Samu Ahvenjärvi

TIETOSUOJAVASTAAVAN TEHTÄVÄSSÄ ONNISTUMINEN KUNTAORGANISAATIOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Ahvenjärvi, Samu
Tietosuojavastaavan tehtävässä onnistuminen kuntaorganisaatiossa
Jyväskylä: Jyväskylän yliopisto, 2020, 69 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Niemimaa, Marko

EU:n yleinen tietosuoja-asetus muutti merkittävästi henkilötietojen käsittelyä ja tietosuojaa koskevaa lainsäädäntöä kansainvälisellä tasolla. Se yhtenäisti EU:n alueen henkilötietojen käsittelyn käytäntöjä ja toi uusia velvoitteita rekisterinpitäjille ja henkilötietojen käsittelijöille. Yksi näistä vaatimuksista, nimitystä koskevien edellytysten täyttyessä on tietosuojavastaavan nimitys. Tietosuojavastaava on asemaltaan riippumaton erityisasiantuntija, jonka tehtävänä on tukea rekisterinpitäjää tai henkilötietojen käsittelijää tietosuojaa koskevissa asioissa ja valvoa tietosuojan toteutumista. Tietosuoja-asetus määrittää tietosuojavastaavan nimitykseen, asemaan ja tehtäviin koskevia vaatimuksia, jotka jättävät organisaatioille tulkinnanvaraa ja tämän vuoksi esimerkiksi tietosuojavastaavan asema eri organisaatioissa vaihtelee. Tämän tutkielman tavoitteena on tutkia tehtävässä onnistumiseen vaikuttavia tekijöitä tietosuojavastaavan kompetenssien ja roolin organisoinnin näkökulmista kuntaorganisaatiossa. Millaisia työelämätaitoja tietosuojavastaava työssään tarvitsee ja miten tehtävä tulisi organisoida kuntaorganisaatiossa, jotta tietosuojavastaava pystyy hoitamaan työtehtävänsä vaatimusten mukaisesti? Näihin kysymyksiin tutkielmassa pyritään vastaamaan.

Tutkielman aineisto kerättiin haastattelemalla yhdeksän kunnan ja kaupungin tietosuojavastaavia. Haastattelut toteutettiin teemahaastatteluilla ja niistä kerättyä aineistoa analysoitiin etsimällä toistuvia virkkeitä ja teemoja. Tutkielman lopputuloksena esitellään tietosuojavastaavan tarvitsemia työelämätaitoja sekä esitetään näkökulmia, joita tulisi huomioida, kun tehtävää organisoidaan kuntaorganisaatioon. Tutkielmassa havaittiin, että tietosuojavastaavalla tulee olla muun muassa hyvät sosiaaliset- ja viestintätaidot sekä tuntea organisaatio hyvin. Tutkielmassa havaittiin myös, että tietosuojavastaavan aseman tulisi olla erityisasiantuntijan roolissa mahdollisimman korkealla kunnan tai kaupungin hierarkiassa. Tietosuojavastaavalla voi olla muitakin tehtäviä, mutta hänen työnsä resursointi tulee varmistaa ja sitä tulee seurata. Muiden tehtävien hoitaminen ei tule asettaa tietosuojavastaavaa eturistiriitatilanteeseen eikä vaarantaa hänen riippumattomuuttansa. Tietosuojavastaavan resursoinnilla ja tehtävien suorittamisen välillä havaittiin myös riippuvuuksia, joten tehtävien hoitamiseen tulee varata riittävästi aikaa.

Asiasanat: tietosuoja, henkilötietojen käsittely, tietosuojavastaava, tietoturva, kuntaorganisaatio, työelämätaito, asema

ABSTRACT

Ahvenjärvi, Samu
Succeeding in the role of data protection officer in a municipality
Jyväskylä: University of Jyväskylä, 2020, 69 p.
Cyber security, Master's Thesis
Supervisor: Niemimaa, Marko

General Data Protection Regulation (hereinafter GDPR) remarkably changed the way of processing personal data and the legislation regarding the protection of natural persons and the processing of their data on a global level. GDPR unified the practices of personal data processing within European Union and European Economic Areas and enforced new compliance requirements to data controllers and data processors. One of these new compliance requirements is to designate a Data Protection Officer (hereinafter DPO), if terms apply to the organisation. DPO position is an independent specialist whose duties involve supporting the organisation he/she works for in matters related to data privacy and protection of personally identifiable information and monitoring compliance. GDPR applies requirements to the designation, position and tasks of the DPO but they leave room for interpretation and therefore the position and tasks vary by the organisation. The study examines the requirements in regard of the DPO's competence and position in a municipality in order for them to succeed in their role. What work-life skills does the DPO need and how the position should be aligned within the municipality to best support the DPO in his/her role? The aim of the study is to answer to these questions.

The data for this study was collected by interviewing nine DPO's working in different municipalities. The data was analysed by identifying similar themes occurring within the collected data. The results indicate that the competences required in the role of a DPO consists of five classes of different skills which include good social and communication skills and organisational knowledge among others. In addition the DPO's position within the municipality should be an independent specialist high in the organisations hierarchy. The DPO may have other tasks and duties but it should be ensured that he/she has sufficient resources such as available time. The other tasks and duties should not put the DPO in a situation where there are conflict of interests or might endanger his/her independence. The study also indicates that there are correlations with sufficient resources and committing to the tasks fo the DPO. Therefore ensuring the sufficient resourcing of the DPO is a necessity.

Keywords: General Data Protection Regulation, Data Protection Officer, information security, position, work-life skill set, municipality

KUVIOT

TAULUKOT

SISÄLLYS

1. Johdanto

Digitalisaatio ja teknologian räjähdysmäinen kehitys ovat mahdollistaneet uusien liiketoimintamallien luomisen käyttäen Internetiä alustanaan. Näissä liiketoimintamalleissa keskiössä ovat henkilötiedot ja joidenkin yritysten liiketoiminta perustuukin täysin henkilötietojen keräämiseen ja käsittelyyn. Sen lisäksi, että henkilötietojen keräämiseltä ja käsittelyltä on yhä vaikeampi välttyä, myös yhteydeltä Internetiin on nykyään vaikea välttyä ja omaa yksityisyyttään on yhä vaikeampi suojata, kun henkilötietoja kerätään myös laitetasolla. Mitä tuotteita katseltiin tai tilattiin ja mihin käyttäjät reagoivat esimerkiksi tykkäyksin tai palautetta jättämällä ovat rahanarvoista tietoa esimerkiksi myyjille ja mainostajille. Käyttäjien henkilötietoja kerätään hyvin laajasti eri digitaalisista palveluista kuten verkkosivuilta ja esimerkiksi sosiaalisesta mediasta ja peleistä (Sitra, 2020).

Smith (1993) mukaan tietosuojan merkitys ja kuluttajien huoli omista henkilötietojen käsittelystä ovat olleet jyrkässä kasvussa 90-luvun alusta lähtien, kun henkilötiedot ovat toimineet kaupankäynnin maksuvälineenä. Henkilötietojen kerääminen ja hyödyntäminen mullisti tavan käydä kauppaa kuluttajien kanssa, jonka myötä uudet liiketoimintamallit lähtivät nopeaan kasvuun. Tietosuojan huono taso ja sen myötä tapahtuneiden julkisten tapahtumien myötä huoli omista henkilötiedoista herätti kuluttajat vaatimaan valtiotason puuttumista yksityisten organisaatioiden toimintaan. (Milberg, Smith & Burke, 2000.) Tietosuojalla pyritään varmistamaan luonnollisten henkilöiden yksityisyys ja riittävä suoja henkilötietojen keräämisen ja käsittelyn yhteydessä. Yksi suurimmista muutoksista henkilötietojen käsittelyyn ja yksityisyyden suojaan liittyen on EU:n yleinen tietosuoja-asetus, joka on ollut 25.5.2018 lähtien sovellettavaa lainsäädäntöä jokaisessa unionin jäsenvaltiossa. Tietosuoja-asetusta sovelletaan myös EU:n ulkopuolella, jos käsittelyn piiriin kuuluu EU:n kansalaisen henkilötietoja.

Tietosuoja-asetus korvasi aiemmin voimassa olleen henkilötietodirektiivin (95/46/EY), joka oli ollut voimassa vuodesta 1995. Suomessa direktiivin perusteella on säädetty Henkilötietolaki (523/1999), joka kumottiin 1.1.2019 Tietosuojalailla (1050/2018). Direktiivin tarkoitukset turvata sisämarkkinoiden toiminta ja taata yksilön perusoikeudet ja suojata yksilöä ovat edelleen keskiössä yleisessä tietosuoja-asetuksessakin, mutta teknologian kehitys oli ajanut direktiivistä ohi

eikä se taannut enää riittävää yksityisyyden suojaa nykyisen alustatalouden aikakaudella. Tietosuoja-asetuksen yhtenä tarkoituksena oli palauttaa kansalaisten luottamus palveluntarjoajiin ja kehittää sisämarkkinatoimintaa sekä yhtenäistää EU:n tietosuojalainsäädäntöä.

Yhtenä muutoksena tietosuoja-asetus velvoittaa muun muassa julkishallinnon organisaatioita ja viranomaisia, pois lukien lainkäyttötehtäviään hoitava tuomioistuin, nimittämään tietosuojavastaavan. Tietosuojavastaava toimii organisaation ensisijaisena neuvonantajana ja yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä kysymyksissä sekä valvoo tietosuojan toteutumista. Tietosuojavastaava on nimitettävä myös yksityisen sektorin organisaatioihin, joissa esimerkiksi henkilötietojen käsittely on luonteeltaan tai laajuudeltaan säännöllistä tai se käsittelyn piirissä on erityisryhmiin kuuluvia arkaluonteisia henkilötietoja.

Tietosuoja-asetuksen voimaantulon myötä jokaiseen kuntaorganisaatioon on viimeistään tullut velvoite nimittää tietosuojavastaava. Monissa kunnissa tietosuojavastaavan tehtävässä on ollut nimetty henkilö jo ennen tietosuoja-asetuksen voimaantuloa johtuen sosiaali- ja terveydenhuoltoalan erityislainsäädännöstä, jonka mukaan potilastietoja käsitellessä organisaation on tullut nimittää tietosuojavastaava. Organisaatiot, joilla on ollut nimetty tietosuojavastaava jo aiemmin ovat muun muassa sosiaali- ja terveyspalvelujen tarjoajat, Kela ja apteekit (Kuntaliitto 2018).

Tietosuojavastaavan aseman ja tehtävien suorittamisen mahdollistamiseksi on tietosuoja-asetuksessa asetettu erilaisia velvoitteita. Nimitettävältä tietosuojavastaavalta edellytetään esimerkiksi vahvaa tietosuojalainsäädännön tuntemista, jotta tehtävistä suoriutuminen on mahdollista. Tietosuoja-asetus ei kuitenkaan yksiselitteisesti velvoita tai ohjeista millaista osaamista tietosuojavastaavalla tulisi olla, joka asettaa omat haasteensa esimerkiksi kuntaorganisaatioille. Tietosuojavastaavalla tulisi olla riittävät resurssit toteuttaa työtehtäviään, mutta näitä resursseja ei ole määritelty tai ohjeistettu selkeästi. Riittävien resurssien määrittäminen ja tarjoaminen tietosuojavastaaville jää näin rekisterinpitäjien ja henkilötietojen käsittelijöiden vastuulle.

Tietosuoja-asetuksen resitaalissa 97 tarkennetaan, että julkishallinnon organisaatioiden, kuten kuntien tulee nimittää tietosuojavastaavan tehtävään sellainen henkilö, jolla on erittäin vahva tietosuojalainsäädännön ymmärrys ja kokemus käytännöstä. On selvää, että kuntaorganisaatio on haasteellinen ympäristö tietosuojavastaavalle johtuen sen laajasta tietojenkäsittelyn ympäristöstä ja moninaisuudesta. Tämä asettaa tietosuojavastaavan tehtävässä toimivalle monenlaisia osaamisvaatimuksia ja edellyttää kokemusta kuntaorganisaatiossa työskentelystä. Tietosuoja-asetus asettaa tietosuojavastaavan asemaa ja nimittämistä koskien vaatimuksia, jotka kuntaorganisaatioiden tulee huomioida tarkasti, jotta tehtävää voidaan hoitaa itsenäisesti ja riippumattomasti sekä työtehtävissä onnistuen. Tietosuoja-asetus ei kuitenkaan yksiselitteisesti ohjeista sektoreittain rekisterinpitäjiä ja henkilötietojen käsittelijöitä millaisia asioita heidän tulisi huomioida, kun tietosuojavastaava nimitetään.

Kelan Kanta-palvelut on usean vuoden ajan kyselytutkimuksin selvittänyt, miten Reseptikeskuksen asiakasorganisaatiot kuten esimerkiksi apteekit ja sosi-

aali- ja terveydenhuollon toimintayksiköt huolehtivat tietosuojan toteutumisesta. Tuorein vuoden 2019 tutkimus toteutettiin yhteistyössä tietosuojavaltuutetun toimiston ja Terveyden ja hyvinvoinnin laitoksen kanssa ja se keskittyy tietosuojan hallintaan organisaatiossa. Tutkimuksessa selvisi, että vastaajien edustamien organisaatioiden tietosuojan hallinta on suhteellisen hyvällä tasolla, mutta niissä on kuitenkin huomattavasti parannettavaa etenkin tietosuojavastaavan aseman ja tehtävien määrittämisessä. Tutkimuksessa havaittiin myös, että näissä organisaatioissa tietosuojan toteutumiselle ei ole varattu riittäviä resursseja ja joissain ei ole nimitetty lainkaan tietosuojavastaavaa. (Kanta 2019) Tutkimus antaa viitteitä, että etenkin tietosuojavastaavan tehtävien ja aseman määrittäminen voi olla haastavaa eri sektorien organisaatioissa. Vaikka tutkimuksessa todetaan tietosuojan hallinnan olevan suhteellisen hyvällä tasolla, siinä ei tutkita tietosuojavastaavien valmiuksia hoitaa tehtäviä, vaikka tehtävää hoitavan henkilön valmiuksilla voi olla vaikutuksia tietosuojan lopulliseen toteutumiseen. Kanta-palveluiden kaltaista tutkimusta ei ole tehty kuntien tietosuojavastaaville, mutta yleisellä tasolla tietosuojaan liittyvää kirjallisuutta on verrattain paljon. Aiemmassa kirjallisuudessa ei kuitenkaan ole kiinnitetty huomiota tietosuojavastaaviin tai heidän tehtävien hoidon kannalta keskeisiin tekijöihin kuten osaamiseen, henkilökohtaisiin valmiuksiin tai organisaation rooliin, jotka vaikuttavat merkittävästi tehtävässä onnistumiseen tahi miten tietosuoja lopulta toteutuu kuntaorganisaatioissa.

Tässä tutkimuksessa tavoitteena on selvittää, miten kuntaorganisaatioissa tietosuojavastaavan tehtävä on organisoitu ja millaista osaamista kuntien tietosuojavastaavilla tulisi olla, jotta työn tekeminen onnistuneesti olisi mahdollista. Tutkimuskysymykset ovat määritelty seuraavasti:

- Millaisia työelämätaitoja tietosuojavastaava työssään tarvitsee?
- Miten tietosuojavastaavan rooli tulee organisoida kuntaorganisaatiossa, jotta hän kykenee suorittamaan tehtävät vaatimusten mukaisesti?

Aihe-aluetta esitellään teoreettisessa viitekehyksessä, johon on haettu aineistoa tietosuoja-asetuksesta ja muusta soveltuvasta lainsäädännöstä sekä viranomaisten ohjeistuksista ja määräyksistä. Lainsäädännön lisäksi aineistoa on kerättyä aihepiirin kirjallisuudesta, joka käsittelee tietosuojan hallintaa ja kehittämistä sekä tietosuojavastaavan roolia ja tehtäviä organisaatioissa. Tutkimusongelmaan ja tutkimuskysymyksiin on pyritty vastaamaan laadullisen tutkimuksen keinoin suorittamalla eri kuntien tietosuojavastaaville teemahaastatteluita. Haastatteluiden vastaukset ja empiirisen osuuden tutkimustulokset ovat esitelty tutkimuksessa myöhemmin.

2. EU:n yleinen tietosuoja-asetus

Luvussa käsitellään tietosuoja-asetuksen taustaa, keskeisimpiä periaatteita ja rekisterinpitäjää koskevia uusia velvoitteita sekä tietosuojavastaavaa koskevia muutoksia.

2.1. Tietosuoja-asetuksen tausta

Smith (1993) mukaan yksityisyys ja yksilön oikeus omaan rauhaan ovat koko yhteiskunnan kannalta merkittäviä tekijöitä. Yksityisyys on yksilöiden suhteiden ja luottamuksen mahdollistaja, jonka vuoksi yksityisyyden suojan, eli tietosuojan, toteutuminen on yhteiskunnan näkökulmasta merkittävä kannustin. Täydellinen yksityisyys ei kuitenkaan ole vaihtoehto, sillä se estää yhteiskunnan toimintojen toteuttamisen. Suomi ym. (2018) mukaan yksityisyyden ja yhteiskunnan toimintojen mahdollistaminen edellyttää tietojen vaihtamista, mutta yksilöllä tulisi olla valta päättää tietojen käsittelyn laajuudesta, jotta yksityisyyden suojan tunne säilyy. Samanlaista tiedonvaihtoa käydään myös yritysten ja yksilöiden välillä. Yksilöt ja yritykset vaihtavat tietoa esimerkiksi kaupankäynnin yhteydessä. Siksi yrityksille on hyvin tärkeätä, että yksilöt luottavat ja valitsevat juuri heidät kumppanikseen. (Koskinen, Alapuranen, Heino & Lehtonen, 2012).

Dhillon, Oliveira ja Syed (2018) mukaan yksi keskeisimmistä ajureista yleisen tietosuoja-asetuksen taustalla oli luottamuspula henkilötietoja hyödyntäviin yrityksiin, joiden tuotot muodostuivat osittain tai pääasiallisesti yksilöiden henkilötiedoiksi luokiteltavien tietojen myynnistä, tietojen yhdistelystä ja analysoinnista. Toiminnasta puuttui läpinäkyvyys ja kohtuullisuus, joka lisäsi huolta ja vähensi merkittävästi yksilöiden kykyä tehdä päätöksiä. Erityisesti huolta aiheuttivat muun muassa toissijaiset käsittelytarkoitukset sekä luvaton pääsy tietoihin. (Smith, Milberg & Burke, 1996). Tämän vuoksi digitaalisien alustojen kuten verkkokauppojen käyttö oli tietoisille kuluttajille haastavaa ja osittain luottamuksen puute vähensi näiden käyttöä. Tietosuojasta tuli kilpailukykyä edistävä tekijä niille palveluntarjoajille, jotka ymmärsivät haastavan asetelman henkilötietojen hyödyntämisen ja yksityisyydensuojan välillä. Organisaatiot, jotka kontrolloivat omaa palveluntarjonnan ympäristöään sekä viestivät avoimesti ja läpinäkyvästi omista käytännöistään henkilötietojen käyttämisestä saivat luotettavan toimijan maineen, joka sai kuluttajien kiinnostuksen ja kulutuksen kasvamaan. (Karwatzki, Dytynko, Trenz & Veit, 2017.)

Lindqvistin (2018) mukaan EU:n direktiivin (95/46/EY) mukaiset periaatteet olivat ennen yleisen tietosuoja-asetuksen voimaantuloa edelleen kelvolliset, mutta velvoitteet tietojenkäsittelijöille ja rekisterinpitäjille eivät olleet pysyneet teknologian kehityksen mukana. Direktiivin velvoitteiden katsottiin olevan riittämättömät suojaamaan henkilöiden yksityisyyttä esimerkiksi erilaisia verkkopalveluita käytettäessä, sillä dataa kerättiin aiempaa enemmän ja sen käyttö ei

ollut riittävän läpinäkyvää käyttäjille. Tästä syystä yksilöiden luottamus yritysten toimiin henkilötietojen käsittelyssä ja yksityisyyden toteutumiseen oli alkanut hälventymään, joka haittasi liiketoiminnan kehitystä. Yksi tietosuoja-asetuksen EU:n alueen tietosuojalainsäädännössä oli myös hyvin paljon eroavaisuuksia, jota yleisellä tietosuoja-asetuksella pyrittiin yhdenmukaistamaan. Lisäksi asetuksen tavoitteina oli edistää eri maiden tietosuojaviranomaisten ja rekisterinpitäjien välistä kommunikointia. (Euroopan parlamentti ja Euroopan neuvosto 2016).

Hannisen, Laineen, Rantalan, Rusin ja Varhelan (2017) mukaan tietosuoja-asetus toi paljon uusia velvoitteita rekisterinpitäjille ja tietojenkäsittelijöille. Vaikka muutos oli iso, on tietosuoja-asetuksen kantavana ajurina riskiperusteisuus. Riskiperusteisuudella tarkoitetaan sitä, että rekisterinpitäjän tulee mitoittaa käsittelytoimien suojaustoimet käsittelyn laajuuden ja riskipitoisuuden mukaan ja niiden tulee olla tasapainossa rekisteröidyn oikeuksien ja vapauksien kanssa. Andreasson, Ylipartanen ja Koivisto (2017 s. 115-116) mukaan tällä tarkoitetaan, että laajamittaista, yksilöivää ja säännöllistä käsittelyä tulee suojata ja kontrolloida tarkemmin kuin harvemmin toistuvaa ja vähemmän yksilöivää käsittelyä. Näin säädetään tietosuojan investointitarpeita esimerkiksi pienen puutyöverstaan ja suuren työterveyspalveluita tarjoavan yrityksen välillä. Tietosuoja-asetus myös määrittelee erityiset tietoryhmät, joiden käsittelyssä tulee huomioida käsittelylle säädetyt velvoitteet sekä erityisesti käsittelyn tietosuoja. Näin eri alojen ja toimintojen rekisterinpitäjät ja tietojenkäsittelijät voivat arvioida tietosuojan hallinnan laajuutta ja suojaustoimien tarpeellisuutta sekä laajuutta oman toimintansa riskien näkökulmasta. (Andreasson, Riikonen & Ylipartanen 2019, s. 62-64).

2.2. Keskeiset periaatteet

Tietosuoja-asetuksen henkilötietojen käsittelyn keskeiset periaatteet ovat annettu artiklassa 5 ja periaatteita on määritelty tarkemmin asetuksen johdanto-osassa. Tietosuojaperiaatteita ei ole täysin uudistettu, vaan niitä on täydennetty ja tarkennettu tietosuojadirektiivistä 95/46/EY. Tietosuoja-asetuksen henkilötietojen käsittelyn periaatteita ovat:

- kohtuullisuus, läpinäkyvyys ja lainmukaisuus,
- käyttötarkoitussidonnaisuus,
- tietojen minimointi,
- täsmällisyys,
- säilytyksen rajoittaminen,
- eheys ja luottamuksellisuus.

Näiden lisäksi käsittelyn yhtenä periaatteena on myös rekisterinpitäjän osoitusvelvollisuus. Osoitusvelvollisuuden periaatteella tarkoitetaan sitä, että rekisterinpitäjä on velvollinen näyttämään toteen, että henkilötietojen käsittelyä on toteutettu periaatteiden edellyttämin tavoin. (Euroopan parlamentti ja Euroopan neuvosto 2016).

Hanninen ym. (2017) mukaan kohtuullisuuden, läpinäkyvyyden ja lainmukaisuuden periaatteen mukaisesti rekisterinpitäjältä edellytetään kaikessa henkilötietojen käsittelyssä kohtuullisuutta ja lainmukaisuutta sekä rekisteröidyn näkökulmasta läpinäkyvyyttä. Käsittelyn kohtuullisuutta tulisi arvioida rekisterinpitäjän toimesta ennen käsittelyn aloittamista, että voidaanko sitä toimintoa suorittaa kohtuullisesti ilman henkilötietojen käsittelyä. Lainmukaisuuden periaate velvoittaa, että käsittelyn laillisuus perustuu johonkin asetuksessa määriteltyihin perusteisiin, joita ovat esimerkiksi rekisteröidyn suostumus tai rekisterinpitäjän oikeutettu etu. Läpinäkyvyyden periaatteella korostetaan rekisteröidyn oikeuksia saada tietää henkilötietojensa keräämisestä ja käytöstä tai niiden käsittelijöistä sekä rekisterinpitäjän velvollisuuksista viestiä avoimesti ja ymmärrettävästi käsittelyn laajuudesta. (Voigt & von dem Bussche, 2017).

Henkilötietojen käsittelyn tulee toteutua nimenomaisesti ennalta määritettyä käyttötarkoitusta varten. Käyttötarkoitussidonnaisuudella tarkoitetaan, että rekisterinpitäjä ei voi kerätä henkilötietoja tai käsitellä niitä laajemmin kuin mitä on ennalta ilmoittanut. Käyttötarkoitussidonnaisuuden periaate on myös keskeisessä roolissa seuraavien kolmen henkilötietojen käsittelyn periaatteen toteutumisessa. (Voigt & von dem Bussche, 2017). Hannisen ym. (2017) mukaan käyttötarkoitussidonnaisuuden periaatteen tarkka huomioiminen ja tavoittelu mahdollistavat rekisterinpitäjälle helpomman työn seuraavan kolmen periaatteen, tietojen minimoinnin, täsmällisyyden sekä säilytyksen rajoittamisen, toteuttamiseksi. Tietojen minimoinnin periaatteella ei pyritä rajoittamaan rekisterinpitäjän tietojenkäsittelyn laajuutta tai säännöllisyyttä. Tietojen minimoinnin tavoitteena on rajoittaa tietojen keräämistä ja yhdistelyä mahdollisimman vähäiseksi, joilla on kuitenkin mahdollista päästä tavoiteltuun lopputulokseen. Henkilötietoja ei siis tule kerätä enempää kuin on välttämätöntä ja keräämisen tulee olla oikea-aikaista.

Hannisen ym. (2017) mukaan täsmällisyyden periaatteella velvoitetaan rekisterinpitäjää ja henkilötietojen käsittelijää huolehtimaan rekisteröityjen henkilötietojen oikeellisuudesta. Henkilötietojen ajan tasaisuudesta ja oikeellisuudesta tulee varmistua säännöllisin väliajoin ja havaitut virheet tulee oikaista ilman aiheettomia viivytyksiä. Rekisterinpitäjän tulee huolehtia tietojen oikeellisuudesta kaikin keinoin, joita voidaan pitää kohtuullisina. Rekisterin tietosisällön täsmällisyydellä pyritään huolehtimaan rekisteröidyn oikeuksista.

Voight ja Von dem Busschen (2017) toteavat, rekisterinpitäjien tulisi määritellä rekisteröityjen tunnistamiseen liittyville tiedoille elinkaaren ja säilytysajan, jonka päätteeksi poistetaan. Rekisteröityjen henkilötietoja ei tule säilyttää kauempaa kuin se on perusteltavissa laillisin perustein. Voight ja Von dem Busschen (2017) ehdottavat, että periaatteen toteutumisesta huolehtimiseksi rekisterinpitäjät implementoivat tekniset ja organisatoriset kontrollit, joilla huolehditaan hen-

kilötietojen oikea-aikaisesta tuhoamisesta. Tällaisia kontrolleja voi olla säännönmukaisesti toistuvat rekisterin katselmoinnit tai järjestelmään määriteltävä säilytysaika, jonka päätteeksi tiedot tuhoutuvat automaattisesti.
Hanninen ym. (2017) mukaan rekisterinpitäjää koskevan eheyden ja luottamuksellisuuden periaate tarkoittaa sitä, että rekisterinpitäjän tulee varmistua käsittelyn turvallisuudesta asianmukaisin teknisin ja organisatorisin menetelmin. Käsittelyn turvallisuudella tarkoitetaan muun muassa luvattoman tai lainvastaisen käytön estämistä sekä suojaamista tahattomalta häviämiseltä, tuhoutumiselta ja vahingoittumiselta.

