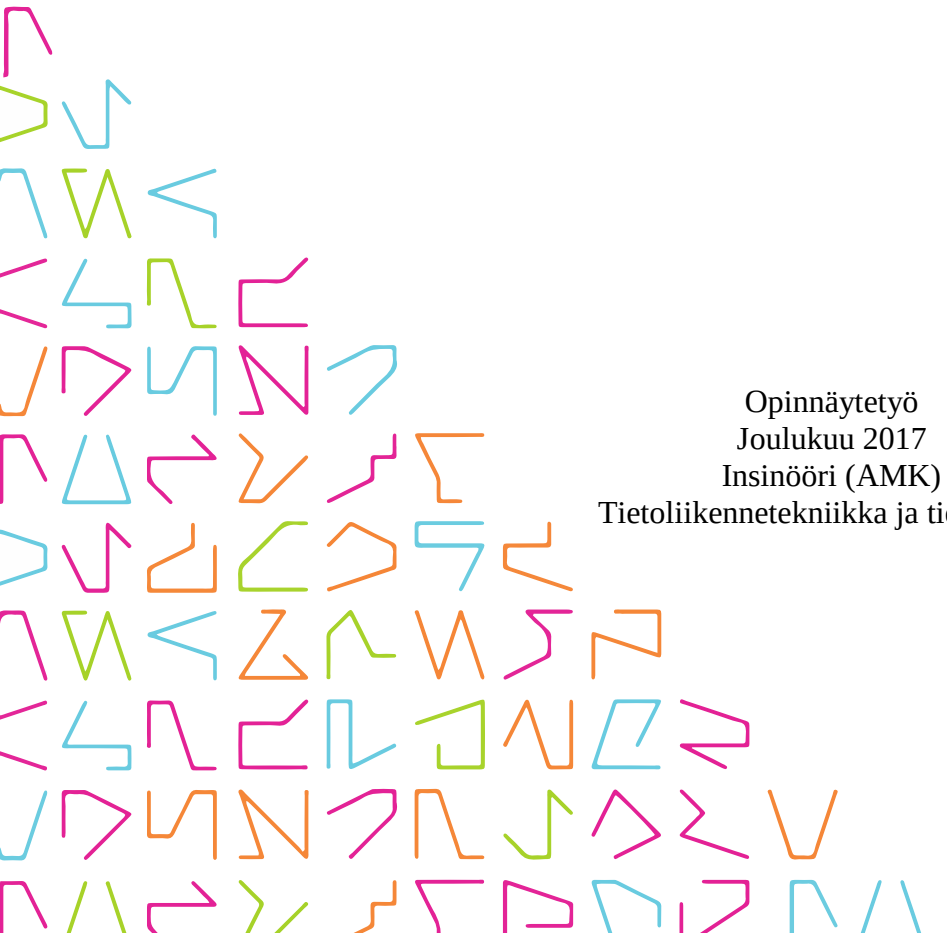
TAMPEREEN
AMMATTIKORKEAKOULU

GDPR - VAIKUTUKSET YRITYKSEN TIETO-SUOJA- JA TIETOTURVATYÖSSÄ

Henni Helander



Opinnäytetyö
Joulukuu 2017
Insinööri (AMK)
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Insinööri (AMK)
Tietoliikennetekniikka ja tietoverkot

HELANDER HENNI:
GDPR – vaikutukset yrityksen tietosuoja- ja tietoturvatyössä

Opinnäytetyö 45 sivua, joista liitteitä 6 sivua
Joulukuu 2017

GDPR *(General Data Protection Regulation)* on uusi EU:n yleinen tietosuoja-asetus (2016/679), jota tarkasteltiin tässä opinnäytetyössä pienten ja keskisuurten yritysten näkökulmasta. Opinnäytetyön tavoitteena oli soveltaa tutkittua tietoa GDPR:stä ja muodostaa sen avulla yrityksille kattava selonteko asetuksesta sekä sen vaatimuksista. Lisäksi opinnäytetyössä opastettiin yrityksiä tietosuojaselosteiden ja tietotilinpäätöksen tekemisessä. Opinnäytetyötä varten tehtiin yrityshaastatteluja, mutta salassapitosopimusten vuoksi yrityksiä ei mainittu nimeltä tässä opinnäytetyössä. Yrityshaastattelujen lisäksi tutkimuksessa käytettiin tietolähteinä pääosin internetistä saatavilla olevaa materiaalia ajan tasalla olevan tiedon saamiseksi. Valtaosa tiedoista kerättiin erilaisilta GDPR- ja viranomaissivustoilta sekä webinaari-esityksistä.

Opinnäytetyön alussa käytiin läpi GDPR:ää yleisellä tasolla ja tutustuttiin asetuksessa käytettävään sanastoon. Seuraavissa kappaleissa syvennyttiin rekisteröityjen oikeuksiin, rekisterinpitäjän velvollisuuksiin ja tietosuojavastaavan toimintaan. Kuudennessa kappaleessa esiteltiin GDPR-sovelluksia, jotka helpottavat yritysten tietosuojatyötä. Opinnäytetyön lopussa kerrottiin tietotilinpäätöksen tekemisestä sekä tietosuojatyön teknisestä toteutuksesta.

Yleisellä tasolla opinnäytetyön tavoitteissa onnistuttiin, mutta opinnäytetyön aikana haastateltujen yritysten tietotilinpäätökset eivät ehtineet valmistua, vaan niiden parissa työ jatkuu edelleen. Myös ennakkopäätösten puuttuminen opinnäytetyön tekohetkellä jätti avoimia kysymyksiä, joihin tullaan todennäköisesti saamaan selkeämpää linjausta kevään 2018 aikana tai mahdollisesti vasta myöhemmin soveltamisajan jo alettua.

Asiasanat: GDPR, tietosuoja-asetus, tietotilinpäätös

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Information Technology
Telecommunications and Networking

HELANDER HENNI:
GDPR – Impacts on Data Protection and Information Security in a corporate environment

Bachelor's thesis 45 pages, appendices 6 pages
December 2017

In this thesis, the EU General Data Protection Regulation (GDPR) is being explored from the point of view of small and medium enterprises (SME). The purpose was to adapt researched information about GDPR and to produce a comprehensive briefing regarding the regulation and its requirements on SMEs. Additionally, the thesis guided SMEs in preparing privacy policies and data balance sheets.

SME representatives were interviewed to get a better understanding of the state of their data protection. The SMEs were not mentioned by name in this thesis, due to the Non-Disclosure agreements (NDAs). In addition to the interviews, information was gathered mainly from GDPR websites, public authority websites and webinar presentations to get up to date information regarding the regulation.

At the beginning of the thesis, the GDPR was reviewed at a general level and the vocabulary of the regulation was introduced. The following chapters focused on the rights of the data subject, responsibilities of the controller and activities of the data protection officer. The sixth chapter presented the GDPR-software, which were made to aid the SMEs' data protection work. The last chapters included information regarding the preparation of the data balance sheet and the technical part of data protection work.

The targets of the thesis were generally accomplished, however there was not enough time to complete SMEs data balance sheets, during the making of this thesis. Also the lack of prejudicates left some open questions, which will most likely be answered when more explicit policy will be presented during spring 2018 or possibly after the application of the regulation.

Key words: GDPR, data balance sheet

SISÄLLYS

ERITYISSANASTO

B2B	Business-to-Business, yritysmarkkinointi
B2C	Business-to-Customer, kuluttajamarkkinointi
BPDU	Bridge Protocol Data Unit, STP-informaatiota sisältävä kehys
CPE	Customer Premises Equipment, reitittävä laite yrityksen tiloissa
DHCP	Dynamic Host Configuration Protocol, verkkoprotokolla IP-osoitteiden jakamiseen
DPIA	Data Protection Impact Assessment, vaikutusarviointi
GDPR	General Data Protection Regulation, yleinen tietosuoja-asetus
ICT	Information and communications technology, tieto- ja viestintäteknologia
IEE 802.1X	Port Based Authentication -standard, porttikohtaisen todentamisen standardi
IPsec	IP Security Architecture, yhteyksien turvaamiseen tarkoitettu tietoliikenneprotokolla
LAN	Local Area Network, lähiverkko
MAC-address	Media Access Control Address, laitteen yksilöivä osoite lähiverkossa
MPLS	Multiprotocol Label Switching, menetelmä yritysverkkojen tekemiseen
PE	Provider Edge, palveluntarjoajan reunareititin
PIA	Privacy Impact Assessment, tietosuojan nykytilan arviointi
SHA-2	Secure Hash Algorithm 2, salaukseen käytetty kryptografinen tiivistefunktio
SSH	Secure Shell, salatun tietoliikenteen protokolla
STP	Spanning Tree Protocol, silmukoiden muodostumisen estävä verkkoprotokolla
WP29	Working Party 29, EU:n tietosuojaryhmä

1 JOHDANTO

GDPR *(General Data Protection Regulation)* on uusi EU:n laajuinen tietosuoja-asetus (2016/679), jonka soveltaminen alkaa 25.5.2018. Uusi tietosuoja-asetus parantaa luonnollisen henkilön henkilötietojen yksityisyyttä sekä henkilön oikeuksia omiin tietoihinsa. GDPR:n myötä henkilötietojen käsittelyn sääntely yhtenäistyy, kun sama asetus koskee kaikkia EU/ETA-jäsenmaita. GDPR edistää myös EU:n digitaalisia sisämarkkinoita, koska muun muassa EU:n sisällä toimivista verkkokaupoista tulee entistä luotettavampia henkilötietojen käsittelyn suhteen. GDPR tulee myös kumoamaan nykyisen EU:n henkilötietodirektiivin 95/46/EY [14]. Uuden asetuksen mukaan rekisterinpitäjän on jatkossa pystyttävä muun muassa konkreettisesti osoittamaan, että uudet tietosuojasäännökset on huomioitu yrityksen toiminnassa. GDPR tuo mukanaan uutena asiana myös esimerkiksi mittavat sanktiot asetuksen rikkomisesta tai laiminlyömisestä. Asetuksessa on vielä jonkin verran tulkinnanvaraa, vaikka joitakin linjauksia asetuksen tulkintaan on jo saatukin. Käytännönkokemus ja ohjeistusten määrä kasvavat viikko viikolta.

Tämän opinnäytetyön tarkoituksena on selvittää, miten pienten ja keskisuurten yritysten tulisi huomioida EU:n uusi tietosuoja-asetus toiminnassaan. Lisäksi tarkoituksena on soveltaa tutkimuksessa käytettyä lähdetietoa tietosuojaselosteiden ja tietotilinpäätöksen luomiseen. Opinnäytetyössä on käytetty hyväksi internetistä löytyviä GDPR-lähteitä, webinaari-esityksiä sekä yrityshaastatteluja. Haastateltujen yritysten nimet ovat salaisia salassapitosopimusten vuoksi ja siksi yrityksistä mainitaan tässä opinnäytetyössä vain yleisellä tasolla.

Tehdyissä yrityshaastatteluissa selvisi, että kyseisten yritysten tietosuojatyössä on vielä paljon kehitettävää, ennen kuin päästäisiin GDPR:n edellyttämälle tasolle. Monet haastatelluista yrityksistä olivat kuitenkin jo alkaneet selvittämään asetuksen vaatimuksia sekä mahdollisesti jopa palkanneet apua asetuksen vaatiman tietosuojatason saavuttamiseksi. Yrityksissä huomattiin, että henkilötietoa oli kertynyt lukuisiin eri paikkoihin, ja näin ollen henkilörekistereiden määrä oli merkittävä. Yrityksillä olikin alkuun suuri työ selvittää tietoinventaariota tehdessään, mitä henkilötietoa heillä oli, missä tietoa oli, kenellä oli pääsy tietoihin ja kuinka tieto oli suojattu.

2 GDPR YLEISESTI

Tässä kappaleessa kerrotaan GDPR:stä eli EU:n yleisestä tietosuoja-asetuksesta yleisesti sekä tutustutaan asetuksessa käytettävään sanastoon, jota tullaan jatkossa käyttämään tässä opinnäytetyössä. Kappaleen lopussa perehdytään tarkemmin suostumukseen ja henkilötiedon käsittelyyn.

