KARELIA-AMMATTIKORKEAKOULU

Johtaminen ja liiketoimintaosaaminen
Ylempi ammattikorkeakoulututkinto

Auli Karjalainen
Pirjo Uusoksa

TIETOSUOJAN TOTEUTUMINEN KARELIA-AMMATTIKORKEA-KOULUSSA

Opinnäytetyö
Kesäkuu 2020

OPINNÄYTETYÖ
Kesäkuu 2020
Johtaminen ja liiketoimintaosaaminen
Ylempi ammattikorkeakoulututkinto
Tikkarinne 9
80200 JOENSUU
+358 13 260 600 (vaihde)

Tekijä(t)
Auli Karjalainen ja Pirjo Uusoksa

Nimeke
Tietosuojan toteutuminen Karelia-ammattikorkeakoulussa

Toimeksiantaja
Karelia-ammattikorkeakoulu

Tiivistelmä

Opinnäytetyön tavoitteena on selvittää EU:n tietosuoja-asetuksen (EU) 2016/679 mukaisen henkilötietojen käsittelyn tietosuojaosaamisen taso ja tietosuojan toteuttamisen nykytila Karelia-ammattikorkeakoulussa. Lisäksi tarkastellaan tietosuojatyön organisointia sekä johdon ja esimiehen roolia tietosuojan toteuttamisessa.

Teoreettisena viitekehyksenä toimivat kansainvälinen EU:n yleinen tietosuoja-asetus sekä sitä täsmentävä ja täydentävä kotimainen lainsäädäntö ja tietosuojavaltuutetun toimiston tuottama aineisto. Opinnäytetyö on tapaustutkimus, jonka tiedonkeruumenetelminä on käytetty kvantitatiivista, puolistrukturoitua henkilöstökyselyä ja kvalitatiivista henkilöhaastattelua. Henkilöstökyselyn kohteena oli koko henkilökunta (n=267), pois lukien ylin johto. Kyselyn vastausprosentti oli 31,5 %.

Kyselystä ja haastattelusta saatujen vastausten perusteella henkilökunnan henkilötietojen käsittelyn tietosuojaosaamisen taso on hyvä, mutta sitä tulisi vahvistaa eri kohderyhmille osoitetuilla koulutuksilla, ohjeistuksilla ja tiedottamisella. Henkilötietojen käsittelyn tietosuoja on toteutettu asetuksen mukaisesti. Opinnäytetyön lopussa on esitetty ehdotuksemme kehittämistoimenpiteistä.

Kieli
suomi

Sivuja 59
Liitteet 3
Liitesivumäärä 11

Asiasanat
tietosuoja-asetus, tietosuoja, henkilötietojen käsittely

THESIS
June 2020
Johtaminen ja liiketoimintaosaaminen
Ylempi ammattikorkeakoulututkinto
Tikkarinne 9
80200 JOENSUU
FINLAND
+ 358 13 260 600 (switchboard)

Author (s)
Auli Karjalainen ja Pirjo Uusoksa

Title
Implementation of Data Protection at Karelia University of Applied Sciences

Commissioned by
Karelia University of Applied Sciences

Abstract

The aim of the thesis is to clarify the level of data protection competence for the processing of personal data in accordance with the EU Data Protection Regulation (EU) 2016/679 and the current state of data protection implementation at Karelia University of Applied Sciences. In addition, the organisation of data protection work and the role of management and supervisor in the implementation of data protection will be examined.

The theoretical reference framework is the International EU General Data Protection Regulation and its detailed and complementary domestic legislation and the material produced by the Office of the Data Protection Ombudsman. The thesis is a case study whose data collection methods have been based on a quantitative, semi-structured personnel survey and qualitative personal interview. The personnel survey focused on all personnel (n=267), excluding senior management. The query response rate was 31.5%.

Based on the answers received from the survey and interview, the level of data protection competence for the processing of staff's personal data is good, but it should be strengthened by training, guidance and communication addressed to different target groups. At the end of the thesis, our proposals for development measures are presented.

Language
Finnish

Pages 59
Appendices 3
Pages of Appendices 11

Keywords
data protection regulation, data protection, processing of personal data

Sisältö

Liitteet

1 Johdanto

Euroopan parlamentin ja neuvoston asetus yleisestä tietosuojasta (EU) 2016/679 (yleinen tietosuoja-asetus, General Data Protection Regulation, GDPR), jäljempänä *tietosuoja-asetus*, astui voimaan 24.5.2016 ja sen soveltaminen alkoi 25.5.2018 Euroopan Unionin alueella. Tietosuoja-asetus ajantasaistaa ja yhtenäistää tietosuojaa koskevaa lainsäädäntöä ja vahvistaa rekisteröidyn itsemääräämisoikeuksia Euroopan Unionin alueella. Tietosuoja-asetuksen voimaantulon myötä, kaikki rekisterinpitäjät ovat joutuneet tarkastelemaan omia toimintatapojaan ja prosessejaan sekä päivittämään ne huomioiden tietosuoja-asetuksen tuomat vaatimukset.

1.1 Opinnäytetyön tausta ja lähtökohdat

Tietosuoja-asetuksen soveltamisen käyttöönotosta jäsenmaissa on nyt kulunut lähes kaksi vuotta, joten on ajankohtaista kartoittaa, miten asetuksessa säädetyt velvollisuudet tietosuojan soveltamisesta on toteutettu. Myös tietosuoja-asetus kehottaa organisaatioita arvioimaan henkilötietojen käsittelykäytäntöjään. Asetuksen soveltamisen käyttöönoton jälkeen on tullut voimaan kansallisia, tietosuoja-asetusta tukevia lakimuutoksia, joiden vaikutusta tietosuojan toteuttamiseen myös tarkastellaan. Aiheena tietosuoja-asetus on laaja ja sitä voidaan tutkia eri näkökulmista. Useammassa viime vuosina tehdyssä opinnäytetyössä on tutkittu tietosuoja-asetuksen tuomia muutoksia henkilötietojen käsittelyyn ja rekisterinpitäjän velvollisuuksiin, sekä toimenpiteitä asetuksen velvollisuuksien toteuttamiseksi tietyssä yrityksessä.

Opinnäytetyön toimeksiantaja on Karelia-ammattikorkeakoulun (jäljempänä Karelia) laatutyöryhmä. Karelia on Joensuussa toimiva monialainen ammattikorkeakoulu, joka tarjoaa päivä- ja monimuotototeutuksena toteutettavaa ammattikorkeakoulu- ja ylempään ammattikorkeakoulututkintoon johtavaa koulutusta

toimintaluvan mukaisissa koulutusvastuissa. Lisäksi toteutetaan täydennyskoulutusta sekä tarjotaan opintoja avoimen ammattikorkeakoulun kautta. Lakisääteisesti ammattikorkeakoulun tehtäviin kuuluu koulutuksen lisäksi myös tutkimus-, kehittämis- ja innovaatiotoiminta sekä palveluliiketoiminta. Kareliassa on lähes 3900 tutkinto-opiskelijaa ja yhteensä 303 työntekijää, josta päätoimisen henkilöstön määrä on 271. (Karelia-ammattikorkeakoulu 2020a, 4, 16.)

Karelian ydintoimintoja ovat Koulutus, Tutkimus-, kehittämis- ja innovaatiotoiminta (jäljempänä TKI-toiminta) sekä Palveluliiketoiminta. Niitä tukevat Hallinto- ja tukipalvelut, joihin kuuluvat mm. henkilöstö-, opintoasiain-, laskenta-, kirjasto- ja tietohallintopalvelut sekä rehtorin toimisto. Ammattikorkeakoulun ylimmän johdon muodostavat rehtori, vararehtori sekä hallinto- ja talousjohtaja. Lisäksi ydintoimintoihin liittyy kehittämisryhmiä, joilla on tärkeä merkitys ammattikorkeakoulun johtamisessa, kehittämisessä ja päätöksenteon valmistelussa. Kehittämisryhmiä ovat laaturyhmä, koulutuksen kehittämisryhmä, TKI-ryhmä ja palveluliiketoiminnan ryhmä. (Karelia-ammattikorkeakoulu 2020a, 26.)

1.2 Opinnäytetyön tavoitteet ja rajaukset

Opinnäytetyö toteutetaan Karelia laatutyöryhmän toimeksiannosta. Laaturyhmä on yksi Karelian kehittämisryhmistä, joilla on tärkeä merkitys ammattikorkeakoulun johtamisessa, kehittämisessä ja päätöksenteon valmistelussa. Opinnäytetyön aiheena on EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 mukaisen tietosuojan toteutuminen Karelia-ammattikorkeakoulun ydinprosesseissa ja niitä tukevissa hallinto- ja tukipalveluissa. *Tietosuoja* on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Opinnäytetyön tavoitteena on kartoittaa henkilötietojen käsittelyyn liittyvän tietosuojan toteutumisen nykytilanne Karelian ydintoiminnoissa. Tässä opinnäyte-

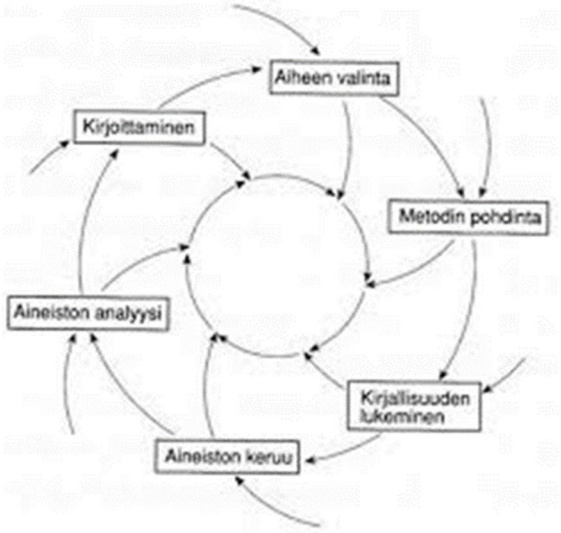
työssä *henkilötietojen käsittely* ymmärretään sen vakiintuneen määritelmän mukaisesti. Henkilötietojen käsittelyllä tarkoitetaan kaikkia henkilötietoihin kohdistuvia toimenpiteitä henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen. Työn edetessä otettiin tarkastelun kohteeksi myös ydintoimintoja tukevat Hallinto- ja tukipalvelut, joissa pääasiallinen henkilötietojen käsittely tapahtuu. Lisäksi tarkastellaan tietosuojatyön organisointia sekä johtamisen roolia tietosuojan toteuttamisessa muutos- ja tietojohtamisen näkökulmasta. Kartoituksen avulla kerätään tietoa EU:n tietosuoja-asetuksen asettamien velvoitteiden toteutumisesta henkilötietojen käsittelyssä, rekisterinpitäjän velvollisuuksien täyttymisestä, henkilökunnan tietosuojaosaamisen tasosta ja tietosuojatyön organisoinnin tilanteesta Karelia-ammattikorkeakoulussa.

Tutkimustyön kohderyhmäksi on rajattu Karelian henkilöstö; opiskelijoiden osalta työssä käsitellään opiskelijoiden ja hakijoiden henkilötietojen käsittelyä sekä huomioidaan opiskelijoille suunnatut henkilötietojenkäsittelyä ja tietosuojaa koskevat ohjeistukset. Tietosuojan mahdollistava tietoturva on laajana jätetty tutkimuksen ulkopuolelle. *Tietoturva* on yksi tietosuojan toteuttamisen keino, jonka tarkoituksena suojata tietoaineisto ja tietojärjestelmät. Sillä tarkoitetaan muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen.

Tutkimustyö kehittää myös kirjoittajien tietosuojasäännösten tuntemista ja soveltamista omassa työssään. Uutta osaamista voidaan hyödyntää omissa työtehtävissä opiskelijoiden ja hakijoiden henkilötietojen käsittelyssä, sekä jakamalla tietosuojaosaamista omassa työyksikössä. Samalla osallistutaan koko Karelian tietosuojatyön toteuttamiseen.

1.3 Opinnäytetyön rakenne

Hirsjärven, Remeksen & Sajavaaran (2016, 14) mukaan tutkimustyö on toisiaan seuraavien vaiheiden jopa päättymätön prosessi, joka voidaan aloittaa lähes jokaisesta prosessin kohdasta ja joka ohjaa tehtyjen valintojen uudelleen harkintaan. Tutkimustyö alkaa aiheen valinnalla ja aiheen löydyttyä aihepiirin rajauksella, jota säätelee tehtävänanto. Laadulliselle ja toimintatutkimukselle tyypillinen rakenne on esitetty kuviossa 1. (Hirsjärvi ym. 2016, 14 – 16.)



Kuvio 1. Tutkimusspiraali. (Teoksessa Tutki ja kirjoita. Hirsijärvi ym. mukaan 2016, 14.)

Työmme teoreettisen viitekehyksen eli tutkimuksen teoreettisen osuuden luovat kansainvälinen EU:n yleinen tietosuoja-asetus ja sitä täsmentävä ja täydentävä kotimainen lainsäädäntö; - Suomen perustuslaki (731/1999 § 10), Tietosuojalaki (1050/2018), Laki yksityisyyden suojasta työelämässä (759/2004), Laki ammattikorkeakouluista (932/2014) - ja Tietosuojavaltuutetun antamat tarkemmat määräykset ja -ohjeet sekä Karelian tietoturva- ja tietosuojapolitiikkaa ja niitä täydentävät ohjeet ja toimintamallit. Pääasiassa tutkitaan kuitenkin tietosuoja-asetuksen mukaista henkilötietojen käsittelyä, rekisterinpitäjän vastuita ja rekisteröidyn oikeuksia sekä tietosuojan organisointia. Teoreettiseen viitekehykseen kuuluvat myös muutos- ja tietojohtaminen. Kokemusperäisen (empiirinen) viitekehyksen muodostavat omat havaintomme, kvantitatiivinen tietosuojakysely henkilöstölle

sekä kvalitatiivinen yksilöhaastattelu. Näitä tarkastellaan tarkemmin luvussa 5. Lähestymistapa ja tutkimusmenetelmät.

Opinnäytetyön alussa esitellään työn tausta, lähtökohdat, tavoite ja rajaukset. Toisessa luvussa käydään läpi tietosuoja-asetuksen keskeisimpiä käsitteitä ja osa-alueita sekä tietosuojatyötä ohjaavaa kansallista lainsäädäntöä. Kolmannessa luvussa keskitytään tietosuojatyön organisointiin sekä johtamiseen yleisesti ja neljännessä luvussa kuvataan sen toteutuminen Karelia-ammattikorkeakoulussa. Opinnäytetyön lähestymistapa ja tutkimusmenetelmät on kuvattu viidennessä luvussa. Tutkimusaineiston analysointi- ja kehitysehdotukset on kuvattu kuudennessa luvussa. Työn johtopäätökset esitetään viimeisessä luvussa.

2 EU:n tietosuoja-asetus ja sitä täydentävä kansallinen lainsäädäntö

Teknologinen kehittyminen, maailmanlaajuinen verkottuminen (globalisoituminen) ja digitalisoituminen ovat johtaneet siihen, että henkilötietoja kerätään entistä enemmän. Euroopan unionin (EU) mukaan tämä aiheutti tarpeen uudistaa ja nykyaikaistaa henkilötietojen suojaa koskevaa sääntelyä. Tietosuoja-asetuksen tavoitteena on "*riittävän perusteellisella johdon ja henkilöstön tietosuojaosaamisella lisätä organisaatioiden tuottavuutta ja tehokkuutta sekä saada aikaan kustannussäästöjä."* Tietotosuoja-asetuksessa säädellään rekisterinpitäjän vastuista ja velvollisuuksista sekä määritellään rekisteröidyn oikeuksista, jotka vastaavat pitkälti Suomessa jo käytössä olevaa aiempaa sääntelyä. Kansallinen lainsäädäntö täydentää tietosuoja-asetusta. (Andreasson, Koivisto, Ylipartanen 2016, 11 – 12; Valtiovarainministeriö 2016, 6.)

Tietosuoja-asetusta sovelletaan kaikkeen automaattiseen henkilötietojen käsittelyyn sekä henkilötietojen käsittelyyn, kun henkilötiedot muodostavat rekisterin osan. Sitä sovelletaan sekä yksityisellä että julkisella sektorilla riippumatta esi-

merkiksi henkilötietojen käsittelyn laajuudesta, käsiteltävien henkilötietojen luonteesta tai käytetystä teknologiasta. Tietosuoja-asetus koskee kaikkia sen soveltamisalaan kuuluvia henkilötietoja käsitteleviä organisaatioita, rekisterinpitäjiä ja henkilötietojen käsittelijöitä. (Oikeusministeriö 2017, 9.)

Digitalisaation ja innovaatioiden myötä kysymykset henkilötietojen käsittelyyn liittyen ovat lisääntyvät ja rekisteröidyt ovat yhä tarkempia siitä, mihin henkilötietojaan antavat; mikä on henkilötietojen keräämisen tarkoitus ja mihin tietojärjestelmiin niitä tallennetaan. Henkilötietojen käsittelytoimia voidaan kuvata kirjallisissa selosteissa, joista käy ilmi muun muassa rekisterinpitäjä, henkilörekisterien vastuuhenkilöt, käsiteltävät henkilötiedot ja niiden lähteet sekä tiedot rekisterin ylläpitämiseen käytettävistä tietojärjestelmistä. Lainsäädännön velvoitteiden toteutumisen varmistamiseksi rekisterinpitäjän on kiinnitettävä huomiota henkilörekisterihallinnon suunnitteluun ja sen määrityksiin. Rekisterinpitäjän tulee huolehtia henkilörekisterihallinnon dokumentaation ajantasaisuudesta. (Andreasson, Riikonen, Ylipartanen 2019, 82.)

2.1 Tietosuoja-asetuksen yleisiä periaatteita

Tietosuoja-asetuksen tarkoituksena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. Tietosuoja-asetusta sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn, kun henkilötietojen käsittely on kokonaan tai osittain automatisoitu tai henkilötiedot muodostavat rekisterin osan. Tietosuoja-asetuksessa noudatetaan *riskiperustaista lähestymistapaa.* Rekisterinpitäjän on huolehdittava *tietosuojaperiaatteiden*, *sisäänrakennetun ja oletusarvoisen tietosuojan* sekä *osoitusvelvollisuuden toteuttamisesta*.

2.1.1 Riskiperustainen lähestymistapa

Riskiperustainen lähestymistapa tarkoittaa, että tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyvät riskit voidakseen toteuttaa asetuksen sisäänrakennettua ja oletusarvoista tietosuojaa sekä muita asetuksessa säädettyjä velvollisuuksia. Tietosuoja-asetuksessa riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun käsittely voi johtaa syrjintään tai taloudellisiin menetyksiin. Käsiteltäessä erityisiä henkilötietoryhmiin kuuluvia tietoja, esimerkiksi lapsen tiedot tai sairauskertomukset, riski voi olla suurempi. Korkean riskin käsittelytilanteissa tulee toteuttaa erityinen riskiarvio käsittelytoimien vaikutuksista henkilötietojen suojalle. (Andreasson ym. 2019, 29.)

2.1.2 Tietosuojaperiaatteet ja osoitusvelvollisuus

Tietosuoja-asetus edellyttää rekisterinpitäjiä huolehtimaan sisäänrakennetusta ja oletusarvoisesta tietosuojasta. *Sisäänrakennetun tietosuojan periaate* edellyttää rekisterinpitäjää huolehtimaan tietosuojaperiaatteiden noudattamisesta kaikissa henkilötietojen käsittelyä sisältävissä toiminnoissa ja kaikissa käsittelyn vaiheissa. Tietosuoja-asetus velvoittaa rekisterinpitäjiä huomioimaan tietosuoja-asetuksen vaatimukset jo palvelujen ja toimintojen suunnitteluvaiheesta lähtien. *Oletusarvoisen tietosuojan periaate* tarkoittaa sitä, että rekisteripitäjän tulee oletusarvoisesti käsitellä vain käsittelyn kunkin vaiheen kannalta tarpeellisia henkilötietoja. Velvollisuus koskee kerättyjen henkilötietojen määrää, laajuutta, säilytysaikaa ja saatavilla oloa. Rekisterinpitäjän on huolehdittava siitä, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta. Tietosuojaperiaatteet ovat

- käsittelyn lainmukaisuus, asianmukaisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen

- tietojen eheys ja luottamuksellisuus. (Andreasson ym. 2019, 30 – 31.)

Henkilötietojen käsittelyn asianmukaisuuden ja lainmukaisuuden varmistamiseksi tietosuoja-asetus edellyttää rekisterinpitäjältä *osoitusvelvollisuutta* (accountability -periaate). Rekisterinpitäjän on pystyttävä osoittamaan, että se noudattaa tietosuojaperiaatteita omassa toiminnassaan. Rekisterinpitäjän tulee määritellä, mitä tietosuojaperiaatteet tarkoittavat ja miten ne käytännössä toteutuvat omassa organisaatiossa. Osoitusvelvollisuuden todentamiseksi rekisterinpitäjän tulee aktiivisesti ja oma-aloitteisesti kuvata kirjallisten suunnitelmien ja dokumentaation avulla henkilötietojen käsittelytavat ja prosessit. Kirjallisen dokumentaation, sertifiointien ja tietotilinpäätöksen avulla organisaatio voi todistaa (prove it), että tietosuojavaatimukset ovat osa henkilötietojen käsittelyprosessia. Osa osoitusvelvollisuuden täyttämisen varmistamista on myös vaikutustenarviointien, ennakkokuulemisten ja henkilötietojen tietoturvaloukkauksien dokumentointi ja niitä varten suunnitellun prosessin kuvaaminen. Rekisterinpitäjä on velvollinen pitämään dokumentaation ajantasaisena päivittämällä sitä aina tarvittaessa. Osoitusvelvollisuuden tavoitteena on lisätä toimintaprosessien tuottavuutta ja tehokkuutta sekä säästää kustannuksia. Asetuksen velvoitteiden noudattamista tuetaan tehokkaalla täytäntöönpanolla. Tietosuojavelvoitteiden noudattamisen ja osoitusvelvollisuuden toteuttamisen laiminlyönneistä seurauksena (sanktiot) voivat olla valvontaviranomaisen määräämät, jopa satojentuhansien eurojen, hallinnolliset sakot. (Andreasson ym. 2019, 25, 31; Hanninen, Laine, Rantala, Rusi & Varhela 2017, 51 – 53.)