2.3. Rekisterinpitäjää koskevat merkittävimmät muutokset

Tämän tutkimuksen kannalta on tärkeätä käsitellä niitä muutoksia, joita tietosuoja-asetus asetti rekisterinpitäjille, sillä niiden johdosta tutkimuksen aihe ja tutkimuskysymykset ovat aiheellisia ja ajankohtaisia. Tietosuoja-asetus oli globaalisti merkittävä muutos tietosuojalainsäädäntöön, mutta tässä tutkimuksessa käsitellään vain osa sen asettamista muutoksista. Muutokset käsitellään siitä näkökulmasta, miten ne vaikuttivat rekisterinpitäjien velvoitteisiin ja etenkin tietosuojavastaavien asemaan ja tehtäviin.

Ustaran ym. (2018, s. 74) mukaan tietosuoja-asetus määrittelee eri roolit sekä vastuut ja velvoitteet eri toimijoille, rekisterinpitäjälle ja henkilötietojen käsittelijälle, ja nämä roolit on tunnistettava ja määritettävä. Roolit perustuvat tosiasialliseen asemaan eikä niitä voida vaihtaa tai sopia tilanteen mukaan. Roolit vastaavat henkilötietodirektiivin (95/46/EY) mukaisia rooleja, mutta tietosuoja-asetuksen myötä nämä roolit, vastuut ja velvoitteet on sovittava kirjallisesti sopimuksessa. Rekisterinpitäjän on myös huolehdittava, että henkilötietojen käsittelijä toteuttaa tosiasiallisesti näitä sopimuksessa sovittuja toimenpiteitä ohjeistusten ja velvoitteiden mukaisesti. Ustaran ym. (2018, s. 349-350) painottavat myös, että mikäli henkilötietojen käsittelijä hyödyntää käsittelyssään alikäsittelijöitä, tulee käsittely olla hyväksytty rekisterinpitäjän toimesta ja alikäsittelijöiden kanssa olla sovittuna kirjallisesti vastuista ja rooleista, käsittelyn laajuudesta ja muista velvoitteista.

Ustaran ym. (2018, s. 195-197) mukaan henkilötietojen käsittelyn periaatteena, muista periaatteista eroavana funktionaalisena osana, on määritelty osoitusvelvollisuus. Osoitusvelvollisuus on myös asetettu yleisvelvoitteeksi artiklassa 24. Rekisterinpitäjän vastuulla on riskiperusteisesti toteuttaa ne organisatoriset ja tekniset toimenpiteet, joilla voidaan varmistua käsittelyn turvallisuudesta ja osoittaa rekisterinpitäjän toteuttaneen käsittelyssä rekisterinpitäjälle määritellyt velvoitteet. Rekisterinpitäjän velvoitteisiin kuuluu muun muassa tietosuojaa koskevien toimintaperiaatteiden määrittely ja toimeenpano. Näiden toimintaperiaatteiden voidaan katsoa olevan yksi tehokkaan tietosuojan varmistamisen sekä yksi osoitusvelvollisuuden merkittävimmistä kulmakivistä. (Korpisaari, Pitkänen & Lehtinen-Warma, 2018, s. 269-271.)

Hannisen ym. (2017) mukaan osoitusvelvollisuuden periaatteen toteutuminen edellyttää rekisterinpitäjiltä suunnitelmallista ja huolellista lähestymistapaa prosessien määrittelyyn ja dokumentointiin. Osoitusvelvollisuuden vuoksi rekisterinpitäjän tulisi pystyä todentamaan miten se on toteuttanut henkilötietojen käsittelyn periaatteita, tietosuoja-asetuksen velvoitteita ja miten organisaatiossa tietosuojan kokonaisuus on hallittu. Mikäli valvontaviranomainen, Suomessa Tietosuojavaltuutetun toimisto, katsoo, että henkilötietojen käsittelyn periaatteet eivät toteudu, tai rekisterinpitäjä on muuten toiminnassaan ollut huomaamaton tai tarkoituksellisesti välinpitämätön, on viranomaisella valtuudet antaa rekisterinpitäjälle esimerkiksi varoitus tai huomautus, määrätä käsittelykielto pysyvästi tai määräajaksi tai määrätä hallinnollinen sakko. Sakon suuruus on viranomaisen päätettävissä tapauskohtaisesti, mutta se voi olla enimmillään 20 miljoonaa euroa tai 4% organisaation globaalista liikevaihdosta.

Uutena tietosuoja-asetuksessa on myös rekisterinpitäjille asetettu 25 artiklassa velvoitteet sisäänrakennetusta ja oletusarvoisesta tietosuojasta. Ustaran ym. (2018, s. 202-203) mukaan sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa niitä organisatorisia ja teknisiä hallintamenetelmiä, joilla voidaan varmistua, että tietosuoja-asetuksen tuomat velvoitteet ja hyvän tietosuojan hallintatavan mukaiset toiminnot ovat huomioituna kaikessa henkilötietojen käsittelyssä. Sisäänrakennetulla tietosuojalla (privacy by design) tarkoitetaan tietosuojavelvoitteiden ja etenkin rekisteröityjen oikeuksien huomioon ottamista ennakoidusti esimerkiksi uusien tuotteiden tai palveluiden kehittämishankkeissa tai hankinnoissa. Vaikka näkökulma onkin tulevien prosessien, järjestelmien ja toimintojen suunnittelussa, henkilötietojen suoja tulisi toteuttaa myös nykyisissä henkilötietojen käsittelytoiminnoissa. Suunnittelussa olevien muutosten osalta henkilötietojen suoja tulee arvioida ja toteuttaa koko käsittelytapauksen elinkaaren ajaksi.

Ustaran ym. (2018, s. 203) mukaan oletusarvoisella tietosuojalla (privacy by default) tarkoitetaan tietosuojan- ja tietoturvallisuuden hallintamenetelmien ja tietosuojan periaatteiden toteutumista jokaisessa henkilötietojen käsittelytapauksessa. Oletusarvoisen tietosuojan toteutumisesta varmistuakseen rekisterinpitäjien tulisi pystyä arvioimaan käsittelytapauskohtaisesti riittävä tietosuoja sekä yleisen tietosuoja-asetuksen mukaisten henkilötietojen käsittelyn periaatteiden toteutuminen ja korjaamaan mahdolliset puutteet. Esimerkkinä oletusarvoisesta tietosuojasta voitaisiin katselmoida esimerkiksi fyysisen arkiston aineistoa. Aineistoa tulisi pystyä henkilötietojen osalta arvioimaan vuosittain sekä poistamaan arkistosta aineisto, jonka säilytysajan on määritellyt paikallinen erityislainsäädäntö, ja hävittämään aineisto asianmukaisesti turvallista hävittämistapaa noudattaen. (Ustaran ym. 2018, s. 203-206.)

Voight ja Von dem Busschen (2017) mukaan henkilötietojen käsittelyn eheydestä ja luottamuksellisuudesta huolehtiminen on artiklassa 5 määritelty yksi käsittelyä koskeva periaate, jonka mukaan rekisterinpitäjän ja käsittelijän tulee arvioida ja asettaa riittävät organisatoriset ja tekniset suojausmenetelmät henkilötietojen käsittelylle. Yleisessä tietosuoja-asetuksessa näitä suojaus- ja hallintamenetelmiä painotetaan artikloissa pääasiallisesti 24 (rekisterinpitäjän vastuu)

ja 32 (käsittelyn turvallisuus) sekä 28 (henkilötietojen käsittelijä), 33 (henkilötietojen käsittelyn tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle) ja 34 (henkilötietojen käsittelyn tietoturvaloukkauksesta ilmoittaminen rekisteröidylle). Kuvaukset kaikista organisatorisista ja teknisistä suoja- ja hallintamenetelmistä tulisi ylläpitää ajantasaisesti artiklan 30 mukaisessa seloste käsittelytoimista. (Tietosuoja-asetus 2016/679.)

Ustaran ym. (2018 s. 172-176.) mukaan yleinen tietosuoja-asetus edellyttää hyvää tietojen hallintatapaa sekä riittäviä suojausmenetelmiä, mutta ne eivät ole täysin ehdottomia. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee arvioida käsittelyn riskit ja perustaa riittävät ja asianmukaiset suoja- ja hallintamenetelmät tunnistettuihin riskeihin perustuen. Riskiperusteisuus tulisi arvioida käsittelytapauksittain ja arvioinnin tulosten perusteella asettaa käsittelylle riittävät suojaus- ja hallintamenetelmät kuten tietojen salaus liikkeessä ja levossa, pseudonymisointi ja anonymisointi sekä henkilöstön yleinen tietoisuus ja ohjeistus käsittelyn suojaamisesta. Mikäli käsittely on tavanomaista riskialttiimpaa kuten käsiteltävät tietoaineistot sisältävät erityisluokkiin kuuluvia henkilötietoja, tai käsittely koskee laajoja joukkoja rekisteröityjä, käsittelylle tulisi suorittaa tietosuoja-asetuksen artiklan 35 mukainen vaikutustenarviointi. (Hanninen ym., 2017.)

Voight ja Von dem Busschen (2017) mukaan artiklan 35 mukainen vaikutustenarviointi on riskienhallintamenetelmä, joka on tarkoitettu erityisesti rekisteröidyn oikeuksien turvaamiseksi, mutta sillä voidaan arvioida mitä tahansa käsittelytoimenpidettä ja niiden vaikuttavuuksia, kuten riskejä, sekä niiden hallintamenetelmiä. Tyypillisesti vaikuttavuudenarviointi tehdään osana projektinhallintaa, hankintoja tai prosessien uudistuksia, joilla voi olla vaikutuksia henkilötietojen käsittelyyn tai rekisteröityjen oikeuksiin ja vapauksiin. Toteutuessaan riskit saattavat aiheuttaa rekisteröidyille aineettomia tai aineellisia vahinkoja, jotka voivat johtaa muun muassa taloudellisiin tai mainetta koskeviin haittoihin. Vaikutustenarviointia tehtäessä rekisterinpitäjän tulee konsultoida organisaation nimettyä tietosuojavastaavaa tai tarvittaessa jopa valvontaviranomaista sekä huomioida erityisesti käsittelytoimien laajuus, asiayhteys, luonne ja tarkoitukset. Andreasson ym. (2019, s. 72-75) mukaan arvioinnin lopputuotoksena rekisterinpitäjällä tulisi olla dokumentoitu kuvaus käsittelytoimista, niiden tarkoituksista sekä arvio tarpeellisuudesta ja oikeasuhteisuudesta sekä riskeistä, jotka voivat realisoituessaan vaikuttaa haitallisesti rekisteröidyn oikeuksiin ja vapauksiin. Mikäli arvioinnissa havaitaan, että riskit eivät ole tasapainossa tai hyväksyttävissä, ne tulee käsitellä asianmukaisesti ja tarvittaessa pienentää ennen kuin käsittelyä voidaan aloittaa. Jos riskit eivät käsittelystä huolimatta ole hyväksyttävissä, rekisterinpitäjän tulisi pystyä luopumaan henkilötietojen käsittelystä tai siirtämään sen aloitusta, kunnes valvontaviranomaiselta on saatu asiasta virallinen päätös.

Tietosuoja-asetuksen artikloissa 33 ja 34 asetetaan rekisterinpitäjille vaatimus ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle sekä loukkausta koskeville rekisteröidyille. Hanninen ym. (2017) määrittelevät tietoturvaloukkauksen tapahtumaksi, jonka seurauksena on käsittelyn piiriin kuuluvien henki-

lötietojen lainvastainen tai tahaton luvaton käyttö, muuttaminen tai tietojen katoaminen, luovutus tai pääsy. Ustaran ym. (2018, s. 176-178) mukaan ilmoitus tietoturvaloukkauksesta oli merkittävä uudistus tietosuojalainsäädäntöön, sillä sen johdosta rekisteröidyt saavat varmemmin tiedon tarpeesta suojata omia henkilötietojaan väärinkäytösten varalta ja valvontaviranomaiset osaavat ilmoitusten perusteella kohdentaa rekisterinpitäjien ohjausta ja valvontaa. Tietoturvaloukkausten ilmoittaminen valvontaviranomaisille tulee tehdä 72 tunnin sisällä loukkauksen havainnoinnista. Mikäli havainnon tekee henkilötietojen käsittelijä, tarpeellinen ilmoitus rekisterinpitäjälle tulee tehdä ilman aiheetonta viivytystä. Annetussa aikarajassa toimiminen on rekisterinpitäjille usein haastavaa, sillä ilmoitukseen tulee sisällyttää kuvaus tietoturvaloukkauksesta. Kuvauksessa on arvioitava todennäköiset seuraukset ja ilmoitettavia tietoja ovat muun muassa rekisteröityjen ryhmät ja henkilötietotyypit sekä näiden arvioidut lukumäärät. Ilmoituksessa on myös kuvattava tietoturvaloukkauksen johdosta toteutetut tai ehdotetut suojaustoimenpiteet sekä mahdolliset toimenpiteet loukkauksen vaikutusten rajaamiseksi. Rekisterinpitäjän tulee myös nimittää yhteyshenkilö valvontaviranomaiselle, jolta saa tarvittaessa lisätietoja. Mikäli rekisterinpitäjä on nimittänyt tietosuojavastaavan, hän toimii yhteyshenkilönä. Kaikkia tietoja ei tarvitse ilmoittaa kerralla, vaan ilmoitusta voidaan täydentää myöhemmin, kun rekisterinpitäjän tutkinnasta selviää lisätietoja. Rekisterinpitäjän tulee dokumentoida kaikki tietoturvaloukkaukset. Mikäli rekisterinpitäjän arvioinnin mukaan tietoturvaloukkauksella voivat aiheuttaa korkean riskin rekisteröidyn oikeuksiin tai vapauksiin on rekisterinpitäjän ilmoitettava rekisteröidyille artiklan 34 vaatimusten mukaisesti. (Andreasson ym., 2019, s. 171-172.)

Tietosuoja-asetus määrittelee tietosuojan erityisasiantuntijan roolin, tietosuojavastaavan, jonka tehtävänä on toimia rekisterinpitäjän apuna tietosuojan hallintaan, kehittämiseen ja vaatimuksenmukaisuuteen liittyvissä asioissa. Tietosuojavastaavan asema ja tehtävät on asetettu artikloissa 37-39. WP29 (2016) näkemyksen mukaan kaikkien organisaatioiden ei tarvitse nimittää tietosuojavastaavaa, vaikka se olisikin suositeltavaa. Organisaatiot voivat vaihtoehtoisesti nimittää tietosuojasta vastaavan henkilön, jonka asemaa ja tehtäviä eivät sido tietosuoja-asetuksen vaatimukset.

2.4. Tietosuojavastaava

Andreasson ym. (2019, s. 92-93) mukaan tietosuojavastaava on rekisterinpitäjien ja henkilötietojen käsittelijöiden pääasiallinen neuvonantaja ja ensisijainen yhteyshenkilö liikekumppaneille, viranomaisille ja rekisteröidyille tietosuojaan liittyvissä kysymyksissä. Erityisasiantuntijan roolissa tietosuojavastaava muun muassa valvoo tietosuojan toteutumista, neuvoo organisaation työntekijöitä ja johtoa sekä osallistuu henkilötietojen käsittelyprosessien ja kehityshankkeiden suunnitteluun ja toteutukseen.

2.4.1. Tietosuojavastaavan nimittäminen

EU:n yleisen tietosuoja-asetuksen mukaan tietosuojavastaava tulee nimittää seuraavissa tilanteissa:

- rekisterinpitäjä on viranomainen tai julkishallinnon organisaatio, lukuun ottamatta tuomioistuimia;
- rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtäviin kuuluu käsittelytoimet, jotka vaativat laajamittaista tai säännöllistä rekisteröityjen seurantaa; ja/tai
- rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtäviin kuuluu erityisten henkilötietoryhmien liittyvää tietojenkäsittelyä taikka rikostuomioita ja rikkomuksia koskevaa käsittelyä.

Rekisterinpitäjän ollessa viranomainen tai julkishallinnon organisaatio, kuten kuntien, on nimitettävä tietosuojavastaava. WP29 (2016) määrittää ydintehtävien käsittelyn olevan toimintaa, jotka ovat välttämättömänä osana niitä toimenpiteitä, joilla organisaatio voi saavuttaa asettamansa tavoitteet. Laajamittaisella käsittelyllä voidaan WP29 (2016) mukaan tarkoittaa esimerkiksi numeerista määrää rekisteröityjä tietystä otannasta henkilöitä tai henkilötietojen määrää tai niiden pysyväistä luonnetta ja pitkää säilytysaikaa. Rekisteröityjen seurantaa WP29 (2016) tarkentaa koskemaan Internetissä evästeiden ja analytiikan keinoin toteutettavan seurannan kuten kiinnostuksen kohteiden keräämistä ja analysoimista sekä esimerkiksi sitä seuraavan suoramarkkinoinnin. Seuranta ei ole kuitenkaan rajattu verkossa tapahtuvaan seurantaan, vaan se voi olla muun muassa paikkatietojen perusteella tehtävää seurantaa.

Vaikka edelliset ehdot ei suoraan täyttyisikään WP29 (2016) mukaan tietosuojavastaavan nimittäminen voi olla kannattavaa, koska tietosuojalla voidaan edistää merkittävästi liiketoiminnan kilpailuetua. Toimiva tietosuojavastaava on myös yksi osoitusvelvollisuuden kulmakivistä. WP29 (2016) täydentää, että organisaatiot voivat nimittää vapaaehtoisesti tietosuojavastaavan, mutta tällöin artikloissa 37-39 tietosuojavastaavan nimittämistä, asemaa ja tehtäviä koskevat velvoitteet tulevat sovellettavaksi. Mikäli organisaatiorakenne on konserni, joka koostuu useista yhtiöistä, tietosuojavastaava voi palvella jokaista yhtiötä sillä edellytyksellä, että tietosuojavastaava on helposti tavoitettavissa jokaisesta toimipaikasta. Lambert, (2017, s. 48-49) painottaa, että tietosuojavastaavan ei kuitenkaan tarvitse olla sijoitettu fyysisesti tiettyyn paikkaan, kunhan tavoitettavuus toteutuu turvallisin keinoin kuten vaikka sähköpostitse tai puhelimitse. Tietosuojavastaavan suositellaan olevan sijoitettuna EU:n alueella, mutta jos organisaatiolla ei ole toimipaikkaa EU:ssa tämä ei ole kuitenkaan välttämätöntä. Tietosuojavastaavan yhteystiedot tulee myös aina ilmoittaa valvontaviranomaiselle.

WP29 (2016) päätelmän mukaan tietosuojavastaavan tavoitettavuudessa korostetaan organisaation sisäistä tietoisuutta tietosuojavastaavan olemassaolosta ja yhteystiedoista sekä minkälaisissa tehtävissä häntä voidaan hyödyntää.

Tavoitettavuudella tarkoitetaan myös paikallista kielitaitoa, jotta tietosuojavastaava voi palvella ymmärrettävästi rekisteröityjä sekä tarvittaessa avustaa valvontaviranomaisia tehokkaasti. Tietosuojavastaavan rooli voidaan täyttää organisaation sisältä, tai sitä varten voidaan perustaa uusi rooli organisaatioon, mutta tietosuojavastaavan roolia ja tehtäviä voidaan toteuttaa myös palvelusopimuksen perusteella. Ustaran ym. (2018, s. 211-212) painottavat, että kaikissa edellä mainituissa kohdissa tulee huomioida tietosuojavastaavan nimittämistä, asemaa ja tehtäviä koskevat velvoitteet. Tilanteessa, jossa tehtävien hoitaminen perustuu palvelusopimukseen, tietosuojavastaavan roolia voi hoitaa yksi tai useampi henkilö. Tietosuojavastaavan tueksi voidaan nimittää tiimi henkilöitä, jotka kaikki suorittavat tietosuojavastaavan tehtäviä. Mikäli tietosuojavastaavan tukena on tiimi, jokaisen tiimiin kuuluvan henkilön tulee täyttää tietosuojavastaavan nimittämistä, asemaa ja tehtäviä koskevat vaatimukset. Ustaran ym. (2018, s. 211-213) mukaan tietosuojavastaavan roolin ulkoistaminen voi useissa tilanteissa olla hyödyllistä, jos organisaation sisällä ei ole taustansa puolesta sopivaa henkilöä tai organisaation on vaikea houkutella riittävän kokeneita osaajia ulkoisella rekrytoinnilla. Tietosuojavastaavan roolia ulkoistaessa tulee kiinnittää riittävää huomiota tietosuojavastaavan, tai tiimin perehdyttämiseen, jotta voidaan varmistua kompetenssivaatimusten vaatimusten täyttymisestä.

Tietosuojavastaavan nimittämisessä tulee huomioida nimitettävän henkilön ammatillinen pätevyys ja kompetenssit, etenkin hyvä tietosuojalainsäädännön ymmärrys sekä kyky suoriutua artiklassa 39 määritellyistä tehtävistä. WP29 (2016) mukaan tietosuojavastaavan kompetensseja tulee arvioida organisaatiokohtaisesti ja sen mukaan, kuinka laajasti sen toiminnassa käsitellään henkilötietoja ja kuinka kompleksi käsittely-ympäristö on. Tietosuojavastaavan kompetensseissa kuitenkin korostuvat sovellettavan tietosuojalainsäädännön ja siihen vaikuttavan erityislainsäädännön tunteminen ja soveltamiskyky sekä organisaation liiketoimintaa ja siihen liittyvän tietojen käsittely-ympäristön tunteminen. Lisäksi tietosuojavastaavan tulisi ymmärtää riittävällä tasolla informaatioteknologiaa sekä tietoturvallisuutta. Kansainvälisissä organisaatioissa korostuu myös tietosuojavastaavan kielitaito ja viestintätaidot korostuvat, jotta hänellä on kyvykkyys viestiä niin rekisteröityjen kuin valvontaviranomaisenkin kanssa ymmärrettävästi. Tietosuojavastaavalla tulisi myös olla kyvykkyydet kehittää organisaation tietosuoja- ja tietoturvakulttuuria ja yleistä tietoisuutta. Andreasson ym. (2019, s. 98-99) listaavat, että tietotaitojen lisäksi tietosuojavastaavalla tulisi olla ajantasaiset kyvyt etsiä lisää tietoa ja soveltamaan sitä toisaalta yksilötasolla, mutta myös yhteisötasolla. Lisäksi tietosuojavastaavalla tulisi olla henkilökohtaisia ominaisuuksia kuten halu tarttua haasteisiin, positiivinen asenne ja sopeutumiskykyä. Henkilökohtaisten ominaisuuksien, kompetenssien ja työkokemustaustan lisäksi uskottavan erityisasiantuntijan asemaan pääsemiseksi vaikuttaa myös koulutustausta ja ammatilliset käytännöt.

2.4.2. Tietosuojavastaavan asema

Tietosuoja-asetus määrittää tietosuojavastaavan asemalle kuusi vaatimusta, jotka organisaation johdon tulee huomioida, kun tietosuojavastaavaa nimitetään. Lambert (2017, s. 68) painottaa, että tietosuojavastaavan roolin tulee olla itsenäinen ja riippumaton eikä häntä tule ohjata tai ohjeistaa tehtävässä toimiessaan tai työtehtäviä suorittaessaan. Tällaisia tehtäviä voi olla esimerkiksi henkilötietojen käsittelyn lainmukaisuuden valvonta, organisaation tai valvontaviranomaisen konsultointi tai lainsäädännön tulkintaan liittyvät päätökset. Lisäksi tietosuojavastaavalla on salassapitovelvollisuus työtehtäviä suorittaessaan ja tehtävässä saamaansa tietoihin liittyen. Riippumattoman asemansa puolesta tietosuojavastaavalla on mahdollisuus raportoida suoraan ylimmälle johdolle. Organisaatiolla ja tietosuojavastaavan työnantajalla ei ole oikeutta rangaista tai erottaa häntä työtehtävien hoitamisen vuoksi. Rankaisemiseksi voidaan katsoa myös uhkaukset, mikäli ne liittyvät työtehtävien hoitamiseen. (Andreasson ym., 2019, s. 95.)

Tietosuojavastaavaa nimittäessään organisaation, rekisterinpitäjän tai tietojen käsittelijän, tulee varmistaa ja huolehtia, että tietosuojavastaavaa osallistetaan riittävän ajoissa kaikkiin henkilötietojen käsittelyyn ja tietosuojaan liittyviin kysymyksiin ja asioihin. Näin tietosuojavastaava voi tarjota aikaisessa vaiheessa neuvoja sekä valvoa, että myös rekisteröityjen oikeudet tulevat huomioiduksi asianmukaisesti. Rekisterinpitäjän tulisi huolehtia, että tietosuojavastaava osallistetaan vähintään silloin, kun tietojen käsittely-ympäristössä tapahtuu muutoksia kuten tietojärjestelmävaihdoksia tai prosessimuutoksia. Tietosuojavastaava voi olla sitä mieltä, että muutoksia ei voida viedä käytäntöön esimerkiksi korkean riskin vuoksi. Mikäli johto ei ole samaa mieltä tietosuojavastaavan kanssa ja toteuttaa muutoksia neuvoja vastaan, tulisi tällaiset päätökset dokumentoida osoitusvelvollisuuden periaatteen mukaisesti. (WP29 2016.) Andreasson ym. (2019, s. 95-96) toteavat teoksessaan, että mahdollisimman aikainen osallistuminen esimerkiksi uuden palvelun tai tietojärjestelmän hankintaan mahdollistaa tietosuojavaatimusten huomioimisen määrittelyvaiheesta lähtien. WP29 (2016) ohjeistaa myös, että tietosuojavastaava olisi hyvä kutsua säännöllisesti johdon tapaamisiin. Tietosuojavastaavaa tulisi konsultoida aina myös tietoturvaloukkausten myötä aloitettaviin selvityksiin. Lisäksi rekisteröidyillä pitäisi olla kyky muodostaa yhteys tietosuojavastaavaan suoraan, jolloin he voivat pyytää neuvoa tai ohjeistusta. Tietosuojavastaavan yhteystiedot tulee julkaista erillisenä vaatimuksena tietosuoja-asetuksessa artikloissa 13 ja 14, joissa määritellään vaatimukset rekisteröidyille informoinnista henkilötietojen käsittelystä.

Organisaation johdon tulee olla sitoutunut tietosuojatyöhön ja tukea tietosuojavastaavaa määrittelemällä riittävät resurssit, jotta tietosuojavastaavan tehtävät ovat mahdollista hoitaa. Riittävällä resursoinnilla tarkoitetaan WP29 (2016) mukaan muun muassa riittävästi aikaa, rahallista tukea ja työtehtävien tehokkaaseen hoitamiseen liittyvät työvälineet ja työtilat sekä tarpeen mukaan myös muita henkilöresursseja. Andreasson ym. (2019, s. 102.) painottavat, että tietosuojavastaavan tärkeimpiä resursseja ovat jatkuvan kouluttautumisen mahdolli-

suus ja aika. Erityisesti aika on tärkeätä sen vuoksi, että se on rajallista ja erityisasiantuntijan työ on usein pirstaleista, jonka vuoksi syvällinen ajatustyö ja keskittyminen voivat keskeytyä avunannon tai kokousten vuoksi. Aikaa pitäisi varata etenkin tietosuojatyön kehitysvaiheessa, jolloin tekemistä on enemmän. Lisäksi tietosuojavastaavalle tulisi pystyä tarjoamaan riittävästi koulutusta. Mikäli organisaatio ei itse pysty tarjoamaan koulutusta, tulee tietosuojavastaavalle tarjota mahdollisuus osallistua ulkopuolisen palveluntarjoajan tarjoamaan koulutukseen. Johdon pitää myös varmistaa, että tietosuojavastaavalle tarjotaan riittävä pääsy sellaisiin tietoihin, joita hän tehtäviä hoitaessaan tarvitsee. Tällaista pääsyä saattaa edellyttää henkilötietojen käsittelyssä hyödynnettävät tietojärjestelmät, joihin tietosuojavastaava tarvitsee käyttöoikeudet esimerkiksi käytönvalvontaa tehdessään. (Andreasson ym., 2019, s. 96.)

