kuin fyysisestikin. Omille henkilötietoryhmille voi tehdä oman riskiarvion ja miettiä miten käsittelyä tehostaisi tai miten pitäisi toimia tietojen vuotaessa ulkopuolisten käsiin
- Suunnitelman luonti auttaa hahmottamaan ja organisoimaan henkilötietojen käsittelyä. Suunnitelmassa tulee tulla ilmi, miten näistä edellä mainituista kohdista huolehditaan ja miten prosesseja kehitetään.

- Kaikki työ mitä on tehty uuden tietosuoja-asetuksen hyväksi, on hyvä dokumentoida talteen. Näin tietoja on helppo ymmärtää ja hahmottaa kokonaisuuksia kehittämisen kannalta. Asetuksessa myös kerrotaan, että rekisterinpitäjän on tarvittaessa todistettava toimivansa laillisesti. (Korpisaari 2018, 17-18)

Myös rekisteröidyn eli useassa tilanteessa asiakkaan oikeudet laajenevat uuden tietosuojalain myötä. Rekisteröidyllä on muun muassa oikeus tietää käsitteleekö yritys häntä koskevia henkilötietoja sekä mitä henkilötietoja ja tarvittaessa päästä käsiksi häntä koskeviin henkilötietoihin. Virheelliset tiedot on myös oikeus korjata, siirtää tai tulla unohdetuksi kokonaan yrityksen järjestelmistä. On myös oikeus vastustaa henkilötietojen käsittelyä, tai siirtää ne toisen organisaation haltuun. Näissä rekisteröidyn oikeuksissa on pitää muistaa, että edellä mainittuja oikeuksia ei voi käyttää kaikissa tilanteissa. (Hanninen ym. 2017, 51-56) Tätä asiaa voi verrata yrityksen ja asiakkaan väliseen kauppasopimukseen: jos asiakas on kirjoittanut tilaussopimuksen, asiakas ei voi kieltää yritystä käsittelemästä hänen henkilötietojaan. Eli tilanteeseen vaikuttaa muun muassa se mikä on henkilötietojen käsittelyperuste.

3. TIETOTURVA AUTOLIIKKEESSÄ

3.1 Autoliike ja tietoturva

Autoliikkeissä henkilötiedot ovat tärkeässä asemassa niin asiakkuuden hoitamisen kuin myös autojen rekisteröimisen ja vakuutuksien tekemisen kannalta. Henkilötietoja kerätään erilaisten dokumenttien kautta muun muassa tilaussopimuksissa, huoltokirjoissa sekä koeajopapereissa. Asiakkaiden henkilötietojen säilyttäminen ei pääty uuden auton luovutuksen yhteydessä, vaan autoliikkeellä on velvollisuus säilyttää kauppakirjoja kirjanpitolain mukaisesti kuluvan vuoden sekä kuusi seuraavaa vuotta. Lisäksi autoliikkeellä on oikeus käyttää henkilötietoja asiakassuhteen perusteella lain vaatimukset huomioiden. Henkilötietojen käsittely tarvitsee kuitenkin aina käsittelyperusteen, kuitenkaan asioimisviesti esimerkiksi huollon muistutus ei edellytä suostumusta. (Autoliikkeen tietoturvamateriaali 2018)

3.2 Arkaluonteiset henkilötiedot

Tärkeitä henkilötietoja autoliikkeiden kannalta ovat erityisesti puhelinnumerot asiakkuuksien hoitamisen ja yhteydenottamisen kannalta. Autoliikkeessä käsitellään myös usein arkaluonteisia henkilötietoja, joita ovat muun muassa terveydentilaan, sosiaaliturvan tarpeeseen tai yhteiskunnalliseen asemaan liittyviä tietoja (Finlex 2019). Lisäksi henkilötunnukset ovat arkaluontoisia ja kriittisiä osamaksusopimuksien ja autojen rekisteröinnin yhteydessä. Erityisen arkaluonteisia asiakkaita koskevia tietoja autoliikkeessä ovat henkilötunnukset tai esimerkiksi invaliditeetin tuoma veroalennussopimus. Jokaisen toteutuneen auton oston tai myymisen myötä yritys säilyttää niihin liittyviä sopimuksia, joissa on asiakkaiden henkilötunnuksia, osoitteita ja puhelinnumeroita sekä muita henkilötietoja. Autojen rekisterinumerot ovat myös tärkeitä tietoja, niiden avulla pystytään yksilöimään autot ja yhdistämään asiakkaaseen. Autojen huoltohistoria ei varsinaisesti ole henkilötietoa, mutta sen käsittelyyn on säädetty oma ohjeistus seuraavassa luvussa.

Asiakkaiden henkilötunnuksia otetaan talteen kauppakirjoihin sekä osamaksusopimuksiin. Kauppakirjoja säilytetään myymälätiloissa niin fyysisesti kuin sähköisestikin. Autojen tilaussopimuksien säilyttäminen auttaa muun muassa todistamaan riitatilanteissa toteutuneiden kauppojen tilanteen ja sisällön sekä niiden säilyttämisestä on määrätty kirjanpitolaissa. Yhä useammin asiakkaat valitsevat auton

maksutavaksi osamaksun eli rahoituksen, jota maksetaan kuukausittain rahoitusyhtiölle. Tämä tarkoittaa, että asiakas ja rahoitusyhtiö tekevät sopimuksen maksusuunnitelmasta kuukausittain sekä ajoneuvon omistajaksi merkitään rahoitusyhtiö ja haltijaksi asiakas. Rahoitus vaihtoehto luo helpomman tien asiakkaalle hankkia uusi ajoneuvo, sillä rahallista pääomaa ei vaadita niin paljon. Osamaksusopimuksien myötä myös arkaluonteisia tietoja syntyy enemmän ja se asettaa enemmän haasteita yrityksen harteille niin teknisessä kuin fyysisessä tietoturvassa. Toinen osa rahoitussopimuksista säilötään myymälätiloissa ja toinen lähetetään rahoitusyhtiölle sopimuksen toimeenpanon saattamiseksi. Rahoitussopimuksia sekä muita arkaluonteisia tietoja lähetetään päivittäin postin avulla, joten postiliikenteelle tulee luoda turvalliset toimintaperiaatteet.