2.1.3 Henkilötietojen tietoturvaloukkauksiin varautuminen

Rekisterinpitäjän tulee varautua henkilötietojen tietoturvaloukkauksiin. Rekisterinpitäjällä on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta tietosuojan valvontaviranomaiselle, tietosuojavaltuutetun toimistolle sekä rekisteröidylle. Ilmoitus on tehtävä tietosuojavaltuutetun toimistolle mahdollisuuksien mukaan 72 tunnin kuluessa havainnosta. Henkilötietojen käsittelijän on ilmoitet-

tava tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä loukkauksen ilmettyä. Rekisterinpitäjän on ilmoitettava rekisteröidylle tietoturvaloukkauksesta ilman aiheetonta viivytystä, mikäli se todennäköisesti aiheuttaa korkean riskin henkilön oikeudelle ja vapaudelle, esimerkiksi identiteettivarkauden. Rekisterinpitäjän tulee määrittää vastuut ja kuvata prosessi tietosuojaan liittyvien tietoturvaloukkauksien varalta, jotta se pystyy reagoimaan annetun aikarajan puitteissa. Tietoturvaloukkausten reagoimisprosessissa tulee huomioida johdon, tietojärjestelmistä vastaavien tahojen sekä operatiivisten toimien vastuuhenkilöiden roolit. Rekisterinpitäjä on velvollinen dokumentoimaan henkilötietojen tietoturvaloukkaukset ja niihin vaikuttaneet seikat, vaikutukset ja tehdyt korjaustoimenpiteet. Valvontaviranomaisen on pystyttävä tarkistamaan dokumentoinnin avulla, että rekisterinpitäjä on noudattanut ilmoitusvelvollisuuttaan. (Hanninen ym. 2017, 109 – 112.)

Tietosuoja-asetus velvoittaa rekisterinpitäjiä nimittämään tietosuojavastaavan eli organisaation sisäisen asiantuntijan, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa (Tietosuojavaltuutetun toimisto 2018). Tietosuoja-asetuksessa on määritelty tietosuojavastaavan asema sekä tehtävänkuva. Tietosuojavastaavan yhteystiedot on ilmoitettava julkisesti ja hänet tulee tavoittaa helposti. On tärkeää huomata, että tietosuojavastaava ei ole vastuussa tietosuoja-asetuksen velvollisuuksien noudattamisesta. Organisaation johdon on huolehdittava tietosuoja-asetuksen noudattamisesta ja kyettävä näyttämään toteen dokumentaation avulla, että henkilötietoja käsitellään tietosuoja-asetuksen mukaisesti. (Hanninen ym. 2017, 122 – 123.)

2.1.4 Rekisteröidyn oikeudet

Tietosuoja-asetus velvoittaa rekisterinpitäjää huolehtimaan rekisteröidyn oikeuksista. Se on yksi rekisterinpitäjän päävelvollisuuksista. *Rekisteröidyllä* tarkoitetaan henkilöä, jota henkilötieto koskee. *Rekisterinpitäjällä* tarkoitetaan luonnollista henkilöä tai organisaatiota, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä. *Henkilötietoja* ovat sellaiset tiedot, joiden

perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä jokin yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella. (Hanninen ym. 2017, 19 – 22.)

Tietosuoja-asetuksessa säädetyt rekisteröidyn oikeudet ovat:

- oikeus saada tietoa henkilötietojensa käsittelystä
- oikeus saada pääsy tietoihin
- oikeus tietojen oikaisemiseen
- oikeus poistaa tietoja ja tulla unohdetuksi
- oikeus rajoittaa tietojen käsittelyä
- oikeus siirtää tiedot järjestelmästä toiseen
- oikeus vastustaa tietojen käsittelyä
- oikeus olla joutumatta automaattisen päätöksenteon kohteeksi. (Hanninen ym. 2017, 56).

2.1.5 Seloste henkilötietojen käsittelytoimista

Henkilötietolaki (523/1999) edellytti rekisterinpitäjän laatimaan käsittelemistään henkilötiedoista rekisteri- tai tietosuojaselosteen. Laki on kumottu tietosuojalailla (1050/2018), jossa edellytystä ei enää ole. Myöskään tietosuoja-asetus ei edellytä rekisteri- tai tietosuojaselosteen laatimista, mutta tietosuoja-asetuksen artiklan 30 mukainen henkilötietojen kirjallinen kuvaus, seloste käsittelytoimista, sisältää samat tiedot. Seloste on organisaation sisäinen asiakirja ja toimii henkilötietojen käsittelyn hahmottamisen apuvälineenä. Sen tarkoituksena on osoittaa henkilötietojen tietosuojalainsäädännön mukainen käsittely ja se on olennainen osa organisaation osoitusvelvollisuuden toteuttamista. Rekisterinpitäjällä on velvollisuus informoida rekisteröityjä henkilötietojen käsittelyssä (tietosuoja-asetus 12, 13 ja 14 artikla). Se päättää itse, miten täyttää informointivelvoitteen ja voi hyödyntää informaation tuottamisessa selostetta käsittelytoimista. (Tietosuojavaltuutetun toimisto 2018.)

Rekisterinpitäjä tai henkilötietojen käsittelijä on velvoitettu tekemään seloste käsittelytoimista, jos organisaatiossa on yli 250 työntekijää. Tällöin selosteen on katettava kaikki käsittelytoimet. Seloste on tehtävä työntekijöiden määrästä riippumatta, kun

- henkilötietojen käsittely aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille tai
- henkilötietojen käsittely ei ole satunnaista tai
- käsiteltävät henkilötiedot sisältävät erityisiä tietoryhmiä tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja. (Tietosuojavaltuutetun toimisto 2020).

Selosteessa on oltava vain ne käsittelytoimet, jotka kuuluvat edellä mainittuihin kategorioihin. Jos satunnaisen henkilötietojen käsittelyn perusteena on todennäköinen riski rekisteröidyn oikeuksille ja vapauksille tai erityiset henkilötietoryhmät, tulee henkilötietojen käsittely sisällyttää selosteeseen. (Tietosuojavaltuutetun toimisto 2020.)

Tietosuojavaltuutetun toimiston (2018) laatiman ohjeen mukaisesti selosteen käsittelytoimista tulee sisältää, kun selosteen laatijana on

1) rekisterinpitäjä
   - rekisterinpitäjä ja tietosuojavastaavaa,
   - käsittelyn tarkoitukset,
   - kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä,
   - ryhmät, joille henkilötietoja on luovutettu tai luovutetaan,
   - tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle,
   - tietojen säilytysajat ja
   - kuvaus teknisistä ja organisatorisista turvatoimista.

2) henkilötietojen käsittelijä
   - käsittelijä ja tietosuojavastaava,
   - rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät,
   - tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle ja
   - kuvaus teknisistä ja organisatorisista turvatoimista.

2.2 Kansallinen lainsäädäntö ja hallituksen esitykset

Suomen perustuslain (731/1999) 2 luvun 10.1 §:n mukaan tarkemmasta henkilötietojen suojasta säädetään lailla. Näin ollen tietosuoja on perusoikeus ja sen yksityiskohdista sekä rajoituksista voidaan säätää lailla. Myös yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä tulee turvata lainsäädännöllä. Perustuslakivaliokunta on erilaisia rekistereitä arvioituaan esittänyt lainsäädäntöä tarkoittavia edellytyksiä koskien henkilötietojen suojaa rekistereissä:

- rekisteristä on yksityiskohdittain säädettävä lakitasossa mainiten mm. käyttötarkoitus, esimerkiksi rekisteritietojen poistamisajankohta tai säilytysaika
- rekisteriin merkityllä täytyy olla käytettävissään oikeussuojakeino; oikeussuojamenetelmä henkilön oikeudesta tarkastaa itseään koskevat rekisteriin merkityt tiedot
- julkisen vallan harjoittamalla rekisteröinnillä on oltava hyväksyttävä tarkoitus, esimerkiksi rikoksen selvittäminen ja
- lailla säätämiseen liittyvä tarkkuusvaatimus. (Saraviita 2011, 184 – 185.)

Hallituksen esitys (HE 2/2020 vp) eduskunnalle laeiksi oikeusministeriön hallinnonalan eräiden henkilötietojen käsittelyä koskevien säännösten muuttamisesta.

> Esityksessä ehdotetaan tehtäviksi Euroopan unionin tietosuojalainsäädännöstä johtuvat välttämättömät lainmuutokset oikeusministeriön hallinnonalan lainsäädäntöön. Esityksessä ehdotetaan tarkistettavaksi oikeusministeriön hallinnonalan lainsäädäntöä erityisesti tietosuoja-asetuksen ja tietosuojalain soveltamisalalla, mutta myös eräitä rikosasioiden tietosuojalain soveltamisalaan kuuluvia lakeja muutettaisiin.
>
> Esityksen tarkoituksena on yhdenmukaistaa henkilötietojen käsittelyyn liittyviä erityissäännöksiä ja selkiyttää niiden suhdetta sovellettaviin yleislakeihin.

Tietosuojalaki (1050/2018) astui voimaan 1.1.2019. Se kumosi aiemmin voimassa olleet henkilötietolain (523/1999) ja tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain (389/1994). Tietosuojalain tarkoitus on täsmentää ja täydentää luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetusta yleisestä tietosuojasta (EU) 2016/679 (yleinen tietosuoja-asetus, GDPR), ja sen kansallisesta soveltamisesta. Yleinen tietosuoja-asetus on sellaisenaan jäsenvaltioissa sovellettavaa oikeutta. Hallituksen esityksen (HE 9/2018) tarkoituksena on täydentää ja täsmentää EU:n tietosuoja-asetusta henkilötietojen käsittelyssä.

Henkilötietojen käsittelystä työsuhteen yhteydessä säädetään **työelämän tietosuojalaissa** (laki yksityisyyden suojasta työelämässä (759/2004). Lakiin tuli muutoksia 1.4.2019 alkaen, kun Laki yksityisyyden suojasta työelämässä annetun lain muutoksesta (347/2019) astui voimaan. Muutokset koskevat esimerkiksi täsmennyksiä työntekijän terveydentilatietojen säilyttämistä ja sitä, milloin työnantaja voi kerätä työntekijän henkilötietoja ilman tämän suostumusta. Täsmennykset johtuvat tietosuojalaista, henkilötietolain kumoamisesta ja rikoslain muutoksesta. (Tietosuojavaltuutetun toimisto 2018b.)

Laissa ammattikorkeakouluista (932/2014) säädetään opiskelijavalintaan liittyvästä tiedonsaannista (27 §) sekä opiskelijaksi pyrkivän ja opiskelijan terveydentilaa koskevien arkaluonteisten tietojen käsittelystä ammattikorkeakoulussa (40 §). Lain §:ssä 65 säädetään tiedon haltijan oikeudesta antaa opiskelijan terveydentilaa ja toimintakykyä koskevia ja tehtävien hoidon kannalta välttämättömiä tietoja, laissa erikseen nimetyille ammattikorkeakoulun toimenhaltijoille määrätyissä tilanteissa, ilman salassapitosäännösten sitä estämättä.

Laki julkisen hallinnon tiedonhallinnasta (906/2019) astui voimaan 1.1.2020. Laki on yleislaki ja se kumoaa lain Julkisen hallinnon tietohallinnon ohjauksesta (634/2011). Laki edistää tiedonhallinnan yhdenmukaistamista, tietoturvallisuutta ja digitalisointia viranomaistoiminnassa, ja sitä sovelletaan tiedonhallintaan ja tie-

tojärjestelmien käyttöön viranomaisten käsitellessä tietoaineistoja, jotka *koostuvat asiakirjoista tai tiedoista, joista voidaan muodostaa asiakirjoja.* (Valtiovarainministeriö 2020.) Lain säädökset koskevat tiedonhallintaa ja tietoturvaa, ei suoranaisesti henkilötietojen käsittelyä ja tietosuojaa. Hyvä tiedonhallinta sekä hyvin organisoitu ja toimiva tietoturva on kuitenkin edellytys tietosuojan toteutumiselle.

Tiedonhallintalaissa säädetyt tietosuojaa koskevat tavoitteet ovat

- tiedonhallintaan liittyvien vaatimusten yhtenäistäminen ja selkeyttäminen koko julkisessa hallinnossa,
- edistää tietosuojaa, tietoturvallisuutta ja tietoaineistojen vastuullista hyödyntämisestä sekä julkisuusperiaatteen toteutumista (Valtiovarainministeriö 2020, 5 – 6).

3 Tietosuojatyön organisointi ja johtaminen

Andreassonin ym. (2019, 77) mukaan *tietojen käsittelyyn ja tietotekniikkaan liittyvät riskit tulee tunnistaa ja hallita aktiivisesti ja niiden negatiivisia vaikutuksia tulee minimoida teknisillä ja hallinnollisilla keinoilla*. Sähköisten palvelujen laajentuminen ja digitalisaatio lisäävät tietosuojan tärkeyttä. Organisaation palvelujen jatkuvuuden turvaaminen kaikissa olosuhteissa on tietoturvallisuuden ja tietosuojan tärkein päämäärä. Niillä *tuetaan organisaation toiminnalle asetettuja vaatimuksia ja varmistetaan tietojen ja tietojärjestelmien huolellinen käsittely ja kansalaisten yksityisyyden suoja.* (Andreasson ym. 2019, 77.)

Tietosuojan organisoinnissa on olennaista kartoittaa tilannekuva ja kuvata tietosuojatyöllä tavoiteltavat päämäärät. Organisaation ylimmän johdon on tiedettävä millä tasolla tietosuojan organisointi ja henkilöstön tietosuojaosaaminen ovat. Nykytilan selvittämiseksi voidaan tehdä taustakartoitus (muistilista taustakartoituksesta liitteenä 1). Kartoituksen tulosten selvittyä johto voi aloittaa systemaattisemman tietosuojatyön organisoinnin ja edellytysten luonnin tietosuojatyön

toteuttamiselle. Tilannekartoituksen jälkeen tulee tarkistaa, että riittävät, asianmukaiset päätökset on tehty ja ne ovat lain- ja ajanmukaisia. (Andreasson ym. 2019, 78 – 80.)

Henkilötietojen käsittelijöiden ohjeistaminen, rekisteröityjen informointi henkilötietojen käsittelystä ja ennakoiva riskienhallinta kuuluvat rekisterinpitäjän velvollisuuksiin. Tietoturva ja tietosuoja tulee olla sisäänrakennettuna organisaation toimintaan. Riskien arviointi ja tunnistaminen tulisi olla osa tietosuojaa sekä päivittäistä ja normaalia organisaation sisäistä toimintaa. (Arjen tietosuoja, 2018.) Hyvän organisoinnin tavoitteena on tuottavuuden ja tehokkuuden lisääminen sekä tietosuojariskien hallinnointi; ylimmän tason organisointi ja linjaukset tulee siis tehdä huolellisesti. Tietosuoja- ja tietoturvatyön tulee olla osa jokaisen työntekijän jokapäiväistä työtä. Työntekijöille annettavien tietosuoja-asioita koskevien ohjeiden, suunnitelmien, määräysten ja päätösten tulee olla selkeitä, jotta ne tukevat henkilöstön työntekoa. Tietosuojatyön organisointiin ja hallintaan liittyvät johdon velvollisuudet ja vastuut on kuvattu kuviossa 2. (Andreasson ym. 2019, 50 – 51, 77 – 78.)

Kuvio 2. Tietosuojatyön organisointi ja hallinta. (Opi tietosuojaa 2018.)

3.1 Johdon ja esimiesten vastuut ja velvoitteet

Johdolla ja esimiehillä on keskeinen rooli organisaation tietosuojan toteutumisessa ja he voivat omalla toiminnallaan osoittaa, että tietosuoja-asioihin tulee suhtautua vakavasti. Heidän on hallittava henkilötietojen käsittelyn yleiset periaatteet, käsittelyn lainmukaisuus ja tietosuoja-asetuksen rekisterinpitäjälle asettamat vastuut, joihin kuuluu muun muassa rekisteröidyn oikeuksien toteutumisesta huolehtiminen. Henkilötietojen käsittelyä koskevia päätöksiä tehdessään he käyttävät rekisterinpitäjälle kuuluvaa määräysvaltaa. He myös käsittelevät henkilötietoja, jolloin heidän suhtautumistapansa tietosuoja-asioihin välittyy esimerkkinä henkilökunnalle. On hyvä muistaa, että henkilötietojen käsittelyn lainmukaisuudesta vastaa aina organisaaton johto. (Arjen tietosuoja 2018.)

Rekisterinpitäjä voi osoittaa noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä toteuttamillaan teknisillä ja organisatorisilla toimenpiteillä, joita tarkistetaan ja päivitetään tarvittaessa. Tietosuojan toteutuminen tietosuoja-asetuksen mukaisesti edellyttää selkää ohjeistusta ja koulutusta eri kohderyhmille. Organisaatiossa tulee laatia tietosuojapolitiikka, jossa tuodaan esille johdon sitoutuminen tietosuojan toteuttamiseen ja kuvataan eri tahojen vastuut tietosuojan toteuttamisessa. Myös henkilökunnalle ja henkilötietoja rekisterinpitäjän puolesta käsitteleville ulkopuolisille toimijoille tulee laatia ohjeistukset. On tärkeää tunnistaa henkilötietoja käsittelevien henkilöiden tehtävät ja roolit ja luoda ohjeisto sen mukaisesti. Tietosuojan kehittymistä voidaan seurata vuosittain tehtävässä tietotilinpäätöksessä. (Arjen tietosuoja 2018.)

3.2 Tietotilinpäätös

Tietotilinpäätös on organisaation sisäisen tarkastelun tuloksena syntynyt raportti. Siinä kuvataan tietojenkäsittelyprosessin ja tiedonhallinnan tila ja lainmukaisuus, ja sillä voidaan täydentää lakisääteistä tilinpäätöksiin ja toimintakertomuksiin kuuluvaa raportointia. Ensisijaisesti tietotilinpäätös on organisaation johdon työkalu,

jonka avulla voidaan hahmottaa kokonaiskuva henkilötietojen käsittelyn nykytilasta ja tukea organisaation tehokkuutta, vaikuttavuutta ja kilpailukykyä. Tietotilinpäätöstä voidaan käyttää organisaation sisäisenä tietojohtamisen raporttina ja sen avulla voidaan myös raportoida sidosryhmille tietojen käsittelyä koskevista keskeisistä asioista. (Tietosuojavaltuutetun toimisto 2012, 3.)

3.3 Tietosuojavastaava

Hallinnollisen johdon tehtävä on nimetä tietosuojavastaava, hänen tehtävänsä ja toimenkuvansa sekä tiedottaa niistä henkilöstölle. Tietosuojavastaavan nimeäminen julkisella sektorilla, pois lukien tuomioistuimet, on pakollista ja perustuu EU:n yleisen tietosuoja-asetuksen artiklan 37 kohtaan 1. Sen riskiperusteiseen lähestymistapaan perustuen tietosuojavastaava tulee nimittää myös yrityksiin, joiden päätoiminnassa seurataan henkilötietoja laajassa mitassa tai käsitellään arkaluontoisia henkilötietoja laajalti. Tietosuojavastaavaa nimitettäessä tulee ottaa huomioon henkilön ammatillinen pätevyys sekä tuntemus tietosuojalainsäädännöstä ja alan käytänteistä. Tietosuojavastaava toimii hallinnollisen johdon tukena ja henkilöstön apuna, seuraa ja valvoo asiakastietojen käyttöä ja raportoi johdolle. Tehtäviin voi kuulua myös suunnittelu- ja toimenpanotehtäviä sekä henkilöstön kouluttamista henkilötietojen käsittelyyn liittyvistä laeista ja menettelytavoista. (Andreasson ym. 2019, 84 – 85, 92, 98 – 99; Hanninen ym. 2017, 122 – 123.)

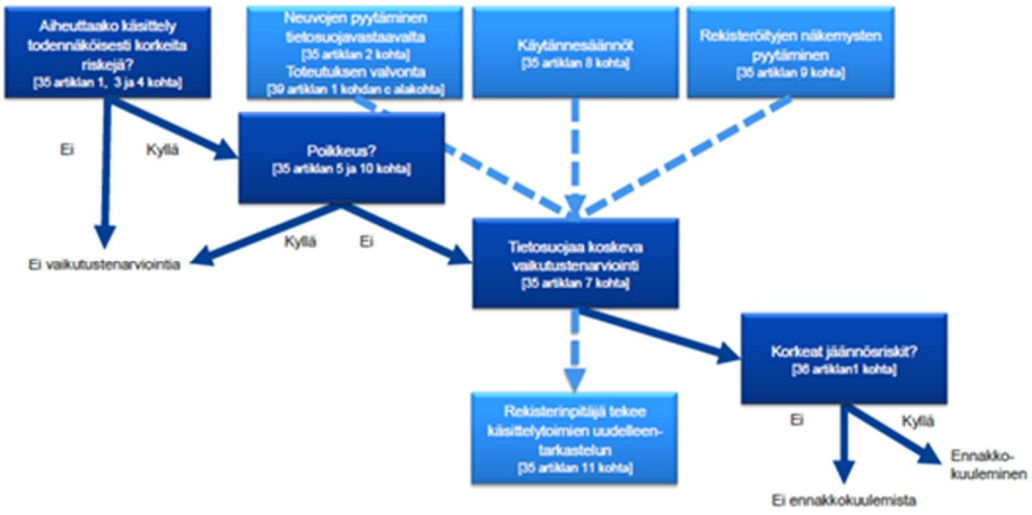
Johdon tulee varmistaa, että tietosuojavastaavalla on riittävät resurssit tietosuojatyön toteuttamiseksi; määritellä riittävä työaika ja järjestää taloudelliset- ja työvälineresurssit sekä kouluttautumismahdollisuus. Tarkemmin tietosuojavastaavan tehtävistä määritetään tietosuojan-asetuksessa. Tietosuojavastaavan avuksi on suositeltavaa nimetä säännöllisesti kokoontuva tietosuoja- ja tietoturvaryhmä ja määritellä sen tehtävät. Suurissa ja keskisuurissa yrityksissä on lisäksi hyvä nimetä tietosuojan ja tietoturvan yhteyshenkilöitä, joiden kautta esimerkiksi ohjeet ja määräykset voidaan jalkauttaa henkilöstölle. (Andreasson ym. 2016, 58 – 59; Arjen tietosuoja 2018.)

