LAB University of Applied Sciences

Tietosuojan johtaminen

Organisaation johdon rooli tietosuojan toteuttamisessa

LAB-ammattikorkeakoulu
Tradenomi (YAMK), Uudistava johtaminen
Ulla Riva

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Riva, Ulla	Opinnäytetyö, YAMK	2021
	Sivumäärä	
	81 + 6	

Työn nimi

Tietosuojan johtaminen

Organisaation johdon rooli tietosuojan toteuttamisessa

Tutkinto

Tradenomi (YAMK)

Toimeksiantajan nimi, titteli ja organisaatio

Sanna Koskimies, hallinto- ja kehittämispäällikkö, Kotkan kaupunki

Tiivistelmä

Tutkimuksen tavoitteena oli selvittää organisaation johdon roolia tietosuojan toteuttamisessa. Tutkimus toteutettiin laadullisena tutkimuksena käyttäen osallistuvaa havainnointia ja työpajatyöskentelyä sekä teoriaohjaavaa aineistoanalyysiä. Tutkimuksessa organisaatiolle luotiin Valtiovarainministeriön (2016) antamaan tietosuojan kokonaisuudistusta koskevaan raporttiin perustuva tietosuojasuunnitelman malli. Tietosuojasuunnitelman mallia täydennettiin johtamisen teoriakirjallisuuden sekä suunnitelman osa-alueiden sisältöä koskevan lainsäädännön vaatimusten sekä kansallisen ohjeistuksen avulla konkretisoiden johdon vastuita ja tarvittavia toimenpiteitä. Tietosuojasuunnitelmaa testattiin organisaation tietosuojaryhmän valitseman osa-alueen osalta linjaorganisaatiossa johdosta henkilöstöön.

Aineistoanalyysi toteutettiin teoriaohjaavasti tutkien organisaation johtamisjärjestelmän määrittelevistä dokumenteista, sekä tietoturva- ja tietosuojapolitiikoista kuinka tietoturvan ja tietosuojan johtamisen vastuut on kuvattu.

Tutkimuksessa havaittiin, että julkisen hallinnon johtamisjärjestelmä koostuu useista säännöistä ja määrittelyistä, joiden lisäksi tietosuojan johtamista kuvataan politiikoissa ja toimintaohjeissa. Yhden dokumentin vastuu määrittelyn muuttuessa kokonaisvastuun ylläpitäminen on haasteellista ja edellyttää useiden dokumenttien päivitystä, jolloin riski kokonaisuuden rikkoutumiseen kasvaa.

Asiasanat

johtaminen, muutosjohtaminen, osallistaminen, tietosuoja, tietosuojasuunnitelma, tietosuojan kehittäminen

Abstract

Author(s)	Type of Publication	Published
Riva, Ulla	Master's thesis	2021
	Number of Pages	
	81 + 6	

Title of Publication

Data protection management

The role of organizational management in implementing data protection

Name of Degree

Master on Business Administration

Name, title and organization of the client

Sanna Koskimies, Administrative manager, City of Kotka

Abstract

The objective of the study was to find out the role of the organization's management in implementing data protection. The research was conducted as a qualitative study using participatory observation and workshops as well as theory-guided material analysis. The study created a model for a privacy program for the organization. The model was based on a report by the Ministry of Finance concerning national data protection reform. In the study, the model was supplemented with literature about management theory as well as legislation and national guidelines.The privacy program was tested in a hiearchical organization based on the selection.of the organization's privacy team.

The material describing the organization's management system, information security and data protection was analyzed by a theory-guided method.

The study showed that the governance system of public administration consists of a number of rules and definitions, in addition to which data protection management is described in policies and guidelines. As the definition of responsibility in a single docu-ment changes, maintaining overall responsibility becomes challenging and requires updating multiple documents, increasing the risk of failure of the entire system.

Keywords

leadership, management, change management, participatory leadership, information security, data protection, privacy program, data protection development

Sisällys

1 Johdanto

1.1 Kehittämishankkeen tausta

Johto on keskiössä tietosuojatyön onnistumisessa (Andreasson ym. 2019,87).

Organisaatioiden toiminnan ja henkilötietojen käsittelyn haavoittuvuus konkretisoitui organisaatioille ja yksityishenkilöille viimeistään 2020 syksyllä Vastaamon tietovuodon tultua julkisuuteen. Tietovuodon käsittely niin rekisteröityjen oikeuksien, ongelmien korjaamisen ja niistä vastuussa olevien määrittelyn kuin tietomurron tekijän kiinni saamisen osalta on kestänyt pitkään. Nähtäväksi jää millaista vahinkoa tietonsa menettäneille koituu tulevaisuudessa. (Rikosuhripäivystys 2021.)

Datasta on tullut organisaatioille uusi öljy, ja samalla kaiken muodostuvan datan johtamisesta on tullut entistä monimutkaisempaa. Liikenne ja viestintäministeriö on vuonna 2014 julkaistussa yritysjohtajien haastatteluihin perustuvassa raportissaan kuvannut digitaalista murrosta, jopa vallankumousta, joka syntyy big datan, pilvipalveluiden, sosiaalisen median ja muiden langattoman tekniikan käytön mahdollistavien innovaatioiden ja uusien liiketoimintamahdollisuuksien myötä. (Lautjärvi 2018, 19–20.) Tiedon ja laitteiden siirtyessä verkkoon tietosuoja ja tietoturvariskit koskettavat kaikkia toimialoja, myös niitä, joilla tietosuoja ja tietoturva osaaminen ei ole toiminnan ytimessä. Tietosuojaan ja tietoturvaan kohdistuvat epäonnistumiset voivat johtaa korvauksien maksamiseen ja muihin taloudellisiin seurauksiin, jopa vaikuttaa yrityksen osakekurssiin.

Vastaamon lisäksi Facebookin ja Cambridge Analytican tietosuojaskandaali aiheutti yhtiöille mainehaitan lisäksi myös huomattavia taloudellisia seurauksia. Jatkossa sijoittajat saattava tarkastella yhtiöitä myös tietosuojan ja tietoturvan toimintamallien näkökulmasta. EU:n yleinen tietosuoja-asetus on saanut vastuulliset organisaatiot niin julkishallinnossa kuin liikemaailmassa kehittämään käytäntöjään. (Silvola & Landau 2019, 274–275.)

Organisaation johdon ja henkilöstön tietosuojaosaamisesta voi tulla tuotanto- ja palveluprosessien sujuvuuden takaava menestystekijä, joka antaa suomalaisille organisaatioille entistä paremmat toimintaedellytykset globaaleilla markkinoilla. Tietosuojaa voidaan pitää yhtenä kansallisen tuottavuusloikan keskeisenä tekijänä, kun sen avulla lisätään tietoturvallista digitalisaatiota, kehitetään tietojärjestelmiä ja niihin kiinteästi kuuluvan työn tekemisen ohjausta, sekä lisätään organisaation koko henkilökunnan tietosuojaosaamista, jolla lopetetaan aikaa vievä sähläys asiakastietojen käsittelyssä. Näiden velvoitteiden toteuttaminen on osa organisaation toiminnan johtamista. (Andreasson ym. 2019, 48.)

Aiempi tutkimus

Tietosuojavastaavan tehtävästä ja roolista organisaatiossa on kirjoitettu useita oppaita mm. Tietosuojavastaavan käsikirjat 1 ja 2 (Andreasson ym. 2014 a; 2014b) Osaava tietosuojavastaava sekä Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (Andreasson ym. 2019). Johdon roolia on tutkittu tietosuojavastaavalle annettavan tuen näkökulmasta Jaana Riikosen Pro Gradu tutkielmassa Johdon tuki tietosuojavastaavalle terveydenhuollon organisaatiossa (2013). Andreasson ym. (2015) ovat kirjoittaneet Johdon tietosuojaoppaan, joka keskittyy riskienhallintaan, tietosuoja- ja tietoturvatyön organisointiin sekä operatiivisen toiminnan tuottavuuteen, tehokkuuteen ja kustannussäästöihin. Muu tietosuojaan liittyvä opinnäytetyötutkimus näyttää keskittyneen muun muassa tietosuojavastaavan tehtävään sekä tietosuoja - asetuksen tuomiin muutoksiin organisaatioiden toiminnassa (Theseus 2021).

Olen toiminut hallinnollisen tietoturvan sekä tietosuojan ammattilaisena useita vuosia ja saanut kokemusta niin julkisen hallinnon kuin ICT- yrityksen tietoturvan ja tietosuojan kehittämisestä ja havainnut, että useilla organisaatioilla on haasteita vastata tietosuojalainsäädännön vaatimuksiin. Olen kirjoittanut johdon tietosuojaoppaaseen (Andreasson ym. 2015) johdon muistilistan, jossa luetellaan tietosuojaan liittyvät vastuut ja toimenpiteet, joiden toteutuminen johdon tulee varmistaa oman organisaationsa toimialan erityisvaatimusten mukaisesti.

1.2 Tutkimusongelma, tutkimuskysymys ja työn tavoitteet

Tutkimuksen tavoitteena on kuvata julkisen organisaation johdon rooli ja vastuu organisaation tietosuojan johtamisessa lainsäädännön, kansallisen tietosuojaviranomaisen ja valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) ohjeiden sekä tietosuojakirjallisuuden avulla sekä tuottaa toimeksiantajalle tietosuojan kehittämistä varten tietosuojasuunnitelman malli. Tutkimuksen lopputulos hyödyttää julkisen hallinnon organisaatioiden johdon lisäksi muiden organisaatioiden johtoa, sekä tietosuojavastaavia, jotka tarvitsevat organisaationsa johdon päätöksentekoa, toimenpiteitä ja tukea menestyäkseen tehtävässään.

Tutkimuskysymyksiä on kaksi: 1. Mitä tietosuojan johtaminen tarkoittaa käytännössä? 2. Mikä on organisaation johdon vastuu tietosuojan toteutumisessa?

Kehittämissuunnitelma muodostetaan johtamisen teoreettisen viitekehyksen, tietosuojaa koskevaa lainsäädännön, EU:n tietosuojaneuvoston (European Data Protection Board, EDPB) ja kansallisen tietosuojaviranomaisen ohjeistusten, muiden kansallisten ohjeiden ja raporttien sekä tietosuojaa koskevaa kirjallisuuden avulla.

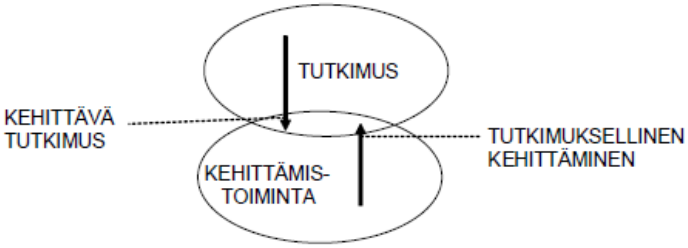
Luvussa 5. käsitellään kehittämissuunnitelmaa, joka pitää sisällään tilaajaorganisaatiolle toteutettavan tietosuojasuunnitelman mallin. Malli pohjautuu Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) asettama työryhmän raporttiin EU – tietosuojan kokonaisuudistus, tietosuojalainsäädäntöön sekä tietosuojaa koskevaan kirjallisuuteen. Tietosuojasuunnitelman mallin tarkoituksena on konkretisoida laajan tietosuojakokonaisuuden sisältöä organisaation jatkuvan tietosuojatyön tueksi. (Valtiovarainministeriö 2016, 31.)

Tietosuojan kokonaisuudistusta koskevan VAHTI – raportin tietosuojasuunnitelma on laaja useita osa-alueita ja niihin sisältyvistä tehtävistä muodostuva kokonaisuus, jota ei voida toteuttaa tutkimuksen puitteissa kokonaisuudessaan, joten tilaajaorganisaation tietosuojaryhmä valitsee suunnitelmasta yhden osa-alueen, josta valitaan tutkimukselle rajattu kohde. Valittavan kohteen tai toimenpiteen tulee olla sellainen, jolla parhaiten mallinnetaan organisaation tietosuojan jatkokehittämistä ja edesautetaan tietosuojan johtamismallin kehittämistä. Luvussa 6. kuvataan dokumentaation ja työpajojen havainnoinnin tuloksia tietosuojan johtamisen näkökulmasta.

1.3 Tutkimusmenetelmä ja rajaukset

Tässä tutkimuksellisessa kehittämissuunnitelmassa käytetään tutkimusmetodina laadullista kehittämistutkimusta, jossa syntyy organisaation johdolle johtamisen teorian ja tietosuojan johtamisen yhdistävä malli. Laadullisen tutkimuksen tavoitteena on tutkittavan ilmiön kuvaaminen, ymmärtäminen ja tulkitseminen, sen avulla pyritään syvälliseen ymmärtämiseen. Laadullisessa tutkimuksessa kerättävän aineiston määrää ei voida määritellä ennakkoon, vaan aineistoa kerätään, kunnes tutkimusongelma ratkeaa ja tutkija ymmärtää tutkimansa ilmiön. (Kananen 2017, 35.)

Kehittämistoimintaa voidaan toteuttaa tutkimuksen näkökulmasta toimintatutkimuksen eli tutkimuksellisen kehittämistoiminnan keinoilla. Tutkimuksellinen kehittämistoiminta kohdentuu tutkimuksen ja kehittämistoiminnan risteyspaikkaan (kuvio 1), jota voidaan lähestyä sekä kehittämistoiminnan että tutkimuksen suunnasta. (Toikko & Rantanen 2009, 21.)



Kuvio 1. Tutkimuksen ja kehittämistoiminnan risteyspaikka (Toikko & Rantanen 2009)

Kehittävässä tutkimuksessa konkreettista kehittämistoimintaa lähestytään tutkimuksellisen kysymyksenasettelun ja metodologisen tarkastelun kautta. Tutkimuksellisessa kehittämisessä käytännön ongelmat ja kysymykset ohjaavat tiedon tuottamista aidoissa toimintaympäristöissä. Tutkimuksellinen kehittämistoiminta on uuden tiedon tuottamista käytännön toimintaan ja rakenteisiin liittyvien kysymysten pohjalta. Tällöin kyseessä on uusi tiedon muodostamisen tapa, jossa tutkimus on avustavassa roolissa. Tutkimuksellisessa kehittämistoiminnassa tavoitellaan konkreettista muutosta, pyrkien samalla perusteltuun tiedon tuottamiseen. (Toikko & Rantanen 2009, 21 – 24.)

Laadullisessa tutkimuksessa pyritään ymmärtämään tarkasteltavaa ilmiötä tutkimuksen kohteena olevien näkökulmasta, tutkimuksessa ollaan kiinnostuneita henkilöiden kokemuksesta, ajatuksista, tunteista sekä tutkimuksen kohteena olevalle asialle annettavista merkityksistä. (Puusa & Juuti 2020, 9.) Tutkimuksessa hyödynnetään johtamisen teoriaa koskevaa kirjallisuutta, jota käsitellään luvussa 2. Teoria osassa perehdytään muun muassa organisaation johdon vastuuseen, muutoksen johtamiseen sekä osallistamiseen johtamisen välineenä.

Laadullisessa tutkimuksessa käytetään tutkimusmenetelmänä havainnointia tilanteissa, joissa ilmiöstä on vähän tietoa ja ilmiötä ei tunneta, jolloin ei voida rajata keskusteltavia teemoja. Suorassa havainnoinnissa tutkittavaan yhteisöön kuuluvat tiedostavat havainnoijan olemassaolon eikä havainnoija toimi osana yhteisöä. Tämä voi vaikuttaa yhteisön jäsenten käyttäytymiseen ja sitä kautta tutkimustulokseen. Osallistuvassa havainnoinnissa tutkija osallistuu yhteisön toimintaan, jolloin hän pääsee syvälle kiinni tutkittavaan ilmiöön, mutta voi myös vaikuttaa tutkimuksen tulokseen. (Kananen 2017, 83–84.)

Havainnointi toteutetaan tutustumalla organisaation johtamisjärjestelmään, tietosuojaa koskeviin sääntöihin, politiikkoihin ja ohjeisiin havainnoiden, kuinka johdon ja päätöksenteon vastuita on niissä kuvattu. Havainnointia tehdään myös tietosuojasuunnitelman käytännön toteutukseen liittyvissä työpajoissa. Ensimmäisessä työpajassa organisaation tietosuojaryhmä valitsee tietosuojasuunnitelman mallista osan, jota käsitellään tarkemmin kahdessa työpajassa, johdon ja esihenkilöiden työpajassa sekä henkilöstön työpajassa. Johdon ja esihenkilöiden työpajassa määritellään tietosuojasuunnitelmasta valitun osa-alueen toteutuksen edellyttämät päätökset ja toimenpiteet huomioiden organisaation johtamisjärjestelmän ja tietosuojavastaavan roolin. Kolmannessa työpajassa johdon päätökset jalkautetaan johdon ja esihenkilöiden toimesta henkilöstötasolle. Edustajat valitaan siten, että johto tai johtaja, sekä esihenkilöt / esihenkilö ja henkilöstö ovat samasta linjaorganisaatiosta. Organisaation tietosuojavastaava osallistuu kaikkiin työpajoihin. Työpajoissa käytetään osallistavia menetelmiä sekä suoraa ja osallistuvaa havainnointia ilmiöön liittyvien tapahtumien

seurantaan. Tietosuojaryhmän sekä johdon ja esihenkilöiden työpajassa käytetään välineenä Orchidea Workshop – sovellusta, joka mahdollistaa useiden erityyppisten digitaalisten aivoriihityöpajojen toteuttamisen Teams – kokouksen yhteydessä. Työtavaksi on valittu Innotiimi-ICG:n BrainGrouping menetelmästä kehittämä ARM - työmalli, joka sopii muun muassa strategian jalkautukseen. (Halme 2018.) Henkilöstön työpajassa havainnoidaan keskustelun avulla tietosuojasuunnitelman osa-alueesta toisessa työpajassa valitun käytännön toimenpiteen toteutuminen, eli johdon päätöksen jalkautuminen henkilöstölle.

Tutkimuksessa ei arvioida toimeksiantajaorganisaation tietosuojan tai sen johtamisen nykytilaa. Luvussa 3. käsitellään digitaalista turvallisuutta ja tietoturvaa koska ne ovat osa tietosuojan toteutumisen edellytyksiä, mutta tutkimuksessa ei arvioida niiden nykytilaa. Tietosuojaan liittyvä niin sanottu ePrivacy, eli sähköisen viestinnän - sääntely rajataan tutkimuksen ulkopuolelle, koska sääntelyn kansallinen ohjaus suhteessa EU:n tietosuojaviranomaisen linjauksiin on vielä vakiintumatonta.

2 Johtaminen

Luukan (2019, 304–307) mukaan ihmisryhmät kaipaavat johtajuutta ja johtajaa, selkeää organisatorista rakennetta sekä esihenkilöä. On organisaatioita, muun muassa Google, jotka ovat kokeilleet mahdollisimman matalaa ja itseohjautuvaa organisaatiota vain havaitakseen, että johtamista ja organisoitumista tarvitaan ja halutaan myös henkilöstön taholta.

Johtamisen sisältö on hyvin laaja ja vaikeasti määriteltävä. Virtanen & Stenvall (2019, 99–102) jakavat julkisen johtamisen kahteentoista johtamisen osaamisen sisältöalueeseen, jotka johtajien on hallittava riippumatta johtajan tai esimiehen organisatorisesta asemasta. Johtamisen sisältöalueita ovat: strateginen ja resurssien johtaminen, innovaatioiden tai innovatiivisuuden johtaminen, prosessien, laadun, osaamisen, työyhteisöjen, verkostojen, muutoksen, viestinnän, suorituksen, sekä älykkään organisaation johtaminen. Minzbergin (1973) mukaan johtamistyöhön kuuluvat päätöksentekijän, tiedottajan ja vuorovaikutteisen toimijan roolit, joissa päätöksen tekeminen tarkoittaa neuvottelemista, epävakauden torjumista ja resurssien varaamista, tiedottaminen tarkoittaa tiedon levittämistä ja organisaation edustamista viestinnässä ja vuorovaikuttaminen tarkoittaa henkilöstön johtamista, yhteistoiminnasta huolehtimista sekä organisaation edustamista (Virtanen & Stenvall 2019, 54).

