TAMPEREEN
AMMATTIKORKEAKOULU

EU:N TIETOSUOJA-ASETUKSEN TOTEUTUMINEN ENERGIA-ALAN YRITYKSESSÄ

Katja Wallin

Opinnäytetyö
Huhtikuu 2018
Liiketalouden koulutusohjelma

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalouden koulutusohjelma

WALLIN, KATJA:
EU:n tietosuoja-asetuksen toteutuminen energia-alan yrityksessä

Opinnäytetyö 69 sivua, joista liitteitä 14 sivua
Huhtikuu 2018

Tässä opinnäytetyössä tarkasteltiin EU:n yleistä tietosuoja-asetusta (2016/679) sekä tutkittiin sen toteutumista energia-alan yrityksessä. Yleinen tietosuoja-asetus astuu voimaan toukokuun 25. päivänä 2018 ja tulee suoraan sovellettavaksi lainsäädännöksi koko Unionin alueella ilman, että sitä tarvitsisi erikseen säätää kansallisesti lailla. Opinnäytetyön tavoitteena oli perehtyä tietosuoja-asetuksen sisältöön sekä edesauttaa asetuksen toteutumista kyseisessä energia-alan yrityksessä. Tutkimuksen tarkoituksena oli selvittää, kuinka hyvin EU:n tietosuoja-asetukseen oli kohdeyrityksessä tällä hetkellä varauduttu sekä kartoittaa mitä mahdollisia toimenpiteitä seuraavaksi tulisi tehdä, jotta henkilötietojen käsittely toteutuisi uuden asetuksen vaatimusten mukaisesti.

Työn teoreettinen viitekehys nojaa pitkälti kansainväliseen sekä kansalliseen lainsäädäntöön, eritoten EU:n tietosuoja-asetukseen. Lähdeaineistona hyödynnettiin lisäksi muuta juridista aineistoa ja kirjallisuutta sekä lain säännösten nojalla annettuja tarkempia viranomaismääräyksiä ja ohjeita. Opinnäytetyön empiirisessä osassa tarkasteltiin tietosuoja-asetuksen toteutumista kohdeyrityksessä ja tuotiin esille havaittuja muutostarpeita yrityksen tietosuojakäytäntöihin liittyen. Tutkimuksen aineistonhankintamenetelminä käytettiin havainnointia sekä opinnäytetyön osana toteutettua kyselytutkimusta. Tutkimuksessa todettiin, että kohdeyrityksen tietosuojakäytännöt ja osaamisen taso eivät kaikilta osin vastanneet tietosuoja-asetuksen mukaisia vaatimuksia. Tämä johtui pitkälti tiedon puutteesta, joten kehitysehdotukset ja toimenpiteet pohjautuivat riittävän ohjeistuksen lisäämiseen.

EU:n yleinen tietosuoja-asetus tuo merkittäviä muutoksia organisaatioiden henkilötietojen käsittelyprosesseihin. Yritysten on jatkossa panostettava tietosuoja-asioihin, tai vastassa voi olla huomattava sakkorangaistus valvonnan kiristymisen seurauksena. Digitaalisen toimintaympäristön kehittyessä sekä palveluiden sähköistymisen myötä, uudelle asetukselle oli kuitenkin tarve, sillä nykyiset henkilötietojen suojaa ohjaavat säädökset perustuvat yli 20 vuotta vanhaan direktiiviin, jolloin sähköinen tiedon käsittely poikkesi huomattavasti nykyisestä. Muutosprosessi on työläs, mutta siihen kannattaa panostaa. Tulevaisuudessa tietosuojatietämys lisääntyy, ja tietosuojan toteutuminen tulee toimimaan yhtenä laatukriteerinä ja luotettavan kumppanin merkkinä. Tietosuoja-asiat kannattaa siis pikemminkin nähdä jatkossa yhtenä yrityksen kilpailuetuna.

Asiasanat: tietosuoja-asetus, Euroopan Unioni, tietosuoja, GDPR

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Administration

WALLIN, KATJA:
The Implementation of the EU General Data Protection Regulation in an Energy Company

Bachelor's thesis 69 pages, appendices 14 pages
April 2018

This thesis focused on the EU General Data Protection Regulation (2016/679) and investigated its implementation in a company in the energy sector. The General Data Protection Regulation will come into force on May 25, 2018 and will become directly applicable legislation throughout the European Union, without the need of a specific regulation by national law. The aim of the bachelor's thesis was to be acquainted with the content of the new data protection regulation and to contribute to the company's operating methods to meet the requirements of the regulation. The purpose of the thesis was to find out how well the target company had prepared for the EU data protection regulation, and to map out what steps should be taken to ensure that personal data is processed in accordance with the requirements of the new regulation.

The theoretical part of the thesis is based on international and national legislation, and especially on the EU General Data Protection Regulation. In addition, other legal material and literature have been used as source material, as well as detailed governmental regulations and instructions issued under the provisions of the law. The empirical part of the thesis examined the implementation of the data protection regulation in the target company and proposed the necessary modification measures to the company's privacy policy. The method of obtaining research material was observation and a survey that was carried out as part of the thesis. The survey revealed that the data protection practices and level of competence in the target company did not fully meet the requirements of the General Data Protection Regulation. This was mainly due to the lack of knowledge, so development suggestions and measures were based on increasing the guidance.

The EU General Data Protection Regulation will bring significant changes in the processing of personal data in the organizations. From now on, companies will have to invest in data protection issues, or they may face a considerable penalty payment when the control is tightened. However, the development of the digital environment and the electrification of services created a need for the new regulation. The process of change is laborious, but it is worth investing in. In the future, data protection issues could be seen as a competitive advantage for the company, when data protection is one of the quality criteria and the sign of a trusted partner.

Key words: data protection regulation, European Union, data protection

SISÄLLYS

1 JOHDANTO

1.1 Työn tavoitteet ja tarkoitus

Tämän opinnäytetyön tavoitteena on perehtyä toukokuun 25. päivänä 2018 voimaan astuvaan Euroopan Unionin yleiseen tietosuoja-asetukseen sekä edesauttaa asetuksen toteutumista energia-alan yrityksessä. Opinnäytetyön toimeksiantajana on työnantajani Tampereen Vera Oy, joka on sähköverkon, ulkovalaistuksen ja liikennevalojen rakentamiseen ja kunnossapitoon erikoistunut yhtiö. Tutkimuskysymyksenä opinnäytetyössä on se, kuinka EU:n tietosuoja-asetus toteutuu Tampereen Verassa, sekä miten uusi asetus vaikuttaa henkilötietojen käsittelyyn ja mitä muutoksia tarvitaan, jotta tietosuoja-asetuksen vaatimukset toteutuvat Tampereen Verassa mahdollisimman hyvin.

Tutkimuksen tarkoituksena on selvittää, kuinka hyvin EU:n yleiseen tietosuoja-asetukseen on Tampereen Verassa tällä hetkellä varauduttu, sekä kartoittaa mitä mahdollisia toimenpiteitä seuraavaksi tulisi tehdä, jotta henkilötietojen käsittely toteutuisi uuden asetuksen vaatimusten mukaisesti. Lisäksi opinnäytetyön avulla tuodaan yritykseen tietämystä uudesta asetuksesta. Henkilökohtaisena tavoitteenani on kehittyä ammatillisesti, ymmärtäen henkilötietojen käsittelyn yleiset toimintaperiaatteet ja lain asettamat vaatimukset. Oppimisprosessista on hyötyä myös toimenkuvani kannalta, koska käsittelen työtehtävissäni henkilötietoja ja toimin osana konsernin tietosuoja-projektitiimiä.

1.2 Taustaa

Tampereen Vera (jatkossa Vera) kuuluu Tampereen Sähkölaitos -yhtiöihin, ja tämä opinnäytetyö on osa laajempaa, emoyhtiöstä lähtöisin olevaa tietosuojatyön kehitysprosessia. Vaikka opinnäytetyössäni tarkastelen tietosuoja-asetuksen toteutumista vain Veran osalta, on hyvä alkuun käydä läpi projektin taustaa, miten se koko konsernissa on edennyt. Viime vuonna Tampereen Sähkölaitos Oy (emoyhtiö) toteutti hankkeen yhteistyössä asiantuntijayrityksen kanssa, jossa kartoitettiin ja arvioitiin Sähkölaitoksen henkilötietojen käsittelyprosessit sekä tietosuojan nykytila suhteessa EU:n tietosuoja-asetuksen vaatimuksiin.

Hankkeen pohjalta laadittiin kehityssuunnitelma, jota lähdettiin toteuttamaan Sähkölaitoksen tietosuojakoordinaattorin Marianne Toivosen johdolla. Tietosuojatyön jalkauttamisen tueksi perustettiin tietosuojaprojektitiimi, johon osallistui henkilötietojen käsittelystä vastaavia henkilöitä eri Sähkölaitos -yhtiöistä. Verassa henkilötietojen käsittely on verrattain vähäistä, eikä selkeää vastuuhenkilöä ollut, joten minut valittiin projektitiimiin sen perusteella, että käsittelen työtehtävissäni henkilötietoja. Uusi asetus ei ollut minulle entuudestaan tuttu, joten tämä antoi syyn lähteä perehtymään tietosuoja-asetukseen, ja sen säännöksiin opinnäytetyön avulla.

1.3 Tutkimuksen toteutus ja työn rakenne

Työn teoreettinen viitekehys pohjautuu kansainväliseen sekä kansalliseen lainsäädäntöön, eritoten EU:n tietosuoja-asetukseen, mutta lähdeaineistona on hyödynnetty myös muuta juridista aineistoa ja kirjallisuutta, sekä lain säännösten nojalla annettuja tarkempia viranomaismääräyksiä ja ohjeita. Opinnäytetyön empiirisessä osassa tarkastellaan tietosuojan toteutumista Verassa, tuodaan esille mahdollisia muutostarpeita ja pohditaan kehitystyön seuraavia askeleita. Tutkimus on rajattu käsittelemään oman toimenkuvani kannalta oleellisia osa-alueita, kuten työntekijätietojen käsittelyä Verassa. Opinnäytetyössä tutkitaan myös Veran esimiesten tietosuojaosaamisen tasoa, koska esimiesten rooli koettiin tärkeäksi tietosuojan toteutumisen kannalta. Lisäksi tutkimuksen rajaukseen vaikutti osaltaan myös emoyhtiön tietosuojatyön eteneminen.

Tutkimuksen toteutusta ohjaavana menetelmänä voidaan pitää toimintatutkimusta. Toimintatutkimus on tutkimusstrategia, jonka tarkoituksena on vaikuttaa kehittävästi tutkimuskohteeseen tai sen toimintaan, ja jossa oleellista on tutkijan osallistuminen tutkimuskohteen toimintaan (Jyväskylän yliopisto 2015). Tässä opinnäytetyössä tutkitaan ja pyritään kehittämään tutkittavan organisaation eli Veran toimintaa ja tutkijan asema työyhteisön jäsenenä on merkittävä. Tutkimuksen aineistonhankintamenetelminä käytettiin omaan työkokemukseen pohjautuvaa osallistuvaa havainnointia sekä opinnäytetyön osana toteutettua kyselytutkimusta. Osallistuvalla havainnoinnilla tarkoitetaan Hirsjärven, Remeksen ja Sajavaaran (2014, 214) mukaan havainnoin lajia, jossa havainnointi voi olla täysin vapaata sekä luonnolliseen toimintaan mukautuvaa, ja jossa havainnoija on tarkkailtavan ryhmän jäsen. Kyselytutkimuksen avulla selvitettiin Veran esimiesten

tietosuojaosaamisen tasoa, mutta tätä ei käydä työssä läpi yhtä laajasti kuin kyselytutkimukseen pohjautuvissa opinnäytetöissä, vaan kysely toimi lähinnä selvityksenä täydentäen muuta aineistoa.

Opinnäytetyössä tarkastellaan ensin lainsäädännön taustaa, kuten miten henkilön perusoikeudet yksityisyyteen ja henkilötietojen suojaan ovat historian saatossa kehittyneet. Tämän jälkeen käydään läpi EU:n tietosuoja-asetuksen keskeiset osa-alueet sekä muutokset verrattuna nykyiseen lainsäädäntöön siltä osin kuin se tämän opinnäytetyön kannalta on oleellista. Asetuksen osalta käydään läpi muun muassa henkilötietojen käsittelyn yleiset periaatteet, rekisterinpitäjän velvollisuuksia sekä rekisteröidyn oikeuksia. Lisäksi sivutaan myös tietoturvallisuutta, joka keskeisesti liittyy tietosuojan toteutumiseen. Luvussa neljä käydään läpi Veran esimiehille suunnatun tietosuojakyselyn tulokset, ja luvussa viisi tarkastellaan Veran tietosuojatyön etenemistä sekä esitetään mahdolliset kehitystoimenpiteet. Viimeisessä luvussa, eli luvussa kuusi, pohditaan lopuksi työn onnistumista ja matkan varrella heränneitä ajatuksia.

2 LAINSÄÄDÄNNÖN TAUSTAA

2.1 Kansainvälinen kehitys

Henkilötietojen suojalla yksilön perusoikeutena on pitkä kansainvälinen kehitys. Andreassonin, Koiviston ja Ylipartasen (2016, 49) mukaan maailman ensimmäiseksi tietosuojasäännökseksi voitaisiin luonnehtia 2 500 vuotta vanhaa Hippokrateen valaa, jonka lääkärit vannovat vielä tänä päivänäkin. Ihan näin kaukaa ei kuitenkaan henkilötietojen suojan kehitystä lähdetä tarkastelemaan, vaan lainsäädännön kehitys nykymuotoon on tapahtunut hieman lähempänä historiassamme.

OECD:n tietosuojasuositus ja Euroopan neuvoston yleissopimus

Nykytilaan verrattaessa, mittavina edistysaskelina voidaan pitää Taloudellisen yhteistyön ja kehityksen järjestön OECD:n (Organisation for Economic Cooperation and Development) vuonna 1980 antamaa ohjeistusta yksityisyyden suojasta ja kansainvälisestä henkilötietojen siirrosta, sekä vuoden 1981 Euroopan neuvoston yleissopimusta yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä. OECD:n ohjeistus ja Euroopan neuvoston tietosuojasopimus pitivät pitkälti sisällään nykyiselläänkin voimassa olevat henkilötietojen suojan perusperiaatteet. Yleissopimus oli tietosuoja-alan ensimmäinen, oikeudellisesti sitova kansainvälinen sopimus, jonka seurauksena monissa maissa säädettiin omat, sopimukseen perustuvat kansalliset henkilötietojen käsittelyä koskevat lait. (Vanto 2011, 13-15.)

EU:n henkilötietodirektiivi

Lokakuussa 1995 Euroopan unionin lainsäädäntöä ja henkilötietojen suojaa yhtenäistettiin hyväksymällä henkilötietodirektiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (Direktiivi 1995/46/EY). Direktiivin tavoitteena oli säännösten yhtenäistämisen lisäksi helpottaa henkilötietojen siirtoa jäsenmaiden välillä sekä lisätä entisestään yksilön perusoikeuksia ja tietosuojaa henkilötie-

tojen käsittelyyn liittyen. Direktiivi on kaikkia EU:n jäsenvaltioita velvoittava, joten näiden tuli saattaa kansalliset lainsäädäntönsä vastaamaan henkilötietodirektiivin säännöksiä. (Koskinen, Alapuranen, Heino & Lehtonen 2012, 12-15.) Henkilötietodirektiivi on tätä opinnäytetyötä kirjoittaessa edelleen voimassa, ennen kuin uusi EU:n tietosuoja-asetus korvaa henkilötietodirektiivin toukokuussa 2018.

2.2 Kansallinen lainsäädäntö

Yksityiselämän suoja kuuluu Suomessa jokaisen perusoikeuksiin. Perustuslain 10 §:n mukaan, jokaisen yksityiselämä, kunnia ja kotirauha tulee olla turvattu, ja henkilötietojen suojasta tulee säätää tarkemmin lailla (Suomen perustuslaki 1999/731). Jälkimmäinen kohta, eli henkilötietojen suojan tarkempi säätäminen lailla, on toteutettu henkilötietolailla (523/1999), mutta henkilötietojen suojaan vaikuttaa tämän lisäksi monet muut erityissäännökset. Kansallisen lainsäädännön taustalla näkyy vahvasti kansainväliset ohjeistukset ja säännökset, jotka ovat vaikuttaneet yksityisyyden ja henkilötietojen suojan kehittymiseen nykymuotoonsa Suomessa.

Henkilörekisterilaki

Euroopan neuvoston vuoden 1981 yleissopimuksen voimaantulon jälkeen Suomessa säädettiin ensimmäinen henkilötietojen käsittelyä koskeva yleislaki, kun henkilörekisterilaki astui voimaan 1987 (Vanto 2011, 16-17). Laissa määriteltiin yleiset tietosuojaperiaatteet henkilötietojen käsittelyn suhteen, ja sen tarkoituksena oli saada rekisterinpitäjät huolehtimaan itsenäisesti lainsäädännön toteutumisesta rekisterinpidossa, hyvää rekisteritapaa noudattaen. Keskeisinä periaatteina olivat mm. henkilörekisterin ja sen sisältämien tietojen tarpeellisuusvaatimus, arkaluontoisten tietojen keräämisen rajoittaminen, virheellisten tietojen oikaisuvelvollisuus sekä tietosuojavaatimukset. (Koskinen ym. 2012, 11.) Henkilörekisterilaki sisälsi siten jo henkilötietojen käsittelyn ja tietosuojan peruskulmakivet, jotka on sisällytetty nykyiseenkin lainsäädäntöön. Henkilörekisterilaki ei kuitenkaan riittänyt vastaamaan EU:n vuoden 1995 henkilötietodirektiivin asettamia vaatimuksia, jonka seurauksena kansallista lainsäädäntöä tuli uudistaa.

Henkilötietolaki

Suomessa EU:n henkilötietodirektiivi 95/46/EY pantiin täytäntöön säätämällä uusi yleislaki, henkilötietolaki (523/1999). Henkilötietolaki astui voimaan kesäkuussa 1999, ja korvasi kokonaisuudessaan henkilörekisterilain. (Andreasson, Koivisto & Ylipartanen 2016, 34.) Lakiin sisällytettiin pitkälti jo henkilörekisterilaistakin tutut henkilötietojen käsittelyn yleiset perusperiaatteet, mutta lisäksi sitä täydennettiin uusilla säännöksillä, joita EU:n direktiivi toi mukanaan. Henkilötietolailla toteutetaan henkilön yksityiselämän ja yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä, ja sen tarkoituksena on myös edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Henkilötietolakia sovelletaan kaikkeen henkilötietojen automaattiseen käsittelyyn, sekä muuhun henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat, tai tietojen on tarkoitus muodostaa, henkilörekisteri tai sen osa. (Henkilötietolaki 1999/523.) Suomen henkilötietolaki on, EU:n henkilötietodirektiivin tavoin, tätä opinnäytetyötä kirjoittaessa edelleen voimassa, mutta väistyy toukokuussa 2018, kun uusi asetus astuu voimaan ja tulee suoraan sovellettavaksi lainsäädännöksi koko EU:n alueella.

Muut lait ja säädökset

Henkilötietolain ohella, yksityisyyden suojaan ja henkilötietojen käsittelyyn vaikuttavat myös muut lait ja erityismääräykset. Näistä mainittakoon yleisellä tasolla kaikkia koskeva rikoslaki (39/1889), laki yksityisyyden suojasta työelämässä (759/2004), sekä tietoyhteiskuntakaari (917/2014) joka tunnetaan 1.6.2018 alkaen lakina sähköisen viestinnän palveluista. Lisäksi on olemassa lukuisia alakohtaisia erityislakeja henkilötietojen käsittelyyn liittyen, joita sovelletaan vain tietyn toimialan tai hallinnonalan toiminnassa. Tällaisia ovat esimerkiksi niin sanotut rekisterilait sekä viranomaistoimintaa koskevat erityissäännökset. Erityislakeja sovelletaan soveltamisalueidensa mukaisesti ensisijaisina ja täydentävästi henkilötietolakiin nähden, mutta esimerkiksi henkilötietolain yleisvelvoitteet pätevät aina, koska näitä ei ole missään muussa lainsäädännössä säädetty. (Tietosuojavaltuutetun toimisto 2013, 2014.) Nämä lait eivät EU:n tietosuoja-asetuksen myötä automaattisesti väisty kuten henkilötietolaki, mutta niitä joudutaan tarkastelemaan uudestaan, sillä myös muu kansallinen lainsäädäntö tulee sopeuttaa asetuksen ympärille.

2.3 EU:n tietosuojauudistus

EU:n tietosuojauudistus sai alkunsa tammikuussa 2012, kun Euroopan komissio julkaisi ehdotuksen tietosuojan lainsäädännön uudistamisesta. Tarpeen uudistukselle oli luonut teknologian, digitalisoitumisen ja globaalin toimintaympäristön kehittyminen sekä henkilötietojen käsittelyn lisääntyminen. (Valtiovarainministeriö 2016, 6.) Uudistukselle oli kysyntää, sillä nykyinen lainsäädäntö perustuu yli 20 vuotta vanhaan direktiiviin, ja henkilötietojen käsittelyn luonne sekä laajuus ovat kuitenkin muuttuneet merkittävästi tuosta ajasta, jolloin sähköinen toimintaympäristö oli vielä ns. lapsen kengissä. Noin neljä vuotta kestäneen uudistusprosessin tuloksena syntyi yleinen tietosuoja-asetus (EU) 2016/679 sekä tietosuojadirektiivi (EU) 2016/680 (Eduskunta 2017).

EU:n tietosuojadirektiivin tarkoituksena on tietosuojavaltuutetun toimiston mukaan ”taata korkeatasoinen suoja henkilötietojen käsittelyssä rikosasioissa ja helpottaa henkilötietojen vaihtoa jäsenvaltioiden toimivaltaisten viranomaisten kesken”, ja sitä ”sovelletaan poliisin ja muiden viranomaisten suorittamaan henkilötietojen käsittelyyn rikosasioissa” (Tietosuojavaltuutetun toimisto 2017). Tietosuojadirektiivi tulee kansallisesti panna täytäntöön 6.5.2018 mennessä, ja tätä varten Suomessa perustettiin oikeusministeriön TATTI-työryhmä valmistelemaan uutta yleislakia tietosuojasta (Eduskunta 2017). Tietosuojalaki tulisi tietosuoja-asetuksen rinnalle täydentämään EU:n tietosuoja-asetusta. Sen avulla pantaisiin tietosuojadirektiivi täytäntöön, mutta myös täsmennettäisiin joitain EU:n tietosuoja-asetuksen kohtia. Tätä opinnäytetyötä kirjoittaessa lakiesitys on edennyt eduskunnalle 1.3.2018, kun hallitus antoi työryhmän mietinnön pohjalta laaditun esityksen uudesta tietosuojalaista. Uuden yleislain olisi ehdotuksen mukaan tarkoitus astua voimaan samaan aikaan tietosuoja-asetuksen kanssa (Valtioneuvosto 2018). Opinnäytetyön kirjoitusprosessin aikana sitä ei vielä hyväksytty.