WP29 (2016) mukaan tietosuojavastaavalla voi olla muitakin työtehtäviä ja rooleja kuin tietosuojavastaavalle määritellyt tehtävät. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee huolehtia, että nämä muut tehtävät tai roolit eivät aiheuta eturistiriitoja tai uhkaa tietosuojavastaavan roolin riippumattomuutta. Muut roolit tai tehtävät eivät saa suoraan olla sellaisia, joissa tietosuojavastaava joutuisi tekemään päätöksiä henkilötietojen käsittelyn tarkoituksiin tai keinojen määrittelyyn liittyen. Tällaisia rooleja tyypillisesti on esimerkiksi ylimmän johdon roolit kuten talousjohtaja, henkilöstöjohtaja, tietohallintojohtaja tai toimitusjohtaja. Roolit ja työtehtävät sekä niistä mahdollisesti muodostuvat eturistiriidat ovat organisaatio- ja joskus jopa tilannekohtaisia. Tästä syystä organisaatioiden olisikin suositeltavaa listata ne roolit ja tehtävät, joissa eturistiriitoja voi syntyä sekä laatia tarvittaessa ohjeet, joilla voidaan välttää tällaiset tilanteet. Joissain organisaatioissa eturistiriitoja voi muodostua kaikissa muissa rooleissa, joten tietosuojavastaavalla ei voisi olla käytännössä muuta roolia. Tällaisissa tilanteissa voi olla suositeltavaa ulkoistaa tietosuojavastaavan rooli palveluntarjoajalle. (Andreasson ym., 2019, s. 95-96.)

2.4.3. Tietosuojavastaavan tehtävät

WP29 (2016) mukaan tietosuoja-asetuksen artikla 39 määrittää tietosuojavastaavalle ne tehtävät, jotka hänelle tulee olla vähintään vastuutettuna. Tietosuojavastaavan yksi tärkeimmistä tehtävistä on valvoa organisaation tietosuojalainsäädännön vaatimustenmukaisuutta. Toisena korostettuna tehtävänä on neuvoa ja ohjeistaa organisaatiota sekä sen työntekijöitä henkilötietojen tietojenkäsittelyyn liittyvissä asioissa. Lisäksi tietosuojavastaava antaa tukea tietosuoja-asetuksen artiklan 35 mukaisen tietosuojan vaikutustenarvioinnin tekemisessä ja valvoo sen toteutusta sekä arvioi lopputuotoksen. Tietosuojavastaavan tehtäviin kuuluu myös yhteyshenkilönä toimiminen valvontaviranomaiselle ja avunanto tietosuojaan liittyvissä asioissa. Andreasson ym. (2019, s. 92-93) listaavat tietosuoja-asetuksessa velvoitettujen lisäksi tietosuojavastaavan tehtäviksi myös osoitusvelvollisuutta tukevan dokumentaation laatimisen sekä sen elinkaaresta huolehti-

misen. Sen lisäksi tietosuojavastaavan tehtäviin kuuluu tietosuojariskien arviointiin osallistuminen ja tunnistettujen riskien hallintakeinojen, kuten korjaavien toimenpiteiden suorittamisen valvonta. Tietosuojavastaavan tulisi myös seurata ilmoitusvelvollisuuden toteutumista tai huolehtia siitä itse sekä tukea rekisteröityjen oikeuksien toteuttamisessa. Lisäksi tietosuojavastaavan tehtäviin kuuluu tietosuojatietoisuuden kasvattaminen ja henkilöstön kouluttaminen laaditun ohjelman mukaisesti. (Andreasson ym., 2019, s. 92-94)

Tietosuojavastaavan tehtäviin kuuluvan vaatimustenmukaisuuden arviointi ja valvonta on hyvin moninainen ja vaativa tehtävä riippuen henkilötietojen käsittelytoimenpiteiden laajuudesta, säännöllisyydestä ja arkaluontoisuudesta sekä rekisteröityjen määrästä. WP29 (2016) mukaan tietosuojavastaava valvoo tietosuojan toteutumista prosessien, käytännön käsittelyn ja laadittujen asiakirjojen ja muun dokumentaation näkökulmasta. Andreasson ym. (2019, s. 125-128) lisäävät vielä, että tietosuojavastaavan tulisi suorittaa käytönvalvontaa ja lokivalvontaa, jotka ovat teknisiä suoritteita ja vaativat riittävää teknistä osaamista. WP29 (2016) jatkaa, että valvontatehtävissä onnistuminen edellyttää sitä, että käsittelytoimet, prosessit ja käytännöt ovat kuvattu ja ohjeistettu riittävällä laajuudella. Tietosuojavastaavan tulisi kerätä mahdollisimman paljon tietoa ja laaja ymmärrys henkilötietojen käsittelystä, tunnistaa käsittelytoimet ja dokumentoida ne. Tämän jälkeen ne voidaan analysoida tarkemmin ja arvioida ovatko käsittelytoimet soveltuvan lainsäädännön kanssa vaatimustenmukaisia. Mikäli käsittelytoimet eivät ole vaatimustenmukaisia, tietosuojavastaavan tulee raportoida puutteet toimivalle johdolle ilman aiheetonta viivytystä. Lisäksi tietosuojavastaavan tulee valvoa yleisen tietosuoja-asetuksen ja muun tietosuojalainsäädännön velvoitteiden toteutumista, mutta seurata myös toimialan soveltuvan lainsäädännön kehittymistä ja arvioida sen muutosten vaikutuksia tietosuojan hallintaan, jotta valvontatehtävässä voidaan onnistua. (WP29, 2016; Andreasson ym., 2019, s. 93-94).

Tietosuojavastaavan tehtävissä ja roolissa voi olla eroavaisuuksia, jos organisaatiossa on nimettynä esimerkiksi tietosuojajohtaja (Chief Privacy Officer) tai muita tietosuojaan liittyviä rooleja. Fusaran (2000) mukaan tietosuojajohtaja on vastuussa tiedonhallinnan strategian suunnittelusta tietosuojatavoitteiden osalta. Hän myös vastaa tietosuojapolitiikoiden sekä toimintamallien suunnittelusta ja toimeenpanosta sekä käytäntöön viemisestä. Lisäksi tietosuojajohtaja raportoi muulle toimivalle johdolle ja ylimmälle johdolle tietosuojan tilasta.

Andreasson ym. (2019, s. 67) mukaan aina, kun rekisteröityjen oikeuksiin tai vapauksiin kohdistuu riskejä, tai tietojenkäsittely-ympäristön muutostilanteissa, kuten uusia järjestelmiä hankkiessa, tietosuojavastaavan tulee arvioida tarve tietosuoja-asetuksen mukaisen vaikutustenarvioinnin tekemiselle. Mikäli käsittely vaatii vaikutustenarviointia tietosuojavastaavan tulee olla mukana ohjeistamassa ja valvomassa sen tekemistä. WP29 (2016) listaa seuraavat asiat, mitä tietosuojavastaavan tulee arvioida vaikutustenarviointia tehdessä:

- onko vaikutustenarviointi tarpeellinen,
- mitä metodologiaa käyttäen se tulisi toteuttaa,

- tulisiko se tehdä itse vai käyttäen ulkopuolista apua,
- mitä suojakeinoja tai kontrolleja tulisi sisällyttää käsittelyyn, jotta siitä tulisi turvallista rekisteröidyille ja huomioisi heidän oikeutensa, ja
- onko vaikutustenarviointi tehty oikein ja perustuuko johtopäätökset tosiasioihin ja ovatko ne vaatimustenmukaiset.

Andreasson ym. (2019, s. 68) täydentävät listausta sillä, että tietosuojavastaava voi konsultoida valvontaviranomaista niissä tilanteissa, jolloin käsittelyn riskejä ei saada pienennettyä, tai organisaatio ei osaa itse arvioida tilannetta riittävällä laajuudella. Käsittelyä ei tule aloittaa ennen kuin valvontaviranomainen on antanut tilanteeseen hyväksynnän. Ustaran ym. (2018, s. 208-209) mukaan tietosuojan vaikutustenarviointi tulisi aina dokumentoida asianmukaisesti ja siinä tulisi olla sisällytettynä vähintään:

- järjestelmällinen kuvaus käsittelyn tarkoituksista ja käsittelytoimenpiteistä sekä kaikki ne käsittelytoimet, joiden lainmukaisuus perustuu rekisterinpitäjän oikeutettuun etuun,
- käsittelyn tarpeellisuuden arviointi,
- rekisteröityjen vapauksiin ja oikeuksiin kohdistuva riskien arviointi ja niiden suojauskeinojen ja tietoturvakontrollien määrittely, joilla käsittelyä suojataan.

Tietosuojavastaava toimii yhteyshenkilönä valvontaviranomaiselle edustamansa organisaation henkilötietojen käsittelyyn liittyvissä asioissa ja tekee heidän kanssaan yhteistyötä. Yhteistyötä edellyttävä tilanne voi liittyä esimerkiksi artiklan 36 mukaiseen ennakkokuulemiseen tai artiklan 31 mukaiseen yhteistyöpyyntöön. Tilanteita, joissa ennakkokuulemista voitaisiin soveltaa ovat esimerkiksi rekisteröityjen tekemät ilmoitukset oikeuksien tai vapauksien rikkomisesta, havaituista puutteista tai tietoturvaloukkauksen yhteydessä. Ennakkokuulemisessa korostuu osoitusvelvollisuuden yleisvelvoitteen merkitys, joka edellyttää organisaatiot dokumentoimaan muun muassa tietosuojan vaikutustenarvioinnit, seloste käsittelytoimista, tietosuojapolitiikan sekä ohjeistukset ja muun mahdollisen dokumentaation kuten johdon tekemät päätökset tietosuojaa koskien. Tällaisella dokumentaatiolla organisaatio pystyy ennakkokuulemistilanteessa osoittamaan ne toimet, mitä on tehty rekisteröityjen oikeuksien ja vapauksien toteuttamiseksi ja miten ne on otettu huomioon tietosuojan johtamismallissa tai johdon päätöksissä. (Ustaran ym., 2018, s. 204-207).

Rekisterinpitäjä ja henkilötietojen käsittelijät voivat määrittää tietosuojavastaavalle myös muita tehtäviä. Andreasson, Koivisto ja Ylipartanen (2016, s. 139-141) täydentävät, että tietosuojavastaavan muita tehtäviä voivat olla muun muassa henkilötietorekisterien käytönvalvonta. Käytönvalvonta on osa tietosuojan toteutumisen valvontaa ja sitä toteutetaan esimerkiksi säännöllisillä käyttölokien katselmoinneilla ja käyttöoikeuksien ajantasaisuuden valvonnalla. Tietosuojavastaava voi olla käytönvalvonnan lisäksi mukana määrittelemässä tieto-

turvan hallintaan liittyviä asioita oman osaamisen mukaan. Tietoturvallisuudessa korostuvat muun muassa käyttövaltuushallinta. Käyttövaltuushallinnalla tarkoitetaan niitä periaatteita ja käytännön toimia, joilla käyttäjille määritellään rooliin perustuvat oikeudet ja laajuudet käyttää tietojärjestelmiä sekä käsitellä niiden tietosisältöä kuten muun muassa henkilötietoja. (Andreasson, Koivisto & Ylipartanen, 2014, s. 47-49).

Andreasson ym. (2016, s. 151-155) mukaan tietosuojavastaavan tehtäviin voidaan lisäksi sisällyttää organisaation sisäinen ja ulkoinen raportointi sekä viestintä tietosuoja-asioissa. Raportointiin kuuluu oleellisten mittareiden kuten rekisteröityjen ja valvontaviranomaisten selvitys- ja tietopyyntöjen määrä, tietoturvaloukkausten määrä ja koulutettujen työntekijöiden seuranta. Raportointia tehdään ensisijaisesti oman organisaation johdolle, mutta näitä tunnuslukuja voidaan liittää myös ulkoiseen raporttiin kuten esimerkiksi vuosittain julkaistavaan tietotilinpäätökseen. Tietotilinpäätös on vapaaehtoinen, mutta hyvin laajalti käytössä oleva keino raportoida rekisteröidyille ja sidosryhmille esimerkiksi kuinka henkilötietoja käsitellään organisaatiossa. Se on myös hyvin tehokas keino toteuttaa osoitusvelvollisuuden periaatetta. Rekisterinpitäjä ja henkilötietojen käsittelijä määrittävät tietosuojavastaavan resurssit, joten tästä syystä tietosuojavastaavan ei tarvittaessa ole pakollista olla kokoaikainen rooli. Tällä perusteella tietosuojavastaava voi hoitaa myös täysin muita tehtäviä, kunhan ne eivät aiheuta eturistiriitoja tai vaaranna tietosuojavastaavan riippumattomuutta. (Andreasson ym. 2019, s. 94-95).

3. Tietosuojan hallinta

Tietosuojan kehittämistä ja hallintaa ohjaavat ne vähimmäisvaatimukset, jotka lainsäädäntö, määräykset ja ohjeistukset organisaatioille asettaa. Vaatimuksia voi olla muualtakin kuin lainsäädännöstä, kuten toimialan käytännöistä, asiakkaiden tai muiden sidosryhmien vaatimuksista ja odotuksista sekä erilaisista vapaaehtoisista sertifioitavista hallintajärjestelmistä tai laatuohjelmista. Rose (2013) mukaan tieto on organisaatiolle merkittävä ja erottamaton osa sen omaisuutta ja sitä tulisi hallita huolellisesti. Tiedon hallinnalla tarkoitetaan niitä hallintamalleja ja -menetelmiä, joilla varmistetaan informaation ja datan eheys, ajantasaisuus ja luotettavuus. Tiedon hallinnan merkitys on kasvanut merkittävästi, sillä informaation ja datan perusteella tehdään päätöksiä, jotka vaikuttavat organisaation tulevaisuuteen ja tästä syystä jokaisen organisaation tulisi varautua ja turvata oma informaationsa luomalla tietoturvallisuuden ja tietosuojan hallintamalli. Abdullah, Labuschagne ja Young (2016) mukaan taas organisaatioiden omistajaohjauksen tulisi määritellä, ei pelkästään informaation suojaksi, vaan koko liiketoiminnan suojaamiseksi hallintaohjelma. Koko liiketoiminnan kattavaan hallintaohjelmaan määritellään varautumisen näkökulmasta hallinnolliset ja johtamiseen (governance) liittyvät vaatimukset, riskienhallinnan (risk) vaatimukset kuin vaatimustenmukaisuuden (compliance) velvoitteet. GRC-ohjelman tavoitteena on valvoa ihmisiä, prosesseja ja teknologiaa ja näin hallita tehokkaasti riskejä ja olla vaatimustenmukainen eri velvoitteiden, lainsäädännön sekä määräysten ja ohjeiden kanssa.

Rose (2013) mukaan tietoturvallisuuden ja tietosuojan hallintamallin tarkoituksena on luoda informaation suojaksi riittävät keinot ja menetelmät, joiden perusteella voidaan luottaa siihen, että tieto on saatavissa, ajantasaista ja se on luotettavaa. Smith ym. (2000) ovat samaa mieltä, että organisaation tietosuojalle on suunniteltava ja toteutettava viitekehys, joka toimii sisäisesti myös hallinnollisena käyttäytymismallina. Malli toimii ohjaavana ja määrittelevänä kehyksenä kaikkeen henkilötietojen keräämiseen, ja käsittelyyn liittyvään toimintaan henkilötietojen elinkaaren ajan. Viitekehyksen määrittelyä ohjaavat soveltuva lainsäädäntö sekä rekisteröityjen huolenaiheet ja organisaation omat tarpeet.

Smith ym. (1996) tunnistivat ja jakoivat huolenaiheet neljään kategoriaan, joita ovat tarpeettoman tiedon kerääminen, toissijainen käyttötarkoitus ilman rekisteröidyn suostumusta, luvaton käyttö ja virhetilanteet. Huoli tarpeettoman tiedon keräämisen taustalla oli käyttötarkoitukseen liittymättömien henkilötietojen kerääminen. Toissijainen käyttötarkoitus ilman rekisteröidyn suostumusta viittaa tilanteisiin, joissa organisaatio käsittelee itse keräämiään henkilötietoja sellaiseen käyttötarkoitukseen, johon rekisteröity ei ole antanut suostumustaan tai ei ole tietoinen käsittelystä. Esimerkkinä toissijaisesta käyttötarkoituksesta voi olla esimerkiksi tietojen myynti eteenpäin tai erilaisten tietojen yhdistely ja mahdollisten profiilien muodostaminen sellaisiin tarkoituksiin, joista ei ole sovittu rekisteröidyn kanssa. Kolmanneksi kategoriaksi määriteltiin luvaton käyttö, jolla

tarkoitetaan organisaation henkilötietojen käsittelyn käyttöoikeuksia ja niiden oikeellisuutta. Käyttöoikeuksilla rajataan katselu- ja muokkausoikeudet tietoihin ja oletusarvoisesti niiden tulisi olla rajattu vain sellaiseen käyttöön, jonka tarve perustuu työrooliin. Rekisteröidyn huolena ovat ne tilanteet, joissa organisaation käyttöoikeudet eivät ole myönnetty rooliperusteisesti, vaan heidän tietoihinsa pääsisi käsiksi myös oikeudettomat henkilöt. Viimeiseksi kategoriaksi tunnistettiin henkilötietojen käsittelyyn liittyvät virhetilanteet. Virhetilanteilla viitataan joko tahattomiin tai tahallisiin virhetilanteisiin, joissa käsittely ei vastaa organisaation lupausta tai käsittelyä, johon rekisteröity ei ole antanut suostumustaan.

Myöhemmässä huolenaiheita käsittelevässä tutkimuksessa Smith, Dineva ja Xu (2011) tunnistivat, että tietosuojaa ja yksityisyyttä koskeviin huolenaiheisiin vaikuttivat erityisesti rekisterinpitäjien ja henkilötietojen käsittelijöiden harjoittamat tekniset käsittelytoimet sekä teknologian nopea kehittyminen. Tutkijat jakoivat huolenaiheet kuuteen eri luokkaan, joita olivat muun muassa datan louhinta ja profilointi, valvonta ja seuranta sekä kaikkialla läsnä oleva teknologia ja tietojenkäsittely. Muita vaikuttavia tekijöitä olivat suoramarkkinointi, verkkokaupat ja Internet, lisääntynyt asiakasviestintä ja alati muuttuvat liiketoimintamallit Internetissä. Lisääntyneet huolenaiheet eivät johdu kuitenkaan pelkästään organisaatioiden muuttuvista liiketoimintamalleista ja henkilötietojen riippuvuuksista niihin, vaan lisääntyneistä tietomurtojen määrästä. Smith ym. (2000) mukaan rekisteröityjen huolenaiheiden ja soveltuva lainsäädäntö ohjaavat viitekehyksen kehitystä ja luovat perustan organisaation tietosuojan viitekehykselle sekä toiminnan parantamiselle. Viitekehyksen kehityksen ajurina pitäisikin siis toimia paitsi muuttuva lainsäädäntö, asiakkaiden huolenaiheet ja oikeudet, myös organisaation omat tarpeet sekä sisäinen toimintakulttuuri.

Ustaran ym. (2018, s. 172-176) mukaan yleinen tietosuoja-asetus ei vaadi täydellistä käsittelyn tietosuojaa tai tietoturvaa, mutta sen tulee perustua toimialan hyviin käytäntöihin sekä käsittelyn riskiperusteisuuteen. Riskiperusteisuus tulisi arvioida käsittelytapauksittain ja arvioinnin tulosten perusteella asettaa käsittelylle riittävät suojaus- ja hallintamenetelmät kuten tietojen salaus siirrossa ja levossa, pseudonymisointi ja anonymisointi sekä henkilöstön yleinen tietoisuus ja ohjeistus turvallisesta käsittelystä sekä henkilötietojen suojaamisesta käytännön toiminnassa. Näin saadaan aikaiseksi käsittelyn riskiperusteisuuden kanssa suhteessa oleva hallintamalli.

3.1. Tietosuojan hallintamalli

Merrick ja Ryan (2019) kehottavat teoksessaan organisaatioita aloittamaan hallintamallin rakentamisen soveltuvan lainsäädännön tunnistamisella sekä riskin hyväksymiskyvyn määrittämisellä. Soveltuvan lainsäädännön tunnistamisen jälkeen organisaation tulisi laatia tietoturvallisuuden ja tietosuojan politiikat sekä nimittää tietosuojasta vastaavan henkilön, kuten esimerkiksi tietosuojavastaavan. Politiikassa tulisi määritellä organisaatioon pääasialliset henkilötietojen kä-

sittelyn periaatteet sekä niitä tukevien prosessien linjaukset, vastuut ja velvollisuudet sekä raportointi ja seuranta. Kesan, Hayes ja Bashir (2013) mukaan organisaatiolle on tärkeätä myös määritellä henkilötietojen käsittelylle ja hyödyntämiselle periaatteet. Nämä periaatteet julkaistaan ja ne toimivat ikään kuin lupauksena asiakkaille ja muille sidosryhmille siitä miten ja miksi henkilötietoja käsitellään ja kuinka niitä suojataan. Periaatteet voidaan määritellä tietosuojapolitiikan muodossa, joka myös jalkautetaan organisaatioon käsittelytoiminnan perustaksi. Näin tietosuojalle muodostuu ikään kuin toimintaa säätelevä viitekehys, joka koostuu organisaation tarpeista, lainsäädännöstä ja asiakaslupauksesta. Organisaation oman toiminnan mukaan voi olla perusteltavaa myös julkaista tietosuojapolitiikka esimerkiksi organisaation verkkosivuilla. Linden, Khandelwal, Harkous ja Fawaz (2019) tunnistivat omassa teoksessaan tietosuojapolitiikan julkistamisella ja sen sisällöllä olevan luottamusta parantavia tekijöitä. Julkaistulla politiikalla voidaan herättää rekisteröityjen luottamus tai parantaa olemassa olevaa luottamusta entisestään. Luottamuksella havaittiin olevan vaikutuksia erilaisten palveluiden käyttämiseen kuten esimerkiksi verkko-ostojen suorittamiseen, tai palveluun rekisteröitymiseen ja hyödyntämiseen. Niiden organisaatioiden, joilla oli olemassa tietosuojapolitiikka ja viestivät siitä käyttäjille avoimesti, tarjoamia palveluita käytettiin useammin kuin niitä, joilla ei ollut politiikkaa tai eivät viestineet siitä. Tietosuojapolitiikassa tulisi olla selkeästi ilmaistu rekisteröityä mahdollisesti kiinnostavia asioita kuitenkin niin, että lainsäädännölliset vaatimukset tulevat huomioiduksi. (Wu, Huang, Yen & Popova, 2012.) Linden ym. (2019) esittävät analyysissaan, että ulkoisen politiikan tulisi sisältää vähintään seuraavat asiat: henkilötietojen keräämiseen liittyvät tiedot, kolmansien osapuolten tiedonkeruu ja tietojen käyttäminen, kuinka rekisteröity voi itse vaikuttaa tietojen keräämiseen sekä käyttöön, keräävät ja käsittelevät osapuolet, tietojen suojauskeinot, tiedon pääsyn, muokkauksen ja poistamisen mahdollisuudet, tiedon elinkaari sekä politiikkaan liittyvät mahdolliset muutokset. Näiden lisäksi siihen voidaan määritellä muita asioita, kuten osapuolten yhteystiedot.

Merrick ja Ryan (2019) jatkavat, että tietosuojapolitiikan jälkeen määritellään eri prosesseja ja laaditaan organisaation käyttöön dokumentteja, joihin kuuluvat rekisteröityjen oikeuksiin ja vapauksiin liittyvän dokumentaation, kuten käsittelyyn liittyvän informoinnin, laadinta ja julkaisu. Dokumentaatioon kuuluu myös rekisteröityjen oikeuksien toteuttamiseen liittyvien prosessien suunnittelu ja kuvaaminen. Merrick ja Ryan (2019) kehottavat myös selvittämään ja kuvaamaan henkilötietojen keräämiseen, käsittelyyn ja säilyttämiseen liittyvät käytännöt ja dokumentoimaan ne yhdeksi asiakirjaksi. Lisäksi tulisi selvittää kaikki nykyiset organisatoriset ja tekniset tietoturvakäytännöt, joilla suojataan tietoja sekä arvioimaan näiden riittävyys. Viimeisenä dokumentaatioon liittyvänä huomiona he kehottavat parantamaan toimittaja- ja sopimushallintaa. Toimittaja- ja sopimushallinnalla tarkoitetaan eri kumppanien kanssa tehtävää yhteistyötä, hankintoja tai muita sopimuksia, joihin kuuluvat mahdolliset henkilötietojen käsittelyn ulkoistamiset tai tietojen luovutukset ja niihin kuuluvia hallintamenetelmiä. Sopivia hallintamenetelmiä eri sopimuksiin voivat olla asianmukaiset henkilötietojen käsittelyn sopimukset tai sopimusliitteet sekä toimittajien arvioinnit ja auditoinnit tai muut riskienhallintakeinot. Neljäntenä kohtana Merrick ja Ryan

(2019) listaavat poikkeamanhallintaan sekä tietomurtojen varalle laadittavan prosessin ja siihen liittyvän dokumentoinnin. Poikkeamanhallinnan prosessi nopeuttaa erilaisten poikkeamien tunnistamiseen, rajoittamiseen ja palautumisen nopeuttamiseen liittyviä toimintoja ja menetelmiä. Tällä myös luodaan valmiuksia oikean tilanteen varalle, jolloin nämä toiminnot tulee pystyä toteuttamaan selkeästi ja oikea-aikaisesti. Viidentenä kohtana myös poikkeamanhallintaan osaksi kuuluvana toimintona on viestintästrategian laatiminen ja vastuuttaminen sekä muutoshallintaan liittyvien käytäntöjen sopiminen. Muutoshallinnalla tarkoitetaan organisaation sisäisiä käytäntöjä, millä huolehditaan esimerkiksi politiikoiden ja ohjeiden päivittämiseen liittyvää viestintää ja muutosten jalkauttamista käytäntöön. Viimeisenä kohtana he listaavat jatkuvan parantamisen käytännön. Jatkuvalla parantamisella tarkoitetaan säännöllistä riskiarviointia, oman toiminnan itsearviointeja sekä puuteanalyyseja, joilla pystytään havainnoimaan erilaisia parantamiskohteita hallintamallista. Nämä voivat olla prosessitasolla tai yksittäisiä kontrollipisteitä, joita pyritään havainnoimaan, joilla hallintakeinoja pystytään kehittämään paremmaksi. Merrick ja Ryan (2019) painottavat, että jatkuva parantaminen on toistuva prosessi, joka toistuu erilaisten harjoitusten myötä säännöllisesti.

Swartz, Da Veiga ja Martins (2019) mukaan tietosuojan hallintamalliin kuuluu paljon muutakin Merrick ja Ryan (2019) listaamat asiat. Swartz ym. (2019) jakavat tutkimuksessaan hallintamallin neljään pääluokkaan, jotka koostuvat yhteensä neljästätoista (14) alaluokasta. Pääluokat ovat organisaation sitoutuminen ja johtaminen, politiikat ja toimintamallit, tietosuojaohjelma ja kontrollit sekä jatkuvat arvioinnit ja toiminnan parantaminen. He lisäävät, että yksi tietosuojaohjelmaan ja kontrolleihin kuuluva alaluokka on henkilöstön tietoisuuden aktiivinen kasvattaminen ja säännöllinen kouluttaminen. Toiseksi tietosuojaohjelman ja kontrollien alaluokaksi he tunnistivat, että organisaation ulkopuolisia asiantuntijoita tulee hyödyntää säännöllisesti tietosuojan hallintamallin auditointiin ja arviointiin.