3.4 Riskienhallinta ja vaikutustenarviointi

Henkilötietojen käsittelyn suojaaminen perustuu tietoturvallisuuden eri osa-alueiden toteuttamiseen. Tietosuojan toteutumisen perusedellytyksenä on toiminnan jatkuvuudesta, tietojen ja palveluiden saatavuudesta, eheydestä ja luottamuksellisuudesta huolehtiminen. Tämä on myös osa rekisterinpitäjän tietosuoja-asetuksen mukaisen osoitusvelvollisuuden täyttämistä. Riskienhallinta on osa tietosuojan toteuttamista. Laatimalla riskienhallintaprosessin ja toimintamallin johto varmistaa riskienhallintaprosessin organisaation eri tasoilla. Eri tilanteita varten laaditaan ohjeet ja luodaan prosessi sekä varmistetaan henkilöstön valmius toimia tietoturvaloukkaustilanteissa. Johdon tehtävänä on myös varmistaa, että riskienhallinnan ja tietoturvaloukkausten prosessit voidaan varmasti toteuttaa ja että ne ovat toiminnassa. Vakavan henkilötietojen tietosuojaloukkauksen tai rikkomuksen tapahtuessa, organisaation tulee tietosuoja-asetuksen osoitusvelvollisuuden velvoittamana voida osoittaa, että sillä on toimivat prosessit tietoturvallisuuden ja tietosuojan toteuttamiseksi. Tietosuojaloukkauksista tulee ilmoittaa rekisteriviranomaiselle ja rekisteröidylle. Rekisterinpitäjän tulee dokumentoida kaikki henkilötietojen tietoturvaloukkaukset, niihin vaikuttaneet seikat, loukkausten vaikutukset ja toteutetut korjaavat toimenpiteet. (Andreasson ym. 2019, 57 – 58; Arjen tietosuoja 2018.)

Vaikutustenarviointi (data protection impact assessment, DPIA) on jatkuva riskien tunnistamisen ja hallitsemisen prosessi, jonka tarkoituksena on auttaa *tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Se auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, sen dokumentoinnissa ja osoittamisessa.* Päivitys on syytä tehdä ainakin käsittelytoimista aiheutuvien riskien muuttuessa. Vaikutusten arvioinnin tekeminen koskee myös ennen 25.5.2018 alkaneita, käynnissä olevia käsittelytoimia. Rekisterinpitäjän on arvioitava vaikutustenarvioinnin tarpeellisuus. Rekisterinpitäjän tulee tehdä vaikutustenarviointi, kun suunniteltu henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja vapauksille. (Hanninen ym. 2017, 115; Tietosuojavaltuutetun toimisto 2018c.)

Tietosuoja-asetuksen tietosuojaa koskevaan vaikutuksenarviointiin liittyvät perusperiaatteet on kuvattu kuviossa 3. Arviointi voi kohdistua yksittäiseen käsittelytoimeen tai käsittelytoimien ryhmään ja velvoite sen tekemiseen voi seurata tietosuoja-asetuksessa yksilöytyjen käsittelytilanteiden johdosta, siitä että käsittelytoimenpide on lisätty tietosuojaviranomaisen luetteloon ja kansallisesta lainsäädännöstä. Arvioinnin on sisällettävä vähintään järjestelmällinen kuvaus käsittelytoimista ja sen tarkoituksista, arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden, arvio rekisteröidyn oikeuksia ja vapauksia koskevista riskeistä sekä suunnitellut toimenpiteet riskeihin puuttumiseksi. (Tietosuojavaltuutetun toimisto 2018c.)



Kuvio 3. Tietosuoja-asetuksen tietosuojaa koskevaan vaikutuksenarviointiin liittyvät perusperiaatteet. (Tietosuojatyöryhmä 2017, 8.)

3.5 Sopimukset ja hankintaprosessi

Henkilötietojen käsittelyä voi tapahtua organisaation sisällä tai se voidaan antaa ulkopuolisen tahon hoidettavaksi. Silloin on tietosuoja-asetuksen mukaisesti tehtävät rekisterinpitäjän ja henkilötietoja rekisterinpitäjän lukuun suorittavan tahon, henkilötietojen käsittelijän kesken tietojenkäsittelysopimus. Siinä tulee huomioida asetuksen vaatimat henkilötietojen käsittelyä koskevat ehdot, muun muassa hen-

kilötietojen käsittelyn kohde, kesto, luonne ja tarkoitus ja tiedot käsiteltävistä henkilötiedoista. Tietojenkäsittelysopimuksessa on oltava määräys rekisterinpitäjän oikeuksista ja velvollisuuksista sekä henkilötietojen käsittelijän itsenäisistä vastuista. (Arjen tietosuoja 2018; Hanninen ym. 2017, 82 – 83.)

Tietosuojavastaavan on hyvä käydä rekisteripitäjän ja johdon kanssa läpi henkilötietojen käsittelyyn ja rekisterinpitäjyyteen liittyvä, tietosuoja-asetuksen 4. artiklassa määritelty käsitteistö. Käsitteistön tunteminen on erityisen tärkeää tehtäessä palvelujen ulkoistuksia ja ostamisia sekä tietojärjestelmähankintoja. On myös tarkistettava, että voimassa olevat, vanhat sopimukset ovat tietosuoja-asetuksen mukaisia eikä niissä ole ristiriitoja asetuksen sisältämien rekisterinpitäjän ja henkilötietojen käsittelijän vastuiden kesken. (Andreasson ym. 2019, 82 – 84.)

Kulmala (2017) toteaa, että rekisterinpitäjän on myös kyettävä osoittamaan muiden, sen lukuun toimivien yritysten, lainmukainen toiminta, esimerkiksi järjestelmät, jotka liittyvät henkilötietojen käsittelyyn. Henkilötietojen käsittelijällä tulee olla rekisterinpitäjän lupa alihankkijoiden käyttöön. Henkilötietojen käsittelijä on vastuussa alihankkijan toimista rekisterinpitäjälle. Henkilötietojen käsittelijän ja alihankkijan välille on tehtävä kirjallinen alihankintasopimus. Alihankkijaa koskee samat tietosuojavelvoitteet, jotka on kirjattu rekisterinpitäjän ja henkilötietojen käsittelijä väliseen sopimukseen. Alihankkijan tulee tietää ja tuntea henkilötietojen käsittelyn sopimusketjun muiden osapuolten väliset sopimusehdot. (Hanninen ym. 2017, 87; Kulmala 2017.)

Tietosuoja-asetuksen vaatimukset on huomioitava myös kilpailutusten suunnittelussa. Rekisterinpitäjän on jo ennen hankintamenettelyn aloittamista tapauskohtaisesti arvioitava sopimusvastuut ja asetuksen vaikutukset niihin. Asetuksen sopimusvaikutusten takia rekisterinpitäjän ja henkilötietojen käsittelijän on huomioitava tietosuojan vaatimukset osana sopimusneuvotteluita, kilpailutusprosessien suunnittelussa ja vaatimusten tapauskohtaisessa asettelussa. Vastuiden määrittely on osa rekisterinpitäjän osoitusvelvollisuutta, joka vaatii, että tietosuojan huomioimisesta on oltava dokumentit. (Arjen tietosuoja 2018.) On tärkeää or-

ganisoida huolellisesti erilaiset ICT-projektit, tietojärjestelmäkilpailutukset ja sopimusten laadinta sekä huolehtia, että projektipäälliköt ja hankintavastaavat saavat tarvitsemansa asiantuntija-avun tietosuoja-asioissa. (Andreasson ym. 2019, 79.)

3.6 Muutosjohtaminen ja tiedolla johtaminen tietosuojan toteuttamisessa

Tietosuoja-asetuksen tuomat muutokset organisaatioiden toimintatapoihin ja prosesseihin vaativat laajaa ja oikeanlaista viestintää. Johdolla on keskeinen rooli tietosuojatyön onnistumisessa. Johdon keskeisimpiä tehtäviä tietosuojan näkökulmasta ovat *tietosuojatyön organisointi, tietosuojavastaavan osaamisen hyödyntäminen sekä koko henkilöstön tietosuojaosaamisen varmistaminen*. Oikein toteutettuna toimenpiteiden avulla saavutetaan hyötyä ja etua organisaatiolle, työntekijöille sekä myös asiakkaille. (Andreasson ym. 2019, 87.) Muutosjohtamisen ja tiedolla johtamisen avulla pyritään varmistamaan muuttuneiden toimintatapojen integroituminen osaksi organisaation jokapäiväistä toimintaa.

3.6.1 Muutosjohtaminen

Organisaation rakenteessa tai toimintatavoissa tapahtuvan muutosprosessin läpivieminen vaatii muutoksen johtamista. Muutosjohtamisen käsitetään usein liittyvän organisaation viestintä- ja henkilöstöjohtamiseen, niin kutsuttuihin organisaation pehmeisiin osatehtäviin. Muutoksen johtaminen, muutosprosessin läpivieminen taas yhdistetään usein operatiiviseen johtamiseen ja taloudellisiin vastuisiin, organisaation koviin osatehtäviin. Erottelua niin kutsuttuihin pehmeisiin ja koviin osatehtäviin tulisi välttää. Hyvässä muutosjohtamisessa viestintä- ja henkilöstöosaaminen kytkeytyy tiiviisti operatiiviseen ja taloudelliseen johtamiseen. (Mattila 2007, 26 – 27.)

Globalisaatio, nopeasti kehittyvät teknologiset ratkaisut, kansainvälinen talouden integraatio, markkinatilanteiden muutokset, kommunististen valtioiden hajoaminen ja yksityistäminen luovat tarpeita muutoksille. Organisaatioiden on kyettävä muuttamaan toimintojaan pärjätäkseen vallitsevissa kilpailutilanteissa. (Kotter 2012, 20 – 21.) Muuttuvan lainsäädännön myötä organisaatiot ovat myös velvoitettuja muuttamaan omia käytänteitään vastaamaan sen vaatimuksia.

John Kotter (2012, 22 – 24) on esitellyt mallin johtamisen kahdeksanvaiheisesta muutosprosessista, jonka avulla muutos saadaan onnistuneesti vietyä läpi ja uusi toimintatapa juurrutettua osaksi organisaation toimintaa. Kotterin mallin kahdeksan vaihetta ovat: 1. muutoksen kiireellisyyden ja välttämättömyyden esille nostaminen, 2. ohjaavan tiimin perustaminen, 3. vision ja strategian laatiminen, 4. muutosvisiosta viestiminen, 5. henkilöstön valtuuttaminen vision mukaiseen toimintaan, 6. lyhyen aikavälin onnistumisten varmistaminen, 7. parannusten vakiinnuttaminen ja uusien muutosten toteuttaminen sekä 8. uusien toimintatapojen juurruttaminen yrityksen kulttuuriin. Kotterin mallissa neljän ensimmäisen vaiheen avulla pyritään purkamaan vallitseva nykytila. Vaiheiden 5 – 7 avulla luodaan ja otetaan käyttöön uusia toimintatapoja. Viimeisen vaiheen tarkoitus on varmistaa, että uudet toimintatavat vakiintuvat osaksi organisaation toimintaa.

Pekka Mattilan (2007, 1301 – 132) muutoksen johtamisen malliin kuuluu neljä avaintehtävää, vaihetta: 1. perustan luominen, 2. käynnistystoimet, 3. hallittu eteneminen, 4. vakiinnuttaminen. Mattilan mukaan muutosprosessin neljä avaintehtävää seuraavat toisiaan lähes kaikissa muutostilanteissa, mutta niiden sisällöt eivät ole tarkkarajaisia ja määritettyjä. Muutosprosessissa on tavallista, että prosessin seuraavassa vaiheessa palataan vielä tarkastelemaan tai työstämään edellisen vaiheen tehtäviä.

Onnistuneen muutosprosessin läpivieminen vaatii kaikkien muutoksen vaiheiden läpikäyntiä. Åhman (2005, 78 – 79), Kotter (2012, 37 – 38) sekä Mattila (2007, 135) painottavat alkuvalmistelujen tärkeyttä muutosprosessin onnistumisen kannalta. Hyvin suunniteltu pohjatyö, muutostarpeen tunnistaminen, muutoksen vision luominen ja konkreettiset muutokselle asetetut tavoitteet mahdollistavat

muutosprosessin etenemisen ja uusien toimintatapojen lanseerauksen. Henkilöstön osallistaminen muutosprosessiin jo mahdollisimman varhaisessa vaiheessa lisää henkilöstön sitoutumista muutokseen.

Organisaation johdon sitoutuminen muutoksen läpiviemiseen on tärkeää. Neljä yleisintä johtamisen virhettä, jotka vaikeuttavat muutoksen läpiviemistä ovat:

1. Johto ei kykene tuomaan esille muutoksen tärkeyttä ja sen priorisointi epäonnistuu
2. Johdon ei onnistu viestimään selvästi ja toimimaan itse esimerkkinä muutoksen toteuttamisessa.
3. Muutosta ei malteta viedä loppuun asti, vaan toimenpiteet muutoksen loppuun viemiseksi lopetetaan ensimmäisten positiivisten merkkien jälkeen.
4. Johto kuvittelee näkevänsä vastarintaa väärissä paikoissa. (Kotter 1998, Mattilan 2007, 27 mukaan).

Muutos aiheuttaa usein ihmisessä epävarmuutta. Uusi, tuntematon aiheuttaa pelkoa ja se koetaan uhkaavana. Ymmärtämättömyys muutoksen syistä, pelko ja muuttuvat toimintaympäristöt tai –tavat lisäävät muutosvastarintaa. Esimiesten tulee tukea alaisiaan muutosprosessia ja auttaa työntekijöitä ymmärtämään muutostarve ja näkemään se mahdollisuutena uhan sijasta. Muutosjohtamisen taidot, ajantasainen viestintä ja esimiesten läsnäolo työntekijöiden arjessa auttavat muutosvastarinnan murtamisessa. (Kukkola 2018, 120 – 121; Garber 2013.)

Muutosviestintä on osa strategista viestintää, eikä se voi olla irrallinen osa organisaation viestintää. Sen tavoitteena on auttaa henkilöstöä ymmärtämään muutoksen tarve ja toivottu tavoitetila. Inhimillisellä, ennakoivalla ja rakentavalla muutosviestinnällä tuetaan työyhteisön sitoutumista muutokseen. Onnistuneen muutosviestinnän avulla voidaan hyödyntää henkilöstön asiantuntemusta muutosprosessissa ja vuorovaikutus organisaation sisällä kehittyy. Muutoksista viestittäessä on tärkeää painottaa muutoksen tavoitteiden merkitystä, jotta työntekijöiden luottamus organisaatioon ja itse muutosta kohtaan ei horju. (Heiskanen & Lehikoinen 2010, 19-22; Kukkola 2018, 123 – 134.)

Muutoksesta viestittäessä on hyvä luoda viestintäsuunnitelma. Suunnitelmallinen viestintä muutosprosessin aikana mahdollistaa osaltaan muutosprosessin onnistuneen toteutumisen. (Åhman 2005, 78 – 79.) Mattilan (2007, 188 – 190) mukaan muutosviestinnässä hyvä kiinnittää huomiota viestien kieleen ja viestinnän sävyyn. Piilomerkityksiä ja tulkintaa herättävää viestintää on syytä välttää.

3.6.2 Tiedolla johtaminen

Tieto on yksi yrityksen resursseista ja sen eri tasoja voidaan kuvata käsitteillä data, informaatio ja tietämys. Tieto erotetaan myös hiljaiseen tietoon ja eksplisiittiseen tietoon. Hiljainen tieto on osin tiedostamatonta, kokemuksen kautta kertynyttä tietämystä, osaamista. Sen siirtäminen toiselle henkilölle on haasteellista. Eksplisiittinen tieto puolestaan on kirjallisessa muodossa olevaa tietoa, jota on helppo siirtää ja jakaa. Datan ja informaation voidaan katsoa olevan eksplisiittistä tietoa, sillä ne voidaan esittää yksiselitteisesti jollakin kielellä. Tietämys ja ymmärrys puolestaan ovat suurimmaksi osaksi kokemuksen kautta karttuvaa hiljaista tietoa. Tietojohtamisen peruskäsitteistö muodostuu tiedon tasoista ja ymmärryksestä. (Laihonen ym. 2013, 17 – 21.) Tiedolla johtamisessa on kyse organisaation ymmärryksen kasvattamisesta sisäisen tiedon ja informaation tunnistamiseen ja välittämiseen sekä tiedon käyttöön liittyvien prosessien hallinnasta ja johtamisesta (Jalonen 2015, 4).

Laihosen ja Lönnqvistin (2013) mukaan tietojohtamisen voi jakaa tiedolla johtamiseen ja tiedon johtamiseen:

> **Tiedolla johtamisella** tarkoitetaan olemassa olevan tiedon hyödyntämistä - toimintotapoja, joilla tietoa jalostetaan ja hyödynnetään organisaation toiminnan kehittämisessä ja päätöksenteon tukena. **Tiedon johtamisella** tarkoitetaan arvonluonnin perustana olevien tietoresurssien tunnistamista, johtamista ja tehokasta hyödyntämistä.

Tiedolla johtaminen mahdollistaa erilaisten näkökulmien, vaihtoehtojen ja riittävän informaation huomioon ottamisen johtamisessa ja päätöksenteossa, sekä

edellyttää todellisten, tilanteeseen kuuluvien tietojen keruuta johtamisen ja päätöksenteon tueksi. Tiedon käyttö johtopäätösten ja tulkintojen tekemiseksi edellyttää riittävää keskustelua ja vuorovaikusta. Silloin tiedon merkitys muuttuu tiedon jakamisesta tiedolla johtamiseksi. (Kuntaliitto 2019.)

Andreassonin ym. (2016, 9 – 10) mukaan tietosuoja liittyy johdon ja tietoperustaisen arvonluonnin näkökulmiin ja se liitetään usein tiedolla johtamiseen. Organisaation eri tasoilla ja tehtävissä tapahtuu tiedolla johtamista, jossa on määriteltynä vastuut, roolit, tehtävät ja niiden edellyttämät taidot. Yritykselle tieto on kykyä toimia ja luoda tiedon ja tietämyksen pohjalta uutta arvoa, johon tarvitaan sekä osaamisen tunnistamista että kykyä oppia jatkuvasti uutta (Kosonen 2019, 1 – 2).

> Tiedolla johtaminen on päätöksentekoa analysoidun tiedon pohjalta. Tiedolla johtaminen on kokonaisuus: tiedon tuottamista, hallintaa, säilyttämistä, analysointia ja tiedon hyödyntämistä, sekä ihmisten kykyä, mahdollisuuksia ja motivaatiota soveltaa tietoa päätöksentekoon. (Kosonen 2019, 1.)

Tietojohtaminen (Knowledge Management) on organisaation ihmisten, tekniikan, prosessien ja organisaatiorakenteen tarkoituksellista ja systemaattista tiedon luontia, jakamista ja soveltamista, sekä opittujen arvojen ja parhaiden käytäntöjen tallettamista organisaation jatkuvan oppimisen edistämiseksi (Dalkir 2005, 3). Tietojohtamisessa on kyse organisaatioiden ja työntekijöiden toiminta- ja johtamismalleista, joilla pyritään edistämään työn sujuvuutta ja organisaatioiden suorituskykyä. Tietojohtaminen on siirtynyt keskittymään tiedon tuotannosta - tuottamisesta ja jakamisesta - tiedon hyödyntämiseen. Tietojohtamisesta on tullut koko organisaation läpäisevä toimintamalli, josta ovat käytännössä vastuussa kaikki työntekijät. Onnistuneella tietojohtamisella voidaan olemassa olevaa tietoa hyödyntää uudelleen ja saamaan tehokkuushyötyjä. Tietoa tarvitaan asioiden ymmärtämiseen, päätöksentekoon sekä uuden tiedon luomiseen. Tietojohtamisella tuetaan organisaation arvonluontiprosessia. Onnistuneessa tietojohtamisessa saavutetaan merkittäviä tehokkuushyötyjä hyödyntämällä uudelleen jo olemassa olevaa tietoa. (Laihonen ym. 2013, 8 – 14.)

Karelia-ammattikorkeakoulussa entistä toimivampi tiedolla johtaminen on mahdollistettu kiinnittämällä aikaisempaa enemmän huomiota tiedon laatuun ja sen käytettävyyteen, tiedon tuottamisen ja raporttien tekemisen lisäksi. Kareliassa on kehitetty ja joitakin vuosia sitten käyttöönotettu Karelia-Vipunen –järjestelmä, joka tuottaa tietoa Karelian toiminnallisista tuloksista. Järjestelmän avulla on aikaisemmin tuotettu tietoa koulutustoiminnan seurantaan, ja kehitystyön tuloksena sen tuottamaa tietoa voidaan nyt hyödyntää myös talouden seurannassa. Nykyisin järjestelmää käyttävät koulutustoiminnan vastuuhenkilöiden lisäksi hallinnon ja TKI-toiminnan henkilöstö. Samalla tiedolla johtamisesta on muodostunut osa koko organisaation johtamista.

4 Tietosuojan organisointi ja henkilötietojen käsittely Kareliassa

Karelia-ammattikorkeakoulun johto on vastuussa tietosuojan toteuttamisesta ja henkilötietojen käsittelyn lainmukaisuudesta. Kareliaan on nimetty tietosuojavastaavaa, jonka tehtävänä on muun muassa ohjata ja kehittää tietosuojan toteuttamista ammattikorkeakoulussa. Tietosuojavastaavan lakisääteiset tehtävät on kuvattu tarkemmin luvussa 3. Tietosuojavastaavan tueksi on nimetty tietosuoja- ja tietoturvatyöryhmä, johon kuuluvat hallinto- ja talousjohtaja, tietosuojavastaava, henkilöstöpäällikkö, opiskelijapalveluiden päällikkö ja työsuojeluvaltuutettu. Tietosuoja- ja tietoturvaryhmän tehtävä on kehittää ja edistää Karelia-ammattikorkeakoulun tietosuojan ja tietoturvan toteutumista. Se muun muassa käsittelee, kommentoi ja hyväksyy tietosuojaan ja tietoturvaan liittyviä ohjeita ja linjauksia sekä käsittelee niihin liittyvät merkittävät poikkeamat. (Karelia-ammattikorkeakoulu 2018.)

Esimiesten rooli on tärkeä henkilötietojen käsittelyn toteuttamisessa. He ovat mukana määrittämässä henkilötietojen käsittelyyn ja käytännön toimintaan liittyviä ohjeita. Esimiehet vastaavat ohjeistuksen jalkauttamisessa omassa työyhteisössä. Myös jokaisen työssään tai opiskeluissaan henkilötietoja käsittelevän

työntekijän ja opiskelijan tulee noudattaa annettuja toimintaohjeita sekä tuntea ja hallita henkilötietojen käsittelyn tietosuojasääntely ja –riskit. (Karelia-ammattikorkeakoulu 2018.)

