Markus Valtonen

EU:N TIETOSUOJA-ASETUKSEN MUUTOKSET JA VAIKUTUKSET CASE-YRITYKSESSÄ

Kansainvälisen kaupan koulutusohjelma

2019

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

EU:n tietosuoja-asetuksen muutokset ja vaikutukset Case-yrityksessä

Valtonen, Markus
Satakunnan ammattikorkeakoulu
Kansainvälisen kaupan koulutusohjelma
Maaliskuu 2019
Ohjaaja:
Sivumäärä: 28
Liitteitä: 0

Asiasanat: tietosuoja, henkilötieto, tietoturva

Opinnäytetyön aiheena oli tutkia 2018 keväällä tulleen EU:n tietosuoja-asetuksen muutoksia, ja vaikutuksia Case-yrityksen toimintaan. Tutkimus toteutettiin toimeksiantona Case-yritykselle, heidän pyynnöstään eli todelliseen tarpeeseen.

Tutkimuksen tavoitteena oli selvittää, mitä yrityksen tulee ottaa huomioon tietosuoja-asetuksen tultua voimaan, missä kaikissa järjestelmissä Case-yritys säilyttää henkilötietoa, kenellä siihen on pääsy ja onko säilytys asianmukaista. Tämän seurauksena yritykselle tehtiin ohjeistus koskien toimenpiteitä parantamaan tietosuoja-asetuksen mukaista henkilötietojen säilytystä.

Opinnäytetyön teoreettisessa osassa selvitettiin kirjallisuuteen ja muihin lähteisiin nojaten, tietosuoja-asetuksen pääkohdat, sekä tärkeimmät muutokset. Lähteinä käytettiin pääasiassa internetlähteitä ja useampaa kirjaa. Kirjoja oli aiheesta vielä sen ajankohtaisuuden vuoksi hyvin vähän, joten internetlähteisiin nojautuminen oli välttämätöntä.

Empiirisessä osassa käytiin ensin Case-yrityksen järjestelmät läpi, jotta saatiin selville missä ja minkälaista henkilötietoa siellä säilytetään. Tämän jälkeen tehtiin kehityskehotuksia toimintatapoihin, jotta asetuksen mukaan oltaisiin tarvittavalla tasolla. Yrityksen vastuulle jää kehotuksien tekeminen henkilöstön kesken.

Opinnäytetyöstä jää yritykselle ensisijaisesti opas toimintatapojen kehittämiseen. Kehotuksien käyttöönotto jää yrityksen henkilöstön vastuulle. Toiseksi yritys voi käyttää tutkimuksen teoriaa tarkistaessaan mahdollisia pulmatilanteita, koskien tietosuojaa.

OPINNÄYTETYÖN NIMI ENGLANNIKSI

Valtonen, Markus
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in International Business
March 2019
Supervisor:
Number of pages: 28
Appendices: 0

Keywords: data protection, personal data, information security

---

The purpose of this thesis was to study EU's general data protection policy of 2018 spring, and the changes and impacts to the Case-company. Thesis was carried out as an assignment for the Case-company from their request.

The objective of the thesis was to examine, what the company should consider when the regulation becomes valid, where the company preserves personal data, who has the access to it and is the preservation of personal data appropriate. As a result, instructions were made for the company to improve the personal data preservation.

In the theoretical part of the thesis, examination was made based on the references about the main point of the new general data protection policy and the most important changes coming to force. There were few book sources about the policy because it was so recent, so internet references were essential.

In the empirical part of the thesis the company's systems were reviewed for personal data first to find out where and what personal data was stored. After this improvement propositions were made, so that the procedures for the company were up to date. The improvement propositions are left for the company to implement.

First and foremost, thesis leaves the company a guide for improving procedures inside the company. Secondly, the company may use the theoretical part as a note for possible troubling situations regarding the data protection policy.

SISÄLLYS

1 JOHDANTO 6
2 OPINNÄYTETYÖN TAVOITTEET JA KÄSITTEELLINEN VIITEKEHYS 6
2.1 Tutkimuksen tavoite 6
2.2 Teoreettinen viitekehys 7
3 EU:N TIETOSUOJA-ASETUS JA MUUTOKSET 8
3.1 Tietosuoja-asetuksen voimaantulo 8
3.2 Tietosuoja-asetuksen tarkoitus 9
4 REKISTERÖIDYN OIKEUDET 10
4.1 Henkilötiedon määritelmä 10
4.2 Oikeus saada pääsy henkilötietoihin 10
4.3 Oikeus henkilötietojen käsittelyn rajoittamiseen ja tietojen oikaisuun 11
4.4 Oikeus siirtää tiedot järjestelmästä toiseen ja tietojen poistaminen 11
5 HENKILÖTIEDON KÄSITTELIJÄN JA REKISTERINPITÄJÄN VELVOLLISUUDET 12
5.1 Roolien määritelmät 12
5.2 Lainmukaisuus ja läpinäkyvyys 13
5.3 Tietojen minimointi, täsmällisyys ja käyttötarkoitussidonnaisuus 13
5.4 Osoitusvelvollisuus 14
6 DOKUMENTOINTI JA MUUT TOIMENPITEET 14
6.1 Tietosuojaseloste 14
6.2 Tietotilinpäätös ja tietosuojavastaava 15
7 TIETOTURVA 16
7.1 Tietojen salaaminen ja luottamuksellisuus 16
7.2 Tietoturvaloukkaus 16
8 HENKILÖTIETOJEN SÄILYTYSAJAT 17
8.1 Työaikalaki ja vuosilomalaki 17
8.2 Henkilötietolaki ja työsopimuslaki 18
8.3 Yhdenvertaisuuslaki 18
9 OPINNÄYTETYÖN TOTEUTTAMINEN 18
9.1 Lähtökohdat 18
9.2 Tutkimustyyppi 19
9.3 Reliabiliteetti ja validiteetti 19
10 LÄHTÖTILANNE 20

11 POHDINTA 20
11.1 Henkilötieto järjestelmissä 21
11.2 Tietoturva 24
12 YHTEENVETO JA SUOSITELLUT TOIMENPITEET 25
12.1 Tietoturvaharjoitus 25
12.2 Henkilötiedon tarkasteluoikeudet ja minimointi 26
12.3 Henkilötiedon säilytysajat 26
12.4 Henkilötietojen luovutus 27
13 LOPPUSANAT 27
LÄHTEET 28
LIITTEET

1 JOHDANTO

Tämän opinnäytetyön aiheena on EU:n tietosuoja-asetuksen muutokset ja vaikutukset Case-yrityksessä. Sain Case-yritykseltä toimeksiannon tähän aiheeseen, koska se on yritykselle tällä hetkellä ajankohtainen, ja heille olisi siitä suuri hyöty valmistautuessaan ja kehittäessään toimintamallejaan tietosuoja-asetusta varten. Opinnäytetyöni on rajattu keskittymään vain Case-yrityksen eri tietokantoihin, enkä käsittele muiden linkittyneiden yritysten tai asiakkaiden tietokantoja opinnäytetyössäni.

Aloitan opinnäytetyöni esittelemällä case-yrityksen lyhyesti, tarkastelemalla tietosuoja-asetukseen tulevia muutoksia, joita on paljon. Kun olen kartoittanut ja avannut erilaiset muutokset ja lisäykset läpi, siirryn opinnäytetyön empiiriseen osuuteen, jossa keskityn teoriatiedon pohjalta yrityksen tietokantoihin. Listaan ensin kaikki yrityksen tietokannat, ja alan tietokantojen tietojen pohjalta selvittämään, onko henkilötietojen säilytys asianmukaista, ja pohdin pitääkö asiaan tehdä muutoksia. Empiirisessä osiossa myös ennustan mahdollisia tietosuoja-asetuksen vaikutuksia, joita ei ole vielä mahdollista tutkia.