2.1 Yleistä

Euroopan parlamentti ja neuvosto antoivat 27.4.2016 uuden koko EU:n laajuisen tietosuoja-asetuksen (2016/679). Tällä hetkellä eletään siirtymäkautta, joka päättyy 25.5.2018, jonka jälkeen asetuksen soveltaminen virallisesti alkaa [3]. GDPR:n tehtävänä on suojella luonnollisten henkilöiden perusoikeuksia ja -vapauksia sekä heidän oikeuttaan henkilötietojensa suojaan. Asetuksen tavoitteena on myös yhdenmukaistaa henkilötietojen käsittelyn sääntely EU:n sisällä sekä lisätä digitaalista kulutusta EU:n sisämarkkinoilla [13, luku 1]. Uusi asetus kumoaa myös direktiivin 95/46/EY ”yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta”, joka astui voimaan vuonna 1995 [15].

GDPR tuo mukanaan selkeämpiä sääntöjä rekisteröidyn oikeuksista sekä erityisesti rekisterinpitäjän velvollisuuksista. Soveltamisajan alettua ei enää riitä, että yritys sanoo noudattavansa asetusta, vaan jatkossa yrityksen pitää myös osoittaa se omassa toiminnassaan esimerkiksi dokumentaation avulla. Mutta kaikista puhututtanein muutos on GDPR:n hallinnolliset sanktiot, joita valvontaviranomaisella on valtuutus antaa asetusta rikottaessa. Pahimmillaan sanktio voi olla jopa 20 miljoonaa euroa tai neljä prosenttia yrityksen vuoden globaalista liikevaihdosta [14]. Sanktioidenkin vuoksi on ensiarvoisen tärkeää, että myös yrityksen johto on sitoutettu asetuksen noudattamiseen.

Nykyisessä tietoyhteiskunnassa henkilötietoa käsitellään lähes kaikkialla, joten käytännössä tietosuoja-asetus koskee kaikkia yrityksiä ja organisaatioita. Tietoa säilytetään niin digitaalisessa kuin fyysisessäkin muodossa. Vaikka yrityksessä ei käsiteltäisi varsinaisesti asiakastietoja, niin silti yrityksen sisältä löytyy työntekijöiden tietoja, jotka ovat henkilötietoja siinä missä asiakastiedotkin. Asetuksen kannalta ei ole merkitystä, toimiiko

yritys B2B- vai B2C-rajapinnassa, koska samat säännöt koskevat kaikkia yrityksiä ja organisaatioita henkilötietojen käsittelyn osalta.

2.2 GDPR-sanastoa

Henkilötiedoksi luetaan kaikki tunnistettu tai tunnistettavissa oleva luonnolliseen henkilöön liitettävä tieto, kuten nimi (etu- ja sukunimi), osoite, puhelinnumero, sähköpostiosoite, henkilötunnus, IP-osoite, rekisteritunnus, kuva, sijaintitieto ja pankkitieto. On olemassa myös erityisiä henkilötietoryhmiä, joista ilmenee esimerkiksi henkilön rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveystietoja, biometrisiä tietoja, geneettisiä tietoja tai seksuaaliseen käyttäytymiseen liittyviä tietoja [13, artikla 4 kohta 1].

Rekisteröity on henkilö, jonka henkilötietoja käsitellään [10]. Asetus vaatii, että rekisteröidyltä tulee olla saatu suostumus ennen kuin hänen henkilötietojaan käsitellään. Rekisteröidyllä on GDPR:ssä erilaisia oikeuksia omiin tietoihinsa. Tällaisia oikeuksia ovat esimerkiksi tarkastusoikeus, oikeus saada tietonsa korjatuiksi ja poisto-oikeus.

Henkilörekisteri on henkilötietoja sisältävä tietojoukko [13, artikla 4 kohta 6]. Henkilörekistereitä voivat olla esimerkiksi asiakastietorekisteri, työntekijätietorekisteri ja jäsenrekisteri. Rekisteri voi olla joko digitaalisessa tai fyysisessä muodossa. Rekisterit voidaan jakaa vielä käsittelyn luonteen perusteella aktiivisiin tai passiivisiin rekistereihin.

Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä ylläpitää rekisteriä ja on vastuussa asetuksen noudattamisesta [13, artikla 4 kohta 7].

Käsittelijä voi olla luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka toimii rekisterinpitäjän toimeksiannosta henkilötietoja käsittelevänä tahona [10]. Rekisterinpitäjä on lähes aina käsittelijä, mutta käsittelijä voi olla myös jokin yrityksen ulkoinen taho esimerkiksi palkanlaskija.

Käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista [10].

Rekisteröidyn henkilötietoja voidaan käsitellä vain, jos häneltä on saatu siihen suostumus. Suostumus voi olla mikä tahansa vapaaehtoinen, tietoinen ja yksiselitteinen tahdonilmaisu. Suostumus voidaan antaa sanallisesti tai toteuttamalla selkeästi suostumusta ilmaiseva toimi [14], joka voi olla esimerkiksi kuluttaja-asiakkaalle kohdistetussa tietosuojaselosteessa olevan hyväksymisruudun rastittaminen.

Rekisterinpitäjän tulee laatia rekisteri- tai tietosuojaselosteita, jotka ovat tiiviitä, helppolukuisia ja avoimia dokumentteja, joissa kuvataan henkilötietojen käsittely [10]. Tietosuojaseloste on kattavampi kuin rekisteriseloste, koska siinä määritellään myös rekisteröidyn oikeudet ja kerrotaan niiden toteuttamisesta [14]. Tietosuojaseloste on näin ollen GDPR:n kannalta suotavampi selostemuoto kuin rekisteriseloste. Rekisteri- ja tietosuojaselosteita kannattaa yhdistellä rekisterityyppien mukaan selostetyön helpottamiseksi. Tällaisia rekisterityyppejä voivat olla esimerkiksi henkilöstö-, asiakastieto-, kumppani- ja kameravalvontarekisterit.

Tietotilinpäätös on rekisterinpitäjän laatima vapaaehtoinen raportti, joka antaa kokonaisvaltaisen kuvan organisaation tietojenkäsittelystä. Raportti on tarkoitettu erityisesti johdon ja hallinnon työkaluksi sekä lisäämään sidosryhmien luottamusta organisaatiota kohtaan [10].

Tietosuojavastaava voi olla rekisterinpitäjän tai henkilötietojen käsittelijän henkilöstön jäsen, mutta rekisterinpitäjä voi palkata myös yrityksen ulkopuolelta tietosuojavastaavan, jolloin hänen tehtävänsä perustuu palvelusopimukseen. Tietosuojavastaava muun muassa neuvoo ja ohjaa yritystä asetuksen velvollisuuksien täyttämisessä, kouluttaa käsittelyyn osallistuvaa henkilökuntaa, seuraa asetuksen noudattamista ja tekee yhteistyötä valvontaviranomaisen kanssa [21].

Tietosuojaviranomaisia ovat tietosuojavaltuutettu ja tietosuojalautakunta. He valvovat asetuksen noudattamista. Valvontaviranomaisten on tehtävä yhteistyötä keskenään, jotta asetuksen soveltaminen on yhdenmukaista kaikkialla EU:ssa [13, artikla 51].

Tietosuojaviranomaisista koostuva WP29 *(Working Party 29)* on työryhmä, joka on perustettu direktiivin 95/46/EY artiklan 29 mukaan. Työryhmän tehtävä on esimerkiksi jakaa ohjeistuksia asetuksen tulkinnan helpottamiseksi [14].

2.3 Suostumus

Rekisterinpitäjän tulee saada suostumus rekisteröidyltä tämän henkilötietojen käsittelyyn ja rekisterinpitäjän on myös pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen. Asetuksen mukaan alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta, mutta jäsenvaltioilla on mahdollisuus soveltaa myös alempaa ikärajaa, jolloin se voi olla alimmillaan 13 vuotta [13, artikla 8 kohta 1]. Suomessa ikäraja sijoittunee 13−15 ikävuoden välille [23]. Suostumuksen ikäraja on hyvä huomioida esimerkiksi peliteollisuudessa, koska suuri osa pelaajista on alle 16-vuotiaita.

Henkilön antama suostumus ei saa olla edellytys palveluiden käytölle [14]. Tästä syystä henkilötietojen arvo noussee jatkossa palveluntarjoajien silmissä entisestään. Tulevaisuudessa henkilötietoja voitaneen käyttää ”valuuttana” eli henkilö voinee saada esimerkiksi laajemman palvelukokonaisuuden käyttöönsä jostakin palvelusta antaessaan omia henkilötietojaan palveluntarjoajan käyttöön.

Kun työntekijä aloittaa työsuhteen, ei häneltä tarvita erikseen suostumusta henkilötietojen asianmukaiseen käsittelyyn työnantajan toimesta [19]. Mutta jos tietoja käsitellään millään tavalla poikkeuksellisesti, tulee työnantajalla olla siihen työntekijältä erillinen suostumus. Tällainen tilanne voisi olla esimerkiksi, jos työnantaja tarvitsisi uuteen kulunvalvontajärjestelmään jo palveluksessa olevan työntekijöiden sormenjäljet luodakseen heille kulkuoikeuksia. Uuden työntekijän suostumus tähän asiaan kannattaa hankkia jo tekemällä asiasta maininta työsopimukseen. Yrityksen kannattaa tässä tilanteessa vielä pohtia kyseistä kulunvalvontajärjestelmää, sillä sormenjälki on biometristä tietoa, joka kuuluu erityisiin tietoryhmiin. Erityisiin tietoryhmiin kuuluvat henkilötiedot lisäävät rekisterinpitäjän vastuutaakkaa.

2.4 Käsittely

Henkilötietojen käsittelyä ovat kaikenlaiset toiminnot, joita henkilötietoihin kohdistetaan [10]. Henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti ja rekisteröidyn kannalta läpinäkyvästi [15]. Läpinäkyvyysperiaate pystytään osoittamaan esimerkiksi rekisteri- ja tietosuojaselosteiden avulla, jos käsittely kuvataan niissä mahdollisimman selkeästi ja tarkasti. Rekisteröidyn on tällöin myös helpompi luottaa yritykseen, jolle hän on aikeissa luovuttaa henkilötietonsa.

Säilytyksen rajoittamisperiaate tarkoittaa sitä, että henkilötietoja säilytetään ainoastaan niin kauan kuin on tarpeen muodossa, josta rekisteröity on tunnistettavissa. Henkilötietoja voidaan säilyttää pidempiä aikoja, jos niitä käsitellään yleisen edun mukaisia arkistointitarkoituksia varten. Myös tieteelliset tai historialiset tutkimustarkoitukset sallivat henkilötiedoille pidemmän säilytysajan [15]. Henkilötietojen elinkaarta ohjaavat myös erilaiset lait ja säädökset, jotka saattavat mennä tietosuoja-asetuksen edelle tulkinnassa, ellei asetus ole tuonut niihin mukanaan muutoksia. Työnantajan on noudatettava joitakin erityissäännöksiä myös henkilötietojen säilyttämisaikoja ajatellen. Tällaisia säännöksiä ovat esimerkiksi työsopimuslaki, työaikalaki ja kirjanpitolaki (taulukko 1).

TAULUKKO 1. Esimerkkejä henkilötietoaineiston säilytysajasta (www.finlex.fi)

Laki	**Henkilötietoaineisto**	**Säilytysaika (vähintään)**	**Lähteen kohta**
Työsopimuslaki (55/2001)	Työtodistus	10 vuotta	luku 6 § 7
Työaikalaki (605/1996)	Tehdyt työtunnit ja suoritetut korvaukset työtunneista	2 vuotta	luku 7 § 37-38
Kirjanpitolaki (1336/1997)	Tilinpäätös, toimintakertomus, kirjanpidot, tililuettelo sekä luettelo kirjanpidosta ja aineistosta	10 vuotta	luku 2 § 10
	Tilikauden tositteet ja liiketapahtumia koskeva kirjeenvaihto	6 vuotta	

Asetuksessa tulee noudattaa täsmällisyysperiaatetta. Tämä tarkoittaa sitä, että henkilörekistereissä olevien tietojen tulee olla ajantasaisia ja oikeellisia [14]. Rekisteröidyn oikeus tehdä oikaisupyyntö auttaa myös rekisterinpitäjää täsmällisyysperiaatteen toteuttamisessa, koska tällöin rekisteröity itse ilmoittaa ajantasaiset tietonsa. Rekisterinpitäjän tulee

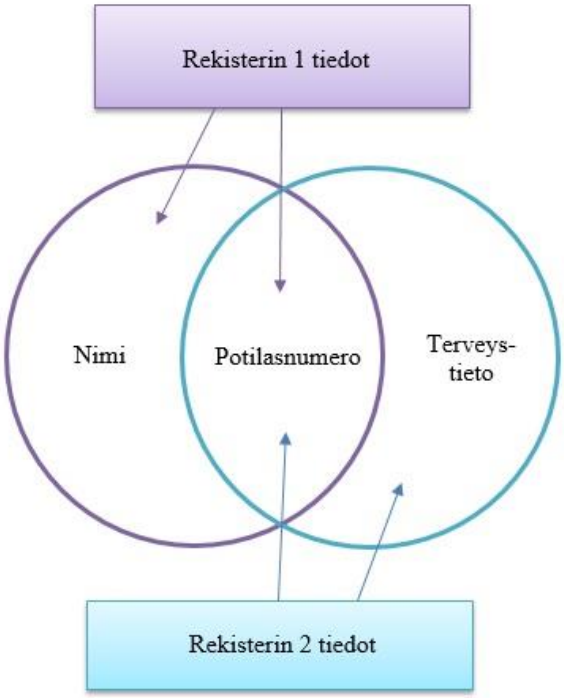
poistaa virheellisiksi havaitut tiedot rekisteristä. Minimointiperiaate toteutuu, kun säilytettävien henkilötietojen määrä on asianmukainen ja rekistereissä säilytetään vain olennaista tietoa. Tietojen tulee siis olla tarpeellisia suhteessa niihin tarkoituksiin, joita varten niitä käsitellään [15]. Henkilötietojen käsittelyn tulee olla myös käyttötarkoitussidonnaista eli tietoja saa käyttää ainoastaan niihin tarkoituksiin, joihin ne on aikanaan kerätty [13, artikla 5, kohta 1b].