Karelian henkilötietojen käsittelyperiaatteet löytyvät sekä julkiselta www-sivulta että intrasta, samoin kuin kaikki henkilörekisterien rekisteriselosteet. Rekisterinpitäjä on Karelia-ammattikorkeakoulu Oy. Henkilörekistereistä on laadittu rekisteri- ja tietosuojaselosteet, joihin kuka tahansa voi tutustua Karelian www-sivuilla olevan linkin kautta. Opiskelijoiden intranetissä, Pakki-portaalissa on erillinen Turvallisuus-sivu, jossa on linkit rekisteriselosteisiin sekä Karelian tietosuoja- ja tietoturvapolitiikkaan ja –ohjeisiin. (Karelia-ammattikorkeakoulu 2018.)

4.1 Tietosuojaosaamisen varmistaminen

Karelia-ammattikorkeakoulussa on laadittu tietosuojatyötä ohjaava tietosuojapolitiikka (2018), jota päivitetään tarvittaessa. Siinä määritellään perusperiaatteet, joiden avulla pyritään varmistamaan henkilötietojen lainmukainen käsittely ja tietosuojan korkea taso kaikissa ammattikorkeakoulun toiminnoissa. Tietosuojapolitiikkaa täydennetään yksikkö- ja toimintokohtaisilla käytännön työohjeistuksilla. Tietosuojapolitiikka on saatavilla Karelia-ammattikorkeakoulun henkilöstön käytössä olevassa intranetissä sekä Karelian julkisilla www-sivuilla. Henkilöstöä tiedotetaan tietosuojaan liittyvissä asioissa intranetissä ja tarvittaessa annetaan sisäisiä ohjeita ja järjestetään tietosuojakoulusta. Tietosuoja ja –turva asiat ovat myös osa uusien työntekijöiden perehdytysohjelmaa. Opiskelijoita tiedotetaan opiskelijoiden sisäisessä intranetissä, Pakissa. Tietosuoja-asioita käsitellään ammatillinen kasvu –opintojaksolla. Henkilötietoja käsitteleviä henkilöitä sitoo laissa säännelty tai muutoin erikseen sovittu ja dokumentoitu vaitiolovelvollisuus. Karelia-ammattikorkeakoulu on varautunut mahdollisten henkilötietojen tietoturvaloukkauksien varalle laatimalla toimintaprosessin, jonka mukaisesti tietoturvaloukkaustilanteissa toimitaan. Jokainen ammattikorkeakoulun henkilöstön jäsen

sekä opiskelija, on velvollinen ilmoittamaan havaitsemistaan tietosuojaan liittyvistä puutteista, uhkista tai menettelyvirheistä tietosuojavastaavalle. (Karelia-ammattikorkeakoulu 2018.)

Karelia-ammattikorkeakoulun tietosuojapolitiikka (2018) määrittää tietosuojan toteutumisen ja arvioinnin perusperiaatteet. Tietosuojan toteutumista arvioidaan ja valvotaan sekä tarvittaessa tehdään tarkastuksia osana normaalia tarkastustoimintaa. Tietoturvan toteutuminen ammattikorkeakoulussa varmennetaan vuosittaisten raporttien ja toimintakertomuksien avulla.

4.2 Henkilötietojen käsittely

Kareliassa käsitellään henkilöstön, hakijoiden ja opiskelijoiden sekä kotimaisten ja ulkomaisten yhteistyökumppanien ja muiden asiakkaiden henkilötietoja. Tietoja käytetään niiden keräysvaiheessa kuvattuihin tarkoituksiin lainsäädännön sallimissa rajoissa (Karelia-ammattikorkeakoulu 2020d). Kaikkien henkilörekisterien henkilötietojen käsittelystä on tehty kirjalliset selosteet, joiden ajantasaisuudesta vastaavat nimetyt henkilöt. Henkilötietojen käsittelyä tapahtuu kaikissa ydintoiminnoissa, mutta pääosa sitä tehdään koulutuksen ydintoiminnossa sekä hallinto- ja tukipalveluihin kuuluvissa henkilöstö- ja tietohallinnossa sekä opiskelijapalveluissa. Työntekijät käsittelevät vain sellaisia henkilötietoja, jotka ovat välttämättömiä heidän tehtäviensä hoitamiseksi. Ydintoimintojen sekä hallinto- ja tukipalvelujen esimiehet käsittelevät omien alaistensa henkilötietoja ja ylin johto kaikkien työntekijöiden tietoja omien toimintavastuidensa puitteissa. Karelian työntekijöiden ja esimiesten henkilöstöasiakirjana toimii intranetissä oleva henkilöstöasiat –sivusto, joka sisältää henkilöstöjohtamisen, työsuhdeasioiden, työhyvinvoinnin ja henkilöstön kehittämisen osiot. Kuhunkin osioon on koottu aiheeseen liittyvät työohjeet, ohjeistukset ja lomakkeet. Työssä saatujen ja käsiteltävien tietojen salassapitovelvoite on kirjattu jokaisen työntekijän kanssa allekirjoitettuun työsopimukseen.

Osaa henkilötietojen käsittelyn järjestelmistä hallinnoi ulkopuolinen palveluntuottaja suojatusta konesalipalvelustaan, esimerkiksi henkilöstöhallinnon järjestelmät. Karelian omat järjestelmät sijaitsevat erillisessä, kulkutunnistein varustetussa tilassa ja niitä hallinnoidaan Karelian tietohallinnon toimesta. Henkilötietojen käsittelyä ei ole ulkoistettu, vaan järjestelmien sisältämien erilaisten henkilöryhmien (rekisteröityjen) henkilötietoja käsittelevät Karelian nimetyt työntekijät tehtäviensä mukaisin käyttäjäoikeuksin, jotka määrillään käyttäjähallinnossa. Henkilötietojen käsittely perustuu rekisteröidyn suostumukseen tai laissa määriteltyyn muuhun perusteeseen ja tietoja käsitellään käyttötarkoituksen kannalta tarpeellisessa määrin ja ajan (Karelia-ammattikorkeakoulu 2020d). Henkilötietojen antamisen perusteena puolestaan on esimerkiksi tietojen tarve lakisääteisten tehtävien tai palvelussuhteen asioiden hoitamiseen, palvelun tuottamiseen tai toteuttamiseen tai rekisterinpitäjän etu. Kaikkien Karelian henkilörekistereiden osalta rekisteröidyn oikeudet määrittyvät käsittelyperusteen mukaan ja rekisteröidyllä on tietosuoja-asetuksen mukaiset tiedonsaantioikeudet järjestelmiin tallennettuihin omiin tietoihinsa. (Karelia-ammattikorkeakoulu 2019.)

Arkaluonteisia henkilötietoja käsitelleen useissa hallinto- ja tukipalvelujen yksiköissä. Opiskelija- ja hakijapalveluissa käsitellään opiskelijoiden ja hakijoiden SORA-lainsäädännön piiriin kuuluvia henkilötietoja sekä opiskeluoikeuteen ja läsnäoloon liittyviä hakemuksia liitteineen. Myös koulutusvastuiden opinto-ohjaajat ja koulutuspäälliköt käsittelevät SORA-lainsäädännön alaisia henkilötietoja, samoin kuin opintokuraattori, joka käsittelee lisäksi opiskelijoiden terveyteen liittyviä tietoja. Henkilöstöhallinnossa käsitellään muun muassa henkilökunnan työsuhdetietoja, terveystietoja ja henkilöstön rekrytointiin liittyviä arkaluontoisia henkilötietoja. Esimiesten käsittelemät arkaluonteiset henkilötiedot ovat esimerkiksi omien alaisten sairauspoissaolotietoja sekä kehityskeskustelujen aineistoa.

Osa joidenkin henkilöstörekisterien henkilötiedoista ovat salassa pidettäviä, jolloin tietoja käsitteleviä työntekijöitä koskee vaitiolovelvollisuus ja muut tietojen käsittelystä annetut ohjeet. Vaitiolovelvollisuus jatkuu myös palvelussuhteen päätyttyä. Paperille kirjattuja rekisteritietoja käsitellään luottamuksellisesti projektin

toimijoiden toimesta ja säilytetään tiloissa, jotka ovat lukittuna virka-ajan ulkopuolella. ESR-henkilötietojen käsittelyssä noudatetaan erikseen annettuja ohjeita. Tällöin henkilötiedot muodistavat Karelian toteuttamien projektien osallistujarekisterin.

Tietosuoja-asetus määrittää edellytykset henkilötietojen siirtämiselle Euroopan talousalueella (ETA) ja sen ulkopuolelle. Tietojen siirto on sallittua ETA-maihin, jolloin noudatetaan samoja perusteita kuin Suomen sisällä. Siirrettäessä henkilötietoja Euroopan unionin ja kolmansien maiden välillä tai kansainvälisille järjestöille on henkilötietojen käsittelyn oltava sallittua Suomessa kyseisessä tilanteessa ja henkilötietojen siirron on täytettävä tietosuoja-asetuksen luvussa V määritellyt edellytykset. Molempien edellä mainittujen edellytysten on täytyttävä, jotta henkilötietojen siirtäminen on mahdollista. (Tietosuojavaltuutetun toimisto 2020.) Kaikissa Kareliassa tapahtuvassa tietojen siirrossa käytetään asianmukaisia suojaustekniikoita. Euroopan unionin alueelta ja sen ulkopuolelta tulevien tutkinto- ja vaihto-opiskelijoiden henkilötietojen käsittely ja siirtäminen täyttävät tietosuoja-asetuksessa määritellyt edellytykset. Pääsääntöisesti Kareliassa ei siirretä henkilötietoja Euroopan unionin ulkopuolisiin maihin. (Karelia-ammattikorkeakoulu 2019.)

Asiakirjahallinto ja arkistotoimi ovat osa tietosuojan toteutumista. *Asiakirjahallinto alkaa asiakirjojen ja tietojärjestelmien suunnittelusta* ja siihen kuuluu *tiedon tuottaminen, tiedon siirto ja kopiointi, tietopalvelu, julkisuus- ja salassapitonäkökohdat, tietoturvallisuus ja hyvä tiedonhallintatapa*. Asiakirjahallinnon toimintaperiaatteet ja käytännöt on kirjattu koko henkilökuntaa koskevaan, henkilökunnan sisäisessä käytössä olevaan Karelian asiakirjahallinnon oppaaseen. Kareliassa on laadittu arkistolain mukainen arkistonmuodostussuunnitelma, jossa on hallinnonaloittain asiakirjakohtaiset rekisteröintipaikat sekä tietojen arkistointiin ja hävittämiseen liittyvät ajat ja tavat ja rekisterin vastuuhenkilö. (Karelia-ammattikorkeakoulu 2020b.)

5 Lähestymistapa ja tutkimusmenetelmät

Kaikissa yrityksissä tarvitaan kehittämistyötä esimerkiksi toiminnan tehostamiseen ja prosessien kehittämiseen tai ilmenneiden ongelmien ratkaisemiseksi. Nopeasti kehittyvä ja muuttuva toimintaympäristö sekä samalla kasvava tiedon määrä ja sen hallinta, ovat tuoneet muutostarpeita yritysten toimintoihin. Tutkimusongelma, tutkimuskysymykset ja niihin vastaaminen hyväksyttäjä menetelmiä käyttäen on olennaista tieteelliselle tutkimukselle. Tutkimuksellisessa kehittämistyössä korostuu muun muassa toiminnallisuus ja erilaiset lähtökohdat, esimerkiksi organisaation kehitystarpeet tai halu saada muutoksia. Kehittämistyössä pyritään luomaan uusia ratkaisuja ja parannuksia olemassa oleviin käytäntöihin sekä uuden tiedon tuottamista tutkittavasta ilmiöstä. (Ojasalo, Moilanen & Ritalahti 2009, 13 – 20.)

Kehittämistyön lähestymistapa liittyy keskeisesti kehittämisen tavoitteisiin. Soveliaimman lähestymistavan kehittämistyöhön määrittää kehittämistehtävä. Koska lähestymistavat ovat osittain päällekkäisiä, voi kehittämistyössä olla piirteitä useasta lähestymistavasta. Keskeisiä lähestymistapoja ovat tapaustutkimus, toimintatutkimus, konstruktiivinen tutkimus ja innovaatioiden tuottaminen. Valitulle lähestymistavalle valitaan yksi tai useampi tutkimusmenetelmä, joka voi olla laadullinen tai määrällinen menetelmä tai niiden yhdistelmä. (Ojasalo ym. 2009, 36 – 37.)

5.1 Lähestymistapa

Tapaustutkimuksen (case study) tavoitteena on tuottaa kohteesta tutkittua tietoa. Menetelmä soveltuu lähestymistavaksi kehittämistyöhön, jonka tehtävänä on ratkaista organisaatiossa ilmennyt ongelma, luoda kehittämisideoita tai ratkaisuehdotuksia tiettyyn ongelmaan. Tapausta (esim. koko yritys, henkilöstöryhmä, järjestelmä, prosessi) tutkitaan sen omassa ympäristössä. Tapaustutkimuksessa on

tyypillistä, että tapauksesta kokonaisvaltaisen kuvan saamiseksi, tutkimiseen käytetään useita erilaisia tutkimusmenetelmiä. (Ojasalo ym. 2009, 37 – 38.)

Tämä opinnäytetyö on tutkimuksellinen kehittämistyö, jonka lähestymistapana on tapaustutkimus. Kehittämistyön tehtävänä on kartoittaa tietosuojan toteutumisen nykytilanne Karelian ydinprosesseissa ja niitä tukevissa hallinto- ja tukipalveluissa sekä selvittää henkilöstön tietosuojaosaamisen taso. Lisäksi tehtävänä on tuottaa Karelian ylimmälle johdolle kehittämisehdotuksia tietosuojan toteuttamisen parantamiseksi Kareliassa. Tutkimuskohteen muodostaa edellä mainittujen tahojen toistaiseksi voimassa olevassa tai määräaikaisessa työsuhteessa oleva henkilöstö.

5.2 Tutkimusmenetelmät

Tutkimusmenetelmät jaetaan yleensä laadullisiin (kvalitatiivisiin) ja määrällisiin (kvantitatiivisiin) menetelmiin. Erilaisia menetelmiä rinnakkain käyttämällä kehittämistyön tueksi saadaan erilaista tietoa sekä monenlaisia näkemyksiä ja ideoita. Menetelmiä valittaessa on ensin selvitettävä, millaista tietoa tarvitaan ja mihin sitä käytetään. Käytettäessä rinnakkain useampia menetelmiä ne täydentävät toisiaan, jolloin saadaan varmuutta kehittämistyöhön liittyvään päätöksentekoon. (Ojasalo ym. 2009, 40.) Tuomen ja Sarajärven (2009, 71) mukaan tutkimuksellisen kehittämistyön yleisimpiä tutkimusmenetelmiä ovat haastattelu, kysely, havainnointi ja erilaisiin dokumentteihin perustuva tieto, joista seuraavassa käymme läpi haastattelun ja kyselyn.

Kysely ja haastattelu eroavat toisistaan sillä, että kyselyssä vastaajat täyttävät itse kyselylomakkeen ryhmätilanteessa tai kotona, ja haastattelussa haastattelija esittää suullisia kysymyksiä ja merkitsee vastaajan antamat tiedot muistiin. Haastattelu on joustava tapa kerätä tietoa ja siinä haastattelijalla on mahdollisuus toistaa kysymykset tai esittää täydentäviä kysymyksiä ja oikaista väärinkäsityksiä

sekä keskustella haastateltavan kanssa. Kysymykset voidaan lähettää haastateltaville etukäteen, jolloin he voivat tutustua niihin ja haastattelussa saadaan mahdollisimman paljon aineistoa. Haastattelija voi myös haastattelun ohessa tehdä havaintoja haastateltavan vastaustavasta. Haastatteluista on hyvä sopia haastateltavien kanssa etukäteen. (Tuomi ja Sarajärvi 2009, 72 – 74.)

Haastattelu on moneen tilanteeseen soveltuva perusmenetelmä, joka voidaan jaotella strukturoituihin, puolistrukturoituihin ja avoimiin haastatteluihin. Yleensä strukturoitu haastattelu on lomakehaastattelu, jossa valmiit kysymykset esitetään kaikille vastaajille samassa järjestyksessä. Haastattelumuotoa voidaan käyttää silloin, kun haastateltavana on suuri, yhtenäinen joukko. Puolistrukturoitua eli teemahaastattelua voidaan käyttää esimerkiksi silloin, kun tutkimus kohdistuu heikosti tiedostettuihin asioihin. Haastattelun keskeiset, viitekehykseen perustuvat teemat on valittu etukäteen ja ne ohjaavat haastattelua, mutta kysymyksiä ja niiden esittämisjärjestystä ei ole ennakolta tarkasti määritelty. Avoin haastattelu voi olla keskusteluomainen, vapaa haastattelu, jonka etenee haastateltavan aloitteesta. Tuomen ja Sarajärven (2019) mukaan haastattelun sisältö liittyy tutkimuksen tarkoitukseen, ongelmanasetteluun tai tutkimustehtävään. Haastattelua voidaan käyttää esimerkiksi silloin, kun henkilöiden kokemukset vaihtelevat paljon, jos käsitellään menneisyyttä tai heikosti tiedostettuja asioita. (Metsämuuronen 2008, 40 – 41, Tuomi & Sarajärvi 2009, 74 – 76.)

Lomakekysely (lomakehaastattelu) on yleensä määrällisen tutkimuksen aineistonkeruumenetelmä, joka voi olla strukturoitu (ennalta määritellyt kysymykset) tai puolistrukturoitu (kysely sisältää sekä ennalta määriteltyjä kysymyksiä että avoimia kysymyksiä). Kysymysten tulee olla tutkimuksen tarkoituksen ja ongelmanasettelun kannalta merkityksellisiä ja niiden tulee perustua tutkimuksen viitekehykseen, jo tiedettyyn tietoon tai tutkittavaan ilmiöön. (Tuomi & Sarajärvi 2009, 74 – 75.)

Kyselyn avulla voidaan kerätä laaja tutkimusaineisto kysymällä monia asioita, useilta eri henkilöiltä. Huolellisesti suunnitellulla kyselyllä saatava aineisto on helposti käsiteltävää olemassa olevilla analyysitavoilla ja raportointimuodoilla, eikä

tutkijan tarvitse miettiä uusia aineiston analysointitapoja. Kyselytutkimuksen heikkoutena on, että tutkijan ei ole mahdollista varmistua siitä, miten “tosissaan” vastaajat ovat vastauksia antaessaan olleet tai siitä, miten kyselyn vastausvaihtoehdot sopivat vastaajille. Etukäteen ei välttämättä ole tietoa siitä, kuinka perehtyneitä vastaajat ovat aihealueesta. Yhtenä haittatekijänä on myös se, että läheskään kaikki kohderyhmän jäsenet eivät välttämättä vastaa kyselyyn, jolloin voidaan miettiä, kuinka hyvin saatu aineisto vastaa koko kohdejoukon näkemyksiä. (Hirsijärvi ym. 2016, 195.)

Kyselyssä voidaan käyttää avoimia ja monivalintakysymyksiä sekä asteikkoihin perustuvia kysymyksiä. Avoimet kysymykset antavat vastaajille mahdollisuuden kertoa oman mielipiteensä, osoittavat tutkijalle vastaajien tietämyksen aiheesta sekä tuovat esille vastaajille keskeisiä asioita. Monivalintakysymyksiin vastaaminen voi olla helpompaa ja ne auttavat vastaajaa tunnistamaan asian. Annettuja vastauksia on helppo verrata ja niitä on helpompi käsitellä ja analysoida kuin avoimiin kysymyksiin annettuja vastauksia. Asteikkoihin perustuvissa kysymyksissä vastaaja valitsee sen vaihtoehdon, joka tuo parhaiten esille hänen mielipiteensä esitettyyn väittämään. (Hirsijärvi ym. 2016, 198 – 201.)

Tämän tutkimustyön tutkimusmenetelminä on käytetty Karelian henkilöstölle lähetettyä kvantitatiivista, puolistrukturoitua kyselylomaketta (liite 2) sekä Karelian tietosuojavastaavalle tehtyä kvalitatiivista henkilöhaastattelua (kyselyrunko liitteenä 3). Kyselylomake sisälsi ennalta määriteltyjä, kaikilta vastaajilta samalla tavoin kysyttyjä monivalintakysymyksiä, avoimia kysymyksiä, sekä asteikkoon perustuvia väittämiä. Kyselyn kohdejoukkona oli Karelian henkilökunta (n=267) pois lukien ylin johto. Henkilöt toimivat erilaisissa koulutus-, TKI-, palveluliiketoiminnan sekä hallinto- ja tukipalvelujen tehtävissä. Tietosuojavastaavan henkilöhaastattelu tehtiin face-to-face –haastatteluna. Haastattelurunko koostui kuuteen eri teemaan sisältyvistä, ennakkoon tutustuttavaksi lähetetyistä kysymyksistä

6 Tutkimusaineiston analysointi ja kehitysehdotukset

Henkilöstökysely toteutettiin Microsoft Forms:lla tehdyllä sähköisellä kyselylomakkeella. Kysely jakautui kolmeen pääteemaan; vastaajien taustatietoihin, henkilötietojen käsittelyyn ja tietosuojan toteuttamiseen Kareliassa. Kyselylomakkeen kysymysten laadinnassa on huomioitu sekä opinnäytetyönohjaajan että toimeksiantajapuolen ohjaajan kommentit. Viisi henkilöä testasi lomakkeen ennen sen lähettämistä henkilökunnalle. Kohderyhmän työntekijöille lähettiin sähköpostitse linkki kyselyyn, johon he vastasivat anonyymina. Vastausaikaa annettiin aluksi yksi viikko, mutta vastausajan päätyttyä aikaa jatkettiin viikolla, jotta saataisiin kattavampi vastausprosentti. Kyselyn tavoitteena oli saada tietoa ydinprosesseissa sekä hallinto- ja tukipalveluissa käsiteltävistä henkilötiedoista, niiden säilyttämisestä ja hävittämisestä, sekä työntekijöiden osaamisesta henkilötietojen käsittelyyn liittyvistä tietosuojamenetelmistä ja siitä, miten he kokevat saaneensa koulutusta ja ohjeistusta henkilötietojen käsittelyyn.

Kyselylomakkeen kysymykset oli jaettu eri teemoihin, joten oli johdonmukaista käyttää analyysimenetelmänä teemoittelua. Saatu aineisto pilkottiin ja järjestettiin tutkimusongelmaa kuvaaviin teemoihin alleviivaamalla vastauksista eri värein eri teemoihin liittyvät sanat ja lauseet, jonka jälkeen ne sijoitettiin värien mukaisesti eri teemoihin. Tiedot esitetään prosenttiosuuksilla tietyistä kokonaisuuksia ja kuvataan kuvioissa eri värein.