Case-yrityksen pyynnöstä teen opinnäytetyössäni yritystä ei mainita sen oikealla nimellä. Case-yritys on palvelualan yritys, joka myy eri alojen asiakkailleen palveluita. Yrityksellä on Suomessa 4 toimipistettä, joiden kautta on töissä yli 300 työntekijää. Yrityksen viime vuoden liikevaihto oli n. 15 miljoonaa euroa.

2 OPINNÄYTETYÖN TAVOITTEET JA KÄSITTEELLINEN VIITEKEHYS

2.1 Tutkimuksen tavoite

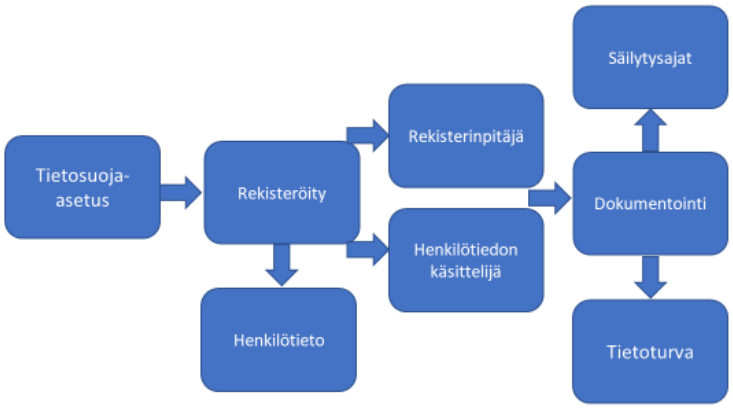
Opinnäytetyön tavoitteena on käydä läpi EU:n tietosuoja-asetuksen muutokset, jonka perusteella case-yritykselle kootaan suunnitelma/ohjeistus suositelluista toimenpiteistä. Opinnäytetyön teoriaosuudessa käydään läpi muuttuva uuden tietosuoja-

asetuksen lainsäädäntö. Empiriaosuudessa käyn läpi yrityksen järjestelmät, jotka sisältävät henkilötietoa. Teoriaosuuden pohjalta laadin tarvittavat toimenpiteet ja suositukset case-yrityksen henkilöstölle, josta tulee myös apuväline toimintatapojen kehittämiseen.

Tutkimuksessa vastataan seuraaviin tutkimuskysymyksiin:

- Mitä toimenpiteitä tarvitaan ja mitä tulee ottaa huomioon, kun uusi tietosuoja-asetus tulee voimaan?
- Missä kaikissa järjestelmissä yritys säilyttää henkilötietoa, missä sitä säilytetään ja kuinka pitkään?
- Ketkä henkilöstön jäsenet saavat käsitellä case-yrityksen henkilötietoja?

2.2 Teoreettinen viitekehys



Kuvio 1 Teoreettinen viitekehys (Valtonen 2018)

Kuvion 1 teoreettinen viitekehys havainnollistaa, kuinka henkilötieto kulkee case-yrityksessä. Viitekehys sisältää henkilöiden ja organisaatioiden roolit, sekä henkilötiedon käsittelyn ohjeistuksen säilytysajoista, dokumentoinnista ja tietoturvasta.

3 EU:N TIETOSUOJA-ASETUS JA MUUTOKSET

3.1 Tietosuoja-asetuksen voimaantulo

Euroopan unionin alueella sovellettavaksi tuleva uusi tietosuoja-asetus eli kansainvälisesti GDPR (General Data Protection Regulation) tulee voimaan 25. päivä toukokuuta 2018. Asetus tulee automaattisesti lainvoimaiseksi kaikissa EU-maissa sellaisenaan. (Hanninen ym. 2018, 13.)

Tietosuoja-asetuksen voimaantulo päätettiin Euroopan parlamentissa 27. päivä huhtikuuta 2016. Uuden tietosuoja-asetuksen (2016/679,) voimaantulolle annettiin kahden vuoden siirtymäaika, jolloin yrityksillä on mahdollisuus valmistautua ja pyrkiä toimimaan lainmukaisesti 25. päivä toukokuuta 2018 alkaen. (Euroopan parlamentin ja neuvoston asetus 2016/679) Asetus korvaa Euroopan Unionin maiden paikallista lainsäädäntöä. Suomessa asetus tulee osittain korvaamaan 22.4.1999 säädettyä henkilötietolakia. (Finlex, 2016)

Kuva 1 Tietosuoja-asetuksen lainsäädännön tuleva rakenne (Elinkeinoelämän keskusliitto 2018)

3.2 Tietosuoja-asetuksen tarkoitus

Asetuksen tärkeimpänä tavoitteena on tullut yhdenmukaistaa EU:n laajuiset tietosuojalait, jotta EU:n alueella olevilla henkilöillä ja yrityksillä on samat velvollisuudet ja oikeudet. (Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela 2018, 13.)

Tavoitteena on myös parantaa rekisteröityjen henkilöiden oikeuksia. Yritysten tulee parantaa henkilötietojen suojaa järjestelmissään. Asetuksen tavoitteena on myös edistää digitaalisten sisämarkkinoiden kehittymistä. (Tietosuojavaltuutetun toimisto 2015.)

Päivitetyssä asetuksessa henkilötietojen käsittely Tietosuoja-asetuksen voimaantulo vaikuttaa kaikkien yritysten, sekä pienten ja suurten, toimintaan. Yrityksillä on vastuu toimia asetuksen mukaisesti, sanktioiden uhalla. Asetuksen rikkomisesta koituvat sanktiot ovat tuntuvia. Enimmäissakot tietosuojalain rikkomisesta ovat 4% yrityksen maailmanlaajuisesta kokonaisliikevaihdosta, tai 20 miljoonaa euroa. (Tietosuojaseminaari, Dittmar & Indrenius 2018)

Kuva 2 EU:n tietosuoja-asetuksen sisältö ja tavoite (Opi tietosuojaa 2018)

4 REKISTERÖIDYN OIKEUDET

4.1 Henkilötiedon määritelmä

Uudessa EU:n tietosuoja-asetuksessa, suurimmat muutokset näkyvät rekisteröityjen lisääntyneinä oikeuksina. Seuraavassa käydään läpi rekisteröidyn oikeuksia, jotka asetuksen mukaan ovat lainvoimaisia.

“Asetuksessa henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (ihmiseen) liittyviä tietoja.” (Hanninen ym. 2018, 19-20.)