Henkilötietoja tulee käsitellä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus eli puhutaan tiedon eheydestä sekä luottamuksellisuudesta. Rekisterinpitäjän tulee huolehtia, että henkilötietoja suojataan luvattomalta ja lainvastaiselta käsittelyltä. Tulee varmistaa myös, että tieto ei pääse vahingossakaan vääristymään eli häviämään, tuhoutumaan tai vahingoittumaan [15].

Käsittelyä on sekä manuaalista että automaattista käsittelyä. Manuaalinen käsittely tarkoittaa fyysisen henkilörekisterin käsittelyä. Tällainen tilanne tulee esiin esimerkiksi silloin, kun työntekijä saa messuilta käyntikortin ja päättää säilyttää sen. Myös mapissa olevien papereiden käsittely on manuaalista käsittelyä. Automaattista käsittelyä on esimerkiksi profilointi, jossa arvioidaan tai analysoidaan henkilötietojen perusteella henkilön ominaisuuksia. Analysoinnissa keskitytään usein erityisesti henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin tai kiinnostuksen kohteisiin, sijaintiin tai liikkeisiin liittyviin asioihin [20]. Profilointia on käytetty esimerkiksi sellaisessa tilanteessa, kun rekisteröity on etsinyt internetistä vuokramökkiä tulevaa hiihtolomaa ajatellen. Poistuttuaan mökkisivustolta jollekin muulla sivustolle, kuten Facebookiin, saattaa sinnekin ilmestyä vuokramökkimainoksia. Tällaisessa tilanteessa on käytetty profilointia, joka perustuu rekisteröidyn kiinnostuksen kohteisiin. Työnantajan ominaisuudessa profilointia ei tule tehdä.

Arkaluontoisten henkilötietojen käsittely voidaan tehdä turvallisemmaksi hyödyntämällä pseudonymisointia. Pseudonymisoimisella tarkoitetaan henkilötietojen käsittelyä niin, että henkilötietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaisessa tilanteessa lisätiedot tulee säilyttää erillään ja niihin voidaan soveltaa esimerkiksi teknisiä toimia, joilla varmistetaan, ettei henkilötietojen ja luonnollisen henkilön yhdistämistä tapahdu [13, artikla 4 kohta 5]. Pseudonymisointia voidaan hyödyntää vaikkapa terveyskeskuksissa, kun potilaasta halutaan käyttää nimen sijaan potilasnumeroa terveystiedon yhteydessä. Tällöin toisessa rekisterissä lukee nimi ja potilasnumero,

kun taas toisessa rekisterissä lukee potilasnumero ja terveystieto. Henkilön nimeä ei voida siis yhdistää terveystietoon, koska ne sijaitsevat eri rekistereissä. Rekistereiden välillä tulee olla jokin salausavain tai vastaava salaustapa, jotta kukaan valtuuttamaton henkilö ei pääse yhdistämään nimeä ja terveystietoa (kuvio 1).



KUVIO 1. Esimerkki pseudonymisoinnista

3 REKISTERÖIDYN OIKEUDET

Rekisteröidyllä on tiedollisia oikeuksia omiin henkilötietoihinsa. Nämä oikeudet tarkoittavat parempaa tietosuojaa rekisteröidyn henkilötiedoille sekä mahdollisuutta kontrolloida sitä, mitä tietoja hänestä missäkin yhteydessä käsitellään. Rekisterinpitäjillä on kuukausi aikaa vastata rekisteröidyn pyyntöihin, mutta mikäli pyyntö on monimutkainen tai niitä on ollut määrällisesti paljon, voidaan harkita kahden kuukauden lisäaikaa [21]. Rekisterinpitäjän tulee antaa rekisteröidyn pyytämät tiedot sähköisesti luettavassa muodossa ja rekisteröidyn toiveesta myös kirjallisesti. Rekisteröidyllä on myös oikeus tehdä valitus valvontaviranomaiselle, mikäli hänen oikeuksiensa toteutumisessa ilmenee ongelmia [14].

3.1 Tarkastusoikeus ja tietojen oikaisemisoikeus

Tarkastusoikeuden mukaan rekisteröidyllä on oikeus saada tietoa omista henkilötiedoistaan ja niiden säilytyksestä. Mikäli rekisterinpitäjä kieltäytyy antamasta rekisteröidyn pyytämiä tietoja, tulee hänen antaa tästä rekisteröidylle kirjallinen todistus, josta tulee ilmetä syyt tarkastusoikeuden epäämiselle. Ainakin kulutusasiakkaalle tietojen tarkastaminen on ilmaista kerran vuodessa [14]. Oikaisupyynnöllä rekisteröity saa virheelliset henkilötietonsa korjattua oikeiksi. Rekisterinpitäjän on oikaistava tiedot ilman aiheetonta viivytystä. Oikaisu voidaan tehdä esimerkiksi niin, että rekisteröity toimittaa rekisterinpitäjälle lisäselvityksen epätarkoista tai virheellisistä henkilötiedoistaan [13, artikla 16].

3.2 Siirto-oikeus

Rekisteröidyllä on oikeus siirtää tietonsa palveluntarjoajalta toiselle. Rekisteröity voi pyytää rekisterinpitäjältä saada tietonsa yleisesti käytössä olevassa siirtomuodossa, jonka jälkeen hän voi itse toimittaa ne toiselle rekisterinpitäjälle. Rekisteröidyn halutessa tiedot voidaan toimittaa myös automaattisesti järjestelmästä toiseen, mikäli se on teknisesti mahdollista [20].

3.3 Vastustamisoikeus

Asetus takaa rekisteröidylle oikeuden vastustaa henkilötietojensa käsittelyä. Vastustamisoikeuden avulla rekisteröidyn on entistä helpompaa kieltäytyä esimerkiksi suoramarkkinoinnista. Rekisteröidyn käyttäessä vastustamisoikeuttaan rekisterinpitäjä ei saa enää käsitellä kyseisiä henkilötietoja, mutta asetuksessa määritellään kuitenkin edellytykset myös käsittelykiellosta poikkeamiseen [14].

3.4 Automatisoidut yksittäispäätökset

Automatisoidut yksittäispäätökset eivät saa perustua erityisiin tietoryhmiin kuten esimerkiksi rekisteröidyn poliittiseen mielipiteeseen. Automatisoidut yksittäispäätökset tarkoittavat sitä, että jokin automaattinen sovellus tekee päätöksiä luonnollisen henkilön puolesta sovellukseen syötettyjen tietojen perusteella. Rekisteröidyllä on asetuksen mukaan oikeus vaatia, että hänen tietojaan käsittelee rekisterinpitäjän lukuun toimiva luonnollinen henkilö, jolla on valtuudet esittää oma kantansa sovelluksen päättämään asiaan ja jonka on mahdollista riitauttaa sovelluksen tekemä päätös [14].

3.5 Henkilötietojen poisto rekisteristä

GDPR:n mukaan henkilöllä on oikeus tulla ”unohdetuksi” eli kun rekisteröity haluaa henkilötietonsa poistettavan, tulee rekisterinpitäjän poistaa tiedot rekisteristä ilman aiheetonta viivytystä, lukuun ottamatta tilanteita, joissa on olemassa jokin laillinen peruste tietojen säilyttämiseen. Jokin seuraavista poistoa edellyttävistä perusteista tulee aina täyttyä, jotta rekisterinpitäjä voi poistaa henkilötiedot rekisteristään:

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joihin ne on alun perin kerätty.
- Rekisteröity peruuttaa suostumuksensa.
- Rekisteröity vastustaa käsittelyä eikä käsittelyyn ole olemassa perusteltua syytä.
- Henkilötietoja on käsitelty lainvastaisesti.
- Henkilötiedot on poistettava EU:n oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan lakisääteisen velvoitteen noudattamiseksi.
- Henkilötiedot on kerätty alle 16-vuotiaalta tietoyhteiskunnan palvelujen tarjoamisen yhteydessä [13, artikla 17 kohta 1].

4 REKISTERINPITÄJÄN VELVOLLISUUDET

Yrityksen tulee varautua GDPR:n noudattamiseen tekemällä pakolliset muutokset tietosuojadokumentaatioon, joka koskee esimerkiksi asiakassopimuksia, palvelusopimuksia, käyttöehtoja sekä rekisteri- ja tietosuojaselosteita. Osoitusvelvollisuutta noudatettaessa tulee ottaa huomioon myös sisäisten toimintamallien, dokumentaation ja vaikutusarvioinnin käyttöönotto. Yrityksen tulee pohtia myös, miten huomioida tietojärjestelmissään käyttöoikeuksien jakaminen. Jatkossa yrityksellä on velvollisuus ilmoittaa tietoturvaloukkauksista, jolloin yrityksellä tulee olla valmiudet tietoturvaloukkauksen havaitsemiseen, niistä ilmoittamiseen sekä vahinkojen minimoimiseen [4]. GDPR:n tuomien haasteiden lisäksi yritysten on hyvä huomata asetuksen noudattamisen olevan myös myyntivaltti. Yritys voinee jatkossa todistaa asiakkailleen ja yhteistyökumppaneilleen olevansa luotettava yhteistyökumppani esimerkiksi suorittamalla tietosuoja-asetus sertifikaatin.

Yrityksessä on todella tärkeää huomata, milloin yritys on rekisterinpitäjä ja milloin käsittelijä, jotta vastuunjaosta ollaan selvillä. Rekisterinpitäjä on se taho, joka tallentaa henkilötiedot rekisteriin ja on siis viimekäden vastuussa rekisterin sisältämistä tiedoista. Yritys on käsittelijä, jos kyseiselle yritykselle luovutetaan henkilötietoa jossakin kumppanuussuhteessa. Tällainen tilanne on kyseessä esimerkiksi, kun työvaateyritys saa asiakasyritykseltä heidän henkilöstönsä nimiä ja vaatekokoja työvaatetilauksen yhteydessä. Tällöin asiakasyritys on rekisterinpitäjä ja työvaateyritys käsittelijä. Työterveyden kohdalla tilanne on hieman monimutkaisempi, sillä yritys on rekisterinpitäjä luovuttaessa työntekijän tietoja työterveydelle, joka toimii tässä tilanteessa käsittelijänä. Mutta työterveydestä tulee rekisterinpitäjä, kun se muodostaa työntekijästä terveystietoa, jota taas yritys ei saa käyttöönsä [25].

Rekisterinpitäjän ja käsittelijän välille tulee tehdä GDPR-artiklan 28 mukainen palvelusopimus, josta selviää käsittelyn kohde, kesto, luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityneiden ryhmät sekä rekisterin pitäjän velvollisuudet ja oikeudet [13]. Sopimuksessa kuvataan myös esimerkiksi, miten rekisteröidyn oikeuksien kohdalla tietojen tarkastuksen, oikaisun ja poiston kanssa toimitaan yrityksessä [21]. Jo olemassa olevia palvelusopimuksia ei kuitenkaan tarvitse GDPR:n myötä hävittää, vaan useimmissa tapauksissa GDPR:n osuus tehdään liittämällä sopimusliite valmiiseen sopimukseen. Pal-

velusopimuksella siis varmistetaan, että palveluntarjoaja käsittelee rekisterinpitäjän ylläpitämiä henkilötietoja rekisterinpitäjän haluamalla tavalla. Henkilötiedot saattavat yhteistyön merkeissä kulkeutua vielä eteenpäin palveluntarjoajan alihankkijalle, jolloin taas palveluntarjoaja on vastuussa siitä, että myös heidän alihankkijansa käsittelee henkilötietoja rekisterinpitäjän antaman ohjeistuksen mukaisesti [23]. Myös salassapitosopimusten on syytä olla kunnossa, kun käytetään palveluntarjoajia ja näiden alihankkijoita.