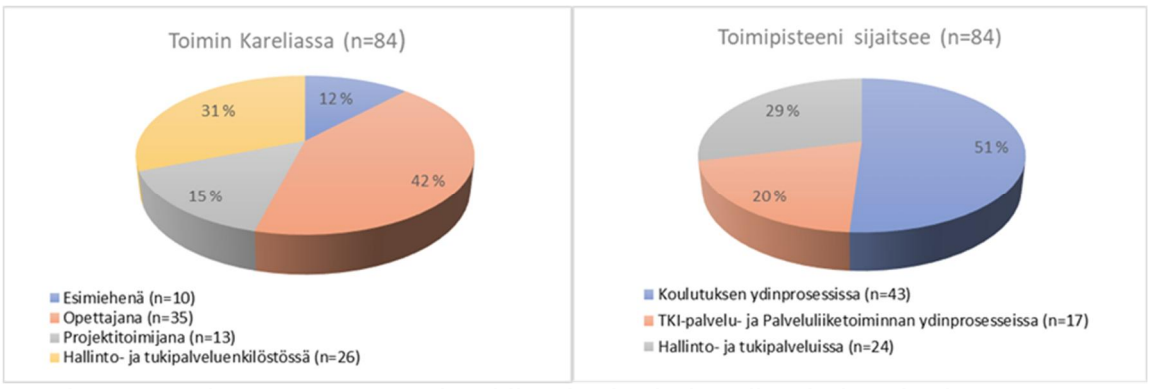
Henkilöstökyselyn lisäksi haastateltiin tietosuojeluvastaavaa. Haastattelu toteutettiin henkilöhaastatteluna, haastateltavalle ennakkoon lähetettyjen kysymysten mukaisesti. Haastattelun kysymykset sisältyivät kuuteen eri teemaan. Haastattelun tarkoituksena oli saada pohjatietoa Kareliassa toteutetusta tietosuojatyöstä ja rekisterinpitäjän velvollisuuksien toteuttamisesta sekä tietosuojavastaavan asemasta ja tehtävistä.

6.1 Henkilöstön tietosuojakysely

Henkilöstön tietosuojakyselyssä oli kolme pääteemaa, joihin kysymykset jakautuivat; vastaajien taustatiedot (kysymykset 1-3), henkilöstötietojen käsittely (kysymykset 4-11) ja tietosuojan toteuttaminen (kysymykset (12 - 18). Kysymyksistä kolme oli avoimia kysymyksiä. Kyselyn vastauksista on pääteltävissä, että kysyttäessä henkilötietojen käsittelyssä käytettävästä järjestelmästä yksittäiset vastaajat käsittivät virheellisesti kysymyksen sisältävän myös vastaajan omien henkilötietojen käsittelyn (esimerkiksi ESS-, Reportronic- ja SYMPA-järjestelmien käyttö).

6.1.1 Taustatiedot

Henkilöstökysely lähetettiin 267:lle Karelian työntekijälle, joista kyselyyn vastasi 84 henkilöä (31,5 %). Kaikista vastanneista esimiesten osuus oli 12 %, opettajien osuus 42 %, projektitoimijoiden osuus 15 % ja hallinto- ja tukipalvelujen henkilöstön osuus 31 %. Vastanneista 51 % toimi Koulutuksen ydinprosessissa, joka on 26 % kyseisen ydintoiminnon koko henkilöstön määrästä (n=168). TKI-palvelujen ja Palveluliiketoiminnan ydintoiminnoista vastanneiden osuus oli 20 % joka on 43 % kyseisten ydintoimintojen henkilöstön määrästä (n=40). Hallinto- ja tukipalveluista vastanneiden osuus oli 29 %, joka on 40 % palvelujen koko henkilöstön määrästä (n=60). Kyselyyn vastanneiden osuus henkilöryhmittäin ja ydinprosesseittain on esitetty kuviossa 4.

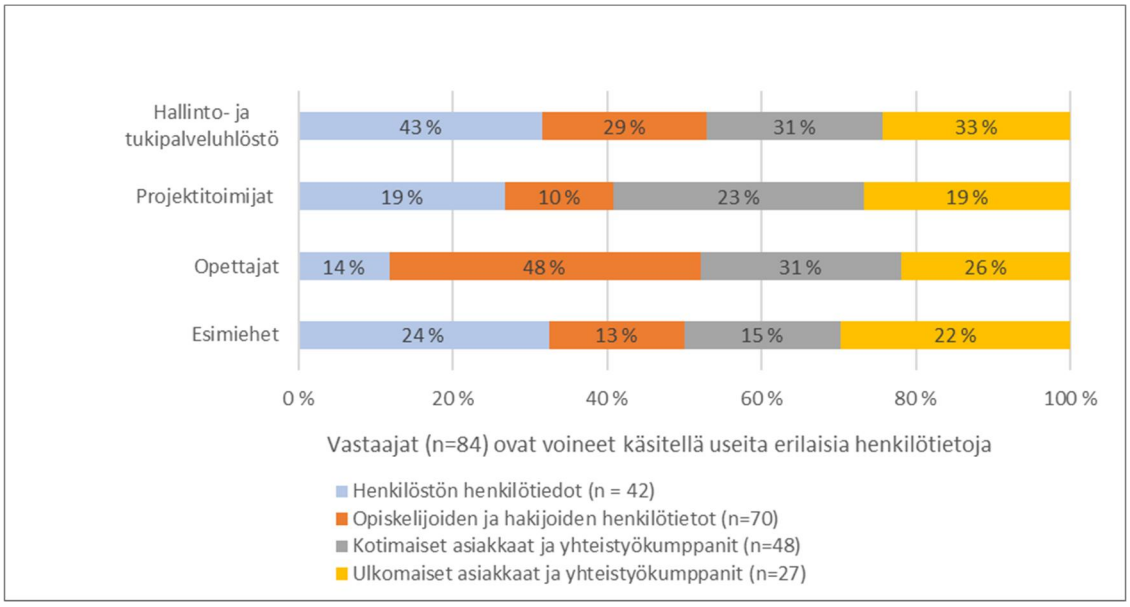


Kuvio 4. Kyselyyn vastanneet henkilöryhmittäin ja ydintoiminnoittain.

Kuviossa 4 TKI-palveluiden että Palveluliiketoiminnan ydintoimintoja on käsitelty yhdessä, koska Palveluliiketoiminnassa työskentelee kaksi henkilöä, ja vastaukset olisi voinut yhdistää tiettyyn henkilöön.

6.1.2 Henkilötietojen käsittely

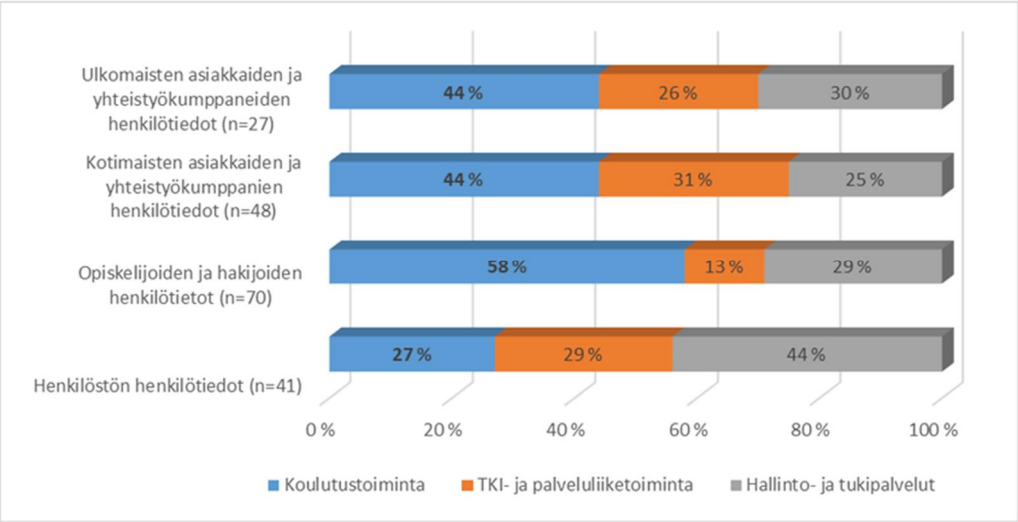
Kareliassa käsitellään henkilökunnan, opiskelijoiden ja hakijoiden sekä muiden kotimaisten ja ulkomaisten asiakkaiden ja yhteistyökumppaneiden henkilötietoja. Vastaajista 50 % ilmoitti käsittelevänsä henkilökunnan henkilötietoja, opiskelijoiden ja hakijoiden henkilötietoja 83 %, kotimaisten asiakkaiden ja yhteistyökumppaneiden henkilötietoja 57 % ja ulkomaisten asiakkaiden ja yhteistyökumppaneiden henkilötietoja 32 %. Vastausten perusteella useat ydintoimintojen työntekijät käsittelevät erilaisten henkilöryhmien tietoja. Vastauksissa kiinnitti huomiota, että myös opettajat ilmoittivat käsittelevänsä henkilöstön henkilötietoja. Tämä selittynee sillä, että vastaajat ovat sisällyttäneet henkilöstön henkilötietojen käsittelyyn omien tietojensa käsittelyn, esimerkiksi omien poissaolojen merkintä ESS-järjestelmään tai kehityskeskustelutietojen tallentaminen Sympaan. Sama ilmiö esiintyy kysyttäessä henkilötietojen käsittelyssä käytettäviä järjestelmiä (kuvio 7). Henkilötietojen käsittelyä eri henkilöstöryhmissä on kuvattu kuviossa 5.



Kuvio 5. Henkilötietojen käsittely henkilöryhmittäin.

Saatujen vastausten perusteella henkilökunnan henkilötietojen käsittely jakautuu melko tasaisesti eri ydinprosesseissa sekä hallinto- ja tukipalveluissa. Sen sijaan hakijoiden ja opiskelijoiden henkilötietoja käsitellään eniten koulutuksen ydinprosessissa. Tämä selittyy sillä, että opettajat tallentavat arvosanat opiskelijoille. Opettajista useat toimivat myös harjoittelu- ja opinnäytetyön sekä projektiopintoihin liittyvien toimeksiantojen ohjaajina. Vastausten perusteella myös koti- ja ulkomaisten asiakkaiden ja yhteistyökumppaneiden henkilötietoja käsitellään eniten koulutuksen ydinprosessissa. Opettajat käyttävät koti- ja ulkomaisten kumppanikorkeakoulujen henkilöstön tietoja sekä käsittelevät harjoittelujen ja opinnäytetöiden toimeksiantajien ja projektiopintoihin liittyvien yritysten yhteyshenkilöiden yhteystietoja. Eri henkilöryhmien henkilötietojen käsittelyä ydintoiminnoissa sekä hallinto- ja tukipalveluissa on kuvattu kuviossa 6.

Kaikkien henkilöryhmien henkilötiedoista käsiteltiin eniten nimi- ja yhteystietoja. Henkilöstöhallinnon tapahtuva henkilötietojen käsittely sisältää myös henkilöstön työsuhde-, työajanseuranta- ja kehityskeskustelutietoja. Opiskelija- ja hakijapalveluissa käsitellään kotimaisten ja ulkomaisten hakijoiden ja opiskelijoiden henkilötietoja, jotka sisältävät yhteystietoja, opiskelijanumeron, syntymäajan, henkilötunnuksen ja arviointeja. Taloushallinnossa tapahtuva henkilötietojen käsittely sisältää oman henkilöstön matkustus sekä ulko- ja kotimaisten asiakkaiden ja yhteistyökumppaneiden matkustustietoja.

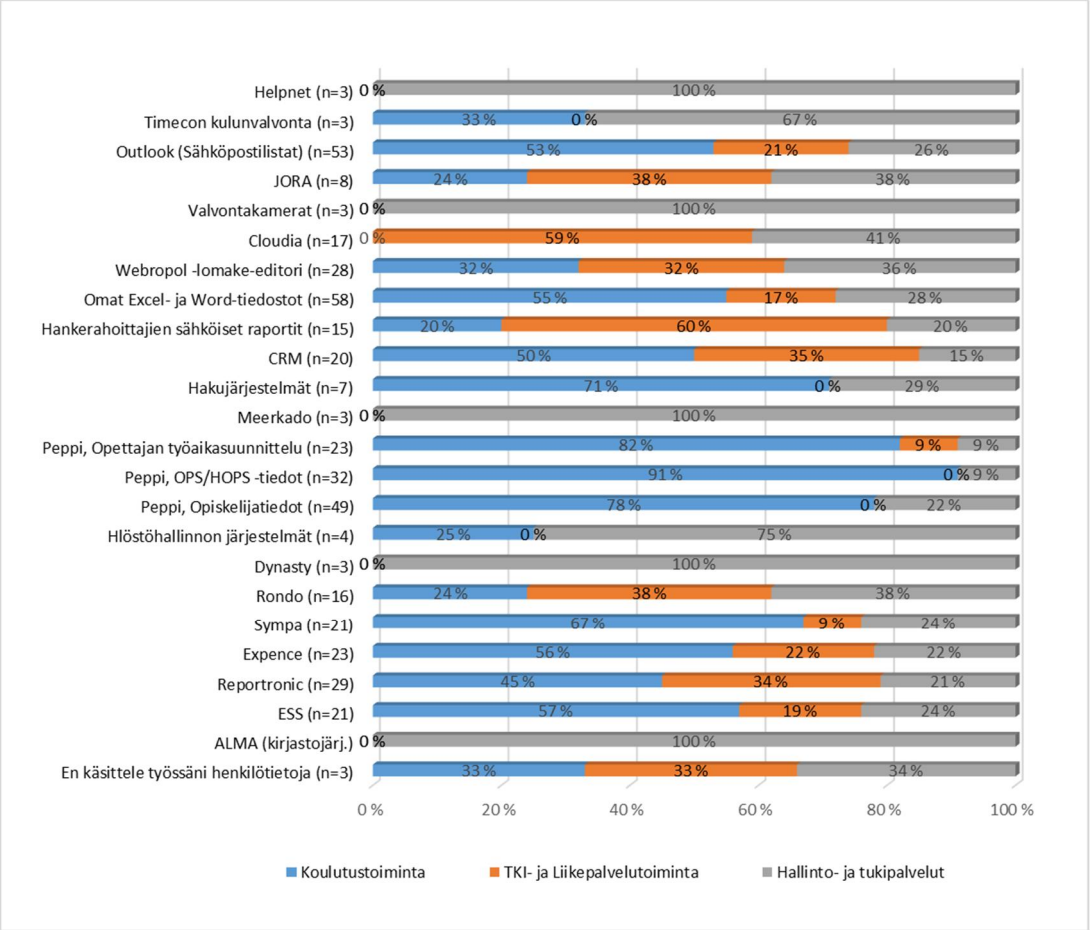


Kuvio 6. Henkilötietojen käsittely toiminnoittain.

Koulutustoiminnan käytetyimmät järjestelmät ovat Peppi-järjestelmän eri osiot, Reportronic -työajanseuranta ja projektihallinnan seurantajärjestelmä, Webropol-lomake-editori ja hankerahoittajien sähköiset raportit, jonka runsas käyttö selittyy sillä, että osa opettajista toimii myös projekteissa. Useat koulutustoiminnan opettajat ilmoittivat käyttävänsä henkilöstöhallinnon järjestelmiä. Heillä ei kuitenkaan ole oikeuksia käsitellä muiden henkilöiden henkilötietoja, joten kyse on todennäköisesti omien tietojen käsittelystä. TKI ja palveluliiketoiminnoissa käytettiin eniten hankerahoittajien sähköisiä raportteja, CRM-, Reportronic-, Rondo- ja Cloudia –järjestelmiä. Hallinto- ja tukipalvelut jakautuvat useisiin eri toimintoihin, joten siellä henkilötietoja käsitellään useissa, eri toimintoihin liittyvissä järjestelmissä. Käytetyimmät olivat ESS, Reportronic, Rondo, Sympa ja Peppi-järjestelmät. Eri järjestelmien käyttäjämääristä on nähtävissä järjestelmien käyttörajoitukset; esimerkiksi kirjaston ALMA-järjestelmä ja tietohallinnon järjestelmät (Timecon, Valvontakamerat ja Helpnet) ovat vain yksittäisten henkilöiden käytössä.

Vastanneista 69 % käyttää henkilötietojen käsittelyssä omia Excel-ja Word –listoja ja 63 % ilmoitti käyttävänsä henkilötietojen käsittelyssä Outlook-sähköpostilistoja. On kuitenkin todennäköistä, että vastanneet lähettävät sähköpostitse viestejä postituslistojen kautta – joka ei ole henkilötietojen käsittelyä. Virheellinen tulkinta vastattaessa johtuu kysymyksen epäselvästä asettelusta. Henkilötietojen käsittelyssä käytettäviä järjestelmiä ydintoiminnoittain on kuvattu kuviossa 7.

Vastaajat saivat työssään käsittelemänsä henkilötiedot tietojärjestelmistä (55 %), henkilöltä itseltään (33 %), yhteyshenkilöltä (7 %) tai muualta (5 %). Avoimissa vastauksissa ilmeni, että muilla lähteillä tarkoitettiin esimerkiksi yritysten tai oppilaitosten www-sivustoja. Sivustoilla käytettiin nimi- ja yhteystietojen hakupalveluita.

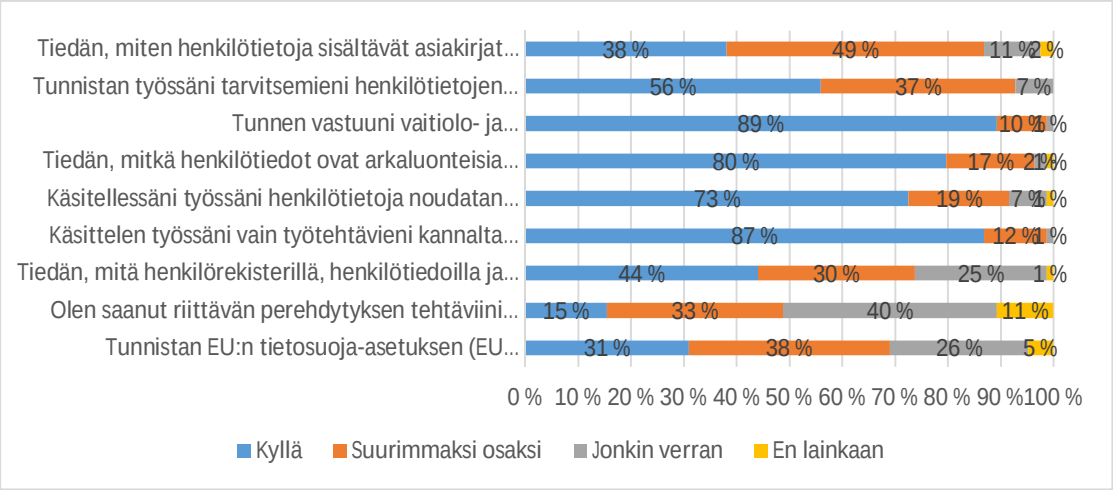


Kuvio 7. Henkilötietojen käsittelyssä käytetyt järjestelmät.

Kyselyssä kartoitettiin henkilöstön käsitystä henkilötietojen käsittelyyn liittyvistä käytänteistä väittämien avulla. Vastaajia pyydettiin arvioimaan esitettyjä väittämiä asteikolla kyllä-suurimmaksi osaksi-jonkin verran-ei lainkaan. Tämän osion tulosten analysoinnissa on yhdistetty kyllä ja suurimmaksi osaksi vastaukset, ellei toisin mainita.

Rekisterinpitäjän tulee varmistaa tietosuoja-asetuksen sisäänrakennetun ja oletusarvoisen tietosuojaperiaatteen toteutuminen. Työtehtävien kannalta käsitellään vain välttämättömiä henkilötietoja. Kuviossa 8 on esitetty vastauksien jakautumista. Voidaan todeta, että henkilöstö on hyvin tietoinen henkilötietojen käsittelyyn liittyvistä seikoista. Kyselyn vastaajista 69 % vastaajista tunnistaa EU:n tietosuoja-asetuksen vaikutuksen työhön liittyvissä henkilötietojenkäsitte-

lyssä. Lähes puolet vastaajista (48%) kokee, että on saanut riittävän perehdytyksen työtehtäviin kuuluvien henkilötietojen käsittelyn suhteen. Vastaajista 74 % ilmoittaa tietävänsä mitä henkilörekisterillä, henkilötiedoilla ja niiden käsittelyllä tarkoitetaan. Vastaajista 87 % ilmoitti käsittelevänsä ainoastaan työtehtävien kannalta välttämättömiä henkilötietoja ja 99 % vastaajista ilmoitti käsittelevänsä ainoastaan tai suurimmaksi osin työtehtävien kannalta välttämättömiä henkilötietoja. Kyselyn vastausten mukaan vastaajat noudattavaa henkilötietojenkäsittelyä koskevaa lainsäädäntöä ja tunnistavat hyvin arkaluontoiset henkilötiedot ja noudattavat niiden käsittelyssä erityistä huolellisuutta. Henkilötietojen käsittelyyn ja henkilörekistereihin liittyvät vaitiolo- ja salassapitovelvollisuudet ovat hyvin vastaajien tiedossa. Vastaajat ovat tietoisia henkilötietojen käsittelyyn liittyvistä tietosuojariskeistä (93 %) sekä henkilötietoja sisältävien asiakirjojen säilyttämiseen ja tuhoamiseen liittyvistä seikoista (87%).



Kuvio 8. Henkilötietojen käsittely.