EU:n yleistä tietosuoja-asetusta ei puolestaan tarvitse erikseen kansallisesti panna täytäntöön, vaan se tulee suoraan sovellettavaksi lainsäädännöksi kaikissa jäsenvaltioissa. Euroopan parlamentin ja neuvoston asetus (EU) 2916/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta annettiin huhtikuun 27. päivänä 2016, ja se astuu voimaan kahden vuoden siirtymäajan jälkeen 25.5.2018 (Asetus 2016/679/EU). Asetuksesta puhuttaessa käytetään yleisesti lyhennettä

GDPR, mikä tulee englannin kielisistä sanoista General Data Protection Regulation (Hanninen ym. 2017, 13). Tietosuoja-asetus korvaa kokonaisuudessaan EU:n henkilötietodirektiivin sekä Suomen henkilötietolain. Asetus pitää sisällään 11 lukua ja 99 artiklaa sekä johdanto-osan (Asetus 2016/679/EU). Tietosuoja-asetuksen säännöksiin on sisällytetty pitkälti samat henkilötietojen käsittelyn ja yksityisyyden suojan perusperiaatteet kuin mitä nykyinenkin lainsäädäntö pitää sisällään, mutta tämän lisäksi on tehty täydennyksiä, tarkennuksia ja tiukennuksia. Seuraavassa luvussa perehdymme tarkemmin EU:n tietosuoja-asetuksen sisältöön ja sen tuomiin muutoksiin, siltä osin kuin se on tämän opinnäytetyön kannalta tarpeellista.

3 EU: N YLEINEN TIETOSUOJA-ASETUS

3.1 Asetuksen käsitteet

Alkuun on hyvä käydä läpi muutamia tietosuoja-asetuksen yleisempiä käsitteitä. Näin ymmärretään paremmin asetuksen terminologiaa ja osataan tulkita säännöksiä oikein. Seuraavaksi käydään siis läpi muutamia tietosuoja-asetuksen ja tämän opinnäytetyön kannalta keskeisimpiä termejä.

- **Henkilötieto** – Henkilötiedolla tarkoitetaan kaikkea luonnolliseen henkilöön liittyvää tietoa, josta henkilö voidaan suorasti tai epäsuorasti tunnistaa. Tällaisia tunnistetietoja ovat esimerkiksi nimi, henkilötunnus, kuva, sijaintitieto tai verkkotunnistetiedot. (Valtiovarainministeriö 2016, 10.)
- **Rekisteri** – Rekisterillä tarkoitetaan 4 artiklan kohdan 6 mukaan ”mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu” (Asetus 2016/679/EU).
- **Rekisterinpitäjä** – Rekisterinpitäjällä tarkoitetaan tietosuoja-asetuksessa ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot” (Asetus 2016/679/EU). Eli yleisesti rekisterinpitäjällä tarkoitetaan yritystä tai muuta organisaatiota, joka päättää mitä ja miten henkilötietoja käsitellään.
- **Rekisteröity** – Rekisteröity on luonnollinen henkilö, jonka henkilötietoja käsitellään. Yritys ei voi olla rekisteröidyn asemassa, vaan rekisteröidystä puhuttaessa tarkoitetaan aina ihmistä. (Hanninen ym. 2017, 20).
- **Henkilötietojen käsittelijä** – Henkilötietojen käsittelijällä tarkoitetaan ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun” (Asetus 2016/679/EU). Pääsääntöisesti henkilötietojen käsittelijällä tarkoitetaan tietosuoja-asetuksessa ulkopuolista toimijaa, joka käsittelee yrityksen henkilötietoja. Esimerkiksi jos yritys on ulkoistanut palkanlaskennan tilitoimistolle, on tilitoimisto tällöin henkilötietojen käsittelijän roolissa.

- **Henkilötietojen käsittely** – Henkilötietojen käsittely pitää sisällään kaikki henkilötietoihin kohdistuvat toimet koko tiedon elinkaaren ajan aina suunnittelusta hävittämiseen (Tietosuojavaltuutetun toimisto 2018a). Henkilötietojen käsittelyä ovat esimerkiksi kaikenlainen henkilötietojen automaattinen tai manuaalinen kerääminen, tallentaminen, järjestäminen, muokkaaminen, säilyttäminen tai hävittäminen (Valtiovarainministeriö 2016, 10).
- **Pseudonymisoiminen** – Pseudonymisoiminen on EU:n tietosuoja-asetuksen myötä tullut uusi käsite, joka juontuu salanimeen viittaavasta sanasta pseudonyymi. Pseudonymisoimisella tarkoitetaan henkilötietojen käsittelyä siten, että tietoja ei pystytä yhdistämään tiettyyn rekisteröityyn käyttämättä lisätietoja. Nämä lisätiedot tulee säilyttää erillään, teknisin ja organisatorisin toimenpitein suojattuna. (Tarhonen 2017.) Käytännössä pseudonymisoiminen voisi tarkoittaa esimerkiksi työntekijälle HR-järjestelmän muodostamaa satunnaista numerosarjaa, jolloin dataa pystytään käsittelemään ilman että suoria, henkilöön yhdistettäviä tunnistetietoja tarvitaan. Edellyttäen toki, että numerosarjan yhteydessä ei käytetä muita yksilöiviä tunnisteita, vaan nämä säilytettäisiin toisessa, tarkemmin suojaussa ja käyttöoikeuksin rajatussa järjestelmässä.

3.2 Asetuksen tavoitteet ja soveltamisala

Tietosuoja-asetuksen 1 artiklassa määritellään että ”asetuksella suojellaan luonnollisten henkilöiden perusoikeuksia ja -vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan” (Asetus 2016/679/EU). Asetuksen tavoitteena on vahvistaa yksilön oikeuksia ja henkilötietojen suojaa, samalla edistäen digitaalisen tiedonsiirron kehittymistä Euroopan alueella. Lisäksi asetuksella halutaan yhdenmukaistaa EU:n alueen tietosuojasäännöksiä, kun yksi ja sama asetus tulee suoraan sovellettavaksi lainsäädännöksi kaikissa jäsenvaltioissa. Näin päästään eroon kansallisen lainsäädännön eroavuuksista, mitä EU:n henkilötietodirektiivin täytäntöönpano osittain aiheutti. (Hänninen 2017.) Opitietosuojaa.fi-sivuston (2017) kuviossa asetuksen sisältö ja tavoite kiteytyvät hyvin (kuvio 1). Kuviosta 1 nähdään, että tietosuoja-asetuksen myötä kansalaiset saavat enemmän oikeuksia, kun taas rekisterinpitäjille tulee uusia velvoitteita. Viranomaiset puolestaan saavat laajemmat valtuudet valvoa asetuksen toteutumista, ja tämän kaiken tarkoituksena on luoda Euroopan Unionille vahva, yhtenäinen tietosuojakehys, mikä puolestaan mahdollistaa EU:n digitaalisten sisämarkkinoiden kehittymisen.

KUVIO 1. Asetuksen sisältö ja tavoite (Opitietosuojaa.fi 2017)

Asetuksen 2 artiklan mukaan asetusta sovelletaan kaikkeen henkilötietojen käsittelyyn, joka on joko osittain tai kokonaan automaattista sekä myös muuhun henkilötietojen käsittelyyn, jos henkilötiedot muodostavat, tai niiden on tarkoitus muodostaa rekisterin osa (Asetus 2016/679/EU). Käytännössä tämä tarkoittaa sitä, että tietosuoja-asetus tulee sovellettavaksi aina kun henkilötietoja käsitellään organisaatiossa. Tähän riittää, jos yrityksellä on yksikin työntekijä tai vaikka kyseessä olisi itsenäinen yrittäjä, asetus tulee sovellettavaksi viimeistään asiakkaan tietoja käsiteltäessä. Asetusta ei kuitenkaan sovelleta yksityisen henkilön henkilökohtaisessa tai kotitalouttaan koskevassa henkilötietojen käsittelyssä (Asetus 2016/679/EU). Alueellisesti, asetusta sovelletaan paitsi EU:n alueella sijaitsevien rekisterinpitäjien ja henkilötietojen käsittelijöiden toimipaikoissa, myös tietyin edellytyksin unionin ulkopuolella, jos kyse on esimerkiksi tavaran toimittamisesta Euroopan jäsenvaltioon ja vaatii henkilötietojen käsittelyä (Hanninen ym. 2017, 19).

Asetuksen avulla saadaan tietosuoja-asiat päivitettyä digiaikakaudelle, globaalin toimintaympäristön vaatimalle tasolle. Yritysten on pakko kiinnittää huomiota henkilötietojen käsittelyyn ja tietosuoja-asioihin, tai vastassa voi olla huomattava sakkorangaistus kun asetuksen myötä myös valvonta ja sanktiot kiristyvät. Muutosvaihe voi olla organisaatiolle raskas prosessi, mutta kun tietosuoja-asiat saadaan saatettua lain vaatimalle tasolle,

asetus tulee helpottamaan tulevaisuuden toimintatapoja alati muuttuvassa digiympäristössä, joten se tulisikin ennen kaikkea nähdä mahdollisuutena. Pyritäänhän asetuksella myös lisäämään luottamusta. Nimittäin luottamusta siihen, että henkilötietoja, olivatpa ne sitten asiakkaan, yhteistyökumppanin tai työntekijän, käsitellään asianmukaisesti ja turvallisesti. Jos tietoturva pettää ja yrityksen maine luotettavana kumppanina tai työnantajana menetetään, voi olla vaikea saada rakennettua luottamusta uudelleen, muista mahdollisista vahingoista puhumattakaan. Tietosuoja-asiat voidaankin nähdä yhtenä kilpailukeinona, johon yrityksen kannattaa panostaa.

3.3 Henkilötietojen käsittelyn yleiset periaatteet

Tietosuoja-asetuksen 5 artiklassa määritellään henkilötietojen käsittelyä koskevat yleiset periaatteet mitä henkilötietojen käsittelyssä on noudatettava (Asetus 2016/679/EU):

- **Lainmukaisuus, kohtuullisuus ja läpinäkyvyys** – Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.
- **Käyttötarkoitussidonnaisuus** – Henkilötietojen kerääminen tulee olla käyttötarkoitussidonnaista, eli näitä saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä henkilötietoja saa myöhemmin käsitellä muuhun, alkuperäisestä poikkeavaan tarkoitukseen.
- **Tietojen minimointi** – Henkilötietojen suhteen on noudatettava tietojen minimointi- periaatetta, eli henkilötietoja tulee kerätä ja käsitellä vain siltä osin kuin on tarkoitukseen nähden tarpeellista.
- **Täsmällisyys** – Henkilötietojen on oltava täsmällisiä sekä tarvittaessa päivitettyjä. Epätarkat ja virheelliset tiedot tulee viipymättä poistaa tai oikaista.
- **Säilytyksen rajoittaminen** – Henkilötietoja on säilytettävä ainoastaan niin kauan, kuin on tarpeen henkilötietojen käsittelyn tarkoituksen toteuttamista varten. Pidempiä aikoja tietoja saa säilyttää ainoastaan tietyin edellytyksin, jos kyseessä on yleisen edun mukainen arkistointitarkoitus, tieteellinen tai historiallinen tutkimustarkoitus taikka tilastollinen tarkoitus.
- **Eheys ja luottamuksellisuus** – Henkilötietoja käsiteltäessä tulee varmistaa tietojen asianmukainen turvallisuus teknisin ja organisatorisin toimenpitein. Henkilötietoja tulee suojata luvattomalta ja lainvastaiselta käsittelyltä, sekä estää tietojen muu mahdollinen tuhoutuminen, häviäminen tai vahingoittuminen.

3.4 Käsittelyn lainmukaisuus

Henkilötietojen käsittelylle tulee aina olla lainmukainen peruste. Tämä peruste voi esimerkiksi olla suostumus, sopimus tai lakisääteisten velvoitteiden täyttäminen. Väestörekisterikeskuksen johtavan asiantuntijan Noora Kallion mukaan suostumuksella tarkoitetaan rekisteröidyn antamaa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla hän hyväksyy henkilötietojensa käsittelyn. Suostumus ja sen merkitys tulee olla ymmärrettävässä muodossa, ja etukäteen informoituna ennen suostumuksen antoa. Suostumuksen anto tulee toteuttaa aktiivisena tapahtumana, ja suostumus pitää pystyä myös milloin tahansa helposti peruuttamaan. (Kallio 2018.) Suostumuksen muoto voi olla kirjallinen, suullinen tai sähköinen, mutta se tulee tarvittaessa pystyä osoittamaan. Suostumusta käytetään esimerkiksi henkilötietoja kerättäessä suoramarkkinointitarkoituksiin tai erilaisiin sähköisiin palveluihin rekisteröidyttäessä. Suostumus on aina käyttötarkoituskohtainen, ja jos tietoja käytetään hyväksi muuhun tarkoitukseen, tulee pyytää uusi lupa.

Asetuksen luvun kaksi 6 artiklassa määritellään, että henkilötietojen käsittely voi perustua myös sopimusperusteeseen, kun ”käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä” (Asetus 2016/679/EU). Tällainen sopimus voi olla esimerkiksi kauppatapahtuma, jossa asiakas haluaa maksaa ostamansa tuotteen laskulla. Sopimuksen täytäntöönpanoa varten, tarvitaan tällöin asiakkaan henkilötietoja kuten nimi ja osoite laskun toimittamista varten, sekä mahdollisesti henkilötunnus yksilöintiä ja luottoselvitystä varten. Myös työntekijän ja työnantajan välinen työsopimus on sopimusperuste, jolloin työnantaja saa käsitellä erinäisiä työntekijän eli rekisteröidyn henkilötietoja työsopimuksen täytäntöön panemiseksi. Työnantajan oikeuksiin käsitellä työntekijöidensä tietoja, vaikuttavat kuitenkin myös muutkin oikeusperusteet, ei pelkästään sopimus.

Tietosuoja-asetuksen 6 artiklan kohdassa c määritellään lakisääteisten velvoitteiden noudattamisen olevan yksi käsittelyn peruste (Asetus 2016/679/EU). Työnantajan osalta tämä tulee kyseeseen esimerkiksi työntekijöiden palkkatietojen ilmoittamisessa veroviran-

omaisille tai lakisääteisten maksujen suorittamisessa vakuutusyhtiölle. Työnantajan oikeutta käsitellä työntekijöiden henkilötietoja ohjaa myös Suomessa säädetty erityislaki yksityisyyden suojasta työelämässä (759/2004), jossa määritellään minkälaisia henkilötietoja työnantaja saa käsitellä (Nyyssölä 2014, 30). Kyseisen lain 3 §:ssä määritellään tarpeellisuusvaatimus, jonka mukaan ”työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta” (Laki yksityisyyden suojasta työelämässä 2004/759).

Muita asetuksen 6 artiklassa mainittuja henkilötietojen laillisia käsittelyperusteita ovat lisäksi elintärkeä etu, yleinen etu tai julkisen vallan käyttö, sekä oikeutettu etu (Asetus 2016/679/EU). Elintärkeä etu voi tulla kysymykseen esimerkiksi ensiapu- tai onnettomuustilanteiden hoitamisessa, kun taas yleisellä edulla ja julkisella vallalla viitataan julkisten tehtävien hoitamiseen yhteiskunta- ja viranomaistoiminnassa. Oikeutettu etu on käsitteenä uudempi ja laveampi määritelmä rekisterinpitäjän oikeudesta käsitellä henkilötietoja. Tietosuoja-asetuksen johdanto-osion kohdissa 47 ja 48 selvennetään, että oikeutettua etua voidaan käyttää käsittelyperusteena, mikäli muuta laillisuusperustetta ei löydy, mutta rekisterinpitäjän ja rekisteröidyn välillä on olemassa merkittävä suhde. Tämä suhde voi olla esimerkiksi asiakas- tai palvelussuhde, ja oikeutettu etu voi pitää sisällään myös konsernin sisäisen henkilötietojen käsittelyn emoyhtiön ja tytäryhtiöiden välillä. Oikeutetun edun olemassaoloa on kuitenkin arvioitava huolellisesti, eikä tämä voi syrjäyttää rekisteröidyn perusoikeuksia tai vapauksia henkilötietojen suojaan. (Asetus 2016/679/EU.)

3.5 Erityiset henkilötietoryhmät

Asetuksen artiklassa 9 on määritelty tiukemmat käsittelyperusteet erityisille henkilötietoryhmille eli ns. arkaluonteisille tiedoille. Tällaisia henkilötietoja, joiden käsittely on kielletty ilman erityistä perustetta, ovat sellaiset tiedot, joista ilmenee henkilön rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset ja biometriset tiedot, kun näitä käytetään tunnistautumistarkoituksessa, sekä henkilön terveydentilaa tai seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot. Erityinen peruste arkaluonteisten tietojen käsittelylle voi esimerkiksi olla

rekisteröidyn oma nimenomainen suostumus kyseisten henkilötietojen käsittelyyn, ellei unionin tai jäsenvaltion lailla ole säädetty toisin. Erityisten henkilötietoryhmien käsittely voi olla tarpeen myös rekisterinpitäjän tai rekisteröidyn lakisääteisten velvoitteiden ja erityisten oikeuksien noudattamiseksi. (Asetus 2016/679/EU.)

Hannisen ym. (2017) mukaan työnantaja saa käsitellä työntekijän arkaluonteisia tietoja, mikäli tämä on ”tarpeen yrityksen ja rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattamiseksi työoikeuden alalla ja siinä laajuudessa kuin se sallitaan lainsäädännössä tai työehtosopimuksessa” (Hanninen ym. 2017, 42). Esimerkiksi työntekijän terveydentilaan liittyvien tietojen käsittelystä säädetään laissa yksityisyyden suojasta työelämässä. Työnantajalla voi olla oikeus käsitellä työntekijän terveydentilatietoja esimerkiksi silloin, kun työnantaja on maksamassa työntekijälle sairausajan palkkaa tai muita terveydentilaan liittyviä etuuksia, selvittää onko sairauspoissaoloon perusteltu syy, tai jos työntekijä itse haluaa selvittää omaa työkykyisyyttään terveydentilaa koskevien tietojen perusteella. (Hanninen ym. 2017, 43.) Työnantajalla on myös oikeus saada tieto ammattiliittoon kuuluvista työntekijöistään lakkouhan alla, ja usein myös työntekijä itse ilmoittaa ammattiliiton kuulumisesta työnantajalle, jotta jäsenmaksu voidaan periä palkasta.

3.6 Rekisterinpitäjän velvoitteet

Rekisterinpitäjä on lähtökohtaisesti aina vastuussa henkilötietojen käsittelyn lainmukaisuudesta siten, että tietosuoja-asetusta noudatetaan kaikessa sen toiminnassa, koko henkilötietojen käsittelyn elinkaaren ajan. Siksi onkin tärkeää tietää rekisterinpitäjän yleiset velvoitteet ja toimia näiden mukaisesti. Jos velvoitteita laiminlyödään, tai niitä ei noudateta, seurauksena voi olla huomattava sakkorangaistus tai jopa henkilötietojen käsittelykielto. EU:n tietosuoja-asetuksen myötä rekisterinpitäjille on asetettu uusia velvoitteita, joita ei nykyisessä lainsäädännössä ole.

3.6.1 Osoitusvelvollisuus

Yksi keskeisimmistä muutoksista on osoitusvelvollisuus. Aiemmin on riittänyt, että lakia noudatetaan, mutta nyt uuden tietosuoja-asetuksen myötä, organisaation tulee pystyä

myös osoittamaan, että se noudattaa asetusta ja toteuttaa tietosuojaperiaatteita käytännössä. Tämä tarkoittaa muun muassa henkilötietojen käsittelyn aiempaa tarkempaa suunnittelua sekä prosessien ja käytänteiden dokumentointia. (Hänninen 2018.) Valtiovarainministeriön VAHTI-ohjeessa todetaan, että dokumentaatio voi käytännössä sisältää esimerkiksi organisaation tietosuojapolitiikan kuvaamisen, käsittelytoimien tietosuojaselosteet, tietoturvatestauksien tulokset ja riskirekisterit, henkilöstölle suunnatut ohjeet taikka tietotilinpäätöksen (Valtiovarainministeriö 2016, 27-28).

Tietosuoja-asetuksen myötä, osana osoitusvelvollisuutta, rekisterinpitäjien ja henkilötietojen käsittelijöiden on ylläpidettävä kirjallista selostetta vastuullaan olevista henkilötietojen käsittelytoimista (Asetus 2016/679/EU). Tämä vastaa kutakuinkin nykyistä henkilötietolain mukaista rekisteriselostetta henkilörekistereistä, mutta samaa dokumenttia ei voida hyödyntää täysin sellaisenaan, vaan nämä tulee päivittää asetuksen mukaisiksi. Tietosuojaseloste on organisaation sisäiseen käyttöön tarkoitettu asiakirja, mutta se on tarvittaessa toimitettava valvontaviranomaiselle. Velvollisuus selosteen laatimiseen koskee kaikkia yli 250 työntekijän organisaatioita, ja myös tätä pienempiä yrityksiä, jos henkilötietojen käsittely todennäköisesti aiheuttaa riskin henkilön oikeuksille ja vapauksille, henkilötietoja käsitellään yrityksessä säännöllisesti tai yritys käsittelee erityisiin tietoryhmiin kuuluvia henkilötietoja, jotka koskevat rikostuomioita tai rikkomuksia. (Tietosuojavaltuutetun toimisto 2018b.) Asetuksesta ei kuitenkaan käy ilmi, mitä tarkoitetaan todennäköisellä riskillä tai milloin henkilötietoja ei käsitellä säännöllisesti, joten tulkinta jää organisaation oman harkinnan varaan. Selosteen sisällöstä, mitä tietoja sen tulee sisältää, on tarkemmin määritelty tietosuoja-asetuksen 30 artiklassa.

Osoitusvelvollisuuden todentamiseksi organisaatiot voivat lisäksi käyttää yhtenä keinona tietosuoja-asetuksen mukaisia tietosuojaa koskevia sertifikaatteja tai alakohtaisia käytännesääntöjä. Sertifikaatti käy tietosuojan toteuttamisen osoituksena viranomaiselle, ja sen lisäksi rekisteröity pystyy helposti arvioimaan organisaation tietosuojan tasoa tuotetta tai palvelua ostaessa. (Oikeusministeriö 2017, 14.) Asetuksen noudattamisen osoittaminen, on paitsi osa lain velvoitteiden täytäntöönpanoa ja viranomaisvalvontaa, myös eräänlainen yrityksen kilpailukeino. Läpinäkyvyys ja luottamuksen lisääminen ovat asetuksen keskeisempiä tavoitteita, ja nämä tulevat varmasti vaikuttamaan yhä enenevässä määrin eri tahojen toimintaan. Olipa kyse sitten yksityisistä kuluttajista, yritysasiakkaista, yhteis-

työkumppaneista tai organisaation omista työntekijöistä, tietosuoja-asiat nousevat varmasti yhdeksi kriteeriksi, kun puhutaan laadusta ja turvallisuudesta tämän hetken ja etenkin tulevaisuuden digitaalisessa toimintaympäristössä.

3.6.2 Sisäänrakennettu ja oletusarvoinen tietosuoja

Osoitusvelvollisuuden lisäksi, toinen EU:n tietosuoja-asetuksen myötä tuleva uusi rekisterinpitäjän velvoite on sisäänrakennetun ja oletusarvoisen tietosuojaperiaatteen noudattaminen. Väestörekisterikeskuksen johtavan asiantuntijan Noora Kallion mukaan sisäänrakennetun ja oletusarvoisen tietosuojan periaate merkitsee sitä, että tietosuojaperiaatteet otetaan huomioon henkilötietojen käsittelyä sisältävien toimintojen kaikissa vaiheissa, ja että tietoja tulee käsitellä vain siltä osin kuin se on käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellista. Tietosuojaperiaatteiden toteutuminen tulee varmistaa teknisin ja organisatorisin toimenpitein. (Kallio 2018.)

Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan erilaisia suojatoimia, jotka rekisterinpitäjä pääsääntöisesti itse määrittelee, ottaen huomioon käytettävissä olevan tekniikan, toteuttamiskustannukset, riskit sekä henkilötietojen käsittelyn luonteen, laajuuden ja tarkoitukset. Tällaisilla suojatoimilla voidaan tarkoittaa esimerkiksi henkilöstön kouluttamista, tietojärjestelmien tietoturvaa tai erilaisia tarkastus- ja valvontajärjestelmiä. (Kallio 2018.) Eli yritystoiminnassa toteutetut suojakeinot voisivat yksinkertaisimmillaan olla työntekijöiden ohjeistamista tiedon oikeanlaiseen käsittelyyn, tai kulunvalvontaa, jolloin tiettyihin tiloihin, esimerkiksi arkistoon, jossa säilytetään työntekijöiden palkkatietoja, asiattomilta pääsy evätään lukitusjärjestelmien avulla. Teknisillä toimenpiteillä puolestaan voidaan tarkoittaa esimerkiksi tietojärjestelmien käyttöoikeuksien rajausta, eli henkilötietoja pääsee käsittelemään sähköisissä järjestelmissä vain ne henkilöt, joiden työtehtävien puitteissa on näitä tarpeen käsitellä.

Kallion mukaan ”sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet edellyttävät, että tietosuojaa koskevat kysymykset tunnistetaan ja otetaan huomioon jo siinä vaiheessa, kun suunnitellaan henkilötietojen käsittelyä sisältäviä toimintoja tai kehitetään tietojärjestelmiä” (Kallio 2018). Käytännössä tämä tarkoittaa sitä, että tietosuoja-asetus tulee huomioida automaattisesti kaikessa yrityksen toiminnassa missä henkilötietoja liikkuu,

ikään kuin taustalla jatkuvasti vaikuttaen. Jos uusia tietojärjestelmiä otetaan käyttöön, tulee ensin varmistaa, että nämä täyttävät tietosuoja-asetuksen vaatimukset. Tietosuoja-asioiden huomioiminen jo suunnitteluvaiheessa on järkevää ja usein myös edullisempaakin kuin että olemassa olevia, heikkoja tietojärjestelmiä yritettäisiin muokata ja saattaa lain vaatimalle tasolle.

3.6.3 Riskiperusteinen lähestymistapa

Jotta rekisterinpitäjä pystyisi itse määrittelemään ja arvioimaan tarvittavat tekniset ja organisatoriset suojatoimet, tulisi organisaation tunnistaa henkilötietojen käsittelyyn liittyvät riskit sekä osata luokitella nämä ns. matalan ja korkean tason riskeihin. Tätä kutsutaan riskiperusteiseksi lähestymistavaksi, millä pyritään suhteuttamaan asetuksen velvoitteet ja asianmukaiset suojakeinot sen mukaan, minkälainen riski henkilötietojen käsittelyssä kulloinkin kohdistuu rekisteröidyn oikeuksiin ja vapauksiin. Riskeillä tarkoitetaan rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja. Esimerkiksi henkilötietojen huolimaton tai luvaton käsittely voi johtaa henkilön syrjintään, petokseen, identiteettivarkauteen, taloudellisiin menetyksiin tai sosiaaliseen vahinkoon. Arkaluonteisia tietoja käsiteltäessä riski on koreampi, ja näin ollen arkaluonteiset tiedot vaativat myös erityisiä suojatoimia. Tavallista korkeampi riski on myös silloin kun käsitellään suuria määriä rekisteröidyn henkilötietoja, tai suurta rekisteröityjen määrää, vaikka tiedot itsessään ei muuten olisi arkaluonteisia. (Hanninen ym. 2017, 26-27; Oikeusministeriö 2017, 16.)

Sanonta kuuluu, että yrityksen suurin tietoturvariksi istuu tietokoneen näytön ja tuolin välissä, eli on ihminen. Työntekijän huolimattomuus, uteliaisuus, tietämättömyys tai inhimillinen vahinko ovat tavallisimpia uhkia henkilötietojen käsittelyyn liittyen. Jos esimerkiksi terveydentilaa koskevia tietoja käsittelevä henkilö ei osaa sovittaa keskustelujaan ympäristön mukaan salassapitosäännöksiä noudattaen, vaan kertoo eteenpäin arkaluonteisia tietoja sellaisille henkilöille joille nämä eivät kuulu, voi rekisteröity joutua syrjinnän kohteeksi esimerkiksi sairautensa vuoksi. Tai pieni huolimattomuus sähköpostin vastaanottajakentässä, voi johtaa tiedon nopeaan leviämiseen tahoille, joille se ei kuulu. Jos vahinko tapahtuu, sitä on usein jopa mahdotonta enää korjata, eikä menetettyä luottamusta tai mainetta saa helposti takaisin, muista mahdollisista aineettomista tai aineellisista menetyksistä puhumattakaan.

Riskiperusteisessa lähestymistavassa olennaista on, että yritys tunnistaa tiedon käsittelyyn liittyvät riskit, olivatpa ne sitten ulkoisia tai sisäisiä, ja osaa arvottaa nämä. Kaikki tieto ei ole saman arvoista, eikä kaikkea tietoa kannata lähteä suojaamaan järeästi, vaan resurssit tulee mitoittaa oikein sinne, missä suojausta eniten tarvitaan. Tiedon luokittelu helpottaa yrityksiä toteuttamaan tarvittavat tekniset ja organisatoriset toimenpiteet, kun henkilötiedot on jaoteltu eri suojausluokkiin, esimerkiksi avoimiin, suojattaviin ja arkaluonteisiin tietoihin. Eriasteinen tiedon luokittelu, yleisesti yrityksen asianhallintaan liittyen, ei vain tietosuojaan, on toki ollutkin jo käytössä, mutta tietosuoja-asetuksen myötä henkilötietojen käsittelyprosessien tarkastelu ja dokumentaation päivittäminen on myös paikallaan, jotta nämä vastaavat uuden asetuksen mukaisia vaatimuksia.

3.7 Henkilötietojen käsittelyn ulkoistaminen

Yritys voi siirtää haluamansa osan henkilötietojen käsittelystä ulkoiselle toimijalle, josta asetuksessa käytetään nimitystä henkilötietojen käsittelijä. Asetuksen 28 artiklan mukaan rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka täyttävät tietosuoja-asetuksen mukaiset vaatimukset. Käsittely on aina määritettävä sopimuksella, josta tulee käydä ilmi ainakin henkilötietojen käsittelyn kohde, kesto ja tarkoitus, käsiteltävien henkilötietojen tyyppi sekä rekisterinpitäjän velvollisuudet ja oikeudet. (Asetus 2016/679/EU.) Henkilötietojen käsittelijän tulee käsitellä henkilötietoja ainoastaan rekisterinpitäjän määrittelemien tarkoituksien ja ohjeiden mukaisesti. Jos henkilötietojen käsittelijä määrittelee itse tietojen käsittelytarkoitukset ja keinot, voidaan henkilötietojen käsittelijä tulkita rekisterinpitäjäksi. (Hanninen ym. 2017, 27.) Joissain tapauksissa, henkilötietojen käsittelijä voi kuitenkin laatia ohjeet, ikään kuin palvelunkuvauksena, jonka rekisterinpitäjä taas hyväksyy ”omina ohjeinaan” (Hanninen ym. 2017, 84).

Vaikka rekisterinpitäjä on viimekädessä vastuussa rekisteröidyn oikeuksien ja vapauksien toteutumisesta, on henkilötietojen käsittelijä myös vastuussa omista käsittelytoimistaan, sekä siitä, että tämä noudattaa asetuksen yleisiä periaatteita. Yhtä lailla kuin rekisterinpitäjälle, voidaan siten myös henkilötietojen käsittelijälle määrätä sanktioita asetuksen velvoitteiden laiminlyömisestä. Vastuukysymykset onkin hyvä määritellä rekisterinpitäjän ja henkilötietojen käsittelijän välisissä käsittelysopimuksissa. Yrityksen on tiedos-

tettava tietosuoja-asetuksen vaatimukset, jotta se osaa ottaa nämä huomioon jo tarjouspyyntövaiheessa, kun ulkoistamista tai uusia järjestelmiä suunnitellaan. Voimassa olevat sopimukset tulee myös käydä läpi, ja tarkastaa, että ne vastaavat asetuksessa säädettyä. Lisäksi on tärkeä tunnistaa roolinsa, eli missä kohtaa yritys toimii rekisterinpitäjänä ja missä mahdollisesti toisen organisaation henkilötietojen käsittelijänä.

3.8 Rekisteröidyn oikeudet

Nykyisessä henkilötietolaissa määritellään rekisteröidyn oikeus informointiin tietojen käsittelystä, tarkastusoikeus, tiedon korjaaminen sekä kielto-oikeus (Vanto 2011, 199, 125, 131, 135). Tietosuoja-asetuksessa rekisteröidyn oikeudet vastaavat pitkälti nykyisen lainsäädännön mukaisia oikeuksia, mutta lisäksi asetuksessa on säädetty uusista oikeuksista, sekä määritelty tarkemmin näiden toteuttamiseen liittyviä prosesseja (Oikeusministeriö 2017, 23). Tietosuoja-asetuksen luvussa kolme määritellään rekisteröidyn oikeudet, joiden toteutuminen tulee ottaa huomioon kaikessa henkilötietojen käsittelyssä. Kun rekisteröity käyttää oikeuksiaan, on rekisterinpitäjä velvollinen varmistamaan rekisteröidyn henkilöllisyyden, jotta vältytään muiden oikeuksien ja vapauksien loukkaamiselta (Valtiovarainministeriö 2016, 13). Erillistä tunnistautumisprosessia ei kuitenkaan vaadita, jos esimerkiksi yrityksen henkilöstö tuntee toisensa, ja työntekijä pyytää henkilökohtaisesti HR-assistentilta hänestä kerättäviä tietoja, mutta tunnistautumisen menettely tarvitaan, jos rekisteröidyn henkilöllisyydestä ei voida olla varmoja.

Oikeus saada läpinäkyvää tietoa ja pääsy omiin tietoihin

Rekisteröidyllä on oikeus avoimeen informointiin, mikä perustuu henkilötietojen käsittelyn läpinäkyvyyden periaatteeseen. Tieto henkilötietojen käsittelystä tulee olla helposti saatavilla, rekisteröidyn näkökulmasta ymmärrettävästi ja selkeällä kielellä esitettynä. Tiedonanto voidaan toteuttaa esimerkiksi selosteen muodossa, joka on osa laajempaa tietosuojaperiaatteiden kuvausta. (Hänninen 2018.) Asetus mahdollistaa kirjallisen tiedonannon lisäksi informoinnin myös tapauskohtaisesti sähköisessä muodossa tai muulla tavoin. Asetuksen 13 ja 14 artikloissa on määritelty yksityiskohtaisemmin tietosisältö mitä tietoja rekisterinpitäjän tulee rekisteröidylle antaa. Tällaisia tietoja ovat esimerkiksi rekisterinpitäjän yhteystiedot, henkilötietojen käsittelyn tarkoitus ja oikeusperuste sekä

tietojen säilytysaika. Toimitettaviin tietoihin vaikuttaa onko henkilötiedot kerätty rekisteröidyltä itseltään vai ei. (Asetus 2016/679/EU.)

Asetuksen 15 artiklan mukaan rekisteröidyllä on myös oikeus päästä omiin tietoihinsa eli rekisteröity voi pyytää rekisterinpitäjältä tietoa siitä, mitä henkilötietoja hänestä käsitellään tai ei käsitellä (Asetus 2016/679/EU). Rekisterinpitäjällä on tällöin yksi kuukausi aikaa reagoida pyyntöön ja toimittaa jäljennökset käsiteltävistä rekisteröidyn henkilötiedoista. Tarvittaessa määräaikaa voidaan jatkaa enintään kahdella kuukaudella, jos se on perusteltua, ottaen huomioon pyyntöjen monimutkaisuuden tai määrän. Aikaa jatkettaessakin, rekisteröidylle tulee vastata kuukauden sisällä pyynnön esittämisestä ja kerrottava viivästymisestä. Lähtökohtaisesti pyynnöt tulee toteuttaa rekisteröidylle maksuttomina, mutta mikäli rekisteröidyn pyynnöt ovat perusteettomia tai kohtuuttomia, voi rekisterinpitäjä tietyin edellytyksin periä rekisteröidyltä tietojen toimittamisesta aiheutuneet kustannukset, tai kieltäytyä kokonaan toimittamasta tietoja. (Oikeusministeriö 2017, 24-25.) Tilanne, jossa rekisterinpitäjä kieltäytyisi toimittamasta tietoja, voisi käytännössä tulla eteen esimerkiksi silloin, kun henkilö toistuvasti pyytää tietojaan kiusantekomielessä.

Oikeus tietojen oikaisemiseen ja poistamiseen

Tietosuoja-asetuksessa määritellään rekisteröidyn oikeus tietojen oikaisemiseen sekä tietyin edellytyksin oikeus tietojen poistamiseen, eli ns. ”oikeus tulla unohdetuksi”. Nämä vastaavat pitkälti nykyisen henkilötietolain mukaisia tiedonkorjaamisoikeuksia. Asetuksen 16 artiklassa määritellään, että rekisteröidyllä on oikeus vaatia rekisterinpitäjää korjaamaan tai täydentämään rekisteröityä koskevat epätarkat, virheelliset tai puutteelliset tiedot ilman aiheetonta viivytystä. Artikla 17 puolestaan täsmentää, milloin rekisteröidyllä on myös oikeus häntä koskevien henkilötietojen poistamiseen. Rekisteröity voi vaatia rekisterinpitäjältä tietojensa poistamista, jos esimerkiksi henkilötietoja ei enää tarvita siihen käyttötarkoitukseen johon nämä kerättiin, rekisteröity peruuttaa suostumuksen johon henkilötietojen käsittely on perustunut tai henkilötietoja käsitellään lainvastaisesti. Poisto-oikeus ei kuitenkaan ole aina sovellettavissa, mihin vaikuttaa käsittelyn oikeusperuste. Muun muassa rekisteröidyllä ei ole oikeutta tietojensa poistamiseen, jos henkilötietojen käsittely perustuu lainsäädäntöön tai lakisääteisten velvoitteiden noudattamiseen. (Asetus 2016/679/EU.) Esimerkiksi laki velvoittaa työnantajaa säilyttämään työntekijän

palkkatietoja kymmenen vuotta tilikauden päättymisestä. Rekisteröidyllä ei tällöin ole oikeutta poistaa häntä koskevia palkkatietoja, vaikka työsuhde olisikin päättynyt. Henkilö ei voi myöskään pyytää verohallintoa poistamaan tietojaan, koska verotusmenettelystä on säädetty laissa.

Oikeus siirtää tiedot järjestelmästä toiseen

EU:n tietosuoja-asetuksen myötä, uutena oikeutena rekisteröidylle tulee oikeus siirtää tiedot järjestelmästä toiseen. Uuden oikeuden tarkoituksena on helpottaa henkilötietojen siirtoa järjestelmien välillä, samalla edistäen digitaalisten palvelujen kehittymistä. Asetuksen 20 artiklassa säädetään että ”rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä” (Asetus 2016/679/EU). Rekisteröidyn tiedot tulee lisäksi saada siirrettyä suoraan rekisterinpitäjältä toiselle, jos se teknisesti on vain mahdollista. Tietojen siirto-oikeus koskee vain sopimukseen tai suostumukseen perustuvaa henkilötietojen käsittelyä, joka suoritetaan automaattisesti. (Asetus 2016/679/EU.) Eli kuten tietojen poisto-oikeudessa, siirto-oikeudessakin tulee tunnistaa henkilötietojen käsittelyn oikeusperuste, jotta tiedetään, milloin lakia sovelletaan ja milloin ei. Huomionarvoista on myös se, että siirto-oikeus koskee vain rekisteröidyn itsensä antamia tietoja, ei muulla tavoin kerättyä dataa kuten esimerkiksi profiloinnin tuloksia.

Muut oikeudet

Muita asetuksessa säädettyjä rekisteröidyn oikeuksia, joita sovelletaan tietyin edellytyksin, on oikeus henkilötietojen käsittelyn rajoittamiseen, vastustamisoikeus sekä oikeus olla joutumatta automatisoitujen yksittäispäätösten, mukaan lukien profiloinnin kohteeksi. Oikeus käsittelyn rajoittamiseen tulee kyseeseen esimerkiksi sellaisissa tilanteissa, joissa rekisteröity epäilee henkilötietojen paikkansapitävyyttä tai käsittelyn lainmukaisuutta. Tällöin rekisterinpitäjän on rajoitettava henkilötietojen käsittelyä selvityksen ajaksi, kunnes paikkansapitävyys on varmistettu tai epäily lainvastaisuudesta kumottu. Vastustamisoikeutta puolestaan sovelletaan etenkin suoramarkkinoinnissa, sekä

muutamassa muussa erityistilanteessa henkilötietojen käsittelyperusteesta riippuen. Rekisteröidyllä on oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä suoramarkkinointia varten, jolloin rekisteröidyn tietoja ei saa käsitellä enää kyseiseen tarkoitukseen. (Asetus 2016/679/EU.) Automatisoitujen päätösten osalta, asetuksen 22 artiklassa säädetään että ”rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.” (Asetus 2016/679/EU). Tätä kohtaa ei kuitenkaan sovelleta, jos automatisoitu päätös perustuu henkilön nimenomaiseen suostumukseen, on hyväksytty lainsäädännössä, tai on välttämätön rekisterinpitäjän ja rekisteröidyn välisen sopimuksen tekemistä tai täytäntöönpanoa varten (Asetus 2016/679/EU). Esimerkiksi tilanteessa, jossa asiakas tilaa tavaraa verkkokaupasta, voidaan edellyttää automatisoitua päätöksentekoa luottokelpoisuuden selvittämiseksi, jotta asiakas saa ostaa tuotteen laskulle.

3.9 Tietoturva

Tietosuojasta puhuttaessa tulee puhua myös tietoturvallisuudesta, jolla on keskeinen asema tietosuojan toteutumisessa. Kun tietosuojalla tarkoitetaan henkilön yksityisyyden ja perusoikeuksien suojaamista henkilötietojen käsittelyssä, on tietoturvallisuus laajempi käsite, joka on muodostunut IT-alan kehityksen myötä. Tietoturvallisuudella viitataan tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamiseen. Luottamuksellisuudella tarkoitetaan tiedonsaannin rajaamista, etenkin salassa pidettävässä materiaalissa, eli että tietoa saavat käsitellä vain sellaiset tahot joiden on näitä tehtäviensä hoitamiseksi tarpeen käsitellä. Eheydellä puolestaan tarkoitetaan tiedon hallintaa, että tietoa saa muuttaa vain sellaiset käyttäjät, joilla on tähän oikeus, ja tiedon saatavuudella viitataan siihen, että tieto tulee olla helposti saatavilla sitä tarvitseville. (Rousku 2014, 47-50.)

Tietoturvaa voidaan ajatella käytännön toimenpiteinä ja keinoina, joilla yleisesti tieto suojataan, olipa kyse sitten henkilötiedoista tai muusta suojattavasta materiaalista, kuten yrityksen liikesalaisuuksista. Usein tietoturvallisuus mielletään pitkälti tekniseen tietoturvaan kuten erilaisten sähköisten tietojärjestelmien suojaamiseen palomuurein ja virustorjuntaohjelmin, mutta se kattaa paljon muutakin. Tietoturvallisuus pitää sisällään myös yrityksen yleiset toimintatavat, koko henkilöstön osaamisen sekä niin kutsutun fyysisen tietoturvallisuuden, jota voidaan toteuttaa esimerkiksi rajaamalla tiettyihin tiloihin pääsyä

lukitusten avulla. Tietoturvallisuus, niin kuin tietosuojakaan, ei siis ole pelkästään IT-alan asia, vaan perusasiat tulisi olla hallussa jokaisella tehtävänimikkeeseen tai alaan katsomatta.

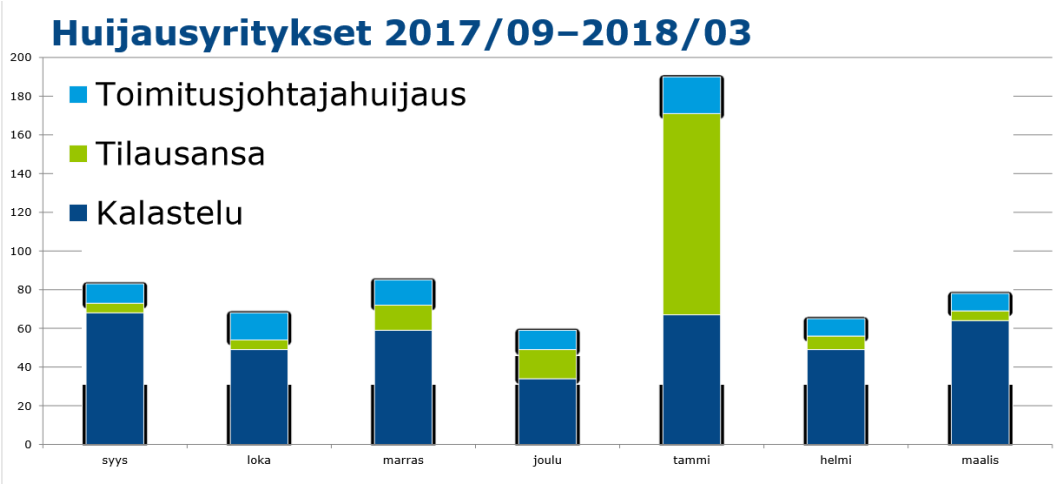
3.9.1 Kyberturvallisuus

Käsitteiden tietosuoja ja tietoturva rinnalle, on viime vuosina noussut myös uudempi termi, kyberturvallisuus. Digitalisoitumisen ja sähköisten palvelujen lisääntymisen myötä on tullut uusia uhkakuvia, jotka koskettavat kaikkia ja kaikkialla, niin yksilökohtaisesti, yhteiskunnallisesti kuin organisaatiotasollakin. Enää ei voi puhua, että vain tietokone olisi linkki internetin ihmeelliseen maailmaan, vaan netti on kaikkialla ympärillämme, mukana jokapäiväisessä tekemisessä. Tästä yleisin esimerkki lienee lähes jokaisen taskusta löytyvä älypuhelin. Internet of Things (IoT) eli suomeksi esineiden tai asioiden internet tulee olemaan vahvasti osana tulevaisuutta, kun tietoverkkoihin kytketyt älykkäät laitteet lisääntyvät ja luovat uusia mahdollisuuksia. Toisaalta myös uhkia. Muun muassa näitä uhkia tunnistetaan, ehkäistään ja niihin varaudutaan kyberturvallisuuden avulla.

Kyberturvallisuuden tarkoitus on varmistaa, että sähköisistä tietojärjestelmistä koostuvaan kybertoimintaympäristöön voi luottaa ja että sen toiminnasta huolehditaan. Valtaosa yhteiskunnan toiminnoista nojaa nykypäivänä ICT-teknologiaan ja kybertoimintaympäristöön. Tähän toimintaympäristöön kohdistuvat uhkakuvat eli ns. kyberuhat voisivat lamauttaa yhteiskunnan tai yrityksen kannalta kriittisen toiminnan, tai pahimmillaan kohdistua suureen määrään toimintoja. (Rousku 2014, 54-56.) Tällaisia uhkia ovat esimerkiksi erilaiset palvelunestohyökkäykset, haittaohjelmien leviäminen, tietojen kalastelu-yritykset ja vakoilu.