Henkilötiedoksi voidaan siis määritellä lähes mitä vain tietoa, josta henkilö on tunnistettavissa. Henkilötiedot voidaan luokitella kolmeen ryhmään: Henkilötietoihin, ”herkkiin henkilötietoihin” ja erityisiin henkilötietoihin. Henkilötietoihin voidaan lukea ns. helposti saatavat henkilötiedot, kuten yhteystiedot, valokuvat ja muut julkiset tiedot. ”Herkkiin henkilötietoihin” voidaan lukea esimerkiksi palkkatiedot ja kehityskeskustelumuistiot. Edellä olevat tiedot eivät ole yleisesti ottaen julkisesti saatavilla. Erityiset henkilötietoryhmät, tai ns. ”arkaluonteiset henkilötiedot”, sisältävät tietoa henkilöstä, jota ei myöskään ole julkisesti saatavilla, ja tieto on yleisesti ottaen salattua. Arkaluonteisena henkilötietona voidaan pitää esimerkiksi henkilön terveydentilaa koskevat tiedot, etninen tausta, sekä erilaisiin ammattiliittoihin kuuluminen. Tällaista tietoa saavat käsitellä vain määrätyt henkilöt yrityksessä. (Tietosuojaluento, Dittmar & Indrenius, 2018)

4.2 Oikeus saada pääsy henkilötietoihin

Rekisteröidyllä henkilöllä on oikeus saada tieto onko hänestä tietoa, sekä millaista tietoa, yrityksen henkilötietorekistereissä. Tilanteessa, jossa rekisteröidystä on henkilötietoa jossakin henkilötietorekisterissä, on rekisteröidyllä oikeus saada häntä koskevat tiedot. Rekisteröity voi myös vaatia tietojen suunnitellusta säilytysajasta sekö tieto onko rekisteröidyn henkilötietoa annettu kolmansille osapuolille. (Hanninen ym. 2018, 59.)

Henkilön oikeuksiin kuuluu myös tieto hänen henkilötietonsa käsittelyn tarkoituksesta, eli siitä mihin henkilötietoa käytetään ja miksi. Jos tietojen käsittely ei ole asianmukaista, rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle. (Hanninen ym. 2018, 59.)

4.3 Oikeus henkilötietojen käsittelyn rajoittamiseen ja tietojen oikaisuun

Rekisteröidyllä henkilöllä on joissakin tapauksissa oikeus henkilötietojensa rajoittamiseen. Henkilön huomatessa, että hänestä olevat henkilötiedot ovat virheelliset, vanhentuneet tai muuten paikkansapitämättömät, voi henkilö vatia henkilötietojensa käsittelyn rajoittamista. Vastaavassa tilanteessa yrityksen tulee rajoittaa henkilötietojen käsittelyä sen ajaksi, että henkilötieto on varmistettu oikeelliseksi tai päivitetty vastaamaan todellista tilannetta.

Rekisteröity voi myös vaatia henkilötietojensa käsittelyn rajoittamista, jos yrityksellä ei ole perusteltua säilyttää kyseistä henkilötietoa oikeudellisista syistä, tai tietoa ei ole muuten perusteltua säilyttää tai käsitellä. (Hanninen ym. 2018, 61, 63-64.)

4.4 Oikeus siirtää tiedot järjestelmästä toiseen ja tietojen poistaminen

Rekisteröidyllä henkilöllä on oikeus saada henkilötietonsa siirrettäväksi yrityksen tietojärjestelmästä kolmannelle osapuolelle seuraavissa tapauksissa. Rekisteröidyn henkilötietojen käsittely perustuu hänen omaan suostumukseensa tai tilanteessa, jossa henkilötietojen käsittely on automaattista. (Hanninen ym. 2018, 61, 64-65.)

Henkilötietojen poistaminen yrityksen tietokannoista, eli ”oikeus tulla unohdetuksi” on rekisteröidyn vahvin oikeus, ja henkilö voi vaatia tätä joissakin tilanteissa. Yritys ei tarvitse henkilötietoa enää tarkoitukseen, johon se on kerätty. Jos yritys ei pysty osoittamaan oikeudellisia perusteita tiedon säilyttämiseksi, tulee tiedot poistaa. (Hanninen ym. 2018, 61.)

Rekisteröidyn oikeuksiin kuuluu oikeus vaatia tietojen poistamista tilanteessa, jossa henkilötietojen säilyttäminen ja käyttö perustuu rekisteröidyn suostumukseen. Henkilö voi päättää evätä suostumuksensa jälkeenpäin tiedoistaan, jolloin tiedot tulee hänen pyynnöstään poistaa, jos ei henkilötiedon käsittelylle löydy laillisia perusteita. (Hanninen ym. 2018, 62.)

Lisäksi tilanne, jossa rekisteröity voi todistaa, että henkilön henkilötietoja on käytetty lainvastaisesti, on perusteltu tilanne poistaa tiedot yrityksen järjestelmistä. (Hanninen ym. 2018, 62.)

5 HENKILÖTIEDON KÄSITTELIJÄN JA REKISTERINPITÄJÄN VELVOLLISUUDET

5.1 Roolien määritelmät

Uusi tietosuoja-asetus on lisännyt henkilötiedon käsittelijän ja rekisterinpitäjän velvoitteita. Ensiksi on tärkeää määritellä, kuinka roolit jakautuvat, ja missä roolissa yritys tai luonnollinen henkilö milloinkin toimii.

”Rekisterinpitäjä on luonnollinen henkilö eli ihminen, yritys, viranomainen tai vastaava taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.” (Hanninen 2018, 24) Henkilötietojen käsittelijänä toimii yritys, joka käsittelee yrityksen tai muun organisaation henkilötietoja yrityksen tai organisaation saamalla suostumuksella. Tällainen yritys voi olla esimerkiksi tilitoimisto, johon rekisterinpitäjän yritys toimittaa palkanmaksua varten työntekijöiden henkilötietoja palkanmaksua varten. (Hanninen ym. 2018, 24-25)

5.2 Lainmukaisuus ja läpinäkyvyys

Luonnollisten henkilöiden henkilötietojen käsittelyn tulee yrityksissä tai organisaatioissa olla läpinäkyvää. Henkilöille, joiden henkilötietoja käsitellään, tulisi olla vaivattomasti saatavilla tieto missä, miten ja minkä vuoksi henkilötietoja käsitellään tai tullaan tulevaisuudessa käsittelemään. Läpinäkyvyyden toteutumiseksi rekisterinpitäjän täytyy arvioida, onko perusteltua laatia tietosuojaseloste, jossa käydään läpi henkilötietojen käsittelyn periaatteet. (EU) 2016/679, 39/40. artikla.)

Jotta henkilötietojen lainmukainen käsittely käy toteen, tulee rekisteröidylle tiedottaa henkilötietojen käsittelystä ennen käsittelyä, ja saada rekisteröidyltä kirjallinen suostumus. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 39/40. artikla.)

Rekisterinpitäjällä voi olla jossain tapauksissa myös lainmukainen velvollisuus käsitellä henkilötietoja, jos tarkoitus lakisääteinen. Lakisääteinen henkilötietojen käsittelyn velvollisuus on esimerkiksi voimassa tilanteissa, jossa yrityksen tulee toimittaa jotakin laissa määriteltyä tietoa viranomaiselle. Tällainen henkilötieto voi olla esimerkiksi palkkatietoja veroviranomaiselle verotusta varten. (Hanninen ym. 2018, 31)

5.3 Tietojen minimointi, täsmällisyys ja käyttötarkoitussidonnaisuus

Rekisterinpitäjän tulisi kerätä rekisteröidyistä vain sen verran henkilötietoa, joka on tarpeellista ja perusteltua. Esimerkiksi yritykselle välttämätöntä tietoa on työntekijän tilinumero, jotta palkanmaksu voidaan suorittaa. Rekisterinpitäjän tulee myös toteuttaa tarvittavat toimenpiteet, jotta henkilötiedot ovat täsmällisiä ja ajan tasalla. Virheellisen henkilötiedon oikaisu ja poistaminen kuuluvat rekisteröidyn oikeuksiin, joten yrityksen tulee pyrkiä pitämään henkilötiedot oikeellisina. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 39. artikla.)