Suomen kielessä johtamiselle on vain yksi sana: johtaminen kun esimerkiksi englannin kielessä johtamista kuvataan käsitteillä management ja leadership. Luukka (2019, 304) kääntäisi managementin asioiden johtamiseksi ja leadershipin ihmisten johtamiseksi.

Jokaisessa organisaatiossa perimmäinen vastuu organisaation strategian ja siitä johdettujen tavoitteiden määrittelemisestä ja saavuttamisesta kuuluu ylimmälle johdolle. Julkisen hallinnon organisaatioissa ylintä päätösvaltaa käyttää kuntalain (410/2015) 14 pykälän mukaan poliittinen johto, eli valtuusto, joka päättää muun muassa kuntastrategiasta, hallintosäännöstä, omistaja- ja konserniohjauksesta, sisäisestä valvonnasta ja riskienhallinnasta sekä toimivallan siirtämisestä toimielimille ja viranhaltijoille. Yrityksissä ylintä päätösvaltaa käyttää osakeyhtiölain (624/2006) 1 ja 2 pykälien mukaan osakkeenomistajista koostuva yhtiökokous, joka päättää muun muassa yhtiöjärjestyksestä, sekä hallituksen ja toimitusjohtajan tehtävistä ja toimivallasta.

Strategiassa kuvataan mihin organisaatio pyrkii, miksi ja millä keinoilla. Perinteisesti strategian laatii organisaation johto, mutta yhä useammin myös henkilöstö osallistuu strategiatyöhön, koska toteuttamiseen tarvitaan jokaisen panosta ja strategian tulee olla olennainen osa jokaisen organisaatioon kuuluvan arkea. Strategian jalkautus, eli asetettujen tavoitteiden tiedottaminen, on yleensä esihenkilöiden vastuulla. Esihenkilöiden tulisikin kyetä omak-

sumaan uudet tavoitteet ja tunnistaa toimintatapojen muutostarpeet, muuten toiminnan todellinen muuttuminen jää saavuttamatta. Esihenkilöiden tehtäväksi jää pilkkoa strategian kokonaistavoitteet osatavoitteiksi ja keskustelun avulla saada henkilöstö ymmärtämään nämä molemmat, sekä toimintatavat ja erityisesti niiden muutokset. Uutta toimintatapaa tulee vahvistaa päivittäisessä toiminnassa. (Kupias 2013.)

Ylin johto on viime kädessä vastuussa siitä, että organisaatiolle asetettuihin tavoitteisiin päästään lakeja, toimintaohjeita ja eettisiä standardeja noudattaen. Johdon velvollisuutena on varmistaa, että organisaatiossa on selkeästi määritellyt roolit, vastuut ja tilivelvollisuudet. Lisäksi johdon vastuulla on huolehtia, että organisaatiossa on riittävät resurssit, prosessit ja rakenteet toimintaohjeiden ja politiikkojen noudattamiseen, tarkoitustenmukaisten kontrollien ja toimenpiteiden käyttöönottamiseen sekä kontrollien toimivuuden varmistamiseen. (Ratsula 2016, 163.)

Johto vastaa strategian ja tavoitteiden lisäksi organisaatiokulttuurista sekä siitä, että organisaatio pystyy hyödyntämään ympäristön sille suomat mahdollisuudet toiminnaksi, rakentamaan omistajuutta, vastuuta ja kyvykkyyksiä osallistamalla ja toimimalla johdonmukaisesti osoittaen millaisille arvoille sen kulttuuri rakentuu. Johdon tulee luoda organisaatiolle visio, joka kuvaa henkilöstölle jokapäiväisen toiminnan tavoitteet, sekä missio, joka toimii eettisenä ohjenuorana. (Jabe 2017, 272.) Sydänmaanlakan (2015) mukaan organisaation johdon vastuulle kuuluu myös laatuajattelun kokonaisvaltainen hallitseminen ja sen johtaminen siten, että laatu on jokaisen henkilöstöön kuuluvan vastuulla organisaation tavoitteiden toteuttamisessa.

Virtanen & Stenvall (2019, 209) kuvaavat johtamisen olevan ennen kaikkea yhdessä tekemistä, jossa tulee kuitenkin olla nimetty yksi henkilö, jonka tehtävä on varmistaa johtamisen toimivuus ja määritellä selkeät vastuusuhteet. Lainsäädäntö määrittelee tietosuojaa koskevan vastuun rekisterinpitäjälle ja henkilötietietojen käsittelijälle, mutta organisaation ylimmällä ja keskijohdolla sekä esimiehillä on lisäksi merkittävä rooli tietosuojan sekä siihen liittyvän digitaalisen turvallisuuden kokonaisuuden toteuttamisessa.

Toimialajohtaminen ja esimiestyö

Organisaatiosta riippumatta lainsäädäntö määrittelee organisaation hallituksen ja ylimmän johdon tehtäviä muun muassa nimenkirjoitusoikeuteen, päätöksentekoon, toimivaltaan, valvontaan, sekä hyvän hallintotavan käytänteisiin liittyen. Organisaation operatiivisen ja päivittäisen toiminnan vastuu on johdolla, joka raportoi säännöllisesti ylemmille päätöksentekoelimille, kuten esimerkiksi hallitukselle. (Lautjärvi 2018, 70–72.)

Organisaation hallituksella ja johdolla on vastuu toiminnan tavoitteiden asetannasta, strategiasta, johtamis- ja hallintojärjestelmien luomisesta, tavoitteiden saavuttamisesta, riskien hallinnasta, toiminnan valvonnan järjestämisestä sekä tavoitteisiin ja valvontaan liittyvästä raportoinnista. Organisaation keskijohdolla tulee olla edellytykset ylimmän johdon asettamien tavoitteiden johtamiseen jokaisella organisaation osa-alueella sekä kiinnostusta siihen mitä organisaatiossa tapahtuu. Keski- ja operatiivisen johdon on toteutettava päivittäin erilaisia vaikeitakin toimintaan liittyviä päätöksiä. Esihenkilöt ovat keskeinen linkki johdon ja henkilöstön välillä. Heidän tehtävänsä on välittää johdon asettavat tavoitteet, periaatteet ja toimintatavat sekä toimintakulttuuri henkilöstölle, tuntea jokaisen henkilöstöön kuuluvan tehtäväkuva ja valvoa sääntöjen noudattamista. Esihenkilö on merkittävä linkki henkilöstön ja johdon välillä tiedottamaan ja toimeenpanemaan uusia toimintatapoja sekä raportoimaan havaituista epäkohdista ja organisaation toimintaperiaatteiden vastaisesta toiminnasta. Sekä johto, että esihenkilöt ovat omalla toiminnallaan esimerkkejä henkilöstölle. (Ratsula & Ratsula 2021, 63–72.) Johtamisen osaamisen sisältöalueista toimialajohtamiseen ja esimiestyöhön kuuluvat erityisesti strateginen johtaminen, resurssien johtaminen, prosessien johtaminen, työyhteisön johtaminen sekä suorituksen johtaminen.

Laadun ja tiedon johtaminen

Tiedon johtaminen liittyy julkisen johtamisen sisältöalueista laadun johtamiseen. Laadun johtaminen ja laadunhallinta ovat Leclin & Laine (2009, 32, 34) mukaan osa organisaation johtamisjärjestelmää, johon liittyy organisaation kyky tuottaa laadukasta toimintaa. Organisaation tuottamien tuotteiden ja palveluiden laadun lisäksi tulee johtaa koko toimintaprosessin laatua, joka pitää sisällään myös organisaation sidosryhmät, esimerkiksi omistajat, rahoittajat, yhteistyökumppanit ja toimittajat. Kokonaisvaltaisessa laadunhallinnassa laatu sisältyy organisaation johtamiseen, strategiseen suunnitteluun ja toiminnan kehittämiseen. (Leclin 2006, 17.) Laadun johtaminen on osa organisaation johtamista ja johtamisjärjestelmää lähtien organisaation perusarvoista ja maailmankatsomuksesta, visiosta, missiosta aina strategiaan ja sen avulla asetettuihin tavoitteisiin saakka. (Leclin 2006, 37-38.)

Jalonen (2015) kuvaa tiedolla johtamista johdon päätöksenteon apukeinoksi, jossa toiminnassa syntyvä ja toimintaan vaikuttava olennainen tieto yhdistetään tai siitä erotetaan epäolennainen tieto (Virtanen ym. 2015, 40). Ennen tiedolla johtamista on johdettava tiedon muodostustumista sisällöltään laadukkaaksi sekä sen luottamuksellisuutta ja eheyttä. Sydänmaanlakka (2015) kuvaa tiedon johtamista prosessiksi, joka pitää sisällään tiedon luomisen, hankkimisen, varastointiin, jakamiseen ja soveltamiseen liittyvät alaprosessit, joissa yksilön hallussa oleva tieto muuttuu organisaation tiedoksi ja piilossa oleva tieto havaitta-

vaksi. Tiedolla johtaminen kuuluu julkisen hallinnon johtamisen älykkään organisaation johtamisen osa-alueeseen ja on yksi sen kulmakivistä. Virtanen & Stenvall (2019, 195) mukaan älykkäästi johdetun organisaation johdolla on kyky ennakoida tulevaisuuden muutoksia ja seurata heikkoja signaaleja, jotka ennakoivat muutosta, jolloin tulevaisuus ei ole yllätyksellinen vaan siihen on voitu varautua.

Tiedon muodostumiseen ja tiedolla johtamiseen liittyy myös informaation välttäminen, joka Jalosen (2015) mukaan liittyy tietoiseen tietämättömyyteen, jolloin johto vetoaa tietämättömyyteen tilanteissa, joissa päätöksen tekeminen tai kannan ottaminen voi johtaa konfliktiin tai muulla tavoin vaikeaan tilanteeseen. Tieto itsessään voi olla laadultaan heikkoa, virheellistä, puutteellista tai sellaisessa muodossa, että sitä ei voida hyödyntää. Lisäksi tietoa syntyy useista eri lähteistä niin paljon, että kaiken tiedon laatua ei voida varmistaa tai ylläpitää riittävällä tasolla, joten johdon on valittava toiminnan kannalta keskeinen ydintieto (master data) ja huolehdittava sen laadusta luomalla käytänteitä, malleja ja ohjeita laadun varmistamiseksi. (Virtanen ym. 2015, 53.)

Organisaation hallussa ja käytössä olevaa tietoa tulee myös turvata ja siihen liittyy keskeisenä osana tietoturvan johtaminen. Tietoturvaprosessin avulla pyritään tunnistamaan organisaation toiminnan kannalta arvokas tieto, arvioimaan siihen liittyvät riskit sekä kehittämään tarvittavat suojakeinot. Prosessia ohjataan johdon määrittelemällä tietoturvapolitiikalla. (Laihonen ym. 2013, 21.) Tavallisimpia organisaation tietoon ja sen johtamiseen liittyviä riskejä ovat muun muassa, että organisaatiossa ei tunnisteta vastuuta tietojen valvonnasta eikä siksi määritellä kenelle valvonta kuuluu, tietoriskejä ei hallinnoida, jolloin niiden nykytilasta ei ole riittävää käsitystä, tiedonhallintaan liittyviä vaarallisia työyhdistelmiä ei ole tunnistettu tai niiden muodostumista ei ole estetty, kriittistä tietoa ei ole dokumentoitu minkä vuoksi muodostuu henkilöriski jos osaaja lähtee, henkilöstön lähtö ei ole hallittu prosessi, jolloin voi jäädä pääsy järjestelmiin ja tiloihin, sekä sopimuskumppaneihin luotetaan sokeasti eikä heidän taustojaan selvitetä. (Viitala 2005, 212.) Tiedon varastointiin käytetään erilaisia tietojärjestelmiä, -kantoja, ohjelmistoja ja sovelluksia, joiden osalta henkilötiedoksi luokitellun tiedon käsittelyssä tulee huomioida EU:n yleisen tietosuoja-asetuksen (EU 679/2016) 25 artiklassa säädetty sisäänrakennetun ja oletusarvoisen tietosuojan (privacy by design, privacy by default) vaatimus.

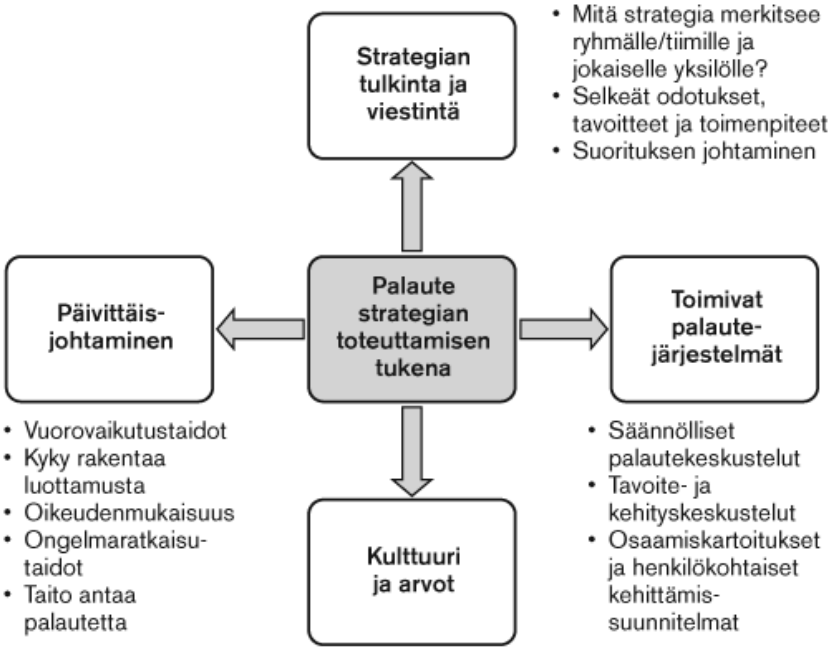
Muutosjohtaminen

Organisaatiot joutuvat kehittämään ja muuttamaan toimintaansa jatkuvasti, joko jatkuvana kehittämisenä aikaa seuraten tai suurempana muutosprojektina sisäisen tai ulkoisen pakon sanelemana. Molemmat edellyttävät organisaation johdolta päätöksiä ja linjauksia organisaation pitkän tähtäimen suunnasta ja visiosta muutoksen toimenpiteiden ja päämäärän

määrittelemiseksi. Lisäksi johdon tulisi kehittää organisaation suhtautumista ja reagointikykyä muutoksiin, tätä kutsutaan resilienssiksi, eli selviytymis- ja muutoskyvyksi ennakoimattomissa ja yllättävissä muutostilanteissa. (Kuitunen & Sutinen 2018, 165.)

Muutoksen toteuttamiseen on erilaisia teoreettisia malleja, joista johdon tulee valita organisaatiolleen parhaiten sopiva. Johdon tulee jäsennellä ja priorisoida muutoksessa tarvittavat toimenpiteet ja mitoittaa ne realistisesti, sekä kartoittaa muutokseen tarvittavat resurssit ja osaaminen. Muutoksen jälkeinen aika voi vaatia osaamisen päivittämistä läpi organisaation. (Pirinen 2015.) Muutoksen suunnitteluvaiheessa johdon tulee määritellä millä tavoin muutoksen onnistumista arvioidaan tai mitataan. Arviointimenetelmiä on erilaisia, esimerkiksi organisaation tilanteen alku- ja loppuanalyysi, itsearviointi, ulkoinen arviointi tai sidosryhmien haastattelu. Arvioinnin suorittamisesta saadaan hyötyjä myös seuraavien muutosten suunnitteluun. (Kauhanen 2018, 58.)

Strategisen tason muutoksissa tarvitaan jatkuvaa palautetta suorituksen ohjaamiseen ja organisaation tulevan menestyksen varmistamiseen. Kuvio 2 kuvaa niitä osa-alueita ja toimintoja, jotka ovat edellytyksenä strategian toteuttamisen tueksi käytettävän palautteen toteutumiselle. Palautteen tehtävänä on ohjata strategian toteutumista, motivoida ja edistää uuden toimintatavan oppimista. (Kupias 2013.)



Kuvio 2. Edellytykset palautteen toimimiselle strategian toteuttamisen tukena (Kupias 2013).

Pihan ja Sutisen (2020, 149) mukaan strategian ja vision johtamisen lisäksi johdon tulee keskittyä myös käytöksen, ajattelutavan ja tunteiden muuttamiseen, nämä ovat avaimia onnistuneeseen muutokseen. Lisäksi muutoksen onnistumiseen vaikuttaa onnistunut muutosviestintä. Kauhasen (2018, 54) mukaan henkilöstö motivoituu ja pystyy parempiin suorituksiin, kun sillä on riittävästi informaatiota johdon tahtotilasta. Tämän päivän johtamismallissa pelkät käskyt ja määräykset eivät toimi vaan tarvitaan keskustelua ja päätösten perustelua. Sisäisen viestinnän tulee olla avointa ja monikanavaista kaikkia nykyaikaisia viestintämenetelmiä ja välineitä hyödyntävää. Muutoksen suunnittelussa tuleekin siksi huomioida myös muutosviestintäsuunnitelma. Tietoyhteiskunnassa tiedolla on suuri merkitys, eikä viestintä ole enää pelkästään organisaation ylimmän johdon tai viestintäyksikön tehtävä, vaan viestinnän osaamisen vaatimukset koskevat koko henkilöstöä. Jokainen henkilöstöön kuuluva osallistuu organisaation sisäisen viestinnän toteuttamiseen. (Virtanen & Stenvall 2019, 177.)

Muutokseen liittyy myös sen vastustaminen, muutosvastarinta, joka on henkilön tai organisaation luonnollinen reaktio muutokseen tai sen suunnitteluun. Muutosvastarinnan taustalla on ihmisen luontainen itsesuojeluvaisto, jolla pyritään tasapainoon ja hallinnan tunteeseen. Johdon tulee kohdata muutosvastarinta eikä jättää sitä käsittelemättä. Aikaisemmissa muutoksissa käsittelemättä jätetty muutosvastarinta saattaa vaikuttaa tulevissa muutoksissa, joten uuden toimintatavan juurruttamisen vuoksi on välttämätöntä keskustella avoimesti ja ymmärtävästi muutosta vastustavien kanssa. Jokainen organisaation jäsen tulee saada ymmärtämään muutoksen syyt, vaikkeivat he muutosta varsinaisesti hyväksy ja samalla johdon tulee varautua siihen, että ainakin osa muutosta vastustavista tulevat lähtemään organisaatiosta. (Kauhanen 2018, 56–57.) Virtasen ja Stenvallin (2019, 169) näkemyksen mukaan muutosvastarintaan liittyy myös oman valta-aseman menettämisen pelko, mahdollisen sanktion pelko, jos henkilö ei sopeudu uuteen toimintatapaan tai organisaatioon sekä osaamattomuuden pelko, koska uudessa toimintatavassa tai organisaatiossa tarvitaan uusia taitoja ja uutta tekemisen kulttuuria.

Osaamisen johtaminen

Viitalan (2005, 12) mukaan osaamisen johtaminen on organisaation toiminta – ja kilpailukyvyn vahvistamista ja varmistamista käyttämällä hyväksi osaamisen suuntaamista, määrittelyä, arviointia, suunnittelua ja kehittämistä. Osaamisen johtamisen lähtökohtana on osaamisen valitseminen organisaation tietoisen johtamisen kohteeksi, jolloin siihen suunnataan riittävää huomiota ja resursseja.

Organisaation toiminta perustuu strategiaan, jossa suunnataan toimintaa tulevaisuuteen, varaudutaan toimintaympäristön muutoksiin aktiivisin toimin ja ennakoiden. Organisaation

osaamisen kehittämisen johtamisen tulee olla osa strategiaa. Strategiasta johdetaan niin organisaation toiminnan tulevaisuus ja osaamisen kehittämisen tavoitteet. Osaamisen johtaminen ei ole yksittäisen osaamisen lisäämistä kouluttamalla tai ostamalla vaan jokapäiväistä työn johtamista ja johtamistyötä. Osaamisen kehittäminen edellyttää aktiivista johtamista, sitä ei saada aikaan vahingossa. (Sumkin & Tuomi 2012.) Johdon tulee kuuntelemalla, kyselemällä, eri näkökulmia hakemalla ja kommentoimalla sekä tulokset yhteen vetämällä hyödyntää saamaansa tietoja ja samalla johtaa organisaation jäsenten ajattelua. Johdon tulee vähintään seurata organisaatiossa käytävää keskustelua, saadakseen selville millaisena henkilöstö näkee organisaation tulevaisuuden, tehdä keskustelusta johtopäätökset mahdollisia toimenpiteitä varten sekä viestiä nämä organisaation sisällä. (Otala 2018, 296.)