Digitalisoitumisen myötä tietoverkkoihin kohdistuva laiton toiminta ja tietotekniikkarikollisuus ovat lisääntyneet. Puhutaan kyberrikollisuudesta, jossa valtioiden rajat eivät ole rajoittava tekijä. (Poliisi 2018.) Erilaisista tietoverkon kautta tulleista huijausyrityksistä saa lukea mediasta tämän tästä ja kyberrikollisuuden kohteeksi ovat joutuneet niin yksityiset henkilöt, eri toimialojen yritykset, julkishallinto kuin muutkin organisaatiot. Yrityksiin kohdistuvia huijauksia ovat esimerkiksi erilaiset laskutushuijaukset, jossa yrityksen sähköpostiviestintää voidaan seurata ja lähettää laskun tiedot lähes identtisestä osoit-

teesta kun mihin tilaus on alun perin tehty. Laskujen sijaan, voidaan väärentää myös tilauksia. Toinen ansa mihin yritykset ovat langenneet on niin kutsuttu toimitusjohtajahuijaus, missä viestin lähettäjä lähestyy organisaation talousosaston työntekijää tekeytyen yrityksen toimitusjohtajaksi tai muuksi johtohenkilöksi vaatien pikaista tilisiirtoa tärkeän kaupan loppuun saattamiseksi. Työntekijän voi olla vaikea kyseenalaistaa johtajan kiireellistä käskyä, varsinkin kun viestissä saatetaan painottaa luottamuksellisuutta. Kuviosta 2 näemme Viestintäviraston kyberturvallisuuskeskuksen tietoon tulleet huijausyritykset Suomessa viimeisen puolen vuoden ajalta. Huijauksista suurin osa koostuu tietojen kalastelusta, mutta myös tilausansoja ja toimitusjohtajahuijauksia kirjataan kuukausittain. Mielenkiintoinen piikki näkyy tammikuun kohdalla jossa etenkin tilausansat ovat moninkertaistuneet (kuvio 2). Kysymyksenä herää, voisiko syynä tähän olla yritysten tilinpäätöskiireiden hyödyntäminen vai onko joulun ja uuden vuoden jälkeinen aika itsessään huijauksille otollinen ajankohta?



KUVIO 2. Huijausyritykset 2017/09-2018/03 (Viestintävirasto 2018)

3.9.2 Tietoturvaloukkauksista ilmoittaminen

Olipa kyse sitten kyberuhasta tai jostain muusta tietoturvaa vaarantavasta toiminnosta, jatkossa EU:n tietosuoja-asetuksen myötä tietoturvaloukkauksista on ilmoitusvelvollisuus. Tietoturvaloukkauksella tarkoitetaan Hannisen ym. mukaan ”loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin” (Hanninen ym. 2017, 108). Käytännössä tietoturvaloukkaus voi esimerkiksi olla palvelunestohyökkäys, jolloin yrityksen palveluita, useimmin verkkosivuja ei pystytä käyttämään, tai vastaavasti jokin

inhimillinen erehdys tietojen käsittelyssä, jonka seurauksena henkilötietoja on päässyt vuotamaan sellaisille tahoille, joilla ei ole oikeutta nähdä näitä.

Tietosuoja-asetuksen 33 ja 34 artikloissa määritellään, että rekisterinpitäjä on velvollinen ilmoittamaan tietoturvaloukkauksista sekä valvontaviranomaiselle että rekisteröidylle, paitsi jos tietoturvaloukkaus ei todennäköisesti aiheuta henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä. Valvontaviranomaiselle ilmoitus tietoturvaloukkauksesta on tehtävä 72 tunnin kuluessa ellei viivästykselle ole perusteltua selitystä. Rekisterinpitäjän on lisäksi dokumentoitava henkilötietoihin kohdistuvat tietoturvaloukkaukset, niiden vaikutukset ja toteutetut korjaavat toimenpiteet osoitusvelvollisuuden täyttämiseksi. Myös henkilötietojen käsittelijä on velvollinen ilmoittamaan havaitsemistaan tietoturvaloukkauksista rekisterinpitäjälle ilman aiheetonta viivytystä. (Asetus 2016/679/EU.) Asetus ei varsinaisesti kerro mistä kaikista tietoturvaloukkauksista ilmoitus tulee tehdä, vaan tämä jätetään rekisterinpitäjän harkinnan varaan.

3.10 Valvonta ja sanktiot

Tietosuoja-asetuksen yksi merkittävimmistä muutoksista on viranomaisille annetut valtuudet määrätä huomattavia sanktioita tietosuoja-asetusta rikkoville toimijoille. Valvontaviranomaiset voivat määrätä velvoitteiden rikkomisesta yritykselle hallinnollisia sakkoja, jotka maksimissaan voivat olla jopa 20 miljoonaa euroa tai 4% yrityksen liikevaihdosta, riippuen kumpi näistä summista on suurempi. (Hanninen ym. 2017, 129-130.) Tietosuoja-asetuksen 83 artiklassa on määritelty seikat, jotka tulee ottaa huomioon hallinnollisen sakon määräämisessä ja määrässä. Vaikuttavia tekijöitä ovat muun muassa rikkomisen luonne, vakavuus ja kesto huomioiden henkilötietojen käsittelyn luonteen, laajuuden ja tarkoituksen, sekä se, kuinka suureen joukkoon rekisteröityjä rikkominen vaikuttaa ja mikä on heille aiheutuneen vahingon suuruus. Huomioon tulee myös ottaa organisaation toteuttamat korjaavat toimenpiteet vahingon lieventämiseksi sekä yrityksen mahdolliset aiemmat vastaavat rikkomiset. (Asetus 2016/679/EU.)

Asetuksen luvussa kuusi säädetään valvontaviranomaisen toimivallasta, tehtävistä ja edellytyksistä. Jokaisen jäsenvaltion on määriteltävä yksi tai useampi viranomainen valvomaan asetuksen soveltamista, ja tämän valvontaviranomaisen tulee toimia täysin riippumattomasti hoitaessaan tehtäviään ja käyttäessään valtuuksiaan tietosuoja-asetuksen

mukaisesti. (Asetus 2016/679/EU.) Valvontaviranomaisen tehtävänä on asetuksen soveltamisen valvomisen lisäksi edistää tietosuojatietoisuutta sekä ohjeistaa tietosuoja-asioissa. Tehtäviensä suorittamiseksi valvontaviranomaisella on laajat valtuudet tutkia yrityksen tietosuoja-asioita kuten oikeus toteuttaa tarkastuksia, oikeus saada pääsy käsiteltäviin henkilötietoihin sekä oikeus päästä yrityksen tiloihin. Hallinnollisen sakon määräämisen lisäksi, valvontaviranomainen voi antaa erilaisia varoituksia, huomautuksia tai määräyksiä tietosuoja-asetuksen noudattamiseen liittyen. Suomessa valvontaviranomaisena on tietosuojalakiluonnoksen mukaan tarkoitus toimia tietosuojavirasto, mikä korvaisi nykyisen tietosuojavaltuutetun toimiston. (Hanninen ym. 2017, 124-125.)

4 ESIMIESTEN TIETOSUOJAKYSELY

4.1 Esimiesten rooli

Tietosuojavaltuutetun Reijo Aarnion mukaan esimiesten ja johdon rooli on keskeinen tietosuoja-asetuksen toteutumisen kannalta. Aarnio kuvailee, että johto on valitettavan usein jopa heikoin lenkki tietoturvaketjussa. Johto ohjeistaa, vastaa järjestelmien laillisuudesta ja tekee investointipäätökset, joten jos tietosuojalainsäädäntöä ei tunneta, on ongelmia väistämättä edessä. Aarnio painottaa, että esimiesten tulee toimia myös esimerkkinä tietosuoja-asioissa ja ohjeistaa alaisiaan toimimaan oikein. Esimiesten tulee osata kertoa mitä oikeuksia ja velvollisuuksia työntekijöillä on henkilötietojen käsittelyyn liittyen sekä kuinka näitä seurataan. (Aarnio 2017a, 2017b.)

Esimiesten rooli on keskeinen myös Verassa tietosuoja-asetuksen toteutumisen kannalta. Vaikka monet henkilötietojen käsittelyä sisältävät prosessit on ulkoistettu, käsittelevät kaikki esimiehet silti vähintäänkin omien alaistensa henkilötietoja, myös arkaluoteisia sellaisia. Esimiehet tekevät myös sopimuksia, ja käsittelevät sekä asiakkaiden että yhteistyökumppaneiden tietoja. Kaikkien esimiesten olisikin hyvä tuntea vähintäänkin uuden asetuksen mukaiset henkilötietojen käsittelyn yleiset periaatteet, käsittelyn laillisuusperusteet, rekisterinpitäjän velvollisuudet sekä rekisteröidyn oikeudet.

4.2 Kyselyn toteutus

Osana opinnäytetyötä Verassa toteutettiin tietosuojakysely, joka suunnattiin Veran esimiesasemassa oleville toimihenkilöille ja ylemmille toimihenkilöille, joita kyselyn toteutushetkellä oli 15. Kyselyn tarkoituksena oli selvittää, kuinka hyvin esimiehet hallitsevat tietosuojan perusasiat ja onko uusi asetus ennestään tuttu. Kyselylle nähtiin tarve, koska konsernin alkukartoituksessa tietosuojaan liittyen Verasta haastateltiin vain yhtä esimiesasemassa olevaa henkilöä. Kyselyyn ei kuitenkaan tässä opinnäytetyössä syvennytä yhtä laajasti kuin kyselytutkimuksiin perustuvissa opinnäytetöissä yleensä, vaan tämä toimi lähinnä selvityksenä täydentäen muuta aineistoa. Kyselyn avulla saatiin todenmukaisempi kuva Veran esimiesten tietosuojaosaamisen tasosta sekä mahdollisista puutteista.

Valmis kysely (liite 1) lähetettiin Veran esimiehelle sähköpostitse lyhyen saatteen ja kyselylinkin kera. Kysely toteutettiin ZEF-kyselytyökalun avulla ja se piti sisällään kyselyn kuvauksen, monivalintakysymykset ryhmiteltynä henkilötietojen käsittelyyn, tietosuojakäytäntöihin ja uuteen asetukseen varautumiseen, numeroarvion omasta tietosuojaosaamisesta sekä vapaapalautekentän. Kyselyssä vastausaikaa oli kaksi viikkoa, koska kaikki esimiehet olivat kyselyn toteuttamishetkellä töissä, eikä pidemmän vastausjakson koettu tuovan sen enempää vastauksia. Kyselystä muistutettiin kertaalleen niitä, jotka eivät kyselyyn olleet vielä ensimmäisen viikon jälkeen vastanneet.

4.3 Vastauksista yleisesti

Kyselytutkimuksen tulosten tulkintaan liittyy yleisesti joitakin heikkouksia. Hirsjärven, Remeksen ja Sajavaaran (2014, 195) mukaan kyselytutkimuksen haittoina voidaan pitää muun muassa sitä, että ei ole mahdollista varmistua kuinka vakavasti vastaajat ovat suhtautuneet kyselyyn, eli kuinka huolellisesti ja rehellisesti vastaajat ovat kysymyksiin vastanneet. Väärinymmärrykset ovat myös vaarana. Ei ole selvää kuinka onnistuneita vastausvaihtoehdot ovat vastaajien näkökulmasta, eikä välttämättä tiedetä kuinka vastaajat ovat ylipäätään selvillä aihealueesta josta kysymykset esitettiin. (Hirsjärvi, Remes & Sajavaara 2014, 195.) Vaikka vastausten tulkintaan liittyy joitakin ongelmia, voidaan kyselyn tuloksia pitää suuntaa antavana informaationa tutkimusaiheesta ja laatia näiden pohjalta erilaisia päätelmiä.

Esimiehet lähtivät vastaamaan kyselyyn aktiivisesti, ja vastausprosentiksi saatiin 80%, eli kyselyyn vastasi yhteensä 12. Vastaajien numeroarvio omasta tietosuojaosaamisestaan oli keskiarvoltaan noin 6,5 asteikolla 1-10 (liite 2). Tämä on laaja arvoasteikko, jossa ehkä paremmin olisi toiminut kouluarvosana 4-10, mutta keskiarvosta voidaan kuitenkin todeta, että puolivälin paremmalla puolella ollaan. Liitteen 2 mukainen raportti ei sovellu parhaiten tämän kohdan tulkintaan, koska raportti ei näytä mistä vastauksista keskiarvo on muodostunut. Raportista ei näe onko vastaukset asettuneet tasaisesti kuuden ja seitsemän väliin, vai onko vastauksien joukossa yksittäisiä poikkeamia suuntaan tai toiseen.

Seuraavaksi käydään tarkemmin läpi monivalintakysymyksien tulokset ja pohditaan kyselyn johtopäätöksiä. Mainittakoon vielä, että vapaapalautekenttään ei tullut kommentteja, tai kommentteja tuli niin vähän, ettei kyselytyökalu näitä anonymiteettisuojan vuoksi raportilla näyttänyt, joten vapaapalautekohtaa ei tämän enempää käsitellä. Voidaan kuitenkin todeta, että kysymyksiä tai kommentteja tietosuoja-asetuksen suhteen ei esimiehillä vielä tässä vaiheessa ollut, ainakaan siinä määrin että näitä olisi useampi esittänyt.

4.4 Monivalintakysymyksien vastaukset

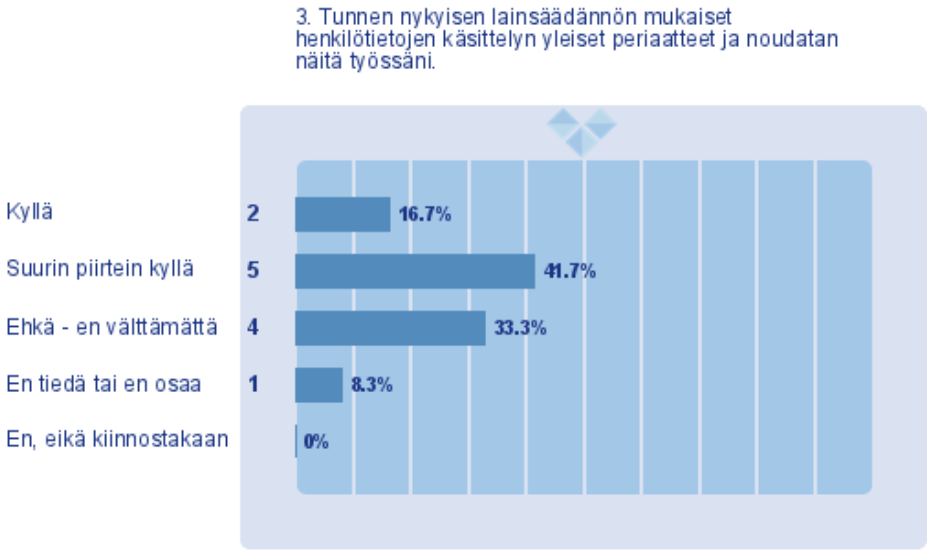
Monivalintakysymysten vastauksia tarkasteltaessa tulee tiedostaa muutama huomio, jotka saattavat vaikuttaa tulosten tulkintaan. Vastauksien totuudenmukaisuudesta ei voida mennä täysin takuuseen, vaikka pidänkin epätodennäköisenä, että vastauksia olisi tässä kyselyssä kovin paljoa vääristelty. Tämän lisäksi, kysymyksissä saattaa olla myös vastaajakohtaisia näkemyseroja. Vastaajan oma luulo ei aina välttämättä pidä paikkaansa, koska vastaajan arvio siitä, mitä tiedolla tarkoitetaan, voi vaihdella todellisen tiedon ja taidon kanssa. Esimerkiksi henkilötunnus luokitellaan usein virheellisesti arkaluonteiseksi, vaikka se ei todellisuudessa sitä ole, suojattava kylläkin. Vastaavasti ammattiyhdistystietojen arkaluonteisuus saattaa taas puolestaan tulla yllätyksenä. Yhtä kaikki, vastaukset kuitenkin kertovat pitkälti esimiesten osaamisen tasosta, vaikka näitä ei voidakaan pitää absoluuttisena totuutena.

4.4.1 Kysymysryhmä: henkilötietojen käsittely

Henkilötietojen käsittelyä koskevissa kysymyksissä pyrittiin selvittämään henkilötietojen käsittelyyn liittyvä perusosaaminen nykyiseen lainsäädäntöön peilaten, mikä kyselyn toteuttamishetkellä oli vielä Suomen henkilötietolaki. Vastanneista lähes kaikki tiesivät, tai suurin piirtein tiesivät mitä henkilötiedoilla, henkilötietojen käsittelyllä ja henkilörekisterillä tarkoitetaan, sekä olivat tietoisia myös siitä, mitä henkilötietoja työtehtävissään käsittelevät ja mihin tarkoitukseen (liite 2). Vain yksi vastaus oli ehkä – en välttämättä, kun kysyttiin termien merkitystä. Esimiesten voidaan siis todeta olevan tietoisia siitä, mitä henkilötietoja nämä käsittelevät ja mihin tarkoitukseen, sekä ymmärtävän, mitä näillä tiedoilla tarkoitetaan. Pieni kertaus ei kuitenkaan välttämättä olisi pahitteeksi, koska EU:n tietosuoja-asetus laajentaa henkilötiedon määritelmää nykyisestä, kun tunnistetietona

voidaan pitää lähes mitä tahansa tietoa, joka pystytään, joko suorasti tai epäsuorasti, yhdistämään luonnolliseen henkilöön.

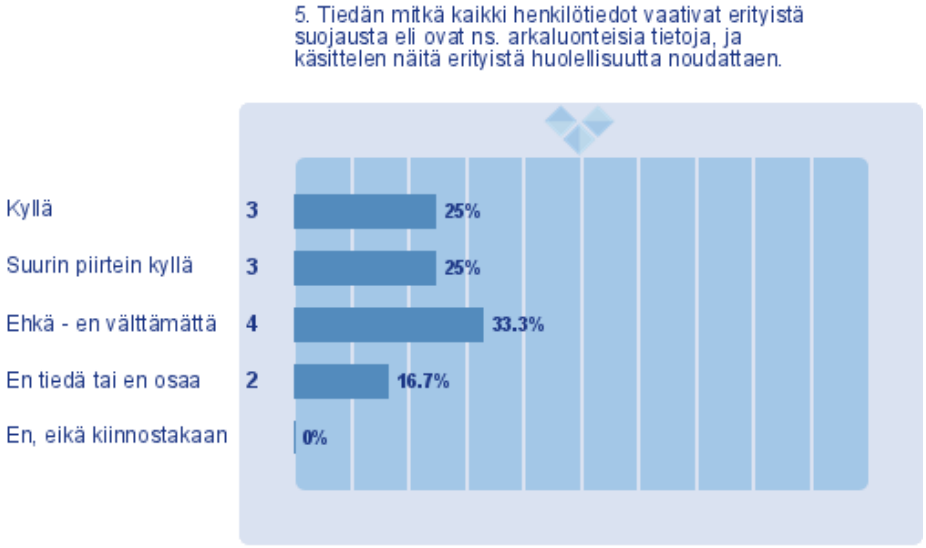
Loput henkilötietojen käsittelyä koskevat kysymykset aiheuttivat enemmän hajontaa. Yli puolet vastanneista ilmoitti tuntevansa, tai suurin piirtein tuntevansa, nykyisen lainsäädännön mukaiset henkilötietojen käsittelyn yleiset periaatteet ja noudattavansa näitä työssään (kuvio 3). Neljä vastaajista oli epävarmoja, antaen vastaukseksi ”ehkä - en välttämättä” ja yksi vastasi ”en tiedä tai en osaa”. Tässä on kehittämisen tai kehittymisen paikka, ja uuden asetuksen myötä on nyt viimeistään aika päivittää oma osaamisensa lain vaatimalle tasolle.



KUVIO 3. Henkilötietojen käsittely, kysymys 3 (liite 2)

Henkilötietojen luokittelusta ja arkaluonteisista tiedoista kysyttäessä, epävarmuus näkyi selvästi. Vain yksi osasi varmasti luokitella henkilötiedot eri suojausluokkien mukaan, eli tiesi miten tiedot tulee säilyttää oikein suojattuna. Vastanneista lähes puolet koki suurin piirtein osaavansa luokitella nämä, neljäsosa ehkä – ei välttämättä, ja toinen neljäsosa ei tiennyt tai ei osannut (liite 2). Arkaluonteisten tietojen kohdalla, puolet vastanneista tiesi, tai suurin piirtein tiesi, mitkä kaikki henkilötiedot vaativat erityistä suojausta eli ovat ns. arkaluonteisia tietoja, sekä käsittelivät näitä tietoja erityistä huolellisuutta noudattaen (kuvio 4). Kolmasosa vastanneista puolestaan kertoi ehkä tiedostavansa arkaluonteiset henkilötietoryhmät ja ehkä käsittelevänsä näitä erityistä huolellisuutta noudattaen, mutta ei-

vät välttämättä. Kaksi vastaajista katsoi, että eivät tiedä tai eivät osaa. Henkilötietoryhmien luokitteluun ja vaadittaviin suojaustoimenpiteisiin kaivataan siis lisäohjeistusta, koska tällä hetkellä nämä eivät kaikille esimiehille ole aivan selvillä.



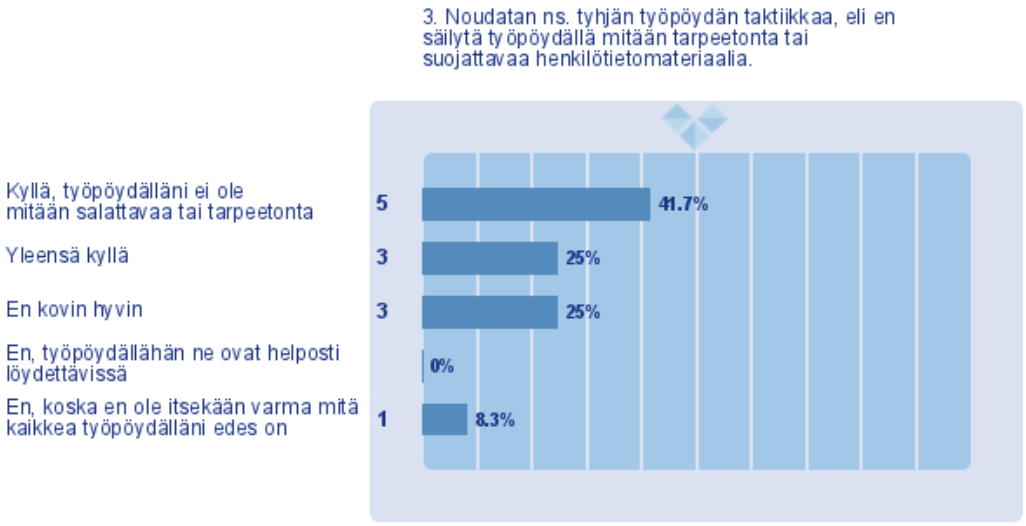
KUVIO 4. Henkilötietojen käsittely, kysymys 5 (liite 2)

4.4.2 Kysymysryhmä: tietosuojakäytännöt

Seuraavaksi kysymyksissä käsiteltiin yleisiä, tietosuojaan liittyviä toimintatapoja. Päätelaitteiden lukitseminen silloin, kun näitä ei käytä, on yksi perusasioista joita jokaisen organisaation työntekijän tulisi noudattaa asemaan katsomatta. Esimiesten tietosuojakyselyssä, puolet vastanneista kertoi lukitsevansa tietokoneensa aina, kun poistuu työpisteeltään, ja neljäsosa vastanneista kertoi lukitsevansa tietokoneen useimmiten. Yksi vastaajista kertoi lukitsevansa koneen työpisteeltä poistuttuaan joskus, jos muistaa, ja kaksi puolestaan ilmoitti lukitsevansa koneen harvoin. Muiden päätelaitteiden, kuten älypuhelimen ja tabletin lukitsemisen suhteen tilanne oli parempi, kun kaksi kolmasosaa vastanneista kertoi lukitsevansa muut päätelaitteet aina, kun ei näitä käytä ja yksi kolmasosakin kertoi lukitsevansa nämä useimmiten (liite 2). Nämä ovat pieniä, helposti toteutettavissa olevia käytäntöjä, jotka ovat korjattavissa yksinkertaisilla toimintatapojen muutoksilla.