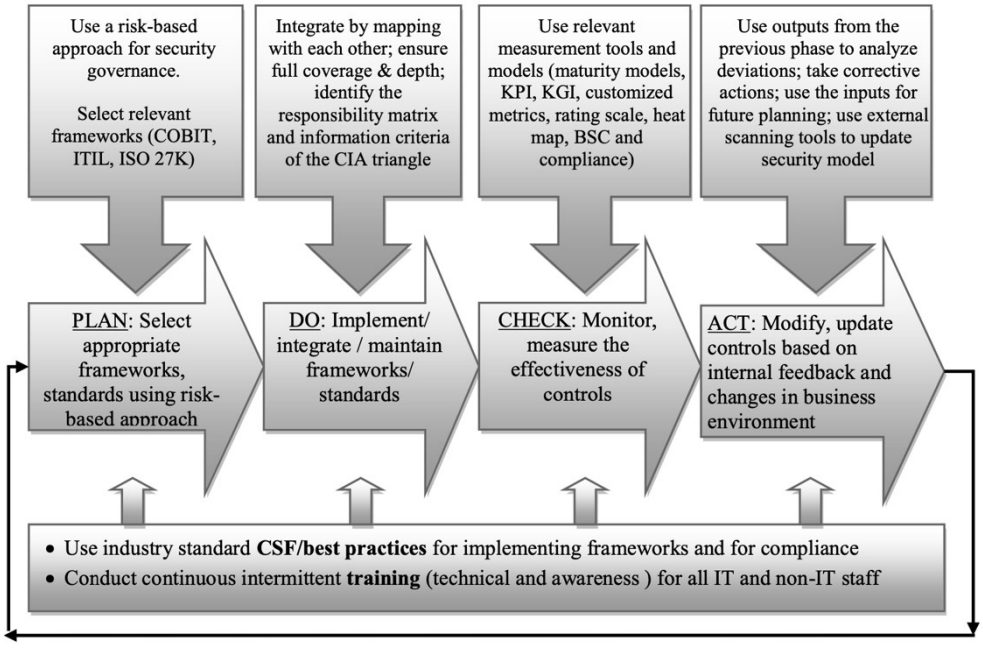
Abdullah ym. (2016) määrittelemään hallintaohjelmaan mukaan tietosuojan lisäksi vaatimustenmukaisuuteen (compliance) kokonaisuuteen kuuluu erottamattomana osana tietoturvallisuus ja lainsäädännölliset vaatimukset. Tietoturvallisuudelle tulee määritellä oma viitekehyksensä, jolla varmistutaan riittävästä tietoturvallisuuden tasosta, joka parhaiten tukee myös tietosuojan toteutumista organisaatiossa. Ustaran ym. (2018, s. 181-183) mukaan liiketoiminnan tietopääoman kriittisyys vaikuttaa siihen, millainen tietoturvallisuuden viitekehys tulee määrittää. Tietoturvallisuuden kehittäminen tulee olla suhteessa liiketoiminnan riskien kanssa. Tietoturvallisuuden kehittämisessä voidaan tukeutua täysin tai soveltuvin osin alan parhaisiin käytänteisiin kuten ISO 27000 -sarja, PCI-DSS- ja NIST -viitekehykset. Näiden viitekehysten lisäksi tietoturvallisuusalan asiantuntijaryhmät julkaisevat säännöllisesti uusia malleja, käytäntöjä sekä ohjeistuksia, joista tunnettuja ovat muun muassa Cloud Security Alliance (CSA) ja Information Security Forum (ISF).

3.2. Hallintamallin toimeenpano, arviointi ja kehittäminen

Organisaatiomuutokset ja uusien käytäntöjen jalkauttaminen voi olla haastavaa etenkin suuremmissa organisaatioissa. Nicho (2018) on teoksessaan vertaillut erilaisia lähestymistapoja toimintatapojen muuttamiseksi ja tietoturvallisuuden hallintamallien käyttöönottamiseksi. Hän havaitsi, että niin sanottu jatkuvan kehittämisen PDCA-malli sekä riskiperusteinen lähestyminen olivat hyväksyttävämpiä tapoja toteuttaa tällainen hanke. Riskiperusteisessa tavassa tunnistetaan organisaation toimintaan kohdistuvia ja jatkuvuutta uhkaavia riskejä ja kehitetään toimintaa niiden perusteella. Riskiperusteisessa lähestymistavassa haetaan nopeita ratkaisuita kustannustehokkaasti, esimerkiksi kontrollien asettamista tunnistettuihin kehityskohteisiin. Hayden (2009) jatkaa, että riskiperusteinen lähestymistapa säästää resursseja ja on nopeampi tapa reagoida organisaatioon kohdistuviin vaatimuksiin. Tämä ei kuitenkaan poissulje sitä, että organisaation tulee seurata myös viitekehyksen kokonaisvaltaista kehittämistä, sillä riski- ja kontrolliperusteinen lähestyminen voivat jättää aukkoja monikerroksiseen turvallisuuteen. Tätä varten Nicho (2018) ehdottaa teoksessaan PDCA-mallia, jolla pystytään arvioimaan tehtyjä toimenpiteitä ja niiden tehokkuutta ja tarvittaessa parantaa toimintaa. Nicho (2018) jakaa PDCA -mallin neljään jatkuvaan vaiheeseen, joissa ensimmäisessä Plan (suunnittele) -vaiheessa valitaan viitekehys, joka sopii liiketoimintaan ja vastaa olemassaoleviin riskeihin parhaiten. Seuraavaksi Do (toteuta)-vaiheessa jalkautetaan viitekehyksen vaatimukset käytäntöön ja seuraavaksi Check (arvioi)-vaiheessa arvioidaan tehtyjen toimenpiteiden tehokkuutta esimerkiksi erilaisten mittareiden avulla. Viimeisessä Act (toimi)-vaiheessa tunnistetaan Check-vaiheen poikkeamat ja toteutetaan korjaavat toimenpiteet. Tämän jälkeen prosessi käynnistetään uudestaan ja arvioidaan tehtyjen toimenpiteiden riittävyyttä tai seuraavia kehityskohteita. Työssä voidaan käyttää tarvittaessa myös ulkopuolista, kuten konsulttien apua, jotka pystyvät arvioimaan puolueettomasti ja riippumattomasti kontrollien ja prosessien tehokkuutta (Swartz ym., 2019).

Zhang, Yuan ja Qi (2011) arvioivat myös teoksessaan, että PDCA -mallia voidaan hyödyntää osana organisaation tietoturvallisuuden riskienhallintaa. He painottavat, että tietoturvallisuuden kontekstissa erityisesti Check-vaiheen jatkuva valvonta ja monitorointi sekä korjaavien toimenpiteiden merkitys korostuu. Act-vaihe sulautuu Check-vaiheeseen ja kehittäminen perustuu toiminnan ja kontrollien jatkuvalle arvioinnille. Prosessi toimii muuten vastaavasti, eli Plan-vaiheessa suunnitellaan tarpeellisten kontrollien toteutus ja Do-vaiheessa saatujen kehitystoimenpiteiden jalkauttamisen jälkeen käynnistyy heti Check-vaiheen arviointi ja mittaaminen. Act-vaiheessa perinteisesti tehtävälle koko hallintamallin itsearvioinnille ei näin jää tarvetta, mutta arviointi ja hallintamallin tehokkuuden valvonta on kuitenkin osa prosessia. Taulukossa 1. on kuvattu PDCA-malli ja eri vaiheisiin kuuluvia tehtäviä.

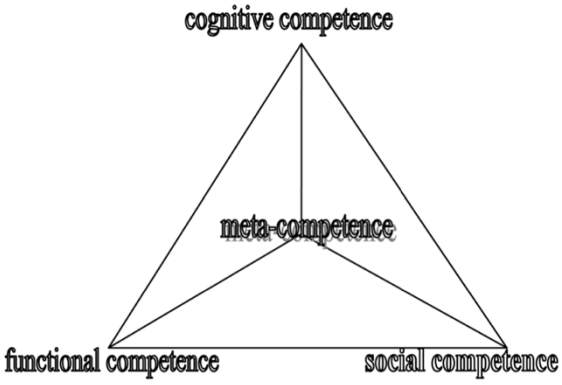
Kuvio 1: PDCA-malli Nichon (2018) mukaan



3.3. Asiantuntijoilta vaadittavat kompetenssit

Van Toorn, Cahalane, D'Ambra ja Cecez-Kecmanovic (2019) mukaan kompetenssit ovat niiden tietojen ja taitojen yhdistelmä, jota työelämässä tarvitaan hyvien lopputulosten saavuttamiseksi. Kompetenssit eivät rajoitu pelkästään osaamiseen, työelämän tietoihin tai taitoihin, vaan siihen kuuluvat myös henkilön persoonaan liittyviä tekijöitä. Van Toornin ym. (2019) tunnistivat tutkimuksessaan, että kompetenssi koostuu muun muassa taidoista, suoriutumisesta työssä, tiedoista ja kokemuksesta, itsetietoisuudesta, luonteenpiirteistä, motivaatiosta, asenteesta ja motiivista sekä sosiaalisuudesta. Henkilön kompetensseja pystytään mittaamaan ja arvioimaan sekä myös kehittämään kouluttautumalla. Le Deist ja Winterton (2005) painottavat, että kompetenssi ei ole vain joukko taitoja, joilla täytetään työelämän vaatimukset, vaan niihin luokitellaan myös luonteeseen ja persoonaan kuuluvia tietoja ja taitoja. Näihin luokitellaan esimerkiksi uuden tiedon etsiminen ja omaksuminen sekä halu oppia uutta. Analyysissaan he tulivat tulokseen, että kompetenssit muodostuvat eri osa-alueista, joihin kuuluvat kognitiiviset kompetenssit, toiminnalliset kompetenssit ja sosiaaliset kompetenssit, jotka ovat esitettynä kuviossa 2.

Kuvio 2: Kompetenssien osa-alueet Le Deisin ja Wintertonin (2005) mukaan



Tietosuoja-asetus määrittää tietosuojavastaavalle kompetenssivaatimuksia, mutta ne liittyvät hänen rooliinsa kuuluvien tehtävien suorittamiseen. Tehtävissä ei oteta kantaa hallintamallin rakentamiseen tai kehittämiseen, jotka voivat kuitenkin olla tietosuojavastaavan vastuualueella. Monfared, Benslimane ja Yang (2018) tunnistivat tutkimuksessaan tietosuoja-asiantuntijan kompetenssivaatimuksia. Viisi tärkeintä kompetenssia tietosuoja-asiantuntijalle olivat: tietosuojaohjelman ylläpitäminen ja kehittäminen, organisaation nykytila-arvioinnit ja tietosuojan vaikutustenarviointien tekeminen, organisaation datan suojakeinojen määrittäminen, tietosuojan hallintamallin kehittäminen ja jalkauttaminen sekä tietosuojaan liittyvien politiikkojen jalkauttaminen. Muita tunnistettuja taitoja olivat tietosuojariskien arviointi ja hallinta, henkilöstön tietosuojan tietoisuuden kasvattaminen ja kouluttaminen sekä tietojärjestelmien käytön ja organisaation vaatimustenmukaisuuden valvonta. Tietosuoja-asiantuntijoilta usein odotettiin ja toivottiin myös erilaisia ammatillisia sertifikaatteja todisteeksi omasta osaamisestaan. Kolme useimmin toistunutta sertifikaattia olivat Certified Information Privacy Professional (CIPP), Certified Information Systems Security Professional (CISSP) ja Certified Information Systems Auditor (CISA).

Lee, Bagchi-Sen, Rao ja Upadhyaya (2010) havaitsivat omassa tutkimuksessaan hyvin samankaltaisia vaatimuksia myös tietoturva-asiantuntijoille. Viisi tärkeintä tietoturva-asiantuntijan kompetenssia olivat tietoturvariskien arvioimien, palvelu- ja järjestelmätoimittajien sekä asiakkaiden kanssa toimiminen, työntekijöiden kouluttaminen ja tietoisuuden kasvattaminen, organisatoristen hallintakeinojen kuten politiikoiden ja ohjeistusten laatiminen ja jalkauttaminen sekä tutkimus- ja kehittämistoiminta, johon kuuluu esimerkiksi kryptografia ja päätelaitteiden hallinta. Kymmenen tärkeimmän taidon joukossa olivat myös hallintamallin sekä siihen kuuluvien kontrollien luominen ja jalkauttaminen. Lee ym. (2010) tutkimuksessa myös erilaiset compliance -vaatimukset sekä lainsäädännöllinen osaaminen olivat tietoturva-asiantuntijoiden osaamisvaatimuksissa, mutta niitä ei arvostettu yhtä korkealle kuin tietoturvaan liittyvää osaamista.

4. Tutkimusmenetelmät

Luvussa esitetään tutkimuksen läpivienti aloittamalla laadullisen tutkimuksen valinnalla, jatkamalla tutkimusmenetelmän valintaan ja sen suorittamiseen. Luvun loppupuolella käsitellään tutkimustulosten analysointiin liittyvät menetelmät.

4.1. Laadullinen tutkimus

Tutkimus on toteutettu laadullisena, empiirisenä tutkimuksena haastatellen henkilökohtaisesti eri kuntien tietosuojavastaavia. Laadullisessa tutkimuksessa tutkimuksen kohteena voi olla oikea elämä, oikean elämän ilmiöt ja kohteet, joita selvitetään ja tutkitaan kokonaisvaltaisella tutkimusotteella. Laadulliselle tutkimukselle on tyypillistä niiden tutkimusmenetelmien valitseminen, joilla saadaan tutkittavien näkökulma ja kokemukset selville. Esimerkkejä näistä menetelmistä ovat muun muassa osallistuva havainnointi, ryhmähaastattelu ja teemahaastattelu sekä dokumenttien ja tekstien diskursiiviset analyysit. (Hirsjärvi, Remes & Sajavaara, 2009.)

4.2. Teemahaastattelu ja haastatteluiden toteutus

Tässä tutkimuksessa aineistonkeruumenetelmänä on käytetty teemahaastattelua, jonka teemat ja apukysymykset on muodostettu olemassa olevan lainsäädännön, kirjallisuuden ja tietosuojaa koskevan tutkimuksen perusteella. Eri tavalla toteutetut haastattelut ovat systemaattinen tutkimusmenetelmä ja tapa kerätä tietoa suorassa vuorovaikutustilanteessa tutkittavan kanssa. Tutkimusmenetelmänä haastattelu on joustava tapa kerätä aineistoa se mahdollistaa verkostoitumisen tutkittavan kanssa. Teemahaastattelu on strukturoidun ja strukturoimattoman haastattelun välimuoto. Teemahaastattelua käytettäessä haastattelun teemat ovat mietitty etukäteen, mutta tutkimustilanne mahdollistaa joustavuuden esimerkiksi kysymysten esittämisen muodon ja järjestyksen kanssa toisin kuin strukturoidussa haastattelussa. Strukturoimaton, eli avoin haastattelu muistuttaa enemmän keskustelua, sillä aihepiirejä ei ole rajattu ja keskustelun aiheetkin voivat muuttua haastattelutilanteen aikana (Hirsjärvi ym., 2009 s. 204–209.) Menetelmäksi valittiin teemahaastattelu, jotta haastateltavan kertomus ja siitä kerättävä aineisto ei jäisi liian suppeaksi. Toisaalta avoimessa haastattelussa olisi ollut haasteellisempaa ohjata haastattelutilannetta siten, että siinä keskityttäisiin tutkimuskysymysten kannalta oleellisiin tekijöihin.

Laadullisessa tutkimuksessa tutkittavat kohteet valitaan yleensä tarkoituksenmukaisesti satunnaisotantojen sijaan (Hirsjärvi ym., 2009, s. 160-162.) Tässä

tutkimuksessa haastateltavaksi valittiin tutkimustavoitteen ja tutkimuskysymysten perusteella kuntien tietosuojavastaavia. Tutkimuksessa olisi voitu haastatella myös esimerkiksi kuntien ylintä johtoa ja kerätä heiltä aineistoa tietosuojavastaavan nimittämiseen ja tehtävän organisoimiseen liittyen. Tämän katsottiin kuitenkin aiheen rajaamisen kannalta haasteelliseksi. Aineisto kerättiin Pirkanmaan alueelta eri kaupungeista ja kunnista. Pienentääkseen liian homogeenisen aineiston riskiä, tutkija otti mukaan yhden kaupungin Keski-Suomen alueelta. Aineisto koostuu yhteensä yhdeksän kunnan tai kaupungin tietosuojavastaavien haastatteluista. Haastateltaviin oltiin yhteydessä sähköpostilla, jossa kerrottiin tutkimuksen tarkoituksesta ja tavoitteista ja ehdotettiin tapaamista. Seitsemän haastattelua toteutettiin henkilökohtaisesti kasvotusten, puhelimitse. Kaksi haastattelua toteutettiin aikataulusyistä johtuen puhelimitse. Haastattelut toteutettiin kevään 2019 aikana.

Tutkimuskysymykset luokiteltiin EU:n yleisen tietosuoja-asetuksen mukaisesti kolmeen tietosuojavastaavaa koskevaan teemaan (artiklat 37-39). Nämä teemat ovat:

- tietosuojavastaavan nimittäminen,
- tietosuojavastaavan asema, ja
- tietosuojavastaavan tehtävät.

Tutkimuskysymykset määritettiin teemakohtaisesti tietosuoja-asetuksesta tulevista vaatimuksista ja niitä täydennettiin kysymyksillä, joiden tavoitteena oli saada aihepiiristä lisää kiinnostavaa aineistoa. Haastatteluiden aikana tutkija esitti haastateltavien vastauksien perusteella myös jatkokysymyksiä, joilla pyrittiin tarkentamaan haastateltavien vastauksia. Teemahaastattelulle tyypillisesti kaikkien haastateltavien kanssa ei käyty läpi aihepiirejä samassa laajuudessa, vaan niitä mukautettiin haastateltavan kiinnostuksen ja taustan mukaan. Kaikki haastattelut nauhoitettiin.

Haastattelut litteroitiin nauhoitusten perusteella, jonka jälkeen ne luettiin useaan kertaan läpi ja tekstistä pyrittiin tunnistamaan haastattelujen yhteneväisyyksiä ja eroavaisuuksia. Varsinainen analyysi tehtiin Excel-ohjelmistossa, jonka avulla tehtiin vastausten luokittelu ja tunnistettujen luokkien perusteella teemoittelu.

4.3. Tulosten analysointi

Tutkimuksen analyysin tavoitteena on saada ymmärrystä tutkittavasta ilmiöstä ja havainnoida niitä asioita, joita tutkittavat näkevät tutkittavassa kontekstissa. Laadullisessa tutkimuksessa käytetään usein aineistolähtöistä, teorialähtöistä tai teoriasidonnaista analyysimenetelmää. Teoriaohjaavassa analyysissa aineiston analyysi ei perustu suoraan johonkin teoriaan, vaan teoria ohjaa aineiston ana-

lyysia. Tällöin analyysiyksiköt tulevat esiin aineistosta ja analyysia ohjaa tutkimuksen teoreettinen viitekehys. Analyysin helpottamiseksi tutkimuksen teoreettinen viitekehys tuleekin valita huolella, sillä siihen valitut käsitteet vaikuttavat aineiston analyysiin. (Tuomi & Sarajärvi, 2018, s. 107-108.) Tässä tutkimuksessa haastattelukysymykset on muodostettu tutkimusaiheeseen liittyvän kirjallisuuden ja lainsäädännön pohjalta, mutta aineiston analyysissa analyysiyksiköt ovat nousseet kuitenkin aineistosta, jolloin tutkimuksessa käytettyä analyysimenetelmää voidaan kuvata teoriaohjaavaksi analyysimenetelmäksi.

Yksi laadullisen tutkimuksen aineiston analysoinnin menetelmistä on teemoittelu. Teemoittelussa kerättyä aineistoa paloitellaan ja luokitellaan aihepiirien perusteella. Teemoittelussa painottuu aihealueet, jotka nousevat aineistossa esiin. (Tuomi & Sarajärvi 2018, s. 104-107.) Haastattelujen jälkeen tutkija etsi aineistosta ilmiöön liittyviä asiakokonaisuuksia ja virkkeitä, jonka jälkeen ne yhdisteltiin isommiksi asiakokonaisuuksiksi näiden muodostaessa eri teemoja. Tutkija tunnisti aineistosta useamman pääteeman, jotka esitellään tutkimustuloksia käsittelevässä luvussa.

4.4. Tutkimuskohde

Suurimmalla osalla haastateltavien työkokemus tietosuojavastaavana olemisesta oli yhden ja kahden vuoden välistä. Yli kaksi vuotta, mutta alle neljä vuotta työtaustaa oli kolmella haastateltavista ja kahdella haastateltavista työtaustaa tietosuojavastaavan roolista oli yli kymmenen vuotta. Yli puolet haastateltavista oli suorittanut ylemmän korkeakoulututkinnon, kahdella oli alempi korkeakoulututkinto ja niin ikään kahdella oli toisen asteen koulutustausta. Neljä haastateltavista oli suorittanut rooliin suoraan liittyvää täydentävää koulutusta Itä-Suomen Yliopistossa.

Haastateltavien organisaatiosijoitus ja tehtävänimikkeet organisaatiossa vaihtelivat ja ovat esiteltynä taulukossa 1. Taulukossa on myös viittauskoodit eri henkilöiden haastatteluihin.

Taulukko 1: Tehtävänimikkeet ja viittauskoodit

Vastaajan tehtävänimike	**Määrä**	**Viittauskoodi**
Tietosuojavastaava	2	T1 & T2
Hallintopäällikkö	2	T3 & T4
Erityisasiantuntija	2	T5 & T6
Toimistosihteeri	1	T7
ICT-palvelukoordinaattori	1	T8
Hallinnon suunnittelija	1	T9

Kahden haastateltavan henkilön virallinen tehtävänimike oli tietosuojavastaava. Kaksi haastateltavaa kuuluivat oman organisaationsa johtoryhmään. Kaikki haastateltavista olivat sijoitettu organisaationsa hallintopalveluihin ja sen eri alayksiköihin.

5. Tutkimustulokset

Luvussa esitetään tutkimustulokset kaikista kolmesta pääosa-alueesta. Haastattelukysymysten runko on esitettynä tutkimuksen liitteissä.

5.1. Tietosuojavastaaville asetetut osaamisvaatimukset

Haastateltavista yli puolet painottivat, että ennen nimittämistä tietosuojavastaavan tehtävään organisaation johdon tulee arvioida henkilön soveltuvuutta. Suurin osa haastateltavista olivat yhtä mieltä siitä, että henkilön aihealueen ymmärryksen ja kokemuksen laajuus sekä organisaation tuntemus ja henkilökohtaiset ominaisuudet tulee arvioida ennen nimittämispäätöksen tekemistä. Lisäksi johdon tulee pohtia tietosuojavastaavan aseman organisoimista organisaatiossa, jotta se mahdollistaisi tietosuojavastaavan täyden mandaatin toteuttaa tehtävää vaatimustenmukaisesti. Yksi haasteltava reflektoi nimittämistä seuraavasti:

> On ihan keskeinen asia, että johto mieltää asianmukaisesti tehtävän vastuullisuuden, luonteen ja roolin. Kunnissa on tehty hyvin erilaisia ratkaisuja tämän asian kanssa enkä halua ottaa kantaa siihen, miten muut organisaatiot ovat ratkaisseet tämän tilanteen, mutta tiedän kyllä, että hyvin erilaisilla taustoilla ja organisaatioasemalla on nimitetty henkilöitä tähän tehtävään. Näkisin, että johtoryhmään kuuluminen vahvistaa edellytyksiä tehtävää varten eikä siitäkään mihinkään pääse, että asema siinä organisaatiossa saattaa vaikuttaa siihen, että miten se aihepiiri mielletään. (T3)

Haastateltavien joukosta yli puolet kertoivat, että heitä oli arvioitu ennen tehtävään valintaa tai nimittämistä. Osa haastateltavista aloittivat tehtävässä uutena henkilönä, jolloin rekrytointia suorittaneet henkilöt arvioivat kandidaattien soveltuvuutta kuten tavanomaisessa rekrytoinnissa henkilöitä arvioidaan. Nimitettävien henkilöiden soveltuvuutta tehtävään arvioitiin eri osa-alueilla kuten henkilökohtaisten ominaisuuksien sopivuutta ja asiantuntemuksen tasoa. Joidenkin haastateltavien kanssa johto oli käynyt aktiivisesti keskusteluja muun muassa tietosuojavastaavan tehtäviin kuuluvista vastuualueista, tehtävien suorittamisesta sekä asemasta. He olivat myös pohtineet, että vastaako nimitettävä henkilö yleisen tietosuoja-asetuksen vaatimuksia, tai onko asema todella riippumaton. Kaksi haastateltavaa kertoivat omasta arviointikokemuksestaan:

> Se oli ihan normaali työhaastattelu. Tehtävänkuva oli tehty ja sitä vasten minua haastateltiin ja arvioitiin. En ole siis siirtynyt tehtävään talon sisältä, vaan minut rekrytoitiin talon ulkopuolelta. (T2)

> Meillä oli organisaation sisäinen haku ja siihen oli tietyt vaatimukset koulutuksen ja kokemuksen suhteen. Jouduin hakemaan ihan virallisesti ja ihan täysin panostin työhakemukseen, eli valinta ei ollut mikään läpihuutojuttu. (T8)

Henkilöiltä, jotka valittiin tehtävään organisaation sisältä, kysyttiin suostumus ja halukkuutta tehtävään nimittämisestä. Yksi haastateltavista kertoi, että häntä pyydettiin tehtävään sen vuoksi, että sen hetkisessä tehtävässä olisi ollut ylimääräistä aikaa ja sen vuoksi katsottu sopivaksi henkilöksi sen sijaan, että hän olisi ollut muutoin soveltuva. Osa haastateltavista ei osannut sanoa tehtiinkö soveltuvuuden arviointia ennen nimitystä, sillä se ei ollut heille mitenkään läpinäkyvää. Yksi haastateltava vastasi seuraavasti:

> Arviointia ei tehty mitenkään ainakaan minulle näkyvällä tavalla. Täällä se menee vähän niin, että tekisitkö sinä tämän homman. Kuitenkin näen sen kohtuullisen luontevana osana omaa työnkuvaani eikä siinä ole ollut ristiriitoja ja kyllä minulta kysyttiin, että haluatko tehtävän. (T9)

Kysyttäessä haastateltavien mielipidettä omasta asemasta, tehtävistä ja vastuista, lähes kaikki olivat sitä mieltä, että ne ovat määritelty riittävän selkeästi eikä epäselvyyksiä roolista ollut. Yhden haastateltavan mielestä hänen tehtäviään ja vastuualueitaan ei ole määritetty riittävän selkeästi ja olisi kaivannut selvennystä niihin. Kuntaorganisaatioissa laaditaan usein työntekijän roolia vastaava tehtävänkuvaus, jossa määritellään kaikki rooliin kuuluvat tehtävät ja niiden ajankäyttö. Lähes kaikilla haastateltavista tehtävät olivat määritetty työsopimuksen liitteenä olevaan tehtävänkuvaukseen ja yhdellä tehtävät olivat määritetty työsopimuksessa. Haastateltavien joukosta suurimman osan tehtävät olivat kopioitu täysin yleisestä tietosuoja-asetuksesta, tai ne olivat määritelty vastaamaan tietosuoja-asetuksessa lueteltuja tehtäviä.

Kysyttäessä ansiontason kehittymisestä tietosuojavastaavan tehtävään nimittämisen myötä, haastateltavista alle puolet kertoivat tehtäväkohtaisen ansion kehittyneen positiivisesti. Tyypillisin tehtäväkohtaisen ansainnan kehitys oli 200 euroa kuukaudessa. Haastateltavista pienen osan tehtäväkohtaisessa osuudessa ei tapahtunut kehitystä. Niiden henkilöiden, jotka valittiin tehtävään uutena tehtävän palkkataso oli määritelty tehtävän ilmoitushetkellä. Suurin osa haastateltavista kertoivat olevansa tyytyväisiä kokonaisansioonsa, mutta kokivat, että palkkataso ei vastaa tietosuojavastaavan tehtävien haasteellisuutta ja näkivät, että tehtävästä tulisi saada suurempi korvaus sen tuoman vastuun vuoksi. Kolme haastateltavista olivat palkkatasostaan tätä mieltä:

> Käytännössä kahdella sadalla eurolla organisaatio ei saa yhtään mitään, ehkä yhden työpäivän. Onhan tämä tehtävä huomattavasti laajempi ja onhan siinä kuitenkin omat vastuut. Ei se kyllä mielestäni ihan ole juuri kohdallansa, mutta kokonaisuudessaan ansiotasoon olen ihan tyytyväinen. (T5)

> Saan kaksisataa (200) euroa kuukaudessa siitä, että olen tietosuojavastaava ja musta se on aika vähän. Periaatteessa se on siis yksi, tai puolitoista päivää kuukaudessa eikä se mun mielestä vastaa ollenkaan tietosuojavastaavan palkkaa. (T6)

> Omaan palkkatasooni en ole enää nykyään tyytyväinen. Vielä 2 vuotta sitten olin. Nyt työn vaativuus on noussut GDPR-lainsäädännön myötä korkeaksi sekä on

> saanut aikaan sen, että tehtävien vastuu on kasvanut ja kansalaiset ovat päivittäin yhteydessä asiasta ja asian vierestä. Palkkatason pitäisi olla isossa kunnassa tai isossa yrityksessä saman kuin esimerkiksi tietohallintopäällikön. (T1)

Kysyttäessä tietosuojavastaavan tehtävälle sopivan palkkatason suuruudesta, haastateltavat määrittelivät keskiarvolliseksi kokonaisansioksi 3800 euroa kuukaudessa. Vastaajien mielestä kokoaikaisen tietosuojavastaavan roolin houkutteleva kokonaisansio tulisi olla yli 4000 euroa, jotta se kiinnostaisi organisaation ulkopuolisia asiantuntijoita hakeutumaan tehtävään. Vertailun vuoksi KT Kuntatyönantajien verkkosivuilla julkaistun, vuoden 2019 lokakuussa kerättyjen tietojen mukaan tietosuojavastaavan tehtäväkohtainen palkka oli 3685 euroa ja kokonaisansiot, joissa on myös henkilökohtaiset lisät ja ylityökorvaukset, oli 4034 euroa. (KT Kuntatyönantajat, 2020).