Oppimista edistävällä ilmapiirillä ja esimerkillä konkretisoidaan henkilöstölle osaamisen kehittämisen merkitys niin organisaation kuin yksilön menestymisen kannalta, jolloin osaamiseen kohdistuvista vaatimuksista tulee helpommin hallittavia ja osallistumisesta mielekästä. Henkilöstön ei ole aina helppo ymmärtää miten esimerkiksi tietosuojaan liittyvä koulutus liittyy työtehtävään, jolloin esihenkilön omalla asenteella on merkitystä osaamisen kehittymisessä. (Huttunen 2018, 214.)

Osaamisen johtamiseen liittyy myös osaamista koskeva riskienhallinta. Osaamiseen liitettävät riskit liittyvät organisaatiossa missä tahansa muodossa olevaan tietoon, joka voi joutua vääriin käsiin ja aiheuttaa vahinkoa organisaation toiminnalle sekä osaajien lähtöön, joka voi heikentää toimintakykyä ja pahimmillaan aiheuttaa vakavia katkoksia toimintaprosesseille. (Viitala 2005, 209.) Osaamisen riskeihin liittyy myös johdon työssä uudistuminen ja uuden tiedon omaksuminen. Virtasen ja Stenvallin (2019, 208–210) mukaan johtajien omia taitoja koskevan käsityksen ja niiden todellisen tason välillä on merkittävä kuilu. Johtamisen uudistumisen lähtökohtia ovat omia tietoja koskeva realistinen arvio, aito halu muuttua ja uudistua, sekä uuden tiedon omaksuminen. Johtamisen kehittäminen vaikuttaa aina kehittävästi koko organisaatioon.

Osallistaminen

Jatkuva kehittyminen ja muutos edellyttävät uusien toimintamallien toteutumista läpi koko organisaation alkaen strategiasta ja päättyen johtamisjärjestelmän päivittämisen kautta vision toteuttamiseen päivittäisessä toiminnassa (Tienari & Harviainen 2020, 161). Organisaation johdon tulee luoda puitteet, jossa henkilöstöllä on mahdollisuus osallistua uusien asioiden käsittelyyn aktiivisesti ja havainnoida omakohtaisesti millaisia puutteita organisaation toimintamalleissa on, jolloin heillä herää halu kehittää toimintaa. Osallistavilla menetelmillä muutosten vaikutuksista saadaan pitkäkestoisempia, koska henkilöstö ei koe olevansa

ainoastaan muutoksen kohde vaan aktiivinen vaikuttaja yhteiseen päämäärään pääsemisessä. Tässä auttaa myös muutoksen omakohtaiseksi kokeminen. (Huhtala 2015, 266.)

Osallistamiseen liittyy yhteiskehittäminen, joka tarkoittaa henkilöstön, asiakkaiden, toimittajien ja muiden yhteistyökumppaneiden hyödyntämistä organisaation toiminnan kehittämisessä vuorovaikutteisilla ja avoimilla menetelmillä. Yhteiskehittämisen avulla organisaation johto saa monipuolisesti erilaisia näkemyksiä ja sitä käytetäänkin usein strategian, toimintaprosessien tai palveluiden kehittämiseen. Yhteiskehittäminen edellyttää avointa vuorovaikutusta ja dialogia osapuolten välillä, työn tuloksista tiedottamista sekä osallistujien palkitsemista. (Vuorinen 2013, 132–135.)

2.1 Johdon esimerkki

Kunta- ja uudistusministeri Anu Vehviläinen (Rousku 2018, 9) painottaa Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman alkusanoissa turvallisuuden toteuttamisen olevan esimerkiksi toiminnan johtamista, viestintää, henkilöstön osaamista, toimittajaketjujen hallintaa, kokonaisarkkitehtuurin noudattamista sekä teknologiaratkaisuja, joiden muodostumisessa organisaation johdolla on keskeinen merkitys. Organisaation johto toimii omalta osaltaan esimerkkinä henkilöstölle.

Hyvä johtaminen, niin julkisessa hallinnossa kuin yrityksissä, on organisaation tavoitteiden saavuttamiseksi tehtävien päätösten toimeenpanoa, toimeenpanon valvomista ja toteutumisen raportointia. Johdon tulee huolehtia siitä, että jokaisella esihenkilöllä on ajantasainen tieto organisaation menestymisen kannalta keskeisistä päätöksistä ja tavoitteista ja esihenkilöt vastuutetaan kehittämään toimintaa. Organisaation johdon vastuulla on huolehtia toiminnan eettisyydestä, rehellisyydestä ja laillisuudesta. Johtamisen ja valvonnan ongelmat näkyvät usein väärinkäytöksinä tai organisaation ohjeiden ja sääntöjen rikkomisina. (Lautjärvi 2018, 67–69.)

Guhr ym. (2019, 353–354) tutkimuksessa johtajuuden (leadership) vaikutuksesta työntekijöiden tietoturvakäyttäytymiseen selvitettiin vaikuttaako johtamistapa henkilöstön tietoturvan noudattamista koskevaan aikomukseen ja tietoturva ylläpitämiseen osallistumiseen. Tutkimuksessa havaittiin, että passiivisella tai välttävällä johtajuudella tai henkilöstön tietoturvaan liittyvä käyttäytymisen huomiotta jättämisellä on negatiivinen vaikutus henkilöstön suunniteltuun tietoturvakäyttäytymiseen. Tutkimuksen mukaan johdon tulee osallistua tietoturvan toteuttamiseen myös muilla keinoilla kuin sääntöjen ja ohjeiden antamisella. Mikäli organisaation keskijohto ei ole kiinnostunut tietoturvasta tulee kehittää muita tapoja jalkauttaa tietoturvan mukainen toimintamalli henkilöstölle. Tällaisia ovat esimerkiksi tietoturvakoulutus- ja tietoisuusohjelmat, joiden jälkeen seurataan henkilöstön tietoturvatoimintaa.

Tutkimuksessa havaittiin myös, että hyvillä muutosjohtajilla on kyky saavuttaa myös tietosuojaan liittyviä muutostavoitteita, vaikka he eivät olisi itse tietoturvaan suuntautuneita. Guan & Hsu (2020, 1399) tutkimuksessa valvonnan ja organisaation sitoutumisen vaikutuksesta työntekijöiden tietoturvapolitiikkojen noudattamiseen havaittiin, että ylemmän johdon tulisi huomioida esihenkilöiden ja henkilöstön välisten suhteiden vaikutus organisaatioon sitoutumiseen, joka puolestaan vaikuttaa tietoturvapolitiikkojen noudattamiseen. Ylimmän johdon sitoutuminen ja esimerkki eivät riitä motivoimaan henkilöstöä, jos esihenkilön johtamistapa koetaan huonoksi. Vaikka johdon roolista ja vaikutuksista henkilöstön tietosuojatietoisuuteen ja tietosuojan noudattamiseen ei vielä ole laajasti tutkimusta, voidaan Guan & Hsu (2020) tietoturvaan liittyvän tutkimuksen havaintoja soveltaa etenkin, kun tietoturvan toteutuminen on edellytys tietosuojan toteutumiselle.

Luukan (2019, 304) leadership ja management käännöksen pohjalta voidaan tietosuojaan liittyvien lakisääteisten roolien valossa ajatella, että rekisterinpitäjällä ja henkilötietojen käsittelijällä on molemmilla sekä management, että leadership johtajuutta, mutta myös useita muita organisaation jokapäiväisen toiminnan johtamisen rooleja ja keinoja. Organisaation tietosuojan johtamisen näkökulmasta management olisi esimerkiksi johdon päätöksentekoa, tavoitteiden ja vastuiden määrittelemistä sekä tietosuojan nykytilan seurantaa ja siinä havaittuihin puutteisiin ja poikkeamiin reagointia. Leadership taas olisi johdon esimerkin näyttämistä, muutosten loppuun viemistä ja viestintää, tietosuojan kouluttamista sekä ilmapiirin luomista tietosuojamyönteiseksi ja poikkeamista avoimesti raportoivaksi.

2.2 Kehittämisprosessi

Kehittäminen ei ole projekti vaan prosessi, joka muodostuu tehtäväkokonaisuuksista, joita ovat: perustelu, organisointi, toteutus, levittäminen ja arviointi. Perustelu on kannanotto siihen, mitä ja miksi kehitetään, perusteluvaiheessa määritellään myös kehittämisprosessin lähtökohdat, joita voivat olla esimerkiksi nykytilanteen ongelma tai tulevaisuuteen tähtäävä visio. Organisointivaiheessa määritellään mitä tehdään ja mitä resursseja tekemiseen voidaan käyttää, koska tarvittavien resurssien saatavuus voi vaikuttaa oleellisesti toteutuksen laajuuteen. Organisointiin liittyy myös kehittämistä koskeva johdon päätöksenteko sekä viestintä ja informointi niin organisaation sisällä kuin sen sidosryhmille. Toteutuksessa tuotetaan ongelman ratkaiseva tai vision toteuttava kehittämistoiminta ideoimalla, kokeilemalla, testaamalla sekä priorisoimalla ja kohdentamalla toimenpiteitä. Levittämisvaiheessa juurrutetaan uutta toimintatapaa tai levitetään kehittämisprosessin kohdetta, esimerkiksi palvelua tai tuotetta. Viimeinen osa kehittämistoimintaa on sekä kehittämisen, että saadun

tuloksen arviointi, joiden avulla saadaan kehittämisprosessia ohjaavaa tietoa tulevia kehittämishankkeita varten sekä näyttöä tuloksen toimivuudesta. (Toikko & Rantanen 2009, 56–61)

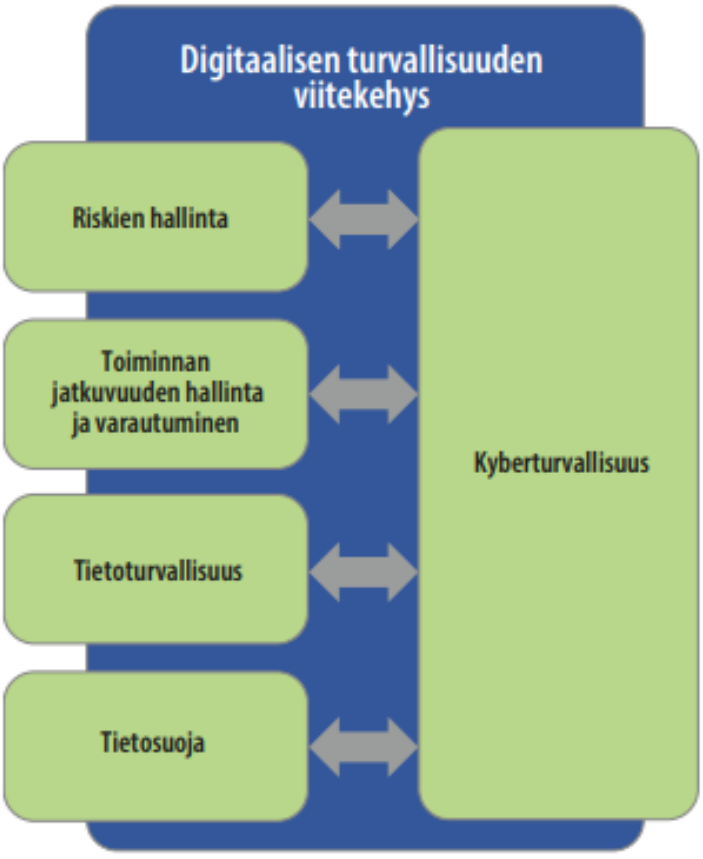
Organisaation kehittämistoiminnan lähtökohtana voi olla ulkoa tuleva muutospaine, esimerkiksi kansallinen sääntely, jonka Alasoini (2016, 20–22) jakaa koviin ja pehmeisiin sääntelymuotoihin. Kovaa sääntelyä on esimerkiksi lainsäädäntö sekä erilaiset normit ja standardit, kun pehmeäksi sääntelyksi katsotaan poliittinen ei-sitova puuttuminen ja vaikuttaminen. Organisaatioiden kehittämistoiminnan lähtökohtana on käytetty yleisemmin pehmeää sääntelyä, koska se sopii hyvin tilanteisiin, joissa muutostarve ja muutoksen kohteena olevat organisaatiot ovat erilaisia, samoin kuin muutokseen tähtäävät toimenpiteet, prosessit ja keinot. Kovan sääntelyn käyttäminen kehittämistoiminnan lähtökohtana on ollut harvinaista, koska esimerkiksi lainsäädäntöön perustuvan toiminnan johtamista pidetään organisaation sisäisen johdon vastuulla olevana toimintana.

Rannan (2021, 47) mukaan kehittämisprosessi kuten muutkin prosessit edellyttävät johtamista. Kehittämisjohtamiseen kuuluu kyky suunnitella organisaation kehittämistyötä tukeva systemaattinen järjestelmä, joka sisältää kehittämisprosessin tehtäväkokonaisuudet. Johdolla ja esimiehillä tulee olla kehittämisosaamista, eli kyky osallistaa henkilöstö kehittämiseen luomalla osallisuuden tunne, joka muodostuu vuorovaikutuksen ja kehittämiseen osallistumisen kautta. Johdon ja esimiesten kehittämisjohtamisen osaaminen sisältää kyvyn suunnitella systemaattinen organisaation kehittämistyötä tukeva järjestelmä, joka pitää sisällään kehittämisen aiheet, aikataulut ja seurantajärjestelmän. Johdon tulee pystyä määrittelemään kehittämisen tavoitteet ja viestimään niistä siten, että henkilöstöllä on riittävästi tietoa, resursseja ja tukea muuttaa toimintaa sovittujen tavoitteiden saavuttamiseksi. Henkilöstön kehittämisosaamista parannetaan lisäämällä ongelman ratkaisutaitoja, uusien toimintatapojen kokeilemista ja niiden tulosten arviointia, pienempien kehittämistoimien toteuttamista sekä muita jatkuvan parantamisen toimenpiteitä. Kehittämisosaaminen kasvaa käytännön kautta. Kehittäminen perustuu Leclin & Laine (2009, 53–56) mukaan muutoksiin, joiden taustalla voi olla uusi toteuttamistapa, eli innovaatio. Innovaatioiden syntymistä varten organisaatioon tulee pystyä luomaan innovaatiomyönteinen ilmapiiri, jossa kokeiluihin ja innovaatioihin kannustetaan ja niistä palkitaan.

3 Digitaalinen turvallisuus

3.1 Digitaalinen turvallisuus ja tietoturva

Digitaalinen turvallisuus on Valtionvarainministeriön käyttöön ottama termi kokonaisuudesta, johon kuuluvat keskeisinä turvallisuuden osa-alueina digitaalisen turvallisuuden johtaminen ja riskienhallinta, toiminnan jatkuvuus ja varautuminen, kyberturvallisuus, tietoturvallisuus sekä tietosuoja. Digitaalisen turvallisuuden kehittäminen on sen osa-alueiden avulla tapahtuvaa riskienhallintaan perustuvaa turvallisuuden kehittämistä, jossa samalla kehitetään myös kyberturvallisuutta. Kuviossa 3 esitetään digitaalisen turvallisuuden viitekehyksen sisältö. Viitekehykseen kuuluu kyberturvallisuus, riskienhallinta, jatkuvuuden hallinta ja varautuminen, tietoturvallisuus sekä tietosuoja. (Valtiovarainministeriö 2020, 16.)



Kuvio 3. Digitaalisen turvallisuuden viitekehys (Valtiovarainministeriö 2020, 16).

Digitaalinen turvallisuus on terminä uusi ja siksi vielä vakiintumaton niin kansallisesti kuin kansainvälisesti mistä johtuu termin käyttäminen kyberturvallisuuden synonyyminä. Kyberturvallisuus tarkoittaa verkottuneen ja digitaalisen organisaation tai yhteiskunnan turvallisuutta ja sen vaikutusta niiden toimintaan. Digitaalisen toimintaympäristön synonyyminä voidaan käyttää termiä kybertoimintaympäristö. Kyberturvallisuuden sisältämiä osa-alueita

ovat esimerkiksi kybervaikuttaminen, hybridivaikuttaminen, kyberdiplomatia sekä kyberresilienssi. (Valtiovarainministeriö 2020, 16–17.)

Digitaalisen turvallisuuden johtaminen ja kehittäminen ovat edellytyksiä yhteiskunnan toimintojen turvaamiselle, laadukkaiden ja turvallisten palveluiden tuottamiselle sekä kansalaisten ja sidosryhmien luottamukselle (Rousku 2018, 8). Organisaation johto on vastuussa digitaalisen turvallisuuden kokonaisuudesta ja sen toteutumisesta organisaation omassa toiminnassa, sekä sille tuotettujen palveluiden osalta. Lisäksi johdon vastuulla on digitaalisen turvallisuuden kokonaisuuden näkökulmasta vastuuhenkilöiden tehtäviin ja raportoinnin seurantaan liittyvä määrittely sekä henkilöstölle annettavien ohjeiden ja koulutusten järjestäminen, niihin osallistumisen ja poikkeamailmoitusten seuranta sekä digitaalisesta turvallisuudesta viestiminen (Kuvio 4). Digitaalinen turvallisuus on laaja kokonaisuus, jonka toteuttaminen edellyttää johdolta resurssien lisäksi sen osa-alueiden sitomista osaksi organisaation olemassa olevaa johtamisjärjestelmää. (Rousku 2018, 24).

Kuvio 4. Digitaalisen turvallisuuden osa-alueet johtamisen näkökulmasta (Rousku 2018, 24).

Toiminnan jatkuvuus ja varautuminen ovat erilaisiin toimintaan kohdistuviin häiriötilanteisiin ja poikkeamiin varautumista ennakkoon tehdyillä suunnitelmilla, joita ovat esimerkiksi jatkuvuus-, valmius- ja toipumissuunnitelmat. Osa-alueen avulla mahdollistetaan toiminnan palautuminen normaalille tasolle. Tietoturvallisuus pitää sisällään keinot organisaation suojattavien kohteiden tunnistamiseen sekä näiden saatavuuden, eheyden ja luottamuksellisuuden varmistamisen. Kyberturvallisuus pitää sisällään tietoturvasta huolehtimisen lisäksi

toimenpiteet tietojärjestelmäympäristöstä riippuvaisen fyysisen ympäristön toiminnan turvaamiseen. Kyberturvallisuudessa hallinnoidaan sähköisessä muodossa olevan datan ja informaation käsittelyyn käytettävien tietojärjestelmien uhkia ja riskejä, sekä kyberuhkien ennakoivia toimenpiteitä ja niiden vaikutuksia. Tietosuoja on perusoikeus, jolla turvataan rekisteröidyn eli henkilötietojen käsittelyn kohteena olevan käsittelyyn liittyvien oikeuksien ja vapauksien toteutuminen. Tietosuojalla osoitetaan milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. (Rousku 2018, 10–11.)

Digitaalisen turvallisuuden merkitys tulee kasvamaan sitä mukaa kun liiketoiminnan arvosta yhä suurempi osa muodostuu tietojenkäsittelyn hyödyntämisestä, jolloin tietoturvan ja –suojan riittävän tason varmistaminen on toiminnan välttämätön edellytys. Digitaalinen turvallisuus tulee nähdä teknologian ja digitalisoitumisen välttämättömänä osana ja turvallisen tietojen käsittelyn mahdollistajana. (Andreasson ym. 2015, 21.)