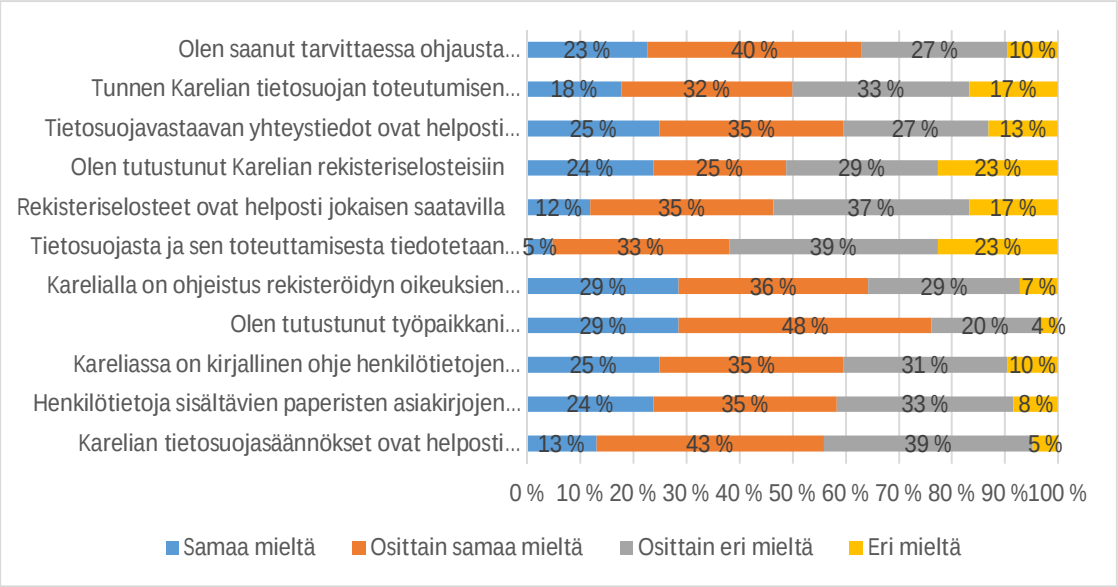
Vastaajilla oli mahdollisuus kirjata ylös havaintojaan ja kehittämisehdotuksia henkilötietojen käsittelyn suhteen. Avoimia vastauksia antoi 33 vastaajaa. Niissä nousi selkeästi esille tarve tiedottamisen kehittämiseen. Vastaajat toivoivat enemmän koulutusta ja tarkempaa ohjeistusta henkilötietojen käsittelyn suhteen. Opettajien vastausten osalta esille nousivat opiskelijoiden hakemusten (esimerkiksi erityinen tuki tai jatkoaika) sekä opinnäytetöihin ja harjoitteluun liittyvien sopimusten sähköistäminen.

6.1.3 Tietosuojan toteuttaminen

Vastaajat ovat saaneet tietoa Karelian tietosuojaan liittyvistä asioista pääasiassa koulutustilaisuuksista (57%), intranetistä (40%) sekä työtovereilta (39%). Tietoa on saatu myös henkilöstön sähköisestä uutiskirjeestä. Kahdeksan prosenttia vastaajista ilmoitti, ettei ole saanut lainkaan tietoa tietosuoja-asioista. Osa vastaajista ilmoitti hakeneensa tietoa myös itsenäisesti.

Kyselyssä kartoitettiin henkilöstön mielipiteitä Karelian tietosuojaohjeistuksiin liittyen. Vastaajia pyydettiin arvioimaan esitettyjä väittämiä asteikolla samaa mieltä-osittain samaa mieltä-osittain eri mieltä-eri mieltä. Tämän osion tulosten analysoinnissa on yhdistetty vaihtoehdot samaa mieltä ja osittain samaan mieltä, ellei toisin mainita. Vastaukset on esitetty kuviossa 9.

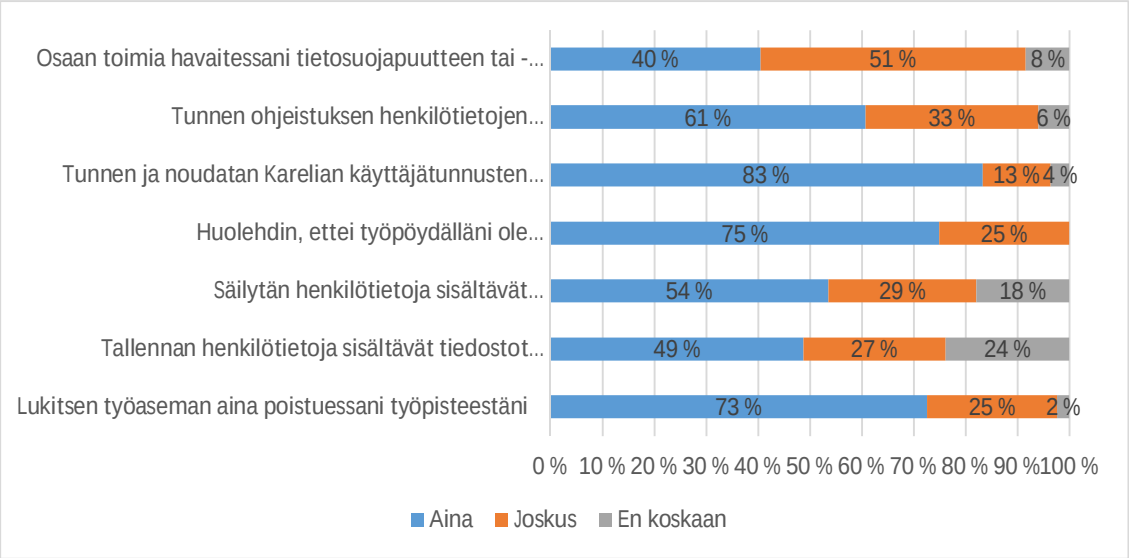
Vastaajista 77 % on tutustunut Karelian tietosuojasäännöksiin ja on tietoinen siitä, mitä tietosuojalla tarkoitetaan. Kuitenkin vain noin puolet vastaajista (56%) oli sitä mieltä, että Karelian tietosuojasäännökset ovat helposti saatavilla. 59 prosenttia vastaajista oli tietoisia Karelian henkilötietoja sisältävien asiakirjojen käsittelyyn ja säilytykseen liittyvästä ohjeistuksesta sekä sähköpostitse lähetettävien henkilötietojen ohjeistuksesta (60%). Vastaajista 65 prosenttia on tietoisia ohjeistuksesta rekisteröidyn oikeuksien toteutumiseen Kareliassa. Tietosuojavastaavan yhteystiedot ovat vastaajista lähes 60 prosentin mielestä helposti löydettävissä. 63 prosenttia vastaajista oli saanut tarvittaessa ohjausta tietosuoja-asioihin liittyvissä asioissa.



Kuvio 9. Karelian tietosuojaohjeistukset.

Kuvion 9 mukaan, vastaajista 62 prosenttia koki, ettei Karelian tietosuojasta ja sen toteutumisesta tiedoteta henkilökuntaa riittävästi. Rekisteriselosteet eivät ole helposti saatavilla (54%) ja niihin ei ole tutustuttu (52%). Vastaukset jakautuivat tasan kysyttäessä Karelian vastuita tietosuojatyön organisoinnin ja vastuiden suhteen. Vastauksista voidaan todeta, että tiedottamista tulee kehittää ja lisätä.

Kyselyssä kartoitettiin henkilöstön käsityksiä tietosuojakäytäntöihin liittyen. Vastaajia pyydettiin arvioimaan esitettyjä väittämiä asteikolla aina-joskus-ei koskaan. Kuvion 10 mukaan, tietosuojakäytännöt ovat toteutuneet suhteellisen hyvin henkilöstön arjessa. Lähes jokaisen väittämän kohdalla yli puolet vastaajista vastasi ”aina” kunkin väittämän kohdalla. On kuitenkin syytä kiinnittää huomiota mihin henkilötietoja sisältäviä dokumentteja tallennetaan sekä ohjeistaa henkilökuntaa tarkemmin toimenpiteistä, jotka tulee toteuttaa, jos havaitsee mahdollisien tietosuojapuutteen tai –loukkauksen.



Kuvio 10. Tietosuojakäytännöt.

Vastaajilla oli mahdollisuus selventää vastauksiaan antamalla avointa palautetta. Vastauksia saatiin 24. Niissä käy ilmi tarve koulutukselle ja perehdyttämiselle tietosuojakäytänteisiin liittyen. Vastaajat kommentoivat väittämää ”Tallennan henkilötietoja sisältävät tiedostot suojattuun ja varmuuskopioitavaan verkkopalveluun”. Vastaajat eivät olleet ymmärtäneet kysymystä, joten kysymyksen asettelu ei ollut siltä osin onnistunut. Palautteissa toivottiin, että kysymysryhmässä olisi ollut en tiedä –vastausvaihtoehtoa.

Kyselyssä pyydettiin arvioimaan omaa tietosuojaosaamista asteikon ollessa 5 = erinomainen – 1 = heikko. Vastaajien oma arvio omasta tietosuojaosaamisen tasosta on 3. Esimiesten arvio omasta tietosuojaosaamisen tasosta on 3.

Avoimessa kysymyksessä 18 kysyttiin vastanneiden ajatuksia ja kehittämisehdotuksia Karelian tietosuoja-asioissa ja niiden toteuttamisessa. Kysymykseen vastasi 27 henkilöä. Vastaukset liittyivät sekä henkilötietojenkäsittelyyn että tietosuojan toteuttamiseen. Useimmat vastaajat toivoivat henkilötietojen käsittelystä ja tietosuojasta aika ajoin järjestettäviä infotilaisuuksia, tiedotusta ja tietoiskuja henkilöstön uutiskirjeessä ja kampuskokouksissa, sekä eri tarpeisiin ja eri käyttäjäryhmille suunnattua koulutusta. Toivottiin myös, että kaikki henkilötietojenkäsittelyyn ja tietosuojaan liittyvät ajantasaiset ohjeistukset olisivat samassa paikassa

intrassa, ja kaivattiin tiivistä yhteenvetoa keskeisistä asioista. Vastauksissa todettiin myös, että tietosuoja-asetus ei sinänsä lisää tietosuojaa, vaan avainasemassa ovat henkilötietoja käsittelevät henkilöt tietojen käyttötapoineen. Vaikeaselkoisen GDPR-asetuksen ja ohjeiden katsottiin jäävän ”dokumentiksi” toisten joukkoon, jolloin asetuksen alkuperäinen tarkoitus ei toteudu. Muutama vastaaja totesi, ettei ollut työsuhteen alussa saanut tarvittavaa perehdytystä henkilötietojen käsittelyyn ja tietosuojaan liittyvissä asioissa. Esille tuli myös, ettei tietosuojaan liittyviä asioita laiminlyödä tarkoituksella, vaan tietämättömyydestä ja kaivattiin perehdytystä asioissa oman työyhteisön esimieheltä.

Esimerkkejä saaduista vastauksista:

> Ohjeistuksia tulisi organisoida ja järjestellä paremmin. Ohjeet tulisi myös kirjoittaa käyttäjän näkökulmasta lyhyemmäksi ja ymmärrettävästi niin, että ohjetta olisi helppo noudattaa.
>
> Asiakirjojen käsittelemisen, lähettämisen ja säilyttämisen osalta tulisi järjestää koulutusta ja kertoa Karelia-ammattikorkeakoulun toimintaperiaatteista ja käytännöistä.
>
> ---tietosuoja-asetus ei lisää varsinaista tietosuojaa juuri lainkaan. Ihmiset ja käyttäjät käyttötapoineen ovat avainasemassa todellisessa tietosuojassa.---
>
> Henkilöstötietojen käsittelyä olisi hyvä kerrata (lyhyesti) vuosittain, esim. kampuskokousten yhteydessä.---

6.2 Tietosuojavastaavan haastattelu

Henkilöstölle tehdyn tietosuojakyselyn lisäksi haastateltiin Karelian tietosuojavastaavaa lisätiedon saamiseksi Karelian tietosuojatyön ja sen organisoinnin toteuttamisesta, tutkimuksen tekijöiden oman käsityksen ja saatavilla olevan tiedon tueksi. Haastattelun kysymykset jakautuivat seuraaviin teemoihin: kuvaukset henkilötietojen käsittelyn vaiheista, henkilötietojen käsittelyn selosteet ja ohjeet, henkilötietoihin liittyvä riskienhallinta, käytönvalvonnan hallinta sekä tietosuojatoiminnan arviointi, raportointi ja kehittäminen. Haastattelussa esille tulleet asiat ovat pääosin samoja, jotka on jo esitetty luvussa 5. ”Tietosuojan organisointi ja henkilötietojen käsittely Kareliassa” ja henkilöstölle tehdyssä tietosuojakyselyssä.

Näin ollen tässä tuodaan esille haastattelusta vain ne asiat, jotka tuovat lisätietoa jo aiemmin esitettyihin seikkoihin.

Haastattelussa tuli esille, että Karelian tietojärjestelmissä tapahtuvasta henkilötietojen käsittelystä laadittuja kirjallisia selosteita (entinen rekisteriseloste) päivitetään tarvittaessa ja niiden ajantasaisuudesta vastaa kunkin rekisterin nimetty vastuuhenkilö. Tietosuojavastaava tarkistaa kaikki selosteet vähintään kerran vuodessa. Yksiköiden esimiehet ovat tärkeässä roolissa tietosuojan toteuttamisesta omassa työyksikössään. He antavat työvälineet sekä työ- ja toimintaohjeita, ja varmistavat niiden ajantasaisuuden.

Ennen tietosuoja-asetuksen soveltamisen voimaantuloa on henkilöstölle järjestetty useita tietosuojakoulutuksia. Lisäksi tietosuojavastaava on eri tilaisuuksissa antanut työyksiköiden henkilöstölle ohjeita henkilötietojen käsittelystä, esimerkiksi kuvauksien laadinta yksiköissä tapahtuvasta henkilötietojen käsittelystä. Kuvausten avulla voidaan tarvittaessa osoittaa työyksiköissä tapahtuvien henkilötietojen käsittelyn kulku. Kukin henkilötietoja käsittelevä henkilö on vastuussa kuvauksien tekemisestä omassa työssään käsittelemien henkilötietojen osalta. Tietosuojavastaavan mukaan kuvaukset tulisi päivittää työyksikön työohjeita muutettaessa, toteutettaessa tehtävämuutoksia koskevia järjestelyitä ja järjestelmien vaihtuessa, mutta hän toteaa, ettei kuvausten tekemistä ole järjestelmällisesti varmistettu. Kuvaukset tullaankin huomioimaan tarkemmin tiedonhallintamallissa, jonka laatimisesta rekisterinpitäjää velvoittaa Laki julkisen hallinnon tiedonhallinnasta (906/2019).

Henkilötietoja käsittävien asiakirjojen tuhoamiseen on kampuksilla paperisilppureita ja useita lukittuja tietosuoja-astioita, jotka ulkopuolinen toimija tyhjentää tilauksesta. Käytetyt laitteet hävitetään suojatusti paikallisen toimijan kautta. Jos laite otetaan uudelleen käyttöön, sen tiedot puhdistetaan ensin Blanco-dataa käyttäen.

Tietosuojavastaava totesi haastattelussa, että opiskelijoilla voi olla henkilötietojen käsittelyssä kaksi roolia; rekisteröity (hakijana ja opiskelijana) ja rekisterinpitäjä.

Opiskelija toimii rekisteripitäjänä silloin, jos hän tekee tutkimusta, jossa käsittelee henkilötietoja, esimerkiksi tekee opiskelijoille opinnäytetyöhön liittyvän kyselyn, jossa kerää opiskelijaan itseensä tai hänen opintoihinsa liittyviä tietoja. Ensimmäisen kerran opiskelijaksi hakevia henkilöitä ohjeistetaan henkilötietojen käsittelystä ja rekisteröidyn oikeuksista Opintopolku.fi -palvelussa. Kaikki Karelian uudet opiskelijat on velvoitettu ennen opintojen aloittamista suorittamaan Kareliastartti -itseopiskelupaketin, jonka kautta he perehtyvät Karelian digitaalisiin ympäristöihin ja palveluihin. Itseopiskelupaketin yhtenä osana on Tietosuojaan ja -turvaan liittyvä osio. Opiskelijoille tietosuoja-asioista tiedotetaan opiskelijoiden sähköisessä uutiskirjeessä ja sähköpostitse sekä opiskelijoiden Pakki-portaalissa, jossa on muun muassa ohjeet tietosuojailmoitusten tekemiseen, selosteisiin henkilötietojen käsittelystä ja opinnäytetöihin liittyviin, henkilötietoja käsitteleviin tutkimuksiin.

Riskienhallinta käsittää tietoturvaan liittyvän riskienhallinnan; tietojärjestelmät (palomuurit, lokitiedot, käyttäjätunnukset, oikeudet) ja fyysisen turvallisuuden (tilojen kulunvalvonta, työhuoneiden lukitseminen, näyttöjen lukitseminen) sekä henkilötietojen käsittelyyn liittyvän riskienhallinnan. Tietosuojavastaava totesi haastattelussa, että riskienhallinta liittyy olennaisesti uusien järjestelmien käyttöön ottoon ja uusien työntekijöiden perehdyttämiseen. Myös uusia henkilötietoja käsiteltäessä arvioidaan, mitä riskejä niiden käsittelyyn liittyy ja miten riskejä voidaan välttää.

Haastateltava toi esille myös, että Karelia osallistui TAISTO-18 harjoitukseen, johon Suomen julkisen hallinnon organisaatioita oli pyydetty osallistumaan. Harjoittelu auttoi organisaatioita löytämään kriittisiä tietosuojan kehitystarpeita ja tarttumaan niihin jo ennen kuin tosi on kyseessä. Tietosuojavastaava mukaan Karelian osalta harjoitus sujui varsin hyvin, eikä harjoituksessa tullut esille kriittisiä kehitystarpeita. Tietosuojavaltuutetun toimisto on julkaissut tulkintaohjeita, millaisissa tilanteissa tulee toimia ja miten toimitaan.

Tietosuojavastaavan mukaan Karelian käytönvalvonnan hallinnassa ei ole varsinaista lokipolitiikkaa, mutta tiettyjä asioita seurataan omien ja ulkopuolisten asiantuntijoiden toimesta. Tietoturvaa valvotaan itse, mm. pääkäyttäjä seuraa lokien täyttymistä. Tietosuojavastaava valvoo järjestelmien tietoturvan ja -suojan toteutumista. Seuraamalla lokikirjaa hän saa tietoa esimerkiksi epäilyttävistä järjestelmissä tapahtuvista tietoturva- ja tietosuojaan liittyvistä toimista. Vakavimpiin tapauksiin ottaa kantaa tietoturva- ja tietosuojaryhmä. Kun tietojärjestelmät on ulkoistettu ulkopuolisten yhteistyökumppaneiden palvelimille, niistä on tehty erilliset sopimukset. Näiden järjestelmien lokeihin pääsy tulee aina pyytää kyseiseltä yhteistyökumppanilta.

Karelia on suhteellisen pieni koulutusorganisaatio, eikä sille ole tehty tietotilinpäätöstä, jota tietosuoja-asetuskaan ei velvoita tekemään. Tietosuojavastaava raportoi tietosuoja-asioista ylimmälle johdolle tarvittaessa, mutta kuitenkin vähintään kerran vuodessa. Kareliassa ei ole laadittu koko organisaatiota koskevaa omavalvontasuunnitelmaa, jonka mukaisilla toimenpiteillä valvottaisiin toimintayksiköitä, henkilökunnan toimintaa ja organisaation tuottamia palveluita. Kyseinen suunnitelma on kuitenkin tehty esimerkiksi Sosiaali- ja terveysalan koulutuksen Voimala oppimis- ja palveluympäristössä, jossa kehitetään uusia tapoja tukea hyvinvointia ja terveyttä moniammatillisesti ja –alaisesti (Karelia 2020c). Tietosuojavastaava toteaakin, että Sosiaali- ja terveysalalla on sen säädellyn luonteen takia henkilötietojen käsittely ja tietosuoja-asiat olleet kunnossa ja valvottuja jo ennen tietosuoja-asetuksen voimaantuloa, kuten on myös Henkilöstöhallinnon sekä Opiskelija- ja hakijapalvelujen toiminnassa

6.3 Kehitysehdotukset

Tietosuoja-asetuksen mukaan rekisterinpitäjän tulee käydä läpi antamansa ohjeistus henkilötietojen käsittelystä sekä varmistaa tietoteknisin toimenpitein, että henkilötietoja käsitellään sisäänrakennetun ja oletusarvoisen tietosuojaperiaatteiden mukaisesti. Tutkimuksessa saatujen vastausten perusteella on todettava, että Kareliassa tulisi varmistaa riittävä perehdytys henkilötietoja käsitteleville

työntekijöille, jotta jokainen työyhteisön jäsen on tietoinen oikeista toimenpiteistä omien työtehtäviensä osalta. Esimerkiksi henkilöstölle tehdyssä kyselyssä nousi esille, että suurin osa henkilöstöstä käyttää henkilötietojen käsittelyssä omia word- ja excel-tiedostoja. Näiden tietojen käsittelyyn, säilyttämiseen ja hävittämiseen olisi syytä laatia ohjeistukset, kuten myös siitä, milloin työntekijän tulee rekisterinpitäjänä tehdä henkilötietojen käsittelystään tietosuojaseloste.

Vastuuhenkilöt tulisi velvoittaa käymään läpi intrassa olevat henkilötietojenkäsittelyyn, tietoturvaan ja tietosuojaan liittyvät ohjeet ja päivittävät ne ajantasaisiksi, esimerkiksi viittaukset lainsäädäntöön. Ohjeita tulisi päivittää vähintään kerran vuodessa tai tarvittaessa ja ne tulisi olla yhdessä paikassa ja helposti saatavilla, esimerkiksi linkki ohjeisiin henkilökunnan intran etusivulle. Tutkimuksen mukaan Karelian jokaisessa ydintoiminnossa sekä hallinto- ja tukipalveluissa käsitellään eri käyttötarkoituksiin liittyviä henkilötietoja. Saatujen vastausten perusteella osa henkilökunnasta tuntee, ettei ole saanut riittävää opastusta työhönsä kuuluvaan henkilötietojen käsittelyyn tai he eivät tiedä, mistä ohjeet löytyvät. Vastauksissa nousi myös esille, että uudet työntekijät eivät välttämättä saa riittävää ohjeistusta työssään tehtävään henkilötietojen käsittelyyn. Siksi olisikin hyvä sisällyttää henkilötietojen käsittelyyn liittyvä ohjeistus yhdeksi osaksi perehdyttämisen Moodlerooms –ympäristöä.

Tutkimuksen henkilöstökyselyssä saatujen vastausten perusteella voidaan todeta, että tiedottamista ja perehdytystä tietosuoja-asioissa tulee tehostaa, esimerkiksi lisäämällä tietosuojaosio viikkotiedotteeseen kerran kuukaudessa tai aina tarvittaessa. Vastaajat toivovat myös, että esimies tiedottaisi ja ohjeistaisi enemmän tietosuoja-asioista omassa työyksikössä. Esimiehet voisivatkin ottaa tietosuojaosaamistarpeen kehittämisen esille ja kartoittaa tietosuojaosaamisen täydentämistarpeen omassa yksikössä ja huolehtia, että sen jäsenillä on mahdollisuus osallistua tietosuojakoulutukseen työaikana. Työnantaja voisi järjestää henkilötietojen käsittelyn tietosuoja-asioihin liittyviä, eri kohderyhmille suunnattuja henkilöstökoulutuksia.