5.1.1. Tietosuojavastaavan työelämätaidot

Aineistossa toistui selkeästi tietosuojavastaavalle erilaisia tarpeellisia kompetensseja, jotka ovat luokiteltu työelämätaidoiksi.

Kysyttäessä tietosuojavastaavalle hyödyllisestä ja soveltuvasta koulutus- ja työtaustasta yli puolet painottivat kuntaorganisaation työkokemuksen merkitystä. Kuntaorganisaation moninaisuuden, johtamisjärjestelmän ja henkilötietojen käsittelyn kompleksisuuden ymmärtäminen koettiin suurena etuna ja voimavarana, joka sujuvoittaa tietosuojavastaavan työtä. Aineiston mukaan tietosuojavastaavan tulee ymmärtää eri toimialojen tehtävät ja toiminnat, jotta pystyy tarvittaessa ottamaan kantaa ja vastaamaan selkeästi toimialalta tuleviin erityiskysymyksiin. Tietosuojavastaavan tulee ymmärtää myös henkilötietojen käsittelytoiminnot, jotta pystyy katselmoimaan ja arvioimaan rekisteröityjen informointiin liittyviä asiakirjoja kuten tietosuojaselosteita. Organisaation ja sen käsittelyprosessien tunteminen on myös kirjallisuudessa monesti esiintynyt kompetenssivaatimus tietosuojavastaaville. Kolmen haastateltavan näkemykset työ- ja koulutustaustasta olivat seuraavat:

> Olen itse huomannut, että se on valtava etu, että on kuntaorganisaation työtausta ja on ollut kunnassa töissä. Tavallaan se (kunnan) byrokratia on tuttua, eli miten asioita esitetään ja miten asioita saadaan eteenpäin. (T2)

> Koulutustaustan tulee olla sellainen, että se antaa tukea tällaisen todella laaja-alaisen asiantuntijatehtävän hoitamiseksi. En halua rajata mitään vaihtoehtoja ulkopuolelle, mutta itse koen, että hallintotieteellinen tutkinto antaa hyvät edellytykset siihen. Omassa tutkinnossa on tullut opiskeltua kunnan toimintaa ja luonnetta ja velvollisuuksia aika laajasti ja monesta näkökulmasta. Toki, kun on suorittanut akateemisen tutkinnon, niin se antaa osaltaan hyviä työvälineitä ja valmiuksia esimerkiksi tiedon hankintaan, tietojen käsittelyyn ja analysointiin. Jatkuvasti täytyy pitää tietoja ja taitoja yllä. Tutkinto antaa hyvät perusvalmiudet, mutta siitä se sitten oikeastaan vasta alkaa. (T3)

> Väitän, että tähän on vaikea hakea puhdasta koulutustaustaa, koska sun periaatteessa pitäisi tietää organisaatiosta ja sen toiminnasta tosi yksityiskohtaisesti, eikä se tule mistään muusta kuin kokemuksesta siellä kunnassa. Pitäisi olla myös ymmärrys ohjelmistojen toiminnasta, toki tietoturva on erikseen, mutta ei tässä duunissa pärjää, jos ei ymmärrä ohjelmistojen toimintaa. Sitten toisaalta pitäisi ymmärtää manuaalista aineiston käsittelyä siinä rinnalla. (T8)

Koulutustaustasta kysyttäessä haastateltavat kertoivat olevan hankala määrittää yhtä oikeata vaihtoehtoa tai tehtävään suoraan soveltuvaa tutkintoa, mutta korkeakoulututkinnon koettiin antavan tietosuojavastaavalle sopivia valmiuksia ja työkaluja tehtävässä onnistumiseen. Sopivaksi koulutustaustaksi määriteltiin muun muassa hallintotieteet, julkisoikeus sekä yleisesti oikeustieteet ja juristin tutkinto. Muutama haastateltava painotti, että koulutustaustan merkitys vähenee, jos tietosuojavastaava voi tehdä yhteistyötä kunnan muiden toimintojen sekä asiantuntijoiden, kuten lainoppineiden ja tietohallinnon eri asiantuntijoiden, kuten tietoturva-asiantuntijan kanssa. Näin vastuita saadaan jaettua eikä tietosuojavastaavan tarvitse ensin tehdä isoa taustatutkimusta, tai ottaa kaikkiin kysymyksiin kantaa, vaan voi hyödyntää organisaation sisäistä asiantuntemusta eri aihealueista.

Kuntaorganisaation tuntemisen ja ymmärtämisen lisäksi haastatteluissa painottuivat tietosuojalainsäädännön tunteminen ja tulkitseminen sekä soveltaminen käytännössä, joka myös on yksi tietosuojavastaavan kompetenssivaatimus tietosuoja-asetuksessa. Haastateltavista kaikki nimesivät lainsäädännön tuntemisen yhdeksi tietosuojavastaavan keskeisimmistä osaamisen osa-alueista, sillä erityislainsäädäntöjä on useita ja joissain tilanteissa rekisteröidyn saattaa olla edullisempaa käyttää erityislainsäädännöstä tulevia oikeuksiaan kuin tietosuoja-asetuksen mukaisia oikeuksia. Kahden kaupungin tietosuojavastaavat nostivat esiin kokonaisvaltaisen juridisen viitekehyksen:

> Lainsäädännön tunteminen ja lakiosaaminen on hyödyksi. Sitä syventääkseni olen käynyt paljon koulutuksissakin, koska täytyy ymmärtää miten lait keskenään seurustelevat ja mikä oikeus menee minkäkin ohi. Näitä asioita paljon mietitään lakimiesten kanssa. Taustalla voi olla useita erityislainsäädäntöjä ja laintulkinnalla on iso merkitys ja tarvittaisiin erilaisia ennakkopäätöksiä, jotta päästään jyvälle tavasta tulkita sovellettavaa lainsäädäntöä. (T2)

> On (tietosuojavastaavan) koulutustausta mikä tahansa, niin keskeisin osaamisen osa-alue on henkilötietojen käsittelykäytänteiden tunteminen, eli kyky ymmärtää mistä lainsäädännöstä tai normiohjauksesta tulee se viitekehys, jossa voidaan toimia. Tässä korostuu myös kyky etsiä tietoa ja ottaa selvää, kun tulee uusia hankkeita. (T1)

Keskeisiä osaamisen osa-alueita olivat lisäksi organisaation tunteminen, jonka lähes kaikki haastateltavat nimesivät. Keskeisistä osaamisista korostuivat myös tietotekniset taidot sekä asiakirjahallinnon osaaminen ja tietojenkäsittely. Asiakirjahallinnon osalta aineistossa nousi esiin tietosuojakontekstissa tiedon elin-

kaaren hallinta ja tiedon luokittelu. Haastateltavat nostivat myös hyvät tietotekniset taidot yhdeksi tietosuojavastaavan ydinosaamisalueeksi. Tietoteknisistä taidoista aineistossa korostui tietoturvallisuuden osaamisen merkitys, mutta lisäksi kokonaisarkkitehtuuri, hankintojen vaatimusmäärittelyt ja tietokanta- ja integraatio-osaaminen sekä käyttöoikeushallinta. Yhdeksi keskeiseksi osaamiseksi aineistossa muodostui myös uuden tiedon hankinta ja omaksuminen sekä projektinhallinta ja -johtamistaidot.

Keskeisiksi osaamisen osa-alueiksi tunnistetut kompetenssit nousivat vahvasti esiin myös niissä osa-alueissa, joita haastateltavat kokivat omiksi kehittämisen osa-alueiksi ja missä eniten tarvitsi tukea. Moni haastateltava koki, että oman vahvuusalueen ulkopuoliset asiat ovat vaikeammin edistettävissä ja niihin on haastavampi tarttua, jolloin selvitystyössä voi kestää kauemmin aikaa kuin sellaisissa. Osaamisalueet, joissa tietosuojavastaavat kaipasivat eniten tukea olivat juridiikka ja tietotekninen osaaminen. Juridisessa osaamisessa eniten tukea tarvittiin aineiston mukaan tietosuojasopimuksiin liittyvissä asioissa, tai erityislainsäädännön tulkintaa vaativissa kysymyksissä. Tietoteknisessä osaamisessa tukitarpeet liittyivät erityisesti tietoturvaan liittyvään syväosaamiseen kuten tietojärjestelmien koventamiseen sekä konfiguraatiomuutoksiin. Tietoteknisessä osaamisessa korostui myös tietojärjestelmien lokitukseen liittyvät asiat sekä tietojärjestelmähankintojen vaatimusmäärittely. Kahden kaupungin tietosuojavastaavat kertoivat tukitarpeistaan seuraavasti:

> Lainsäädännön ja etenkin eri toimialojen erityislainsäädännön tuntemisesta ja osaamisesta olisi hyötyä. Yleishallinnon ja oman vastuualueen ulkopuolisia tiedusteluja tulee jonkin verran ja olisi hyödyllistä, jos pystyisi jotenkin asiaa kommentoimaan. Ohjaan tiedustelut kuitenkin sen alan asiantuntijalle kuten sosiaalipalveluiden tai terveyspalveluiden tietosuojavastaavalle, koska en itse osaa ottaa niihin kantaa. (T8)

> Tukea tarvitsen tietohallinnon osaamisalueelle menevissä asioissa, ja näissä tyypillisesti konsultoinkin tietohallinnon asiantuntijoita. Näitä on etenkin tekniseen tietoturvallisuuteen liittyvät asiat kuten eri teknologioiden tai tietojärjestelmien konfiguraatiot tai koventamiseen liittyvät käytännöt. (T3)

Työelämätaitojen lisäksi aineistossa korostuivat tietosuojavastaavan persoonaan ja temperamenttiin liittyviä tarpeellisia ominaisuuksia ja kyvykkyyksiä jotka ovat esiteltynä seuraavassa kappaleessa.

5.1.2. Tietosuojavastaavan henkilökohtaiset ominaisuudet

Käsiteltäessä tietosuojavastaavan henkilökohtaisia ominaisuuksia, persoonaa ja temperamenttiä haastateltavista kaikki korostivat kommunikointi- ja vuorovaikutustaitojen merkitystä. Kommunikointi- ja vuorovaikutustaidot nähtiin avainkyvykkyyksinä, sillä tietosuojavastaavan rooliin kuuluu keskeisesti ohjaus- ja neuvontatehtävät sekä henkilötietojen käsittelytoimen vaatimustenmukaisuuteen liittyvä valvonta ja raportointi. Tietosuojavastaavan tehtäviin kuuluu niin

organisaation sisäinen neuvonta ja ohjaus, mutta myös kuntalaisten neuvominen tietosuoja-asioissa. Neuvonta- ja ohjaustehtävissä korostui tarve olla ja esittää asiat rauhallisesti sekä ymmärrettävästi. Tietosuojavastaavan tulee ymmärtää, että muut eivät välttämättä ole substanssiasiantuntijoita, vaan voivat kuulla asioista ensimmäistä kertaa. Tietosuojavastaava toimii myös yhteyshenkilönä valvontaviranomaisille ja tarvittaessa vastailee viranomaisen tieto- ja selvityspyyntöihin, tai pyytää viranomaisen näkemystä asioihin.

Kommunikointi- ja vuorovaikutustaitoja tietosuojavastaava tarvitsee aineiston mukaan eniten organisaation sisällä, etenkin eri toimialojen ja johdon kanssa työskentelyssä. Tietosuojavastaavan tulee pysty esittämään asiat tiivistetysti johdolle ja tarvittaessa raportoimaan havaituista puutteista, tai tietosuojarikkomuksista sekä tietomurroista. Tietosuojavastaavalla tulee olla kyky neuvotella sisäisten sidosryhmien kanssa henkilötietojen käsittelytoiminnoista ja tarvittaessa muuttamaan, tai jopa kieltämään käsittely, jos siinä on havaittu puutteita. Johdolle tulee pystyä myös perustelemaan lisäresurssien tarpeet ja niistä tulee pystyä neuvottelemaan.

Tietosuojavastaava tarvitsee myös rohkeutta toteuttamaan tietosuojavastaavan roolia ja asemaa, oli organisaatiosijoitus tai asema organisaatiossa mikä tahansa. Rohkeus nostaa vaikeatkin asiat keskustelun aiheeksi ja esittää näkemyksensä rehellisesti nähtiin monen haastateltavan mielestä tärkeänä ominaisuutena. Hyvän kommunikoijan ja rohkeuden lisäksi tietosuojavastaavan tulee olla jämpti ja seistä näkemystensä takana, vaikka ne eroaisivat esimerkiksi johdon näkemyksistä tai olisivat tavoitteiden tai jopa kehityshankkeiden jarruna. Tietosuojavastaavan roolia tulee pystyä toteuttamaan rohkeasti ja jämptisti, sillä muuten tietosuoja ei välttämättä toteudu ja toiminta voi olla lainsäädännön vaatimusten vastaista. Kaksi tietosuojavastaavaa esittää näkemyksensä seuraavasti:

> Tämä on nimenomaan ihmisten kanssa työskentelyä. Eikä se ole mitään päältä päin päsmäämistä, vaan pitää olla tukena ja aika positiivisella vireellä. Pitäisi pystyä herättämään luottamusta, että kaikki uskaltaisivat ottaa yhteyttä ja esimerkiksi myöntämään virheen, jos sellainen on tapahtunut. Täytyy olla kannustava ja positiivinen ote ja helposti lähestyttävä henkilö. Pitää kuitenkin olla jämpti, koska välillä joutuu vääntämään, siis kankeamaan ihan kunnolla, etenkin johdon kanssa. Siinä ei saa mennä sisu kaulaan. (T2)

> Pitää olla sosiaalinen ja verkostoituva ihminen, koska muuten ei pääse sisään siihen organisaation toimintaan, jos et pysty luovimaan organisaation sisällä ja keskustelemaan ihmisten kanssa. Liian hyökkäävä ei saa olla, mutta ei myöskään sellainen, että antaisit jyrätä itsesi, että siinä on haastava tehtävä jo pelkästään tällä sosiaalisella puolella. Pitäisi saada ihmiset myös ymmärtämään sen asian tärkeyden, mutta toisaalta liiallisella painostuksella ei saa muuta kuin sen organisaation lukkoon, eikä sieltä saa sen jälkeen enää mitään tietoja. (T4)

Aineistossa korostui kommunikointi- ja vuorovaikutustaitojen, rohkeuden ja jämptiyden lisäksi myös oma-aloitteisuus ja itseohjautuvuus, joka mainittiin lähes kaikkien haastateltavien toimesta. Itsensä ja oman työnsä johtaminen nähtiin kriittisenä etenkin tietosuojaohjelman kehittämisvaiheessa, jolloin organisaation

kypsyystaso on matalampi ja päätoimisen kehittäjän tulee omatoimisesti pystyä edistämään asioita. Tietosuojavastaavan tulee myös pyrkiä aktiivisesti olemaan yhteydessä eri toimialojen kanssa, jotta saa aktiivisesti ajantasaista tietoa eri kehityshankkeista ja projekteista, joilla voi olla merkitystä tietosuojan kanssa.

Haastateltavat korostivat sitä, että organisaation sisältä ei aina muisteta kysyä neuvoa tietosuojavastaavalta, jolloin itseohjautuvuuden merkitys kasvaa, jotta tietosuoja-asiat ja vaatimukset pystytään huomioimaan oikea-aikaisesti eri projekteissa tai hankinnoissa. Itsensä johtamisen lisäksi haastateltavat korostivat tiedon omaksumiskykyjä ja analyyttista otetta tehtäviin. Tämä on tärkeä taito, koska aineiston mukaan tietosuojavastaavien eteen tulee usein täysin uusia asioita tai kysymyksiä, joiden selvittämisellä on tiukka aikataulu. Tietosuojavastaavan tulee pystyä selvittämään ja antamaan vastaukset selkokielisesti ja perustelemaan näkemyksensä tarvittaessa useista eri näkökulmista. Usein näissä kysymyksissä yhdistyvät useat eri erityislainsäädännöt ja mahdollisesti rekisteröidyn oikeudet. Tällöin tietosuojavastaavan tulee pystyä hahmottamaan kokonaisuus selkeästi ja antaa selkeät ohjeistukset, joiden mukaan voidaan toimia. Yhden tietosuojavastaavan näkemys asiaan oli:

> Korostaisin tietosuojavastaavan tehtävissä vaadittavia kykyjä kokonaisuuksien ja juridisen viitekehyksen hahmottamiseen. Tällä en tarkoita, että tietosuojavastaavan tulisi muistaa kaikki lait ulkoa, mutta kun joltain toimialalta otetaan yhteyttä ja kysytään jotain asiaa, niin yleensä järkevin tapa on yrittää hahmottaa, että minkä lain piirissä tässä liikutaan ja yrittää sen jälkeen analysoida ja peilata sitä tietosuoja-asetukseen ja tähän viitekehykseen. On tärkeätä pitää mielessä kokonaiskuva ja lähestyä asiaa useasta eri näkökulmasta, koska voi olla kyseessä rekisteröidyn subjektiivinen näkemys ja organisaation tarve, jotka voivat olla ristiriidassa. (T3)

5.1.3. Haastateltavien itsearviointi osaamisestaan

Kaikkiaan kaksi kolmesta haastateltavien joukosta olivat sitä mieltä, että heidän osaamisensa on riittävä suoriutumaan tietosuojavastaavan tehtävistä onnistuneesti. Yli puolet kuitenkin täydensivät vastaustaan niin, että tietosuojavastaavien tehtävässä tulee jatkuvasti täydentää ja päivittää omaa osaamistaan ja omia kyvykkyyksiä, jotta tehtävissä voi onnistua jatkossakin. Osaamisen täydentämisen keinoiksi nimettiin täydennyskoulutukset, kurssit ja tiedon hakeminen ja analysoiminen. Kaksi tietosuojavastaavaa tiivisti osaamisen ylläpitämisen merkityksellisyyttä ja toisaalta kuvasivat tehtävän haasteita:

> Kyllä minä koen, että se on riittävä, mutta koko ajan pitää olla hereillä ja tutkailla, mitä ympärillä tapahtuu. Täytyy jatkuvasti seurata eri uutislähteitä ja esimerkiksi, että mitä ratkaisuja tietosuojavaltuutetun toimisto tekee. (T3)

> Tässä on pakko vastata, että keskitasolla koen olevani riittävän osaava, mutta yllätyksiä tuntuu enemmissä määrin tulevan, joissa oma osaaminen menee aivan äärimmilleen. Globalisaatio, pidemmät alihankintaketjut, enemmissä määrin pilvi-

> teknologiaan siirtyminen ja tieto on koko ajan hajautetumpaa ovat syitä, jotka tekevät tehtävästä kokonaisuudessaan äärimmäisen haastavan. Vianselvitys hankalampaa ja vastuiden selvitys on myös hankalampaa, vaikka vastuista onkin sovittu kirjallisesti, mutta se on täysin paperia. Miten ne prosessit oikein kulkee ja toimii on se, mihin sen tietosuojavastaavan pitäisi perehtyä. (T1)

Ne haastateltavat, joiden mielestä oma osaaminen ei ollut riittävää kokivat, että tehtävän laajuus ja vaatimukset ylittivät heidän odotuksensa. He kokivat myös, että heidän tarvitsemaansa tukea ei ollut helposti saatavilla, vaan asioihin olisi tarvittu useampaa asiantuntijaa eri osaamisalueilta, jotta niitä olisi saatu edistettyä asian edellyttämällä tavalla. Asioiden selvittäminen useiden asiantuntijoiden kanssa, tai vastausten odottaminen tuntuu kuormittavalta ja pitkittää kokonaisuudessaan asioiden ratkaisua, joilla voi olla kovakin kiire. Kaksi tietosuojavastaavaa kokivat asian seuraavasti:

> Ei ole varmaan ikinä sellainen olo, että olisi riittävä osaaminen. Tulee melkein päivittäin sellainen olo, että pitääpä tähänkin asiaan perehtyä. Se on varmaan tämä hetki, kun on uusi tehtävä ja uusi lainsäädäntö eikä ole valmiita saappaita, mihin hypätä. Kun aloitin tehtävässä ei ollut ketään keneltä kysyä neuvoa. (T2)

> Ei kyllä ole. Aina on jotain sellaista, mistä pitäisi olla enemmän kokemusta ja osaamista, joka tuntuu todella kuormittavalta. (T4)

5.2. Tietosuojavastaavan asemaan kohdistuvat vaatimukset

Haastateltavat olivat lähes yksimielisiä siitä, että tietosuojavastaavan asema on määritelty riittävän selkeästi tietosuoja-asetuksessa. He myös kokivat, että asetus kattaa riittävän yksiselitteisesti ne vaatimukset, joita tietosuojavastaavan asemaa koskien tulee olla määriteltynä. Haastateltavista osa täydensi, että tietosuoja-asetuksen myötä tulleet määritelmät olivat selkeä parannus aiempaan lainsäädäntöön, jossa tietosuojavastaavan asemaa koskien ei ollut asetettu velvoitteita. Yksi tietosuojavastaava kuvasi asetuksen tuomia hyötyjä seuraavasti:

> Asetushan on selkeä parannus lainsäädäntöön esimerkiksi tietosuojavastaavalle, sillä asetus täydentää ja määrittää tarkemmin työnkuvaa, asemaa ja nimittämistä. (T1)

Vain yksi haastateltava oli toista mieltä ja hänen mielestään tietosuoja-asetus ei ollut riittävän selkeä aseman organisoimisen määrittelyn suhteen. Hänen mielestään tietosuoja-asetus on liian yleismaailmallinen ja jättää liikaa liikkumavaraa ja toisaalta epävarmuutta toiminnan riittävyydestä ja vaatimustenmukaisuudesta. Kaikki haastateltavat olivat kuitenkin sitä mieltä, että tietosuoja-asetuksessa ei ole sellaisia puutteita tai ristiriitoja, jotka asettaisivat haasteita tai esteitä tietosuojavastaavan asemalle tai tehtävien hoitamiselle. Suurin osa haastateltavista ei

myöskään ollut sitä mieltä, että muut vaatimukset kuten erityislainsäädäntö, asettaisi haasteita tietosuojavastaavan asemalle tai tehtävien hoitamiselle. Osa tietosuojavastaavista kuitenkin täydensivät vastaustaan niin, että etenkin niiden tietosuojavastaavien, jotka hoitavat tehtävää omien työtehtävien ja vastuiden ohessa, tulee kiinnittää paljon huomiota siihen, että tietosuojavastaavan rooli ja asema eivät kärsi muiden työtehtävien vuoksi. He painottivat, että erityisesti tietosuojavastaavan riippumattomuus voi vaarantua muiden vastuualueiden vuoksi.

Kaksi haastateltavista kuitenkin kokivat, että velvoittavaa erityislainsäädäntöä on niin paljon, että se aiheuttaa suuria haasteita kokonaisuuden hahmottamiseksi. He painottivat, että sovellettavan lainsäädännön arviointi on työlästä kuntaorganisaatiossa tai yleisesti julkishallinnon organisaatioissa. Toinen heistä täydensi lisäksi, että kokee haasteelliseksi riippumattomuuden toteutumisen tietosuojavastaavan tehtävissä, koska hänen vastuullaan on myös päätöksentekoa ja on joutunut tilanteisiin, jossa tulee tehdä päätöksiä henkilötietojen käsittelyyn liittyen. Haastateltavista kolmasosa olivat myös sitä mieltä, että kuntaorganisaation toimintaympäristö, johtamisjärjestelmä ja sidosryhmiltä tulevat vaatimukset asettavat haasteita tietosuojan toteutumiselle. Haastateltavat painottivat, että julkishallinnon organisaatioiden henkilötietojen käsittelyä säädetään todella monessa eri laissa. Tämä pirstaloittaa lainsäädäntöä ja aiheuttaa haasteita sovellettavuuden arvioinnissa ja mahdollisesti myös tietosuojan toteutumisessa. Kaksi tietosuojavastaavaa antoivat konkreettisen esimerkin:

> Esteitä tai ainakin haasteita aiheuttaa ehkä jossain määrin esimerkiksi se, että julkislainsäädännön tulisi olla linjassa läpinäkyvyyden periaatteen kanssa. Tällä hetkellä joudutaan salaamaan joitain asiakirjoja tai valmisteluja, koska jokin osa näissä on salassa pidettävää ja sen vaikutuksista ei ole selvyyttä. Todennäköisesti tällä rikotaan läpinäkyvyyden periaatetta, jos asia koskee jotenkin kunnan henkilötietojen käsittelyä. (T4)

> Sen verran on haasteita kyllä, että mitä muut viranomaiset kuin kunta itse toivoo, että missä kunta olisi mukana ja osittain myös rahoittaa niitä. Näistä hankkeista henkilötietojen käsittelyohjeistukset puuttuvat lähes aina. Muoti-ilmiönä tällainen moniviranomaisyhteistyö aiheuttaa sen, että jokainen kunta itse pähkäilee, että miten he toimivat rajapinnassa: Sosiaali- ja terveyspalvelut, Poliisi, Työllisyydenhoitopalvelut, Aluehallintovirastot, ELY-keskus ja TE-palvelut. Hankkeiden pitäisi pohjautua niin, että lainsäädäntö on otettu huomioon jo etukäteen ennen kuin annetaan mitään määräyksiä, missä kuntien pitäisi olla mukana. Tämä on yleisesti tietosuojavastaavien piireissä tunnistettu kunnissa pahaksi ongelmaksi. (T1)

Lainsäädännön moninaisuus aiheuttaa päällekkäisyyttä ja tekee näin soveltamisen haasteelliseksi, jonka lopputuloksena voi olla este tietosuojan toteutumiselle ja selkeä puute vaatimustenmukaisuudessa. Tämä asettaa myös tietosuojavastaavien lainsäädännön tuntemiseen selkeitä vaatimuksia.

Suurin osa tietosuojavastaavista kokivat, että organisaation johto on sitoutunutta tietosuojatyöhön ja ymmärtää oman vastuunsa. Kaksi haastateltavista epäilivät, että kunnanjohto ei täysin ymmärrä omaa vastuutaan tietosuojatyössä

eivätkä näin myöskään sitoudu työhön ja toteuta omaa rooliaan täysimääräisesti organisaatiossa. Tästä seurasi myös se, että tietosuojavastaavat kokivat, että eivät saa riittävästi tukea tai resursseja tietosuojatyön kehittämiseen.