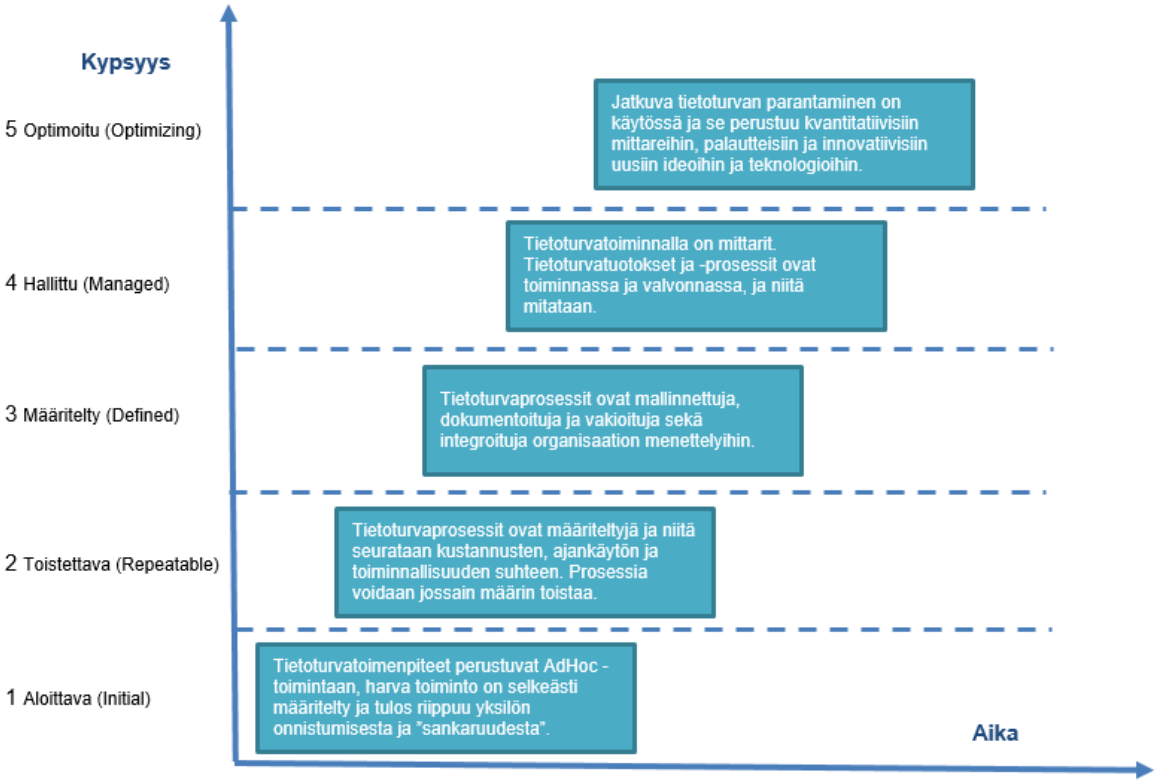
3.2 Tietoturva ja sen johtaminen

Tietoturvalla on merkitystä organisaation toimintakyvyn varmistamisessa, häiriöttömän ja tuloksellisen toiminnan ylläpitämisessä, toiminnan tehokkuuden ja laadun parantamisessa sekä organisaation palvelukyvyn lisäämisessä. Sen avulla varmistetaan organisaatiossa käsiteltävän tiedon luottamuksellisuus, eheys, käytettävyys ja saatavuus, joita toteutetaan kahdeksan tietoruvan osa-alueen avulla. Näitä ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. Tietoturva ei koske ainoastaan teknisiä ratkaisuja, kuten palomuureja, virustorjuntaa ja laitteita, vaan sen vaikutukset ulottuvat koko organisaation toimintaan kattaen myös turvallisuustoiminnan yleiset järjestelyt sekä ihmisten toiminnan. Hyvin johdettu tietoturva muodostaa perustan organisaation toiminnan luotettavuudelle ja jatkuvuudelle sekä perustan digitaalisten palveluiden tarjoamiselle. (Valtiovarainministeriö 2006a, 5, 15-16.)

Tietoturvan johtamisessa tarvitaan oikea aikaista ja luotettavaa tietoa tietoturvan tilasta, sekä organisaation tietoturvakulttuuri, joka pitää sisällään linjaukset oikeista menettelytavoista ja johdon asettamista tavoitteista, valvonnan kohteista ja perusteista. Organisaation johdon tulee sisällyttää tietoturva osaksi organisaation toimintaprosesseja ja luoda tietoturvan hallintajärjestelmä. (Bärlund & Perko 2013, 65.)

Hallintajärjestelmän avulla organisaation johdon valmius hallita tietoturvaa kehittyy ja hallintajärjestelmän kypsyyttä ja kehitysastetta voidaan arvioida. Arvioinnin avulla organisaa-

tion johto tuntee tietoturvan nykytilan ja pystyy tunnistamaan siihen liittyvät kehittämistarpeet. Kuviossa 5 on esitetty organisaation tietoturvan hallintajärjestelmän kehittyminen prosessien kypsyysarviointimalliin (CMM) perustuen. (Valtiovarainministeriö 2006b, 21)



Kuvio 5. Tietoturvan kypsyystasot (Valtiovarainministeriö 2006b, 21).

Organisaation johto aloittaa hallintajärjestelmän kehittämisen herätteestä, joka voi olla viranomaismääräys, ulkoa tuleva odotus, laatuvaatimus tai suositus, tietoturvariskeihin valmistautuminen tai havaittu tietoturvaongelma. Ensimmäisessä vaiheessa tietoturvatoiminta on organisoitumatonta ja reaktiivista, jolloin ohjeistusta tuotetaan käsillä olevaan tarpeeseen. Organisaation johdon tulee määritellä tietoturvan kehittämisen mahdollistavat tietoturvalinjaukset ja kirjata nämä tietoturvapolitiikkaan sekä määrittää tietoturvasta vastaavat. Toisessa vaiheessa tietoturvapolitiikkaa toteutetaan kehittämällä säännönmukaisia menettelyjä ja luomalla tietoturvan kehittämissuunnitelma. Systemaattisen toiminnan avulla tietoturva saavuttaa kolmannen vaiheen, jossa organisaation tietoturvaprosessit ja tavoitteet on määritelty ja tietoturvan hallintajärjestelmä syntyy. Organisaatiolle on luotu kattava tietoturvaohjeistus, henkilöstön säännöllinen koulutus on osa toimintamallia ja kehittämissuunnitelmaa toteutetaan. Hallintajärjestelmän neljännessä vaiheessa tietoturvatoiminta noudattaa laadittua suunnitelmaa ja toiminnalle on asetettu kehittämistarpeita ja tuloksellisuutta kuvaavat mittarit. Vasta vaiheessa neljä organisaatiolle on kehitetty tietoturvan johtamis- ja hallintajärjestelmä. Viidennessä ja viimeisessä vaiheessa johto optimoi tietoturvallisuuden

johtamis- ja hallintajärjestelmää auditointien ja niiden tulosten, muiden organisaatioiden kokemusten ja muun osaamisen kehittymisen avulla. Tietoturva on kiinteä osa organisaation joka päivästä toimintaa. (Valtiovarainministeriö 2006b, 22.)

3.3 Tietoturvan sääntely

Tietoturvatoimintaa ohjaavat säädökset, sekä suositukset kuten esimerkiksi VAHTI – ohjeet ja sertifikaatit, esimerkiksi ISO 27001, joissa määritellään tietoturvan minimi- ja tavoitetaso sekä suositukset tietoturvaratkaisujen toteuttamiselle. Tietoturvatoimintaa johdetaan asettamalla turvallisuustasoon liittyviä tavoitteita ja seuraamalla tuloksia määritellyillä mittareilla. Organisaation tietoturvatoiminnan tavoitteiden tulee linkittyä kuvion 6 mukaisesti organisaation toimintaa koskevaan lainsäädäntöön, toiminnan jatkuvuuteen ja laatuun, muutoksenhallintaan, sidosryhmiin sekä asiakkaisiin. (Valtiovarainministeriö 2006b,16.)

Kuvio 6. Tietoturvaa ohjaavat vaatimukset (Järvinen & Rousku 2017).

EU:n yleinen tietosuoja-asetus (EU 679/2016) ohjaa henkilötietojen käsittelyyn liittyvää tietoturvaa organisaatiosta riippumatta. Julkisen hallinnon ja viranomaisten osalta ohjausta sisältää sekä toimintaa koskeva lainsäädäntö, että yleislakina tiedonhallintalaki (906/2019). Organisaatiolla on palvelu- ja muussa hankinnassa määriteltyjä tietoturvavaatimuksia, jotka muodostavat osan sopimusta. Sopimuksen vastainen toiminta saattaa aiheuttaa tietoturvapoikkeaman tai – rikkomuksen, josta aiheutuvista kustannuksista voi seurata korvausvastuu tai muu sanktio. Organisaation tietoon liittyvän toiminnan turvallisuus ja jatkuvuus mahdollistavat häiriöttömän ja kustannustehokkaan toiminnan. Ongelmat tiedon saatavuudessa ja niiden aiheuttamat käyttökatkot lisäävät kustannuksia ja vähentävät sidosryhmien ja asiakkaiden luottamusta organisaation tuottamiin palveluihin. (Järvinen & Rousku 2017)

Tiedonhallintalain (906/2019) 4 luvussa säädetään tiedonhallintayksikön tietoturvaa koskevista velvollisuuksista, joihin sisältyy luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuuden varmistaminen, tietoaineistojen ja tietojärjestelmien tietoturvallisuus, tietojen turvallinen siirtäminen tietoverkossa, tietoaineistojen turvallisuuden varmistaminen, tietojärjestelmien käyttöoikeuksien hallinta, tietojärjestelmien käytön ja luovutettavien tietojen lokitietojen kerääminen, sekä valtion virastoja ja laitoksia erikseen velvoittavana asiakirjojen turvallisuusluokittelu.

Valtiovarainministeriön (2020, 5, 17) suositus tiedonhallintamallista on tiedonhallintalautakunnan antama tiedonhallintalain soveltamisen tukimateriaali, jonka avulla laissa määritelty tiedonhallintayksikkö, eli julkisen hallinnon viranomainen, pystyy määrittelemään tiedonhallintaan liittyvät tehtävät ja vastuut, laatimaan organisaatiolle tiedonhallintamallin ja ylläpitämään sitä. Tiedonhallintamallissa viranomainen, eli julkisen hallinnon organisaation johto, kuvaa kuinka tietoturvallisuus on suunniteltu ja toteutetaan, mitä menettelyjä tietojärjestelmien ja niiden sisältämien tietoaineistojen sekä tietojenkäsittelyn turvaamiseksi on toteutettu tai suunniteltu toteutettavaksi ja kuinka nämä toimenpiteet ovat vastuutettu. Tiedonhallintaan kohdistuvien tietoturvavaatimusten vähimmäisvaatimukset on kuvattu aikaisemmin mainitussa tiedonhallintalain 4 luvussa, minkä lisäksi henkilötietojen käsittelyn osalta tulee noudattaa tietosuoja-asetuksen (EU 679/2016) vaatimuksia. Tiedonhallintamalliin sisällytetään luetteloksi olemassa olevat tietoturvapolitiikat tai -periaatteet, ohjeet sekä muut organisaation tietoturvan toteuttamista kuvaavat dokumentit. (Valtiovarainministeriö 2020, 33.)

Julkisen hallinnon, eli viranomaisten ja muiden julkista hallintotehtävää hoitavien tulee huomioida tietoturvalle asetetut vaatimukset myös digitaalisten palveluiden tarjoamista (306/2019) koskevan, niin sanotun digipalvelulain lainsäädännön osalta. Lain 5 § velvoittaa viranomaisia tarjoamaan kaikille asiointia varten muiden asiointikanavien rinnalle sähköisiä viestintävälineitä ja digitaalisia palveluita. Lain 4 §:ssä viranomainen velvoitetaan suunnittelemaan ja ylläpitämään digitaaliset palvelunsa huomioiden niiden tietoturva, tietosuoja, löydettävyys ja helppokäyttöisyys sekä yhteensopivuus sähköisen asioinnin tukipalveluiden ja muiden viranomaisten digitaalisten palveluiden kanssa.

Kuntaliitto (Seppo 2020) on julkaissut Itä-Suomen yliopiston tuottaman taulukkopohjan (Digipalvelulaki ja tiedonhallintalaki - vaatimukset ja tilanne Excel-tiedosto työskentelyn tueksi), jonka avulla julkisen hallinnon organisaation johdon ja nimettyjen vastuuhenkilöiden on helppo arvioida tiedonhallintalain ja digipalvelulain vaatimukset.

3.4 Tietoturvan merkitys tietosuojalle

Palveluiden digitalisoituminen ja siirtyminen verkkoon, erilaiset massatiedot (Big Data) ja tietoaltaat, uudenlaiset päätelaitteet, sensorit ja älylaitteet sekä ajasta ja paikasta riippumaton toiminta edellyttävät organisaatioilta tieto- ja kyberturvallisuuden hallintaa ja varautumista tietoverkkorikollisuuteen, terrorismiin sekä valtiollisten tiedusteluorganisaatioiden toimintaan. (Valtiovarainministeriö 2016, 7.)

Digitaalisen ja kyberturvallisuuden vaikutusta tietosuojaan on kuvattu alla kuviossa 7. Siihen liittyvät tietoturvan (tietoturvallisuus) luottamuksellisuuden, eheyden ja saatavuuden

varmistaminen, häiriötilanteisiin varautuminen ja jatkuvuussuunnittelu, riskienhallinta, määritellyt mittarit, raportointi ja valvonta, sekä kokonaisuuden jatkuva kehittäminen. Kaikki nämä osa-alueet luovat perustan ja keinot tietosuojan toteutumiselle. (Valtiovarainministeriö 2016, 8).

Kuvio 7. Tietosuojan toteutumisen edellytykset.

EU:n yleinen tietosuoja-asetus (EU 679/2016) edellyttää 25 artiklassa henkilötietojen käsittelyyn sisäänrakennettua ja oletusarvoista tietosuojaa ja 32 artiklassa käsittelyn turvallisuudesta huolehtimista, eli henkilötietojen luottamuksellisuudesta ja eheydestä huolehtimista sekä lisäksi henkilötietojen käsittelyä tavalla, jolla varmistetaan niiden asianmukainen turvallisuus. Tämä tarkoittaa henkilötietojen suojaamista luvattomalta ja lainvastaiselta käsittelyltä, vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Nämä toteutetaan organisaation toimeenpanemilla teknisillä tietoturvatoimenpiteillä sekä organisatorisilla toimilla, joita ovat esimerkiksi tehtävien ja käyttövaltuuksien määrittely. Tietosuoja-asetuksen 35 artiklassa edellytetään henkilötietojen käsittelyn vaikutusten arviointia. Arviointi vahvistaa asetuksessa säädettyä riskiperusteista henkilötietojen käsittelyn suunnittelua, sillä se on pakollinen henkilötietojen käsittelyssä, johon kohdistuu arvioinnin mukaan korkea riski. Tietoturvan ja tietojen suojaamisen suunnitteleminen ja toteutus sekä sopimuksissa määritellyt yksityiskohtaiset tehtävät, vastuut ja henkilötietojen käsittelyn sisällöt, ovat tietosuojan onnistumisen edellytys (Andreasson ym. 2019,151).

4 Tietosuoja

4.1 Tietosuojan sääntely

Tietosuojavaltuutetun toimisto (2021) määrittelee tietosuojan perusoikeudeksi, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan avulla voidaan osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. EU:n yleisen tietosuoja-asetuksen (EU 679/2016) 5 artiklassa määritellään henkilötietojen käsittelyä koskevat periaatteet, joita ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus. Rekisterinpitäjä vastaa siitä, että henkilötietojen käsittelyssä noudatetaan näitä periaatteita, lisäksi rekisterinpitäjällä on osoitusvelvollisuus osoittaa, että periaatteita on noudatettu.

Henkilön yksityisyyden suoja rakentuu Euroopan ihmisoikeussopimuksen 8 artiklan, kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen 17 artiklan sekä perustuslain 10 pykälän yksityiselämän suojan sääntelylle. Henkilötietojen suoja kattaa laajemman alan kuin yksityisyyden suoja, koska henkilötietojen suojaan kuuluvat myös yksityisen elämän ja kotirauhan ulkopuoliset, esimerkiksi työsuhteeseen tai julkiseen asemaan liittyvät tiedot. (Korpisaari ym. 2018, 5.)

Perustuslain mukaan henkilötietojen suojasta tulee säätää lailla, jossa huomioidaan perusoikeussuojan keskeinen sisältö, jolloin henkilötietojen käsittelyn perusteet ja vaatimukset määräytyvät EU:n yleisen tietosuoja-asetuksen (EU 679/2016) ja sitä täydentävän ja täsmentävän tietosuojan lain perusteella. Rikosasioissa viranomaisen suorittaman henkilötietojen käsittelyn sääntely perustuu rikosasioiden tietosuojadirektiiviin (EU 680/2016), joka on kansallisesti saatettu voimaan lailla henkilötietojen käsittelystä poliisitoimessa (616/2019) ja rikosasioiden tietosuojalailla (1054/2018). Lisäksi erityislainsäädäntö määrittelee henkilötietojen käsittelyä muun muassa Puolustusvoimien, Rajavartiolaitoksen ja Tullin toiminnassa. (Mäenpää 2021.)

Tietosuoja-asetus (EU 679/2016) korvaa direktiivin 95/46/EY, joka on Suomessa pantu täytäntöön henkilötietolailla (523/1999). Tietosuojadirektiivin voimaantullessa 1995 henkilötietojen käsittely ja niiden hyödyntäminen liiketoiminnassa oli hyvin erilaista verrattuna tämän päivän sosiaalista mediaa, pilvipalveluita ja sijaintitietoja hyödyntäviin globaaleihin digitaalisiin palveluihin. Henkilötietojen käsittelyä ulkoistetaan osittain tai kokonaan, joko kotimaassa tai globaalisti. Henkilötietojen käsittelyn ja tietosuojatarpeiden luonne ovat muuttu-

neet merkittävästi ja onkin ollut tarpeen luoda eurooppalainen riskilähtöinen ja teknologiariippumaton tietosuojasääntely, joka toimia myös digitaalisen liiketoiminnan mahdollistajana.

Direktiivi on lainsäädäntöohje, jonka kukin jäsenvaltio toteuttaa omassa kansallisessa lainsäädännössään, eli kussakin jäsenvaltiossa on ollut kansallinen henkilötietojen käsittelyä koskeva lainsäädäntö. Useassa EU:n jäsenvaltiossa toimiva rekisterinpitäjä joutui selvittämään jokaisen maan tietosuojalainsäädännön sekä asioimaan erikseen jokaisen maan tietosuojaviranomaisen kanssa. Tietosuoja-asetuksen on tarkoitus harmonisoida tietosuojasääntely EU:ssa tasapuolisilla säännöksillä, jotka koskevat sekä EU:ssa että sen ulkopuolella toimivia rekisterinpitäjiä. (Valtiovarainministeriö 2016, 6.)

Valtioneuvoston kanslian rahoittamassa yleisen tietosuoja-asetuksen kansallista toimeenpanoa selvittäneessä hankkeessa IPR University Centerin, Helsingin yliopiston ja Lapin yliopiston tutkijat kävivät läpi lähes 800 säädöstä arvioiden ovatko ne oikeusperustan osalta sopusoinnussa yleisen tietosuoja-asetuksen kanssa. Arvioinnin perusteella havaittiin, että suurimmaksi osaksi säädökset ovat yhteensopivia ja erot direktiivin 95/46/EY sekä yleisen tietosuoja-asetuksen vaatimusten välillä osoittautuivat tässä suhteessa melko pieniksi. Hanke löysi muutamia toimenpiteitä edellyttäviä säännöksiä. (Oikeusministeriö 2017, 21.)

Tietosuojalainsäädännön muutosta ja tietosuoja-asetuksen vaikeaselkoisuutta käytetään perusteena tietosuojatoimenpiteiden puuttumiselle, vaikka tietosuojan muutostarvetta koskevassa hankkeessa (Oikeusministeriö 2017, 21) osoitettiin, että erot aikaisempaan lainsäädäntöön olivat melko pieniä. Suomessa henkilötietojen käsittelyn sääntely alkaa henkilörekisterilaista (471/1987), joka tuli voimaan vuonna 1988. Seuraava vaihe sääntelyssä oli Euroopan Unionin 1995 antama henkilötietodirektiivi (95/46/EY), jonka pohjalta säädettiin kansallinen henkilötietolaki (523/1999) vuonna 1999. Henkilötietolakia sovellettiin vuoteen 2019 saakka, jolloin tietosuoja-asetuksen täydentävä kansallinen tietosuojalaki (1050/2018) astui voimaan. Voidaankin sanoa, että organisaatioiden johdon tulisi pohtia onko lainsäädäntöä noudatettu alkuperinkään riittävällä tasolla, jos tietosuoja-asetuksen siirtymäajan muutokset tuntuivat kohtuuttoman suurilta.