4.1 Nykytilan arviointi

Tietosuoja-asetuksessa käytetään riskipohjaista lähestymistapaa, joka tarkoittaa, että henkilötietojen käsittelyyn liittyvät riskit rekisteröidyn oikeuksille ja vapauksille on arvioitava etukäteen ennen käsittelyn aloittamista. Yrityksen kannattaakin tehdä tämän vuoksi lähtötilanteen arviointi eli PIA *(Privacy Impact Assessment)*, jonka kautta yritys pääsee myös paremmin tutustumaan GDPR:n muihin vaatimuksiin. PIA on tietosuojan arviointimenetelmä, jonka avulla voidaan tehdä yrityksen jonkinasteinen nykytilan arviointi GDPR:n kannalta. Yrityksen kannattaa selvittää ainakin, mitä henkilötietoja heillä käsitellään, onko käsittely GDPR:n mukaista, miten rekisteröidyille tiedotetaan heidän tietojensa käsittelystä sekä mitä toimintatapoja, prosesseja ja dokumentteja tulee muuttaa tai luoda asetuksen myötä [4].

4.2 Vaikutusarviointi

Yleisesti ottaen vaikutusarvioinnin eli DPIA:n *(Data Protection Impact Assessment)* tekeminen on vapaaehtoista, mutta tietyissä tapauksissa arvion tekeminen on pakollista. EU:n tietosuojavaltuutettujen työryhmä (WP29) on antanut ohjeistuksen, jonka mukaan DPIA on tehtävä, mikäli henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin henkilön oikeuksien ja vapauksien kannalta. Ohjeistuksen mukaan arvioinnissa on otettava huomioon muun muassa seuraavia seikkoja:

- arviointi tai pisteytys (esimerkiksi rekisteröidyn työsuorituksen analysointi)
- automaattinen päätöksenteko, jolla on merkittäviä vaikutuksia rekisteröidylle
- systemaattinen valvonta julkisilla paikoilla
- arkaluontoisten tietojen käsittely
- laajamittainen tietojen käsittely

- tietojen yhdistäminen useammasta lähteestä
- heikommassa asemassa olevien rekisteröityjen tietojen käsittely (esimerkiksi lapset ja työntekijät)
- uusien teknologioiden käyttöönottaminen
- tietojen siirto EU:n ulkopuolelle tai
- jos rekisteröidyn on tietojen käsittelyn johdosta hankalampi käyttää oikeuksiaan [2].

WP29:n kannanoton mukaan jo kahden yllä mainitun tunnusmerkin täyttyminen tarkoittaa todennäköistä korkeaa riskiä tietojen käsittelyä ja näissä tapauksissa DPIA on laadittava [2]. Yrityksen on tehtävä DPIA ennen tietojen käsittelyn aloittamista ja WP29 suosittelee DPIA:n tekemistä jo ennen 25.5.2018 aloitettavan soveltamisen alkamista, vaikka DPIA koskeekin niitä prosesseja, jotka aloitetaan vasta asetuksen voimaantulon jälkeen. DPIA:n tulee sisältää minimissään seuraavat asiat:

- kuvaus käsittelytoimista ja tarkoituksista
- arvio käsittelyn tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden
- arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä
- kuvaus suunnitelluista toimenpiteistä riskeihin puuttumisen suhteen [2].

4.3 Osoitus- ja ilmoitusvelvollisuudet

Rekisterinpitäjän on huolehdittava, että kaikkia tietosuoja-asetuksen periaatteita noudatetaan jokaisessa henkilötietojen käsittelyvaiheessa. Osoitusvelvollisuuden myötä rekisterinpitäjän on jatkossa pystyttävä osoittamaan toimivansa tietosuoja-asetuksen mukaisesti, kun aiemmin riitti vain asian sanallinen toteaminen. Osoitusvelvollisuus edellyttää myös, että yritys huolehtii henkilötietojen käsittelyssään seuraavista periaatteista: lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tarkoituksellisuus, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus [10]. Yritys voi osoittaa toteuttavansa edellä mainittuja osa-alueita tekemällä esimerkiksi kattavan tietotilinpäätöksen.

Rekisterinpitäjällä on myös ilmoitusvelvollisuus, jonka mukaan rekisterinpitäjän tulee ilmoittaa tietoturvaloukkauksista tietosuojaviranomaiselle ja loukatuille rekisteröidyille.

Tietosuojaviranomaiselle tulee tehdä ilmoitus 72 tunnin sisällä loukkauksen havaitsemisesta sekä rekisteröityneille ilman aiheetonta viivytystä ja loukkauksen vakavuus huomioiden [23].

4.4 Rekisteröidyn oikeuksiin vastaaminen

Rekisterinpitäjän yksi tärkeimmistä velvollisuuksista on rekisteröidyn oikeuksien toteuttaminen. Eli mikäli rekisteröity tekee esimerkiksi tarkastuspyynnön, on rekisterinpitäjän velvollisuus vastata tähän pyyntöön kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella, mikäli pyyntö on monimutkainen tai niitä on määrällisesti paljon [21]. Rekisterinpitäjän on tehtävä ilmoitus rekisteröidylle viimeistään kuukauden kuluessa tietopyynnön saamisesta, mikäli tietopyynnössä esitettyjä toimenpiteitä ei voida toteuttaa. Ilmoituksessa tulee kertoa syyt tietopyynnön toteuttamatta jättämiselle sekä opastaa rekisteröityä halutessaan tekemään asiasta valitus valvontaviranomaiselle [13, artikla 12]. Rekisterinpitäjän on varmistettava rekisteröidyn henkilöllisyyden oikeellisuus ennen tietojen luovuttamista [21].

4.5 Rekisteri- ja tietosuojaseloste

Rekisterinpitäjän tulee laatia henkilötietolain (523/1999) mukaan yleisesti saatavilla oleva rekisteri- tai tietosuojaseloste, joka on tiivis ja helppolukuinen dokumentti, jossa kerrotaan

- kuka on rekisterinpitäjä
- kuka on rekisterin yhteyshenkilö
- mitä henkilötietoja rekisterissä on
- mikä henkilötietojen käsittelyn tarkoitus on
- miten henkilötiedot ovat suojattu
- tietojen säilytysaika
- minne henkilötietoja sääntöjenmukaisesti luovutetaan [14].

Tietosuojaseloste on rekisteriselostetta laajempi seloste, jossa kerrotaan yllä mainittujen seikkojen lisäksi rekisteröidyn oikeuksista ja niiden toteutumisesta [14]. GDPR:n näkökulmasta tietosuojaseloste on parempi vaihtoehto kuin rekisteriseloste. Malliesimerkki

tietosuojaselosteesta löytyy liitteestä 1 [5, 14]. Erityisesti selosteen harmaat kohdat ovat tarkoitettu muokattavaksi yrityksen tarpeen mukaan.

Tietosuojaselosteita kannattaa tehdä henkilörekisterityypeittäin kuten esimerkiksi henkilöstö-, asiakastieto-, kumppani-, jäsen- ja kameravalvontarekisteriseloste. Tämä helpottaa selostetyötä, kun esimerkiksi jokaiseen Exceliin tai vastaavaan henkilörekisteriin ei tarvitse tehdä omaa selostetta, vaan voidaan hyödyntää yhtä selostepohjaa kaikkiin saman rekisterityypin henkilörekistereihin. Selosteiden kohdalla on hyvä muistaa myös monistettavuus, kun joitakin samoja lauseita voidaan käyttää useammassakin eri selosteessa. Tämä helpottaa yrityksen tietosuojatyötä. Helpotusta tietosuojatyöhön saadaan, kun kirjoitetaan tietosuojaseloste muotoon, jossa rekisteröidyn oikeuksista kerrotaan, mutta samalla pyritään kuitenkin minimoimaan tulevien tietopyyntöjen määrä ja niistä aiheutuva työ.

4.6 EU:n ulkopuolinen käsittely

Henkilötietoja tulee säilyttää EU/ETA -alueella, jotta tietosuojan taso on varmasti sovitulla tasolla eli uuden tietosuoja-asetuksen mukainen. EU/ETA-alueen ulkopuolella on kuitenkin olemassa myös riittävän tietosuojatason maita, joissa on komission mielestä riittävän kattava tietosuojan taso. On myös olemassa niin sanottuja ”kolmansia maita”, joissa taas tietosuojan taso ei ole komission mielestä tarpeeksi korkea [14]. Lähtökohtaisesti asetus kieltää henkilötietojen siirrot EU:n ulkopuolelle ”kolmansiin maihin”, mikäli vastaanottajamaa ei tarjoa riittävää tietosuojan tasoa [22].

4.6.1 Milloin henkilötietoa siirtyy EU:n ulkopuolelle?

Henkilötietoja voidaan todeta siirretyksi EU:n ulkopuolelle esimerkiksi tutkimalla mobiilisovellusten henkilötietojen käyttöä ja sitä, minne kaikkialle tiedot leviävät. Tutkimus voidaan tehdä ohjelmalla, joka pyrkii analysoimaan, mihin tietoja päätyy. Tutkimuksissa on huomattu, että suurin osa sovellusten käytössä olevista palvelimista sijaitsee Yhdysvalloissa ja näin ollen tietoa siirtyy myös sinne. Henkilötietoa saattaa siirtyä EU:n ulkopuolelle myös, jos yrityksestä siirretään henkilötietoja eri pilvipalveluihin, joiden palve-

limia sijaitsee myös EU:n ulkopuolella olevissa konesaleissa. Jos sovellusten ja palveluiden tarjoajilla ei ole riittäviä sopimuksia EU:n ulkopuolella sijaitsevan kumppaniyrityksen kanssa, on kysymys laittomasta tietojen siirrosta tai luovutuksesta [11]. Siirto ja luovutus eroavat siinä mielessä, että luovutuksen yhteydessä toinen yritys myös vastaanottaa tiedot. Siirron kohdalla tietoja ei oteta haltuun.

4.6.2 Privacy Shield -järjestelmä

Yhdysvalloissa yritykset ovat voineet hyödyntää *EU-U.S. Privacy Shield* -järjestelmää henkilötietojen siirtämiseen EU-alueelta Yhdysvaltoihin. *Privacy Shieldiä* noudattavien yhdysvaltalaisten yritysten etu on se, että jos henkilötietoja halutaan siirtää EU:sta Yhdysvaltoihin, ei siihen tarvita enää erillistä lupaa. Yhdysvalloissa sijaitsevan yrityksen on rekisteröidyttävä Yhdysvaltojen kauppaministeriössä ja sitouduttava noudattamaan *Privacy Shield* -ehtoja sekä pystyttävä osoittamaan ehtojen noudattaminen, jotta se voi hyödyntää *Privacy Shield* -järjestelmää. Järjestelmään kuuluvien yritysten tulee noudattaa myös eurooppalaisten tietosuojavaltuutettujen antamia lausuntoja ja päätöksiä EU:sta tulleita henkilötietoja käsitellessään [8].

4.7 Sertifikaatit

Jäsenvaltiot, valvontaviranomaiset, tietosuojaneuvosto ja komissio kannustavat ottamaan käyttöön erilaisia sertifiointimekanismeja, tietosuojasinettejä ja -merkkejä, joiden tarkoitus on osoittaa rekisterinpitäjän ja henkilötietojen käsittelijöiden noudattavan asetusta suorittaessaan henkilötietojen käsittelyä. Sertifiointien tulee olla vapaaehtoisia ja läpinäkyvän menettelyn perusteella helposti saatavilla. Sertifiointeja myöntävät artiklassa 43 mainitut sertifiointielimet tai toimivaltaiset valvontaviranomaiset. Sertifiointi myönnetään enintään kolmeksi vuodeksi ja se voidaan peruuttaa, mikäli sertifiointia koskevat vaatimukset eivät enää täyty [13, artikla 42].