Ennen henkilötiedon käsittelyä, rekisteröidylle informoidaan hänen henkilötietojensa käsittelyn tarkoituksesta, johon vaaditaan rekisteröidyn suostumus. Läpinäkyvän henkilötiedon käsittelyn seurauksena rekisteröity tietää mihin tarkoitukseen henkilötietoa

käytetään. Henkilötietoa tulee käyttää aiemmin määriteltyyn tarkoitukseen. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 39. artikla.)

5.4 Osoitusvelvollisuus

Osoitusvelvollisuus on uusi tietosuoja-asetuksessa määritelty velvoite rekisterinpitäjälle. Rekisterinpitäjän tulee voida osoittaa, että henkilötietoja käsitellään tietosuoja-asetuksessa määritellyin perustein. ”Osoitusvelvollisuus edellyttää rekisterinpitäjältä muun muassa henkilötietojen käsittelyn aiempaa tarkempaa suunnittelua, dokumentointia sekä sisäistä ohjeistusta ja tarvittaessa henkilötietoja käsittelevän henkilöstön koulutusta.” (Elinkeinoelämän keskusliiton www.sivut 2018.)

Pelkkä lainsäännöllinen velvoite henkilötietojen käsittelyyn ei tietosuoja-asetuksen voimaantulon jälkeen enää siis riitä. Rekisterinpitäjän, yrityksen tai organisaation, tulee jatkuvasti pyrkiä kehittymään ja parantamaan käytäntöjään henkilötietojen käsittelyssä, ja dokumentoida tiedot todisteeksi velvoitteen täyttämiseksi. (Andreasson ym. 2017, 23)

6 DOKUMENTOINTI JA MUUT TOIMENPITEET

6.1 Tietosuojaseloste

Osoitusvelvollisuuden mukaisesti, rekisterinpitäjän tulee osoittaa ja dokumentoida pyrkimystä toimia tietosuoja-asetuksen mukaisesti. Yrityksillä dokumentointiin on erilaisia tapoja, joita käydään läpi tässä kappaleessa.

Läpinäkyvyyden lisäämiseksi ja organisaation henkilötietojen käsittelyn tiedottamiseksi, voidaan laatia tietosuojaseloste. Tietosuojaselosteella pystytään

informoimaan rekisteröidyillä heidän oikeuksistaan, sekä organisaation velvoitteista koskien rekisteröidyn henkilötietoja. (Hanninen ym. 2018, 75-76)

6.2 Tietotilinpäätös ja tietosuojavastaava

Tietotilinpäätös on vapaaehtoinen tapa, jolla organisaatio voi dokumentoida tietosuoja-asetukseen reagoimista. Tietotilinpäätöksen tavoitteena on luoda arvio organisaation tietosuojan nykytilanteesta. Tietotilinpäätöksessä voidaan käydä läpi henkilötietojärjestelmiä, tietojen laatua, tietojen suojaamista, valvontaa ja muita menettelytapoja. Tietotilinpäätöksen laatimisella voidaan osoittaa, että rekisterinpitäjä pyrkii täyttämään ja kehittämään tietosuoja-asetuksessa asetetut velvoitteet. (Tietosuojauutiset, 2016.)

Organisaatiosta riippuen, voi olla perusteltua nimittää organisaatioon tietosuojavastaava. Tietosuojavastaava on perusteltua nimittää, jos organisaation ydintehtävät koostuvat laajamittaisesta henkilötietojen käsittelystä. Tietosuojavastaava voidaan kuitenkin nimittää ilman velvoitteitakin. Tietosuojavastaavan tehtäviin kuuluu henkilötietojen asianmukaisen käsittelyn ja muiden tietosuoja-asetuksen velvoitteiden valvonta. Tietosuojavastaavan roolissa toimivan henkilön tulee toimia myös rekisterinpitäjän ja henkilötietojen käsittelijöiden apuna mahdollisissa pulmatilanteissa. Dokumentoinnin laatiminen, tietoturvariskien huomioiminen, sekä yhteistyö valvontaviranomaisten kanssa kuuluvat myös tietosuojavastaavan mahdollisiin tehtäviin. (Andreasson ym. 2017, 64)

7 TIETOTURVA

7.1 Tietojen salaaminen ja luottamuksellisuus

Rekisterinpitäjän tulee toimenpiteillään varmistaa, että henkilötietojen käsittely on turvallista. Yrityksen tulee erilaisella dokumentoinnillaan osoittaa, että henkilötietojen turvalliseen käsittelyyn on pyritty.

Rekisteröidyn henkilötiedot voidaan henkilötietojärjestelmissä salata ja tehdä tunnistamattomaksi. Tapauksissa, joissa henkilötietoja lähetetään kolmansille osapuolille, voi olla perusteltua joko salata tieto tai tehdä henkilötiedosta tunnistamatonta eli pseudonymisoida tieto, josta henkilöä ei voida tunnistaa. Varsinkin arkaluonteista henkilötietoa käsiteltäessä tulee arvioida, ovatko ylläolevat piteet tarpeellisia. (Hanninen ym. 2018, 106-107)

Henkilötietojen turvallisuuden varmistamiseksi, yrityksen tulee rajoittaa henkilötietoihin pääsyä henkilöiltä, joille tiedot eivät ole oikeutettuja: tämä koskee myös omaa henkilöstöä. Henkilötietojen luottamuksellisuuden varmistamiseksi organisaatiolla on useampia keinoja, kuten tietojen salaus, vahvat salasanat, sekä turvallinen tietojen hävitys. Henkilötietojen vuotaminen ulkopuolisille on vakava tietoturvarikkomus, josta voidaan myös tilanteen mukaan jakaa organisaatiolle sanktiota. (Hanninen ym. 2018, 107)

7.2 Tietoturvaloukkaus

”Tietoturvaloukkauksella tarkoitetaan loukkausta, joka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy henkilötietoihin.” (Hanninen ym. 2018, 108)

Tilanteessa, jossa on tapahtunut tietoturvaloukkaus, on rekisterinpitäjällä velvoite tehdä ilmoitus valvontaviranomaiselle. Tietoturvaloukkauksen vakavuutta tulee kuitenkin arvioida, eikä pienen riskin tietoturvaloukkauksesta tarvitse ilmoitusta tehdä.