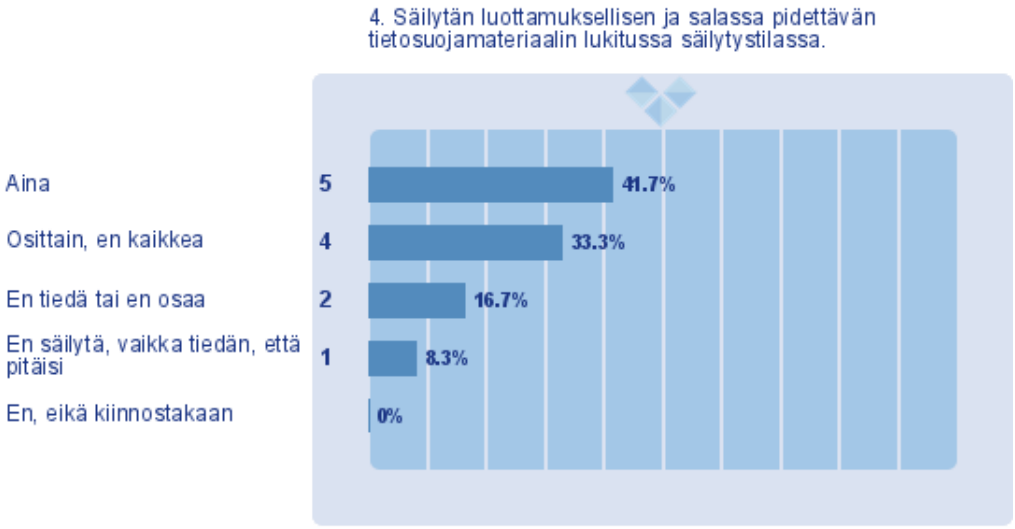
Toinen perusasia, on tiedostaa mitä työpöydällä saa säilyttää ja mitä ei. Työpöydällä lojuvat luottamuksellisia tai arkaluonteisia tietoja sisältävät dokumentit ovat yksi huomattava tietoturvariski, etenkin avokonttorissa. Lähes puolet vastanneista oli sitä mieltä, että

heidän työpöydillään ei säilytetä mitään salassa pidettävää tai tarpeetonta henkilötietomateriaalia eli noudattavat ns. tyhjän työpöydän taktiikkaa (kuvio 5). Neljäsosa vastanneista kertoi noudattavansa tätä taktiikkaa yleensä, kun taas toinen neljäsosa katsoi, että eivät noudata kovin hyvin. Yksi vastaajista kertoi, että ei ole itsekään varma mitä työpöytä pitää sisällään, joten tyhjän työpöydän taktiikkaa ei silloin toteudu. Kukaan vastaajista ei ollut kuitenkaan sitä mieltä, että työpöydällä on hyväksyttävää säilyttää henkilötietoja, kuten kuvion 5 vastauksitta jääneellä vastausvaihtoehdolla haettiin takaa.



KUVIO 5. Tietosuojakäytännöt, kysymys 3 (liite 2)

Seuraava kysymys viittaa jokseenkin edelliseen, ja voisikin olettaa, että samat viisi vastaajaa, jotka kertovat noudattavansa tyhjän työpöydän taktiikkaa, säilyttävät myös aina luottamuksellisen ja salassa pidettävän tietosuojamateriaalin lukitussa säilytystilassa kuten kuviosta 6 näemme. Kolmasosa katsoi toteuttavansa tätä osittain, mutta ei kaikilta osin, ja kaksi vastaajista taas ei tiedä tai ei osaa toteuttaa tätä kohtaa. Yksi vastaajista kertoo, että ei säilytä luottamuksellista ja salassa pidettävää tietosuojamateriaalia lukitussa säilytystilassa, vaikka tietää että pitäisi (kuvio 6). Tässä kysymyksessä tietosuojamateriaalilla tarkoitettiin nimenomaan fyysistä materiaalia, mikä näkyi kyselytyökalussa kysymyksen kohdalla sulkeissa huomiona (liite 1).



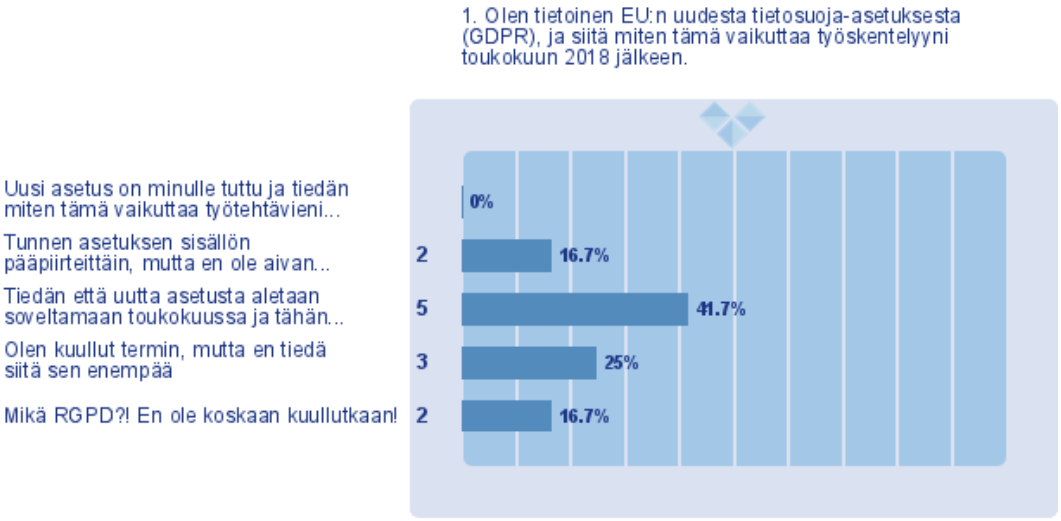
KUVIO 6. Tietosuojakäytännöt, kysymys 4 (liite 2)

Viimeiseksi tietosuojakäytäntöihin liittyen, tiedusteltiin sähköisen toimintaympäristön toimintatavoista, eli kokeeko henkilö tuntevansa asianmukaiset suojaustoimenpiteet digitaalisessa ympäristössä. Asianmukaiset suojaustoimenpiteet voidaan nähdä vastaajasta riippuen hyvin erilaisina, mutta kysymys kertoo kuitenkin jotain vastaajan osaamisen tasosta. Kaksi vastaajista osasi omasta mielestään toimia digitaalisessa ympäristössä turvallisesti, ja lähes puolet, eli viisi vastaajaa kertoi hallitsevansa perusasiat, mutta kaipaavansa lisäohjeistusta. Kolmasosa vastanneista katsoi tuntevansa asianmukaiset suojaustoimet jotenkuten, ja yksi vastaaja oli sitä mieltä, että ei tiedä tai ei osaa (liite 2). Ymmärsipä vastaaja asianmukaiset suojaustoimenpiteet miten hyvänsä, digitaalisen toimintaympäristön turvallisiin toimintatapoihin tulisi ehdottomasti ohjeistaa enemmän, niin esimiehiä kuin koko henkilöstöä. Ohjeistamisen tulisi olla jatkuvaa, koska digiaikakauden sähköinen toimintaympäristö muuttuu ja kehittyy jatkuvasti.

4.4.3 Kysymysryhmä: varautuminen uuteen tietosuoja-asetukseen

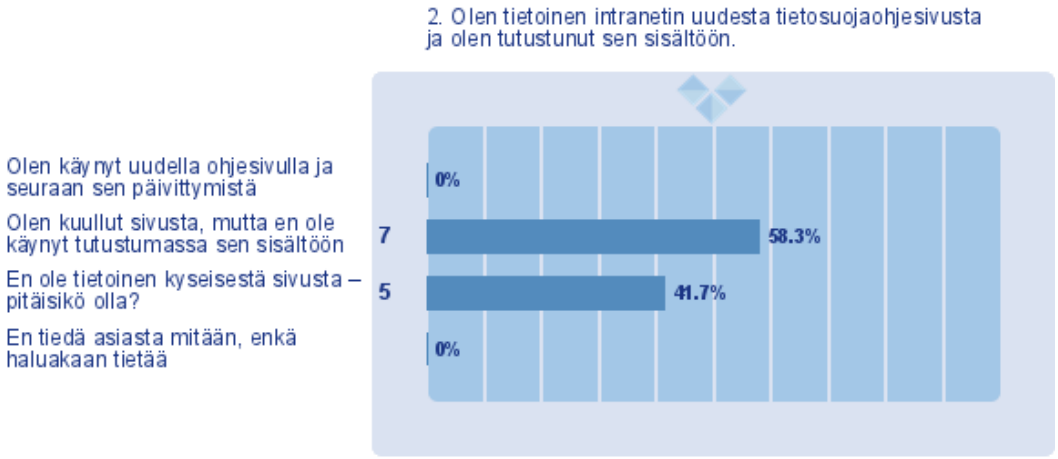
Viimeinen kysymysryhmä koski EU:n tietosuoja-asetukseen varautumista, eli kysymyksillä kartoitettiin, miten hyvin uusi asetus oli kyselyn toteuttamishetkellä vastaajilla hallussa. Kaksi vastanneista kertoi tuntevansa asetuksen sisällön pääpiirteittäin, mutta eivät olleet aivan varmoja, kuinka asetus koskettaisi omaa toimenkuvaa (kuvio 7). Kukaan vastanneista ei ollut perehtynyt tietosuoja-asetukseen niin hyvin, että olisi tuntenut asetuksen sisällön sekä tiennyt miten tämä vaikuttaa omien työtehtävien hoitamiseen. Lähes puolet

vastanneista kertoi tietävänsä, että uutta asetusta aletaan soveltamaan toukokuussa 2018, ja tähän tulisi jotenkin varautua, mutta eivät tienneet miten. Neljäsosa puolestaan oli kuullut termin, mutta ei tiennyt tästä sen enempää, ja kaksi vastaajaa ei ollut koskaan kuullutkaan ”RGPD:stä” (kuvio 7). GDPR aiheena on ajankohtainen ja uusi, joten on ymmärrettävää, että tämä ei käytännön tasolla ole vielä monellekaan avautunut.



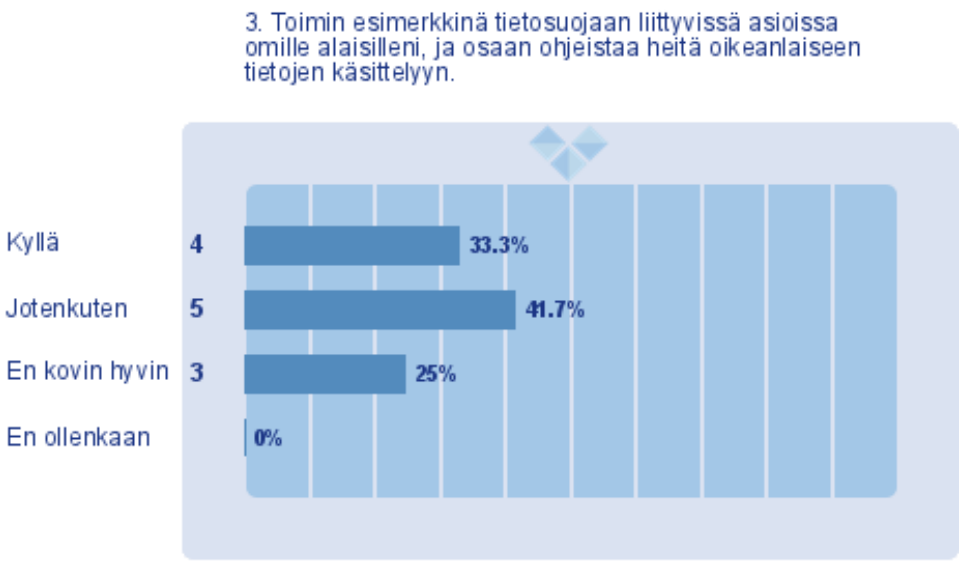
KUVIO 7. Varautuminen uuteen tietosuoja-asetukseen, kysymys 1 (liite 2)

Kyselyssä tiedusteltiin myös, olivatko esimiehet tietoisia Sähkölaitoksen intranetin uudesta tietosuojaohjesivusta, josta tietoa voisi tarvittaessa hakea, ja johon tietosuoja-asetuksen toteutumiseen liittyviä asioita jatkossa päivitettäisiin. Suurin osa vastanneista, eli seitsemän esimiestä oli kuullut sivusta, mutta eivät olleet vielä käyneet tutustumassa sen sisältöön, kun taas loput vastaajat eivät olleet tietoisia kyseisestä sivusta (kuvio 8). Kuviosta 8 näemme, että vastausvaihtoehdot ”en tiedä asiasta mitään, enkä haluakaan tietää” ja ”olen käynyt uudella ohjesivulla ja seuraan sen päivittymistä” jäivät tyhjiksi. Uusi tietosuojaohjesivu toivottavasti tulee jatkossa esimiehille enemmän tutuksi, kun uutta tietosuoja-asetusta aletaan soveltamaan, ja ohjesivu saa enemmän sisältöä myös käytännön toimintatapoihin ja työmenetelmiin liittyen.



KUVIO 8. Varautuminen uuteen tietosuoja-asetukseen, kysymys 2 (liite 2)

Viimeinen monivalintakysymys tässä osiossa kartoitti esimiesten esimerkkinä toimimista tietosuoja-asioissa, minkä tärkeyteen viitattiinkin jo luvun alussa. Esimiehen rooli tietosuoja-asetuksen toteutumisen kannalta on keskeinen, ja käytännön toimintatapojen jalkauttaminen vaatii oikeanlaista ohjeistamista sekä esimerkkinä toimimista. Kolmasosa vastanneista oli sitä mieltä, että he toimivat esimerkkinä tietosuojaan liittyvissä asioissa omille alaisilleen ja osaavat ohjeistaa näitä oikeanlaiseen tietojen käsittelyyn (kuvio 9). Lähes puolet vastanneista, eli viisi vastaajaa kertoi tämän käyvän toteen jotenkuten, kun taas neljäsosa ei pitänyt itseään kovin hyvänä esimerkkinä (kuvio 9).



KUVIO 9. Varautuminen uuteen tietosuoja-asetukseen, kysymys 3 (liite 2)

4.5 Kyselyn johtopäätökset

Yleisesti ottaen, alkuun voidaan mainita, että vastauksia tulkittaessa oli positiivista huomata, että yhtäkään ”en, ei kiinnosta” tai vastaavaa vastausta ei ollut missään osiossa. Tämä vastausvaihtoehto lisättiin valintoihin, koska haluttiin selvittää mahdollinen negatiivinen asenne tietosuoja-asioita kohtaan. Tietämättömyys tai ohjeistuksen puute on kuitenkin aina paljon helpompi korjata kuin ns. asennevika.

Kyselyn yhteenvetona voidaan todeta, että esimiesten tietosuojaosaamisessa havaittiin joitakin puutteita. Nykyistä lainsäädäntöä ei kaikilta osin tunnettu ja tietosuojakäytännöissäkin oli jonkin verran parannettavaa. Suurin tiedon puute näkyi EU:n tietosuoja-asetuksessa ja sen vaikutuksissa suhteessa omiin työtehtäviin. Vastausten perusteella voidaan päätellä, että havaitut heikkoudet johtuvat pitkälti tietämättömyydestä, joten kehitystoimenpiteiden tulisi pohjautua riittävän ohjeistuksen lisäämiseen.

Kouluttautumista on osin jo toteutettu, kun Tampereen Sähkölaitos -konserni järjesti ja järjestää huhti-toukokuussa henkilöstölle GDPR-koulutukset. Nämä koulutukset olivat kyselyn toteutushetkellä kuitenkin vasta suunnitteilla, joten voidaan olettaa, että esimiesten tietämys uudesta asetuksesta sekä henkilötietojen käsittelyn lainmukaisuudesta paranevat näiden koulutustilaisuuksien myötä. Henkilöstön osaamisen lisäämiseen palataan vielä tarkemmin seuraavassa luvussa, jossa lisäksi pohditaan myös muita toimenpiteitä tietosuojakyselyn tulosten pohjalta.

5 TOIMENPITEET VERASSA

5.1 Konsernin kehitystyö

Seuraavaksi tarkastellaan tietosuoja-asetuksen toteutumista Verassa sekä esitetään mahdollisia muutostarpeita Veran toimintaan liittyen. Kehitystoimenpiteitä pohditaan niin esimiesten tietosuojakyselyn tulosten valossa, kuin omaan työkokemukseen perustuvan havainnoinnin pohjalta. Kun puhutaan Veran tietosuojasta, sen nykytilanteesta tai kehityksestä, on oleellista avata ensin emoyhtiön eli Tampereen Sähkölaitos Oy:n roolia ja tämän suhdetta tytäryhtiöönsä eli Veraan.

Tietosuojan nykytilakartoitus, niin kuin monet muutkin kehityshankkeet ovat konsernitasolta lähtöisin, ja näin emoyhtiöstä käsin johdettuja projekteja. Tietosuojan kehitystyö ja toteuttamiskäytänteet priorisoidaan, ja projekti etenee työvaihe kerrallaan, kohti tietosuoja-asetuksen toteutumista kaikissa Sähkölaitos -yhtiöissä. Tätä opinnäytetyötä kirjoittaessa emoyhtiössä on toteutettu jo tietosuojatyön osalta koko konsernin nykytila-analyysi, kehityssuunnitelma sekä riskien kartoitus. Tätä opinnäytetyötä kirjoittaessa tietosuojatyö etenee myös muilta osin, kun tietosuojakoordinaattorin johdolla kehitetään Sähkölaitos -yhtiöiden tietosuojan hallintamallia ja tietosuojapolitiikkaa, käydään läpi yhteisiä sopimuspohjia, laaditaan tietosuojaselosteita, koulutetaan henkilöstöä sekä toteutetaan muita tietosuoja-asetuksen vaatimia toimenpiteitä. (Toivonen 2018a.) Konsernilla on samaan aikaan myös muita tietosuojatyötä tukevia hankkeita kuten tietoturvan kehittämisprojekti ja tietojärjestelmien osittainen uusiminen. Tietosuojatyön kehittäminen ja asetuksen toteutuminen etenevät siis vauhdilla konsernitasolla, ja tästä hyötyvät kaikki yhtiöt.

Tampereen Sähkölaitoksen tietosuojakoordinaattorin Marianne Toivosen mukaan konsernia voidaan ajatella yhtenä rekisterinpitäjänä eikä emo- ja tytäryhtiöiden välillä tarvita erillisiä käsittelysopimuksia. Roolikysymyksissä jokainen toimintayksikkö on kuitenkin vastuussa omista toiminnoistaan ja viimekädessä tietosuojan toteutumisesta vastaa yhtiön toimitusjohtaja. Kun konsernia käsitellään yhtenä rekisterinpitäjänä, jokaisen yhtiön ei tarvitse esimerkiksi erikseen tehdä selosteita henkilötietojen käsittelytoimista vaan yksi ja sama tietosuojaseloste käy kaikissa Sähkölaitos -yhtiöissä. Toivosen mukaan konser-

nissa selosteet tullaan laatimaan loogisten kokonaisuuksien mukaan eli selosteita ei toteuteta järjestelmäkohtaisesti vaan luodaan yksi kattava tietosuojaseloste kutakin tiedon käsittelyprosessia kohtaan. Esimerkiksi asiakastiedon käsittelyseloste pitää sisällään koko asiakastiedon elinkaaren, aina asiakkuuden alkuvaiheista sen päättymiseen asti. (Toivonen 2018b.)

5.2 Tiedon läpikäynti

Vuosien saatossa, henkilötietojen kerääminen ja tallettaminen on Verassa ollut vaihtelevaa. Henkilötietoja saattaa olla henkilöstön omilla työasemilla, verkkolevyillä, työpöydällä, sähköpostissa, OneDrivessa, intranetin SharePointissa, muistitikuilla tai kaapeissa ja laatikoissa. Ei välttämättä tiedetä, mitä tietoa missäkin on ja onko tiedon säilyttämiseen olemassa laillinen peruste. Tieto saattaa olla vanhentunutta tai sitä ei ole suojattu riittävin teknisin ja organisatorisin keinoin. Jokaisen esimiehen ja muiden henkilötietoja käsittelevien työntekijöiden tulisikin ennen tietosuoja-asetuksen voimaan tuloa käydä läpi henkilökohtaiset työasemat, tallennuslaitteet sekä fyysinen tietosuojamateriaali ja tarkastaa mitä henkilötietoja näissä säilötään. Myös sähköpostin sisältö olisi hyvä käydä läpi koska sähköpostia ei ole tarkoitettu tiedon tallentamiseen. Asetuksen tietojen käsittelyn minimointia ja tarpeellisuusperiaatetta noudattaen, kaikki tarpeeton tieto tulisi hävittää asianmukaisesti ja jäljelle jäävä tieto tallettaa riittäviä suojaustoimenpiteitä noudattaen.

Fyysisen tietosuojamateriaalin osalta tietojen läpikäynti toteutettiin Verassa pitkälti jo helmi-maaliskuussa, kun toimitilaremontin yhteydessä ohjeistettiin henkilöstöä käymään läpi kaikki kaapit ja laatikostot. Vanha toimistotila remontoitiin, jolloin saman katon alle saatiin sopimaan koko henkilöstö, kun se aiemmin oli jakautunut kahteen eri rakennukseen. Remontin yhteydessä tuli säilyttää vain tarpeellinen materiaali ja hävittää kaikki tarpeeton asianmukaisesti, eli luottamuksellinen tai salassa pidettävä tietosuojamateriaali lukittaviin tietosuoja-astioihin ja muu julkinen materiaali paperinkeräykseen. Jos remontin jäljiltä on jäänyt vielä joitakin laatikoita tai kansioita odottamaan tarkempaa tarkastelua, tulee nämä viimeistään nyt käydä läpi. Ohjeistetaan siis esimiehiä, ja muita toimistohenkilöitä toteuttamaan tiedon, eritoten sähköisen, läpikäynti ennen asetuksen voimaan tuloa.

Niiden tietojärjestelmien osalta, jotka ovat vain Verassa käytössä on myös hyvä käydä läpi henkilötietojen käsittelyprosessi ja käyttöoikeushallinta. On selvitettävä, kuka tiedon eheydestä kussakin järjestelmässä Verassa vastaa eli kuka pitää huolen käyttöoikeuksien ajantasaisuudesta sekä lisää, poistaa ja ylläpitää tietoa. Tulee myös selvittää ovatko kyseiset tietojärjestelmät tietoturvallisuudeltaan riittäviä täyttämään asetuksen mukaiset vaatimukset. Verassa esimerkiksi ainakin seuraavat järjestelmät ovat konsernista poikkeavia: palkkojen esitietojärjestelmä, tuntikirjausjärjestelmä, henkilökorttien tilausjärjestelmä, kyselytyökalu sekä lounaskorttijärjestelmä. Näistä kuitenkin muut kuin kyselytyökalu ja henkilökorttien tilausjärjestelmä, ovat konsernin kehitystyön ja käytäntöjen yhtenäistämisen tuloksena lyhyellä aikavälillä poistumassa tai vaihtumassa, joten näihin ei ole tarvetta tietosuojatyön puitteissa käyttää nyt aikaa. Uusissa järjestelmissä huomioidaan sisäänrakennetun ja oletusarvoisen tietosuojan periaate eli selvitetään asetuksen mukaiset vaatimukset jo näiden hankintavaiheessa.