4.2 Lainmukaisuuden johtaminen tietosuojan näkökulmasta

Ratsulan (2016, 12) mukaan vaatimustenmukaisuuden (compliance) lähtökohtana on lakien ja säännösten mukainen toiminta, ulkopuolisten tahojen asettamat moraaliset ja eettiset vaatimukset, sekä organisaation itselleen asettamat vaatimukset, jotka organisaation johto ilmaisee toimintaperiaatteina ja sääntöinä. Vaatimustenmukaisuus liitetään myös eettisyyteen, joka on organisaation arvoja ja kulttuuria, sekä käsitys siitä, mikä on sallittua ja

mikä ei. Vaatimustenmukaisuuden näkökulmasta organisaation johdon on hyvä laatia erillinen tietosuojaohjelma tai -suunnitelma (Privacy program), joka on jäsennelty suunnitelma vastuullisen tietosuojan toteuttamisesta (Ratsula 2016, 131).

Tietosuoja-asetuksen (EU 679/2016) mukaan kaiken henkilötietojen käsittelyn tulee olla lainmukaista ja vastuu tästä on rekisterinpitäjällä. Tämä tarkoittaa käytännössä, että organisaation johdon tulee määritellä, mikä taho, rooli tai henkilö on rekisterinpitäjä kussakin organisaation henkilötietojen käsittelyn kokonaisuudessa (ns. henkilörekisteri) ja mikä taho, rooli, henkilö tai henkilöt edustavat rekisterinpitäjää. Tietosuojan johtamismalli ja resursointi tulee suunnitella mukautumaan toiminnan tarpeisiin myös poikkeustilanteissa. Organisaation johdon tulee määritellä kuka käytännössä johtaa ja koordinoi tietosuojaa. Tässä roolissa tulee voida toimia organisaation ylimmän johdon mandaatilla siten, että päätöksentekoprosessi on koko organisaatiolle selvä. Mikäli useat henkilöt voivat tehdä tietosuojan organisoinnin linjauksia, syntyy väistämättä ristiriitatilanteita. (Andreasson ym. 2019, 77–78.)

Niin yrityksiä kuin julkista hallintoa koskee hyvän hallintotavan periaate, johon lainsäädännön noudattamisen lisäksi sisältyy riskienhallinnan ja sisäisen valvonnan järjestäminen. Sisäinen valvonta on menettelytapa, jolla varmistetaan, että organisaatio toimii säädösten ja ohjeiden mukaisesti sekä hyvää hallintotapaa noudattaen. Sisäinen valvonta varmistaa, että organisaatio toteuttaa johdon asettamat toimintaohjeiden mukaiset tavoitteet, sekä kehittää organisaation toimintatapoja, sekä ehkäisee ja paljastaa erehdykset, virheet ja väärinkäytökset. (Lautjärvi 2018, 85–86.)

4.3 Tietosuojan kehittäminen

Tietoturva- ja tietosuojatyön ensisijaisena päämääränä on turvata organisaation vastuulla olevien palveluiden jatkuvuus. Tietosuojatyön johtamismallista ja resursoinnista tulee tehdä sellaiset, että ne pystyvät nopeasti ja oikeilla toimintatavoilla mukautumaan poikkeustilanteisiin sekä osaltaan pienentämään mahdollista syntyvää vahinkoa ja nopeuttamaan toipumista. Tietosuojatyön kehittämisen varmistamiseksi organisaation ylimmän johdon tulee määritellä ylin tietosuojasta tilivelvollinen taho, jolla on oikeus nimetä organisaation tietosuojaa johtava ja kokonaisuudesta vastaava. (Andreasson ym. 2019, 77.)

Silvola & Landau (2019) mukaan yritystoimintaan sijoittavat tahot selvittävät yrityskohtaisia riskejä arvioidessaan myös tietoturvaan ja tietosuojaan liittyviä riskejä yritysten itsensä julkaisemien periaatteiden ja tietojen pohjalta ilman kovin syvällisiä ja yksityiskohtaisia tietoja. Toisaalta organisaation sisäisten tietojen julkaisemisessa tuleekin olla varovainen, mutta tietoturvaan ja tietosuojaan liittyvien riskien todennäköisyyteen ja seurauksiin vaikuttavat tekijät, kuten esimerkiksi varmuuskopiointi, ohjelmistopäivitykset, tietoturvaloukkauksiin ja

–murtoihin varautumisaste sekä organisaation yleinen kulttuuri tietoturvan ja tietosuojan johtamisen osalta tulisi voida arvioida ennen sijoittamista. Organisaation tietoturvan ja tietosuojan toimintakulttuuria voidaan arvioida muun muassa sillä, onko organisaatiolla nimetty tietoturvasta vastaava henkilö, mihin hän sijoittuu organisaatiossa ja kenelle hän raportoi, kuinka organisaatio viestii verkkosivuillaan tietoturvasta ja tietosuojasta ja niiden merkityksestä, julkaiseeko organisaatio esimerkiksi tietotilinpäätöksen tai auditoinnin tuloksen, onko sillä johonkin palveluun liittyvä sertifiointi, onko organisaatiolla niin sanottu “bug nounty” -ohjelma, jossa maksetaan palkkio jokaisesta havaitusta tietoturva-aukosta, onko organisaatiolla tietoturvaan tai kyberturvallisuuteen liittyvä vakuutus, jonka edellytyksenä on perustason vaatimusten läpäiseminen sekä, kuinka usein organisaation hallituksessa ja muissa johdon kokouksissa käsitellään tietoturvaan ja tietosuojaan liittyviä asioita. (Silvola & Landau 2019, 276–278.)

4.4 Tietosuojan kustannusvaikutukset

Oikeusministeriön (2017, 14, 25) mukaan tietosuoja-asetuksen (EU 679/2016) soveltamisesta aiheutuu organisaatioille toimintaan liittyvien muutosten lisäksi myös kustannusvaikutuksia muun muassa seuraamusjärjestelmän tehostamisen ja yhdenmukaistamisen myötä. Seuraamuksilla edistetään tietosuoja-asetuksen noudattamista mikä ennaltaehkäisee tietosuoja- ja tietoturvaloukkauksia ja parantaa henkilötietojen suojan toteutumista.

Tietosuoja-asetuksen (EU 679/2016) kustannusvaikutuksista uutisoitaessa esille nousee useimmiten 83 artiklassa säädetty hallinnollinen sakko, josta kansallisesti säädetään tietosuojalain 24.1 pykälässä (1050/2018). Hallinnollisella sakolla tarkoitetaan hallinnollista seuraamusmaksua, eli rangaistusluonteista taloudellista seuraamusta, joka voidaan määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle. Kyse on siis hallinnollisesta eikä rikosoikeudellisesta seuraamuksesta, jonka määrää tietosuojavaltuutetun toimiston sisäinen tietosuojavaltuutetusta ja kahdesta apulaistietosuojavaltuutetusta koostuva toimielin, seuraamuskollegio.

Tietosuoja-asetus (EU 679/2016) säätää tietosuojaviranomaisen, Suomessa tietosuojavaltuutetun, toimivallasta antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle hallinnollista ohjausta, jonka keinoja ovat esimerkiksi huomautus tai varoitus, oikeudesta nataa määräyksiä muun muassa ilmoitusvelvollisuudesta rekisteröidylle, rekisteröidyn oikeuksien toteuttamiseksi, käsittelytoimien saattamiseksi tietosuoja-asetuksen tai siihen liittyvien muiden säännösten mukaisiksi, henkilötietojen käsittelyn rajoittaminen tai käsittelykiellon asettaminen väliaikaisesti tai pysyvästi, sekä henkilötietojen siirron keskeyttäminen kolmanteen maahan. Tietosuojavaltuutettu voi myös peruuttaa tai määrätä sertifiointielimen perumaan

tietosuojaan liittyvä sertifiointi. Tietosuojavaltuutetun antamat päätökset ja ratkaisut julkaistaan Finlex –palvelussa (Finlex).

Hallinnollista sakkoa voidaan käyttää edellä mainittujen seuraamusten lisäksi tai niiden sijaan, mutta sen määräämistä on rajoitettu kansallisesti tietosuojalain (1050/2018) 24.4 pykälässä siten, että seuraamusmaksua ei voida määrätä valtion viranomaisille tai niiden liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle, Suomen evankelisluterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille. Edellä lueteltuihin viranomaisorganisaatioihin sovelletaan kuitenkin rikosoikeudellista virkavastuuta koskevia säännöksiä, joten hallinnollisen seuraamusmaksun sijaan rekisterinpitäjän toiminnasta vastuussa oleva virkamies voi joutua vastaamaan rikosoikeudellisesti tietosuoja-asetuksen vastaisesta henkilötietojen käsittelystä rikosnimikkeellä virkavelvollisuuden rikkominen. (Voutilainen 2019, 208–211.)

Tietosuoja-asetuksen (EU 679/2016) 82 artiklassa säädetään erikseen vahingonkorvauksesta rekisteröidylle, jos asetuksen rikkomisesta seuraa tälle aineellista tai aineetonta vahinkoa. Korvausvelvollisia ovat rekisterinpitäjät ja henkilötietojen käsittelijät, mutta ensisijaisesti vastuu on rekisterinpitäjällä. Rekisterinpitäjän ja henkilötietojen käsittelijän keskinäiset vastuut ja velvollisuudet tulee selvittää vasta korvauksen maksamisen jälkeen.

Ciscon vuonna 2020 (3–5) tekemä tutkimus osoitti, että tietosuojaprosessien tehostaminen mahdollistaa ketteryyttä ja innovointia, minimoi tietoturvaloukkausten seuraamuksia, sekä parantaa yrityksen asemaa sijoittajien silmissä, rakentaa luottamusta kuluttajien suuntaan ja tehostaa myyntiä ja yli 40 % tutkimukseen vastanneista yrityksistä kertoi saavansa tietosuojaan kohdentamansa investoinnit yli kaksinkertaisesti takaisin. Tästä näkökulmasta olisikin järkevää, että organisaatiolla on tietoturvan kehittämiseen varatun budjetin lisäksi myös tietosuojabudjetti. Tietosuojan jatkuvalla kehittämisellä organisaatio minimoi vaikeammin arvioitavia tietosuojapoikkeamien seurauksia kuten esimerkiksi maineriskiä.

5 Tietosuojasuunnitelma

5.1 Tietosuojasuunnitelman malli

Tietosuojasuunnitelma (Privacy program) on jäsennelty suunnitelma, jonka avulla organisaatio voi täyttää lakisääteiset tietosuojaan kohdistuvat vaatimuksensa. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) asettama työryhmä esittää raportissaan EU – tietosuojan kokonaisuudistus (Valtiovarainministeriö 2016, 31) organisaation tietosuojan kehittämistoimien jakamista neljään osa-alueeseen kuvion 8 mukaisesti: johtaminen, kehittäminen, ohjeet ja koulutus sekä seuranta ja raportointi. Vaiheita edeltää tietosuojan nykytila-analyysi, jonka avulla organisaation henkilötietojen käsittelyn ja tietosuojakyvykkyyksien nykytilaa arvioidaan suhteessa tietosuoja-asetuksen vaatimuksiin.

Kuvio 8. Tietosuojan kehittämistoimien osa-alueet (Valtiovarainministeriö 2016, 31).

Valtiovarainministeriön Vahti – raportissa (Valtiovarainministeriö 2016, 36) todetaan, että tietosuojavaatimusten toteuttaminen ja toiminnan kehittäminen edellyttävät jokaiselta organisaatiolta toimenpiteitä. Toteutettavan kokonaisuuden ja tarvittavan muutoksen laajuuteen, haastavuuteen ja kestoon vaikuttavat muun muassa johdon tuki ja ymmärrys, mitä paremmin organisaation johto on tietoinen kokonaisuudesta ja sitoutunut sen johtamiseen, tukemiseen ja toteuttamiseen, sitä helpompi tietosuojan nykytila on saada lainsäädännön edellyttämälle tasolle. Mitä pidempään ja enemmän organisaatiossa on tehty tietosuojatyötä ja henkilötietojen käsittelyn prosessien suunnittelua ja kehittämistä, sitä helpompaa toiminnassa olevien prosessien kehittäminen ja päätöksenteon nopeus ja joustavuus ovat verrattuna organisaatioihin, jotka ottavat menetelmät käyttöön kokonaan uusina asioina.

Ensimmäinen ja yksi tärkeimmistä toimenpiteistä on organisaation johdon osallistuminen ja tuen antaminen tietosuojatyölle. Johdon tulee omistaa organisaation tietosuojatoiminta ja sisällyttää se osaksi strategista ohjausta ja vastata siitä, että tietosuoja sidotaan osaksi organisaation jokapäiväistä toimintaa ohjaamalla tietosuojan nykytilan arvioimiseksi tarvittavia resursseja, antaa riittävät valtuudet ja mahdollistaa arvioinnin tuloksena tunnistettujen kehitystoimenpiteiden toteuttaminen käyttäen hyväksi organisaatiossa jo olemassa olevia välineitä sekä seurata tietosuojan kehittämistä säännöllisesti raportoinnin avulla. (Valtiovarainministeriö 2016, 31, 36.)

Tietosuojasuunnitelman sisältö

Vahti – raportti (Valtiovarainministeriö 2016) sisältää useita suosituksia toimenpiteistä, joihin organisaation johto voi ryhtyä tunnistaakseen mahdolliset puutteet ja saattaakseen tietosuojan tilan lainsäädännön edellyttämälle tasolle sekä osaksi jokapäiväistä strategialähtöistä operatiivista toimintaa. Seuraavassa luetellaan Vahti – raportissa kuvatut kehittämiskohteet. Organisaation johdon tulee priorisoida nämä kehittämiskohteet esimerkiksi tietosuojan nykytila-analyysilla, jossa organisaation henkilötietojen käsittelyn ja tietosuojakyvykkyyden nykytila analysoidaan suhteessa tietosuoja-asetuksen vaatimuksiin. Analyysimenetelmänä voidaan käyttää esimerkiksi puuteanalyysiä (GAP – analyysi), jossa verrataan organisaation tietosuojan ja henkilötietojen käsittelyn nykytilaa tietosuoja-asetuksen, tietosuojalain sekä henkilötietoja koskevan erityislainsäädännön vaikutuksiin tai kuvataan henkilötietojen käsittelyn nykytilan tai tavoitetilan välistä eroa. (JHS 171.) Julkisen hallinnon organisaatioille on tarjolla Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) ja julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) vuosina 2017–2018 järjestämien tietosuojan yhteishankkeiden materiaaliin sisältyvä Julkisen hallinnon GDPR-itsearviointityökalu – versio 12.2.2018 (xlsx). (Valtiovarainministeriö 2017b.)

RACI-malli

Tietosuojasuunnitelman osa-alueista esimerkiksi henkilötieto- ja sopimusinventaariossa, organisaation tietosuojavastuiden määrittelyssä ja riskienhallinnan kehittämisessä voidaan käyttää hyväksi RACI – mallia. RACI – lyhenne tulee sanoista responsible eli vastuullinen, accountable eli vastuussa oleva, consulted eli neuvonantaja ja informed eli tiedotettava. Malli on esitelty 1950 – luvulla ja siitä käytetään myös nimitystä vastuumatriisi. Mallia käytetään erilaisissa yrityksissä sekä projekteissa maailmanlaajuisesti ja se auttaa määrittelemään minkä verran ja kenelle organisaatiossa kuuluu päätöksentekovaltaa, vastuuta ja toimenpiteiden suorittamista. (Solomon 2020, 4–7.)

Responsible, eli vastuullinen on nimetty rooli tai henkilö, jonka tehtävänä on suorittaa annettu toimenpide tai kuulua toimenpidettä suorittavaan ryhmään. Jokaisella toimenpiteellä

tulee olla nimettynä vähintään yksi vastuullinen tekijä. Accountable, eli vastuussa oleva on nimetty valvomaan toimenpiteen suorittamista. Jokaisella toimenpiteellä on vain yksi vastuussa oleva. Consulted, eli neuvonantaja ohjeistaa ja neuvoo toimenpiteen suorittamiseen liittyvissä kysymyksissä. Toimenpiteellä voi olla rajaton määrä neuvonantajia, tietosuojaan liittyvissä tehtävissä näitä ovat yleisesti tietosuojavastaava ja tietoturvasta vastaava. Informed, eli tiedotettava on rooli tai henkilö, jolle tiedotetaan toimenpiteen suorittamisen tilasta ja lopputuloksesta. Toimenpiteellä voi olla rajaton määrä tiedotettavia. Tietosuojaan liittyvissä toimenpiteissä näitä ovat aina rekisterinpitäjät, ellei rekisterinpitäjä ole määritellyt itseään toimenpiteestä vastuussa olevaksi. Rekisterinpitäjä voi määritellä itselleen henkilötietojen käsittelystä vastaavan edustajan, jolloin tämä rooli on yleensä vastuussa käsittelyn ohjaamisesta sekä muutoksista ja poikkeamista tiedottamisesta rekisterinpitäjälle. (Rousku 2017 Liite 4, 7.)

5.2 Henkilötieto- ja sopimusinventaario

Henkilötieto- ja sopimusinventaario- osiossa selvitetään organisaation keräämien ja käsittelemien henkilötietojen kokonaiskuva sekä tunnistetaan henkilötietoja käsittelevät kolmannet osapuolet ja näihin liittyvät sopimukset (Valtiovarainministeriö 2016, 32).

Organisaation johdon ja rekisterinpitäjien tulee pitää kirjaa kaikista henkilötietojen käsittelytoimista, olla selvillä sen keräämien ja käsittelemien henkilötietojen kokonaiskuvasta sekä tunnistaa missä ja kenen toimesta henkilötietoja käsitellään. Organisaation lukuun henkilötietoja käsittelevät osapuolet tulee tunnistaa ja arvioida näihin käsittelyihin liittyvät tietosuojavaatimukset sekä selvittää käsitelläänkö henkilötietoja tai siirretäänkö niitä EU:n tai ETA – alueen ulkopuolelle ja jos siirretään, onko siihen olemassa tämän päivän lainsäädännön mukaiset perusteet. Mm. Yhdysvaltoja koskevat henkilötietojen käsittelyn ja siirron lakiperusteet ovat muuttuneet viimeisten vuosien aikana useasti eivätkä kaikki Brexitin vaikutukset, ja sääntelyn lopullinen muoto ole vielä selvillä. Organisaation johdolla tulee olla ajantasainen tieto siitä mitkä sen henkilötietojen käsittelyistä ovat näiden muutosten alaisia ja millaisia päätöksiä käsittelyä koskien tulee tehdä. Organisaatio voi esimerkiksi joutua muuttamaan omia prosessejaan, vaihtamaan tietojärjestelmiään tai henkilötietoja käsitteleviä osapuolia mukaan lukien näiden alihankkijat. (Valtiovarainministeriö 2016, 28–29.)

Organisaatio voi mallintaa henkilötietojen käsittelyä kuvaamalla jokaisesta käsittelykokonaisuudesta / rekisteristä siihen liittyvät henkilötietotyypit, mistä henkilötiedot tulevat, henkilötietoja käsittelevät sovellukset, järjestelmät ja roolit sekä miten henkilötiedot liikkuvat niiden välillä, käsittelyyn liittyvät fyysiset sijainnit sekä luovutetaanko tai siirretäänkö henkilötietoja edelleen kolmansille osapuolille sekä kuinka kauan henkilötietoja käsitellään ja kuinka ne

tullaan hävittämään. Tätä kuvausta kutsutaan henkilötietojen tietovirraksi. Tietovirtakuvauksen yhteydessä on syytä arvioida ovatko henkilötietojen käsittelyn dokumentit eli seloste käsittelytoimista, käsittelyn riskienarviointi ja mahdollinen käsittelyn vaikutustenarviointi sekä rekisteröidylle annettava informointi tai tietosuojaseloste ajan tasalla. Dokumentaatio on osa tietosuoja-asetuksessa säädettyä osoitusvelvollisuutta. (Valtiovarainministeriö 2016, 32.) Dokumentaation luomisessa voidaan hyödyntää organisaatiossa olevaa tietoa, esimerkiksi palvelukuvauksia – ja lupauksia, tiedonohjaussuunnitelmaa sekä laatudokumentaatiota.