3.3 Huoltohistoria

Autoliikkeiltä kysytään usein ajoneuvojen huolto-, omistus- ja muuta historiaa koskevia tietoja. Kysymyksiä voivat esittää esimerkiksi ajoneuvon nykyinen omistaja, potentiaalinen ostaja, toinen autoliike tai viranomainen. EU:n tietosuoja-asetuksen myötä 25.5.2018 alkaen, henkilötietoja sisältävän datan luovuttamiseen tulee kiinnittää aiempaa enemmän huomiota. Asetus ja sen nojalla annettava uusi kansallinen tietosuojalainsäädäntö korvaa käytännesäännöissä viitatun henkilötietolain. Autojen huoltohistorian avulla pystytään taas näkemään auton huoltohistoria ja näkemään onko ajoneuvoa huollettu asianmukaisesti merkkiliikkeissä ja mihin ajankohtaan tapahtumat sijoittuvat. Ajoneuvoon liittyvä huoltodata ei pääsääntöisesti ole henkilötietoa, mutta ei voida poissulkea sitä, että jossain tilanteissa huoltohistoriatietoihin sisältyisi esimerkiksi ajoneuvon edellisen omistajan henkilötietoja. Henkilötiedon määritelmä on hyvin laaja. Periaatteessa kaikki tiedot, josta tietty henkilö voidaan epäsuorastikin tunnistaa, katsotaan henkilötiedoiksi. Tämän vuoksi henkilötietolainsäädännön velvoitteet tulee huomioida huoltohistoriatiedon luovuttamiseen liittyvissä tilanteissa. Auton omistajan, potentiaalisen ostajan tai toisen autoliikkeen kysyessä ajoneuvoon liittyviä tietoja, tulee lähtökohtaisesti antaa ainoastaan ajoneuvon huoltoon ja korjauksiin liittyvää teknistä tietoa. Ajoneuvon aikaisempiin omistajiin liittyviä henkilötietoja ei yleensä ole perustetta antaa. Aikaisempia omistajia koskevat henkilötiedot eivät yleensä edes ole tarpeellisia kysyjälle. Viranomaisille tiedot tulee kuitenkin antaa viranomaisen esittämän pyynnön mukaisessa laajuudessa. (AKL 2018)

3.3.1 Huoltohistorian luovuttaminen ajoneuvon ostajalle

Myytäessä omasta liikkeestä autoa kuluttajalle, myyjällä on kuluttajansuojalain nojalla velvollisuus antaa maksutta kaikki se tieto tuotteesta, joka on myyjän tiedossa ja jolla voi olla merkitystä ostopäätökseen. Tällainen tieto voi olla esimerkiksi tieto kolarikorjauksista, muista laajoista korjauksista ja huolloista.

3.3.2 Huoltohistoriatietojen luovuttaminen toiselle autoliikkeelle

Toisesta liikkeestä kysyttäessä huoltohistoriaa, ei yleensä ole lakisääteistä velvollisuutta tietojen antamiseen. Tietojen antaminen kannattaa pitää varsin suppeana, rajoittuen lähinnä huoltokirjasta ilmeneviin tietoihin. Esimerkiksi tiedot siitä, ovatko huollot tehty kyseessä olevassa liikkeessä säännöllisesti. Autoliikkeellä on lähtökohtaisesti oikeus veloittaa tietojen antamisesta aiheutuneet kulut.

3.3.3 Huoltohistoriatietojen luovuttaminen muualta ajoneuvon ostaneelle kuluttajalle

Pääsääntöisesti autoliikkeellä ei ole lakisääteistä velvollisuutta antaa ajoneuvon huoltohistoriaan liittyviä tietoja kuluttajalle, joka on ostanut ajoneuvon muualta, ja jolla ei ole minkäänlaista sopimussuhdetta kyseessä olevaan autoliikkeeseen. Tietojen antaminen on vapaaehtoista, ja autoliikkeellä on lähtökohtaisesti oikeus veloittaa tietojen antamisesta aiheutuneet kulut. Yleensä tietojen antaminen on perusteltua siinä laajuudessa, mitä huoltokirjasta ilmenee. Ennen tietojen antamista tulee kuitenkin varmistaa, että ajoneuvo on tietoja kysyvän henkilön omistuksessa.

3.3.4 Huoltohistoriatietojen luovuttaminen viranomaiselle

Mikäli viranomaiset tiedustelevat ajoneuvoon liittyviä tietoja, tulee tietopyynnön mukaiset tiedot antaa. Ennen tietojen luovuttamista tulee varmistua, että tietopyyntö on todella viranomaisen esittämä. Erilaiset tietojenkalastelut ja huijausyritykset voivat olla mahdollisia. (Autoliikkeen tietoturvamateriaali 2018)

3.4 Fyysinen tietoturva

Tietoturvan myötä tietyillä aloilla on omia ominaispiirteitä, jotka pitää huomioida yrityksen toimintaperiaatteissa. Tietosuoja on tärkeä osa autoliikkeen jokapäiväistä toimintaa ja on perusedellytyksiä menestyksekkäälle yritystoiminnalle. On tärkeää arvostaa nykyisiä tietosuojakäytäntöjä, jotta henkilötietoja käsiteltäisiin mahdollisen turvallisesti sekä kouluttaa henkilökunta tietosuojaperiaatteiden mukaisesti. Turvallinen tietosuojakäsittely

edellyttää turvatoimia eri osa-alueilla, jotta henkilötiedot eivät pääse vääriin käsiin. Turvallista tietosuojakäytäntöä tuetaan muun muassa fyysisellä tietoturvaamisella. Fyysisellä tietoturvalla pyritään maksimaaliseen tiedon turvaamiseen myymälätiloissa ja estämään arkojen tietojen pääsyn vääriin käsiin tai sen tuhoamisen. Fyysisen tietoturvan keinoja autoliikkeessä on lueteltu seuraavana.