5.3 Avokonttorin haasteet

Toimitilaremontin myötä, uusi avokonttori tuo haasteita tietosuojan toteutumiselle. Erilliset työhuoneet on purettu ja kahden eri liiketoimintayksikön työpisteet sijoitettu nyt yhteen avoimeen tilaan. Uuden toimistotilan myötä, tiedonkulku paranee ja yhteistyö lisääntyy, mutta tietosuojan toteutumisen suhteen tiivis avokonttori ei ole ihanteellinen. Toimistoon pääsy ulkopuolisilta on rajattu kulkuoikeuksin, mutta myös omat työntekijät sekä toimitiloissa vierailijat aiheuttavat mahdollisen tietosuojariskin, kun esimerkiksi salattava materiaali saattaa päättyä inhimillisen virheen tai huolimattoman toiminnan seurauksena väärille tahoille. Jotta eheys ja luottamuksellisuus toteutuisivat henkilötietojen käsittelyssä, tulee henkilöstön osata sopeuttaa toimintansa avokonttoriympäristöön. Esimerkiksi, koska avokonttorin työpisteiden sermit eivät takaa täydellistä näkösuojaa koneen näytölle, tulee suojattavia tietoja käsiteltäessä olla erityisen varovainen, jotta sivulliset eivät näe luottamuksellisesti käsiteltäviä tietoja. Esimiehille sekä niille työntekijöille jotka käsittelevät työtehtävissään salaista tietosuojamateriaalia, voisi harkita tietokoneiden näyttöihin tietosuojakalvojen hankintaa, joka rajaisi näkyvyyttä paremmin sivullisten katseilta. Toisaalta, kukaan henkilöstöstä ei käsittele salattavia henkilötietoja päätoimisena tehtävänään, vaan käsittely on lähinnä satunnaista, joten voisiko luottaa siihen, että käsittelijät osaavat seurata toimintaympäristöään ja ajoittaa käsittelytoimet niin, ettei sivullisia ole näköetäisyydellä? Kannettavissa tietokoneissa tietosuojakalvo olisi kuitenkin

hyvä olla ns. vakiovarusteena kun liikutaan työpaikan ulkopuolella, jolloin toimistoympäristöä tarkemmin tulee huomioida myös muiden yrityksen liiketoimintaan liittyvien tietojen suojaus.

Koen tarpeellisena, että avokonttorin perustietosuojakäytänteistä olisi hyvä muistuttaa henkilöstöä, erityisesti esimiehiä sekä muita toimistossa työskenteleviä. Työpisteeltä poistuttaessa, tietokoneet sekä muut päätelaitteet tulisi aina lukita ja keskustelu sovittaa avokonttoriin sopivaksi. Suojattavaa paperiaineistoa ei saa jättää työpöydälle, tai muuallekaan toimistoon nähtäville, ja salassa pidettävä tietosuojamateriaali tulee säilyttää jatkossa lukitussa säilytystilassa. Säilytystilat ja kaappiratkaisut tulee uudessa toimistossa katsoa niin, että kaapit ja laatikostot ovat tarpeen mukaan lukittavia, ja että pääsy sisältöön on rajattu vain niille, joilla on työtehtäviensä puitteissa oikeus käsitellä kyseistä tietoa. Jotta tietosuoja-asiat huomioitaisiin uuden konttorin myötä entistä paremmin, luotiin kymmenen kohdan ohjeistus Veran toimiston tietosuojakäytännöistä. Tämä ohjeistus on suunnattu esimiehille sekä niille, joilla Veran toimitiloissa on kiinteä työpiste ja käsittelevät työtehtäviensä puitteissa tietosuojattavaa materiaalia. Ideoinnin tukena käytettiin Tampereen seudun kuntien ja kaupunkien henkilöstölle tarkoitettua tietoturva- ja tietosuojaopasta (Tampereen seudun tietoturvaryhmä 2016).

1. Seuraa ja noudata sekä konsernin yhteisiä, että Veran omia tiedotteita ja tietosuojaohjeita. Ylläpidä ja kehitä mahdollisuuksien mukaan omaa osaamistasi tietosuojaan ja tietoturvallisuuteen liittyen.
2. Sovita keskustelusi, tapahtuivatpa nämä sitten kasvotusten, puhelimitse tai muiden viestintävälineiden kuten Skypen välityksellä, avokonttoriympäristöön sopiviksi aina kunkin vallitsevan tilanteen mukaan. Jos keskusteluissa käsitellään luottamuksellista sisältöä, tulisi tällöin siirtyä vetäytymistiloihin (”puhelinkoppi”, erilliset neuvottelutilat) puhumaan asiasta.
3. Kiinnitä erityistä huomiota ympäristöön silloin, kun käsittelet suojattavaa materiaalia päätelaitteella. Avokonttorin sermit eivät takaa täydellistä näkösuojaa koneen näytölle ja riskinä on, että sivulliset näkevät nämä tiedot.
4. Noudata ns. tyhjän työpöydän taktiikkaa. Älä säilytä työpöydällä mitään tarpeetonta tietoa, etenkään salassa pidettävää aineistoa. Kaikki salattava tietosuojamateriaali tulee säilyttää lukitussa säilytystilassa, jonne vain niillä henkilöillä on pääsy jotka ovat oikeutettuja näitä työtehtäviensä puitteissa käsittelemään.

5. Hävitä tarpeeton suojattava tietosuojamateriaali turvallisesti, käyttämällä esimerkiksi lukittua tietosuoja-astiaa luottamuksellisen paperidokumentin hävittämiseen.
6. Vältä turhaa tulostamista ja kopiointia.
7. Lukitse tietokoneesi aina kun poistut työpisteeltä tai sen välittömästä läheisyydestä. Lukitse myös muut päätelaitteet (kuten puhelin tai tabletti) aina kun nämä eivät ole käytössä.
8. Käytä matkapuhelimissa ja/tai tableteissa suojakoodia sekä automaattista lukitusta. Säädä tarvittaessa myös näytölle tulevien ilmoitusten näkyvyyttä. Vaihda laitteissa valmiina olevat oletusarvoiset PIN-koodit ja huolehdi aina laitteiden ajantasaisista päivityksistä.
9. Käytä vahvoja salasanoja, jotka sisältävät niin isoja kuin pieniäkin kirjaimia, numeroita sekä erikoismerkkejä. Älä käytä salasanana mitään käyttäjään helposti yhdistettävää tunnusta kuten omaa sukunimeä tai syntymäaikaa. Pidä salasanat aina salassa muilta, myös kollegoilta. Vältä saman salasanan käyttöä useammassa eri järjestelmässä, äläkä käytä työpaikan tunnuksia tai salasanoja muualla Internetissä, jos nämä eivät liity työtehtävien hoitamiseen.
10. Huolehdi myös muiden työvälineiden, joiden katoaminen tai väriin käsiin joutuminen voi aiheuttaa tietoturvariskin, asianmukaisesta käsittelystä ja säilyttämisestä. Tällaisia ovat esimerkiksi avaimet, kulkunapit, henkilökortit sekä luottamuksellista tietoa sisältävät muistitikut.

5.4 Arkaluonteisten henkilötietojen käsittely

Erityisten henkilötietoryhmien eli ns. arkaluonteisten tietojen käsittelyyn tulee jatkossa kiinnittää Verassa erityistä huomiota. Aiemmin arkaluonteista tietoa sisältävät dokumentit on saatettu jättää työpöydälle ja luotettu siihen, että kun lääkärintodistus on käännetty pöydälle nurin päin, niin sitä eivät sivulliset tällöin käännä ja katso. Arkaluonteisten tietojen luokittelusta tulisi muistuttaa henkilöstöä ja ohjeistaa näiden oikeaoppiseen käsittelyyn. Tietosuojamateriaalille tulee hankkia toimistoon lukittu lokero tai postilaatikko, johon lääkärintodistukset ja muu luottamuksellinen materiaali jätetään, jos dokumenttia ei toimiteta henkilökohtaisesti sen käsittelijälle.

Arkaluonteisia tietoja, kuten työntekijöiden sairauslomatodistuksia, ovat Verassa saaneet käsitellä esimiehet, lähtökohtaisesti omien alaistensa osalta sekä sihteeri, joka on lähettänyt lääkärintodistukset keskitetysti palkanlaskentaan ja kirjannut nämä myös palkkojen esitietojärjestelmään. Palkkojen esitietojärjestelmään kirjataan kuitenkin vain tuntipalkkaisten työntekijöiden sairauslomajaksot, joten kuukausipalkkaisten työntekijöiden sekä toimihenkilöiden lääkärintodistukset on toimitettu sihteerille vain jatkolähetystä varten. Koska sihteeri ei tarvitse muiden kuin tuntipalkkaisten sairauslomatodistustietoja, tulisi käytäntö miettiä käsittelyn tarpeen ja minimoinnin valossa uudestaan. Joko esimiehen tulisi itse postittaa nämä tai jos posti halutaan lähettää keskitetysti, tulisi sairauslomatodistukset toimittaa suljetussa sisäisessä kirjekuoressa lukittuun lokeroon, josta nämä niputettaisiin ulos lähtevään kirjekuoreen.

Jatkossa, kun käytössä oleva palkkojen esitietojärjestelmä poistuu, tulee miettiä uudelleen, onko sihteerin kautta enää tarpeen kierrättää mitään sairauslomatodistuksia. Jos erityistä tarvetta arkaluonteisen tiedon käsittelyyn ei löydy, tulee tämä käsittelyn vaihe poistaa ja esimiehen huolehtia lääkärintodistuksen toimittamisesta itse. Tulevaisuudessa mahdollista voisi olla, että fyysisistä sairauslomatodistuksista päästäisiin kokonaan eroon ja lääkärin todistukset siirtyisivät suojattua yhteyttä pitkin työterveyshuollolta esimiehelle sekä muille tarvittaville tahoille, mutta niin kauan kuin tämä ei vielä ole mahdollista, tulee suojaustoimenpiteitä parantaa nykyisestä.

Lääkärintodistukset, niin kuin moni muukin fyysinen tietosuojamateriaali lähetetään tällä hetkellä postitse Veran toimipisteestä. Sekä lähtevä että saapuva posti sijaitsee rakennuksen aulassa, johon toimiston aukioloaikana on pääsy kenellä tahansa. Kirjesalaisuus on laissa säädetty, mutta riskinä on kirjepostin luvaton avaaminen tai varastaminen. Vaikka kirjeiden lähetys ja postiliikenne ovat Verassa verrattain vähäistä, ja tulevaisuudessa oletettavasti vielä vähenemään päin, olisi nykyisiin postituskäytäntöihin harkittava parempia suojaustoimenpiteitä. Saapuva posti olisi hyvä saada lukittuun postilaatikkoon, sekä lähtevän postin kohdalla miettiä ratkaisua, jolla lähtevää postia pystyttäisiin paremmin suojaamaan. Voisiko postin työntekijällä olla avain meidän lukittuun säilytystilaan, saisiko postilta itseltään suojattua kirjelaatikkoa käyttöön tai olisiko jokin muu käytännön ratkaisu parempi?

5.5 Henkilöstön osaaminen ja ohjeistus

Henkilöstön kouluttaminen ja ohjeistus ovat osana EU:n tietosuoja-asetuksen osoitusvelvollisuuden toteuttamista. Sähkölaitos -yhtiöiden työntekijöille järjestettiin ja järjestetään huhti-toukokuun aikana GDPR-koulutukset, jotka kirjataan koulutusrekisteriin. Koulutuksia on kaksi erilaista. Laajempi ”luokkahuonekoulutus” on tarkoitettu HR- ja asiakastiedon käsittelijöille, missä käydään läpi myös yleiset henkilötietojen käsittelyn perusperiaatteet. Suppeampi nettiperehdytys toimii peruskoulutuksena muulle henkilöstölle. Osaamista ylläpidetään kerran vuodessa toteutettavin tietosuojakoulutuksin ja lisäksi laaditaan roolikohtaisia käytännön työohjeita. Intranetin tietosuojaohjesivulle päivitetään aiheeseen liittyvää materiaalia ja opastetaan tietosuoja-asioissa. (Toivonen 2018b.) Verasta laajempaan GDPR- koulutukseen on nimetty esimiehet, sihteerit, luottamushenkilöt sekä työsuojeluvaltuutetut. Koulutus antaa kattavan kuvan uudesta tietosuoja-asetuksesta ja sen sisällöstä. Koulutuksessa kerrotaan myös, kuinka tietosuojatyö konsernissa etenee. Varsinaisia käytännön ohjeistuksia, esimerkiksi esimiehille, koulutus ei vielä sisältänyt, vaan näihin palataan myöhemmin yksityiskohtaisemmalla tasolla.

Veran koulutusyhteyshenkilönä seuraan tilaisuuksiin osallistumista siten, että pakollinen koulutus tulisi kaikilla Veran työntekijöillä suoritetuksi. Jos ns. luokkahuonekoulutuksiin ei määrätyt henkilöt syystä tai toisesta pääse, on koulutuksesta katsottavissa myös tallenne, jonka avulla koulutuksen voi suorittaa. Muun henkilöstön perehdytyksen suhteen tulee Verassa miettiä tarkempi toteutustapa, sekä se, kuinka nettiperehdytyksien suorittamista valvotaan. Asentajien osalta, järkevin vaihtoehto voisi olla verkkokoulutuksen suorittaminen esimerkiksi tiimipalaverin yhteydessä, jolloin esimies voisi valvoa perehdytyksen suorittamista, olisi paikalla vastaamassa mahdollisiin kysymyksiin ja antaisi tarvittaessa yksityiskohtaisempia ohjeistuksia.

Mitä tulee käytännön ohjeisiin, niin nykyiset, voimassaolevat ohjeistukset tulisi käydä läpi ja selvittää mahdolliset muutostarpeet. Esimerkiksi asiakirjahallinnan ohje ei välttämättä ole Veran osalta ajantasainen koska tämän päivittämisestä on kulunut pidempi aika. Tulisi myös selvittää, tarvitaanko Verassa konsernin yhteisten ohjeistuksien lisäksi joitakin yhtiökohtaisia käytännön ohjeita tai näiden täydennystä, jos yhteiset dokumentit eivät kaikilta osin palvele Veran toimintatapoja. Liian yksityiskohtaiseen kuvaukseen ei kuitenkaan ole syytä mennä, ja riittäviä toimenpiteitä arvioitaessa on aina otettava huomioon mahdollinen henkilötietojen käsittelyyn kohdistuva riski, sen suuruus ja vaikutukset.

6 POHDINTA

6.1 Yhteenveto ja onnistuminen

Tutkimuksen yhteenvetona voidaan todeta, että Veran tietosuojakäytännöt ja esimiesten osaamisen taso eivät kaikilta osin vastanneet tietosuoja-asetuksen mukaisia vaatimuksia. Havaitut puutteet johtuivat kuitenkin pitkälti tietämättömyydestä, joten toimenpiteet pohjautuivat riittävän ohjeistuksen lisäämiseen. Esimiehet, niin kuin muutkin henkilötietoja merkittävästi käsittelevät työntekijät osallistuivat tai tulevat osallistumaan konsernin sisäiseen GDPR-koulutukseen, jonka myötä uusi asetus tulee tutuksi. Kouluttautumista täydennetään yhtiökohtaisin käytännön ohjein, kiinnittäen erityistä huomiota etenkin arkaluonteisten henkilötietojen käsittelyyn.

Tietosuoja-asetuksen toteutumista ei ratkaista yhden opinnäytetyön avulla, vaan tietosuojatyö jatkuu Verassa niin ennen asetuksen voimaan tuloa kuin sen jälkeenkin. Avoimia kysymyksiä, tehtävälistaa ja selvitystä riittää, kuten tässä opinnäytetyössä näitä on käsiteltykin, puhumattakaan niistä osa-alueista, joihin ei tämän työn puitteissa edes perehdytty. Opinnäytetyö antaa kuitenkin hyvät valmiudet jatkaa tietosuojatyötä, myös enemmän sinne konkretian puolelle, ja toimiihan opinnäytetyö itsessäänkin jo yhtenä dokumenttina asetuksen osoitusvelvollisuuden osoittamiseksi. Voidaan siis todeta, että tavoitteessa onnistuttiin ja tietosuoja-asetuksen toteutumista edistettiin Verassa. Myös henkilökohtaista tavoitetta asetuksen perehtymisen suhteen voidaan pitää onnistuneena. Olen oppinut ja kehittynyt opinnäytetyön myötä paljon, ja uusi asetus on nyt eittämättä tutumpi kuin mitä se olisi ilman opinnäytetyöprosessia. En koe, että olisin vielä niinkään tietosuojan suhteen osaaja, koska aihe on niin laaja ja tähän liittyen on vielä paljon opittavaa, mutta pystyn nyt paremmin toimimaan osana konsernin tietosuojatiimiä sekä jatkamaan tietosuojatyön kehittämistä Verassa.

6.2 GDPR:n voimaanastuminen

On vaikea sanoa, kuinka valmistautunut yrityksen tulisi olla toukokuun 25. päivään mennessä. Asetus ei juurikaan kerro tai ohjeista, miten säännöksiä tulisi käytännössä toteuttaa, vaan harkinta jätetään pitkälti organisaation oman arvioinnin varaan. Myös tarkemmat

viranomaisohjeistukset ja esimerkit puuttuvat lähes täysin. On vaikea uskoa, että heti asetuksen voimaan tulon jälkeen alkaisi tarkastukset ja sakkojen määrääminen, mutta toisaalta, on varmaa, että valvonta tulee kiristymään, joten tuskin kovin pitkälle läpi sormienkaan enää katsotaan. Yrityksillä kuitenkin on ollut kaksi vuotta aikaa valmistautua asetuksen voimaan tuloon, joten on organisaation oma ongelma, jos siirtymäaikaa ei ole käytetty hyväksi, vaan GDPR-paniikkiin herätään kevään 2018 aikana niin kuin nyt suurin osa yrityksistä tuntuu tekevän. Ainakin jos on median uutisointiin uskominen.

Uskon, että tärkeintä kuitenkin on, että tietosuojan toteutumisen eteen tehdään jatkuvasti töitä ja se otetaan osaksi yrityksen kokonaisvaltaista liiketoimintaa. Se, kuinka pitkälle mikäkin tekeminen riittää, jää nähtäväksi, kun valvontaviranomaiset tulevat määräämään ensimmäiset sanktiot. Sanktiot ovatkin olleet mediassa isona pelotteena GDPR :n suhteen, kun puhutaan jopa 20 miljoonan sakkorangaistuksesta, mutta kaikella todennäköisyydellä, miljoonien sakkoja ei varmasti tulla määräämään yrittäjille tai yhdistyksille, joiden vuotuinen liikevaihto on vain murto-osan tästä summasta. Sen lisäksi, että on mielenkiintoista nähdä, miten valvonta tullaan linjaamaan, on myös mielenkiintoista seurata miten kansa reagoi. Vaikka suuri osa rekisteröidyn oikeuksista ovat jokseenkin sisältyneet henkilötietolakiinkin, on asetus tuonut mukanaan merkittäviä muutoksia näiden toteuttamiselle, kuten tiukan aikarajan rekisteröidyn pyyntöihin vastattaessa. Lisääntyykö kansan tietosuojatietämys uuden asetuksen myötä, ja tulevatko rekisteröidyt käyttämään jatkossa oikeuksiaan enemmän, vai meneekö GDPR-hypetys ohi ymmärryksen, ja kaikki on tuon maagisen toukokuun 25. päivän jälkeen kuten ennenkin?

6.3 Oppimisprosessi

Sanotaan, että opinnäytetyö ei saisi olla pintaraapaisu aiheesta. Sanotaan myös, että opinnäytetyön aiheen pitäisi olla jokseenkin lähellä omaa tietämystä tai jopa intohimon kohteena. Nämä normit eivät kuitenkaan aivan toteutuneet tässä opinnäytetyöprosessissa. Monet muut opinnäytetyöt, joissa GDPR-aihetta oli käsitelty, olivat pitkälti joko liiketalouden oikeudellisen linjan käsialaa tai IT-alan insinööripuolen tarkastelemia tekniseen tietoturvallisuuteen viitaten. Itselläni ei ole juridista eikä liioin teknistä tietoturvaosaamisen taustaa. Vaikka käsittelen työtehtävieni puitteissa henkilötietoja, lähtötasoni EU:n uuden tietosuoja-asetuksen suhteen oli lähes olematon. Koin aiheen kuitenkin tärkeänä, koska oletettavasti minun olisi pitänyt tietää asiasta, kun kerta henkilötietoja käsittelen.

Aihe on myös hyvin ajankohtainen ja yhteiskunnallisesti merkittävä. Kun vielä minut nimettiin osaksi tietosuoja-projektitiimiä, oli selvää, että asiaan täytyi perehtyä, vaikka se elefantin kokoiselta haasteelta aluksi tuntuikin, ja osittain sitä olikin.

Aikuisopiskelun varjopuolia, ovat jatkuva kiire ja ajan puute. Kiire varjosti työskentelyä myös tämän opinnäytetyöprosessin aikana, toisaalta tietosuoja-asetuksen voimaan tulon lähestyessä, toisaalta valmistumisen tavoiteaikataulu mielessä. Työ haki lopullista muotoaan koko opinnäytetyöprosessin ajan ja tähän vaikutti pitkälti konsernin tietosuojatyön eteneminen. Opinnäytetyössä eittämättä suurin aika kului tietosuoja-asetukseen perehtyessä. Juridiikka ja lakiteksti ovat haastavaa luettavaa, varsinkaan kun sitä nykyistäkään lainsäädäntöä ei säännöstasolla ole liiemmin lukenut. Puhumattakaan siitä, että näihin osaisi oikeaoppisesti viitata. Suoria lainauksia ei saisi olla liikaa, mutta lakisäännöksiä voi olla hankala toisinkaan selittää, ettei lain sisältö muutu. Haasteista huolimatta, vaivannäkö kannatti ja lopputulokseen voi olla tyytyväinen.

Se, mikä tietosuoja-asetusta tarkasteltaessa tuli jopa yllätyksenä, oli tietoturvallisuuden vahva linkittyminen tietosuojaan. Toisaalta, tämän ei kaiketi pitäisi olla yllätys, digitalisoitumisesta kun pitkälti puhutaan. Kyberturvallisuus ja yleisesti tietoturva-asiat mielletään usein vain IT-alan erityisosaamiseksi. Tavallinen työntekijä, alasta riippumatta, ymmärtää liian vähän sähköisen toimintaympäristön turvallisista toimintatavoista. Tietoturva ja tietosuoja-asiat tulisi kuitenkin nähdä osana yleisiä kansalaistaitoja. Aivan kuten meidät opetetaan pienestä pitäen lukemaan ja laskemaan, meidät tulisi opettaa myös ymmärtämään sähköistä toimintaympäristöä. Yrityksenkään tietoturva-asiat ei näin ollen tulisi olla vain IT-yksikön varassa, vaan tietoturvaosaaminen tulisi jalkauttaa koko henkilöstön toimintaan, ja siten yrityksen vahvuudeksi.

LÄHTEET

Aarnio, R. 2017a. Arjen tietosuojaa – Tietosuojaa meille kaikille koulutusvideo. Katsottu 25.2.2018. https://vimeo.com/222342825

Aarnio, R. 2017b. Johdon ja esimiesten tietosuojakoulutusvideo. Katsottu 25.2.2018. https://vimeo.com/234313084/f874f6b947

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2016. Tietosuojakäsikirja johdolle. 3. painos. Tallinna: Tietosanoma Oy

Asetus 2016/679/EU. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Euroopan unionin virallinen lehti 4.5.2016. Luettu: 24.2.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI

Direktiivi 1995/46/EY. Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Euroopan unionin virallinen lehti 23.11.1995. Luettu 19.2.2018. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fi:HTML

Eduskunta. 2017. Lakihankkeiden tietopaketit. EU:n tietosuojauudistus ja sen kansallinen täytäntöönpano. Luettu 24.2.2018. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely. EU-tietosuoja-asetuksen vaatimukset. Vantaa: Kauppakamari.

Henkilötietolaki 22.4.1999/523.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2014. Tutki ja kirjoita. 19. painos. Porvoo: Bookwell Oy.