4.8 Sanktiot

GDPR-rikkomuksesta voi seurata sanktio, jonka suuruus riippuu rikkomuksen vakavuudesta. Maksimirangaistus GDPR-asetusten rikkomisesta voi olla jopa 20 miljoonaa euroa tai neljä prosenttia yrityksen edellisen tilikauden globaalista liikevaihdosta, mikäli sen osuus on suurempi kuin 20 miljoonaa euroa. Tällaiset sakot ovat monelle yritykselle niin suuria, että ne voivat ajaa yrityksen jopa konkurssiin [21]. Suomessa ennen rahallisia sanktioita GDPR-rikkomuksesta lienee mahdollista saada varoitus, huomautus, sertifioinnin peruuttaminen tai käsittelyn keskeytysmääräys. Sen sijaan esimerkiksi Saksassa voidaan siirtyä suoraan sakkorangaistukseen, eli sanktioiden suhteen jokaisessa jäsenvaltiossa toimittaneen omaan lainsäädäntöön tai käytäntöön pohjautuen [23]. Asetuksen artiklassa 83 todetaan, että valvontaviranomaisten on GDPR-rikkomusten kohdalla arvioitava hallinnollisten sanktioiden suuruus niin, että se on kussakin yksittäisessä tapauksessa tarpeeksi tehokas, oikeasuhteinen ja varottava [14].

5 TIETOSUOJAVASTAAVA

Tietosuojavastaava on yrityksen johdon tietosuojan erityisasiantuntija. Tietosuojavastaavan ja yrityksen johdon välille tulisi muodostua mutkaton yhteistyösuhde. Johdon tulisi olla tietosuojavastaavalle helposti lähestyttävä elin, koska tietosuojavastaavan tehtävänä on antaa asiantuntija-apua erityisesti johtoportaaseen [21]. Myös yrityksen muu henkilöstö on tärkeää sitouttaa noudattamaan asetusta, jotta rikkomukset eivät johdu ainakaan asian jalkauttamisen puutteesta.

Vaikka tietosuojavastaava toimiikin asiantuntijana yrityksen tietosuoja-asioissa, on vastuu asetuksen noudattamisesta kuitenkin aina viimekädessä rekisterinpitäjällä. Tietosuojavastaavalla on riippumaton asema yrityksessä ja hänet tulee ottaa mukaan kaikkiin tietosuojaa koskeviin kysymyksiin. Tietosuojavastaavaa ei saa erottaa tai rangaista tehtäviensä hoitamisen vuoksi [21].

Tietosuojavastaava voi kuulua yrityksen henkilökuntaan, käsittelijäyrityksen henkilökuntaan tai rekisterinpitäjä voi myös ulkoistaa tietosuojavastaavan tehtävät. Mieluiten tietosuojavastaava on kuitenkin joku yrityksen omasta henkilökunnasta, koska tällöin tietosuojavastaava tietää parhaiten, miten kyseisen yrityksen eri osa-alueilla toimitaan tietosuojaa ajatellen. Jos yritys kuitenkin päätyy ottamaan ulkopuolisen konsultin toimimaan tietosuojavastaavana, voi tämä henkilö olla koulutukseltaan esimerkiksi juristi tai tietoturva-asiantuntija [23]. Tietosuojavastaavan pätevyysvaatimuksiin kuuluu tietosuojalainsäädännöntuntemus, lain vaatimusten soveltamistaito ja alan käytäntöjen tuntemus [21]. Rekisterinpitäjän tai henkilötietojen käsittelijän on julkistettava nimitetyn tietosuojavastaavan yhteystiedot rekisteröityjen saataville sekä ilmoitettava ne valvontaviranomaiselle [15].

5.1 Tarve ja nimittäminen

Rekisterinpitäjän tulee nimittää tietosuojavastaava aina, kun tietojen käsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään toteuttava tuomioistuin. Tietoturvavastaava pitää olla nimitetty myös, jos rekisterinpitäjän tai käsitteli-

jän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Myös käsittelyn kohdistuessa erityisiin tietoryhmiin, rikoksiin tai rikostuomioihin, tulee yrityksen nimittää tietosuojavastaava [15].

5.2 Tehtävät

Tietosuojavastaavalla on monta tehtävää. Hänen tehtäviinsä yrityksen tietosuojatyössä kuuluu esimerkiksi

- asetuksen vaatimusten täyttymisen valvonta
- rekisterinpitäjän neuvonta ja ohjaus kaikissa tietosuoja-asioissa
- dokumentaation laadinnan, saatavuuden ja säilytyksen valvonta
- DPIA:n tekemisen tukeminen ja valvonta
- yhteistyö valvontaviranomaisen kanssa
- henkilökunnan koulutus tietosuojan osalta
- rekisteröidyn oikeuksien toteutumisen valvonta [21].

6 GDPR-SOVELLUKSET

Yrityksistä ja organisaatioista löytyy monesti paljon henkilötietoa ja sitä on niin hallitussa kuin strukturoimattomassakin muodossa. Tämä tuottaa haasteita erityisesti tiedon hallittavuuden kannalta. GDPR:n näkökulmasta yrityksen on helpoin päästä selville sisältämästään tietomäärästä tietoinventaarion avulla. Tietoinventaariossa listataan yrityksen tietojärjestelmiä, niissä sijaitsevaa tietoa, käyttöoikeuksia, suojaustapoja ja niin edelleen. Tietoinventaarion tekeminen on työlästä ja sitä tehdessä saattaa silti jäädä jotain asioita huomaamatta, vaikka tietoja listataankin muistiin.

Ohjelmointiyritykset ovat lanseeranneet yrityksille työkalusovelluksia helpottamaan tietoinventaarion, tietotilinpäätöksen ja ylipäätään tietosuojatyön tekemistä, koska kyseessä on jatkuva prosessi eikä 25.5.2018 mennessä valmiiksi saatava kertaluontoinen projekti. GDPR-sovelluksen myyminen on varsin helppoa, koska asetus koskee käytännössä jokaista yritystä. Sovellusten kesken kilpailua on toistaiseksi vielä aika vähän, vaikka Suomen markkinoilta joitakin pilvipalveluna toimivia GDPR-sovelluksia löytyykin. GDPR-sovellusten käyttö tullee vielä jatkossa yleistymään entisestään, kun loputkin yritykset ja organisaatiot havahtuvat siihen, että GDPR koskee myös heitä. Tämä johtanee todennäköisesti myös siihen, että kilpailevia sovelluksia valmistuu lisää. Kappaleessa tutustutaan kahteen eri GDPR-sovellukseen, joita ovat Microsoftin Compliance Manager Preview ja Agendiumin Tietosuojamalli.

6.1 Compliance Manager Preview

Microsoft on julkaissut Compliance Manager Preview -nimisen tietosuojasovelluksen Microsoft Cloud -palveluiden käyttäjille [26]. Opinnäytetyön aikana sovelluksesta oli tarjolla vasta tutustumiskäyttöön tarkoitettu *preview*-versio. Compliance Manager Preview tarjoaa työkalun GDPR:n sekä esimerkiksi ISO 27001- ja ISO 27018-standardien noudattamiseen [9]. Sovellus muodostaa reaaliaikaisen riskiarvion käyttäjän Microsoft Cloud -palveluista sekä ohjaa käyttäjää toimimaan niissä GDPR-määräysten mukaisesti [26].

Sovellus aukeaa *Review Frameworks* -nimiseen osioon, josta näkee yrityksen käytössä olevien Microsoftin pilvipalveluiden tietosuojatyön nykytilan. Yritys voi luoda tähän osioon esimerkiksi Office 365 -palvelua koskevan GDPR-osuuden. GDPR-osuuden sisältä löytyy *Managed Controls* -osio, josta löytyy GDPR-artikloita. Microsoft hallinnoi suurinta osaa artikloiden toteuttamisesta *(Microsoft Managed Controls)*, mutta loput jäävät käyttäjien toteutettaviksi *(Customer Managed Controls)*. Sovelluksessa on mahdollista rajata käyttäjäoikeudet *Managed Controls* -osioon [26].

Customer Managed Controls -osio sisältää ohjeita artikloiden toteuttamista varten. Käyttäjä voi vastuuttaa *Assign Task* -työkalun avulla toisia käyttäjiä toteuttamaan ohjeiden mukaisia toimia. *Assign Task* -työkalulla lähetetään toiselle käyttäjälle tehtäväviesti, jonka prioriteetiksi voidaan valita korkea, keskitaso tai matala. Tämän jälkeen *Assign Task Notes* -kohtaan voidaan kirjoittaa, mitä toisen käyttäjän odotetaan tekevän tehtävän suhteen. Tehtävien tekoon käytetään muita Microsoft palveluita kuten esimerkiksi *Advanced Data Governance* -palvelua. Kun tehtävän kaikki kohdat on saatu tehtyä, sen toimivuutta pyydetään testaamaan [26].

Käyttäjä näkee hänelle osoitetut tehtävät *Action Items* -osiosta. Käyttäjä voi lähettää tehtävän osoittaneelle käyttäjälle viestin, kun on toteuttanut tehtävän. Viestin liitteeksi on mahdollista lähettää tiedosto (*Evidence File*), jossa on tehtävän suorittamiseen liittyvää todistusaineistoa. Tehtävän osoittanut käyttäjä tutkii viestin ja tiedoston sisällöt, jonka jälkeen hän voi merkitä tehtävän toteutetuksi. Tehtävälle voidaan kirjata testauspäivämäärä, jonka jälkeen testaus merkitään joko onnistuneeksi tai epäonnistuneeksi. Sovelluksen muodostaman dokumentaation voi muuntaa Excel-muotoiseksi raportiksi [26].

Sovellus tarjoaa koosteen yrityksen tietosuojasta ja asetuksen noudattamisesta sekä tarjoaa niihin kehitysehdotuksia. Sovelluksen ohjeet ovat kuitenkin vain suosituksia, eivätkä ne takaa, että yrityksen tietosuojatyö on tehty täysin asetuksen mukaisesti [26].

6.2 Tietosuojamalli

Ohjelmistoyritys Agendium Oy lanseerasi markkinoille GDPR-sovelluksen, joka kantaa nimeä Tietosuojamalli. Sovellus tarjoaa tietosuojasuunnitelma-työkalun, jolla yrityksen

on helpompi käynnistää tietosuojatyön tekeminen. Se sisältää myös tietosuojaoppaan, joka tarjoaa ohjeita jokaisessa työvaiheessa [1].

Sovelluksessa vastataan yrityksen tietosuojaan liittyviin kysymyksiin ja näistä vastauksista muodostuu dokumentaatiota, josta yrityksen on helppo nähdä oman tietosuojatyönsä eteneminen. Sovelluksesta on nähtävissä esimerkiksi erilaisia aihekokonaisuuksia, joiden värikooditus kertoo, kuinka paljon huomiotasi mikäkin aihe vaatii. Lisäksi työvaiheille löytyy prosenttimittari, josta ilmenee, kuinka valmiiksi mikäkin työvaihe on saatu.

Koska henkilötietojen käsittely koskee koko yritystä, tarjoaa Tietosuojamalli ratkaisun myös vastuiden jakoon. Sovelluksessa pystytään nimeämään vastuuhenkilö kullekin aihealueelle ja henkilön on ”Minun työni”-näkymän avulla helpompi nähdä, millä mallilla hänen osuutensa yrityksen tietosuojatyöstä on. Sovellus kerryttää myös tapahtumalokia, josta on nähtävissä kuka on tehnyt, mitä ja milloin. Sovelluksen tarjoamat kommenttikentät helpottavat yhteistyötä eri asioiden parissa [1].

Sovellusta käyttämällä on helpompi ymmärtää, mikä GDPR:ssä on oleellista ja mitä toimenpiteitä asetuksen noudattaminen vaatii yritykseltä [1]. Tietosuojamalli koettiinkin varsin kattavaksi ja selkeäkäyttöiseksi GDPR-sovellukseksi.

7 TIETOSUOJATYÖ

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee pystyä osoittamaan, että yrityksen toiminnassa huomioidaan tietosuoja-asetus ja että asetuksen sääntöjä noudatetaan. Tietotilinpäätös on hyvä keino asetuksen noudattamisen osoittamiseen [14]. Lisäksi yrityksen tietosuojatyötä helpottavat tietosuojaorganisaation perustaminen sekä viestintäsuunnitelman pohtiminen.