3.4.1 Arkaluontoisten materiaalien säilyttäminen lukkojen takana

Automyyjien ja muiden asiakastiloissa työskentelevien tulee säilyttää kaikki arkaluontoinen materiaali, henkilötietoja sisältävä aineisto sekä autojen avaimet lukitussa kaapissa tai tilassa. Myymälätiloissa ulkopuolisten on helppo päästä käsiksi arkaluontoisiin materiaaleihin, ellei ne ole lukkojen takana tai valvonnan alla. Tämä tarkoittaa, että poistuessa työpisteeltä siihen ei saa jäädä arkaluontoista materiaalia tai autojen avaimia, sekä työpisteen kaapit ja laatikot tulee olla lukitut. Reitit hallintotiloihin pitää olla lukitut, sillä tilat sisältävät esimerkiksi arkistoituja kauppakirjoja sekä muuta arkaluontoista materiaalia.

3.4.2 Henkilötiedot käytetyissä autoissa

Käytettyjen autojen tullessa yrityksen haltuun asiakkaalta, auton huoltokirjassa voi olla edellisen omistajan henkilötietoja sisältäviä materiaaleja muun muassa huoltokuitteja tai takuutodistuksia. Auton ollessa yrityksen omistuksessa sekä luovutettaessa uudelle omistajalle, se ei saa sisältää edellisten omistajien henkilötietoa, joten tämän tyyppinen materiaali tulee poistaa välittömästi huoltokirjasta. Edellisten omistajien henkilötiedot voidaan sutata tai poistaa kokonaan, pääasiana ettei edellisiä omistajia voida tunnistaa. Tämän prosessin pitäisi automaattisesti toteutua jokaisen käytetyn auton kohdalla, kun yritys saa asiakkaan auton nimiinsä.

3.4.3 Tietokoneen lukitseminen

Tietokone tulee lukita aina poistuessa työpisteeltä. Tietokoneet tulee myös olla vahvalla salasanalla suojattu, jotta suojauksen teho voidaan maksimoida. Pikalukitus on nopea ja tehokas tapa lukita tietokone, jolloin ulkopuoliset eivät pääse käsiksi tietokoneessa oleviin ohjelmiin tai tietoihin. Tietokoneella voi olla auki esimerkiksi henkilötietoja sisältäviä kauppakirjoja, joita ei haluta muiden asiakastiloissa liikkuvien tietoon. Myöskään muuta arkaluonteista materiaalia ei saa jättää työpisteelle vartioimatta.

3.4.4 Arkaluontoisen materiaalin tuhoaminen

Arkaluonteisia tietoja sisältävät paperit tulee laittaa tietoturvaroskakoriin tai vaihtoehtoisesti paperisilppuriin välittömästi, kun niitä ei koeta enää tarpeellisiksi. Näitä tietoa sisältäviä dokumentteja voivat olla esimerkiksi takuutodistukset, huoltosopimukset, koeajoluvat tai kauppasopimukset. Kerätty tieto voi vanhentua asiayhteydestä riippuen, joten turhan tiedon pitäminen hallussa ei ole suotavaa. Tietoturvaroskakorin tai silppurin käyttö varmistaa, ettei tietoja vuoda vääriin käsiin. Henkilötietoja tai muuten arkoja materiaaleja sisältäviä dokumentteja ei missään nimessä saa laittaa yleiseen roska-astiaan, sillä kuka vaan voi päästä tällöin käsiksi niihin.

3.4.5 Postiliikenteen turvallisuus

Autoliikkeessä postin välityksellä saapuu ja lähtee päivittäin useita arkoja henkilötietoja sisältäviä kirjeitä. Postiliikenteen kautta liikkuu muun muassa kaikki toteutuneet osamaksusopimukset, jotka pitää välittää rahoitusyhtiöille allekirjoitettuina sopimuksien toteutumiseksi. Postiliikenteen käsittely ja niiden säilöminen tulee tapahtua mahdollisimman turvallisesti, joten ulkopuoliset uhat eivät pääse niihin käsiksi. Saapuva sekä lähtevä posti tulee säilöä ja käsitellä lukituissa tiloissa eli asiakastilojen ulkopuolella. Posti ei saisi oleskelle myymälätiloissa, sillä kirjeet ja paketit ovat suuremman uhan alaisena.

3.4.6 Vartiointi sekä hälytykset

On myös tärkeä varautua myymälän turvallisuuteen varsinaisten työaikojen ulkopuolellakin. Ulkopuolinen vartiointiliike, ovien ja porttien lukitukset sekä hälytysjärjestelmät estävät ulkopuolisten pääsyn myymälätiloihin autoliikkeen aukioloaikojen ulkopuolella. Myös paloturvallisuus laitteiden tulee olla nykyaikaa vastaavat ja huolletut, kuin myös sähkö- sekä ilmastointilaitteiden. Kameravalvonnan avulla on mahdollista saada tietoa ulkopuolisista vieraista. (Vedenoja 2017, 4-7)

3.4.7 Henkilöstön kouluttaminen

Henkilöstö tulee kouluttaa tietoturvaperiaatteiden mukaisesti ja henkilöstön toimintaa tulee tarkkailla mahdollisten puutteiden varalta. Tulee aihe-alueittain miettiä tärkeitä tietoturvan kokonaisuuksia ja luoda tarkkoja ohjeistuksia henkilökunnalle. Henkilöstön tulee tiedostaa turvalliset tietoturvakäytännöt ja toimia niiden mukaan. Yritys on entistä turvallisempi toimintaympäristö, jos työntekijät toimivat turvallisten

tietoturvaperiaatteiden mukaisesti. Tietoturvan merkitys korostuu erityisesti autoliikkeissä, sillä arkojakin henkilötietoja käsitellään päivittäin myymälätiloissa ja niistä syntyy dokumentoitavia papereita säilöttäväksi. (AKL 2018)