Hänninen, A. 2017. Johdon ja esimiesten tietosuojakoulutusvideo. Katsottu 25.2.2018. https://vimeo.com/234313084/f874f6b947

Hänninen, A. 2018. Tietosuojaa henkilötietoja käsitteleville koulutusvideo. Katsottu 15.3.2018. https://vimeo.com/250133179/9dc258be2e

Jyväskylän yliopisto. 2015. Toimintatutkimus. Luettu 20.4.2018. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/toimintatutkimus

Kallio, N. 2018. Tietosuojaa henkilötietoja käsitteleville koulutusvideo. Katsottu 8.3.2018. https://vimeo.com/250133179/9dc258be2e

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

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Nyyssölä, M. 2014. Yksityisyyden suoja työsuhteessa. 7. uudistettu painos. Helsinki: Talenum Media Oy

Oikeusministeriö. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Oikeusministeriön julkaisu 4/2017. Luettu 23.3.2018. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Opitietosuojaa.fi. 2017. EU:n tietosuoja-asetus. Luettu: 23.2.2018. https://opitietosuojaa.fi/index.php/fi/oikeus/lait/eu-n-tietosuoja-asetus

Poliisi. 2018. Kyberrikollisuus. Luettu 20.4.2018. https://www.poliisi.fi/rikokset/kyberrikollisuus

Rousku, K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Helsinki: Talenum Media Oy

Suomen perustuslaki 11.6.1999/731.

Tampereen seudun tietoturvaryhmä. 2016. Henkilöstön tietoturva- ja tietosuojaopas. Luettu: 14.4.2018. http://docplayer.fi/51832562-Henkiloston-tietoturva-ja-tietosuojaopas.html

Tarhonen, L. 2017. IABlogi: Henkilötietojen pseudonymisointi – ai siis mikä? Luettu 1.3.2018. https://www.iab.fi/iablogi/henkilotietojen-pseudonymisointi-ai-siis-mika.html

Tietosuojavaltuutetun toimisto. 2013. Muiden lakien merkitys henkilötietojen käsittelyssä. Luettu 24.2.2018. http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/muutlaitsuhteessahenkilotietolakiin.html

Tietosuojavaltuutetun toimisto. 2014. Erityislainsäädäntö. Luettu 24.2.2018. http://www.tietosuoja.fi/fi/index/lait/erityislainsaadanto.html

Tietosuojavaltuutetun toimisto. 2017. Työryhmä valmistelemaan EU:n tietosuojadirektiivin täytäntöönpanoa. Tiedote 17.1.2017. Luettu 15.3.2018. http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2017/01/tyoryhmavalmistelemaaneuntietosuojadirektiivintaytantoonpanoa.html

Tietosuojavaltuutetun toimisto. 2018a. Sanastoa tietosuojauudistukseen liittyen. Luettu 1.3.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/sanastoa.html

Tietosuojavaltuutetun toimisto. 2018b. Näin laadit tietosuoja-asetuksen edellyttämän selosteen käsittelytoimista. Tiedote 23.3.2018. Luettu 31.3.2018. http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/on/03/nainlaadittietosuoja-asetuksenedellyttamanselosteenkasittelytoimista.html

Toivonen, M. 2018a. Tietosuoja-projektitiimin palaveri 16.3.2018

Toivonen, M. 2018b. Tampereen Sähkölaitos- yhtiöiden sisäinen GDPR-koulutus 9.4.2018.

Valtioneuvosto. 2018. Työryhmä: Tietosuojaa koskeva erityissääntely on jatkossa harkittava tarkasti. Oikeusministeriön tiedote 1.3.2018. Luettu 15.3.2018. http://valtioneuvosto.fi/artikkeli/-/asset_publisher/tyoryhma-tietosuojaa-koskeva-erityissaantely-on-jatkossa-harkittava-tarkasti?_101_INSTANCE_3wyslLo1Z0ni_groupId=1410853

Valtiovarainministeriö. 2016. EU-tietosuojan kokonaisuudistus. VAHTI-raportti – 1/2016. Luettu 24.2.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128

Viestintävirasto. 2018. Kyberturvallisuuskeskus. Kybersää maaliskuu 2018. Luettu 20.4.2018. https://www.viestintavirasto.fi/attachments/tietoturva/Kybersaa_2018-03.pdf

Vanto, J. 2011. Henkilötietolaki käytännössä. 1. painos. Helsinki: WSOYpro Oy

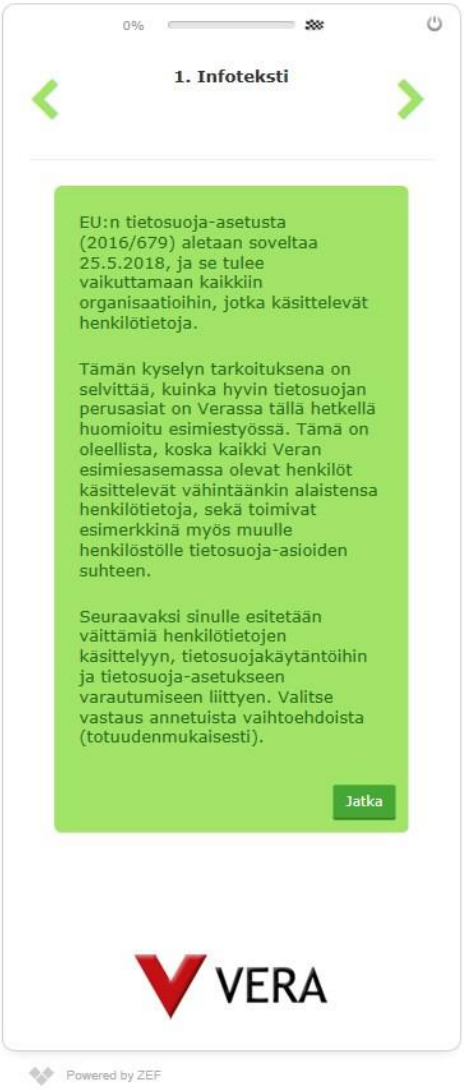
LIITTEET

Liite 1. Esimiesten tietosuojakysely

1 (9)

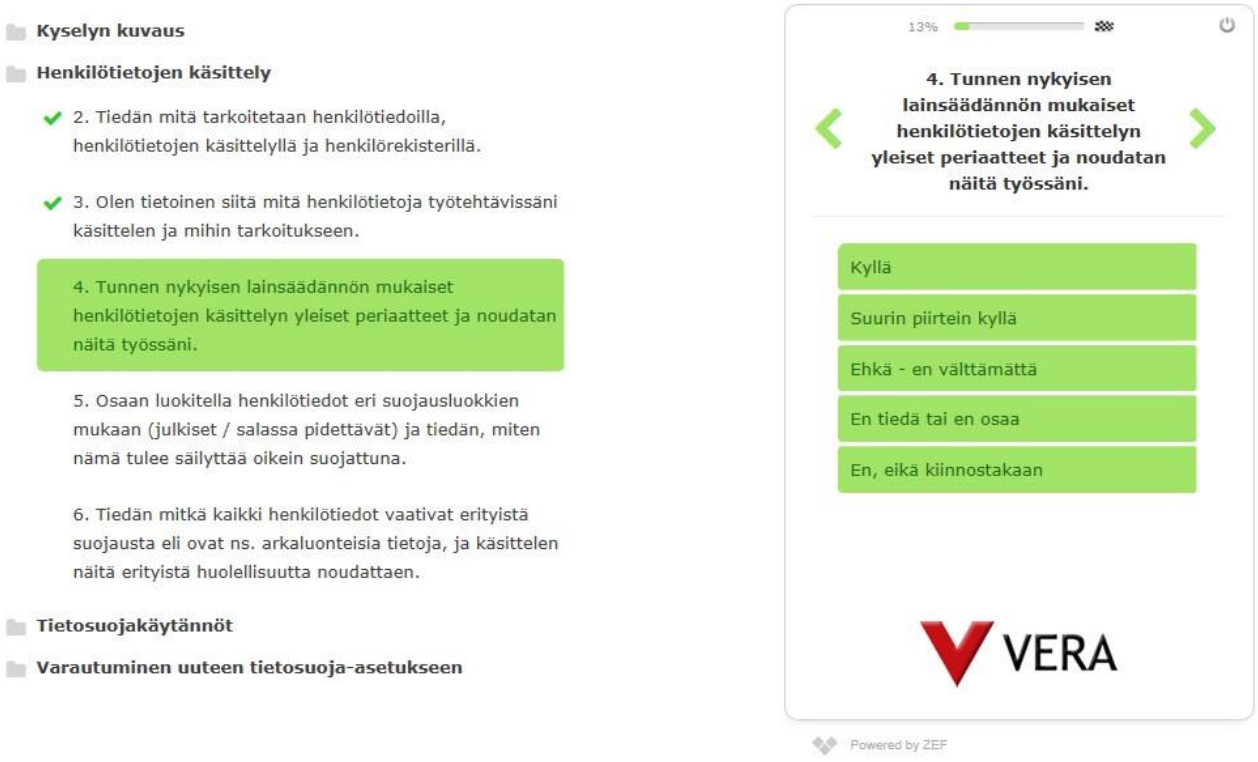
Tietosuojakysely

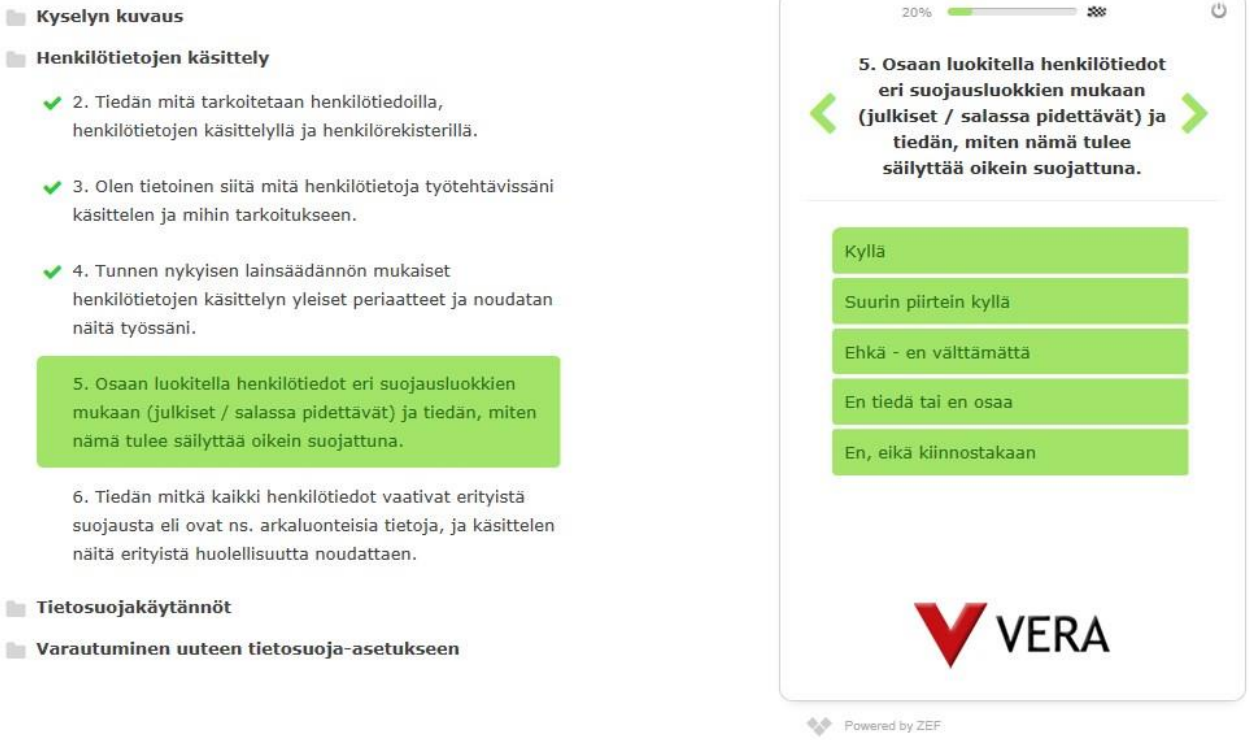
- Kyselyn kuvaus
  - 1. Infoteksti
- Henkilötietojen käsittely
- Tietosuojakäytännöt
- Varautuminen uuteen tietosuoja-asetukseen



- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
  - 2. Tiedän mitä tarkoitetaan henkilötiedoilla, henkilötietojen käsittelyllä ja henkilörekisterillä.
  - 3. Olen tietoinen siitä mitä henkilötietoja työtehtävissäni käsittelen ja mihin tarkoitukseen.
  - 4. Tunnen nykyisen lainsäädännön mukaiset henkilötietojen käsittelyn yleiset periaatteet ja noudatan näitä työssäni.
  - 5. Osaan luokitella henkilötiedot eri suojausluokkien mukaan (julkiset / salassa pidettävät) ja tiedän, miten nämä tulee säilyttää oikein suojattuna.
  - 6. Tiedän mitkä kaikki henkilötiedot vaativat erityistä suojausta eli ovat ns. arkaluonteisia tietoja, ja käsittelen näitä erityistä huolellisuutta noudattaen.
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**

- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
  - ✔ 2. Tiedän mitä tarkoitetaan henkilötiedoilla, henkilötietojen käsittelyllä ja henkilörekisterillä.
  - 3. Olen tietoinen siitä mitä henkilötietoja työtehtävissäni käsittelen ja mihin tarkoitukseen.
  - 4. Tunnen nykyisen lainsäädännön mukaiset henkilötietojen käsittelyn yleiset periaatteet ja noudatan näitä työssäni.
  - 5. Osaan luokitella henkilötiedot eri suojausluokkien mukaan (julkiset / salassa pidettävät) ja tiedän, miten nämä tulee säilyttää oikein suojattuna.
  - 6. Tiedän mitkä kaikki henkilötiedot vaativat erityistä suojausta eli ovat ns. arkaluonteisia tietoja, ja käsittelen näitä erityistä huolellisuutta noudattaen.
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**


Kyselyn kuvaus
Henkilötietojen käsittely
2. Tiedän mitä tarkoitetaan henkilötiedoilla, henkilötietojen käsittelyllä ja henkilörekisterillä.
3. Olen tietoinen siitä mitä henkilötietoja työtehtävissäni käsittelen ja mihin tarkoitukseen.
4. Tunnen nykyisen lainsäädännön mukaiset henkilötietojen käsittelyn yleiset periaatteet ja noudatan näitä työssäni.
5. Osaan luokitella henkilötiedot eri suojausluokkien mukaan (julkiset / salassa pidettävät) ja tiedän, miten nämä tulee säilyttää oikein suojattuna.
6. Tiedän mitkä kaikki henkilötiedot vaativat erityistä suojausta eli ovat ns. arkaluonteisia tietoja, ja käsittelen näitä erityistä huolellisuutta noudattaen.
Tietosuojakäytännöt
Varautuminen uuteen tietosuoja-asetukseen
13%
4. Tunnen nykyisen lainsäädännön mukaiset henkilötietojen käsittelyn yleiset periaatteet ja noudatan näitä työssäni.
Kyllä
Suurin piirtein kyllä
Ehkä - en välttämättä
En tiedä tai en osaa
En, eikä kiinnostakaan
VERA
Powered by ZEF


Kyselyn kuvaus
Henkilötietojen käsittely
2. Tiedän mitä tarkoitetaan henkilötiedoilla, henkilötietojen käsittelyllä ja henkilörekisterillä.
3. Olen tietoinen siitä mitä henkilötietoja työtehtävissäni käsittelen ja mihin tarkoitukseen.
4. Tunnen nykyisen lainsäädännön mukaiset henkilötietojen käsittelyn yleiset periaatteet ja noudatan näitä työssäni.
5. Osaan luokitella henkilötiedot eri suojausluokkien mukaan (julkiset / salassa pidettävät) ja tiedän, miten nämä tulee säilyttää oikein suojattuna.
6. Tiedän mitkä kaikki henkilötiedot vaativat erityistä suojausta eli ovat ns. arkaluonteisia tietoja, ja käsittelen näitä erityistä huolellisuutta noudattaen.
Tietosuojakäytännöt
Varautuminen uuteen tietosuoja-asetukseen
20%
5. Osaan luokitella henkilötiedot eri suojausluokkien mukaan (julkiset / salassa pidettävät) ja tiedän, miten nämä tulee säilyttää oikein suojattuna.
Kyllä
Suurin piirtein kyllä
Ehkä - en välttämättä
En tiedä tai en osaa
En, eikä kiinnostakaan
VERA
Powered by ZEF

4 (9)

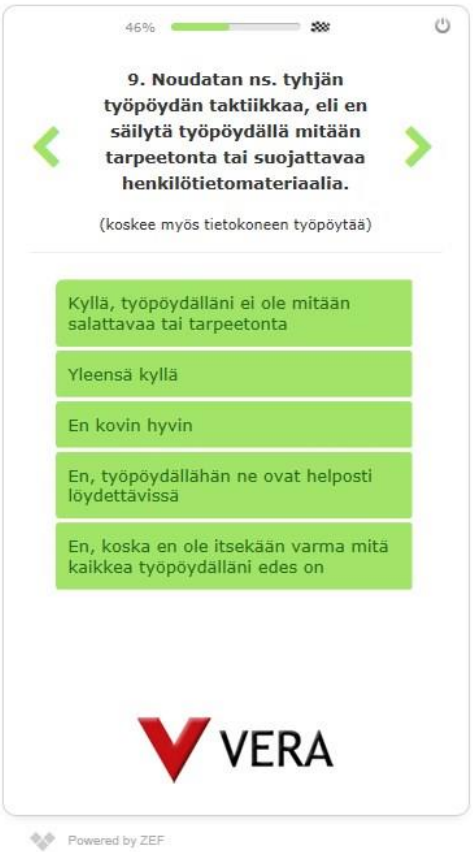
- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
  - ✔ 2. Tiedän mitä tarkoitetaan henkilötiedoilla, henkilötietojen käsittelyllä ja henkilörekisterillä.
  - ✔ 3. Olen tietoinen siitä mitä henkilötietoja työtehtävissäni käsittelen ja mihin tarkoitukseen.
  - ✔ 4. Tunnen nykyisen lainsäädännön mukaiset henkilötietojen käsittelyn yleiset periaatteet ja noudatan näitä työssäni.
  - ✔ 5. Osaan luokitella henkilötiedot eri suojausluokkien mukaan (julkiset / salassa pidettävät) ja tiedän, miten nämä tulee säilyttää oikein suojattuna.
  - 6. Tiedän mitkä kaikki henkilötiedot vaativat erityistä suojausta eli ovat ns. arkaluonteisia tietoja, ja käsittelen näitä erityistä huolellisuutta noudattaen.
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**

- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
  - 7. Lukitsen tietokoneen aina, kun poistun työpisteeltäni.
  - 8. Lukitsen myös muut päätelaitteet, kuten älypuhelimen tai tabletin, jos en näitä käytä.
  - 9. Noudatan ns. tyhjän työpöydän taktiikkaa, eli en säilytä työpöydällä mitään tarpeetonta tai suojattavaa henkilötietomateriaalia.
    (koskee myös tietokoneen työpöytää)
  - 10. Säilytän luottamuksellisen ja salassa pidettävän tietosuojamateriaalin lukitussa säilytystilassa.
    (fyysinen materiaali)
  - 11. Tunnen asianmukaiset suojaustoimenpiteet myös digitaalisessa ympäristössä.
    (turvallinen salasanakäytäntö, käyttöoikeusrajaus, suojattu yhteys, tietoturvariskit)
- **Varautuminen uuteen tietosuoja-asetukseen**

5 (9)

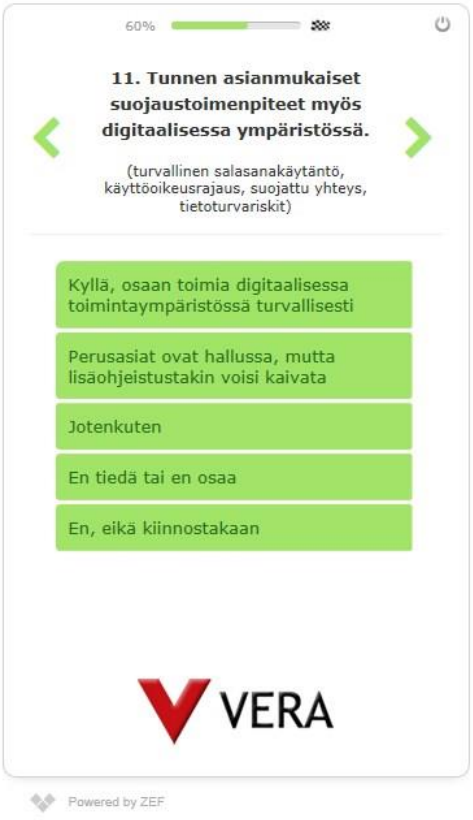
- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
  - ✔ 7. Lukitsen tietokoneen aina, kun poistun työpisteeltäni.
  - 8. Lukitsen myös muut päätelaitteet, kuten älypuhelimen tai tabletin, jos en näitä käytä.
  - 9. Noudatan ns. tyhjän työpöydän taktiikkaa, eli en säilytä työpöydällä mitään tarpeetonta tai suojattavaa henkilötietomateriaalia.
    (koskee myös tietokoneen työpöytää)
  - 10. Säilytän luottamuksellisen ja salassa pidettävän tietosuojamateriaalin lukitussa säilytystilassa.
    (fyysinen materiaali)
  - 11. Tunnen asianmukaiset suojaustoimenpiteet myös digitaalisessa ympäristössä.
    (turvallinen salasanakäytäntö, käyttöoikeusrajaus, suojattu yhteys, tietoturvariskit)
- **Varautuminen uuteen tietosuoja-asetukseen**

- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
  - ✔ 7. Lukitsen tietokoneen aina, kun poistun työpisteeltäni.
  - ✔ 8. Lukitsen myös muut päätelaitteet, kuten älypuhelimen tai tabletin, jos en näitä käytä.
  - 9. Noudatan ns. tyhjän työpöydän taktiikkaa, eli en säilytä työpöydällä mitään tarpeetonta tai suojattavaa henkilötietomateriaalia.
    (koskee myös tietokoneen työpöytää)
  - 10. Säilytän luottamuksellisen ja salassa pidettävän tietosuojamateriaalin lukitussa säilytystilassa.
    (fyysinen materiaali)
  - 11. Tunnen asianmukaiset suojaustoimenpiteet myös digitaalisessa ympäristössä.
    (turvallinen salasanakäytäntö, käyttöoikeusrajaus, suojattu yhteys, tietoturvariskit)
- **Varautuminen uuteen tietosuoja-asetukseen**