5.2.1. Tietosuojatyön resursointi

Tietosuojatyön resursointi koettiin haastateltavien keskuudessa hyvin merkittäväksi osa-alueeksi ja avainasemassa tehtävässä onnistumisen mahdollistajana. Yli puolet haastateltavista kuitenkin kokivat, että tällä hetkellä heidän resurssinsa eivät ole riittäviä. Haastateltavien mukaan työtä oli enemmän kuin sitä pystyttiin tekemään siihen varatulla työajalla. Haastateltavien mukaan resursointia tulisi parantaa hyödyntämällä säännöllisesti ulkopuolisia resursseja ja ostopalveluita kuten konsultointia, tai teettämällä arviointeja tahi auditointeja. Näin tietosuojavastaavan ei tarvitsisi itse tehdä kaikkea sitä työtä, mikä tällä hetkellä kerääntyy tehtävien töiden listalle. Hieman yli puolet tietosuojavastaavista olivatkin pystyneet hyödyntämään ulkopuolista apua helpottaakseen omaa työtään. Moni kuitenkin koki, että resurssit, joita ulkopuoliseen apuun pystyttiin hyödyntämään olivat liian vähäiset, tai ulkopuolisesta avusta saatu hyöty oli alittanut odotukset.

Tietosuojavastaavat kokivat riskiksi sen, että tietosuojatyölle ei ollut varattu omaa budjettia. Missään organisaatiossa tietosuojalla ei ollut omaa budjettia, jota tietosuojavastaava olisi voinut hyödyntää parhaaksi näkemällään tavalla, vaan tietosuojaan käytettävät ulkopuolisilla teetetyt työt tilattiin yksikön budjetista ja tilaukset piti perustella huolellisesti. Kolmasosa haastateltavista vastasi, että tietosuojalle tulisi olla organisaatiossa oma budjetti ja kustannuspaikka, jota he voisivat hyödyntää omassa työssään. Resursointia parantavana tekijänä nähtiin myös kunnolliset varahenkilöjärjestelyt. Tällä hetkellä tietosuojavastaaville ei ollut monessa organisaatiossa nimetty varahenkilöä, joka hoitaisi tietosuojavastaavan tehtäviä varsinaisen henkilön ollessa poissa tai estynyt hoitamaan tehtäviä. Kolmas aineistossa usein esiintynyt vaihtoehto resursoinnin parantamiseksi oli kokoaikaisen tehtävän tai roolin perustaminen, jolloin henkilö hoitaisi pelkästään tietosuojatyöhön liittyviä tehtäviä.

Haastatelluista vain kaksi oli tietosuojavastaavan tehtävässä kokoaikaisesti, kun muut hoitivat tehtäviä muiden tehtävien ohessa. Haastateltavien tehtävänkuvassa oli kahdella henkilöllä määritetty tietosuojatyöhön 50% kokonaistyöajasta. Molemmat henkilöistä täydensivät vastaustaan, että käytetty työaika ei kuitenkaan toteudu, sillä muut työtehtävät ja vastuut vievät suuremman osan työajasta. Haastateltavista yli puolella ei ollut määritelty tietosuojatyöhön käytettävää työaikaa lainkaan. Kolme tietosuojavastaavaa antoivat ehdotuksia miten resursointia voitaisiin parantaa:

> Tällä hetkellä resursointi ei ole riittävää, mutta tätä roolia voisi vahvistaa niin, että tähän määritetty 50% työajasta toteutuisi. Näkisin myös, että kunnassa tietosuojavastaavan rooli voisi olla kokoaikainen. (T9)

> Resursointia voitaisiin parantaa järjestämällä kunnon varahenkilöjärjestelyt. Varahenkilöllä tulisi olla samanlaista osaamista ja, että hän pystyisi hoitamaan sitä tehtävää lähes vastaavasti sen aikaa, kun tietosuojavastaava on esimerkiksi lomalla. Varahenkilö tulisi ostaa jostain tarvittaessa, jos se ei muulla tavalla onnistu. Resursointi tulisi olla lähes 1:1 varahenkilöllä ja tietosuojavastaavalla. (T1)

> Resurssit eivät tällä hetkellä ole riittävät eikä niiden riittävyyttä varmisteta millään tavalla. Jos nyt lähetettäisiin kysely tietosuojatyötä tekeville ihmisille, vastaus olisi, että työn tekemiseksi pitäisi pystyä resursoimaan enemmän aikaa. Resursointia tulisi parantaa määrittelemällä tietosuojavastaavan rooli pääsääntöiseksi ja varmistamalla, että tietosuojavastaavalla on oma budjetti työn tekemiseksi. (T4)

Kolmen haastateltavan mukaan tietosuojatyön resursointia ja sen riittävyyttä ei arvioitu vuosittain organisaatiossa millään tavalla. Loput haastateltavista kertoivat, että he voivat raportoida vuosittaisessa kehityskeskustelussa tietosuojatyön resursoinnista ja sen riittävyydestä oman esihenkilönsä kanssa. Joissain kunnissa tietosuojatyön resursointia oli myös arvioitu sisäisen tarkastuksen toimesta. Yksi tietosuojavastaava kommentoi resursoinnin riittävyyden arviointia seuraavasti:

> Resursointia on selvitetty sisäisellä tarkastuksella ja säännöllisillä kehityskeskusteluilla. Tietosuojavastaavien tulisi myös itse avata suunsa, jos kokevat, että resursointi ei ole riittävää. (T1)

Vaikka resursoinnissa oli useimpien tietosuojavastaavien mielestä parannettavaa, niin koulutuksesta oli huolehdittu organisaatioissa hyvin ja tietosuojavastaavat olivat päässeet osallistumaan erilaisiin tarpeellisiksi kokemiinsa koulutuksiin. Tietosuojavastaavat kokivat, että koulutukset olivat hyvä keino oppia uutta ajankohtaisista asioista ja saada työvälineitä oman organisaation tietosuojan kehittämiseen. Noin puolet haastateltavista olivat saaneet osallistua tietosuojavastaaville tarkoitettuun yliopistotasoiseen koulutuskokonaisuuteen. Muita koulutuksia oli tietosuojavastaaville tarkoitettuja koulutusohjelmia, joissa on useita koulutuspäiviä eri teemoista. Riittävä resursointi ja kouluttautumisen mahdollisuudet ovat myös tietosuojavastaavan asemaan kohdistuvia selkeitä vaatimuksia tietosuoja-asetuksessa.

5.2.2. Tietosuojavastaavan aseman organisointi

Tietosuojavastaavan asemalle on määritelty tietosuoja-asetuksessa monia vaatimuksia ja ne tulee pystyä organisaatiossa varmistamaan. Haastateltavien mukaan tietosuojavastaavan tulee pysyä organisaation riippumattomana erityisasiantuntijana, joka neuvoo ja ohjeistaa sekä valvoo tietosuojan toteutumista lainsäädännön velvoittamalla tavalla. Haastateltavat korostivat, että tietosuojavastaava ei voi valvoa omaa työtään, joten tietosuojavastaavan tulisi pysyä neuvonantajan roolissa ja pääasiallisesti delegoida operatiiviset tehtävät organisaatioon.

Tietosuojavastaava voi valvoa ja ohjeistaa käytännön työn toteutusta, jotta työn lopputulos on laadukasta ja työ on tehty riittävällä tarkkuudella.

Haastateltavat korostivat, että tietosuojavastaavan rooli tulee organisoida organisaatiossa niin, että tehtävää hoitava asiantuntija pystyy säilyttämään riippumattomuutensa, eikä hänen rooliinsa kuulu johtaminen tai henkilötietojen käsittelyyn liittyvä päätöksenteko. Tietosuojavastaavan tulee arvioida kokoajan työtehtäviään sekä organisaation sisältä tulevia kysymyksiä tai pyyntöjä, jotka voivat mahdollisesti asettaa tietosuojavastaavan sellaiseen asemaan, jossa hänen riippumattomuutensa voi vaarantua. Tarvittaessa tietosuojavastaavan tulee pystyä jäävämään itsensä, jotta riippumaton asema säilyy. Mikäli tietosuojavastaavan työtehtävä ei ole kokoaikainen, hänen tulee myös arvioida ja huolehtia, että muut työtehtävät eivät aseta eturistiriitoja tai vaaranna hänen tietosuojavastaavan roolin riippumattomuutta. Tietosuojavastaavat kokivat, että kokoaikainen tietosuojavastaavan rooli mahdollistaisi riippumattomuuden toimia tehtävässä lainsäädännön edellyttämällä tavalla. Lisäksi haastateltavat sanoivat, että näin eturistiriitojen riski olisi vähäisempi, kun ei olisi muita tehtäviä, jotka voivat asettaa tietosuojavastaavan hankalaan tilanteeseen, jossa voi muodostua eturistiriitoja. Yksi haastateltava arvioi omaa riippumattomuuttaan näin:

> Tämä on kyllä hankala asia ja en minäkään sitä omaa riippumattomuuttani allekirjoita. Erityisesti tällaisessa pienessä organisaatiossa se tuntuu aika mahdottomalta. Tehtävät ovat haasteellisia tietosuojavastaavan työhön nähden niin, että riippumattomuus säilyisi. En oikein tiedä voiko sitä varmistaa muuten kuin kokoaikaisella resursoinnilla ja työnkuvalla. (T9)

Suurin osa haastateltavista olivat myös sitä mieltä, että tietosuojavastaavan rooli tulee organisoida organisaatiossa mahdollisimman korkealle niin, että hänellä on suora ja säännöllinen raportointikanava organisaation johtoon. Tehtävän organisointi mahdollisimman korkealle myös mahdollistaa sen, että tietosuojavastaava saa oikeanlaisen mandaatin tehdä työtä sen edellyttämällä tavalla. Oikein organisoitu rooli ja mandaatti ovat hyvin tärkeässä roolissa, sillä tietosuojavastaavan tulee pystyä tarvittaessa tekemään päätöksiä, joilla voi olla vaikutuksia organisaation toimintojen jatkuvuuteen. Tällaisia voivat olla esimerkiksi keskeyttämään henkilötietojen käsittely, jos arvioinnin perusteella käsittelystä aiheutuu merkittäviä riskejä rekisteröidyille. Mikäli tietosuojavastaavan tehtävä on organisoitu organisaatiossa suorittavalle tasolle, voi tietosuojavastaavan olla hankala saada tietoa organisaation johtoon, jos suora raportointikanava puuttuu. Suorittavalla tasolla esihenkilöitä voi olla hierarkiassa useampi ennen johdon edustajia. Kaksi tietosuojavastaavaa korostivat tehtävän organisointia seuraavasti:

> Esimerkiksi toimistosihteerin on aika vaikea mennä koko hallinnon yli sanomaan jotakin, että näin toimitaan. Siinä täytyy olla hyvin vahva ihminen, että pystyy ikään kuin ihmisenä sen roolin toteuttamaan sillä tavalla, että hänellä on vaikutusvaltaa organisaatiossa, jos sitä ei tule roolissa. Tehtävä tulisi asemoida mahdollisimman korkealle, että on mahdollisuus raportoida muun muassa kaupunginhallitukselle. Myös toimivan johdon tulee osoittaa muulle organisaatiolle, että nimitettävälle henkilöllä on riittävästi natsoja hoitaa tehtäviään. (T3)

> Toimistosihteerin tehtäviin en tätä kuitenkaan organisaatiossa asemoittaisi. Asemalla on suuri merkitys, koska sihteerin on aika vaikeaa mennä koko hallinnon yli sanomaan, että näin tämä asia tehdään. Siinä täytyy olla todella vahva ihminen, jotta sen pystyy toteuttamaan, eli ihmisenä täytyisi olla valtavasti vaikutusvaltaa, jos sitä ei ole omassa roolissa. (T6)

Aseman organisointi mahdollisimman korkealle tietosuojavastaava saa helpommin mandaatin toimia. Lisäksi tietosuojavastaavat kokivat, että tällaisessa asemassa saa käyttöönsä helpommin tärkeää ja ajankohtaista tietoa organisaation nykytilasta. Tiedon saamisella tarkoitetaan esimerkiksi kuulemalla erilaisista kehityshankkeista, joita suunnitellaan ja valmistellaan usein eri työryhmissä tai johtotasolla. Näillä kehityshankkeilla voi olla myös vaikutuksia tietosuojaan tai rekisteröityjen oikeuksiin ja vapauksiin, jonka vuoksi tietosuojavastaavan tulisi olla niissä osallisena. Haastateltavat kokivat, että mitä ylemmälle tietosuojavastaavan tehtävä sijoitetaan organisaatiossa, sen helpommin hän pääsee osallistumaan sellaisiin projekteihin tai työ- ja ohjausryhmiin, joissa käsitellään uusia kehitysaihioita, joissa voi tulla arvioitavaksi tietosuojanäkökulmat. Haastateltavat painottivat, että mikäli tietosuojanäkökulmat eivät ole täysin selviä, niitä ei välttämättä tunnisteta. Jos tietosuojaa ei osata huomioida, hankkeet eivät koskaan tule arvioitavaksi tietosuojavastaavalle. Mikäli hanke etenee määrittelyvaiheesta ilman, että tietosuojanäkökulmia ei olla arvioitu, tietosuojan tai tietoturvan määrittely voi olla hankalaa tai tehtävien muutosten hinta voi tulla kalliiksi. Yksi tietosuojavastaava kommentoi asiaa näin:

> On organisaatiokulttuurinen kysymys, että muistetaan tietosuojavastaavan olemassaolo. Se vaatii henkilöstön aktiivista herättelyä. Meilläkin on ollut haasteita esimerkiksi hankintojen kanssa, joiden kanssa on ollut viiveitä ja hankaluuksia viime aikoina. On käynyt niinkin, että on valittu toimittajat ja tehty sopimukset ja sitten huomataan käyttöönoton aikana, että tietosuojan osalta hankinta ei kestäkään päivänvaloa. Sitten joudutaan neuvottelemaan jälkikäteen tietosuoja-asioista. Siinä vaiheessa tietosuojavastaava on se hankala tyyppi, joka lyö jarrut kiinni. (T2)

Useamman haastateltavan mielestä organisaation johdon vastuulla on varmistaa eri keinoin, että tietosuojavastaava saa tietosuojatehtävien hoitamiseen tarvittavat tiedot. Haastateltavat kokivat, että mitä tunnetumpi tietosuojavastaava on, sen enemmän häntä osallistetaan organisaation tietosuoja-asioiden kehittämiseen. Ne keinot, joilla johto voi tietosuojavastaavan tunnettuutta edistää ovat esimerkiksi nimittämisen jälkeen laajalla jakelulla tehty tiedote sekä aktiivinen tietosuojapainotteinen viestintä. Lisäksi haastateltavat painottivat, että tietosuojalla tulisi olla näkyvä johdon tuki ja riittävät resurssit, jotta tietosuojan merkitys tunnistetaan kaikkialla organisaatiossa ja se huomioitaisiin riittävällä tarkkuudella.

Tietosuojavastaavan roolin tavoitettavuus tulisi varmistaa haastateltavien mukaan niin, että tietosuojavastaavan roolista tehdään kokoaikainen tai varmistetaan riittävät varahenkilöjärjestelyt, jotta tietosuoja-asiantuntija on aina tavoi-

tettavissa, vaikka tietosuojavastaava itse olisikin poissa töistä. Varahenkilöllä tulisi olla hyvä ymmärrys tietosuojahallinnan nykytilasta, organisaation henkilötietojen käsittely-ympäristöstä ja laajuudesta sekä riittävä henkilötietolainsäädännön ymmärrys ja osaaminen. Useampi haastateltava painotti, että jos osaavaa henkilöä ei saada täydentämään varsinaisen tietosuojavastaavan tehtävää, varahenkilö tulisi hankkia ostopalveluna.

5.3. Tietosuojavastaavan tehtävät ja niiden toteuttaminen

Tietosuojavastaavan tehtävät muodostavat laajan kokonaisuuden, jonka vähimmäisvaatimukset ovat määritelty tietosuoja-asetuksessa. Tehtäviin lukeutuvat muun muassa tietosuojaan liittyvä neuvonanto, tietosuojalainsäädännön vaatimustenmukaisuuden valvonta, viranomaisten yhteyshenkilönä toimiminen sekä tietosuojan vaikutustenarviointeihin osallistuminen. Haastateltavat täydensivät listaa edellä mainittujen lisäksi myös tietosuojaan liittyvän dokumentaation, kuten toimintaperiaatteiden, ohjeistusten ja tietosuojaselosteiden laatimisesta ja ylläpidon valvomisesta. Tietosuojavastaavien työnkuvaan kuuluivat myös tietosuojaan liittyvien riskien arviointi, henkilöstön kouluttaminen ja johdolle raportointi. Lisäksi oleellisena osana oli tietosuojan hallintamallin kehittäminen sekä erilaiset valvontatoimet kuten käyttöoikeuksien ajantasaisuus ja tietojärjestelmien tarkoituksenmukainen käyttö. Suurin osa oman toimensa ohella toimivista tietosuojavastaavista täydensivät, että heidän käytettävissä oleva työaika kaikkiin näihin tehtäviin rajoittui noin kahteen päivään kuukaudessa. Joillain haastateltavilla ajankäyttö oli jopa vähemmän. Kolme haastateltavaa luonnehtivat omaa ajankäyttöään seuraavasti:

> Se vaihtelee kuukausittain, mutta sanoisin, että se on keskiarvollisesti kaksi päivää, mitä ehdin käyttämään näihin asioihin. (T5)

> Aivan liian vähän. Periaatteessa mun työsopimukseen on määritelty, että se olisi 50%, mutta eihän se sitä oikeasti ole. Se ei toteudu, sillä muut työt vievät enemmän aikaa. (T9)

> Tällä hetkellä ajankäyttö tietosuojaan on noin 10% luokkaa. (T4)

Useampi omien tehtäviensä ohella toimivista tietosuojavastaavista kokivat, että he eivät tällä hetkellä ehdi hoitamaan kaikkia tietosuojaan liittyviä tehtäviä. Suurin osa haastateltavista kuitenkin kokivat, että käytettävissä olevilla työvälineillä työnteko oli riittävän tehokasta eikä työntekoa haitannut mikään työvälineisiin liittyvä asia. Useampi tietosuojavastaava kuitenkin täydensi vastaustaan, että tällä hetkellä heillä ei ole käytettävissään tietosuojan hallintaan tarkoitettua ohjelmistoa. Muutamassa organisaatiossa hankintapäätös oli kuitenkin tehty ja käyttöönottoprojekti oli käynnissä. Näissä kunnissa tietosuojavastaavat olivat hyvin tyytyväisiä siihen, että työnteko tehostuu entisestään. Toinen tehokkuutta

parantava, mutta tällä hetkellä puuttuva, toiminto oli haastateltavien mielestä raportointi. Tietosuojavastaavat kokivat, että he eivät saa ajantasaista raportointia tietosuojan tehokkuudesta eri toimialueilta, joka heikensi heidän omaa kyvykkyyttään kokonaiskuvan muodostamiseen ja raportointiin yleisellä tasolla. Enemmistö haastateltavista ei raportoinut säännöllisesti organisaation johdolle tietosuojan kypsyystasosta millään tavalla. Jotkut kertoivat raportoineensa johdolle tiettyjä tunnuslukuja tai ongelmatapauksia kuten tieturvaloukkauksia, mutta mitään systemaattista tapaa raportointiin ei ollut. Alle puolet haastateltavista kertoivat, että he raportoivat ylimmälle johdolle tietotilinpäätöksellä, tai laatimalla yleisen raportin tietosuojasta tietyin väliajoin. Vain yksi tietosuojavastaava kertoi, että hän osallistuu säännöllisesti johtoryhmän palavereihin ja raportoi siellä tietosuojan kehityksestä organisaatiossaan. Hän kommentoi omaa raportointiaan johdolle seuraavasti:

> Meillä raportoidaan ihan systemaattisesti riskienhallinnan osa-alueena myöskin tästä tietosuoja-asiasta kolmen kuukauden välein kaupunginhallitukselle. Vastuu aina kuntaorganisaatiossa kokonaisuudessaan on hallituksella eikä sitä voi siirtää. Tästä syystä näen itsekin tärkeäksi tämän raportoinnin, että ylimmällä johdolla on tieto siitä, missä mennään. (T6)

Raportointi koettiin aineistossa selkeäksi kehityskohteeksi ja useammalla haastateltavalla tietotilinpäätöksen tai muun vuosittaisen raportin tekeminen oli heidän työlistallaan.

Toinen selkeä kehityskohde raportoinnin lisäksi oli tietosuojan mittaaminen. Yli puolet haastateltavista kertoivat, että tietosuojalle ei ole tällä hetkellä selkeitä mittareita. Ne organisaatiot, missä mittareita oli määritelty, mitattiin pääasiallisesti määrällisiä tunnuslukuja tietoturvaloukkausten määrästä, tietosuojaselosteiden määrästä, rekisteröityjen oikeuspyynnöt ja toteutukset sekä henkilöstön tietosuojakoulutuksen suorittaneiden lukumäärä. Laadullisia mittareita ei ollut määritelty. Haastateltavat kuitenkin kertoivat, että mittaamista tulisi tehdä myös laadullisesti ja painottivat, että esimerkiksi tietosuojan vaikutustenarvioinnit ja niiden lopputulokset sekä tunnistetut riskit olisivat hyviä mittareita. Muita aineistosta erottuvia mittareita olivat henkilöstön tietosuojatietoisuuden taso, jota voitaisiin selvittää sisäisillä kyselyillä tai haastatteluilla. Määrällisistä mittareista aineistossa nousi tietoturvaloukkausten määrä, mutta kaksi tietosuojavastaavaa määritti myös tärkeäksi mitattavaksi kohteeksi tietoturvaloukkausten jälkeisen juurisyyanalyysin ja sen pohjalta tehtävät kehitystoimenpiteet.

Tietosuojavastaavat nostivat merkittäväksi kehitystehtävien tunnistamisen menetelmäksi tietosuojan nykytilan arvioinnit. Yli puolet haastateltavista kertoivat, että nykytilaa arvioidaan säännöllisesti joko itsearvioinnein tai ulkopuolisen osapuolen toimesta ostopalveluna. Ulkopuolisia auditointeja ja arviointeja oli teetetty jonkin verran, että pystytään varmemmin tunnistamaan eri kehityskohteita ja saadaan selkeitä suosituksia, miten kehitystoimenpiteet tulisi toteuttaa. Itsearvioinnin menetelmiksi nostettiin joko sisäisen tarkastuksen tekemät arvioinnit tai valtionhallinnon tietosuojatyöryhmien tekemät ohjeistukset tai julkisen

hallinnon tiedonhallinnan neuvottelukunnan (JUHTA) julkaisema viitekehys Tietosuoja-Asetuksen OsoitusKriteeristö (TAOK).

Kukaan haastateltavista ei tunnistanut, että heidän työnkuvaansa kuuluisi sellaisia tehtäviä, joita heidän ei tietosuojavastaavana kuuluisi tehdä. Suurin osa tietosuojavastaavista kuitenkin tunnistivat, että heidän organisaatiossaan on tehtäviä, joissa heidän tulisi olla mukana, mutta eivät ole. Aineiston mukaan tietosuojavastaavat olivat huolestuneita niistä kehittämishankkeista, joilla on henkilötietojen käsittelyyn liittyviä vaikutuksia tai niissä suoraan tehdään päätöksiä henkilötietojen käsittelyyn, mutta tietosuojavastaavat eivät ole näistä joko tietoisia tai eivät saa kutsua antamaan neuvoja. Kaksi tietosuojavastaavaa esitti huolensa seuraavasti:

> Ongelma on se, että tiedänkö kaikkia hankkeita, projekteja tai uusia sopimuksia, mitä täällä tehdään sillä tarkkuudella kuin pitäisi ehkä tietää. Tässä on tullut tällaisia ilmentymiä aika ajoin, että välttämättä ei tietohallintoon asti tai konsernihallintoon ole kantautunut ollenkaan. On tehty esimerkiksi jonkun ulkopuolisen tai EU:n määrärahoilla tai yhteistyökumppanin jotain sellaista, jossa olisi ollut ensiarvoisen tärkeätä, että tietosuoja- tai tietoturva-asiantuntijan olisi pitänyt olla mukana alusta alkaen. Nämä ovat myös isoja riskejä kunnalle. (T1)

> Nimenomaan nämä kehitysprojektit, että toistaiseksi ainakaan mua ei ole otettu mukaan. Jos kuulen jostain toimialakohtaisista kehitysprojekteista, niin yritän aina viestiä, että olettehan ottaneet nämä ja nämä asiat huomioon tietosuoja näkökulmasta. Meidän organisaatiossa ei ole tietoturvapäällikköä, joka vastaisi meidän tietoturvasta ja tämä on mielestäni puute. Meillä on kyllä organisaatio, joka huolehtii meidän puolesta tietoturvasta, mutta mulla ei ole näkyvyyttä siihen. Se on tällainen seudullinen yhteistyö myös, mutta meillä ei ole oikein näkyvyyttä heidän tekemiseen. Olen yrittänyt viestiä, että tähän tarvittaisiin näkyvyyttä. (T9)

Organisaatiokulttuurin kypsyystaso ja tietosuojavastaavan asemalla on aineiston mukaan suuri merkitys siihen, että kuinka tietosuojavastaava saa riittävät tiedot omien tehtäviensä suorittamiseksi. Moni haastateltavista painottivat, että eivät mielestään saa ollenkaan tai riittävän aikaisessa vaiheessa tietoa eri kehityshankkeista, joissa tulisi huomioida tietosuojanäkökulmat.

6. Pohdinta

EU:n yleistä tietosuoja-asetusta alettiin soveltamaan 25.5.2018 koko Euroopan Unionin alueella. Lakimuutos oli kansainvälisesti hyvin merkittävä, sillä se asetti henkilötietojen käsittelijöille ja rekisterinpitäjille aivan uudenlaisia vaatimuksia henkilötietojen käsittelyyn, joita sovelletaan myös EU:n ulkopuolella, kun käsitellään EU:n kansalaisten henkilötietoja. Yksi iso muutos velvoitteisiin on tietosuojavastaavan nimittäminen, joka on pakollista esimerkiksi kuntaorganisaatioissa. Tietosuojavastaavalla on haastava tehtävä organisaation neuvonantajana kaikkeen tietosuojaan ja henkilötietojen käsittelyyn liittyvissä asioissa sekä valvoa tietosuojalainsäädännön toteutumista. Tässä tutkimuksessa tarkoituksena oli selvittää, minkälaista osaamista kuntaorganisaatiossa työskentelevä tietosuojavastaava tarvitsee työssään ja miten tehtävä tulisi organisoida, jotta tietosuojavastaava voisi toimia tehtävissään tietosuojalainsäädännön edellyttämällä tavalla. Toisaalta tutkimuksessa pyrittiin myös selvittämään organisaation roolia tietosuojavastaavan tukemisessa, jotta hänellä on riittävät edellytykset onnistua tehtävässä. Tietosuojavastaavan tehtävä on haasteellinen niin siihen valitulle henkilölle kuin hänet nimittävälle organisaatiollekin. Nimittävän organisaation tulee arvioida täyttääkö henkilö kaikki lainsäädännön ja erilaisten tukevien ohjeistusten velvoittamat vaatimukset sekä tukea valittavaa henkilöä hyvin laajasti, jotta tehtävässä onnistuminen olisi mahdollista. Tutkimuksen lopputulokset avustavat kuntaorganisaatioita ja antavat näkökulmia, mitä tulee ottaa huomioon tehtävän organisoimisessa ja potentiaalisten kandidaattien arvioinnissa, kun tietosuojavastaavaa nimitetään.

Henkilön nimittämistä tehtävään ei tule tehdä sen perusteella kenellä siihen voisi olla aikaa, vaan organisaation johdon tulee arvioida ja selvittää löytyykö tehtävään kompetensseiltaan soveltuvaa henkilöä organisaation sisältä. Mikäli sellaista henkilöä ei löydy organisaation sisältä, tulee johdon rekrytoida osaava henkilö organisaation ulkopuolelta tai hankkia rooli ostopalveluna konsulttiorganisaatiolta. Johdon tulee tukea tietosuojavastaavaa ja määrittää roolille riittävät resurssit tehtävien hoitamiseksi. Riittäviin resursseihin kuuluu koulutuksiin osallistuminen, varahenkilön nimittäminen sekä riittävän ajankäyttö tehtävien hoitamiseksi. Johdon tulee myös huolehtia, että tehtävä on organisoitu riittävän korkealle organisaatiossa, jotta tietosuojavastaava saa riittävän mandaatin suorittaa kaikki lainsäädännön asettamat tehtävät myös käytännössä. Tutkimuksessa havaittiin, että tietosuojavastaavan aseman organisoinnilla ja tehtävien suorittamisella on riippuvuuksia. Tietosuojavastaavan voi olla esimerkiksi hankala raportoida suoraan organisaation johdolle, jos hänen roolinsa on organisoitu suorittavalle tasolle kuten toimistosihteeriksi. Tehtävien hoitaminen on myös todella haastavaa, jos tietosuojavastaavalle ei järjestetä riittävästi aikaa tietosuojatyön tekemiseksi. Tietosuojavastaavan roolia ei kuitenkaan tule organisoida johtoon, jos on syytä epäillä, että hänen riippumattomuutensa vaarantuu.