4 Kehittämishanke toimeksiantajayrityksessä

4.1 Tiedonkeruun taustoja

Kehittämishankkeeseen valittu erikoisliike käsittelee päivittäin asiakkaiden henkilötietoja, joista osa on niin sanottuja arkoja henkilötietoja. Kävimme opinnäytetyössä aiemmin läpi fyysistä tietoturvaa autoliikkeen näkökulmasta, mutta kehittämishankkeeseen valitsin yrityksen toiselta kulkuneuvoalalta. Kaikkia fyysisen tietoturvan prosesseja ei ole kuvailtu tarkasti, sillä tavoitteena on, ettei kyseistä yritystä voitaisi tunnistaa mahdollisten tietoturva puutteiden johdosta. Esimerkiksi henkilötunnukset tai muu arkaluonteinen tieto ovat usein välttämättömiä tiettyjen prosessien toteuttamiseksi. Tietyissä erikoiliikkeissä kuin muissakin yrityksissä on perusolettamuksena, että kaikki arkaluontoinen tieto ja materiaali pysyisi vain haluttujen osapuolien hallussa. Fyysinen tietoturvallisuus on tärkeä osa edellä mainittua kokonaisuutta sekä yleistä turvallisuutta. Yhteisenä tavoitteena asiakasyrityksen kanssa oli kehittää nykyistä turvallisuutta ja minimoida mahdollisten tietovuotojen uhat. Valitsimme yhteistyössä myymälätilan tärkeimmät fyysisen tietoturvallisuuden prosessit ja mietimme uhkien mahdollisuutta. Päätimme tarkistaa fyysisen tietoturvan nykytilanteen ja sen pohjalta kehittää toimintaperiaatteita.

Suoritin tilannekartoituksen asiakasyrityksessä fyysiseen tietoturvaamiseen liittyen sekä miten tietosuojakäytännöt ja periaatteet toimivat käytännössä. Tavoitteena oli mitata myymälätilan tärkeimpiä fyysisen tietoturvan kipupisteitä henkilötietojen kannalta. Toimeksiantajayritys on erikoisliike, jonka vuosittainen liikevaihto on satoja miljoonia euroja. Oli perusteltu syy olettaa, että näin suuren yrityksen myymälätiloissa käsitellään ja säilytetään paljon arkojakin henkilötietoja. Näiden seikkojen seurauksena sain toimeksiantajayritykseltä tehtäväksi toteuttaa pistokoe tyyppisen tiedonkeruun, jossa yhdessä toimeksiantajan kanssa valitut oleellisemmat fyysisen tietoturvan prosessit käydään läpi ja kehitetään yrityksestä entistä turvallisempi toimintaympäristö.

Saimme haastattelun myötä informaatiota, että kaikki tietosuojaprosessit eivät toimisi tällä hetkellä niin kuin olisi tarkoitus. Haastattelun tuoma informaatio toimi tukena tiedonkeruussa. Fyysinen tietoturva on tärkeä osa sitä, että arkaluontoinen tieto pysyy haluttujen henkilöiden tiedossa. Taustatutkimuksissa on tullut ilmi, että fyysisessä suojaamisessa on puutteita, eikä kaikki prosessit toimi täysin niin kuin olisi tarve. Selvitimme pistokokeilla toimipistekohtaista tilannetta ja keskityimme tärkeäksi koettuihin

osa-alueisiin. Tämän tutkimuksen seurauksena yrityksen ei tarvitse erikseen löytää fyysisen tietoturvan liittyviä epäkohtia, vaan voi keskittää työnsä epäkohtien kehittämiseen. Tiedonkeruu toteutettiin satunnaisena tarkastuksena, jonka avulla tuodaan tietoa toimivista sekä kehittämiskelpoisista toiminnoista yrityksen käyttöön. Tilannekatsauksen tulokset auttavat yritystä saamaan tietoa mahdollisista epäkohdista ja yritys pystyy keskittämään resurssinsa haluttujen prosessien kehittämiseen.

Näkemyksenä oli, että epäkohtia kartoittamalla tuotan parannusehdotuksia erikoisliikkeen tarpeisiin vedoten sekä turvata myymälätiloissa oleva henkilötietomateriaali fyysinen tietoturvan näkökulmasta. Päätimme yhdessä toimeksiantajan kanssa toteuttaa tutkimuksen pistokokeena, jotta saamme mahdollisimman todenmukaista tietoa tietosuojaperiaatteiden toimivuudesta. Tämä tarkoittaa, että henkilöstö ei ollut tietoinen fyysiseen tietoturvallisuuteen liittyvästä tiedonkeruusta. Pistokokeen suoritettiin helmikuussa 2019 ja suoritus päiväksi päätettiin perjantai, sillä tämä päivä on yleensä vilkkain viikonpäivä kyseissä erikoisliikkeessä. Kehittämishankkeen tulosta ei voida pitää täysin tarkkana totuutena, sillä voidaan olettaa, että tietoturvaperiaatteiden toimivuus vaihtelee päivittäin. Saamme kuitenkin yleisarvion fyysisen tietoturvan toimivuudesta. Arviot tehdään aihealueittain ja niitä verrataan organisaation sääntöihin sekä uuteen tietosuojalakiin. Tilannekatsaus painottuu fyysiseen tietoturvaan ja yleisien tietosuojaperiaatteiden kehittämiseen kyseisessä yrityksessä. Tilannekatsaus auttaa yritystä saamaan tietoa mahdollisista epäkohdista ja pystyy keskittämään resurssinsa tehokkaasti niiden ympärille. Saamme tilannekuvan fyysisen tietoturvan toimivuudesta sekä ongelmakohdista.