Ilmoitus tulee tehdä 72 tuntia tietoturvaloukkauksen ilmitulosta, jotta rekisterinpitäjälle ei koidu mahdollisia sanktioita. (Hanninen ym. 2018, 109-110)

Loukkauksen tai haitan vakavuus	Vakava	Matala riski	Korkea riski	Korkea riski
	Tunnistettuja vaikutuksia	Matala riski	Keskimääräinen riski	Korkea riski
	Vähäisiä vaikutuksia	Matala riski	Matala riski	Matala riski
		Kaukainen	Mahdollinen	Hyvin mahdollinen
		Loukkauksen tai haitan todennäköisyys		

Kuva 3 Tietoturvaloukkauksen riskien arvioinnista (Tietosuoja 2018)

8 HENKILÖTIETOJEN SÄILYTYSAJAT

8.1 Työaikalaki ja vuosilomalaki

Tietosuoja-asetuksessa henkilötietojen säilytysaikoja määritellään niin, voiko organisaatio perustella henkilötietoa tarpeelliseksi tai olennaiseksi. Henkilötietolain mukaan säilytysajoissa on kuitenkin lainsäädännöllisiä velvoitteita. Erilaisissa tapauksissa, henkilötiedot ovat säilytettävä vähintään kanneajan umpeuduttua. Kappaleessa käydään läpi eri henkilötietojen lainsäädännöllisiä säilytysakoija. (Paanetoja & Tikkanen 2017, 259)

Työaikalain 37. artiklan mukaan, työaikakirjanpitoa tulee säilyttää vähintään kaksi vuotta. Työaikalaissa kerrotaan, että korvausvaatimuksen umpeutumisaika on kaksi vuotta, joten tämän jälkeen työaikakirjanpitoa ei ole perusteltua säilyttää. Kanneaika vuosilomalaissa on myös kaksi vuotta, joten samaa säilytysaikaa voidaan soveltaa. (Paanetoja & Tikkanen 2017, 260)

8.2 Henkilötietolaki ja työsopimuslaki

”Henkilötietolain 12. artiklan mukaan arkaluonteiset tiedot, kuten työntekijän terveydentilaa koskevat tiedot, on poistettava henkilörekisteristä välittömästä sen jälkeen, kun niiden käsittelylle ei ole perustetta.” (Paanetoja & Tikkanen 2017, 260) Lääkärintodistuksia ja muita terveydentilaa koskevia tietoja voidaan kuitenkin säilyttää kaksi vuotta, vaadeajan umpeutumiseen asti. (Paanetoja & Tikkanen 2017, 260)

Työsopimuslain mukaan saatavien vanhentumisaika on viisi vuotta saatavan erääntymisestä. Organisaation on perusteltua säilyttää työsopimuksia viisi vuotta, kanneajan umpeutumiseen asti. (Paanetoja & Tikkanen 2017, 261-262)

8.3 Yhdenvertaisuuslaki

Yhdenvertaisuuslain 26. artiklan mukaan, työhönottotilanteessa tapahtuneesta syrjinnästä on tehtävä kanne korkeintaan vuoden päästä siitä, kun syrjitty työnhakija on saanut tiedon työpaikan menemisestä toiselle henkilölle. Rekrytoinnin aikana tehtyä dokumentointia työnhakijoista on tämän perusteella perusteltua säilyttää vuosi rekrytoinnin tapahtumisesta. (Paanetoja & Tikkanen 2017, 262)

9 OPINNÄYTETYÖN TOTEUTTAMINEN

9.1 Lähtökohdat

Opinnäytetyöni on Case-yrityksen toimeksiannosta toteutettu. Toteutan opinnäytetyön keräämällä teoriaosaan olennaisen teoriatiedon tietosuoja-asetuksen voimaantulosta ja muutoksista. Empiirisen tiedon pohjalta käyn läpi kaikki Case-yrityksen tietojärjestelmiä, jotka sisältävät henkilötietoa. Tietojärjestelmiin kuuluvat muun muassa työnhakijarekisteri ja palkkatietorekisteri. Pyrin teorian avulla teettämään Case-yritykselle toimintasuosituksia henkilötietojen käsittelystä ja säilyttämisestä. Opinnäytetyöni on kvalitatiivinen eli laadullinen tutkimus, projektiluontoisilla piirteillä. Opinnäytetyön

tavoitteena on lopputuloksena saada ohjeistuksia/toimintasuosituksia, jotka hyödyttävät yrityksen toimintaa.

9.2 Tutkimustyyppi

Tutkimus voi olla sekä määrällinen eli kvantitatiivinen, tai laadullinen eli kvalitatiivinen tutkimus. Valitsin opinnäytetyöni tutkimustyypikseni kvalitatiivisen eli laadullisen tutkimuksen. “Laadullisen tutkimuksen tavoitteena on ilmiön ymmärtäminen, selittäminen, tulkinta ja usein myös mallintaminen ja soveltaminen.” (Pitkäranta, 2014, 33) Laadullinen tutkimus sopii opinnäytetyöhöni hyvin, koska pyrin selittämään ja tulkitsemaan tietosuoja-asetuksen seurauksia, ja tämän perusteella mallintamaan ja soveltamaan ohjeistuksia tietoni pohjalle. Opinnäytetyöni sisältää myös projektimaisia piirteitä, sillä tutkimus on toteutettu toimeksiantona yritykselle yrityksen pyynnöstä. (Pitkäranta, 2014, 33)

Tutkimuksen tarkoitusta voidaan myös tarkastella tarkemmin neljän piirteen avulla. Tutkimus voi olla joko kartoittava, selittävä, kuvaileva tai ennustava, sekä näiden yhdistelmä. Oma opinnäytetyöni on pääasiassa kartoittava tutkimus, koska etsin tietosuoja-asetuksen toimeentulon takia aineistoa ja pyrin kartoittamaan toimenpiteitä Case-yrityksen jatkoa varten. Opinnäytetyöni on toisaalta myös osin ennustava, sillä tietosuoja-asetuksen toimeentulon vaikutuksia ei vielä tarkasti tiedetä. Pyrin siis ennustamaan asetuksen vaikutuksia myös tulevaisuutta varten mahdollisimman tarkasti. (Hirsjärvi ym. 2010, 137-139.)

Tutkimuksessa voidaan käyttää teorian keräämiseen eri tiedonkeruumenetelmiä kuten, dokumentointia, havainnointia, haastatteluja ja kyselyjä. Omassa opinnäytetyössäni tärkeimpänä tiedonkeruumenetelmänä käytän dokumentteja, kuten kirjoja ja tutkimuksia ja verkkosivuja. (Kananen 2014, 64)

9.3 Reliabiliteetti ja validiteetti

Opinnäytetyöni pyrkii toistettavaan lopputulokseen, eli reliabiliteettiin tutkimustulosten toistettavuus on tärkeä osa relibialiteettia. Opinnäytetyössäni käytän useita lähteitä,

sekä kirjallisuudesta ja internet-aineistosta. Opinnäytetyöni perustuu pitkälti lakitekstiin, jonka relibiliateettia voidaan pitää hyvänä. Myös lähteiden tuoreuden voidaan pitää lisäävän relibiliateettia, sillä lähteeni ovat pääosin tältä ja viime vuodelta. (Hirsjärvi ym. 2010, 231.)

Validiteetti eli pätevyys, tarkoittaa tutkimusmenetelmän kykyä mitata sitä mitä pyritään tutkimuksessa mittaamaan. Opinnäytetyöni validius on mielestäni hyvä, sillä pyrin avaamaan tutkimustuloksiani vain siinä määrin, että empiirisessä osiossa selviää, kuinka olen tuloksiini päässyt. Opinnäytetyöni validiteettia voi kuitenkin osalta haitata se, että asetuksen toimeentulon tuloksista ja käytännöistä ei ole vielä täyttä varmuutta, joten tulevaisuuden käytäntöä pyrin ennustamaan tuloksiini vain tuloksieni pohjalta. (Hirsjärvi ym. 2010, 231-233.)