Henkilötietojen käsittelytoimien tunnistamisen lisäksi organisaation johdon tulee huolehtia siitä, että organisaatiolle on luotu sen käyttötarkoituksiin sopiva tietojen luokittelumalli. Tietojen luokittelun tarkoituksena on tunnistaa organisaation käsittelemät, niin sen omassa hallinnassa kuin ulkoistuskumppaneiden ja palveluntarjoajien hallussa olevat tiedot yleisellä tasolla ja määritellä tiedoille tietojoukot, niiden suojausluokat sekä kriittisyystaso. Tiedon suojausluokan ja kriittisyystason tunnistaminen auttaa määrittelemään oikein tiedon käsittelyyn käytettävän tietojärjestelmän ja tietoverkon tietoturvaan ja tietosuojaan liittyvät hallinnolliset ja tekniset toimenpiteet. Oikein määritellyn luokittelun avulla mahdollistetaan myös kustannustehokas ICT-palveluhallinta. (Andreasson ym. 2015, 98–99.)

Organisaation johdon tulee olla selvillä sen lukuun henkilötietoja käsittelevien osapuolten kanssa tehtyjen sopimusten sisällöistä ja siitä, vastaavatko sopimusten tietoturvavaatimukset henkilötietojen suojaamiselle asetettuja vaatimuksia. Voimassa oleviin henkilötietojen käsittelyä koskeviin sopimuksiin tulee viedä tietosuoja- asetuksen (EU 679/2016) vaatimukset erillisenä liitteenä tai uutena henkilötietojen käsittelyn sopimuksena sen mukaisesti, miten sopimusmuutos on alkuperäisessä sopimuksessa määritelty. Organisaation sopimusvastuullisten tulee tarkastella käytettävien sopimuspohjien ajantasaisuus tietosuojavaatimusten osalta ja tarvittaessa päivittää ne, lisäksi tulee hallita sopimuksiin tehtäviä muutoksia esimerkiksi henkilötietojen käsittelyn riskiarvion päivittyessä. (Valtiovarainministeriö 2016, 32.)

Tietosuoja-asetus (EU 679/2016) on selkeyttänyt rekisterinpitäjän (organisaatio) ja käsittelijän (organisaation lukuun henkilötietoja käsittelevä sopimuskumppani) välistä sääntelyä ja aikaisemmasta lainsäädännöstä poiketen osoittaa tietosuojaan liittyviä velvollisuuksia suoraan käsittelijälle. Rekisterinpitäjän lakisääteisiin velvollisuuksiin kuuluu käyttää palveluntuottajana vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa, toteuttavat asianmukaiset tekniset ja organisatoriset toimenpiteet sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta. (Korpisaari ym. 2018, 293.)

Tietosuoja-asetuksen (EU 679/2016) 28 artiklan mukaan henkilötietojen käsittelyä koskevassa sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Lisäksi tulee varmistaa, että henkilötietojen käsittelijä:

- Käsittelee henkilötietoja ainoastaan rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti. Tähän sisältyy myös henkilötietojen käsittelyyn liittyvät sallitut tietojen siirrot ja sijainnit
- Noudattaa salassapitovelvollisuutta
- Toteuttaa tietoturvallisuuden henkilötietojen käsittelyssä tietosuoja-asetuksen vaatimilla toimenpiteillä
- Ei ulkoista henkilötietojen käsittelyn tehtäviä ilman rekisterinpitäjän kirjallista ennakkosuostumusta
- Auttaa rekisterinpitäjää rekisteröidyn oikeuksien toteuttamisessa
- Auttaa rekisterinpitäjää käsittelyn tietoturvallisuuden toteuttamisessa, henkilötietojen tietoturvaloukkausten havaitsemisessa ja niistä ilmoittamisessa sekä vahinkojen minimoinnissa, vaikutustenarviointien tekemisessä ja valvontaviranomaisen ennakkokuulemisessa tietosuoja - asetuksen mukaisesti.
- Joko poistaa tai palauttaa henkilötiedot rekisterinpitäjälle käsittelypalvelujen päättyessä. Käsittelijän tulee myös poistaa niistä hallussaan olevat kopiot.
- Sallii rekisterinpitäjän suorittaa auditoinnit ja osallistuu niihin itse. Käsittelijän tulee myös saattaa rekisterinpitäjän saataville kaikki sellaiset tiedot, jotka ovat tarpeen asetuksen velvollisuuksien noudattamisen osoittamista varten. Lisäksi on syytä erikseen miettiä ja sopia eli ilmoittaa
- rekisterinpitäjälle, mikäli sen ohjeistus rikkoo asetuksen säännöksiä.

Lisäksi organisaation tulee osana turvallisuussopimusta harkita seuraavaa:

- Sitoutumista siihen, että henkilötietojen käsittelyä suorittavat vain sellaiset henkilöt, jotka ovat
- saaneet hyväksyttävän tuloksen turvallisuusselvityksessä, jos rekisterinpitäjällä on lainmukainen oikeus teettää turvallisuusselvityksiä ja jos rekisterinpitäjä selvitysten teettämistä käsittelijältä vaatii.

Sopimusvaatimusten lisäksi tulee määritellä keinot, joilla henkilötietojen käsittelijän palvelun laatua seurataan. Tietosuojan ja tietoturvan osalta tulee määritellä säännöllisen raportoinnin käytännöt sekä järjestää säännöllinen rekisterinpitäjän ja käsittelijän välinen toimintamalli, jonka avulla seurataan tietosuojan ja tietoturvan toteutumista henkilötietojen käsittelyssä. (Valtiovarainministeriö 2016, 29.)

Henkilötietojen käsittelyä koskevassa sopimussuhteessa on huomioitava tietosuoja-asetuksen (EU 679/2016) 28 artiklan velvoitteet joko varsinaisessa sopimuksessa tai erillisenä tietosuojaliitteenä (DPA, data processing agreement). Tietosuojaliite voi olla organisaation oma, palveluntarjoajan, yleisten sopimusehtojen, esimerkiksi IT2018 – ehtojen Erityisehdot henkilötietojen käsittelystä tai Kuntaliiton Henkilötietojen käsittelyn ehdot – mallisopimus. (Lång 2019, Andreasson ym. 2019, 150.) Tietosuojariskien pienentämiseen liittyvät lisäksi sopimuksissa kuvatavat osapuolten tietosuojaan ja tietoturvan liittyvät velvollisuudet ja vastuut, johon voidaan käyttää erillistä turvallisuusliitettä. Turvallisuusliite on osa rekisterinpitäjälle ja henkilötietojen käsittelijälle kuuluvaa tietosuoja suunnitteluvelvoitetta (privacy by design). Sopimuskokonaisuuteen voidaan myös liittää erillinen ja nimenomaisesti sopimukseen liittyvien tietojen ja tietojärjestelmien käyttöä koskeva käyttö- ja salassapitositoumus. Sopimukseen kuuluvat liitteet hyväksyy ja allekirjoittaa pääsopimuksen allekirjoittaja, tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksen hyväksyy ja allekirjoittaa jokainen tietoja käsittelevä. (Andreasson ym. 2015, 114–116.)

Monikansallisten yritysten sisäisessä henkilötietojen käsittelyssä tulee huomioitavaksi tietosuoja-asetuksen (EU 679/2016) 47 artiklan yritystä sitovat säännöt (BCR, Binding Corporate Rules) joka on tietosuojakäytäntönä vanhempi kuin tietosuoja-asetus. Tietosuojavaltuutetun toimiston mukaan yritystä sitovilla säännöillä EU:n alueelle sijoittunut monikansallinen yritys luo itse säännöt henkilötietojen siirtämiseksi ja siirtojen suojaamiseksi EU:n ulkopuolelle konsernin sisällä. Toimivaltainen tietosuojaviranomainen vahvistaa yritystä sitovat säännöt, jonka jälkeen ne ovat oikeudellisesti sitovia niin yritysryhmään kuuluvia yrityksiä kuin näiden henkilöstöä kohtaan. Tietosuojaviranomaisen hyväksymien yritystä sitovien sääntöjen luetteloa ylläpidetään Euroopan tietosuojaneuvoston (EDPB) verkkosivuilla (https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en).

5.3 Hallintatoimien riittävyyden riskianalyysi

Hallintatoimien riittävyyden riskianalyysivaiheessa selvitetään, onko henkilötietojen käsittely turvattu riittävällä tavalla ja onko tulevia tietojärjestelmähankkeita arvioitu (Valtiovarainministeriö 2016, 32).

Kun henkilötietojen käyttötarkoitukset, henkilötietoja käsittelevät sovellukset ja järjestelmät sekä henkilötietojen siirtotilanteet ovat selvillä, on seuraava vaihe henkilötietojen käsittelyä koskeva riskianalyysi, tarvittavien hallintatoimenpiteiden tunnistamiseksi ja mitoittamiseksi. Organisaation johdon tai sen määrittelemien rekisterinpitäjän tai rekisterinpitäjien tulee arvioida, onko tietoturvan toteutus riittävällä tasolla koko henkilötietojen käsittelyn elinkaaren ajan. Riskiarvioon tulee sisällyttää myös meneillään olevien tietojärjestelmähankkeiden uudelleen arviointi. (Valtiovarainministeriö 2016, 32.)

Riskienhallinta on osa johtamisen ja toiminnan prosesseja sekä suunnittelua ja seurantaa, jonka tavoitteena on tuottaa organisaation johdolle johtamista ja päätöksentekoa varten ajantasainen, oikea ja riittävän kattava käsitys riskeistä sekä selkeästi määritellyt riskienhallinnan vastuut ja seurantajärjestelmä. Johtamisen ohella riskienhallinta koskettaa organisaation jokaista työntekijää. (Valtionvarainministeriö 2017, 12.) Riskienhallintaan velvoittavaa lainsäädäntöä on kuvattu Valtionvarainministeriön Vahti – ohjeistoon kuuluvassa ohjeessa Riskienhallinnasta (22/2017). Keskeisiä ja jokaista organisaatiota velvoittavia lakeja ovat EU:n yleinen tietosuoja-asetus (EU 679/2016) ja työturvallisuuslaki (738/2002). Edellä mainittujen lisäksi erityisesti julkisen hallinnon organisaatioiden riskienhallintaan velvoittavaa lainsäädäntöä ovat esimerkiksi kuntalaki (410/2015), laki julkisen hallinnon tiedonhallinnasta (906/2019), laki viranomaisten toiminnan julkisuudesta (621/1999), valmiuslaki (1552/2011). (Rousku 2017, Liite2, 2–3.)

Yksi EU:n yleinen tietosuoja-asetuksen (EU 679/2016) periaatteista on riskilähtöisyys ja asetus velvoittaakin sen johdannon 76 kohdan sekä 35 artiklan mukaan rekisterinpitäjää arvioimaan henkilötietojen käsittelyn riskejä sekä riskien vaikutuksia rekisteröidyn kannalta. Henkilötietojen käsittelyn turvaamiseen kuuluvat olennaisena osana tietosuoja – asetuksen 25 ja 32 artiklojen nojalla toteutettavat tekniset ja organisatoriset toimet, joista johdon on päätettävä. Asetuksen 25 artikla koskee sisäänrakennettua ja oletusarvoista tietosuojaa (privacy by design, privacy by default), joka tarkoittaa, että tietojärjestelmien suunnittelussa ja henkilötietojen käsittelytoimissa huomioidaan tietosuoja alusta alkaen. Asetuksen 32 artikla koskee henkilötietojen käsittelyn turvallisuutta, joka tarkoittaa tietoturvan osa-alueista: luottamuksellisuus, eheys, saatavuus, todennus, vastuullisuus ja kiistämättömyys, huolehtimista. Korpisaari ym. (2018, 272) mukaan organisatorisia toimia ovat johdon määrittelemät ja kuvaamat hallinnolliset toimenpiteet organisaation toimintalinjauksista, periaatteista, organisaatiojärjestelyistä, henkilöstön tehtävien määrittelyistä, tietosuojan ja henkilötietojen käsittelyn ohjeistuksesta, koulutuksesta sekä valvonnasta.

5.4 Organisaation tietosuojavastuut

Organisaation tietosuojavastuut - vaiheessa tunnistetaan henkilötietojen omistajuus ja niiden käsittelystä vastaavat ja käsittelyä suorittavat yksiköt. Lisäksi johdon tulee arvioida, onko organisaatio velvollinen nimeämään tietosuojavastaavan, mikäli sellaista ei ole nimetty. (Valtiovarainministeriö 2016, 33.)

Tietosuojavelvoitteiden toteuttamiseksi tarvittavat käytännön toimenpiteet määräytyvät esimerkiksi organisaation toimialan, koon, toiminnan ja henkilötietojen käsittelyn luonteen, käsiteltävien henkilötietojen arkaluonteisuuden, käsittelyn asiayhteyden ja tarkoitusten, orga-

nisaatiorakenteen ja yritysmuodon perusteella (Andreasson ym. 2019, 22.) Tietosuojavastuiden hoitamiseksi lakisääteisellä tasolla on ensimmäiseksi määriteltävä kokonaisvastuu tietosuojasta, sen johtamisesta ja koordinoinnista, sekä huolehdittava organisaation sisäisestä järjestäytymisestä tietosuojatyön toteuttamiseksi. Edellä kuvatut organisaatioon ja sen toimintaan liittyvät ominaisuudet vaikuttavat siihen onko tietosuojan kokonaisvastuussa esimerkiksi yhden yksikön vastaava johtaja, tietohallintoyksikkö tai muu tietosuojaorganisaatio. Tietosuojan koordinoinnista vastaavan johdon tulee toimia organisaation ylimmän johdon mandaatilla päätöksenteko-oikeuksineen. (Andreasson ym. 2015, 83.)

Koska henkilötietojen omistajuus ja käsittely on yleensä hajautunut useaan organisaation yksikköön, tulee tietosuojan koordinoinnista vastaavan johdon tunnistaa henkilötietojen käsittelyä suorittavat yksiköt sekä käsittelyyn liittyvät ja tietosuojan toteutumisen kannalta olennaiset yksiköt ja valita näistä ne roolit, jotka liittyvät organisaation tietosuojan kokonaisvastuun toteuttamiseen. Nämä roolit voivat olla osa organisaation tietosuojaorganisaatiota. Johdon tulee määritellä tietosuojaorganisaation vastuu ja tehtävät, sekä tiedottaa organisaation henkilöstölle sekä tietosuojatoimintaan liittyville sidosryhmille tietosuojaorganisaation nimeämisestä, toiminnan aloittamisesta sekä sen toimivallasta. (Valtiovarainministeriö 2016, 33.)

Julkisen hallinnon organisaatioiden osalta tiedonhallintalain (906/2019) 4. pykälän 3 momentin luettelon 1 kohdan mukaan johdon tulisi huolehtia siitä, että tiedonhallintayksikössä olisi määritelty tiedonhallintalaissa tai muussa laissa säädettyjen tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut. Tällä tarkoitetaan konkreettisten vastuiden määrittämistä siitä, miten ja kenen vastuulla on, että tiedonhallintalain mukaiset velvoitteet ja palvelut toteutetaan. Vastuut olisi määritettävä tiedonhallintamallin ylläpidon ja tietoaineistojen muodostamisen toteuttamiselle, tietoturvallisuuden ja asianhallinnan järjestämiselle, tietojärjestelmien yhteentoimivuuden turvaamiselle sekä tietoaineistojen säilyttämisen järjestämiselle. Tiedonhallintayksikön johdon tulisi määrittää ja käytännössä määrätä työjärjestyksissä tai hallintosäännöissä, miten tiedonhallinnan vastuut ja niihin liittyvät tehtävät jakautuvat. Tiedonhallintalain esitöissä (HE 284/2018, 72–74) on määritelty tiedonhallintayksikön johdoksi esimerkiksi virastojen ja laitosten työjärjestyksissä sekä toimialojen hallintosäännöissä määritelty virastopäällikkö tai johtava toimielin, eli valtion virastoissa viraston tai laitoksen päällikkö, joka on tyypillisesti virkanimikkeeltään pääjohtaja tai ylijohtaja. Kunnan toimintaa, hallintoa ja taloutta taas johtaa kuntalain (410/2015) 38. Pykälän 2 momentin mukaan kunnanhallitus, joka myös johtaa tiedonhallintalain näkökulmasta tiedonhallintalaissa tarkoitettua tiedonhallintayksikköä, ellei vastuuta ole delegoitu kunnan hallintosäännössä jollekin muulle toimielimelle tai viranhaltijalle, esimerkiksi kunnan- tai kaupunginjohtajalle.

Tietosuoja-asetus (EU 679/2016) määrittelee 24 artiklassa henkilötietojen käsittelyä koskevan tosiasiallisen määräysvallan rekisterinpitäjälle, mutta ei ota kantaa siihen, millainen rekisterinpitäjän rooli tai asema organisaatiossa tulisi olla. Kuntaliitto (Haapalehto 2018, 3) on tietosuojavastaavan nimittämistä, tehtävää ja asemaa koskevassa yleiskirjeessä antanut esimerkkeinä tehtävänimikkeitä kuten kunnanjohtaja, hallintojohtaja, talousjohtaja, johtava asiantuntijalääkäri, henkilöstöjohtaja tai tietoteknisen osaston johtaja, sekä muut vastaavat ylemmät johtoasemat, joihin voidaan katsoa julkisen hallinnon osalta liittyvän vastuu määritellä henkilötietojen käsittelyn tarkoitukset ja keinot. Edellä kuvatut johtoasemat voidaan katsoa sellaisiksi tehtäviksi, joissa toimitaan tietosuoja-asetuksen (EU 679/2016) mukaisena rekisterinpitäjänä, ellei organisaation johto ole määritellyt rekisterinpitäjyyttä esimerkiksi lautakunnalle, hallitukselle, johtoryhmälle tai muulle vastaavalle päätöksentekoelimelle.

Andreasson ym. (2019, 88.) mukaan organisaation tietosuojasta kokonaisvastuussa olevan johdon, sen määrittelemien rekisterinpitäjien sekä organisaatioon mahdollisesti nimetyn tietosuojavastaavan tulee sopia, kuinka organisaatiossa toteutetaan käytännössä selosteet henkilötietojen käsittelystä, suunnitelma tietosuoja- ja tietoturvakoulutusten sisällöstä sekä koulutuksen järjestämisestä, ulkoiset ja sisäiset henkilötietojen käsittelyprosessien, ICT-järjestelmien ja käsittelyn ulkoistussopimusten auditoinnit, henkilötietojen käsittelyyn liittyvän tunnuslukumittariston luominen sekä käsittelyprosessien vertailu ja kehittäminen, käyttövaltuuksien läpikäyminen henkilörekisterien rekisterinpitäjien ja muiden vastuuhenkilöiden sekä tietojärjestelmien omistajien kanssa (tietohuolto), sekä tietosuojaviranomaisten ja muiden henkilötietojen käsittelyä ohjaavien virastojen määräysten ja tiedotteiden seuraaminen. Tehtäväkenttä on erittäin laaja ja edellyttää johdolta riittävien resurssien varaamista toteutusta varten.

Organisaation toimiessa Tietosuoja-asetuksen (EU 679/2016) 28 artiklan mukaisena henkilötietojen käsittelijänä tulee johdon varmistaa, että henkilöstö noudattaa henkilötietojen käsittelyssä tietosuojaa koskevan lainsäädännön lisäksi rekisterinpitäjän antamia kirjallisia käsittelyä koskevia ohjeita sekä käsittelyä koskevan sopimuksen ehtoja. Yleisin tilanne, jossa julkishallinto tai viranomainen on henkilötietojen käsittelijä, on Digi- ja väestötietoviranomaiselta julkisen palvelun tuottamiseksi saatu väestöaineisto. Väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) 4 pykälässä säädetään näiden henkilötietojen rekisterinpitäjyys Digi- ja väestötietovirastolle ja lain 4. luvussa niiden luovuttamisesta. Henkilötietoja sisältävän aineiston käyttö edellyttää käyttäjäorganisaatiolle myönnettävää tietolupaa sekä käyttäjäorganisaation sitoutumista tietoluvan ehtoihin.