4.2 Tiedonkeruu toimeksiantajayritykseltä

Toimeksiannon mukaisesti keskityn haastattelussa yleisesti tietosuojaan sekä tarkemmin yrityksen tilanteeseen. Tehtävänä on ymmärtää asiakasyrityksen tietosuojakäytäntöjä tehokkaammin ja miten uuteen GDPR-tietosuojalakiin on varauduttu sekä mitä prosesseja se on vaatinut. Tavoitteena on pyrkiä saamaan kuva tämän hetkisestä tietosuojan tasosta yrityksessä, sekä mitä voisi mahdollisesti kehittää. Pyrimme haastattelun avulla pohjustamaan tulevaa tutkimustamme sekä saamaan yleistä mielikuvaa, miten tietosuojaan suhtaudutaan. Haastattelimme asiakasyrityksen tietohallintojohtajaa ja pyrimme perehtymään yrityksen tietosuojakäytäntöihin. Pyrimme saamaan tietoa uuden tietosuojalain vaatimista prosesseista ja millaisia toimenpiteitä yrityksen sisällä on toteutettu.

Tietoturvan tilanteen selvittämiseksi haastattelimme yrityksen CIO:ta (Chief Information Officer) tai suomeksi tietohallintojohtajaa. Hänen työtehtäviinsä kuuluu pääasiassa tietoturvan kehittäminen ja valvominen, IT-ympäristön kehittäminen, IT-laitehankinnat, IT-budjetointi, järjestelmäkehitys, kommunikaatiojärjestelmät, uusien liiketoimintamahdollisuuksien kehittäminen yhdessä johdon kanssa. Useat näistä tehdään erilaisten sopimuskumppanien kanssa tai omalla IT-osastollamme, mikä koostuu hänen lisäksi kahdesta henkilöstä. Toimenkuvaan kuuluu myös esimiestyöskentely, GDPR-asetuksen seuraaminen, tiedotus toimipisteissä, Privacy-ANT henkilötiedon ja tietosuojan hallintajärjestelmän rakentaminen.

4.2.1 Mitä tietosuoja tarkoittaa toimeksiantajayrityksessä?

Haastateltavan mukaan arkaluonteisen henkilötietojen suojaaminen yrityksessä on erityisen tärkeää, kun toimitaan myymäläolosuhteissa. Henkilökuntaan kuuluvat käsittelevät jatkuvasti asiakkaiden henkilötietoja. Hallintohenkilöt taas käsittelevät oman henkilökunnan jopa arkaluonteisia tietoja. Nämä pitää käsitellä sovitusti ja tietoja suojaten. Alalla liikkuu paljon toimijoita ja järjestelmiä, jotka tuottavat tietoa myyjistä esimerkiksi suoritustasoja tai asiakkaiden henkilötietoja ja niin edelleen. Asiakkaiden henkilötietoja ja muita arkaluonteisia tietoja käytetään päivittäisessä toiminnassa, jonka takia ne pitää arkistoida lukitusti tai sähköiseen muotoon. Tästä prosessista on menossa projekti, miten ne saadaan sähköiseen arkistoon skannattua.

Uuteen tietosuoja-asetukseen liittyvä työ aloitettiin jo kaksi vuotta ennen GDPR:n voimaan tuloa, opiskelemalla mitä asetus tarkoittaa. Privacy-ANT järjestelmään on kirjattu henkilötietojen käyttötarkoituksia, saatavuutta ja oikeutusta. Yrityksessä on otettu käyttöön paperidokumenttien silppurit, poistettu turhat paperit pöydiltä, koulutettu koko henkilökuntaa suojaamaan tietoja ja välttymään esimerkiksi kyberhyökkäyksien ongelmilta. Jokaisen työntekijän on tullut suorittaa GDPR -videokoulutus sekä tentti. Lisäksi työasemiin on hankittu näyttösuojia, jotka estävät sivustakatselun. Myös Microsoft Office 365 -pilven kirjautumiskäytäntöjä on kovennettu sekä tietokone että mobiilipuolella. Prosesseja valvotaan ja kehitetään jatkuvasti. Uuteen tietosuoja asetukseen on varauduttu kouluttamalla esimiehiä. Tietoa tietosuojasta on jaettu kaikille tasaisin väliajoin yrityksen sisäisissä viestintäpalveluissa, sähköpostilla sekä henkilökohtaisesti. Henkilökunnan on myös pitänyt suorittaa GDPR-aiheinen verkkokurssi.

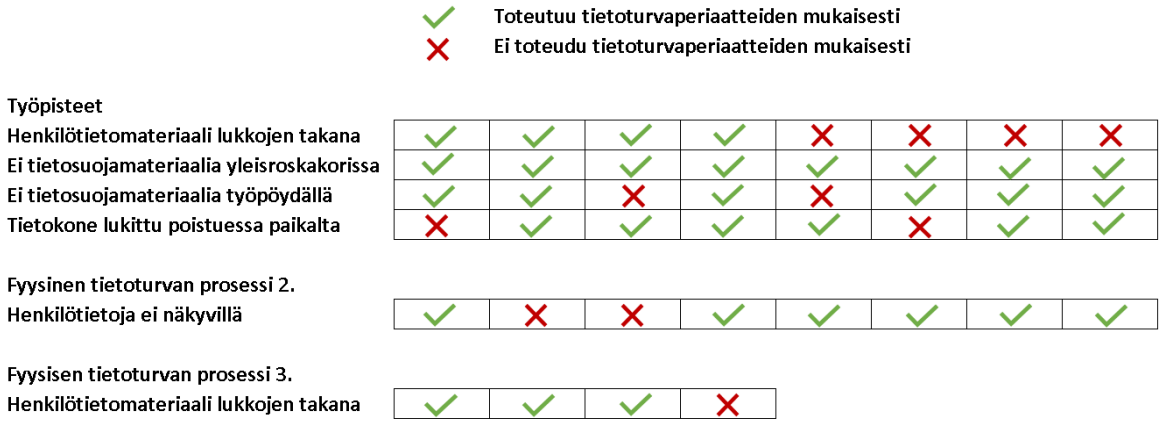
4.2.2 Millainen on tietosuojan nykytilanne sekä mitä haasteita ne asettavat?