7.1 Tietotilinpäätös

Tietotilinpäätöksen on tarkoitus toimia erityisesti johdon työkaluna tukien yrityksen tehokkuutta, vaikuttavuutta ja kilpailukykyä. Tietotilinpäätös on osa tietojohtamista ja yritys pystyy sen avulla näyttämään, että se noudattaa tietosuoja-asetusta, hyvää tietojenkäsittelytapaa ja hyvää tiedonhallintatapaa. Tietotilinpäätöksen tekeminen on vapaaehtoista, mutta erittäin suotavaa, sillä sen avulla yritys pystyy näyttämään sidosryhmilleen, että se pitää parempaa huolta tietosuoja- ja tietoturvasta-asioista kuin mitä GDPR:n vähimmäisvaatimukset edellyttävät [14]. Yritys pysyy myös paremmin ajan tasalla omien tietosuoja-asioidensa suhteen, kun se tekee tietotilinpäätöksen. Tietotilinpäätös vastaa yritykselle muun muassa seuraaviin kysymyksiin:

- mitä henkilötietoja yrityksessä käsitellään
- mihin yrityksen hallussa olevia tietoja käytetään
- mitä menettelytapoja ja periaatteita tietojen käsittelyssä noudatetaan
- miten tiedot on suojattu
- miten tietojen käyttöä valvotaan
- miten rekisteröityjen oikeudet toteutetaan [14].

7.1.1 Tietojen käsittely

Tietotilinpäätöksessä on hyvä kuvata esimerkiksi tietojenkäsittelyyn vaikuttavaa keskeistä lainsäädäntöä ja yrityksen toimintaperiaatteita tietosuoja-asetusta ajatellen. Yrityksen kannattaa mainita myös henkilötietojen käsittelyn ulkoistettuihin palveluihin liittyvistä menettelytavoista ja palvelusopimuksista. Lisäksi on syytä arvioida henkilötietojen

elinkaarta, käyttöoikeushallintaa sekä sähköiseen tiedonsiirtoon liittyviä tietosuoja- ja tietoturvavaatimuksia [14].

7.1.2 Tietojen suojaus

Tietotilinpäätöksessä voidaan arvioida tietojen suojauksen osalta esimerkiksi siihen liittyviä periaatteita ja menettelytapoja. Huomion arvoista on mainita, kuinka rekisterinpitäjä toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi. Myös tietoturvaan liittyvistä keskeisistä tavoitteista, toteutuskeinoista ja sen hallintaan liittyvistä noudatettavista standardeista on hyvä tehdä kuvaus. Lisäksi olisi hyvä pohtia asiaa riskienhallinnan ja kehittämisprosessien osalta [14].

7.1.3 Käsittelyn seuranta ja valvonta

Yrityksen täytyy varmistaa, että heillä noudatetaan ja valvotaan hyvälle tietojenkäsittely- sekä tiedonhallintatavalle annettuja ohjeita ja säännöksiä. Valvonnan tuloksia ja niiden perusteella tehtyjen toimenpiteiden arvioiminen on myös suotavaa. Käsittelyn seurannan ja valvonnan osalta tietotilinpäätöksessä voidaan arvioida esimerkiksi tietojen käsittelyyn kohdistuvia riskejä ja niiden hallintaa, tietojen käsittelyprosessien valvontaa sekä yhteistyökumppaneiden tietojen käsittelytoimenpiteiden valvontaa. Valvonnan ja seurannan perusteella voidaan arvioida myös mahdollisia kehittämistoimia [14].

7.1.4 Rekisteröityjen oikeuksien toteutuminen

Rekisteröityjen oikeuksien toteutumista on mahdollista arvioida henkilötietolain (523/1999) mukaisten tarkastusoikeus- ja oikaisuoikeuspyyntöjen sekä niihin annettujen vastausten lukumäärän perusteella. Myös rekisteri- ja tietosuojaselosteiden saatavuutta on syytä arvioida, koska sekin saattaa vaikuttaa oikeuspyyntöjen määrään [14].

7.1.5 Johtopäätökset ja kehittämiskohteet

Tietotilinpäätöksellä pystytään tekemään johtopäätöksiä esimerkiksi siitä, ovatko tietojen käsittely ja toiminta olleet hyvän tietojenkäsittely- ja tiedonhallintatavan mukaisia sekä onko käsittelyn seuranta ja valvonta ollut lainsäädännön, määräysten ja sisäisen ohjeistuksen mukaista [14]. Tietotilinpäätös tuo esiin myös ne osa-alueet, joissa on kehittämisen varaa. Jatkossa yrityksen tulisi arvioida, mitä ratkaisuja näihin kehittämiskohteisiin on tarjolla. Suppea esimerkki kuvitteellisen Testiyritys Oy:n tietotilinpäätöksestä löytyy liitteestä 2 [14, 16]. Testiyritys Oy:n tietotilinpäätöksestä näkee hieman, mitä tietotilinpäätös voisi esimerkiksi pitää sisällään. Tietotilinpäätöksestä on lähes mahdoton tehdä mitään yleispätevää mallia, koska sen sisältö on riippuvainen muun muassa yrityksen toimialasta ja koosta.

7.2 Tietosuojaorganisaatio

Tietosuojan valvonnan ja toteuttamisen helpottamiseksi yrityksen kannattaa koota henkilöstöstään tietosuojaorganisaatio. Yhden vastuuhenkilön olisi työlästä olla tietoinen koko yrityksen tietosuojan tasosta, joten vastuun jakaminen on erittäin järkevää. Tietosuojaorganisaatioon voidaan valita vastuuhenkilöitä eri yksiköistä esimerkiksi asiakaspalvelusta, henkilöstöhallinnosta, palvelutuotannosta, myynnistä, markkinoinnista ja IT-yksiköstä. Tietosuojaorganisaation tavoitteena on tuoda tietosuojatyö osaksi yrityksen operatiivista toimintaa [20]. Organisaatio kokoontuisi tietyin väliajoin keskustelemaan tietosuojan sen hetkisistä kuulumisista sekä tulevaisuuden näkymistä, jotta yritys toteuttaisi jatkossakin mahdollisimman hyvin niin GDPR:n vaatimukset kuin muutkin tietosuojaan ja -turvaan liittyvät asiat. Vaikka tietosuojaorganisaatio perustettaisiinkin, niin on ensiarvoisen tärkeää, että myös yrityksen johto sitoutetaan asetuksen noudattamiseen.

7.3 Viestintäsuunnitelma

Rekisterinpitäjällä on velvollisuus vastata rekisteröidyn oikeuksiin, kuten esimerkiksi tarkastuspyyntöön [21]. Pyyntöjen määrää on tässä vaiheessa vielä vaikea arvioida, mutta jokaisen yrityksen kannattaa varautua siihen, että pyyntöjä todennäköisesti tulee. Helpoin

tapa varautua tähän on valita yrityksestä vastuuhenkilö, joka vastaa pyyntöihin. Vastuuhenkilöitä voidaan tarvittaessa nimetä useampikin, esimerkiksi jokaiselle rekisterityypille omansa. Yrityksessä voidaan myös tehdä valmiiksi mallipohjia, joita rekisteröidyt täyttävät pyyntöjä esittäessään sekä myös mallipohjia, joiden avulla vastuuhenkilö voi helposti vastata pyyntöihin. Toinen mahdollinen helpotus yritykselle on avata oma sähköpostiosoitteensa pyyntöjä ja kyselyitä varten, jotta yksittäisten työntekijöiden työsähköpostit eivät täyttyisi erilaisista pyynnöistä. Tällainen GDPR-sähköposti voisi olla esimerkiksi muotoa gdpr@yritys.fi tai privacy@yritys.fi.

Rekisterinpitäjällä on myös ilmoitusvelvollisuus mahdollisista tietoturvaloukkauksista [4]. Tietoturvaloukkausten varalle on hyvä tehdä valmiiksi suunnitelma siitä, kuka ilmoittaa asiasta ja kenelle sekä myös se, miten asiasta ilmoitetaan. On hyödyllistä tehdä myös tietoturvaloukkauksesta ilmoittamiseen tarkoitettu mallipohja etukäteen, joka sitten täytetään, kun loukkaus havaitaan. Loukkauksen havaitsemisen jälkeen yrityksellä on 72 tuntia aikaa ilmoittaa valvontaviranomaiselle loukkauksen tapahtuneen [23]. Mallipohjassa on hyvä olla täytettävät kohdat esimerkiksi sille mitä on tapahtunut, milloin loukkaus on havaittu, milloin loukkaus on tapahtunut ja mitä arvioidaan loukkauksen riskeiksi.

8 TIETOSUOJA JA -TURVA

Tämä kappale ottaa kantaa tietosuojaan ja -turvaan sekä fyysisestä että digitaalisesta näkökulmasta. GDPR:n osalta hyvän tietosuojan vaatimukset selviävät vasta helmikuussa, kun WP29 antaa niistä määritelmät julki [24], mutta kunnollisia tietosuojatoimia kannattaa muodostaa ja ylläpitää jo määritelmiä odotellessakin. Omalla henkilöstöllä kannattaa esimerkiksi teetättää salassapitosopimukset, mutta lisäksi voidaan tehdä myös turvallisuusselvitykset, joita on kolmea eri tasoa; suppea, perusmuotoinen ja laaja. Taso valitaan suojattava tieto ja tehtävän merkitys huomioiden. Turvallisuusselvitettävän henkilön antama kirjallinen suostumus on ehdoton edellytys selvityksen tekemiselle. Turvallisuusselvitykset tekee suojelupoliisi [12].

8.1 Fyysinen osuus

Yrityksen tietosuojan ja -turvan osalta on tärkeää muistaa myös fyysinen turvallisuus. On huolehdittava, että fyysisesti säilytettävät henkilötiedot ovat suojattu asianmukaisella tavalla. Fyysiset henkilörekisterit kuten esimerkiksi mapit tulee säilyttää lukollisessa kaapissa, joka sijaitsee lukitussa huoneessa. Huoneen ja kaapin avaimet tulisi olla vain sellaisten henkilöiden hallussa, joiden kuuluu työtehtäviensä puolesta päästä käsittelemään kyseisiä tietoja.

Fyysisiä henkilötietoja voi lisäksi löytyä esimerkiksi käyntikortteina ja kirjepostina. Kirjepostin kohdalla tulisi huolehtia, että postihuone on lukittu ja mieluummin vielä käytettäisiin lukollisia postilokeroita, joihin jälleen avaimet olisivat vain asianosaisilla. Fyysisten palvelimien tulee myös olla asianmukaisesti suojattu lukolliseen tilaan, johon vain tietyillä henkilöillä on pääsyoikeus. Tietosuojan kannalta olisi hyvä pohtia myös kulkulupia eli kuka pääsee ja minne pääsee. Yrityksen kannattaisi kaikkineen toteuttaa sellaista tietoturvapolitiikkaa, jossa tietoihin pääsee käsiksi vain ne työntekijät, joiden työtehtävien suorittaminen sitä vaatii.

8.2 Digitaalinen osuus

Ensimmäisenä digitaalisten henkilötietojen suojaamisessa kannattaa lähteä liikkeelle siitä, että työntekijät lukitsevat tietokoneensa aina poistuessaan niiden ääreltä. Tietokoneissa tulee olla myös vahvat salasanat, joissa on vähintään 12 merkkiä ja ne sisältävät kirjaimia (isoja ja pieniä), numeroita ja erikoismerkkejä. Samaa salasanaa ei tulisi käyttää missään muualla, ja se olisi hyvä vaihtaa aina tietyin väliajoin uuteen. Tietojärjestelmissä yleensäkin tulee käyttää vahvoja salasanoja ja järjestelmien käyttöoikeuksia on tärkeä ryhmittää

Kannettavia tietokoneita käyttävien työntekijöiden kannattaa hankkia kannettaviinsa tietoturvasuojat. Tietoturvasuojan avulla henkilö voi tehdä esimerkiksi junassa istuessaan töitä kannettavallaan ilman, että vieressä istuva matkustaja voi nähdä näytöllä lukevia asioita. Kannettavissa tietokoneissa on myös huolehdittava kirjautumisen kohdalla vahvoista salasanoista. Myös kannettavien salaus on suotavaa. Tänä päivänä myös älypuhelimet sisältävät usein yhtälailla salaista tietoa kuin tietokoneet, mutta kuitenkin niiden salaaminen on monesti jäänyt paljon kevyemmälle tasolle. Yritysten kannattaa kiinnittää myös tähän huomiota.