Tietosuojavastaava

Organisaation johdon tulee arvioida toimintaan liittyvää henkilötietojen käsittelyn luonnetta ja määrää tehdäkseen päätöksen siitä, tuleeko organisaatiossa olla tietosuojavastaava. Tietosuoja-asetuksen (EU 679/2016) 37 artiklassa säädetään velvoitteesta nimetä tietosuojavastaava, kun rekisterinpitäjä tai henkilötietojen käsittelijä on muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtävää hoitava tuomioistuin. Suomessa sosiaali- ja terveydenhuollossa tietosuojavastaavan nimeäminen on ollut lakisääteistä vuodesta 2007 kun laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) tuli voimaan. Tietosuojavastaavan rooli ei siten ole kuntaorganisaatioissa uusi. Näissä johdon ratkaistavaksi on tullut tietosuoja-asetuksen (EU 679/2016) voimaantultua arvioida, onko yhdellä tietosuojavastaavalla riittävästi resursseja toimia koko organisaation tietosuojavastaavana. Mikäli tietosuojavastaavalla ei ole tosiasiallista mahdollisuutta ja riittäviä resursseja toimia, jää työpanos liian alhaiseksi, mistä seuraa organisaation tietosuojan huono tila (Andreasson ym. 2019, 96).

Tietosuoja-asetuksen (EU 679/2016) 37 artiklassa määritellään tietosuojavastaavan ammattipätevyys suhteessa tietosuojalainsäädännön, kyseisen organisaation henkilötietojen käsittelyn käytänteiden sekä tietosuoja-asetuksen 39 artiklan tehtäviin. Ammattipätevyys ei siten ole sidottu mihinkään tiettyyn koulutukseen tai tutkintoon kuin organisaation johdon ja käsiteltävien henkilötietojen rekisterinpitäjän tai -pitäjien arvioon siitä, miten monimutkaista, riskialtista tai vaativaa käsittely on (Korpisaari ym. 2018, 356).

Tietosuoja-asetuksen (EU 679/2016) 39 artiklassa säädetään tietosuojavastaavan tehtävistä, joissa korostuu neuvonta tietosuojalainsäädännön mukaisista velvoitteista sekä tietosuojan vaikutusten arvioinnista sekä seuranta ja valvonta, jotka kohdistuvat tietosuojalainsäädännön noudattamiseen sekä vaikutustenarvioinnin toteutukseen. Vaikutustenarvioinnin tekeminen on säädetty tietosuoja-asetuksen 35 artiklassa rekisterinpitäjän velvollisuudeksi. Lisäksi tietosuojavastaava toimii valvontaviranomaisen yhteyspisteenä sekä tekee tämän kanssa yhteistyötä.

Tietosuojavastaavan asema

Tietosuoja-asetuksen (EU 679/2016) 38 artiklan 2. kohta säätää tietosuojavastaavan asemasta ja suhteesta rekisterinpitäjään tai henkilötietojen käsittelijään. Organisaation johdon sekä sen määrittelemien vastuuhenkilöiden (esimerkiksi rekisterinpitäjä) tulee tukea tietosuojavastaavaa antamalla tälle riittävät resurssit tehtävien täyttämiseksi, sekä pääsyn henkilötietoihin ja käsittelytoimiin. Organisaation johdon tulee arvioida mihin tietosuojavastaava sijoittuu organisaatiossa, jotta asemaan oleellisesti liittyvä riippumattomuus sekä tehtä-

vässä suoriutumiseen tarvittavat riittävät resurssit voidaan taata. Tietosuojavastaavan toimenkuvasta on suositeltavaa laatia kirjallinen tehtäväluettelo tai tehtäväkuvaus. Tämän luettelon tai kuvauksen avulla tietosuojavastaavalla on mahdollisuus määritellä ja aikatauluttaa tehtäviään sekä varata riittävästi aikaa jokapäiväiselle vaihtelevalle tietosuojatoiminnalle. (Valtiovarainministeriö 2016, 33.) Tietosuojavastaavalle määriteltyjen tehtävien toteutumista tulee seurata säännöllisesti esimerkiksi kuukausittaisella raportoinnilla johdolle sekä vuositasolla laatimalla tietotilinpäätöksen (Korpisaari ym. 2018, 369).

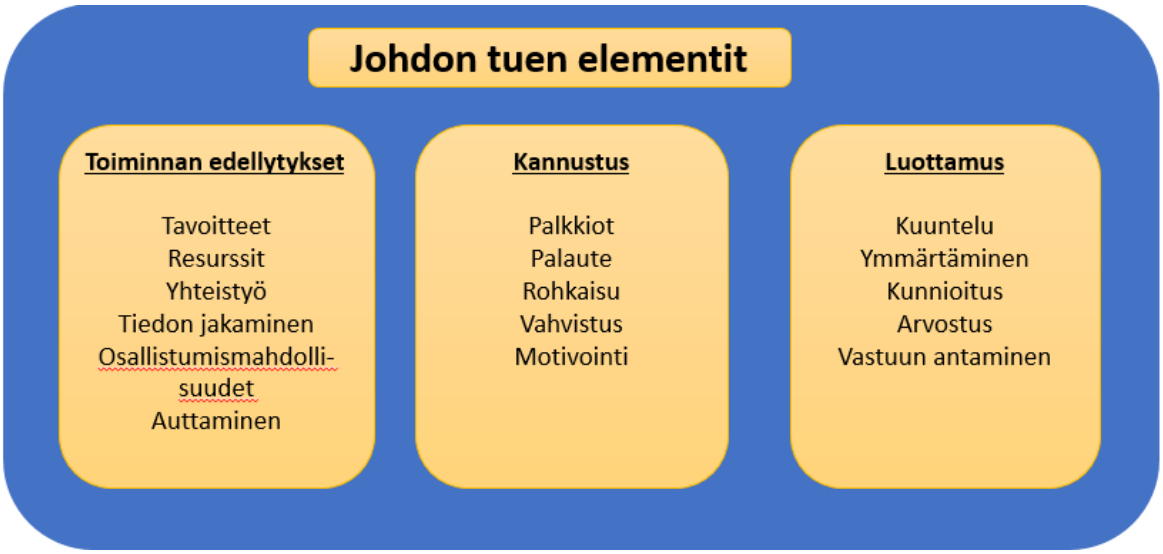
Tietosuoja-asetuksen (EU 679/2016) 38 artiklan 3. kohdassa velvoitetaan rekisterinpitäjää tai henkilötietojen käsittelijää varmistamaan, ettei tietosuojavastaava ota vastaan ohjeita näiden tehtävien hoitamisen yhteydessä. Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle. Tämä riippumattomuus tarkoittaa käytännössä, että tietosuojavastaavalle ei saa antaa ohjeita siitä, miten henkilötietojen käsittelyä koskeva valitus tai poikkeama tulisi tutkia tai onko asian käsittelyssä syytä ottaa yhteyttä tietosuoja- tai muuhun viranomaiseen (Korpisaari ym. 2018, 363). Voutilaisen (2019, 613) mukaan tilanteessa, jossa rekisterinpitäjä tai henkilötietojen käsittelijä tekee henkilötietojen käsittelyyn liittyviä päätöksiä, jotka eivät ole tietosuoja-asetuksen ja tietosuojavastaavan antamien neuvojen mukaisia, tietosuojavastaavalle on varattava mahdollisuus esittää ylimmälle johdolle rekisterinpitäjän tai henkilötietojen käsittelijän tekemään päätöstä koskeva eriävä mielipide.

Tietosuoja-asetuksessa (EU 679/2016) säädetään rekisterinpitäjälle ja henkilötietojen käsittelijälle useita erilaisia velvoitteita ja vastuita henkilötietojen käsittelystä, joten organisaation johdon ei tuli määritellä tietosuojavastaavalle sellaisia tehtäviä tai vastuita, jotka on tietosuoja-asetuksessa määritelty rekisterinpitäjälle tai henkilötietojen käsittelijälle. Tietosuojavastaavan tehtävä on asetuksen 39 artiklan mukaan valvoa henkilötietojen käsittelyä, sekä antaa ohjeistusta ja neuvontaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille, ei toimia rekisterinpitäjän puolesta henkilötietojen käsittelyyn liittyvänä päätöksentekijänä.

Kuntaliitto on tietosuojavastaavan nimittämistä, tehtävää ja asemaa koskevassa yleiskirjeessään (Haapalehto 2018, 3) ohjeistanut tietosuojavastaavan nimittämisen osalta, että tietosuojavastaavan ei tulisi olla sellaisessa johtavassa asemassa, jossa määritellään tietojenkäsittelyn tarkoitukset ja keinot. Tällainen asema aiheuttaa eturistiriidan tietosuoja-asetuksessa (EU 679/2016) rekisterinpitäjälle säädettyjen henkilötietojen käsittelyä koskevien velvoitteiden ja tietosuojavastaavalle säädettyjen käsittelyn ohjaus ja valvonta velvoitteiden välille. Lakisääteisesti neuvontaa ja ohjausta sekä valvontaa ja suoraan johdolle annettavaa raportointia tekevä ei voi näin ollen tehdä henkilötietojen käsittelyyn liittyviä päätöksiä.

Johdon tuki tietosuojavastaavalle

Andreasson ym. (2019, 109) mukaan organisaation johdon sitoutuminen tietosuojatyöhön takaamalla riittävät resurssit ja toimintamahdollisuudet sekä yhteistyö tietosuojavastaavan kanssa ovat edellytys tietosuojatyön onnistumiselle. Tietosuojavastaava tarvitsee johdon tukea tehtävän hoitamiseksi. Riikosen pro gradu – tutkielmassa (2013) tutkittiin johdon tukea terveydenhuollon organisaatioiden tietosuojavastaaville. Tutkimuksen mukaan tietosuojavastaavat pääasiallisesti kokivat saavansa tukea, mutta eriäviä mielipiteitä ilmeni huomionarvoinen määrä. Kaikki tietosuojavastaavat eivät saaneet samanlaisia toiminnan edellytyksiä tai toimintamahdollisuuksia. Kuviossa 9 on kuvattu johdon tuen elementit, joita ovat toiminnan edellytykset, kannustus ja luottamus, joiden sisältö on kuvattu seuraavassa kuvassa.



Kuvio 9. Johdon tuen elementit Andreasson ym. (2019, 109) mukaan.

Tietosuojavastaavan on tärkeää huolehtia omasta jaksamisestaan ja osaamisestaan esimiehen tuella. Tietosuojan vaatimukset muuttuvat ja laajenevat jatkuvasti, jolloin tehtävän laadukas hoitaminen edellyttää organisaation johdolta ja tietosuojavastaavan esimieheltä resurssien riittävyyden ja säännöllisen täydennyskoulutuksen mahdollistamista. Tietosuojavastaavilla on myös erilaisia yhteistyöverkostoja, joissa on tarjolla vertaistukea ja kokemusta, tosin verkostot saattavat myös työllistää tietosuojavastaavaa entistä enemmän. (Andreasson ym. 2019, 201–203.)

5.5 Johdon raportointi

Johdon raportointi- osiossa määritellään organisaation tietosuojavastuiden mukainen raportointi johdolle. Organisaation johdon nimittämälle tietosuojavastaavalle tai muulle tietosuojaorganisaatiolle tulee määritellä tehtäväksi säännöllinen raportointi johdolle, sekä vuosiraportin laatiminen. (Valtiovarainministeriö 2016, 33.)

Organisaation vaatimuksenmukaisuus toimintaan kuuluu, että johto määrittelee miten ja minne tieto väärinkäytöksistä, toimintaperiaatteiden vastaisesta toiminnasta tai näiden epäilystä tulee ilmoittaa sekä miten ja kenen toimesta näitä ilmoituksia käsitellään ja mikä on johdon rooli käsittelyssä. (Ratsula 2016, 207.) Johdon tietoisuus organisaation tietosuojan nykytilasta on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Säännöllisen raportoinnin tulee sisältää tärkeimmät tietosuojaan ja henkilötietojen käsittelyyn liittyvät asiat. Niitä voivat olla esimerkiksi tietosuojamittarit, jotka sisältävät niiden käytön raportointikauden aikana, tietosuojan kehityshankkeet ja niiden tilanne, havaitut puutteet ja tarpeet, merkittävimmät tietosuojavaikutuksia aiheuttaneet tietoturvaloukkaukset, tehdyt riski- ja vaikutustenarvioinnit sekä niiden merkittävimmät löydökset hallintakeinoineen sekä rekisteröityjen oikeuksiin ja yhteistyöhön valvontaviranomaisen kanssa liittyvät tarpeelliset tiedot. (Valtiovarainministeriö 2016, 33.)

Organisaation johdon vuosiraportti voi olla esimerkiksi niin sanottu tietotilinpäätös. Tietosuojavaltuutetun toimisto on vuonna 2012 kehittänyt mallin (Tietosuojavaltuutetun toimisto 2012, 3) dokumentista, joka voi täydentää organisaation lakisääteistä tilinpäätös ja toimintakertomus raportointia. Tietotilinpäätöksen tarkoituksena on toimia dynaamisena työkaluna, joka tukee organisaation tehokkuutta, vaikuttavuutta ja kilpailukykyä ja sen sisältö voi vaihdella organisaation toimialasta ja toiminnan laadusta riippuen. Tietotilinpäätöksen tarkoituksena ei ole tarpeettomasti lisätä organisaation hallinnollista taakkaa vaan antaa väline, jonka avulla johto valvoo ja arvioi organisaation tietosuojan nykytilaa, sekä ohjaa toimenpiteitä ja resursseja sen kehittämiseen. Johto voi osoittaa vuosiraportoinnin tietosuojavastaavan tai muun, esimerkiksi organisaation tietosuojaryhmän jäsenen vastuulle. (Valtiovarainministeriö 2016, 33.)

Tietosuoja-asetuksen (EU 679/2016) 38 artiklan 3. kohdassa määritellään tietosuojavastaavalle oikeus raportoida organisaation tietosuojan tilasta suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle, jolloin esimerkiksi organisaation hallituksella on tieto neuvoista ja näkemyksistä, joita tietosuojavastaava on antanut organisaation henkilötietojen käsittelyyn ja tietosuojaan liittyen. Tietosuojavastaava voi lisäksi antaa yhteenvetoja tai raportteja toiminnastaan kvartaaleittain, puolivuosittain tai kerran vuodessa tietotilinpää-

töksen yhteydessä. Tietosuojavastaavan nimittämisestä huolimatta kokonaisvastuu henkilötietojen käsittelyn lainmukaisuudesta on aina rekisterinpitäjällä tai henkilötietojen käsittelijällä. (Korpisaari ym. 2018, 363.)

5.6 Koulutukset ja ohjeet

Koulutukset ja ohjeet - osion tarkoituksena on varmistaa, että koko henkilöstölle on tarjolla asianmukaista ja rooliperustaista tietosuoja- ja tietoturvakoulutusta. Koulutuksen tulisi sisältää lopputentti ja sen vaikuttavuutta tulisi arvioida säännöllisesti esihenkilöille suunnatuilla kyselyillä. (Valtiovarainministeriö 2016, 33.)

Organisaation johdon tulee huolehtia henkilöstön riittävästä tietosuoja- ja tietoturvaosaamisesta erityisesti niissä rooleissa, joissa käsitellään henkilötietoja tai osallistutaan rekisteröidyn oikeuksien toteuttamiseen luotuihin prosesseihin esimerkiksi tarkastusoikeuden osalta. Johdon tulee myös arvioida, onko tarpeen järjestää syventävää, rooliperusteista tietosuojakoulutusta esimerkiksi asiakaspalvelussa, kehitystyössä ja palveluntuotannossa toimivalle henkilöstölle. Tietosuojakoulutuksen sisällön tulee vastata ajantasaista tietosuojasääntelyä. (Valtiovarainministeriö 2016, 33.)

Organisaation henkilötietoja käsittelevissä rooleissa toimivien henkilöiden ohjeistuksesta vastaa tietosuoja-asetuksen (EU 679/2016) 29 artiklan mukaan rekisterinpitäjä tai henkilötietojen käsittelijä. Henkilötietojen käsittelyä koskevassa ohjeistuksessa on kuvattava, millainen henkilötietojen käsittely kuuluu roolin tehtävänkuvaan ja ohjeistuksen tulee olla henkilöstölle vapaasti saatavilla (Valtiovarainministeriö 2016, 27).

Tiedonhallintalain (906/2019) 4. pykälän 3 momentin luettelon 2 kohdan mukaan johdon tulisi huolehtia tiedonhallintayksikön ajantasaisista ohjeista tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta käytännössä, tiedonsaantioikeuksien toteuttamisesta ja niiden toteuttamisessa noudatettavista menettelytavoista ja vastuista, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta. Lisäksi olisi oltava ohjeistus tietojärjestelmien käytöstä, jotta tietojärjestelmien käyttäjät tietävät miten tietojärjestelmiä käsitellään tietoturvallisella tavalla lainmukaisiin käyttötarkoituksiin. Myös tietojenkäsittelyoikeuksien, sekä käyttöoikeuksien määrittely ja niitä myöntävä tulisi olla määritelty ja ohjeistettu henkilöstölle. Ennen tiedonhallintalakia on julkisuuslain 18 pykälän 1 momentin 5 kohdassa säädetty viranomaisen velvollisuudesta huolehtia siitä, että sen palveluksessa olevilla on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä, tietoturvallisuusjärjestelyistä ja tehtävänjaosta. Valtionhallinnon

osalta viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta annetussa asetuksessa (1030/1999) on 4 pykälässä säädetty ohjeiden laatimisvelvollisuus.

Jokaisella työntekijällä on työturvallisuuslain (738/2002) 14 pykälän mukaan oikeus saada riittävä perehdytys. Henkilötietojen käsittelyyn liittyvissä työtehtävissä tulee saada ohjeistus ja perehdytys vähintään salassapitoon liittyvistä asioista, mutta myös tietoturvasta ja tietosuojasta. (Andreasson ym. 2015, 94.)

5.7 Dokumentaatio ja viestintä

Dokumentaatio ja viestintä - osion toteutuksessa varmistetaan, että henkilötietojen käsittelyyn on olemassa ajantasainen ohjeistus, rekisteröityjä informoidaan käsittelystä selkeästi ja kattavasti ja organisaatiolla on olemassa kriisiviestintäsuunnitelma (Valtiovarainministeriö 2016, 34).

Vaatimuksenmukaisuuden näkökulmasta organisaation johdon on tunnistettava ne toiminnan kannalta merkityksellisimmät osa-alueet, joille on välttämätöntä laatia säännöt ja ohjeet. Näitä ovat esimerkiksi hankintatoimea, tietoturvaa ja tietosuojaa koskevat ohjeet. (Ratsula 2016, 190.) Organisaation johdon tehtävänä on määritellä tietosuojapolitiikka tai muu vastaava organisaation tietosuojaa ohjaava ylin dokumentti, jossa kuvataan organisaation henkilötietojen käsittelyn vastuut ja periaatteet sekä tietosuojan merkitys organisaatiolle. Organisaation eri henkilötietojen käsittelykokonaisuuksia koskeva rekisterinpitäjyyden määrittelytapa, eli mikä organisaation elin tai rooli toimii rekisterinpitäjänä sekä mitkä roolit tai vastuulliset voivat toimia rekisterinpitäjän edustajana, tulee myös kirjata johdon toimesta organisaation hallintosäätöön, sitä vastaavaan dokumenttiin tai tietosuojapolitiikkaan. (Valtiovarainministeriö 2016, 27.) Tietosuoja-asetuksen (EU 679/2016) 5 artiklan 2 kohdassa on säädetty rekisterinpitäjälle osoitusvelvollisuus, jonka mukaan rekisterinpitäjän tulee pystyä jatkuvasti osoittamaan, että se noudattaa tietosuoja-asetusta ja sen periaatteita. Osoitusvelvollisuuteen kuuluvat seuraavat tietosuoja-asetuksessa määritellyt toimenpiteet ja niistä syntyvä dokumentaatio: seloste käsittelytoimista (30 artikla), käsitte4lyn riskienarviointi (5 artikla), tietosuojan vaikutustenarviointi (35 artikla), tietosuojavastaavan nimittäminen (37 artikla), oikeutettuun etuun perustuva henkilötietojen käsittely (6 artikla), suostumukseen perustuva henkilötietojen käsittely (7 artikla), henkilötietojen tietoturvaloukkauksesta ilmoittaminen (33 ja 34 artiklat). (Andreasson ym. 2019, 189.)