Karelia-ammattikorkeakoulun arkistonmuodostussuunnitelmasta käy ilmi muun muassa asiakirjojen säilyttämisajat. Henkilöstökyselyssä saatujen vastausten perusteella on havaittavissa, että arkistonmuodostussuunnitelmaa ei tunneta kovin hyvin. Suunnitelma olisikin hyvä käydä läpi soveltuvin osin kunkin yksikön henkilöstöpalaverissa, jotta jokainen henkilöstön jäsen on tietoinen käsittelemiensä asiakirjojen käsittelyyn liittyvistä reunaehdoista.

Tutkimustulosten mukaan fyysinen tietoturva on pääosin kunnossa. Olisi kuitenkin tarpeellista varmistaa, että kaikilla henkilötietoja käsittelevillä työntekijöillä on käytössä lukittava kaappi tai laatikosto henkilötietoja sisältävien asiakirjojen säilyttämistä varten. Tietosuoja-astioiden ja paperisilppureiden oikea sijoittelu tulostimien lähettyville ja niiden säännöllinen tyhjentäminen ovat tärkeitä asioita tietosuojan toteutumisen kannalta.

Henkilöstön tietosuojakyselyn vastauksista tuli esille, että henkilökuntaa askarruttaa sähköisen asioinnin puutteesta johtuva tietosuojariski. Hakemusten ja niiden liitteiden manuaalinen käsittely ja arkistointi lisäävät muun muassa virheiden mahdollisuutta eikä käsittely ole suojattua. Sähköistä asiointia toivotaan varsinkin opiskelijapalvelujen hakemusten hallinnointiin ja käsittelyyn sekä opiskelijoiden harjoittelu- ja opinnäytetöihin liittyvien asiakirjojen hallinnointiin.

Tietosuojavastaavan haastattelu toi esille, että Kareliassa ei ole tehty tietotilinpäätöstä. Vaikka tietotilinpäätöksen tietosuoja-asetus ei velvoita rekisterinpitäjää sitä tekemään, olisi johdon mielestämme hyvä harkita tietotilinpäätöksen käyttöönottoa yhdeksi ylimmän johdon työkaluista lisäämällä se tilinpäätöksen ja toimintakertomuksen raportteihin. Tietotilinpäätös auttaa ylintä johtoa hahmottaa kokonaiskuvaa henkilötietojen käsittelyn nykytilasta. Mielestämme opinnäytetyön kehitysehdotukset olisi hyvä käsitellä johtoryhmässä sekä tietosuoja- ja tietoturvaryhmässä. Ehdotukset kehittämistoimenpiteistä on esitetty taulukossa 1.

Taulukko 1. Ehdotukset kehittämistoimenpiteistä.

Kehittämiskohde	Ehdotukset kehittämistoimenpiteistä
Henkilöstön tietosuojaosaamisen täydentämistarpeen kartoittaminen	Esimiehet - ottavat tietosuojanosaamisen tärkeyden esille omissa työyksiköissään ja - kartoittavat työntekijöiden tietosuoja-osaamisen täydentämistarpeet - mahdollistavat tietosuojakoulutuksiin osallistumisen työajalla Toteutetaan, esim. Moodle-ympäristössä henkilöstölle suunnattu, vuosittain tehtävä itsearviointi omasta tietosuoja-osaamisen tasosta.
Riittävän perehdytyksen ja järjestäminen henkilötietoja käsitteleville työntekijöille	Lisätään henkilötietojen käsittelyyn liittyvä ohjeistus yhdeksi osaksi uuden työntekijän Perehdyttämisen Moodlerooms –ympäristöön.
Henkilöstön tietosuojaosaamisen varmistaminen	Eri kohderyhmille järjestettäviä tietosuoja-asioihin liittyviä, eri kohderyhmille suunnattuja henkilöstökoulutuksia. Tietosuojavastaavan tietoisku tietosuoja-asioista henkilöstön viikkotiedotteeseen, 3-4 kertaa vuodessa. Työyksikkökohtaisten ohjeiden ja toimintatapojen laatimiseen vastuuhenkilöt.
Osoitusvelvollisuuden täyttäminen	Eri yksiköissä tapahtuvan henkilötietojen käsittelyn kuvaukset kuntoon - yhteinen malli kuvauksen laadinnasta - kaikki kuvaukset samaan paikkaan - tietosuojavastaava tarkistaa kerran vuodessa, että kuvaukset on laadittu ja ovat ajan tasalla
Tietosuojariskien vähentäminen	Sähköinen asiointi opiskelijoiden hakemusten hallinnointiin ja käsittelyyn sekä harjoittelu- ja opinnäytetöihin liittyvien asiakirjojen hallinnointiin Varahenkilön nimeäminen tietosuojavastaavalle.

7 Johtopäätökset ja arviointi

Pekka Mattilan (2007, 131 – 132) muutoksen johtamisen mallissa on neljä vaihetta: 1. perustan luominen, 2. käynnistystoimet, 3. hallittu eteneminen, 4. vakiinnuttaminen. Mattilan mukaan muutosprosessin neljä avaintehtävää seuraavat toisiaan lähes kaikissa muutostilanteissa, mutta niiden sisällöt eivät ole

tarkkarajaisia ja määritettyjä. Muutosprosessissa on tavallista, että prosessin seuraavassa vaiheessa palataan vielä tarkastelemaan tai työstämään edellisen vaiheen tehtäviä. Karelia-ammattikorkeakoulussa tietosuoja-asetuksen mukaisen tietosuojan toteuttamisen pohjatyö ja valmisteluvaihe on hoidettu hyvin. Henkilöstöä koulutettiin ennen tietosuoja-asetuksen voimaan astumista riittävän osaamistason saavuttamiseksi. Kuten Mattila (2007, 132) toteaa, on tavallista, että muutosprosessin aikana on tarpeellista palata muutosprosessin aikaisempiin vaiheisiin. Kareliassa on syytä kerrata vaihe henkilöstön tiedottamisen ja osittain myös perehdyttämisen osalta henkilötietojen käsittelyosaamisen varmistamiseksi.

Opinnäytetyöhön liittyvistä henkilöstölle tehdystä tietosuojakyselystä ja tietosuojavastaavan haastattelusta saatujen tietojen perusteella voidaan todeta, että Siitä yhtenä osoituksena osallistuminen TAISTO-18 harjoitukseen, jossa Karelian osalta ei ilmennyt kriittisiä tietosuojan ja tietoturvan hallintaan liittyviä kehityskohteita. Näemme kuitenkin yhtenä tietosuojaa vaarantavana tekijänä sen, että tietosuojavastaavalle ei ole nimetty varahenkilöä. Tämä voi aiheuttaa ongelmia, jos esimerkiksi tietosuojavastaavan loma-aikana sattuisi tietosuojaloukkaus.

7.1 Johtopäätökset

Opinnäytetyömme yhtenä tavoitteena oli kartoittaa Karelian henkilöstön tietosuojaosaamisen taso. Henkilöstölle tehdyn tietosuojakyselyn useissa vastauksissa nousi esille kolme asiaa: tiedotus ja henkilöstön ajan tasalla pitäminen tietosuoja-asioissa, olemassa olevien ohjeiden näkyväksi tekeminen ja henkilöstön jatkuva perehdyttäminen.

Henkilöstökyselyn tulosten perusteella voidaan todeta, että Karelian henkilöstö on tietoinen henkilötietojen käsittelyyn liittyvistä tietosuoja-asetuksen velvoitteista ja ottaa ne huomioon henkilötietoja käsitellessään. Henkilöstö toivoo kuitenkin lisää koulutusta, ohjeistusta ja tiedottamista tietosuojaan ja sen toteuttamiseen

liittyvistä asioista. Lisäkouluttautumisen toive voidaan nähdä positiivisena asiana; Karelian henkilöstö haluaa kehittää ja varmistaa omaa osaamistaan tältä osin.

Tietosuojakyselyn tulosten analysoinnin yhteydessä tarkasteltiin jokaisen kysymyksen osalta esimiesten vastauksia omana ryhmänään, koska heillä on suuri merkitys tietosuojan toteuttamisessa ja ohjeistamisessa omissa työyksiköissään. Kyselyn vastausten perusteella voidaan todeta, että esimiehet ovat tietoisia Karelian henkilötietojen käsittelyyn liittyvistä toimintaohjeista ja säännöistä sekä tietosuojaohjeistuksesta. Esimiehet pitivät EU:n tietosuoja-asetukseen liittyviä väittämiä tärkeinä tai erittäin tärkeinä. Tiedostusta tulee kuitenkin kehittää ja lisätä. Esimiesten arvio omasta tietosuojaosaamisen tasosta oli kolme. Se on samalla tasolla kuin koko henkilöstön arvio omasta tietosuojaosaamisen tasosta.

Tietosuojavastaavan haastattelussa tuli esille, että toiminta- ja työohjeiden laatiminen on ohjattu työyksiköihin, mutta selvää vastuuhenkilöä ei ole nimetty. Tästä johtuen ohjeet ovat mahdollisesti jääneet ainakin osittain tekemättä ja tehdyt ohjeet voivat poiketa toisistaan, joka aiheuttaa sen, että eri yksiköissä toimitaan eri tavalla. Esimerkiksi henkilötietojen osoitusvelvollisuutta on hankala tarvittaessa täyttää, jos henkilötietojen käsittelyn kuvaukset puuttuvat. Haastattelu toi myös esille, että pienessä organisaatiossa isoja haasteita tuovat esimerkiksi sopimuksiin (etenkin kansainvälisten toimijoiden kanssa), riskienhallintaan (DPIA), hankintoihin sekä kansainvälisiin pilvipalveluihin liittyvät asiat ja digitalisoitumisen voimistuminen. Myös uudet asiat, kuten oppimisanalytiikka tuo lisähaasteita.

Edellä mainitut asiat jäävät tämän opinnäytetyön ulkopuolelle samoin kuin tietosuoja opiskelijahaussa ja -valinnassa ja opetuksessa. Ne ovat kuitenkin kaikki tärkeitä ja ajankohtaisia aiheita opiskelijavalintojen uudistuessa, korkeakoulujen välisen ristiinopiskelun lisääntyessä, oppimisanalytiikan kehittyessä ja kansainvälisen yhteistyön lisääntyessä sekä digitalisaation voimistuessa yhä enemmän yritysten toimintaympäristöissä. Näkisimme niiden olevan hyviä jatkotutkimusaiheita.

7.2 Opinnäytetyön arviointi

Opinnäytetyömme aiheena oleva tietosuoja ja sen toteutuminen on hyvin laaja käsite, jota voidaan tutkia monien aihealueiden kautta, esimerkiksi edellisessä kappaleessa mainitut asiat. Aloitimme opinnäytetyömme tekemisen keväällä 2019 ja tarkoituksenamme oli valmistua samana vuonna. Alkuperäinen aikataulu työn valmistumisesta vuoden vaihteessa ei kuitenkaan toteutunut työkiireiden ja työssä tapahtuneiden muutosten takia. Rajauksen tekeminen käsiteltävistä asioista oli vaikeaa, ja oman haasteensa toi toivomus, että tietosuojaa käsitellään myös johtamisen näkökulmasta.

Aineistoanalyysia tehtäessä huomasimme, että joitakin tietosuojakyselyn kysymyksiä olisi ollut syytä miettiä tarkemmin vastaajien ja tietojen analysoinnin näkökulmista. Vastaajien mielestä osa kysymyksistä oli monitulkintaisia tai vaikeasti ymmärrettäviä ja näin ollen vastauksista saatu tieto ei välttämättä anna oikeaa kuvaa kysytystä asiasta. Myös vastauksista saatujen tietojen luokittelu ja esittäminen graafisesti oli joidenkin kysymysten osalta haasteellista.

Opinnäytetyötä tehdessämme olemme noudattaneet Karelian opinnäytetyöohjeistusta ja Tutkimuseettisen neuvottelukunnan (TENK) “Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa” -ohjeessa määriteltyä hyvää tieteellistä käytäntöä. Sen mukaisesti olemme opinnäytetyömme toimeksiantajan kanssa tehneet toimeksiantosopimuksen, jossa olemme sopineet opinnäytetyön keskeisistä asioista. Teimme tutkimuslupahakemuksen opinnäytetyöhön liittyvän tietosuojakyselyn toteuttamiseksi Karelian henkilökunnalle. Olemme tutustuneet opinnäytetyöprosessiin sovellettavaan lainsäädäntöön ja noudattaneet sitä parhaamme mukaisesti. Opinnäytetyöhön liittyvän tietosuojakyselyn alussa on kerrottu sen tarkoitus, kerättävien tietojen käyttäminen ja niiden säilyttäminen. Kyselyssä ei ole kysytty henkilötietoja ja kyselyyn on vastattu anonyymisti, eikä sen lopussa olevaa arvontaa varten annettua sähköpostiosoitetta ole voitu liittää annettuihin vastauksiin. Olemme noudattaneet annettuja ohjeita tiedonhankinnassa, tutkimusmenetelmissä ja kerätyn tutkimusaineiston analysoin-

nissa sekä rehellisesti tuoneet raportissamme esille tietoturvakyselyssä ja henkilöhaastattelussa ilmenneet asiat, niitä muuttamatta tai olennaisia asioita pois jättämättä. Lisäksi olemme tehneet opinnäytetyön asianmukaiset lähdemerkinnät lainaamistamme aikaisemmin julkaistuista tutkimuksista ja kirjallisuudesta sekä käyttämistämme internet-lähteistä.

Opinnäytetyöprosessin aikana oma osaamisemme henkilötietojen käsittelyn tietosuojasta on laajentunut. Olemme oppineet, että tietosuoja- ja tietoturvatyö ovat osa jokaisen työntekijän päivittäistä työtä. Ymmärrämme myös paremmin yrityksen johdon ja esimiesten sekä tietosuojavastaavan roolin tietosuojatyön organisoinnissa ja toteuttamisessa. Näkemyksemme mukaan Kareliassa henkilötietojen käsittelyn tietosuoja ja henkilöstön tietosuojaosaaminen ovat hyvällä tasolla, ja niitä voidaan ylläpitää ja parantaa esitetyillä toimenpiteillä.

Lähteet

Ammattikorkeakoululaki 932/2014.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2016. Tietosuojakäsikirja johdolle. Helsinki. Tietosanoma.

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Helsinki. Tietosanoma.

Arjen tietosuoja. 2018. Johdon ja esimiesten tietosuojakoulutusvideo. https://vimeo.com/234313084/f874f6b947. 21.5.2020.

Dalkir, K., 2005. Knowledge Management in Theory and Practice. Elsevier Butterworth–Heinemann publications. https://dianabarbosa.files.wordpress.com/2009/03/knowledge-management-kimiz-dalkir.pdf. 4.3.2020.

Euroopan parlamentin ja neuvoston tietosuoja-asetus (EU) 2016/679.

Garber, P.R. 2013. Managing Change at Work. Journal. T + D. Jan2013, Vol. 67 Issue 1, sivut 48 – 51.

Hallituksen esitys 9/2018 eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. https://www.eduskunta.fi/pdf/HE+9/2018. 24.5.2020.

Hallituksen esitys 2/2020 eduskunnalle laeiksi oikeusministeriön hallinnonalan eräiden henkilötietojen käsittelyä koskevien säännösten muuttamista. https://www.eduskunta.fi/pdf/HE+2/2020. 24.5.2020.

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

Hirsjärvi, S., Remes, P., Sajavaara P. 2016. Tutki ja kirjoita. Helsinki. Tammi.

Heiskanen, M. & Lehikoinen, R. 2010. Muutosviestinnän voimapaperi. Helsinki: Talentum.

Karelia-ammattikorkeakoulu. 2018. Tietosuojapolitiikka. https://intranet.karelia.fi/turvallisuus/tietoturvallisuus/Tietosuoja_ja_tietoturva_ryhma/Materiaalia/Tietosuoja/Karelia_amk_tietosuojapolitiikka.pdf. 5.2.2019.

Karelia-ammattikorkeakoulu. 2019. Rekisteriselosteet. http://www.karelia.fi/rekisteriselosteet. 19.4.2020.

Karelia-ammattikorkeakoulu. 2020a. Karelia-ammattikorkeakoulun toimintakertomus 2019. https://issuu.com/karelia-amk/docs/karelia-toimintakertomus2019 2.6.2020.

Karelia-ammattikorkeakoulu. 2020b. Asiakirjahallinto. https://intranet.karelia.fi/johtaminen/Sivut/Asiakirjahallinto.aspx. 24.4.2020.

Karelia-ammattikorkeakokulu. 2020c. Asiantuntijapalvelut. https://www.karelia.fi/fi/asiantuntijapalvelut/palvelu-ja-tutkimusympäristot/voimala-sosiaali-ja-terveysala. 5.6.2020.

Karelia-ammattikorkeakoulu. 2020d. Turvallisuus. https://www.karelia.fi/fi/karelia/turvallisuus. 4.3.2020.

Kosonen, M. 2019. Tiedolla johtamisen periaatteet.

https://www.theseus.fi/bitstream/hanle/10024/227003/URNISBN9789523441835.pdf?sequence=2&isAllowed=y. 15.2.2020.
Kotter, P. J. 2012. Leading Change. Harward Business Review Press. Boston.
Kukkola, E. 2018. En minä, vaan me. Helsinki. Books on Demand.
Kulmala, T. 2017. Uusi tietosuoja-asetus ja yritysten sopimukset. https://www.lrhto.fi/artikkelit/yrityksen-sopimukset/uusi-tietosuoja-asetus-ja-yritysten-sopimukset/. 21.5.2020.
Kuntaliitto. 2019. Henkilötietojen käsittely kunnassa. https://www.kuntaliitto.fi/asiantuntijapalvelut/laki/julkisuus-ja-tietosuoja/henkilotietojen-kasittely-kunnassa. 3.5.2019.
Laihonen, H & Lönnqvist, A. 2013. Tiedolla johtaminen tarkoittaa tiedon hyödyntämistä. https://tietovirta.wordpress.com/2013/11/06/tiedolla-johtaminen-tarkoittaa-tiedon-hyodyntamista/. 16.1.2020.
Laihonen, H., Hannula, M., Helander, N., Ilvonen, I., Jussila, J., Kukkonen, M., Kärkkäinen, H., Lönnqvist, A., Myllärniemi, J., Pekkola, S., Virtanen, P., Vuori, V. & Yliniemi, T. 2013. Tietojohtaminen. Tampereen teknillinen yliopisto tiedonhallinnan ja logistiikan laitos. https://trepo.tuni.fi/bitstream/handle/10024/116695/tietojohtaminen.pdf?sequence=2&isAllowed=y. 16.1.2020.
Laki julkisen hallinnon tiedonhallinnasta 906/2019.
Laki yksityisyyden suojasta työelämässä annetun lain muutoksesta 347/2019.
Mattila, P. 2007. Johdettu muutos – avaimet organisaation hallittuun uudistamiseen. Keuruu. Talentum Media Oy.
Metsämuuronen, J. 2008. Laadullisen tutkimuksen perusteet. Jyväskylä. Gummerus.
Oikeusministeriö. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? https://tietosuoja.fi/documents/6927448/9666681/Miten+valmistautua+tietosuoja-asetukseen/8c5b9a96-a8ce-4c91-ad06-6e36130bd0e5/Miten+valmistautua+tietosuoja-asetukseen.pdf. 30.1.2019.
Ojasalo, K., Moilanen, T., Ritalahti, J. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki. WSOYpro Oy.
Opi tietosuojaa.fi 2018. https://opitietosuojaa.fi/images/tiedostot/pikakuvakkeet/Tietosuojatyön_organisointi2018.pdf. 5.5.2019.
Saraviita, I. 2011. Perustuslaki. Helsinki. Talentum.
Tietosuojalaki 1050/2018.
Tietosuojatyöryhmä. 2017. Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksen (EU) 2016/679 tarkoitettu ”korkea riski”. 14.3.2019. https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9deb-e21bdd2e0a63/Vaikutustenarviointi+fi.pdf. 14.3.2019.
Tietosuojavaltuutetun toimisto. 2012. Laadi tietotilinpäätös. https://tietosuoja.fi/documents/6927448/10594424/Laadi+tietotilinp%C3%A4%C3%A4t%C3%B6s.pdf/4925bd9e-d07d-82fc-3f2d-71c5955310a0/Laadi+tietotilinp%C3%A4%C3%A4t%C3%B6s.pdf. 23.2.2020.
Tietosuojavaltuutetun toimisto. 2018a. Seloste käsittelytoimista. https://tietosuoja.fi/seloste-kasittelytoimista. 23.2.2020.

Tietosuojavaltuutetun toimisto. 2018b. Työelämän tietosuojalaki. https://tietosuoja.fi/tyoelaman-tietosuojalaki. 27.2.2020.
Tietosuojavaltuutetun toimisto 2018c. Vaikutustenarviointi. https://tietosuoja.fi/vaikutustenarviointi. 19.3.2020.
Tietosuojavaltuutetun toimisto. 2019. Tietosuojavastaavat. https://tietosuoja.fi/tietosuojavastaavat. 3.5.2019.
Tietosuojavaltuutetun toimisto. 2020. Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle. 19.3.2020. https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle
Tietosuojavastaavan haastattelu. 2020.
Tuomi, J., Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Jyväskylä. Tammi.
Valtiovarainministeriö. 2016. EU-tietosuojan kokonaisuudistus. https://www.vahtiohje.fi/web/guest/vahti-raportti-1/2016. 30.1.2019.
Valtiovarainministeriö. 2020a. Tiedonhallintalaki. https://vm.fi/tiedonhallintalaki. 27.2.2020
Valtiovarainministeriö. 2020b. Koulutusmateriaali: Tiedonhallintolaki – tiedonhallinnan järjestäminen ja johdon vastuut. https://vm.fi/documents/10623/9949343/Tiedonhallinnan+j%C3%A4rjest%C3%A4minen+ja+johdon+vastuut+v2/a07754fb-ce4e-2fe6-9ea1-a31e02b90590/Tiedonhallinnan+j%C3%A4rjest%C3%A4minen+ja+johdon+vastuut+v2.pdf. 27.2.2020.
Åhman, H. 2005. Menestyvä Johtaminen. Porvoo. WS Bookwell Oy.