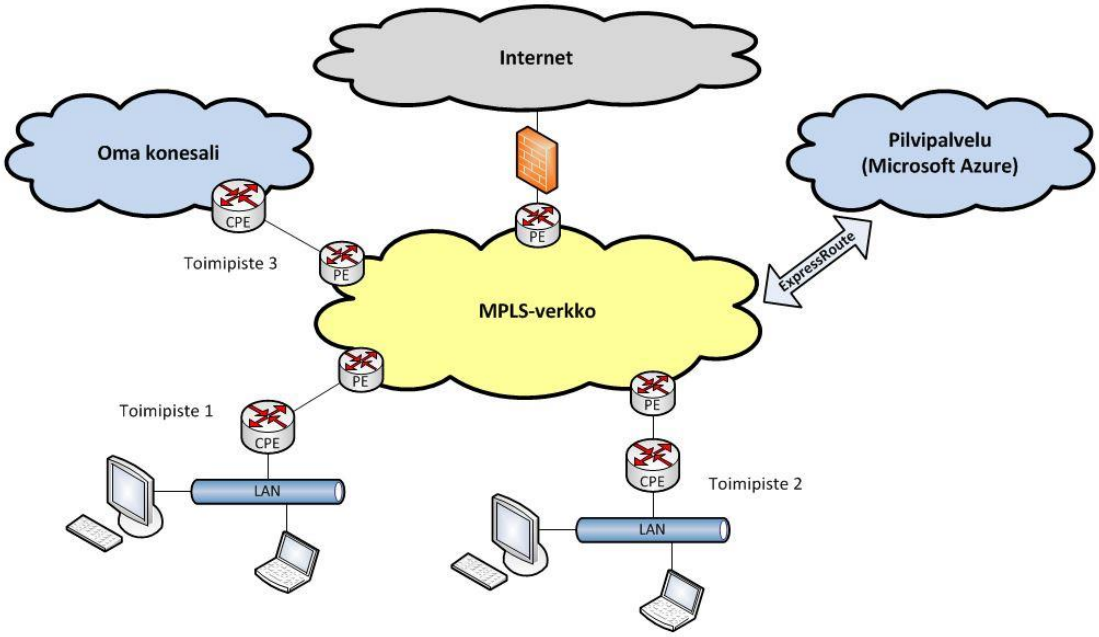
Etätyöskentely on hyvin vahvasti tätä päivää, mutta siihenkin kannattaa yritysten vetää raja, että etätöitä ei tehtäisi omilla henkilökohtaisilla laitteilla. Jo pelkästään katsellessa sähköposteja saattaa henkilökohtaiselle koneelle latautua yrityksen salaista tietoa. Ja koska henkilökohtaisten tietokoneiden ynnä muiden laitteiden tietoturvan tasosta ei ole takeita, voi yrityksen salainen tieto päästä sitä kautta vääriin käsiin.

Yrityksen käytössä olevat muistitikut on hyvä olla kryptattu, mikäli ne sisältävät henkilötietoa. Muistitikkuja voi ostaa valmiiksi kryptattuina tai kryptaus voidaan tehdä ohjelmistoa apuna käyttäen. Muistitikun kryptaamiseen soveltuvia ohjelmia ovat esimerkiksi Encryptstick, BitLocker tai VeraCrypt. Myös muistitikun sisällä olevat tiedostot voidaan kryptata esimerkiksi 7-Zip -ohjelmalla, jos koko muistitikkua ei haluta kryptata.

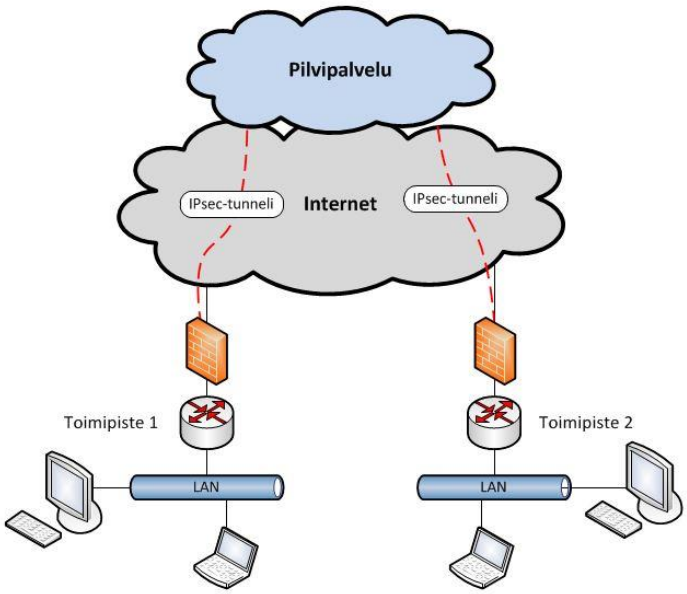
Tietojärjestelmissä tulee myös käyttää vahvoja salasanoja ja järjestelmien käyttöoikeuksia on tärkeä ryhmittää eri käyttöoikeustasoille niin, että järjestelmien osioita pääsevät käyttämään vain ne työntekijät, joiden työtehtävät sitä edellyttävät. Tähän liittyen tulisi

myös muistaa poistaa yrityksen palveluksesta poistuvan henkilön käyttöoikeudet ja kulkuluvat, kerätä avaimet sekä tehdä muut poistuvan työntekijän toimenpiteet, jotta tietosuoja ei pääsisi tätäkään kautta vaarantumaan.

ICT-infrastruktuurin suunnitteleminen tietoturvalliseksi on ensiarvoisen tärkeää. Palvelimien hallintayhteys tulisi toteuttaa tietoturvallisella protokollalla kuten SSH:lla. Olisi myös toivottavaa, että yhteys käyttäjältä palvelimelle tapahtuisi suljetun MPLS-verkon kautta (kuvio 2), eikä internetin yli. Yrityksen verkossa olisi myös hyvä olla asianmukainen palomuuri, jossa on vain tarvittavat avaukset verkkoon. Mikäli yhteys kuitenkin kulkisi internetin yli, tulisi yhteyden olla toteutettu riittävän turvatusti esimerkiksi IPsec-protokollalla (kuvio 3) ja vähintään SHA-2 -salausalgoritmilla.



KUVIO 2. Suljetun verkon ICT-infrastruktuuri



KUVIO 3. Internetiä hyödyntävä ICT-infrastruktuuri

Myös yrityksen sisäverkon tietoturva on hyvä ottaa huomioon. Yritysverkon seinärasioita ei tulisi sijoittaa paikkoihin, joihin ulkopuolisilla saattaa olla pääsy. Yritysverkon kytkinportit tulisi olla *access*-portteja, joissa käytettäisiin Port Securitya, jotta ulkopuoliset eivät pääsisi yritysverkkoon käsiksi kyseisten porttien kautta. Porteissa voisi käyttää esimerkiksi MAC-rajoitusta, DHCP snoopingia ja BPDU Guardia. MAC-rajoituksella rajataan portin käyttäminen vain tietyille laitteille tai tietylle määrälle laitteita. DHCP snoopingilla estetään verkkoon kuulumattomien IP-osoitteiden jakaminen hyökkääjän tietokoneelta, tällöin vältytään *man-in-the-middle* -hyökkäyksiltä. BPDU Guardilla estetään tuntemattomien kytkinten liittäminen verkkoon.

Jos yrityksessä haluttaisiin siirtyä vielä yllä mainittuja keinoja turvallisempaan ratkaisuun, voisi yritys käyttää IEEE 802.1X -standardia eli porttikohtaista todentamista, jolla estetään luvaton kommunikointi kytkinporttien tai langattoman yhteyden kautta. IEEE 802.1X -standardia käytettäessä verkkoon liittyvä käyttäjä autentikoidaan esimerkiksi sertifikaatilla, jonka vuoksi hyökkääjän pääsy verkkoon on entistä vaikeampaa.

9 POHDINTA

Opinnäytetyössä tutkittiin uuden EU:n yleisen tietosuoja-asetuksen vaikutusta yrityksen tietosuoja- ja tietoturvatyöhön. Opinnäytetyön aikana haastateltiin useita yrityksiä, joiden avulla opittiin paljon hyödyllistä tietoa suomalaisten pk-yritysten tietosuojatyöstä. Haastateltujen yritysten tietosuojatyössä huomattiin erilaisia vahvuuksia ja heikkouksia, joita hyödynnettiin opinnäytetyössä koostamalla ohjeistus yritysten tietosuojatyön parantamiseksi.

Opinnäytetyön päätavoite oli tehdä tietosuoja-asetuksesta selkeä ja tiivis tietopaketti, jota yritykset voisivat hyödyntää omassa tietosuojatyössään. Tämän tavoitteen täyttyminen jää vielä nähtäväksi. Tavoitteena oli myös neuvoa teknisen osuuden toteuttamisessa sekä opastaa tietosuojaselosteiden ja tietotilinpäätöksen tekemisessä. Nämä tavoitteet täyttyivät suhteellisen hyvin. Oppimiselle asetetut tavoitteet saavutettiin, ja opinnäytetyön aihe opetti kirjoittajalle paljon uutta tietoa, jota on mahdollista hyödyntää myös työelämässä. Aiheen ajankohtaisuus auttanee myös työllistymisessä.

Opinnäytetyön aikana haasteeksi osoittautui asetuksen tulkinnanvaraisuus. Asetus tulee todennäköisesti saamaan lisää tarkennuksia kevään 2018 aikana, joten moni kirjoitushetkellä tulkinnan varassa ollut asia saattaa vielä muuttua suuntaan tai toiseen. Tämä toi tietyllä tapaa haastetta myös opinnäytetyön luotettavuudelle. Opinnäytetyössä yritettiinkin tästä syystä ilmaista epävarmat asiat säännönmukaisessa potentiaalissa, jotta lukija ei omaksuisi niitä faktoina. Tietotilinpäätöksen tekemisestä löytyi myös suhteellisen vähän malliesimerkkejä, jonka vuoksi oman malliesimerkin muodostaminen havaittiin hieman haasteelliseksi.

LÄHTEET

1. Agendium. GDPR-sovellus. Luettu 23.11.2017
   www.tietosuojamalli.fi

2. Antti-Pekka Keränen. Julkaistu 31.5.2017. Vaikutusarviointi. Luettu 29.11.
   www.lawly.fi

3. Ari Andreasson. Yleistä tietoa asetuksesta. Luettu 4.12.2017
   www.opitietosuojaa.fi

4. Asianajotoimisto Castrén & Snellman. Nykytilan arviointi. Luettu 29.11.2017
   www.castren.fi

5. GDPRtech. Tietosuojaseloste. Luettu 4.12.2017
   https://gdprtech.com

6. Henkilötietolaki 523/1999. Luettu 25.11.2017
   www.finlex.fi

7. Kirjanpitolaki 1336/1997. Luettu 4.12.2017
   www.finlex.fi

8. Merilampi. Julkaistu 8.9.2016. Siirrot EU:sta Yhdysvaltoihin. Luettu 22.11.2017
   www.merilampi.com

9. Microsoft. Compliance Manager Preview is now available. Luettu 10.12.2017
   https://techcommunity.microsoft.com

10. Ohjelmistoyrittäjät ry. Sanasto ja materiaalit. Luettu 7.11.2017
    www.gdpr.fi

11. Panu Pökkylä. Julkaistu 18.4.2017. Henkilötietojen sijainti. Luettu 30.11.2017
    https://jit2015.fi/2017/04/18

12. Poliisi. Turvallisuusselvitys. Luettu 8.12.2017
    www.poliisi.fi

13. Privacy Regulation. Asetuksen kaikki artiklat. Luettu 7.11.2017
    www.privacy-regulation.eu

14. Tietosuojavaltuutetun toimisto. Yleistä tietoa asetuksesta. Luettu 9.11.2017
    www.tietosuoja.fi

15. Tietosuojatieto. Yleistä tietoa asetuksesta. Luettu 28.11.2017
    www.tietosuojatieto.fi

16. Trafi. Tietotilinpäätös 2016. Luettu 7.12.2017
    www.trafi.fi

17. Työ- ja elinkeinoministeriö. Julkaistu 26.9.2008. Työelämän tietosuoja. Luettu 19.11.2017
www.tem.fi

18. Työaikalaki 605/1996. Luettu 4.12.2017
www.finlex.fi

19. Työsopimuslaki 55/2001. Luettu 4.12.2017
www.finlex.fi

20. Valtiovarainministeriö. Tietosuojaorganisaatio ja EU-tietosuojan kokonaisuudistus. Luettu 5.12.2017
www.vahtiohje.fi

21. Verkkoasema. GDPR pikaopas. Luettu 9.11.2017
www.verkkoasema.fi

22. Ville Vainio. Julkaistu 25.5.2016. Henkilötietojen siirrot EU:sta. Luettu 4.12.2017
www.tietosuojauutiset.fi

23. Ville Vainio. Alson GDPR-webinaari. Kuultu 29.11.2017
https://alsofi.play.livearena.com

24. Ville Vainio, Asianajotoimisto Applex Oy. Skype-haastattelu. 14.11.2017

25. Ville Vainio, Asianajotoimisto Applex Oy. Haastattelu. 7.12.2017

26. Compliance Manager preview demo. Julkaistu 16.11.2017. Video. Office Videos. Katsottu 10.12.2017
https://www.youtube.com/watch?v=-ScjtTIOnQs&feature=youtu.be