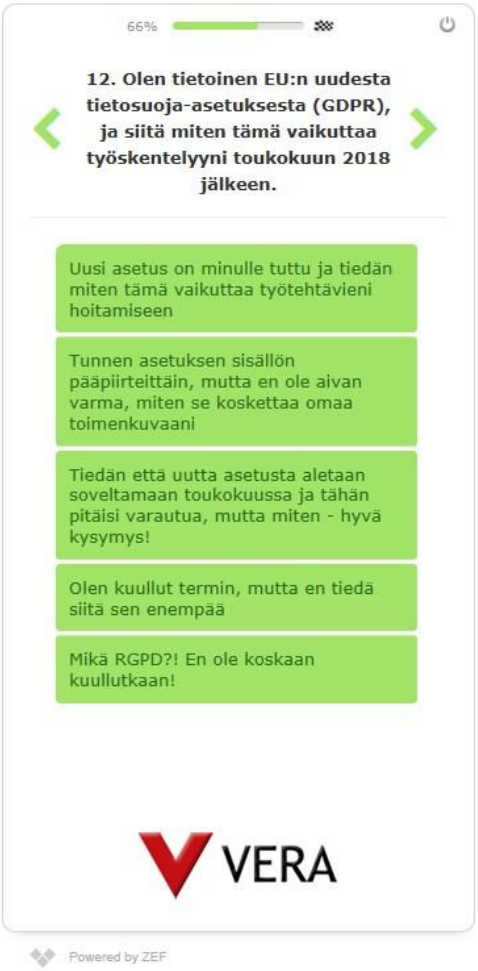


- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
  - ✔ 7. Lukitsen tietokoneen aina, kun poistun työpisteeltäni.
  - ✔ 8. Lukitsen myös muut päätelaitteet, kuten älypuhelimen tai tabletin, jos en näitä käytä.
  - ✔ 9. Noudatan ns. tyhjän työpöydän taktiikkaa, eli en säilytä työpöydällä mitään tarpeetonta tai suojattavaa henkilötietomateriaalia.
    (koskee myös tietokoneen työpöytää)
  - 10. Säilytän luottamuksellisen ja salassa pidettävän tietosuojamateriaalin lukitussa säilytystilassa.
    (fyysinen materiaali)
  - 11. Tunnen asianmukaiset suojaustoimenpiteet myös digitaalisessa ympäristössä.
    (turvallinen salasanakäytäntö, käyttöoikeusrajaus, suojattu yhteys, tietoturvariskit)
- **Varautuminen uuteen tietosuoja-asetukseen**

- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
  - ✔ 7. Lukitsen tietokoneen aina, kun poistun työpisteeltäni.
  - ✔ 8. Lukitsen myös muut päätelaitteet, kuten älypuhelimen tai tabletin, jos en näitä käytä.
  - ✔ 9. Noudatan ns. tyhjän työpöydän taktiikkaa, eli en säilytä työpöydällä mitään tarpeetonta tai suojattavaa henkilötietomateriaalia.
    (koskee myös tietokoneen työpöytää)
  - ✔ 10. Säilytän luottamuksellisen ja salassa pidettävän tietosuojamateriaalin lukitussa säilytystilassa.
    (fyysinen materiaali)
  - 11. Tunnen asianmukaiset suojaustoimenpiteet myös digitaalisessa ympäristössä.
    (turvallinen salasanakäytäntö, käyttöoikeusrajaus, suojattu yhteys, tietoturvariskit)
- **Varautuminen uuteen tietosuoja-asetukseen**



- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**
  - 12. Olen tietoinen EU:n uudesta tietosuoja-asetuksesta (GDPR), ja siitä miten tämä vaikuttaa työskentelyyni toukokuun 2018 jälkeen.
  - 13. Olen tietoinen intranetin uudesta tietosuojaohjesivusta ja olen tutustunut sen sisältöön.
  - 14. Toimin esimerkkinä tietosuojaan liittyvissä asioissa omille alaisilleni, ja osaan ohjeistaa heitä oikeanlaiseen tietojen käsittelyyn.
  - 15. Arvioi oma osaamisesi tietosuojan suhteen asteikolla 1-10.
  - 16. Vapaa palaute.
    (kommentteja, huolia, murheita, kysymyksiä aiheeseen liittyen)



- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**
  - ✔ 12. Olen tietoinen EU:n uudesta tietosuoja-asetuksesta (GDPR), ja siitä miten tämä vaikuttaa työskentelyyni toukokuun 2018 jälkeen.
  - 13. Olen tietoinen intranetin uudesta tietosuojaohjesivusta ja olen tutustunut sen sisältöön.
  - 14. Toimin esimerkkinä tietosuojaan liittyvissä asioissa omille alaisilleni, ja osaan ohjeistaa heitä oikeanlaiseen tietojen käsittelyyn.
  - 15. Arvioi oma osaamisesi tietosuojan suhteen asteikolla 1-10.
  - 16. Vapaa palaute.
    (kommentteja, huolia, murheita, kysymyksiä aiheeseen liittyen)

8 (9)

- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**
  - ✔ 12. Olen tietoinen EU:n uudesta tietosuoja-asetuksesta (GDPR), ja siitä miten tämä vaikuttaa työskentelyyni toukokuun 2018 jälkeen.
  - ✔ 13. Olen tietoinen intranetin uudesta tietosuojaohjesivusta ja olen tutustunut sen sisältöön.
  - 14. Toimin esimerkkinä tietosuojaan liittyvissä asioissa omille alaisilleni, ja osaan ohjeistaa heitä oikeanlaiseen tietojen käsittelyyn.
  - 15. Arvioi oma osaamisesi tietosuojan suhteen asteikolla 1-10.
  - 16. Vapaa palaute.
    (kommentteja, huolia, murheita, kysymyksiä aiheeseen liittyen)

- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**
  - ✔ 12. Olen tietoinen EU:n uudesta tietosuoja-asetuksesta (GDPR), ja siitä miten tämä vaikuttaa työskentelyyni toukokuun 2018 jälkeen.
  - ✔ 13. Olen tietoinen intranetin uudesta tietosuojaohjesivusta ja olen tutustunut sen sisältöön.
  - ✔ 14. Toimin esimerkkinä tietosuojaan liittyvissä asioissa omille alaisilleni, ja osaan ohjeistaa heitä oikeanlaiseen tietojen käsittelyyn.
  - 15. Arvioi oma osaamisesi tietosuojan suhteen asteikolla 1-10.
  - 16. Vapaa palaute.
    (kommentteja, huolia, murheita, kysymyksiä aiheeseen liittyen)

- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**
  - ✔ 12. Olen tietoinen EU:n uudesta tietosuoja-asetuksesta (GDPR), ja siitä miten tämä vaikuttaa työskentelyyni toukokuun 2018 jälkeen.
  - ✔ 13. Olen tietoinen intranetin uudesta tietosuojaohjesivusta ja olen tutustunut sen sisältöön.
  - ✔ 14. Toimin esimerkkinä tietosuojaan liittyvissä asioissa omille alaisilleni, ja osaan ohjeistaa heitä oikeanlaiseen tietojen käsittelyyn.
  - ✔ 15. Arvioi oma osaamisesi tietosuojan suhteen asteikolla 1-10.
  - 16. Vapaa palaute.
    (kommentteja, huolia, murheita, kysymyksiä aiheeseen liittyen)

- **Kyselyn kuvaus**
- **Henkilötietojen käsittely**
- **Tietosuojakäytännöt**
- **Varautuminen uuteen tietosuoja-asetukseen**
  - ✔ 12. Olen tietoinen EU:n uudesta tietosuoja-asetuksesta (GDPR), ja siitä miten tämä vaikuttaa työskentelyyni toukokuun 2018 jälkeen.
  - ✔ 13. Olen tietoinen intranetin uudesta tietosuojaohjesivusta ja olen tutustunut sen sisältöön.
  - ✔ 14. Toimin esimerkkinä tietosuojaan liittyvissä asioissa omille alaisilleni, ja osaan ohjeistaa heitä oikeanlaiseen tietojen käsittelyyn.
  - ✔ 15. Arvioi oma osaamisesi tietosuojan suhteen asteikolla 1-10.
  - ✔ 16. Vapaa palaute.
    (kommentteja, huolia, murheita, kysymyksiä aiheeseen liittyen)

Liite 2. Tietosuojakyselyn vastaukset

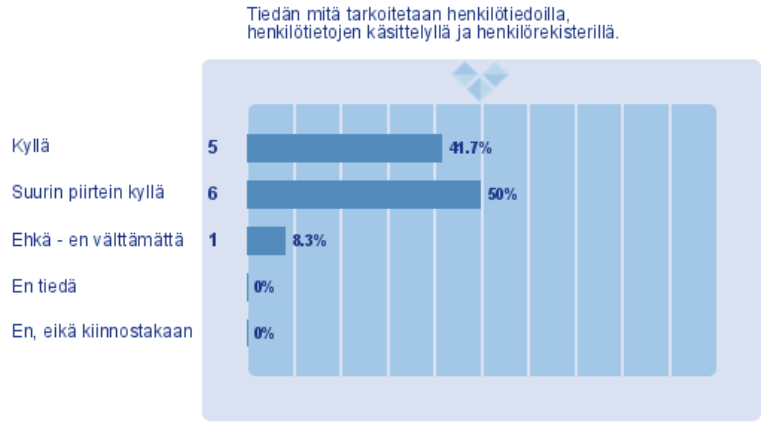
Tietosuojakysely

Nimi	Vastaaja	Vastaamassa	Vastanneet
Esimiehet	15	12	12
Yhteensä	**15**	**12**	**12**

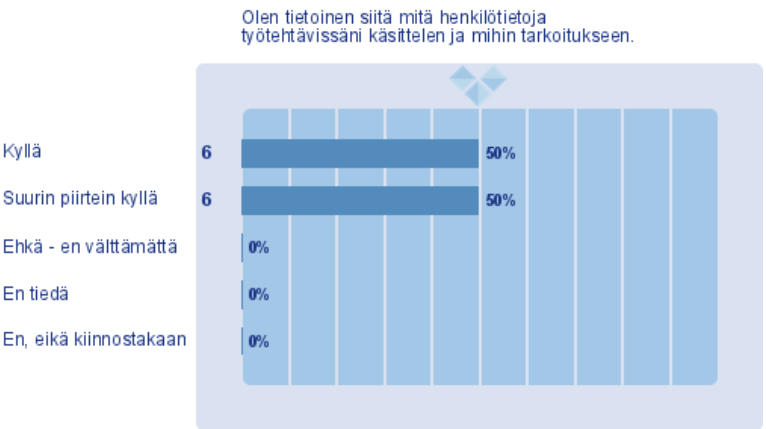
Vastausprosentti	**80**
Lopettaneet	80
Kesken jättäneet	0
Eivät osallistuneet	20

Henkilötietojen käsittely

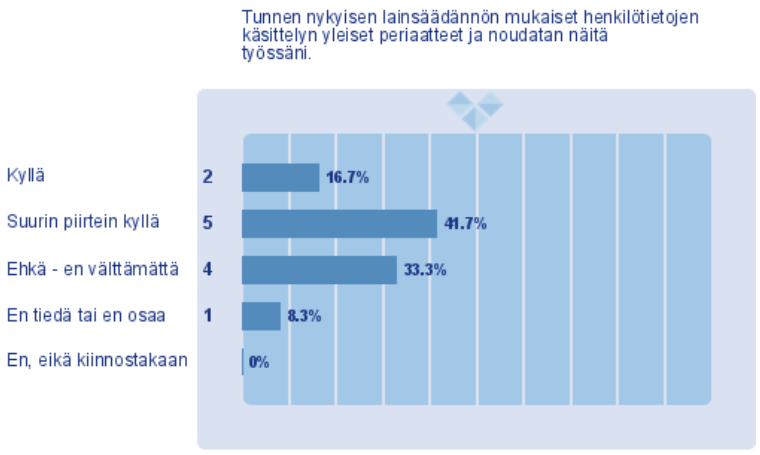
1. Tiedän mitä tarkoitetaan henkilötiedoilla, henkilötietojen käsittelyllä ja henkilörekisterillä.



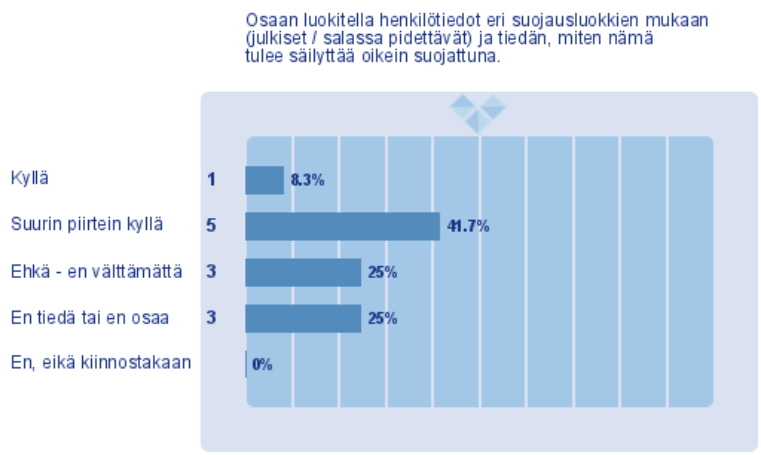
2. Olen tietoinen siitä mitä henkilötietoja työtehtävissäni käsittelen ja mihin tarkoitukseen.



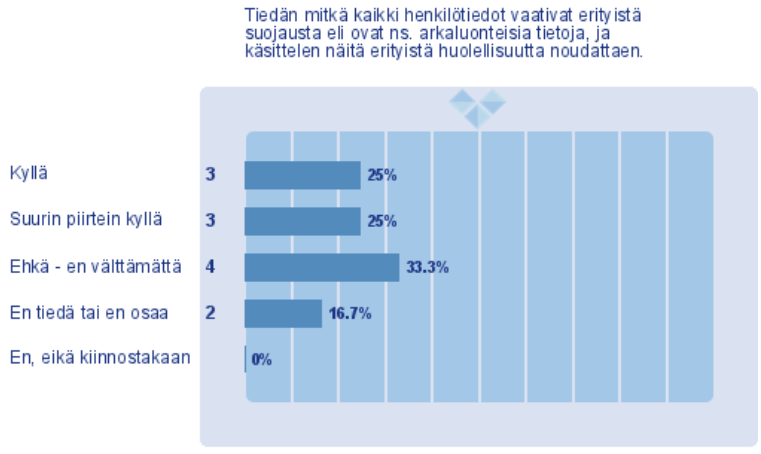
3. Tunnen nykyisen lainsäädännön mukaiset henkilötietojen käsittelyn yleiset periaatteet ja noudatan näitä työssäni.



4. Osaan luokitella henkilötiedot eri suojausluokkien mukaan (julkiset / salassa pidettävät) ja tiedän, miten nämä tulee säilyttää oikein suojattuna.

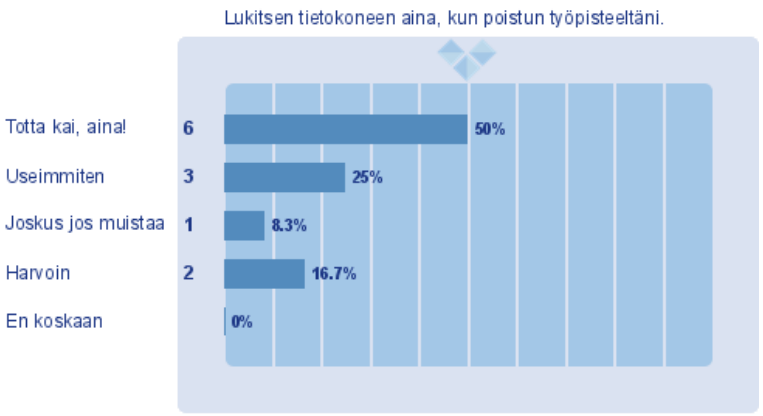


5. Tiedän mitkä kaikki henkilötiedot vaativat erityistä suojausta eli ovat ns. arkaluonteisia tietoja, ja käsittelen näitä erityistä huolellisuutta noudattaen.

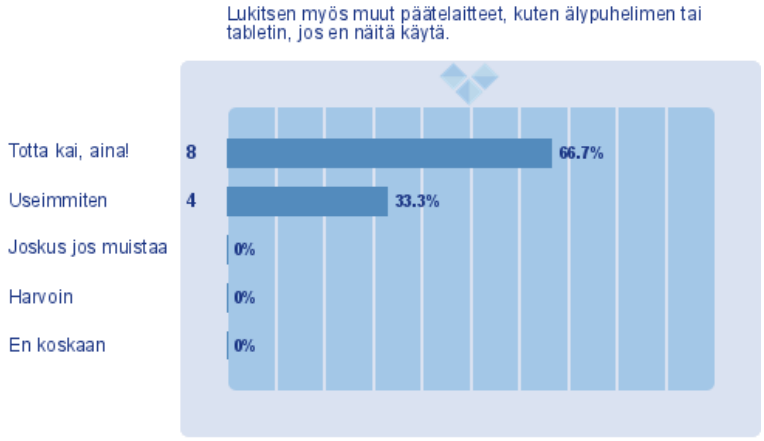


Tietosuojakäytännöt

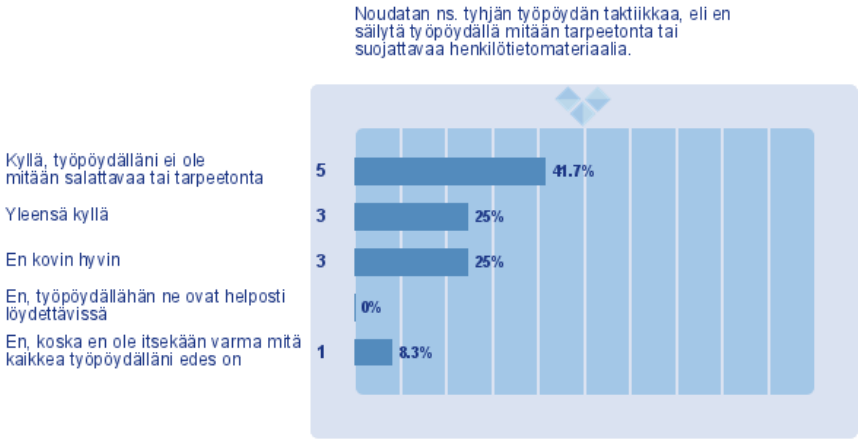
1. Lukitsen tietokoneen aina, kun poistun työpisteeltäni.



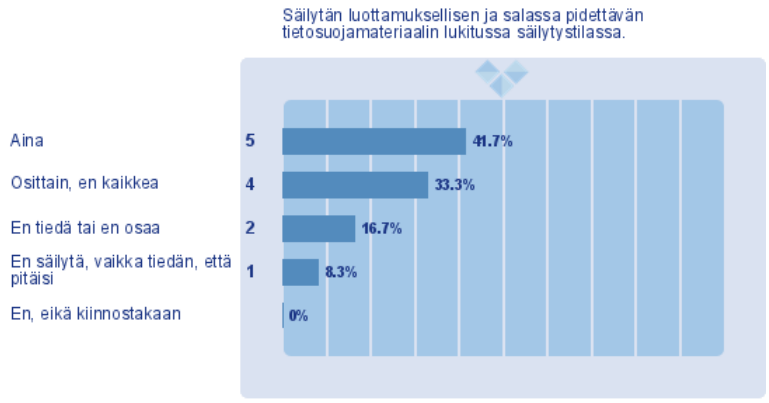
2. Lukitsen myös muut päätelaitteet, kuten älypuhelimen tai tabletin, jos en näitä käytä.



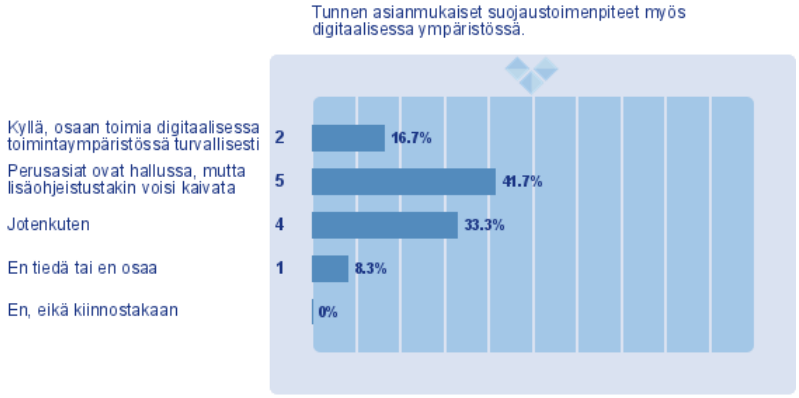
3. Noudatan ns. tyhjän työpöydän taktiikkaa, eli en säilytä työpöydällä mitään tarpeetonta tai suojattavaa henkilötietomateriaalia.
(koskee myös tietokoneen työpöytää)



4. Säilytän luottamuksellisen ja salassa pidettävän tietosuojamateriaalin lukitussa säilytystilassa. (fyysinen materiaali)

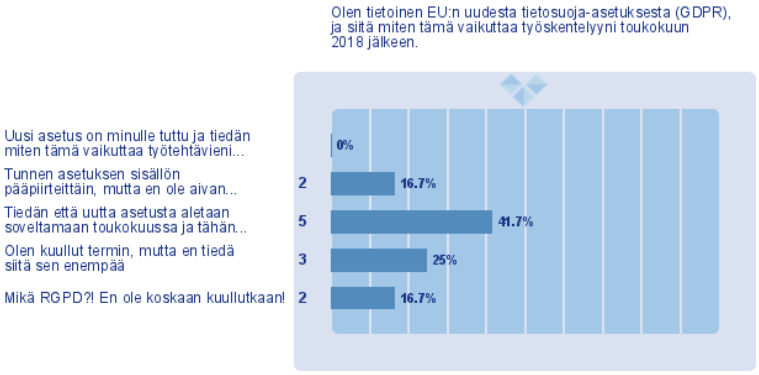


5. Tunnen asianmukaiset suojaustoimenpiteet myös digitaalisessa ympäristössä. (turvallinen salasanakäytäntö, käyttöoikeusrajaus, suojattu yhteys, tietoturvariskit)

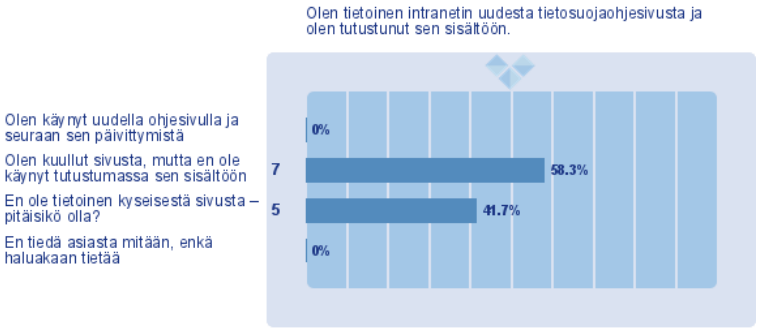


Varautuminen uuteen tietosuoja-asetukseen

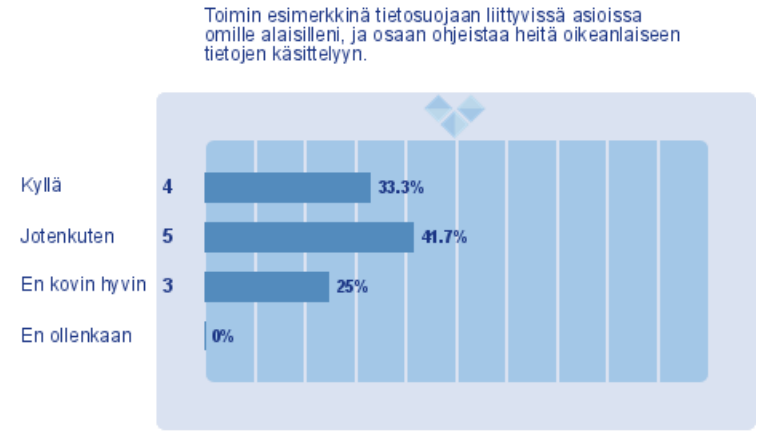
1. Olen tietoinen EU:n uudesta tietosuoja-asetuksesta (GDPR), ja siitä miten tämä vaikuttaa työskentelyyni toukokuun 2018 jälkeen.



2. Olen tietoinen intranetin uudesta tietosuojaohjesivusta ja olen tutustunut sen sisältöön.



3. Toimin esimerkkinä tietosuojaan liittyvissä asioissa omille alaisilleni, ja osaan ohjeistaa heitä oikeanlaiseen tietojen käsittelyyn.



4. Arvioi oma osaamisesi tietosuojan suhteen asteikolla 1-10.