Muistilista - Tietosuojatyön organisoinnin taustakartoitukset

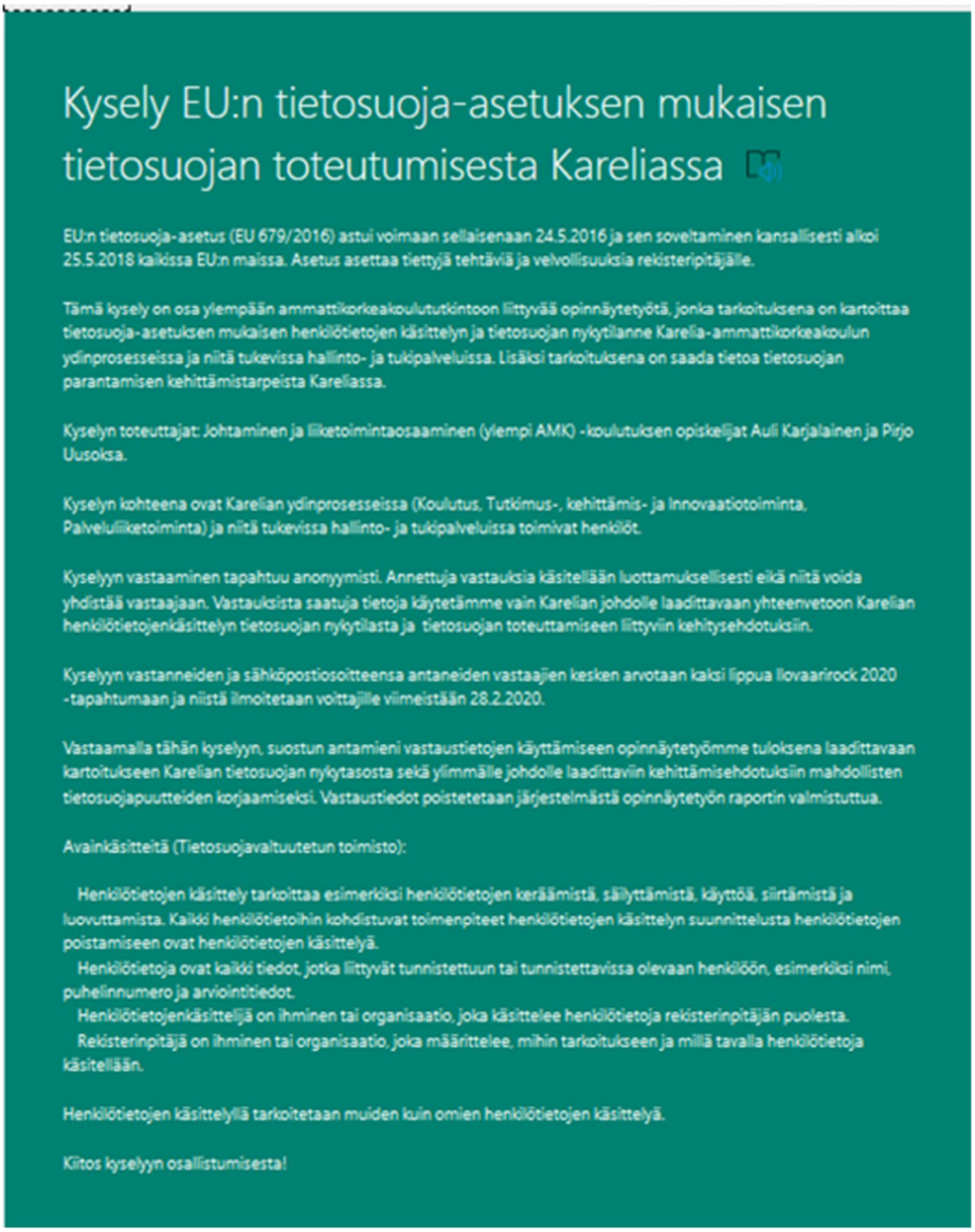
1. Selvitä organisaatiosi tietosuojan ja henkilötietojen tilannekuva.

   Tee henkilöstölle (myös tilivelvolliselle johdolle) kartoittava tietosuojakysely, suorita tietosuojan itseauditointi ja tarvittaessa tilaa ulkopuolinen arviointi. Tarkasta,

   - miten on määritelty ja toteutettu rekisterinpito mukaan lukien henkilörekisteriselosteet,
   - onko tarvittavat asiakas- tai henkilötietojen käsittelyohjeet laadittu ja ajan tasalla,
   - miten käyttövaltuuden tiedoille ja käytönvalvonta on toteutettu ja
   - miten tietosuojattavan jätteen hävittäminen on organisoitu,
2. Selvitä, miten on toteutettu tietosuojaa ja tietoturvaa käsittelevien sopimusliitteiden ja salassapitositoumuksien laadinta ja hallinta.
3. Selvitä, onko tietosuoja- ja tietoturvavaatimuksien määrittely ICT-hankinnoissa hoidettu systemaattisesti.
4. Selvitä, onko arkistonmuodostussuunnitelma(t) laadittu ja käytössä (julkisella sektorilla lain edellyttämät).
5. Selvitä, onko organisaatiossa käytössä tietojen luokittelu ja kuinka liiketoiminnan ydintietojen hallinta on toteutettu.
6. Selvitä, onko organisaatiossa sovittu määrämuotoinen tietosuoja-asioiden raportointi aina vastaavaan johtoon asti.

(Andreasson & Koivisto & Ylipartanen 2016, 93.)

Henkilöstön tietosuojakysely



Kysely EU:n tietosuoja-asetuksen mukaisen tietosuojan toteutumisesta Kareliassa

EU:n tietosuoja-asetus (EU 679/2016) astui voimaan sellaisenaan 24.5.2016 ja sen soveltaminen kansallisesti alkoi 25.5.2018 kaikissa EU:n maissa. Asetus asettaa tiettyjä tehtäviä ja velvollisuuksia rekisteripitäjälle.

Tämä kysely on osa ylempään ammattikorkeakoulututkintoon liittyvää opinnäytetyötä, jonka tarkoituksena on kartoittaa tietosuoja-asetuksen mukaisen henkilötietojen käsittelyn ja tietosuojan nykytilanne Karelia-ammattikorkeakoulun ydinprosesseissa ja niitä tukevissa hallinto- ja tukipalveluissa. Lisäksi tarkoituksena on saada tietoa tietosuojan parantamisen kehittämistarpeista Kareliassa.

Kyselyn toteuttajat: Johtaminen ja liiketoimintaosaaminen (ylempi AMK) -koulutuksen opiskelijat Auli Karjalainen ja Pirjo Uusoksa.

Kyselyn kohteena ovat Karelian ydinprosesseissa (Koulutus, Tutkimus-, kehittämis- ja Innovaatiotoiminta, Palveluliiketoiminta) ja niitä tukevissa hallinto- ja tukipalveluissa toimivat henkilöt.

Kyselyyn vastaaminen tapahtuu anonyymisti. Annettuja vastauksia käsitellään luottamuksellisesti eikä niitä voida yhdistää vastaajaan. Vastauksista saatuja tietoja käytetämme vain Karelian johdolle laadittavaan yhteenvetoon Karelian henkilötietojenkäsittelyn tietosuojan nykytilasta ja tietosuojan toteuttamiseen liittyviin kehitysehdotuksiin.

Kyselyyn vastanneiden ja sähköpostiosoitteensa antaneiden vastaajien kesken arvotaan kaksi lippua Ilovaarirock 2020 -tapahtumaan ja niistä ilmoitetaan voittajille viimeistään 28.2.2020.

Vastaamalla tähän kyselyyn, suostun antamieni vastaustietojen käyttämiseen opinnäytetyömme tuloksena laadittavaan kartoitukseen Karelian tietosuojan nykytasosta sekä ylimmälle johdolle laadittaviin kehittämisehdotuksiin mahdollisten tietosuojapuutteiden korjaamiseksi. Vastaustiedot poistetetaan järjestelmästä opinnäytetyön raportin valmistuttua.

Avainkäsitteitä (Tietosuojavaltuutetun toimisto):

Henkilötietojen käsittely tarkoittaa esimerkiksi henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen ovat henkilötietojen käsittelyä.
Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön, esimerkiksi nimi, puhelinnumero ja arviointitiedot.
Henkilötietojenkäsittelijä on ihminen tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.
Rekisterinpitäjä on ihminen tai organisaatio, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään.

Henkilötietojen käsittelyllä tarkoitetaan muiden kuin omien henkilötietojen käsittelyä.

Kiitos kyselyyn osallistumisesta!

Taustatiedot

1. Toimin Kareliassa *

- Esimiehenä
- Opettajana
- Projektitoimijana
- Hallinto- ja tukipalveluhenkilöstössä

Henkilöstön tietosuojakysely

2. Ydinprosessi, jossa toimin tai Hallinto- ja tukipalvelut *

- Koulutus
- Tutkimus-, kehittämis- ja Innovaatiotoiminta tai Palveluliiketoiminta
- Hallinto- ja tukipalveluissa

3. Työpisteeni sijaitsee *

- Tikkarinne-kampuksella
- Wärtsilä-kampuksella

Henkilötietojen käsittely

4. Työssäni käsittelen henkilötietoja seuraavassa/seuraavissa järjestelmissä (voit valita useamman vaihtoehdon) *

- En käsittele työssäni henkilötietoja
- ESS
- Raportronic
- Expence
- Sympa
- Rondo
- Dynasty
- Meerkado
- Henkilöstöhallinnon järjestelmät
- Peppi: Opiskelijatiedot
- Peppi: OPS/HOPS-tiedot
- Peppi: Opettajien työaikasuunnittelu
- CRM (yhteistyökumppanit ja muut asiakkaat)
- Omat Excel- ja Wordlistat
- Webropol-lomake-editori
- Cloudia (tarjouksen antajien CV:t)
- Valvontakamerat
- HORA
- Outlook (Sähköpostilistat)
- Timecon (kulunvalvonta)
- Halpnet
- Hakujärjestelmät
- Hankerahoittajien sähköiset raportointijärjestelmät
- Muu

Henkilöstön tietosuojakysely

5. Käsittelen työssäni seuraavia henkilökunnan henkilötietoja *

- [ ] En käsittele työssäni henkilökunnan henkilötietoja
- [ ] Henkilötunnus
- [ ] Nimi- ja yhteystiedot
- [ ] Kehityskeskustelutiedot
- [ ] Työsuhdetiedot
- [ ] Poissaolotiedot
- [ ] Terveystiedot
- [ ] Palkkatiedot
- [ ] Matkustusasiakirjat
- [ ] Tilinumero
- [ ] Työnhakuun liittyvät tiedot
- [ ] Muu

6. Käsittelen työssäni seuraavia opiskelijoiden ja hakijoiden henkilötietoja (koskee myös vaihto-opiskelijoita) *

- [ ] En käsittele työssäni opiskelijoiden henkilötietoja
- [ ] Henkilötunnus
- [ ] Opiskelijanumero
- [ ] Oppijan ID-tunnus
- [ ] Nimi- ja yhteystiedot
- [ ] Läsnäolotiedot
- [ ] Arkaluontoiset henkilötiedot
- [ ] OPS/HOPS-tiedot
- [ ] Arvosanat
- [ ] Matkustusasiakirjat
- [ ] Harjoitteluun liittyvät sopimustiedot
- [ ] Opinnäytetyöhön liittyvät sopimustiedot
- [ ] Projektiopintoihin liittyvät sopimustiedot
- [ ] Muu

Henkilöstön tietosuojakysely

7. Käsittelen työssäni seuraavia kotimaisten asiakkaiden ja yhteistyökumppaneiden henkilötietoja (pl. opiskelijat ja hakijat) *

- [ ] En käsittele työssäni kotimaisten asiakkaiden ja yhteistyökumppaneiden henkilötietoja
- [ ] Henkilötunnus (henkilöasiakkaat)
- [ ] Nimi- ja yhteystiedot (henkilöasiakkaat)
- [ ] Yhteyshenkilön nimi- ja yhteystiedot
- [ ] Matkustusasiakirjat
- [ ] Tilinumero
- [ ] Muu

8. Käsittelen työssäni seuraavia ulkomaisten asiakkaiden ja yhteistyökumppaneiden henkilötietoja (pl. opiskelijat ja hakijat) *

- [ ] En käsittele työssäni seuraavia ulkomaisten asiakkaiden ja yhteistyökumppaneiden henkilötietoja
- [ ] Henkilönumero (henkilöasiakkaat)
- [ ] Nimi- ja yhteystiedot (henkilöasiakkaat)
- [ ] Yhteyshenkilön nimi- ja yhteystiedot
- [ ] Matkustusasiakirjat
- [ ] Tilinumero
- [ ] Muu

9. Mistä pääasiassa saat työssä käsittelemäsi henkilötiedot? *

- ( ) Henkilöltä itseltään
- ( ) Tietojärjestelmästä
- ( ) Yhteyshenkilöltä
- ( ) Muu

Henkilöstön tietosuojakysely

10. Valitse itsellesi sopivin vaihtoehto alla olevista henkilötietojen käsittelyä koskevista väittämistä *

	Kyllä	Suurimmaksi osaksi	Jonkin verran	En lainkaan
Tunnistan EU:n tietosuoja-asetuksen (EU 2016/679) vaikutuksen työhön liittyvässä henkilötietojenkäsittelyssä	○	○	○	○
Olen saanut riittävän perehdytyksen tehtäviini kuuluvien henkilötietojen käsittelemiseen	○	○	○	○
Tiedän, mitä henkilörekistereillä, henkilötiedoilla ja niiden käsittelyllä tarkoitetaan	○	○	○	○
Käsittelen työssäni vain työtehtäviäni kannalta välttämättömiä henkilötietoja	○	○	○	○
Käsitellessäni työssäni henkilötietoja noudatan voimassaolevia henkilötietojenkäsittelyä koskevia lainsäädännön periaatteita	○	○	○	○
Tiedän, mitkä henkilötiedot ovat arkaluontoisia tietoja ja noudatan niiden käsittelyssä erityistä huolellisuutta	○	○	○	○
Tunnen vastuuni vaitiolo- ja salassapitovelvollisuudesta käsitellessäni henkilötietoja ja -rekistereitä	○	○	○	○
Tunnistan työssäni tarvitsemieni henkilötietojen käsittelyyn liittyvät tietosuojariskit	○	○	○	○
Tiedän, miten henkilötietoja sisältävät asiakirjat säilytetään ja tuhotaan	○	○	○	○

11. Kirjaa tähän havaintojasi ja kehittämisehdotuksia Karelian henkilötietojen käsittelyyn liittyvistä toimintaohjeista ja säännöistä.

Kirjoita vastaus

Henkilöstön tietosuojakysely

Tietosuojan toteuttaminen

12. Olen saanut tietoa Karelian tietosuojaan liittyvistä asioista *

- [ ] En ole saanut tietoa tietosuojan liittyvistä asioista
- [ ] Koulutustilaisuuksista
- [ ] Intrasta
- [ ] Työtoverilta
- [ ] Henkilöston sähköisessä uutiskirjeessä
- [ ] Muu

13. Valitse itsellesi sopivin vaihtoehto alla olevista tietosuojaohjeistuksia koskevista väittämistä *

	Samaa mieltä	Osittain samaa mieltä	Osittain eri mieltä	Eri mieltä
Karellan tietosuojasäännökset ovat helposti saatavilla	○	○	○	○
Henkilötietoja sisältävien paperisten asiakirjojen käsittelyyn ja säilyttämiseen on olemassa kirjallinen ohjeistus	○	○	○	○
Karellassa on kirjallinen ohje henkilötietojen lähettämisestä sähköpostise	○	○	○	○
Olen tutustunut työpaikkani tietosuojasäännöksiin ja tiedän mitä tietosuojalla tarkoitetaan	○	○	○	○
Karellalla on ohjeistus rekisteröidyn oikeuksien toteutumisesta (esim. tietojen tarkastamis-, oikaisu- ja siirto-oikeus).	○	○	○	○
Tietosuojasta ja sen toteuttamisesta tiedotetaan henkilöstöille riittävästi	○	○	○	○
Rekisteriselosteet ovat helposti jokaisen saatavilla	○	○	○	○
Olen tutustunut Karellan rekisteriselosteisiin	○	○	○	○
Tietosuojavastaavan yhteystiedot ovat helposti saatavilla	○	○	○	○
Tunnen Karellan tietosuojan toteutumisen vastuut ja organisoinnin	○	○	○	○
Olen saanut tarvittaessa ohjausta tietosuojaasioihin liittyvissä asioissa	○	○	○	○

Henkilöstön tietosuojakysely

14. Valitse itsellesi sopivin vaihtoehto alla olevista tietosuojakäytäntöjä koskevista väittämistä *

	Aina	Joskus	En koskaan
Lukitsen työaseman aina poistuessani työpisteestäni	○	○	○
Tallennan henkilötietoja sisältävät tiedostot suojattuun ja varmuuskopioitavaan verkkopalveluun	○	○	○
Säilytän henkilötietoja sisältävät asiakirjat/muistitikut lukitussa kaapissa/laatikostossa	○	○	○
Huolehdin, ettei työpöydälläni ole nähtävissä/saatavilla henkilötietoja sisältäviä asiakirjoja	○	○	○
Tunnen ja noudatan Karelian käyttäjätunnusten salasanan muodostamisesta ja säilyttämisestä annettuja ohjeita	○	○	○
Tunnen ohjeistuksen henkilötietojen lähettämisestä sähköpostitse ja toimin sen mukaisesti	○	○	○
Osaan toimia havaitessani tietosuojapuutteen tai -loukkauksen	○	○	○

15. Halutessasi voit antaa selvennystä kohdassa 14 antamiisi vastauksiin

Kirjoita vastaus

16. Merkitse alle, miten tärkeänä pidät kutakin EU:n tietosuoja-asetuksen säännöksiin liittyvää asiaa *

	Erittäin tärkeä	Tärkeä	En osaa sanoa	Vähän merkitystä	Ei merkitystä
Parantaa henkilötietojen käsittelyn hallintaa	○	○	○	○	○
Parantaa rekisteröidyn henkilötietojen suojaa ja tietosuojaoikeuksia	○	○	○	○	○
Parantaa rekisteröidyn oikeuksia tarkastella itsestään kerättyjä henkilötietoja	○	○	○	○	○
Tehostaa rekisteröintiä-jän henkilötietojen käsittelyn seurantaa ja valvontaa	○	○	○	○	○
Yhdenmukaistaa henkilötietojen käsittelyä EU:n alueella	○	○	○	○	○
Huomioi uudet teknologiat ja tiedonkäsittelymenetelmien riskit	○	○	○	○	○

Henkilöstön tietosuojakysely

17. Arvioi oma tietosuojaosaamisesi taso tähtimerkein (5 tähteä=erinomainen, 1=heikko) *

☆ ☆ ☆ ☆ ☆

18. Ajatuksia ja kehittämisehdotuksia Karelian tietosuoja-asioista ja niiden toteuttamisesta

Kirjoita vastaus

Tietosuojavastaavan haastattelurunko

1. Kuvaukset organisaation henkilötietojen käsittelystä
   - Kenen vastuulla kuvauksien teko on?
   - Miten on varmistettu, että kuvaukset on laadittu?
   - Minne kuvaukset on tallennettu?
   - Miten on varmistettu, että henkilötietojen käsittelijät ovat tietoisia itseään koskevien kuvauksien sisällöstä?
   - Miten varmistetaan kuvauksien ajantasaisuus?

2. Rekisteriselosteet, henkilötietojen käsittelyyn liittyvät ohjeistukset
   - Miten varmistetaan rekisteriselosteiden ajantasaisuus?
   - Miten henkilötietojen käsittelyä on ohjeistettu?
   - Onko ohjeistettu, mitä tietoja voi tallentaa esimerkiksi pilvipalveluun tai intranettiin?
   - Mistä henkilötietojen käsittelyyn liittyvä ohjeistus löytyy?
   - Miten ohjeistuksen ajantasaisuus varmistetaan?
   - Onko Kareliassa laadittu periaatteet henkilötietojen käsittelylle? Kuten esim. UEF:n sivuilla.

3. Tietosuojaan liittyvä ohjeistus
   - Mitä dokumentteja ja ohjeita tietosuojaan liittyen on laadittu? Onko muita kuin tietosuoja- ja tietoturvapolitiikka, Opintoasioiden tietosuoja – usein kysytyt kysymykset, Ohjeita opiskelijalle, jonka tutkimustehtävään liittyy henkilötietojen käsittelyä?
   - Miten henkilöstöä tiedotetaan dokumenteista ja ohjeista?
   - Missä ne ovat henkilöstön saatavilla?
   - Kuinka usein dokumentteja ja ohjeita päivitetään?
   - Kuinka henkilöstöä tiedotetaan tietosuoja asioista?
   - Miten projektihenkilöstöä on ohjeistettu henkilötietojen käsittelyyn liittyvissä tietosuoja-asioissa? Onko olemassa saman tyyppistä ohjeistusta kuin opiskelijoille (Ohjeita opiskelijalle, jona tutkimustehtävään liittyy henkilötietojen käsittelyä)?
   - Kuinka opiskelijoita tiedotetaan tietosuoja asioista?
   - Miten tietosuojan toteutumista seurataan ja arvioidaan?

4. Henkilötietojen käsittelyyn liittyvä riskienhallinta
   - Miten henkilötietojen käsittelyyn liittyvä riskienhallinta on toteutettu?
   - Onko Kareliassa olemassa toimintaohjeet tietosuojariskien varalle?
   - Miten henkilötietoihin kohdistuviin tietoturvaloukkauksiin on varauduttu?
   - Onko määritetty seuraamuskäytännöt tietosuojarikkomuksien varalle?
   - Miten tietosuojahävitettävän jätteen hävitysprosessi on ohjeistettu?
   - Onko olemassa ohjeistus suojatun sähköpostin käyttöön henkilötietojen jakamisessa?

5. Käytönvalvonnan hallinta
   - Onko Kareliassa laadittu lokipolitiikka ja toteutuuko se?
   - Miten tietojärjestelmien tuottamien lokien hallinta on toteutettu?

Tietosuojavastaavan haastattelurunko

6. Tietosuojatoiminnan arviointi, raportointi, kehittäminen
    - Onko Karelia-ammattikorkeakoulussa tehty tietotilinpäätös? Jos on, kuinka sitä on hyödynnetty?
    - Kuinka usein tietosuoja-asioista raportoidaan ylimmälle johdolle?
    - Onko Kareliassa tietosuojan ja tietoturvan omavalvontasuunnitelma?
    - Mitkä ovat keskeisimmät tietosuojan toteuttamiseen liittyvät kehittämiskohteet?