LIITTEET

Liite 1. Tietosuojaselosteen esimerkkipohja

Tietosuojaseloste	
Laatimispäivä: [pp.kk.vvvv]	
Henkilörekisterin nimi:	[Asiakasrekisteri]
[Yritys] käsittelee henkilötietoja GDPR:n mukaisesti huomioiden myös nykyisen henkilötietolain (523/1999, luku 10 § 24). Tietosuojaselostetta saatetaan ajoittain muuttaa julkaisemalla siitä uusi versio, joten ole hyvä ja tarkista seloste säännöllisesti. Tietosuojaseloste on tehty artiklaan 30 pohjautuen.	
Rekisterinpitäjä:	[Yrityksen nimi] [Y-tunnus] [Osoite] [Puhelinnumero]
Rekisteriasioista vastaava henkilö:	[Yrityksen nimi] [Nimi] [Titteli] [Sähköposti] [Puhelinnumero]
[Yrityksen] toiminnassa käsitellään henkilötietoja artiklan 32 periaatteiden mukaisesti. Käsittely on lainmukaista, kohtuullista ja läpinäkyvää. Tietoa käsitellään käyttötarkoitussidonnaisesti, tiedon tallentaminen on minimoitu ja tiedot on pyritty pitämään täsmällisinä. Käsittelyssä huomioidaan tiedoille määrätyt säilytysajat, joiden ylittyessä tiedot poistetaan joko automaattisesti tai manuaalisesti, ellei säilytyksen jatkamiselle ole lakiin perustuvaa syytä. [Yritys] tallentaa vain ehyttä ja luotettavaa tietoa.	
Kerättävät tiedot:	[Nimi, puhelinnumero, sähköposti]
Tietolähteet:	[Asiakas itse, julkinen rekisteri]
Tietojen käyttötarkoitukset:	[Markkinointi jne.]
Säännönmukaiset luovutukset ja siirrot EU:n ulkopuolelle:	[Emme luovuta tietoja eteenpäin EU:n ulkopuolelle.] / [Luovutamme tietoja vain luotettaville yhteistyökumppaneille, joiden kanssa on tehty asianmukaiset sopimukset henkilötietojen käsittelyn suhteen.]

Tietojen suojaus:	[Manuaalissessa muodossa olevat henkilötiedot säilytetään lukituissa huoneissa, joissa on lukitut kaapit. Huoneisiin ja kaappeihin on pääsy vain niillä henkilöillä, joiden työtehtävät sitä edellyttävät. Digitaalisessa muodossa olevat henkilötiedot on suojattu vahvoilla salasanoilla, rajatuilla käyttöoikeuksilla sekä salatuilla yhteyksillä ja sähköposteilla.]
Tietojen säilytysaika:	[Henkilötietoja säilytetään vain lakien määrittelemä aika. Tähän kuvataan lait, jotka rekisterissä olevia henkilötietoja koskevat.]
Rekisteröidyllä on oikeus saada tietonsa tarkastettavaksi ja oikaistavaksi. Rekisteröity voi myös pyytää tietojensa siirtämistä toiseen järjestelmään, pyytää niiden poistamista tai vastustaa tietojensa käsittelyä. [Yrityksessä] suhtaudutaan vakavasti rekisteröidyn oikeuksiin ja tietopyyntöihin vastataan asetuksen määrittelemän ajan sisällä, ellei laissa ilmene jotakin estettä tälle. Rekisterinpitäjä varmentaa tietopyynnön yhteydessä rekisteröidyn henkilöllisyyden.	

Liite 2. Esimerkki tietotilinpäätöksestä

Esimerkki kuvitteellisen Testiyritys Oy:n suppeasta tietotilinpäätöksestä.

Tietotilinpäätös 2016
Laatimispäivä: 31.1.2017
Yritys: Testiyritys Oy
GDPR *General Data Protection Regulation* on uusi EU:n laajuinen tietosuoja-asetus, jonka soveltaminen alkaa 25.5.2018. Uusi tietosuoja-asetus parantaa luonnollisen henkilön henkilötietojen yksityisyyttä sekä henkilön oikeuksia omiin tietoihinsa. GDPR:n myötä henkilötietojen käsittelyn sääntely yhtenäistyy saman asetuksen koskiessa kaikkia EU/ETA-jäsenmaita. GDPR edistää myös EU:n digitaalisia sisämarkkinoita ja se tulee myös kumoamaan nykyisen EU:n henkilötietodirektiivin 95/46/EY. Uuden asetuksen mukaan rekisterinpitäjän on jatkossa pystyttävä konkreettisesti osoittamaan, että uudet tietosuojasäännökset on huomioitu yrityksen toiminnassa. [2016/679]
Keskeiset käsitteet Henkilötiedoksi luetaan kaikki tunnistettu tai tunnistettavissa oleva luonnolliseen henkilöön liitettävä tieto, kuten nimi, osoite, puhelinnumero, sähköpostiosoite, henkilötunnus, IP-osoite, rekisteritunnus, kuva, sijaintitieto ja pankkitieto. Erityisiä henkilötietoryhmiä ovat henkilön rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveystietoja, biometrisiä tietoja, geneettisiä tietoja tai seksuaaliseen käyttäytymiseen liittyviä tietoja. Rekisteröity on henkilö, jonka henkilötietoja käsitellään. Asetus vaatii, että rekisteröidyltä tulee olla saatu suostumus, ennen kuin hänen henkilötietojaan käsitellään. Henkilörekisteri on henkilötietoja sisältävä tietojoukko. Henkilörekistereitä voivat olla esimerkiksi asiakastietorekisteri, työntekijätietorekisteri ja jäsenrekisteri. Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Käsittelijä voi olla luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka toimii rekisterinpitäjän toimeksiannosta henkilötietoja käsittelevänä tahona. [artikla 4]

Rekisterinpitäjän velvollisuudet

Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa (osoitusvelvollisuus), että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. Rekisterinpitäjällä on myös ilmoitusvelvollisuus, joka tarkoittaa sitä, että tietosuojaloukkauksen tapahtuessa, rekisterinpitäjän tulee ilmoittaa loukkauksesta valvontaviranomaiselle 72 tunnin kuluessa loukkauksen havaitsemisesta. Loukatuille rekisteröidyille tulee ilmoittaa loukkauksesta ilman turhaa viivytystä kuitenkin loukkauksen vakavuus huomioiden.

Rekisterinpitäjä on vastuussa ylläpitämänsä henkilörekisterin sisältämistä henkilötiedoista. Rekisterinpitäjän tärkeimpiä velvollisuuksia on toteuttaa rekisteröidyn oikeudet.

[Artikla 24]

Rekisteröidyn oikeudet

Rekisteröidyllä on oikeus tietojensa tarkastamiseen, oikaisuun, poistamiseen, rajoittamiseen ja siirtämiseen. Rekisteröidyn oikeudet antavat henkilölle myös mahdollisuuden vastustaa tietojensa käsittelyä, automatisoituja yksittäispäätöksiä ja profilointia.

Rekisteröidyllä on lisäksi oikeus läpinäkyvään informointiin koskien hänen henkilötietojaan ja niiden käsittelyä.

[Artiklat 12, 16, 17, 18, 19, 20, 21, 22]

Käsittely

Käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Käsittelyn tulee olla lainmukaista, kohtuullista, läpinäkyvää, käyttötarkoitussidonnaista, minimoitua, täsmällistä, aikarajoitettua, ehyttä ja luottamuksellista.

[Artiklat 4, 5]

Tietoinventaario

Testiyritys Oy:n työntekijärekisteri sisältää seuraavat henkilötiedot: nimi, puhelinnumero, osoite, sähköpostiosoite ja henkilötunnus.

Asiakastietorekisterit sisältävät seuraavat henkilötiedot: nimi, puhelinnumero ja sähköpostiosoite.

Henkilötietoa sijaitsee tietokonejärjestelmissä (ERP, CRM, AD), sähköposteissa (Outlook), työpuhelimissa ja fyysisesti paperina. Kaikki rekisterit on suojattu asianmukaisin keinoin.

Tietosuoja ja -turva

Testiyritys Oy:n tietoturvapolitiikka on johdon hyväksymä ja se on julkaistu henkilöstön sekä tietoja käsittelevien ulkopuolisten tahojen käyttöön. Tietoturvaprosessit, -ohjeet ja -riskien hallinta ovat välineitä, joiden avulla yrityksen hallussa oleva henkilötieto suojataan ja käsitellään asetettujen vaatimusten mukaisesti. Yritys suojaa rekisterissään olevia tietoja väärinkäytöksiltä muun muassa teettämällä palveluksessaan oleville henkilöille turvallisuusselvitykset. Tietoturvavastuista sovitaan työnantajan ja työntekijän välisissä työsopimuksissa. Henkilöstön tietoturvatietoutta ja -osaamista edistetään säännöllisillä tietoturvakoulutuksilla sekä ajoittaisilla tietoturvasta muistuttavilla viesteillä, joita lähetetään sähköpostitse tai yrityksen intranetissä. Esimies myöntää työntekijöilleen työtehtäviin perustuvat käyttö- ja pääsyoikeudet, joiden laajuutta arvioidaan säännöllisesti.

Järjestelmien, verkkojen ja tietoliikenteen osalta yrityksessä hyödynnetään erilaisia salausratkaisuja. Tietoturva-asiantuntijat huolehtivat yrityksen tietosuoja-asioista ja niitä käsitellään lisäksi tietosuojaorganisaation kokoontumisissa. Tarvittaessa tietosuoja-asioista keskustellaan myös yrityksen johdon kanssa. Vuonna 2016 yrityksessä tehtiin 10 järjestelmien tietoturva-auditointia. Lisäksi tehtiin 5 järjestelmiin kohdistuvaa lokitarkastusta.

Fyysiset henkilötiedot ovat suojattu lukollisiin huoneisiin, joissa on lukolliset kaapit. Lukkojen avaimet on luovutettu ainoastaan henkilöille, joiden työtehtävät sitä edellyttävät.

Tietoturvariskit kartoitetaan osana yrityksen riskienhallintaprosessia. Tietoturvariskejä arvioidaan ja niille nimetään vastuuhenkilöt. Tietojärjestelmiin kohdistuvia riskejä seuraa ICT-tietoturvatiimi. Riskienhallintaprosessia kehitetään parhaillaan, mutta sen on määrä valmistua ennen vuoden 2017 tietotilinpäätöstä.

[Trafi]

Yrityksen tietovirrat

Viranomaiset, joilta tietoa saadaan rekisteriin

Viranomainen	Vastaanotettava tieto
Verohallinto	Veroprosentti
Suojelupoliisi	Turvallisuusselvityksien sisällöt

Yksityiset tahot, joilta tietoa saadaan rekisteriin

Yksityinen taho	Vastaanotettava tieto
Henkilö itse	Nimi, osoite, puhelinnumero, henkilötunnus, pankkitieto

Julkisten tietojen luovutus		
Vastaanottava toimija	Hakutieto	Luovutettava tieto
Viranomaiset	Henkilötunnus	Syntymäaika
Salassa pidettävien tietojen luovutus		
Toimija	Tiedon käyttö	
Poliisi	Rikosasiat	
Tietojen luovutus muihin käyttötarkoituksiin		
Toiminta	Luovutettava tieto	
Tilastointi*	Tällä hetkellä emme tee luovutuksia tilastointiin.	
*Tietojen luovuttamisesta kyseistä käyttötarkoitusta varten säädetään henkilötietolaissa.		
Tietojen siirto EU:n tai ETA:n ulkopuolelle		
Luovutettava tieto		
Yritys luovuttaa tietoja ”kolmansissa maissa” sijaitseviin kumppaniyrityksiin vain heidän noudattaessaan GDPR:n asettamia vaatimuksia. Asiasta on tehty sopimukset ja sitoumukset kumppaniyritysten kanssa.		