Haastateltavan mukaan tietosuojan kannalta on paljon tehtävää muun muassa asenteissa tietosuojaa kohtaan sekä ovien ja kaappien lukitsemisessa. Järjestelmäpuolen lukituksissa joissakin sovelluksissa tarvitaan vieläkin vahvempaa salasanakäytäntöä. Tarvitaan auditointeja myymälätiloihin, toimivatko kaikki annettujen ohjeiden ja johtoryhmän käskyjen mukaisesti. Paljon on vielä myös asenteissa työmaata, alkaen ylimmästäkin johdosta. Vieläkään ei olla täysin ymmärretty miten asetusta tulee noudattaa. Privacy-ANT -tuotteessa vielä dokumentoimatonta asiakasvirran käsittelyä, jota jatkuvasti kehitetään.

4.3 Fyysinen tietoturva kategorioittain

Yrityksen kanssa yhteistyössä jaoimme tiedonkeruun kolmeen eri kategoriaan: työpisteet, fyysisen tietoturvan prosessiin 2. sekä 3. Emme kuvailleet tietoturvan prosesseja täysin todenmukaisesti ja tarkasti, jotta toimeksiantajayritystä ei voida tunnistaa. Tutkimuksessa pyrimme keskittymään yleisimpiin sekä keskeisempiin fyysisen tietoturvan kriteereihin, jotka edistävät turvallista tietosuojakäytäntöä. Kyseistä tilannekatsausta suunniteltaessa pyrittiin tiedostamaan keskeiset prosessit ja toimenpiteet, joissa käsitellään henkilötietoja tai muuta arkaluonteista materiaalia. Suurin osa myymälätiloissa sijaitsevista henkilötietopapereista sijaitsee henkilökunnan työpisteissä, joten keskittyminen työpisteisiin ja yleisesti henkilökunnan käyttäytymiseen on suuriosa myymälän tietoturvallisuudesta. Pistokokeen tyyppisessä tutkimuksessa muutamat tietosuojaperiaatteet keräsivät erityisesti huomiota ja ne aiheuttavat tietyn asteisia tietosuojariskejä. Suurimmaksi ongelmaksi toimipisteen fyysisessä tietoturvassa nousi esiin myymälätilassa sijaitsevat lukitsemattomat kaapit sekä laatikostot, joissa säilytetään suurehkoja määriä henkilötietoja sisältävää materiaalia. Lisäksi muitakin huomion arvoisia prosesseja nostettiin esiin. Taulukon mukaisesti tarkkailimme satunnaisesti kahdeksaa työntekijän työpistettä. Lisäksi tutkimme kahta muuta tietoturvaprosessia, joissa on kyse lukollisesta henkilötietojen säilytyksestä sekä henkilötietojen olemassa olosta.

Nykytilanne tiivistettynä kuviona.



Kuvio 3. Kartoituksen tulokset

Työpisteet

Työpisteet kategoriana tarkoittaa työntekijöiden työskentelypisteitä, jotka pitävät sisällään niiden säilytystilat sekä työpisteiden siisteyden tietosuojamateriaaleilta. Yleisilme työpisteillä vaikutti esimerkilliseltä, mutta joitain asioita voisi kehittää kuitenkin, yleisempänä puutteena lukitsemattomat kaapit, jotka sisältävät huomattavia määriä henkilötietomateriaaleja. Lukitsemattomat kaapit työpisteillä koettiin ongelmaksi etenkin tiettyjen alueiden kohdalla. Lisäksi osalla työntekijöillä ei välttämättä ollut tietoa missä kaappien tai laatikostojen avaimet ovat tai onko niitä ollenkaan saatavilla toimipisteessä. Lukitsemattomat kaapit tarkoittavat sitä, että niiden sisältö on aina vaarassa, ellei työpisteellä ole ketään työntekijää. Tietosuojaroskakorin käyttö on sisäistetty esimerkillisesti ja tarpeettomat arkaluontoiset paperit ovat löytäneet tiensä silppuriin tai tietosuojaroskakoriin. Normaaleista roskakoreista ei löydetty henkilötietoja sisältäviä asiakirjoja. Henkilötieto materiaaleja löytyi muutamilta työpöydiltä, vaikka työpisteellä ei ollut työntekijää eikä muutakaan valvontaa. Ulkopuolisen on helppo ottaa haltuun työpisteeltä oleva materiaali, jos ne ovat helposti saatavilla eikä valvontaa ole. Lisäksi muutamalla henkilökuntaan kuuluvalla oli jäänyt tietokone lukitsematta poistuessa työpisteeltään. Tietokoneilla usein työstetään työprosesseja sekä asiakasrekistereitä, joten niitä ei haluttaisi muiden tietoon lukitsemattoman tietokoneen seurauksena.

Tietoturvan prosessit 2 ja 3

Tarkastimme tilannekatsauksessa myös myymälän muita fyysisen tietoturvan prosesseja. Tarkastuksessa kiinnitettiin huomiota, löytyykö henkilötietoja halutuista paikoista tai säilytetäänkö henkilötietomateriaaleja lukituissa tiloissa. Suurin osa katsastetuista prosesseista toimi turvallisen tietoturvan mukaisesti. Tietyissä myymäläalueissa kuitenkin oli tietyntasoisia puutteita, joiden seurauksena tietyt prosessit ja materiaalit luovat tietoturvariskejä. Myymälätiloissa säilytettävät henkilötiedot tai muu arkaluonteinen materiaali pitäisi olla lukkojen takana.