10 LÄHTÖTILANNE

Ennen tietosuoja-asetuksen toimeentuloa, case-yritys teki merkittäviä panostuksia tietosuojaan, joten yrityksen lähtötilanne on jo kohtuullisen hyvällä tasolla. Yrityksen toimihenkilöt valmistautuivat yhdessä asetuksen toimeentuloon hyvissä ajoin, hiomalla käytäntöjä sekä muuttamalla tulevia toimintatapoja. Valmistautumiseen käytettiin merkittävä määrä aikaa, koulutuksien ja tehtyjen dokumenttien muodossa. Yrityksen henkilöstö valmisti tietosuojaselosteen internetsivuilleen nähtäväksi, erillisen ohjeen henkilöstölleen henkilötiedon käsittelystä, sekä tietotilinpäätöksen. Case-yritys myös nimitti toimistopäällikkönsä tietosuojavastaavaksi. Jatkuva toimintatapojen ja käytäntöjen kehittäminen on kuitenkin tärkeää pitää uutena normina; kehitettävää riittää jatkossakin. Pyrin omassa opinnäytetyössäni löytämään vielä joitakin kehityskohteita, joihin yrityksen tulisi puuttua.

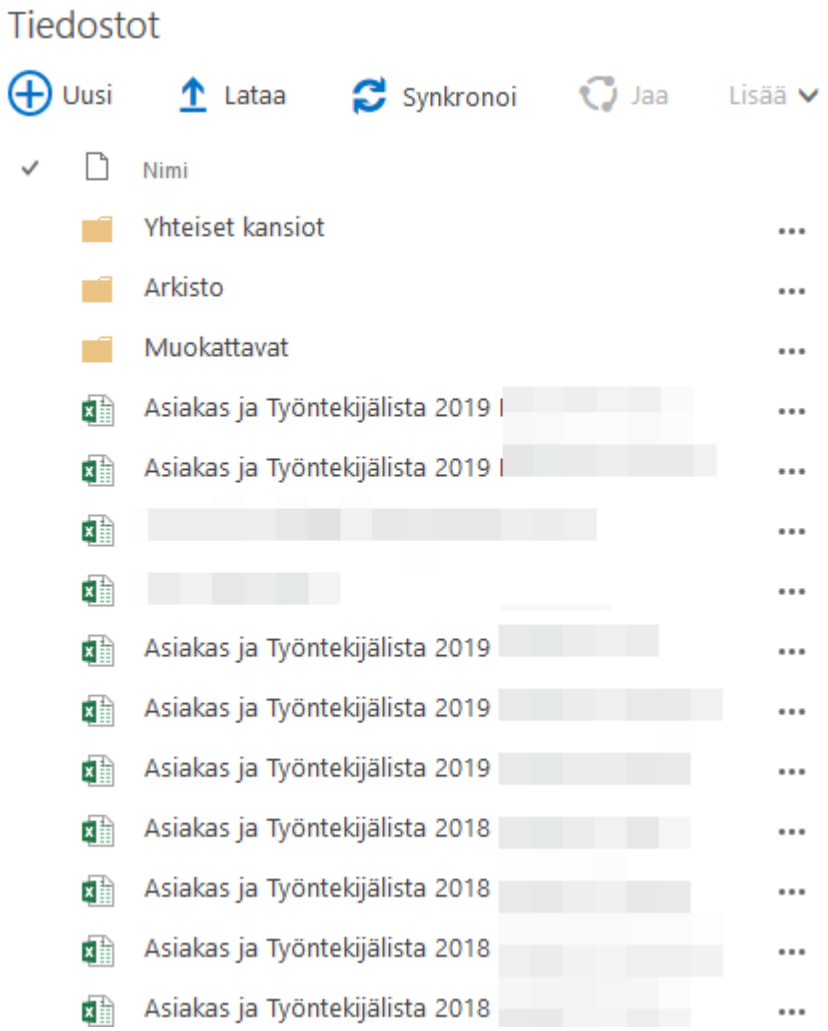
11 POHDINTA

Case-yritys säilyttää henkilötietoa useassa eri paikassa. Aluksi käyn empiirisessä osuudessa läpi yrityksen eri tietokantoja, ja selvitän mitä henkilötietoa missäkin

säilytetään, ja onko henkilötietojen säilyttäminen asianmukaista. Lopuksi pyrin antamaan kehotuksia ja parannusehdotuksia koskien tietojen säilyttämistä.

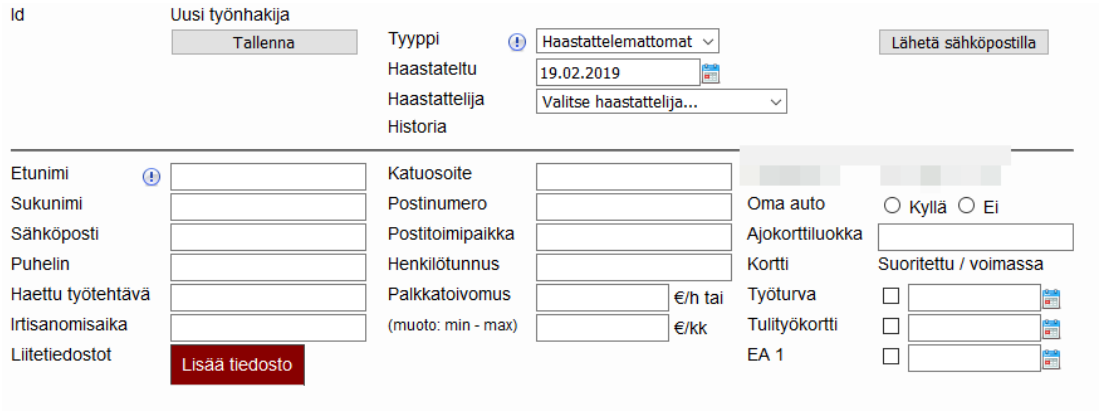
11.1 Henkilötieto järjestelmissä

Keskeisimmät henkilötiedot löytyvät yrityksen Microsoftilta hankkimasta pilvipalvelusta eli SharePointista. Sharepoint yrityksen henkilötiedon säilytyspaikkana on vakiintunut sen helppokäyttöisyyden vuoksi. Yrityksen toimihenkilöt voivat lisätä ja muokata tiedostoja SharePointissa, sekä tarkastella muiden lisäämiä tiedostoja. Pilvipalveluita on käytössä kaksi eri pohjaa, tarpeen mukaan. Toinen puoli sisältää esimerkiksi markkinointimateriaaleja ja työsopimuksia, ja toinen puoli palkkahallinnon tiedostoja kuten palkkatietoja. Palkkahallinnon Sharepoint-pohjassa jotkin tiedostot ovat jaettu tilitoimiston kanssa tarpeen mukaan. Kansioihin pääsyä on rajoitettu siinä määrin, että palkkahallinto ja muut käyttävät eri Sharepoint-pohjia. Eri työntekijöiden kansioihin pääsyä olisi vielä hyvä tarkastella, joten heillä on vain oikeudet kansioihin pääsyyn, joita työssään välttämättä tarvitsevat. Tietoja, kuten työsopimuksia ja palkkatietoja säilytetään toistaiseksi määritellyn ajan, kuitenkin vähintään erinäisten lakien mukaan tarvitun ajan. Ehdotan yrityksen tietosuojavastaavalle ja muulle henkilöstölle kuukausittaista päivää, jolloin henkilötietoa, joka on tarpeetonta, ja jolle ei löydy perusteita säilytykselle, käydään poistamassa. Sharepointissa ei ole mahdollisuutta tietojen automaattiselle poistolle, joten kuukausittainen tietojen läpikäynti on mielestäni paras vaihtoehto. Alla olevassa kuvassa tietoa pohjan kansiorakenteesta.