6.1. Tutkimuksen johtopäätökset

Aineistoanalyysissa tunnistettiin, että tietosuojavastaavan tarvitsemat tiedot ja taidot vastaavat kirjallisuuden perusteella kompetenssin määrittelyä. Kuntaorganisaation tietosuojavastaava ei selviä yksittäisillä työelämätaidoilla, vaan tarvitsee onnistuakseen kognitiivisia, toiminnallisia ja sosiaalisia tietoja ja taitoja, jotka luokitellaan kompetenssien osa-alueiksi. Tietosuojavastaavan keskeisiksi taidoiksi tunnistettiin sosiaaliset ja viestinnälliset taidot, asiantuntijataidot, itsesäätelytaidot, johtamis- ja verkostoitumistaidot sekä organisaatiotuntemus. Tietosuojavastaavan asemaa koskevat edellytykset tehtävässä onnistumiseksi taas olivat haastateltavien mukaan hyvin samankaltaisia kuin lainsäädäntö ne määrittää. Tutkimuksessa kuitenkin havaittiin, että tietosuojavastaavan asemalla on kuntaorganisaatiossa huomattava merkitys, jotta tietosuojavastaava pystyy käytännössä toteuttamaan velvollisuutensa. Esimerkkinä mainittiin, että joidenkin tehtävässä toimivien asemassa voi olla hankala esittää koko hallinnon yli eriäviä mielipiteitä.

Tutkimuksessa tunnistettiin, että asemalla voi olla riippuvuuksia tehtävien suorittamisen kanssa. Lisäksi tietosuojavastaavan tehtävissä korostui aiempaa kirjallisuutta enemmän myös teknisiä tehtäviä kuten tietoturvallisuuden vaatimusten määrittelyä, tietokantaosaamista ja käytönvalvontaa. Nämä taidot ovat tietosuojavastaavalle edellytyksiä, jotta tehtävässä voidaan onnistua. Tutkimuksessa havaittiin myös, että toisin kuin aihetta käsittelevässä kirjallisuudessa, verrattain vähäiseen merkitykseen tietosuojavastaavalta vaadittavissa kompetensseissa jäi toimivan hallintamallin rakentaminen ja ylläpitäminen. Tutkimuksen yksityiskohtaiset johtopäätökset ovat jaettu osa-alueittain tietosuojavastaavan tarvitsemiin kompetensseihin, aseman organisoiminen kuntaorganisaatiossa sekä tietosuojavastaavan suorittamiin tehtäviin.

6.1.1. Tietosuojavastaavan tarvitsemat kompetenssit

Aineistossa avainasemaan nousi tietosuojavastaavan työelämätaidot, joita tietosuojavastaava tarvitsee, että tehtävässä voi onnistua asetuksen velvoitteiden mukaisesti. Aineistossa nousseet vaadittavat työelämätaidot muodostavat yhdessä Le Deist ja Winterton (2005) mukaisesti kompetenssin vaatimukset. Ne vastaavat hyvin myös Van Toorn ym. (2019) mukaista määrittelyä kompetenssin osa-alueista. Aineistosta tunnistetut työelämätaidot ovat jaettu viiteen kategoriaan taulukkoon 2, jonka pohjana hyödynnetään Nykäsen ja Tynjälän (2012) työelämätaitojen ryhmittelyä.

Nykänen ja Tynjälä (2012, 21-22) ovat ryhmitelleet työelämätaidot seuraaviin kategorioihin: Akateemiseen tiedonmuodostukseen ja tieteelliseen ajatteluun, Tiedon integraation taidot, Sosiaaliset ja viestintätaidot, Itsesäätelytaidot sekä Johtamis- ja verkostoitumistaidot. Aiempi ryhmittely ei kuitenkaan suoraan soveltunut tietosuojavastaavan työelämätaitojen ymmärtämiseksi, joten sitä ke-

hitettiin vastaamaan tämän tutkimuksen havaintoja. Uudessa ryhmittelyssä yhdistettiin akateemiseen tiedonmuodostukseen ja tieteelliseen ajatteluun tiedon integraation taidot, jolloin niistä saadaan asiantuntijataidot. Asiantuntijataidoilla tarkoitetaan tässä kontekstissa niitä substanssitietoja ja taitoja, joita tietosuojavastaava tarvitsee kuntaorganisaatioissa. Muuttamattomana pysyivät sosiaaliset ja viestintätaidot, itsesäätelytaidot ja johtamis- ja verkostoitumistaidot. Viidenneksi työelämätaitokategoriaksi on nostettu aineistosta organisaatiotuntemus, jonka merkitys tietosuojavastaavan työelämätaitona on huomattava. Nykäsen ja Tynjälän (2012) ryhmittelyn lisäksi on käytetty aihepiiriä tukevaa teoriapohjaa erilaisista työelämätaitojen tutkimuksista, joissa on aineiston kanssa yhteneväisiä havaintoja.

Tietosuojavastaava tarvitsee työssään vahvoja sosiaalisia- ja viestintätaitoja, jotka ovat luokiteltu Nykäsen ja Tynjälän (2012) ryhmittelyn lisäksi myös Havelkan ja Merhoutin (2009) sekä Schilpzand, Hekman ja Mitchell (2015) tutkimuksissa työelämätaidoiksi. Sosiaalisiin ja viestinnällisiin taitoihin ryhmitellään niin hyvät suulliset- ja kirjalliset taidot kuin yhteistyötaidot muiden ihmisten kanssa. Sosiaalisiin ja viestinnällisiin taitoihin luokitellaan myös esiintymis- ja kouluttamistaidot. (Nykänen & Tynjälä, 2012.) Havelka ja Merhout (2009) lisäävät artikkelissaan, että informaatioteknologia-alalla työskentelevien asiantuntijoiden tulee pystyä tuottamaan helposti ymmärrettäviä raportteja. Raporttien tuottamisen lisäksi asiantuntijoilla tulee olla kyvykkyys ja rohkeus esiintyä ja esitellä muille havaintojaan ja kouluttaa muita. Tietosuojavastaavan työssä sosiaaliset– ja viestintätaidot ovat merkittävässä roolissa, koska tietosuojavastaava vastaa usein niin sisäisestä, ulkoisesta kuin eri sidosryhmille kohdistuvasta viestinnästä.

Nykäsen ja Tynjälän (2012) mukaan sosiaalisilla taidoilla tarkoitetaan myös useissa tilanteissa vaadittavia ryhmätyötaitoja. Tietosuojavastaavan tulee olla myös helposti lähestyttävä, jotta henkilöstö uskaltaa ottaa yhteyttä myös ongelmatilanteissa, jossa he ovat mahdollisesti toimineet väärin, tai vastoin ohjeita, ja joista saattaa seurata laajamittaisia tutkimuksia tai selvityksiä. Yleisesti voidaan sanoa, että sosiaalisilla- ja viestintätaidoilla tarkoitetaan niitä taitoja, joita tarvitaan ihmisten kanssa toimimiseen. Schilpzand ym. (2015) painottavat omassa tutkimuksessaan etenkin rohkeuden merkitystä, jotta voidaan muun muassa puuttua ja raportoida sellaisista epäkohdista, joista voi aiheutua työyhteisölle, raportoijalle, tai molemmille ongelmia. Epäkohdat tulee pystyä raportoimaan toimivalle johdolle, jolla on vastuu puuttua ilmi tuotuihin ja raportoituihin epäkohtiin, puutteisiin tai väärinkäytöksiin. Tällainen vastuu on myös tietosuojavastaavalla omassa tehtävässään, jolloin hänen tulee raportoida johdolle tai viranomaisille omassa organisaatiossa havaitut puutteet, ongelmat ja tietomurrot. Taulukossa 2. on esiteltynä ne työelämätaidot, joita tietosuojavastaavat työssään aineiston mukaan tarvitsevat ja joista yhdessä tulee kompetenssit.

Taulukko 2: Kompetenssien osa-alueet

Kompetenssien osa-alueet	**Työelämätaidot**
1. Sosiaaliset ja viestintätaidot	- Kommunikointitaidot, yhteistyötaidot, tiedon ja osaamisen jakaminen, tilannetajuisuus ja lähestyttävyys. - Vahvat suullisen ja kirjallisen ilmaisun taidot, kouluttamis- ja esiintymistaidot. - Kyky suunnitella ja laatia selviä ja ymmärrettäviä raportteja. - Kyky esittää asiat vakuuttavasti ja rohkeus seistä päätösten takana. - Rohkeus puuttua ongelmiin ja raportoida väärinkäytökset.
2. Asiantuntijataidot	- Analyyttinen ja kriittinen ajattelutapa. - Kuntaorganisaation soveltuvan lainsäädännön tunteminen. - ICT-osaaminen (kokonaisarkkitehtuuri, käyttövaltuushallinta ja tietokantaosaaminen), tietoturvallisuuden ymmärtäminen ja asiakirjahallinto sekä tietojenkäsittelyn osaaminen. - Suunnittelu- ja organisointitaidot ja kyky hahmottaa kokonaisuudet.
3. Itsesäätelytaidot	- Uuden tiedon hankkimisen ja omaksumisen taitot. - Itsensä jatkuva kehittäminen sekä valmiudet muutokseen ja uudistumiseen. - Itsenäisyys ja oman työn johtaminen. - Kyky sopeutua ja hyväksyä muutokset sekä joustavuus.
4. Johtamis- ja verkostoitumistaidot	- Oman itsensä johtamisen taidot, kyky priorisoida sekä verkostotarpeiden hahmottaminen ja osallistuminen. - Henkilöiden ja työn johtamisen taidot, muiden ohjaamisen ja kouluttamisen taidot, kyky suunnitella, organisoida ja johtaa projekteja. - Kyky käsitellä ja kohdata vaikeita ja haastavia asioita.
5. Organisaatiotuntemus	- Organisaation toimintojen ja ihmisten ja roolien tuntemus. - Organisaatiorakenteen ja ympäristön tuntemus. - Henkilötietojen keräämisen ja käsittelyn laajuuden tunteminen sekä käsittelijöiden hallinta. - Kyky tunnistaa ongelmakohdat ja kehittää vallitsevaa organisaatiokulttuuria.

Asiantuntijataidoilla tarkoitetaan niitä tietoja ja taitoja, joita tietosuojavastaava tarvitsee työssään. Ne eivät rajoitu pelkkään substanssiosaamiseen, vaan siihen luokitellaan myös ne taidot, jotka tukevat substanssiosaamista kuten tiedon analysointikyvyt, kriittinen ajattelutapa, kokonaisuuksien hahmottaminen sekä ongelmanratkaisutaidot. (Nykänen & Tynjälä, 2012) Allen ja van der Velden (2007) lisäävät tutkimuksessaan, että vahvan substanssiosaamisen lisäksi asiantuntijalla on kyky vaikuttaa ja vakuuttaa muut. Tällä on myös tietosuojavastaavan tehtävässä merkitystä, jotta hän pystyy torjumaan muutosvastarintaa organisaatioissa tai pystyy perustelemaan lisäresurssien tarvetta johdolle.

Havelka ja Merhout (2009) taas havaitsivat omassa tutkimuksessaan, että kokonaisuuksien hahmottaminen ja analyyttinen ajattelutapa ovat informaatioteknologian alalla asiantuntijatyössä hyvin merkityksellisessä asemassa ja taidot arvotettiinkin kolmen tärkeimmän joukkoon. He myös tunnistivat, että informaatioteknologian parissa työskentelevien kompetensseihin kuuluvat ongelmien ratkaisukyvyt sekä suunnittelu- ja organisointitaidot ja ideoiden mallintaminen. Tietosuojavastaavan työssä tulee pystyä hyödyntämään teoriaa käytännön ongelmien ratkaisemiseksi. Tällainen voi olla esimerkiksi lainsäädännön tulkitseminen ja eri viranomaisratkaisujen tai päätösten analysointia ja niiden soveltamista oman organisaation toimintaan. Toisaalta se voi myös olla teknisten tietoturvakontrollien määrittämistä henkilötietojen suojaamiseksi. Tietosuojavastaavat tarvitsevat lisäksi hyviä suunnittelu- ja organisointitaitoja, jotta he pystyvät tehokkaasti delegoimaan tehtäviä palvelualueille, jotta he voisivat itse säilyttää mahdollisimman hyvin riippumattomuutensa ja suorittaa enemmän valvontaan liittyviä tehtäviä.

Kolmantena työelämätaidon luokkana on itsesäätelytaidot, joilla tarkoitetaan niitä asiantuntijataitoja, joilla edistetään ja mahdollistetaan elinikäistä oppimista kuten uuden tiedon hankinta- ja omaksumiskykyjä. Itsesäätelyllä tarkoitetaan myös joustavuutta sekä mukautumis- ja sopeutumiskykyä erilaisiin työelämän muutostilanteisiin. Allen ja van der Velden (2007) painottavat omassa teoksessaan erityisesti elinikäisen oppimisen merkittävyyttä, jotta työelämässä vaadittavat kompetenssit säilyvät ajantasaisina koko työuran ajan.

Havelka ja Merhout (2009) lisäävät teoksessaan, että asiantuntijalta vaaditaan kykyä saattaa asiat valmiiksi. Lisäksi joustavuus ja sopeutumiskyky oli heidän havainnoissaan arvotettu korkealle. Tietosuojavastaavilta edellytetään asiantuntijataitojen lisäksi mukautumis- ja sopeutumiskykyä, kun sovellettaviin lakeihin ja vaatimuksiin tulee uudistuksia tai lain tulkintaan tulee muutoksia, jotka edellyttävät muutosten ajamista organisaation toimintatapoihin ja prosesseihin. Tämä helpottaa tietosuojavastaavaa myös soveltamaan tietojaan eri toimialoilla ja organisaatioissa. Lisäksi tietosuojavastaavan tulee pystyä aktiivisesti etsimään ja omaksumaan uutta tietoa, jotta työelämätaidot pysyvät ajantasaisena ja organisaation toimintaa pystytään kehittämään määrätietoisesti kohti tavoitteita ja vaatimustenmukaisuutta. Tietosuojavastaavan tulee olla myös kykenevä johtamaan omaa työtään, olemaan aktiivinen ja pystyä työskentelemään itsenäisesti sekä riippumattomasti.

Johtamis- ja verkostoitumistaidot ovat luokiteltuna neljäntenä työelämätaitona. Havelka ja Merhout (2009) kertovat, että oman työn ja muiden ihmisten johtamistaidot ovat asiantuntijan roolissa hyvin merkittävässä roolissa, sillä asiantuntijoiden tulee pystyä johtamaan omaa työtään pitkäjänteisesti ja suunnitelmallisesti priorisoiden erilaisia työtehtäviä. Myös tietosuojavastaavan rooliin kuuluu itsenäinen työskentely, mutta itsenäisen työn lisäksi siihen kuuluu olennaisesti myös erilaisissa hankkeissa ja projekteissa työskentely. Näissä tilanteissa hänen tulee pystyä johtamaan muiden työtä tai toimimaan johtavana asiantuntijana asianmukaisesti vähintään tietosuojan vastuualueiden osalta. Schilpzand ym. (2015) mukaan työyhteisöissä kohtaa välillä vaikeita tilanteita. Tietosuojavastaavan rooliin kuuluu mahdollisesti vaikeiden asioiden käsittely, kuten tietomurtojen selvittely ja näistä ilmoittaminen rekisteröidyille. Ilmoittamisvelvollisuuden lisäksi rekisterinpitäjän tulee pystyä ohjeistamaan rekisteröityjä, miten mahdollisesti voidaan pienentää heidän oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Tietosuojavastaavan työtehtäviin kuuluu lisäksi olennaisesti muiden neuvominen, ohjeistaminen ja kouluttaminen. Nykänen ja Tynjälä (2012) havaitsivat omassa tutkimuksessaan, että verkostotarpeiden hahmottaminen ja verkostoituminen ovat yksi merkittävä työelämätaito, jolla mahdollistetaan ajantasaisen tiedon saamista ja analysointia vertaisilta, tai tarvittavista tietolähteistä. Tämä koettiin myös aineiston perusteella hyvin tarpeelliseksi myös tietosuojavastaavien kesken, koska suurin osa koki saavansa hyvää ja ajantasaista tietoa verkostoilta, kuten seudullista yhteistyötä tekeviltä tietosuojavastaavilta, Kuntaliiton asiantuntijoilta, koulutuksista tai eri viranomaislähteistä. Havelka ja Merhout (2009) havaitsivat, että kyky suunnitella ja johtaa projekteja sekä ihmisiä ovat asiantuntijoilla sellaisia taitoja, joita muut asiantuntijat arvostavat. Myös tietosuojavastaavan tulee pystyä jakamaan tietoa ja kouluttamaan muita tietosuoja-asioissa sekä henkilötietojen käsittelyyn liittyen.

Viimeiseksi työelämätaidoksi luokiteltiin organisaatiotuntemus. Aineiston perusteella organisaatiotuntemus on avaintekijänä tietosuojavastaavan tehtävässä onnistumiselle, sillä hänen täytyy tietää ja ymmärtää kokonaisvaltaisesti organisaation toiminnot ja niiden käytäntöjä, jotta hän pystyy antamaan neuvoja ja ohjeita, kuinka henkilötietojen käsittely ja suojaus tulee niissä toteuttaa. Havelkan ja Merhoutin (2009) mukaan organisaatiotuntemus koostuu ihmisten ja roolien tuntemuksesta, liiketoimintojen tuntemisesta sekä prosessien ja käytänteiden osaamisesta sekä kyvystä kehittää ja mallintaa uusia käytäntöjä. Schilpzand ym. (2015) painottivat teoksessaan organisaatiotuntemuksen merkitystä kontekstissa, jossa vastuuhenkilöiden tulee pystyä havainnoimaan sekä tunnistamaan epäkohtia ja puutteita organisaatiokulttuurissa ja eri toiminnoissa. Epäkohdista tulee pystyä raportoimaan ja niihin tulee puuttua suunnitelmallisesti ja määrätietoisesti, jotta ne saadaan korjattua asianmukaisesti. Tietosuojavastaavan työssä tulee pystyä ymmärtämään eri toimintojen prosesseja ja käytäntöjä, jotta niitä pystytään kehittämään niin, että tietosuoja tulee huomioitua lainsäädännön velvoittamilla tavoilla. Lisäksi tietosuojavastaavan tulee puuttua toimintaan, jos havaitaan epäkohtia tietosuojan toteutumisessa tai puutteita henkilötietojen suojauskeinoissa.

6.1.2. Tietosuojavastaavan tehtävän organisointi

Tietosuojavastaavan asema organisaatiossa vaikuttaa aineiston perusteella selvästi tehtävässä onnistumiseen. Roolin organisointi kuntaorganisaatiossa vaatii suunnittelua, jotta pystytään varmistamaan tietosuojavastaavan aseman vaatimukset lainsäädännön edellyttämällä tavalla. Aineiston mukaan tietosuojavastaavalla tulee olla riittävät resurssit hoitaakseen hänelle määritetyt tehtävät. Mikäli tietosuojavastaavan tehtävä ei ole kokoaikainen, aineiston mukaan riskiksi nousee muun muassa haasteet ajankäytössä sekä mahdolliset muiden tehtävien hoitamisen aiheutuvat tilanteet, joissa tietosuojavastaavan riippumattomuus vaarantuu. Roolin tulisi olla erityisasiantuntijan tehtävä, joka on sijoitettu mahdollisimman korkealle organisaation hierarkiaan. Näin vältytään riskiltä, jossa tietosuojavastaavan tulee edistää tietosuojaan tai rekisteröityjen oikeuksiin ja vapauksiin liittyviä asioita omien esihenkilöiden kautta, jossa raportointi voi pysähtyä. Näin varmistetaan myös johdolle raportoinnin velvoite ja vastuu. (Andreasson ym. 2019, s. 95.)

Andreasson ym. (2019, s. 95) esittävät teoksessaan, että tietosuojavastaavan aseman tulee myös olla sellainen, jossa tietosuojavastaava ei altistu riippuvuuksille esimerkiksi henkilötietojen käsittelyyn liittyvässä päätöksenteossa. Aseman määrittämisessä tulee siis huomioida se, että jos tehtävä sijoitetaan organisaation johtoon, tietosuojavastaava voi kohdata useammin riippumattomuutta uhkaavia tekijöitä. Avuksi voidaan kehitellä esimerkiksi riippuvuusrekisterin ja tunnistaa millaisia eturistiriitoja voi tehtäväkohtaisesti syntyä. Aineiston mukaan tietosuojavastaavan tulisi myös itse tarkastella jatkuvasti omia työtehtäviään ja pyrkiä tunnistamaan riippumattomuuteen kohdistuvia tekijöitä ja tarvittaessa jäävätä itsensä sellaisten tehtävien hoitamisesta. Mikäli työtehtävä ei ole kokoaikainen, tulee muiden työtehtävien olla sellaisia, jotka eivät aiheuta eturistiriitoja tietosuojan ja rekisteröityjen oikeuksien ja vapauksien suojaamiselle ja edistämiselle. Tietosuojavastaava ei myöskään saa ottaa tehtävissään ohjeita vastaan rekisterinpitäjältä. (Brezniceanu, 2017)

Edistääkseen mahdollisuuksia onnistua tehtävässä, tietosuojavastaavalle työhön määritettävien resurssien tulisi aineiston mukaan painottua työhön käytettävään ajankäyttöön sekä ostopalveluiden hyödyntämiseen. Andreasson ym. (2019, s. 102-103) mukaan tärkeimpiä resursseja tietosuojatyössä onkin aika. Ajankäyttö tulee jakaa tehtävien ja prioriteettien mukaan, joka on haastavaa etenkin, jos tietosuojavastaavan työtä tehdään muiden tehtävien ohella. Organisaatio itse määrittelee riittävän ajan, joka vaihtelee henkilötietojen käsittely-ympäristön ja laajuuden mukaan. Aineiston mukaan ajankäyttö on todella haasteellista kuntaorganisaatioissa, jossa muita tehtäviä on paljon. Tästä syystä aineistossakin painottui tarve nimittää kokoaikainen tietosuojavastaava. Useissa kunnissa tietosuojaan varattu aika jäi hyvin vähäiseksi. Sama ilmiö ajankäytön haasteellisuudesta on havaittu Kanta-palvelujen tietosuojakyselyssä, joissa enemmistö ajankäytöstä jää kaikkien vastaajien edustamilla sektoreilla alle 20% kokonaisajankäytöstä. (Kanta, 2019)

Tietosuojatyölle tulisi mahdollisuuksien mukaan allokoida oma kustannuspaikka ja kehitystyön budjetti, jota tietosuojavastaava voisi oman harkintansa mukaan hyödyntää niihin tehtäviin, mihin milloinkin fokusoidutaan. Ostopalveluilla tarkoitettiin muun muassa ulkopuolisten tarjoamia konsultointi- sekä auditointipalveluita. Ostopalveluiden lisäksi tietosuojavastaavalla tulisi olla käytettävissä myös varahenkilö, jolla olisi lähes vastaavanlaiset kompetenssit hoitaa tehtäviään kuin pääasiallisella tietosuojavastaavalla. Näin turvataan pääasiallisen tietosuojavastaan loma- ja poissaoloajat. Varahenkilö voi olla kuntaorganisaation sisältä, tai ostopalveluiden kautta hankittava ulkopuolinen resurssi. Ulkopuolista resurssia hyödyntäessä tulee varmistua siitä, miten hänen organisaatiotuntemuksen vaatimukset täyttyvät.

Tietosuojavastaavan tulee lisäksi saada kouluttautua tehtävissään, jotta taataan ajantasainen sekä riittävä osaaminen. Andreasson ym. (2019, s. 102-103) määrittelevät toiseksi tärkeäksi tekijäksi kouluttautumisen mahdollisuuden. Kouluttautumisen tulee olla säännöllisesti toistuvaa. Aineiston mukaan tietosuojavastaavilla oli tarjottu mahdollisuuksia kouluttautumiseen ja heillä itsellään oli mahdollisuus vaikuttaa koulutuksen laajuuteen, vaikka siitä olisikin tullut kustannuksia organisaatiolle.

6.1.3. Tietosuojavastaavan tehtävien toteuttaminen

Andreasson ym. (2016, s. 58) kertovat teoksessaan, että tietosuojavastaavan tehtävät tulee määritellä työsopimukseen tai sen liitteeksi laadittavaan tehtävänkuvaan. Tehtävien tulee olla vähintään ne, mitä tietosuojalainsäädännössä määritellään, mutta siihen voi kuulua muitakin tehtäviä kuten tietotilinpäätöksen laadinta, käytönvalvonta sekä omavalvontasuunnitelman valmistelua. Andreasson ym. (2019, s. 95-96) lisäävät, että tietosuojavastaavan tehtäviin kuuluu myös tietosuojaa määrittelevän ja tukevan dokumentaation laatiminen, riskien arviointi ja henkilöstön kouluttaminen sekä tietosuojaan liittyvä viestintä. Monfared ym. (2018) listaavat tietosuojan hallintamallin kehittämisen ja ylläpidon sekä tietojärjestelmien käytön ja vaatimustenmukaisuuden valvonnan.

Aineistossa toistui teorian kanssa samoja tehtäviä, mutta johdon raportointi ja tietosuojan mittaaminen eivät kuuluneet tietosuojavastaavien tehtäviin niin laajasti kuin olisi ehkä pitänyt. Säännöllistä raportointia ja mittaamista tehtiin alle puolessa otannasta. Andreasson ym. (2019, s. 185-187) kertovat teoksessaan, että johdon raportointi on tietosuojavastaavalle tärkeä tehtävä, jotta johto pysyy tietoisena tietosuojan nykytilasta sekä siihen mahdollisista liittyvistä uhkista ja riskeistä tai kehitystarpeista. Säännöllinen raportointi voi myös avustaa tietosuojavastaavaa saamaan paremmat resurssit työssä onnistumiseksi. Raportointia voidaan tehdä yksittäisistä asioista, mutta siihen tulisi olla myös säännönmukainen työkalu kuten tietotilinpäätös. Tietotilinpäätös toimii raporttina, joka kuvaa organisaation tietosuojan nykytilaa ja tiedonhallinnan tehokkuutta ja avaa esimerkiksi erilaisia tietosuojan mittareita tai tunnuslukuja. Raportointi tulee tehdä faktojen perusteella ja se tulee laatia riippumattomasti.

Tietosuojan aktiivinen seuranta, arviointi ja mittaaminen ovat merkityksellisessä roolissa, kun haetaan suuntaa kehitystyölle. Andreasson ym. (2019, s. 195) luettelevat teoksessaan useita seurattavia mittareita kuten tietosuojapoikkeamat, rekisteröityjen neuvominen sekä henkilötietojen poisto- ja tarkastuspyynnöt, tietosuojarikkomukset sekä henkilöstön koulutusmäärät. Näiden lisäksi on tärkeätä seurata parhaita käytänteitä ja kerätä käyttäjiltä palautetta. Dhillon, Oliveira ja Syed (2018) havaitsivat tutkimuksessaan, että organisaatioiden tulee seurata omaa kehitystään ja verrata niitä jatkuvasti parhaisiin käytäntöihin, jotta kehitys ja jatkuvan kehittämisen prosessi eivät pysähdy missään vaiheessa. Näin voidaan luoda lisäarvoa kuten uusia ominaisuuksia käyttäjille ja asiakkaille, kuten heidän oma kykynsä vaikuttaa tietosuojaan henkilötietojen käsittelyyn yleisellä tasolla. Tällä voi olla positiivinen vaikutus asiakaskäyttäytymiseen ja vähentää esimerkiksi tarkastus- tai poistopyyntöjen määrää kuntakontekstissa.