Muuta huomautettavaa

Erityistä huomiota sai henkilökunnan postilokerot sekä lähtevän ja saapuvan postin keräysalue. Henkilökunnan postilokerot sijaitsevat asiakastilassa, jossa ei ole jatkuvasti henkilökuntaa valvomassa. Lisäksi samaan tilaan kerätään lähtevät postit päivittäin. Saapuva sekä lähtevä posti sisältävät huomattavan määrän henkilötietoja, eikä niiden pitäisi oleskella asiakastiloissa ulkopuolisten ulottuvilla. Henkilökunnalle saapuva posti sekä postin käsittely ylipäätään pitäisi sijaita hallintotiloissa, minne ulkopuolisilla ei ole vapaata pääsyä.

Vartiointi sekä muut yleisen fyysisen turvallisuuden keinot eivät nostaneet huomautettavia kokonaisuuksia tiedonkeruun aikana. Päähuomio oli kuitenkin myymälätiloissa käsiteltävissä henkilötiedoissa ja niiden säilyttämisessä sekä turvallisessa käsittelyssä. Yrityksen kanssa yhteistyössä toimiva vartiointiliike vastaa erikoisliikkeen vartioinnista liikkeen aukiolojen ulkopuolella. Ulkopuolisten yrittäessä tulla myymälätiloihin niiden ollessa suljettu, hälytysjärjestelmä hälyttää vartiointiliikkeen paikalle. Paloturvallisuus on asian mukaisin keinon huomioitu ja palo- sekä sähkölaitteet huolletaan tarvituin väliajoin.

4.4 Kehitysehdotukset

Tiedonkeruun eli fyysisen tietoturvan tilannekatsauksen avulla saatiin arvokkaita huomioita yrityksen toiminnasta. Yleisellä tasolla fyysinen tietoturva on toiminut tähän päivään asti moitteettomasti eikä varsinaisia tietovuotoja tai varkauksia ole tapahtunut heikon tietoturvan seurauksena. Tietoturvaa voi kuitenkin aina kehittää eteenpäin ja se palvelee jokaista myymälätiloissa liikkuvaa. Fyysiseen tietoturvaan keskittyvä pistokoe paljasti muutamia huomiota kiinnittäviä epäkohtia, joihin pitäisi keskittyä yleisen turvallisuuden kehittämiseksi. Kehittämällä fyysisen tietoturvan toimia, luodaan entistä turvallisempi toimintaympäristö sekä minimoidaan mahdollisiin tietovuotoihin liittyvät riskit. On tärkeä tunnistaa kaikki prosessit, joissa ollaan henkilötietojen kanssa tekemisissä, ja käydä ne läpi turvallisuuden ja riskien kannalta sekä miten ne oikeaoppisesti tulisi hoitaa.

4.4.1 Henkilökunnan kouluttaminen

Tilannekatsauksen myötä on tullut ilmi, että henkilökunnan asenteet ovat osittain välinpitämättömiä tietoturvaa kohtaan, eivätkä he välttämättä halua kunnioittaa kaikkia turvallista tietoturvaa vaalivia prosesseja. Näistä esimerkkeinä ovat muun muassa Kartoituksen tulokset -taulukon punaiset rastit. Yritys voisi luoda ja tuoda enemmän henkilökunnalle selväksi myymälän tietoturvan kriteerejä, joita valvottaisiin yhteisillä tarkastuskäynneillä tai esimiehen voimin. Fyysinen tietoturva voitaisiin jakaa eri kategorioihin, joten toimintaohjeet olisivat selkeitä ja niihin voisi helposti samaistua. Jos toimipisteiden esimiehet valvoisivat fyysisen tietoturvallisuuden toteutumista, saataisiin todenmukaisempaa ja jatkuvaa tietoa hyvistä ja huonoista puolista sekä ongelmakohtiin olisi mahdollista puuttua nopeammalla aikataululla.

4.4.2 Kaappien sekä laatikostojen lukitukset

Suurimpana kehityksen kohteena nousi esiin lukitsemattomat kaapit tai laatikostot työpisteillä. Kaikki asiakastiloissa olevat henkilötietopaperit tai muu arkaluonteinen materiaali tulee olla lukittuna kaapeissa tai laatikoissa, ellei niitä valvota. Työntekijän poistuessa työpisteeltä, pitäisi työpisteen olla siisti arkaluontoisista materiaaleista. Lisäksi työpisteellä oleva tietokone pitäisi lukita, jos työpisteellä ei ole työntekijää. Työpisteissä sijaitsevat kaapit ja laatikostot sisältävät ensisijaisesti lukitusjärjestelmän,

mutta asenteet lukkojen takana säilyttämistä kohtaan ovat epävakaat. Tulisi tarkistaa, että kaikki lukitusjärjestelmät toimivat ja oman työpisteen avaimet löytyvät jokaiselta.

4.4.3 Postiliikenne

Kolmantena kehityskohteena on toimipisteen postiliikenteeseen liittyvät käytännöt ja niiden sijainti. Kehityshankkeen aikana yrityksestä lähtevät kirjekuoret sijaitsivat muoviastiassa asiakastilassa, mikä saattoi olla vartioimatta tiettyinä ajankohtina. Lisäksi henkilökunnan postilokerot sijaitsivat myös asiakastiloissa, jonne kirjekuoria saapuu päivittäin. Yrityksessä postiliikenne sisältää usein arkaluontoista materiaalia, joten näitä materiaaleja tulisi käsitellä suurella tarkkaavaisuudella ja riskit minimoiden. Lähtevä sekä saapuva postiliikenne voitaisiin keskittää muun muassa hallintotiloihin turvallisuuden takaamiseksi, sillä nämä tilat ovat lukittu henkilökuntaan kuulumattomilta.