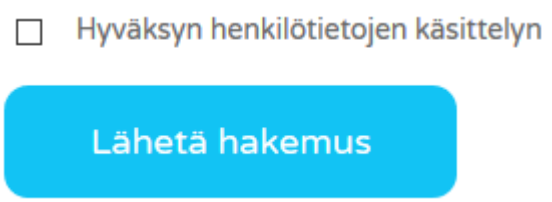
Kuva 4 Microsoftin pilvipalvelun Sharepoint-pohja (Sharepoint 2018)

Toinen tietokanta, joka sisältää henkilötietoa on yrityksen oma työnhakijarekisteri. Työnhakijarekisteriin tulevat kaikki henkilötiedot, jotka ovat liitettynä työhakemuksiin. Nämä tiedot ovat yleisimmin mm. nimet, puhelinnumerot, sosiaaliturvatunnukset ja osoitteet. Tiedot kuten nimi, sukunimi, sähköposti, puhelinnumero ja paikkakunta ovat hakemuksessa pakollisia, muut vapaasti täytettävissä. Alla olevassa kuvassa tyhjät kohdat, jotka työnhakija täyttää lähettäessään hakemuksen.



Kuva 5 Case-yrityksen omasta järjestelmästä (Case-yrityksen oma järjestelmä 2019)

Hakemuksessa kysyttävät tiedot ovat yrityksen toimialan suhteen perusteltuja, joten nämä voidaan sekä kysyä ja säilyttää. Hakemuksessa on myös vapaa hakemus kenttä, johon työnhakija voi vapaasti kirjoittaa tietoja itsestään, ja tähän tulisi yrityksen henkilöstön kiinnittää huomiota. Työnhakija voi kertoa itsestään jotakin arkaluontoista tietoa, jota ei ole tietosuoja-asetuksen mukaan perusteltua säilyttää. Henkilöstöä täytyykin siis ohjeistaa tällaisista tapauksista, ja kuinka kuuluu menetellä tietoja poistaessa. Tällaista arkaluonteista tietoa voi olla esimerkiksi ammattiliittoon kuuluminen tai jokin terveydentilaa koskeva asia. Ohjeistan henkilöstöä tiedosta, joka tulisi tällaisessa tilanteessa poistaa. Yrityksellä ei ole myöskään käytössä vanhentuneen tiedon automaattista poistoa, joka tulisi ottaa käyttöön. Järjestelmästä löytyy työnhakijoiden henkilötietoja vuodelta 2015, ja tällaista henkilötietoa ei ole perusteltua säilyttää. Yrityksen tulisi ottaa yhteyttä palveluntarjoajaan, ja tehdä järjestelmään lisäys, joka poistaa tiedot yli kaksi vuotta vanhat henkilötiedot automaattisesti. Kaksi vuotta on sopiva aika, koska hakijan kanneaika päättyy tämän tullessa täyteen. Henkilötiedon käsittelyyn yritys kysyy luvan jo ennen hakemuksen vastaanottamista, joten tämä puoli on siltä osin kunnossa. Alla kuva työnhakijan suostumuksesta henkilötietojen käsittelyyn.



Kuva 6 Case-yrityksen internetsivuilta hakemusta täytettäessä (Case-yrityksen internetsivut 2019)

Kolmas yrityksen käytössä oleva järjestelmä on Procountor-taloushallintojärjestelmä. Procountor on käytössä palkanlaskennan toimihenkilöillä, ja se syötetään myös työntekijöiden henkilö- ja palkkatietoja. Procountorin käyttö on yrityksessä tietosuoja-asetuksen mukaan tehty oikein.

Viimeisin henkilötiedon säilytyspaikka on paperiversiona. Paperilla yritys yleensä vastaanottaa sairauslomatodistukset sekä verokortit työntekijöiltään. Sairauslomatodistuksia käsittelevät vain henkilöt, jotka vastaavat esimerkiksi sairauslomapalkan maksusta. Paperille säilytetty henkilötieto on yrityksessä asianmukaista, sillä paperit, jotka sisältävät arkaluonteista henkilötietoa, säilytetään lukollisissa kaapeissa.

Case-yrityksen internetsivuilla yritys on pyrkinyt parantamaan tietosuoja-asetuksen mukaisesti henkilötiedon käsittelyn läpinäkyvyyttä. Internetsivuilta löytyy yrityksen laatima tietosuojaseloste, jossa käydään läpi mm. käsiteltävän henkilötiedon käyttötarkoitus, tietojen luovutusperiaatteet, tietosuojavastaavan tiedot, sekä muuta olennaista koskien tietosuoja-asetusta. Tietosuojaseloste on tehty asianmukaisesti ja se sisältää tarvittavat ja olennaiset tiedot, joten tämän suhteen yrityksellä ei ole kehitettävää.

11.2 Tietoturva

Turvallisuus on keskeisimpiä asioita henkilötietoasetuksen seurauksena. Turvallisuus on tietokantojen osalta yrityksellä hyvällä tasolla. Pilvipalveluun ja työnhakijarekisteriin on mahdollista päästä vain rekisteröitynyt käyttäjä, jolle ylläpitäjä on antanut tarvittavat oikeudet tarkastella tai muokata tiedostoja. Myös henkilötieto, jota säilytetään paperisessa muodossa, pidetään lukittujen ovien takana. Paperinen tieto myös hävitetään asianmukaisesti, tasaisin väliajoin. Pois heitettävä tieto säilytetään lukitussa kierrätyslaatikossa, johon vain hallinnolla on pääsy. Ainoita riskejä yrityksen kannalta ovat nähdäkseni jonkin näköinen tietoturvahyökkäys, josta henkilötietoa vuotaa ulkopuolisille, tai toimiston toimihenkilön huolimattomuus. Tietoturvahyökkäyksiin on jo myös varauduttu asianmukaisella viruksentorjunnalla ja palomuureilla. Tapaus, jossa toimihenkilön huolimattomuus vuotaisi henkilötietoa ulkopuolisille vaikuttaa myös

hyvin epätodennäköiseltä. Case-yritys on myös ottanut käyttöön salatun sähköpostin, jolla pyritään ulospäin kulkevan henkilötiedon turvallisuuden pysyvän hyvällä tasolla.

Henkilötiedon suuren määrän, ja osittain myös arkaluonteisuuden takia tulisi henkilötiedon säilytykseen keskittyä entistä tarkemmin. Henkilötiedot ovat pääasiassa kolmessa eri järjestelmässä, sekä paperisena. Rekisteröidyn oikeuksien lisääntymisen myötä, kaikki tiedot rekisteröidystä pitää pyydettäessä näyttää rekisteröidylle tai poistaa. Tämän seurauksena henkilötiedon tulisi olla helposti koottavissa järjestelmistä. Yrityksen olisi myös tärkeä näyttää säilytettyjen tietojen käyttötarkoitus ja pyrkiä minimoimaan tiedon määrää. Yritys saa opinnäytetyöstäni valmiin listauksen paikoista, jossa henkilötietoa säilytetään, joten tapauksessa, jossa rekisteröity haluaa nähdä hänestä säilytetyt henkilötiedot, on yrityksen ne helppo opinnäytetyöni avulla koota.

12YHTEENVETO JA SUOSITELLUT TOIMENPITEET

12.1 Tietoturvaharjoitus

Case-yritys on tehnyt parannuksia henkilötiedon tietoturvaan ottamalla käyttöön salatut sähköpostit, sekä yrityksen internetsivun salatun yhteyden. Tietoturvallisuudessa on siis nähty parantamisen varaa, ja siihen on puututtu.