Aineistossa nousi esiin tietosuojavastaavien huoli sellaisista henkilötietojen käsittelyyn liittyvästä toiminnasta, kuten esimerkiksi kehityshankkeista tai hankinnoista, joissa tietosuojavastaavan tulisi olla mukana, mutta eivät ole. Andreasson ym. (2019, s. 188-189) käsittelevät teoksessaan sisäänrakennetun ja oletusarvoisen tietosuojan vaatimuksia ja listaavat muun muassa tietosuojan vaikutusten- ja riskienarvioinnin (DPIA) sekä erilaisia järjestelmävaatimuksia kuten tietojen anonymisointi- ja pseudonymisointikyvykkyydet. Ustaran ym. (2018, 203-204) lisäävät omassa teoksessaan muita vaatimuksia kuten henkilötietojen ajantasaisen inventaarion sekä järjestelmien kyvykkyydet tuhota tarpeettomat tiedot automaattisesti säilytysajan jälkeen. He myös painottavat enemmän automatisoitua tietojenkäsittelyä, jolloin manuaalisten virheiden määrä vähenee.

Sisäänrakennettu ja oletusarvoinen tietosuoja on merkittävä vaatimus, joka tuo rekisterinpitäjille haasteita etenkin, jos tietosuojavastaavalta ei osata kysyä neuvoa sellaisissa hankkeissa tai hankinnoissa, joissa näitä vaatimuksia tulisi harkita ja ottaa käyttöön. Tietosuojavastaavan asemassa tulisi saada riittävät tiedot tehtävien hoitamiseksi ja hänen tulisikin osallistua kaikkiin tietosuojaa koskevien asioiden arviointiin. Tämä muodostaa riippuvuuden tehtävien suorittamisen ja roolin organisoinnin välille. Tehtävää ei voida suorittaa, jos asema ei ole sellainen, jossa tiedonsaanti ja resursointi toteutuvat riittävän hyvin. Onnistuminen edellyttää johdon sitoutumista tietosuojatyöhön ja vastuuttaa kaikki työntekijät esimerkiksi tietosuojatyön toimintaperiaatteissa tai tietosuojapolitiikassa ottamaan yhteyttä tietosuojavastaavaan kaikissa tilanteissa, joissa he epäilevät, että henkilötietojen käsittely-ympäristössä on tapahtumassa muutoksia, jotka pitää arvioida tietosuojavastaavan kanssa. (Andreasson ym. 2019, s. 93-96.)

Tietosuojavastaavan roolin organisointi luo edellytykset tehtävien toteuttamiselle. Tehtävään nimitettävän tietosuojavastaavan asema, resursointi ja ajankäyttö tulee olla tasapainossa, jotta kaikki tehtävät pystytään toteuttamaan täysimääräisesti ja riittävän hyvällä laadulla määräaikaan mennessä. Taulukossa 3. esitän tunnistettuja tehtävien ja roolin organisoinnin välisiä riippuvuuksia.

Taulukko 3: Roolin ja tehtävien väliset riippuvuudet

Roolin organisointi		Tehtävät
Johdon tuki, riittävä resursointi ja ajankäyttö.	→	Lainsäädännön vaatimustenmukaisuuden arviointi ja valvonta, mittaaminen ja raportointi.
Riippumattomuus, itsenäisyys ja eturistiriitojen välttäminen.	→	Dokumentaation laatiminen, kouluttaminen, ohjeistaminen sekä henkilöstön ja rekisteröityjen neuvontatehtävät.
Erityisasiantuntijan asema mahdollisimman korkealla organisaatiossa.	←	Riskien arviointi, tietosuojan vaikutustenarviointien toteuttaminen ja vaatimustenmäärittely tai muut sisäänrakennetun ja oletusarvoisen tietosuojan edistäminen. Tarvittaessa henkilötietojen käsittelyn keskeyttäminen, jos riski on liian korkea.

Tietosuojavastaavan asema tulee siis olla sijoitettu organisatorisesti riittävän korkealle, jotta hän saa tarpeellisen informaation henkilötietojen käsittelyyn liittyen ja mandaatin toimia tehtävissään lainsäädännön vaatimalla tavalla. Hänellä on mahdollisuus käyttää tietosuojatyöhön aikaa ja resurssit toimia ovat sellaiset, että tehtävät voidaan toteuttaa aikataulujen mukaisesti riittävällä laajuudella ja tehtävien edellyttämien laatuvaatimusten toteutuessa. Lisäksi aseman tulee olla sellainen, jossa tietosuojavastaavan riippumattomuus säilyy, hänelle ei tarjota neuvoja hoitaa tehtäviä ja voi toimia itsenäisesti sekä välttäen eturistiriitoja.

6.2. Tutkimuksen reliabiliteetti

Hirsjärvi ym. (2009) määrittelevät teoksessaan, että reliabiliteetilla tarkoitetaan tutkimuksen toistettavuutta, joka vähentää sattumanvaraisuuden mahdollisuutta tuloksissa. Reliabiliteetin lisäksi tutkimuksissa tulee arvioida tutkimusmenetelmän validiteettia, jolla arvioidaan sitä, mitä tutkimuksessa on tarkoitus mitata. Hirsjärven ym. (2009, 160-164) mukaan laadullisessa tutkimuksessa on haastavaa päästä täydelliseen objektiivisuuteen, sillä tutkijan tieto ja ymmärrys sekä arvot vaikuttavat tutkimusprosessiin. Tuomen ym. (2018, 24) mukaan tutkimustuloksissa näkyy aina tutkijan käyttämät menetelmät ja tietopohja, joka kertoo paljon itse tutkimusprosessista. Tutkijan ymmärrys vaikuttaa tutkimusasetelman muodostamiseen, jonka vuoksi tiedon katsotaan olevan enemmän subjektiivista kuin objektiivista.

Tutkija työskentelee tutkimuskohteena olevan ilmiön ympärillä yksityisellä sektorilla, joten tutkimuksen reliabiliteettiin ja objektiivisuuteen on kiinnitetty huomiota valitsemalla tutkimuksen kohteeksi kuntaorganisaatiot yksityisellä sektorilla toimivien yritysten sijaan. Lisäksi tutkija on pyytänyt kommentteja teemahaastatteluja varten luotuun kysymyspohjaan alalla työskenteleviltä substanssiasiantuntijoilta. Tutkija on pyrkinyt vahvistamaan tutkimuksen luotettavuutta kohdentamalla tutkimuksen kuntaorganisaatioiden tietosuojavastaavien ympäristöön sekä kiinnittämällä huomiota aineiston analyysivaiheessa siihen, että aineistoon ei yhdistyisi liikaa tutkijan omia tulkintoja. Tutkimuksen reliabiliteettia arvioidessa tulee huomioida, että aineisto kerättiin samassa roolissa toimivilta, eri kuntien yleishallinnon tietosuojavastaavilta.

6.3. Tulosten hyödyntäminen, rajoitukset ja aiheita jatkotutkimukselle

Aiempaa tutkimusta tietosuojavastaavien työstä ja asemasta on olemassa verrattain vähän, vaikka yleinen tietosuoja-asetus on ollut voimassa vuodesta 2016. Tämän tutkimuksen tuloksia voidaan hyödyntää etenkin kuntaorganisaatioissa, mutta soveltaen myös muissa organisaatioissa, joissa tulee nimittää tietosuojavastaava. Tuloksia voidaan hyödyntää organisaatioissa ennen tietosuojavastaavan nimittämistä ja roolin organisointia, jotta voidaan varmistaa, että nimitettävällä henkilöllä on vaadittavat kompetenssit. Työn perusteella voidaan myös organisoida jo nimitetyn tietosuojavastaavan tehtäviä ja asemaa vastaamaan tutkimuksen tuloksia. Tutkimuksen rajoituksina ovat kuitenkin tutkimusmenetelmä ja otannan laatu ja määrä, joten työ ei ole sellaisenaan yleistettävissä täysin yksityiselle sektorille eikä se tarjoa käytännönläheisiä työkaluja organisaation johdolle kuinka arvioida organisaation nykytilaa tutkimuksen havaintoja ja suosituksia vasten.

Yleistä tietosuoja-asetusta on sovellettu 25.5.2018 lähtien, joten kuntaorganisaatioiden tietosuojavastaavat ovat toimineet tehtävissään yli kaksi vuotta. Jatkotutkimusaiheina voidaan tutkia niin yksityisellä tai julkisella sektorilla, että vastaako tietosuojavastaavan asema ja kompetenssit organisaatioissa tietosuoja-asetuksen vaatimuksia tai vertailla näitä esimerkiksi ristiin ja tutkia minkälaisia eroja asemassa yksityisen ja julkisen sektorin välillä on. Lisäksi tietosuoja-asetuksessa itsessään on vielä paljon tutkittavaa, kuten esimerkiksi millaisia taloudellisia vaikutuksia tietosuojan kehittämisellä organisaatioilla on ollut tai miten kansalaisten luottamus erilaisiin verkossa toimiviin yrityksiin on kehittynyt tietosuoja-asetuksen voimaantulon jälkeen. Näissä tutkimuksissa aineiston kerääminen organisaation eri tasoilta voisi antaa erilaisia näkemyksiä ja tarjota monimuotoisia havaintoja.

7. Yhteenveto

Yleinen tietosuoja-asetus on ollut merkittävä muutos kansainväliseen tietosuojalainsäädäntöön ja sen voimaantulolla on ollut isoja vaikutuksia siihen, miten rekisterinpitäjät ja henkilötietojen käsittelijät käsittelevät henkilötietoja ja millaisia hallintamenetelmiä on määritetty henkilötietojen suojelemiseksi. Tietosuoja-asetusta sovelletaan koko Euroopan Unionin alueella ja kansainvälisesti aina, kun käsittelyssä on EU:n kansalaisen henkilötiedot. Yksi suuri muutos rekisterinpitäjille ja henkilötietojen käsittelijälle on ollut nimittää tietosuojavastaava. Tämä on luonut tarpeen uudelle ammatille, joka edellyttää nimitettävältä henkilöltä vankkaa ammattitaitoa ja muita kompetensseja, jotta tehtävässä voidaan onnistua vaatimustenmukaisesti. Sen lisäksi, että tietosuoja-asetus määrittelee yleisellä tasolla erilaisia vaatimuksia nimitettävälle henkilölle, se edellyttää myös nimittävältä organisaatiolta tarkkaa arviota roolin organisoinnille sekä paljon tukea itse tietosuojavastaavalle. Koska tietosuoja-asetus määrittelee vaatimukset kompetensseista ja asemasta hyvin yleisellä tasolla, se on luonut tulkinnanvaraisuutta ja tämä näkyy vaihteluna roolin organisoinnissa tutkimuskohteena olevissa kuntaorganisaatioissa.

Tutkielman tarkoituksena oli tutkia kuntaorganisaatioiden tietosuojavastaavien roolia ja siinä tarvittavia kompetensseja. Aihetta lähestyttiin haastattelemalla erikokoisten kuntien ja kaupunkien tietosuojavastaavia, joilla on oman työnsä kautta muodostunutta käytännön kokemusta niistä työelämätaitojen vaatimuksista, mitä työelämässä tarvitaan. Heillä on myös näkemystä siitä, miten rooli tulee organisoida sekä millaista tukea organisaatiolta ja organisaation johdolta vaaditaan, jotta työssä voidaan onnistua. Aineisto kerättiin haastattelemalla yhdeksän kunnan tai kaupungin tietosuojavastaavaa. Haastattelut toteutettiin teemahaastatteluilla ja saatu aineisto analysoitiin teemoittelemalla.

Tutkielmassa havaittiin, että kuntaorganisaatioiden tietosuojavastaavien tarvitsemat työelämätaidot voidaan ryhmitellä viiteen eri luokkaan, joihin kuuluu erilaisia taitoja. Yksi keskeisimmistä työelämätaidoista on sosiaaliset ja viestintätaidot, joihin kuuluu muun muassa hyvät suulliset- ja kirjalliset taidot sekä lähestyttävyys. Tietosuojavastaava tarvitsee myös hyvät ja ajantasaiset asiantuntijataidot, itsesäätelytaidot sekä johtamis- ja verkostoitumistaidot. Merkittäväksi taidoksi aineistossa nousi myös organisaatiotuntemus, johon kuuluu esimerkiksi henkilötietojen käsittelytoimintojen ja prosessien tunteminen. Analyysissa havaittiin, että tunnistetut työelämätaidot vastaavat kirjallisuuden perusteella määritetyjä kompetensseja.

Tutkielman yksi havainto oli, että tietosuojavastaavan rooli tulee olla erityisasiantuntijan tehtävä mahdollisimman korkealla organisaation hierarkiassa. Tietosuojavastaavan tehtävä voi olla joko päätoiminen tai muiden tehtävien ohessa suoritettava. Tietosuojatyöhön tulee varata riittävästi aikaa, eikä muut tehtävät saa vaarantaa tietosuojavastaavan riippumattomuutta tai aiheuttaa eturistiriitatilanteita. Tietosuojavastaavalle tulee varata aikaa ja rahaa kouluttautua

säännöllisesti. Tietosuojatyöhön voidaan myös määrittää mahdollisuuksien mukaan oma budjetti tietosuojan kehitystyötä varten, jota voidaan hyödyntää esimerkiksi ostopalveluina hankittavaan ulkopuoliseen arviointiin tai auditointiin. Tutkielmassa havaittiin myös, että tehtävien suorittamisella ja roolin organisoinnin välillä on riippuvuuksia. Mikäli tietosuojavastaavalle ei ole organisoitu riittävästi resursseja ja muut johdon määrittelemät tehtävät vievät liikaa hänen aikaansa, se voi vaikuttaa tietosuojatyössä suoriutumiseen. Riittämättömät resurssit ovat vastoin tietosuoja-asetuksen vaatimuksia ja voivat johtaa rekisteröityjen oikeuksien ja vapauksien toteuttamatta jättämiseen.

Tutkielman tavoitteisiin pystyttiin vastaamaan ja tuottamaan samalla uutta tietoa siitä, millaisia kompetensseja tietosuojavastaavat tarvitsevat kuntaorganisaatioissa. Aiempaa tutkimustyötä tietosuojavastaavan tarvitsemista työelämätaidoista ei ole tällä tasolla saatavissa ja siksi tutkielma täydentää niiltä osin ollutta tutkimusvajetta. Tutkielman tuloksista voi olla hyötyä organisaation johdolle, kun he ovat nimittämässä tietosuojavastaavan tehtävää uutta henkilöä. Tutkielma antaa kuntaorganisaation johdolle tukea myös roolin organisoimisessa sekä roolin vaatiman tuen laajuuden arvioinnissa.

LÄHTEET

Abdullah, H., Labuschagne, L. & Young, J. (2016). A conceptual framework for integrated information privacy protection. *International Conference on Advances in Computing and Communication Engineering (ICACCE), Durban,* 242-248. Haettu osoitteesta https://dx.doi.org/10.1109/ICACCE.2016.8073755.

Allen, J. & van der Velden, R. 2007. The flexible professional in the knowledge society: General results of the REFLEX project. Haettu osoitteesta http://digitalarchive.maastrichtuniversity.nl/fedora/get/guid:645a542e-02bd-4db6-bad4-b7eeec53a4ef/ASSET1.

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

Andreasson, A., Koivisto, J. & Ylipartanen, A. (2016). *Tietosuojakäsikirja johdolle* (3. painos). Helsinki: Tietosanoma.

Andreasson, A., Koivisto, J. & Ylipartanen, A. (2014). *Tietosuojavastaavan käsikirja 1.* Helsinki: Tietosanoma.

Andreasson, A., Koivisto, J. & Ylipartanen, A. (2014). *Tietosuojavastaavan käsikirja 2.* Helsinki: Tietosanoma.

Article 29 Working Party. (2017). WP 243 - *Guidelines on Data Protection Officers ('DPOs').*

Brezniceanu, A. (2017) Data Protection Officer – a new profession in public administration? *Revista de Stiinte Politice; Craiova, 55,* 79-88.

Dhillon, G., Oliveira, T. & Syed, R. (2018). Value-based information privacy objectives for Internet Commerce. *Computers in Human Behavior, 87*, 292-307. Haettu osoitteesta https://doi-org.ezproxy.jyu.fi/10.1016/j.chb.2018.05.043.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

Fusaro, R. (2000). Chief Privacy Officer. *Harvard Business Review, 78(6),* 20-22. Haettu osoitteesta http://search.ebscohost.com.ezproxy.jyu.fi/login.aspx?direct=true&db=bsh&AN=3720483&site=ehost-live.

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

Havelka, D., & Merhout, J. W. (2009). Toward a theory of information technology professional competence. *Journal of Computer Information Systems, 50*(2), 106-116.

Hayden, L. (2009). Designing Common Control Frameworks: A Model for Evaluating Information Technology Governance, Risk, and Compliance Control Rationalization Strategies. *Information Security Journal, 18(6),* 297-305. Haettu osoitteesta https://doi-org.ezproxy.jyu.fi/10.1080/19393550903324936.

Hirsjärvi, S. Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita* (22. painos). Helsinki: Tammi. 160-164.

Kanta-palvelut. (2019). Tietosuojakysely 2019. Haettu osoitteesta https://www.kanta.fi/documents/20143/414037/Tietosuojakysely+2019+tulokset.pdf/f433e2bd-fa8f-e244-8a22-5abc3d9a8f3d.

Karwatzki, S., Dytynko, O., Trenz, M. & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*, *34*(2), 369-400

Kesan, J., Hayes, C. & Bashir, M. (2013). Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency. *Washington and Lee Law Review, 70(1),* 341-372.

Koskinen, S., Alapuranen, L., Heino, A-M. & Lehtonen, L. (2012). *Henkilötietojen käsittely työelämässä.* Helsinki: Edita.

Kuntaliitto. (16.8.2018). Tietosuojavastaavan nimittäminen, tehtävät ja asema. Yleiskirje 06/2018. Haettu osoitteesta https://www.kuntaliitto.fi/yleiskirjeet/2018/tietosuojavastaavan-nimittaminen-tehtavat-ja-asema.

KT Kuntatyönantajat. (22.9.2020). Palkkatilastot. Haettu osoitteesta https://www.kt.fi/tilastot-ja-julkaisut/palkkatilastot.

Korpisaari, P., Pitkänen, O. & Lehtinen-Warma, E. (2018). *Uusi tietosuojalainsäädäntö*. Helsinki: Alma Talent.

Lambert, P. (2017). *The Data Protection Officer: Profession, rules and role.* New York: Auerbach Publications.

Le Deist, F. & Winterton, J. (2005). What Is Competence? *Human resource development international, 8*(1), 27-46. Haettu osoitteesta https://dx.doi.org/10.1080/1367886042000338227.

Lee, J., Bagchi-Sen, H., Rao, R. & Upadhyaya, J. (2010). Anatomy of the Information Security Workforce. *It Professional, 12(*1), 14-23. Haettu osoitteesta https://doi.org/10.1109/MITP.2010.23.

Linden, T., Khandelwal, R., Harkous, H. & Fawaz, K. (2020). The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies (1),* 47-64. Haettu osoitteesta https://doi.org/10.2478/popets-2020-0004.

Merrick, R. & Ryan, S. (2019). Data Privacy Governance in the Age of GDPR. *Risk Management, 66(*3), 38-40,42-43. Haettu osoitteesta https://search-proquest-com.ezproxy.jyu.fi/docview/2215472110?accountid=11774.

Milberg, S. J., Smith, H. J. & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science, 11(1),* 35-57. Haettu osoitteesta http://www.jstor.com/stable/2640404.

Monfared, Y. A., Benslimane, Y. & Yang, Z. (2018). Information Privacy Practices in Organizations: Activities, Knowledge and Skill Requirements for Information Technology Professionals. *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).* 1001-1005. Haettu osoitteesta https://dx.doi.org/10.1109/IEEM.2018.8607336.

Nicho, M. (2018). A process model for implementing information systems security governance. *Information and Computer Security, 26(1),* 10-38. Haettu osoitteesta https://doi-org.ezproxy.jyu.fi/10.1108/ICS-07-2016-0061.

Nykänen, S. & Tynjälä, P. 2012. Työelämätaitojen kehittämisen mallit korkeakoulutuksessa. *Aikuiskasvatus, 32(1),* 17–28. Haettu osoitteesta https://journal.fi/aikuiskasvatus/article/view/93966/52644.

Rose, A. (2013). Information Governance's Privacy and Security Component. *Journal of AHIMA, 84*(11), 54-56. Haettu osoitteesta https://search-proquest-com.ezproxy.jyu.fi/docview/1448262449?accountid=11774.

Schilpzand, P., Hekman, D. & Mitchell, T. 2015. An Inductively Generated Typology and Process Model of Workplace Courage. *Organization Science. 26 (1)* 52–77. Haettu osoitteesta http://dx.doi.org/10.1287/orsc.2014.0928.

Sitra. (28.01.2020). Ihmisistä kerätty data uppoaa monimutkaisiin verkostoihin. Haettu osoitteesta https://www.sitra.fi/artikkelit/ihmisista-keratty-data-uppoaa-monimutkaisiin-verkostoihin/.

Smith, H. J. (1993). Privacy policies and practices: inside the organizational maze. *Communications of the ACM, 36*(12), 104-122.

Smith, H. J., Milberg, S. J. & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20(2),* 167-196. Haettu osoitteesta http://www.jstor.com/stable/249477.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35(2),* 989-1015. Haettu osoitteesta https://www.jstor.org/stable/41409970.

Suomi, R., Koskinen, J., Haukola, T., Ahvenjärvi, S., Andersson, J., Hartikainen, P., Karhunen, J., Kulta, L., Niemimaa, M., Pitkänen, J., Turunen, S. & Wallgren, W. (2018). *Digiwars – Keeping the force. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 20/2018.* Haettu osoitteesta https://tietokayttoon.fi/julkaisu?pubid=25604.

Swartz, P., Da Veiga, A. & Martins, N. (2019). A conceptual privacy governance framework. *Conference on Information Communication Technology and Society (ICTAS),* Durban, South Africa 1-6. Haettu osoitteesta https://dx.doi.org/10.1109/ICTAS.2019.8703636.

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisältöanalyysi.* Helsinki: Tammi. 109-110.

Ustaran, E. Boardman, R., Filippidis, M., Hordern, V., Jackson, H., Macmillan, M., McMullan, K., Pothos, M., Room, S., Rudgard, S., Schultze-Melling, J., Seinen, W., Streeter, R., Taranto, L. & Westbrook N. (2018). *European data protection. Law and practice.* IAPP.

Lindqvist, J. (2018). Personal data protection on the internet of things. An EU perspective. (Väitöskirja, Helsingin yliopisto). Haettu osoitteesta http://hdl.handle.net/10138/263707.

Van Toorn, C., Cahalane, M., D'Ambra, J. & Cecez-Kecmanovic, D. (2019). CC's for the CIO - Core Competencies for the Chief Information Officer. *Fortieth International Conference on Information Systems, Munich.*

Voigt, P. & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR) - A practical guide*. Sveitsi: Springer International Publishing AG.

Wu, K-W., Huang, S., Yen, D. & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28(*3), 889-897. Haettu osoitteesta https://doi.org/10.1016/j.chb.2011.12.008.

Zhang, J., Yuan, W. & Qi, W. (2011). Research on security management and control system of information system in IT governance. *International Conference on Computer Science and Service System (CSSS), Nanjing,* 668-673. Haettu osoitteesta https://dx.doi.org/10.1109/CSSS.2011.5974703.

LIITE 1 HAASTATTELURUNKO

Taustakysymykset:

Kunta/kaupunki:

Nimi:

Nimike:

Organisaatiosijoitus (toiminto/ryhmä):

Koulutustausta:

Työkokemus vuosina tietosuojasta:

Mistä lähtien olet toiminut tietosuojavastaavana:

Palkkataso:

Tietosuojavastaavan nimittäminen:

1. Arvioitiinko kykyjäsi suoriutua tietosuojavastaavan tehtävistä ennen kuin sinut nimitettiin tehtävään? Miten arviointi suoritettiin?
2. Ovatko vastuut, rooli ja tehtävät määritelty riittävän selkeästi? Miten ne ovat määritetty? Ovatko ne määritetty työsopimuksessa ja/tai onko niistä olemassa muu kirjallinen päätös?
3. Millainen koulutus- ja työtausta tietosuojavastaavalla tulisi olla kuntien toimintaympäristöä ajatellen?
4. Millaiset henkilökohtaiset ominaisuudet tukevat tietosuojavastaavaa tehtävässä onnistumisessa?
5. Mitkä ovat mielestäsi keskeisiä osaamisen osa-alueita tietosuojavastaavana?
6. Koetko, että oma osaamisesi on riittävät tietosuojavastaavan tehtävässä onnistumiseen? Missä osa-alueilla koet tarvitsevasi tukea?
7. Kehittyikö palkkatasosi, kun sinut nimitettiin tietosuojavastaavan tehtävään? Vastaako palkkatasosi mielestäsi tietosuojavastaavan tehtäviä? Mikä palkkataso mielestäsi vastaisi tietosuojavastaavan tehtävää ja olisi houkutteleva?

Tietosuojavastaavan asema:

1. Onko kunnanjohto sitoutunut tietosuojan toteuttamiseen tällä hetkellä? Jos ei, niin miksi? Onko kuntasi johto ymmärtänyt oman vastuunsa tietosuojan hallinnasta?
2. Miten tietosuojavastaavan vaatimustenmukainen asema kunnassa tulisi varmistaa?
    - Riippumattomuuden osalta,
    - Pääsy tietoon ja mahdollisuus osallistua tietosuojaan liittyvien asioiden hoitoon,
    - Riittävät resurssit (aika, raha, tuki, koulutus) tehtävien hoitamiseksi,
    - Tietosuojavastaavan tavoitettavuus,

- Ettei tietosuojavastaavan tehtävistä muodostu eturistiriitoja?

3. Miten tietosuojatyön resursointi on hoidettu kunnassanne? Paljonko sinulla on aikaa käytettävissä tietosuojatyön hoitamiseksi? Ovatko resurssit riittävät? Miten resursointia tulisi parantaa? Arvioidaanko resurssien riittävyyttä säännöllisesti? Miten arviointi suoritetaan?
4. Millä keinoin huolehdit jatkuvasta koulutuksesta tai osaamisen kasvattamisesta?
5. Onko tietosuojavastaavan asema määritelty mielestäsi riittävän selkeästi tietosuoja-asetuksessa? Onko se riittävän kattava kuntakontekstissa? Onko asetuksessa sellaisia puutteita tai ristiriitoja, jotka asettavat haasteita tai esteitä kuntien tietosuojavastaavan asemalle tai tehtävien hoitamiselle?
6. Asettavatko ulkopuoliset vaatimukset kuten muu lainsäädäntö haasteita tietosuojavastaavan asemalle tai tehtävien hoitamiselle?
7. Asettaako kunnan toimintaympäristö, johtamisjärjestelmä tai sidosryhmiltä tulevat vaatimukset haasteita tai esteitä tietosuojan toteutumiselle?

Tietosuojavastaavan tehtävät:

1. Mikä on työnkuvasi tietosuojavastaavana kunnassa? Minkälaisia tehtäviä hoidat säännöllisesti tietosuojavastaavana? Miten paljon työajastasi kuluu näihin tehtäviin?
2. Onko sinulla sellaisia tehtäviä, mitä kunnan tietosuojavastaavana joudut tekemään, jotka eivät välttämättä kuuluisi tietosuojavastaavan toimenkuvaan? Onko joitain tehtäviä, mihin tietosuojavastaavana et osallistu, vaikka ehkä kuuluisi?
3. Mitkä tietosuojavastaavan tehtävät erityisesti motivoivat sinua? Mitkä tehtävät taas eivät?
4. Ovatko käytössäsi olevat työmenetelmät, prosessit ja ohjelmistot tai muut työkalut sellaisia, joilla tietosuojatyö voidaan tehdä tehokkaasti? Mitä kehitettävää niissä mahdollisesti on?
5. Raportoitko tietosuojavastaavana säännöllisesti kunnanjohdolle tietosuojasta? Onko tietosuojan hallinnalle mittareita? Millaisia mittareiden mielestäsi tulisi olla?
6. Arvioidaanko kuntasi tietosuojan tasoa jotenkin? Miten kuntasi tietosuojan tasoa mitataan?