4.5 Yhteenveto

Tietosuoja ja tietoturva ovat aiheina nousseet pinnalle uuden tietosuoja-asetuksen myötä. Asetus asettaa tiettyjä velvollisuuksia rekisterin pitäjille sekä oikeuksia rekisteröidyille. Tavoitteena on luoda entistä läpinäkyvämpää ja turvallisempaa tietojen turvaamista. Fyysinen tietoturva on erittäin tärkeää niin yrityksen kuin asiakkaan kannalta, sillä arkojen tietojen pitää pysyä haluttujen osapuolien hallussa. Avasin tässä opinnäytetyössä fyysisen tietoturvan menetelmiä autoliikkeessä ja mitä turvallinen toiminta edellyttää yleisesti kulkuneuvoalla. Tämän opinnäytetyön avulla kartoitin fyysisen tietoturvan reunaehtoja sekä miten toimeksiantajayrityksen fyysisen tietoturvan menetelmät toimivat käytännön tasolla.

Fyysiseen tietoturvaan pitäisi kiinnittää huomiota kaikissa yrityksissä ja minimoida mahdolliset riskit tietovuodolle tai tietojen tuhoamiselle. Myymälätiloihin kohdistuvassa fyysisen tietoturvan katsauksessa yksi kätevistä näkökulmista on asettua asiakkaan asemaan ja analysoida eri prosessien toimivuutta. Kaikissa yrityksissä ei säilytetä myymälätiloissa suuria määriä henkilötietoja tai ole suurta asiakasvirtaa myymälässä, mutta tietoturvan fyysinen ja tekninen puoli pitäisi silti huomioida sekä nostaa esille tärkeimpiä prosesseja ja kehittää niitä kriittisellä näkökulmalla. Toisissa yrityksissä eri osa-alueet saattavat olla tärkeämmässä roolissa kuin muut. Tärkeää on tunnistaa oman yrityksen pääprosessit, joissa käsitellään arkaluontoista materiaalia ja käydä läpi niiden toimenpiteiden turvallisuus ja eheys. Jo pienillä muutoksilla ja minimaalisilla

kustannuksilla voidaan saavuttaa huomattavaa tietoturvallista hyötyä. Keinoja voivat olla muun muassa prosessien päivittäminen tai tietomateriaalien uudelleen sijoittaminen. Tietosuoja ja tietoturva eivät ole ensisijaisesti lakien noudattamista vaan turvallisuuden vaalimista.

Loin tiedonkeruun tuloksena muutamia kehitysehdotuksia yrityksen käyttöön. Toteutettua tiedonkeruuta ei voida pitää laajalti yleistettävissä olevana, sillä tulokset ovat vain yhden pistokokeen tuloksia. Pistokoe suoritettiin viikon kiireisimpänä päivänä ja sen avulla pyrittiin kuvaamaan nykytilannetta mahdollisimman todenmukaisesti. Tulokset antavat kuitenkin näkökulmaa yleisesti ja kertovat yrityksen käytännöistä. Tilannekartoituksessa esiin tulleiden tuloksien myötä toimeksiantajayritys aikoo keskittyä entistä tehokkaammin fyysisen tietoturvan kehittämiseen. Tässä opinnäytetyössä esille tulleet fyysisen tietoturvan keinot ovat myös tärkeitä monien muiden alojen yrityksissä, joissa käsitellään arkojakin henkilötietoja. Ajantasaiset fyysisen tietoturvan prosessit luovat turvallisuutta sekä yritykselle että asiakkaille.

Lähteet

Autoalan keskusliitto Ry (AKL). 2018. Tietosuojaopas 2018. Viitattu 10.11.2018.

Autoliikkeen tietoturvamateriaali. 2018. Viitattu 20.11.2018.

Finlex. Viitattu 16.01.2019. Henkilötietolaki 523/1999 (kumottu) Saatavilla:https://www.finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523

Hanninen , M.; Laine E.; Rantala K; Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely. EU-tietosuoja-asetuksen vaatimukset. Hansaprint Oy.

Korpisaari P.; Pitkänen O. & Warme-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Alma Talent Oy.

Nykänen P. 2014. Tietoturva – tietosuoja tietojärjestelmien suunnittelussa. Tampereen yliopisto. Viitattu 12.04.2019. Saatavilla:http://www.uta.fi/sis/tie/tjsum/index/TJSUM_Luento6_2014_PirkkoNyk%C3%A4nen.pdf

Tietosuoja.fi. Viitattu 4.1.2019.

Saatavilla:https://tietosuoja.fi/tietosuoja https://tietosuoja.fi/kasittelyperusteet

Tietosuojamalli. Viitattu 16.1.2019.

Saatavilla:https://fakta.tietosuojamalli.fi/gdpr-asetus/83-hallinnollisten-sakkojen-maaraamisen-yleiset-edellytykset

Tietosuojalainsäädäntö. Viitattu 10.11.2019.

Saatavilla:https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679

Toimeksiantajayrityksen GDPR-koulutusmateriaali. Viitattu 10.11.2019

Turun sanomat. Suomessa ryhdytään tekemään GDPR-tarkastuksia, kun Ruotsissa annetaan jo ensimmäisiä tuomioita. Viitattu 14.4.2019. Saatavilla:https://www.ts.fi/uutiset/kotimaa/4117122/Suomessa+ryhdytaan+tekemaan+GDPRtarkastuksia+kun+Ruotsissa+annetaan+jo+ensimmaisia+tuomioita

Vedenoja J. 2007. Yrityksen fyysinen tietoturva. Lahden ammattikorkeakoulu. Viitattu 7.5.2019.

Saatavilla:https://www.theseus.fi/bitstream/handle/10024/11928/2007-12-03-18.pdf;jsessionid=85556A0D9773273B3BFA2F2FA733B396?sequence=1

Viestintävirasto. Viitattu 12.2.2019.

Saatavilla:https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/12/ttn201412031257.html

Yrittäjät.fi. KRP varoittaa Office 365 -tietomurroista: "Pahinta on, ettei huijausta tunnista". Viitattu 31.5.2019.

Saatavilla:https://www.yrittajat.fi/uutiset/605395-poliisi-varoittaa-office-365-tietomurroista-pahinta-ettei-huijausta-tunnista