Näen kuitenkin, että mahdolliseen tietoturvaloukkaukseen, jossa henkilötietoa vuotaa ulkopuolisille olisi hyvä varautua vielä paremmin. Yrityksen tulisi mielestäni luoda hypoteettinen tilanne, jossa henkilötietoa on joko kadonnut tai vuotanut ulkopuolisille, ja keskittyä yhtenäisenä henkilöstönä tilannetta seuraaviin toimenpiteisiin. Tällainen tilanne voisi periaatteessa tapahtua koska tahansa, joten tilanteeseen tulisi henkilöstöllä olla valmiudet jo ennen sen tapahtumista. Henkilöstön pitää tietää, että epäilyksen herätessä vastaavasta tilanteesta, tulee siitä ilmoittaa heti tietosuojavastaavalle. Jos varmistuu että tietoturvaloukkaus on tapahtunut, ryhtyy henkilöstö ennalta sovittuihin toimenpiteisiin, kuten tietojen turvaamiseen ja viranomaisille ilmoittamiseen. Tilanteeseen valmistautuminen antaa henkilöstölle valmiudet puuttua tilanteeseen, ja tehdä

tarvittavat toimenpiteet. Dokumentointi tietoturvaharjoituksesta on myös todiste, että mahdolliseen tilanteeseen on varauduttu.

12.2 Henkilötiedon tarkasteluoikeudet ja minimointi

Yrityksen toimihenkilöiden määrä on n. 15 henkilöä. Toimihenkilöitä työskentelee eri työtehtävissä, sekä rooleissa, joten on perusteltua, että kaikilla työntekijöille ei ole pääsyä kaikkiin tietokantoihin. Lähtökohtana tulisi pitää sitä, että toimihenkilöllä on pääsy vain työtä koskevaan olennaiseen tietoon, joka voidaan perustella. Tässä mielestäni yksi selvä kehityskohde, johon yrityksellä on mahdollisuudet puuttua.

Yrityksen tulisi myös tarkastella tiedon säilytystä vielä tarkemmin, ja pyrkiä poistamaan epäolennainen henkilötieto tietokannoista. Henkilötietolain keskeinen ohjeistus on, että yritys voi säilyttää henkilötietoa jos se on perusteltua, joten tämän kautta säilytetty henkilötieto tulisi käydä järjestelmistä läpi. Dokumentoinnin merkitys on suuressa määrin tärkeää, jos yritys joutuu myöhemmin perustelemaan henkilötietojensa säilytystä. Varsinkin ns. arkaluonteinen tieto tulisi pyrkiä poistamaan, jos sille ei löydy lain pakottamia velvoitteita.

12.3 Henkilötiedon säilytysajat

Henkilötietojen säilytysajat nähdään myös relevanttina uudessa asetuksessa. Case-yrityksen tulee ottaa huomioon säilytysajat tarkasti, mutta pitää kuitenkin kiinni lainmukaisista säilytysajoista. Tämä saattaa olla haasteellista, mutta välttämätöntä. Mielestäni henkilötietojen säilytyksessä yrityksellä on vielä eniten huomioitavaa, esimerkiksi työnhakijoiden henkilötietojen kohdalla, josta mainitsin aikaisemmin. Henkilötiedoissa pitäisi järjestelmässä olla automaattinen poistoaika, tai sopia yrityksen sisällä jokin tietty ajankohta, jolloin vanhentuneet tiedot poistetaan. Ehdotan yritykselle käyttöön molempia toimintatapoja, riippuen henkilötiedosta, lainsäädännön vuoksi. Työhakemuksia on perusteltua säilyttää kanneajan vuoksi kaksi vuotta ja työsopimuksia kanneajan perusteella viisi vuotta.

12.4 Henkilötietojen luovutus

Yritys luovuttaa henkilötietoja eri virastoille, sekä asiakkailleen. Henkilötietojen luovutus on mainittu yrityksen tietosuojaselosteessa. Yritys on tehnyt turvallisen henkilötietojen luovutuksen eteen jo töitä ottamalla käyttöön salatun sähköpostin, jota käytetään henkilötietoa siirrettäessä.

Yrityksen tulisi mielestäni kuitenkin tarkemmin paneutua asiakkaidensa henkilötietojensa käsittelyyn. Yrityksen olisi hyvä varmistaa, että myös asiakkaillaan henkilötietojen säilytys on tarvittavalla tasolla, eikä tietovuotojen uhkaa ole. Myös toimintatavoista henkilötietojen vuotaessa asiakkailta, pitäisi sopia jo etukäteen.

13LOPPUSANAT

Opinnäytetyöni tekeminen sujui pääasiassa hyvin, alkuperäisestä aikataulusta viivästymisestä huolimatta. Teoriaosuuden kokoaminen meni suoraviivaisesti ja hyvin, mutta empiirisessä osuudessa oli hiukan ongelmia aiheen tuoreuden vuoksi. Tutkimustietoa yrityksen suositelluista käytännöistä oli vähän, ja jotkin paikalliset lait asiasta olivat opinnäytetyötä tehdessä edelleen kesken. Tein siis opinnäytetyöni parhaan tietoni mukaan tiedolla, joka oli käytössä. Vaikka paikalliset lait voivat vielä muuttaa henkilötiedon säilytystä, jää yritykselle mielestäni hyvä ohjeistuspohja jatkoa varten.

Opinnäytetyöni aihe tuli case-yrityksen toimeksiannosta, eli todelliseen tarpeeseen. Mielestäni onnistuin tekemään yritykselle hyödyllisen ohjeistuksen henkilötiedon säilytyksestä ja toimintatavoista, joita tulisi vielä kehittää. Pyrin myös opinnäytetyössäni näyttämään, että toimintatapojen kehittäminen jatkuvasti on tärkeää. Sain tarvittaessa yritykseltä tietoa järjestelmistä, sekä tukea opinnäytetyön tekemiseen.

LÄHTEET

Andreasson. A., Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Helsinki: Tekijät ja Tietosanoma Oy.

Dittmar & Indrenius. 2018. Tietosuoja-asetus HR:n näkökulmasta Case-yrityksen koulutuksessa. 21.8.2018.

Elinkeinoelämän Keskusliiton www-sivut. Viitattu: 7.1.2019. https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/#5-2-1--Osoitusvelvollisuus

Eur Lex www-sivut. Viitattu: 14.12.2018. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Finlexin www-sivut. Viitattu: 14.12.2018. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2018. Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset. Vantaa: Hansaprint Oy.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2010. Tutki ja kirjoita. 15.-16. uud. p. Helsinki: Tammi.

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Turku: Suomen Yliopistopaino Oy.

Opi Tietosuojaa. www-sivut. Viitattu: 14.12.2018. https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus

Paanetoja, J. & Tikkanen, H. 2017. Työsuhteen asiakirjat. Helsinki: Alma Talent.

Pitkäranta, A. 2014. Laadullinen tutkimus opinnäytetyönä. Jokioinen: E-Oppi Oy. Viitattu 21.12.2018. https://www.ellibslibrary.com/fi/book/9789522828019

Tietosuojan www-sivut. Viitattu: 10.12.2018. https://tietosuoja.fi/GDPR tietosuojavaltuutentun toimisto 2015

Tietosuoja Uutisten www-sivut. Viitattu: 15.1.2019 https://tietosuojauutiset.fi/2016/06/21/tietotilinpaatos-tyokaluna-tietosuoja-asetukseen-valmistautumisessa/

Tietosuojan www-sivut. Viitattu: 15.1.2019 https://tietosuoja.fi/arvioi-riskit