Organisaation johdon määrittelemän rekisterinpitäjän tai rekisterinpitäjien tulee tietosuoja-asetuksen 12 artiklan mukaisesti informoida rekisteröidyille henkilötietojen käsittelystä. Artiklan mukainen informointivelvollisuus sekä informoinnin sisältö ja muoto ovat eri asia kuin

aikaisemmassa henkilötietolaissa (523/1999) kuvattu rekisterikohtainen henkilörekisteriseloste. Informointi koskee aikaisempaa laajempaa henkilötietojen käsittelyn kokonaisuutta sekä tietoa siitä, mistä lähteestä rekisteröityä koskeva tieto on kerätty. Tietosuoja-asetuksessa (EU 679/2016) ei myöskään säädetä missä muodossa tai millä tavalla informointi on annettava, kunhan tieto on helposti ja ymmärrettävästi rekisteröidyn saatavilla. Tämä mahdollistaa organisaation viestinnästä vastaavalle johdolle ja rekisterinpitäjälle määritellä informoinnin keinot rekisteröityjen kohderyhmälle sopivimmalla tavalla. (Korpisaari ym. 2018, 175.)

Valtionvarainministeriön (2017b, 13) tietoturvapoikkeamatilanteiden hallintaa koskevan ohjeen mukaan julkisen hallinnon organisaatiolla tulee olla johdon määrittelemät toimintavaltuudet ja tietoturvapoikkeamien käsittelyyn käytettävät resurssit (tietoturvapoikkeamien hallintaprosessi / hallintamalli), sekä viestintäsuunnitelma, jossa linjataan sekä sisäinen että ulkoinen viestintä huomioiden kuka viestii, miksi, kenelle, mitä, miten ja milloin. Käytettävät viestintäkanavat määritellään poikkeaman laajuuden, sen aiheuttamien vaikutusten, viestintätapojen käytettävyyden sekä viestinnän kohderyhmän perusteella. Valtiovarainministeriön (2017b) ohjeen mukaan Viestintäsuunnitelmassa on huomioitava myös julkiseen tiedottamiseen ja viestintään käytettävät kanavat kuten sosiaalinen media, TV, radio sekä muut vastaavat mediat, sekä henkilötietoihin kohdistuvasta tietoturvaloukkauksesta viestiminen valvontaviranomaiselle ja rekisteröidyille. Tietosuoja-asetuksen (EU 679/2016) 4. artiklan 12 kohdan mukaan henkilötietojen tietoturvaloukkauksella tarkoitetaan:

> *tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.*

Organisaatioilla on ollut käytäntöjä, joissa pyydetään toisen organisaation luomaa ohjeistusta tai dokumentaatiomalleja oman organisaation käyttöön. Tämä muodostaa riskin sille, että johdolle annetaan vääränlaista informaatiota organisaation kyvykkyydestä ja kypsyystasosta. Toisen organisaation materiaalia käytettäessä tulee arvioida molempien organisaatiokulttuuri, toimialojen yhteneväisyys ja johtamismalli, sekä se sopiiko materiaali sellaisenaan käytettäväksi, sitoutuuko organisaation ylin johto määriteltyihin toimenpiteisiin tai onko niihin yhtäläiset resurssit ja osaamistaso, kannustaako toiselta organisaatiolta suoraan kopioitu materiaali kehittämään oman organisaation osaamista ja kypsyystasoa vai jääkö materiaali ja ohjeistus viitteelliseksi ja “kyllä meillä tämä on” tasolle. (Andreasson ym. 2019, 201–202.) Julkisen hallinnon organisaatioille on tarjolla Digi- ja väestötietoviraston

Vahti - ohjeita sekä Valtionvarainministeriön tiedonhallintolautakunnan ohjeita, lisäksi tietosuojavaltuutetulla on kaikille rekisterinpitäjille ja henkilötietojen käsittelijöille sopivia ohjeita ja malleja.

Rekisterinpitäjän tulee ilmoittaa henkilötietojen tietoturvaloukkauksesta tietosuoja- asetuksen (EU 679/2016) 33 artiklan mukaisesti valvontaviranomaiselle ja 34 artiklan mukaisesti rekisteröidylle. Ilmoitusten tulee sisältää vähintään seuraavat tiedot: kuvattava henkilötietojen tietoturvaloukkausten luonne ja todennäköiset seuraukset, kuvattava toimenpiteet, joihin rekisterinpitäjä on ryhtynyt / tulee ryhtymään tietoturvaloukkauksen takia, ja tarvittaessa myös toimenpiteet haittavaikutusten lieventämiseksi sekä ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoja. Lisäksi valvontaviranomaiselle on kerrottava loukkauksen kohteena olleiden rekisteröityjen ryhmät ja henkilötietotyypit sekä arvioidut lukumäärät. Rekisterinpitäjän tulee huolehtia siitä, että kaikki henkilötietojen käsittelyyn liittyvät tietosuoja-asetuksessa (EU 679/2016) määritellyt dokumentit ovat olemassa, ajantasaisia ja asianmukaisesti saatavilla. (Valtiovarainministeriö 2016, 34.)

5.8 Vaatimusten huomioiminen järjestelmähankkeissa ja –hankinnoissa, sekä järjestelmä- ja sovelluskehityksessä

Järjestelmähankkeiden ja –hankintojen, sekä järjestelmä- ja sovelluskehityksen -osiossa varmistetaan, että henkilötietojenkäsittely on järjestetty siten, että tietosuoja - asetus, tietosuojaperiaatteet ja rekisteröidyn oikeudet huomioidaan kaikessa tietojenkäsittelyssä, sovelluskehityksessä, sekä uusien tietojärjestelmien hankinnoissa ja kilpailutuksissa (Valtiovarainministeriö 2016, 34).

Digitalisaation johdosta henkilötietoja hyödynnetään entistä kattavammin, koska tieto / data on uusien digitalisoitujen palveluiden polttoainetta, jota käytetään uusilla tavoilla tuotettuihin palveluihin (ns. virtualisoidut, jaetut kapasiteetti- ja pilvipalvelut), uusien päätelaitteiden ja käyttötapojen hyödyntämiseen (puhe- ja katseohjaus, virtuaali- ja lisätty todellisuus) sekä uudella tavalla hyödynnettyihin palveluihin (massadata, omadata, avoin data). Palvelupohjainen asiakaskokemukseen painottuva digitaalinen aikakausi asettaa vaatimuksia myös henkilötietojen käsittelylle. (Valtiovarainministeriö 2016, 5.)

Tietosuoja – asetus (EU 679/2016) edellyttää, että rekisterinpitäjä järjestää henkilötietojen käsittelyn tavalla, jossa asetus, tietosuojaperiaatteet ja rekisteröidyn oikeudet tulevat tehokkaasti huomioiduiksi kaikessa tietojenkäsittelyssä. Asetuksen vaatimukset tulee huomioida varsinaisen henkilötietojen käsittelyn lisäksi myös organisaation omassa tai sen hankkimassa sovelluskehityksessä, tietojärjestelmähankkeissa ja näiden kilpailutuksissa. (Valtiovarainministeriö 2016, 34.)

Julkisen hallinnon osalta tiedonhallintalain (906/2019) 5. pykälässä edellytetään tiedonhallintayksikköä arvioimaan tiedonhallintamallin sisältöön vaikuttavien olennaisten uudistusten ja tietojärjestelmien käyttöönoton vaikutuksia suunnitteluvaiheesta alkaen. Arvioinnissa tulee huomioida uudistuksen tai järjestelmän käyttöönoton vaikutus muun muassa suhteessa tiedonhallinnan vastuisiin, tietoturvallisuusvaatimuksiin ja -toimenpiteisiin, asiakirjojen julkisuuteen, salassapitoon, suojaan ja tiedonsaantioikeuksiin.

Organisaation johdon tulee arvioida mitä tietosuojalainsäädännön toteuttaminen edellyttää organisaation toimintaan liittyvässä sovelluskehityksessä. Organisaation johdon tulee varmistaa vaatimusten sisällyttäminen vaatimusmäärittelyihin uusien järjestelmähankkeiden tai muiden kilpailutusten yhteydessä käytettävissä tarjouspyynnöissä. (Valtiovarainministeriö 2016, 34.)

Ruotsalaisen (2019) mukaan tietosuoja ja tietoturvavaatimusten huomioiminen hankinnoissa määräytyy muun muassa järjestelmän käyttötarkoituksen, käsiteltävän henkilötiedon arkaluonteisuuden sekä tiedon suojaustason perusteella. Varsinkin tietoturvaominaisuudet kuten esimerkiksi toimivuus, käytettävyys ja tietojen saatavuus, ovat oleellinen osa järjestelmää ja hankinnan vaatimusmäärittelyä (Andreasson ym. 2019, 145).

Tietosuoja-asetuksen (EU 679/2016) vaatimukset tulee liittää osaksi organisaation projektinhallintamallia siten, että organisaatioon johdon määrittelemä rekisterinpitäjä tai häntä edustava sekä tietosuojavastaava otetaan riittävän aikaisessa vaiheessa mukaan projektin määrittelyyn. Kun uusia järjestelmiä, sovelluksia tai palveluja otetaan projektitoiminnan kautta käyttöön, tulee rekisterinpitäjän varmistaa tietosuojadokumentaation päivittäminen tai luominen ennen käyttöönottoa ja henkilötietojen käsittelyn aloittamista tietosuojan toteutumisen varmistamiseksi. (Valtiovarainministeriö 2016, 23)

Organisaatiolla tulee olla henkilötietojen käsittelyyn käytettävien järjestelmien- ja sovellusten kehitysprosesseissa työvaiheet, joissa rekisterinpitäjän toimesta analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Tietosuojavaatimukset määritellään käsiteltävien henkilötietojen käyttötarkoituksen perusteella sovellettavien lakien, tietosuoja-asetuksen, tietosuojalain sekä toimintaa koskevan erityislainsäädännön perusteella. Erityislainsäädäntöä ovat esimerkiksi sosiaali- ja terveydenhuoltoa, työntekijän työsuhteeseen liittyviä henkilötietoja ja teleoperaattoriliiketoimintaan liittyvien tietojen käsittelyä koskeva lainsäädäntö. (Valtiovarainministeriö 2016, 22)

Järjestelmien ja sovellusten teknisen kehittämisen toteutus tulee suunnitella vastaamaan henkilötietojen käsittelyn riskitasoa. Tämä edellyttää henkilötietojen käsittelyn riskien ja vaikutustenarvioinnin toteuttamista osana kehittämistä sekä kulloinkin voimassa olevien par-

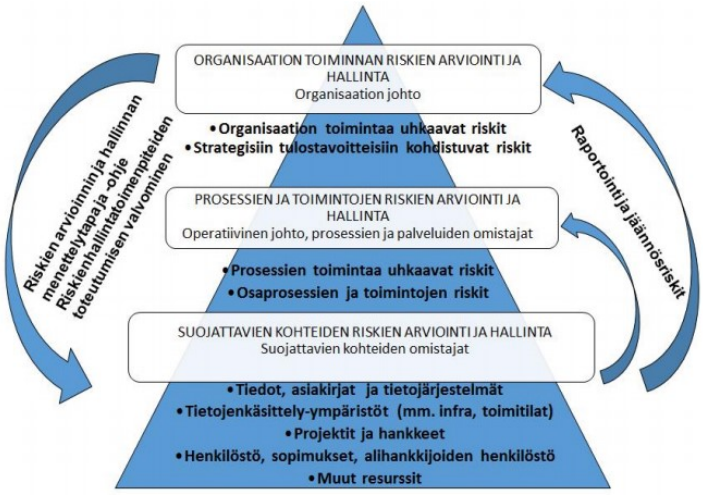
haiden tietoturvan hallintakeinojen valintaa riskien hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Käytettävät hallintakeinot tulee määritellä järjestelmän tai sovelluksen arkkitehtuuriin mahdollisimman aikaisessa vaiheessa, koska niillä voi olla vaikutusta järjestelmän toimintoihin. Esimerkiksi tietojen anonymisointi voi vaikuttaa järjestelmän toimintoihin, koska kaikki järjestelmässä käsiteltävä tieto ei ole käytettävissä alkuperäisessä muodossa. Hallintakeinojen osalta tulee myös suunnitella mahdollisten tulevien hallintakeinojen muutosten toteutettavuus. Väärin suunniteltua järjestelmää tai sovellusta voi olla hankalaa tai jopa mahdotonta muuttaa jälkikäteen.

Järjestelmien ja sovelluksen kehityksen aikana sekä kehitystyön päättyessä on tärkeää varmistaa, että toteutus vastaa suunniteltua, vaaditut tietoturvakontrollit on toteutettu oikein ja ne vastaavat voimassa olevia uusimpia suosituksia ja ovat tarvittaessa päivitettävissä. Tietoturvakontrolleissa olevia puutteita tai virheellistä toimintaa ei välttämättä havaita järjestelmän tai sovelluksen normaalissa käytössä, joten käyttöönottotestaus edellyttääkin sellaisten testitapausten tunnistamista ja toteutusta, joissa käydään läpi erilaiset väärinkäyttötapaukset. Testauksella varmistetaan, että tietosuojaan liittyvät tarpeet on huomioitu ja toteutettu. (Valtiovarainministeriö 2016, 22–23.)

5.9 Riskienhallinnan kehittäminen

Riskienhallinnan kehittämisen osiossa varmistetaan, että organisaatiolla on olemassa menettely ja vastuuhenkilöt henkilötietojen käsittelyn vaikutustenarvioinnin suorittamiseen tietosuoja-asetuksessa määritellyllä tavalla. (Valtiovarainministeriö 2016, 35.)

Organisaation riskienhallinnan kokonaisuus sisältää useita erilaisia osa-alueita ja tasoja, joten johdon tehtävä onkin määritellä, kuinka riskienhallinta organisoidaan ja resursoidaan. Kuviossa 10 on Valtionvarainministeriön riskienhallinnan ohjeen Rousku (2017 Liite 4 16) näkemys organisaatiotasoittain määritellystä riskienhallinnasta, jossa ylin johto arvioi ja hallitsee organisaation toimintaan kohdistuvia riskejä, operatiivinen johto sekä prosessien ja palveluiden omistajat hallitsevat prosessien ja toimintojen riskejä ja suojattavien kohteiden omistajat hallitsevat näihin kohdistuvia riskejä. Suojattavia kohteita ovat muun muassa sopimukset, asiakirjat ja tiedot sekä niiden käsittelyyn käytettävät järjestelmät, organisaation infra ja toimitilat, henkilöstö sekä henkilötiedot.



Kuvio 10. Riskienhallinnan tasot esimerkinomaisesti Rousku (2017) mukaan.

Tietosuoja-asetuksen (EU 679/2016) lähtökohtana on riskilähtöisyys. Rekisterinpitäjä ja henkilötietojen käsittelijä ovat velvollisia arvioimaan henkilötietojen käsittelyyn liittyviä riskejä ja valitsemaan arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on syytä liittää osaksi organisaation riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Jos tietosuojavastaava on nimetty, hänen tulee tukea organisaation eri yksiköitä, jotta tietosuojariskejä tunnistettaisiin paremmin sekä olla mukana määrittelemässä tunnistetuille, hallintaan otettaville riskeille tarvittavia hallintakeinoja. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. (Valtiovarainministeriö 2016,21.)

Tietosuoja - asetus (EU 679/2016) määrittää 35 artiklassa tietosuojan vaikutustenarvioinnin pakolliseksi toimenpiteeksi sellaisille henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tuloksia tulee käyttää niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään riskitasoa, sekä samalla varmistumaan asetuksen vaatimusten toteutumisesta. Jos vaikutustenarvioinnin perusteella riskitaso on suuri, eikä rekisterinpitäjä pysty sitä pienentämään, on otettava yhteyttä valvontaviranomaiseen (ennakkokuuleminen). Vaikutustenarviointi kohdistetaan suunnitteluvaiheessa olevalle järjestelmälle, sovellukselle, palvelulle tai hankkeelle, jossa tullaan käsittelemään henkilötietoja. Arviointi tulee suorittaa mahdollisimman aikaisessa vaiheessa, jotta tarvittavat hallintakeinot saadaan mukaan kehitystyöhön. Valvontaviranomainen, eli tietosuojavaltuutetun toimisto (2018) on julkaissut luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen. Luetteloa ylläpidetään tietosuojavaltuutetun toimiston verkkosivuilla (https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista).

Vaikutustenarviointien tekeminen on suositeltavaa kaikille rekisterinpitäjille, jotta asetuksen vaatimustenmukaisuudesta voidaan varmistua. Arviointien tulokset on hyvä dokumentoida määrämuotoisesti, jotta niiden tulokset ovat vertailukelpoisia ja jotta määriteltyjen hallintakeinojen toteuttamista voidaan seurata. Dokumentaatio on tärkeä osa osoitusvelvollisuuden toteuttamista. Vaikutustenarviointi tehdään asetuksen (ja muun sovellettavan tietosuojasääntelyn) vaatimuksista johdettua kriteeristöä vasten. Vaikutustenarviointia tehtäessä tulee pystyä kuvaamaan henkilötietojen tietovuot ja käyttötarkoitukset, arvioimaan vaatimuksenmukaisuutta ja yksilöiden tietosuojaan liittyviä riskejä sekä muodostamaan hallintakeinoja havaittujen puutteiden ja riskien pienentämiseksi. (Valtiovarainministeriö 2016, 21.) Tietosuojavaltuutetun toimisto (2021b) on julkaissut luonnoksen tietosuojan vaikutustenarvioinnin ohjeesta ja Excel-työkalusta, näitä on hyvä käyttää vaikutustenarvioinnin tekemisen tukena.

Henkilötietojen käsittelyn vaikutustenarvioinnin lisäksi Lång (2019) mukaan ei tule unohtaa sopimusten merkitystä tietosuojariskien hallinnassa ja organisaation vaatimuksenmukaisuus toiminnasta huolehtimisessa. Organisaation johdon tulee tunnistaa sisäisen riskienhallinnan lisäksi rekisterinpitäjyyteen kuuluva tosiasiallinen vastuu ulkopuoliselle palveluntarjoajalle siirrettyjen toimintojen, toiselle organisaatiolle luovutettujen henkilötietojen tai muiden toimenpiteiden lainmukaisuudesta, joiden seurauksena henkilötietojen käsittely ei ole organisaation määrittelemän rekisterinpitäjän välittömässä valvonnassa. "*Vaikka välitön vastuu sopimuksiin liittyen olisi organisaatiossa määritelty jollekin toiselle, on erittäin tärkeää, että sopimussuhteiden tietosuojaulottuvuus tulee käytännössä huomioiduksi. EU:n yleisen tietosuoja-asetuksen myötä tämä on myös organisaation suoranainen velvollisuus."* (Andreasson ym. 2019, 149–150.)

Lautjärven (2018, 58) mukaan useampi kuin joka viides yritys on kokenut sisäisten, esimerkiksi tietoon tai uusiin tuotteisiin kohdistuneiden väärinkäytösten lisääntyneen ja jopa 50 prosentissa yrityksistä on havaittu tietorikoksia. Tämä osoittaa, että yritysten riskienhallintakeinot ovat puutteellisia ja kaipaavat uudistusta, henkilöstöä ei kouluteta tietoon liittyvien rikosten ehkäisemiseen eikä rekrytoinneissa arvioida tarvetta henkilön taustojen tarkastamiselle.

5.10 Tietoturvallisuudesta ja toiminnan jatkuvuudesta huolehtiminen

Tietoturvallisuutta ja toiminnan jatkuvuutta koskevassa osiossa organisaation tulee varmistaa sen kyky taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus, sekä fyysisen tai teknisen vian sattuessa kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin (Valtiovarainministeriö 2016, 35).

Tietoturvallisuuden avulla huolehditaan käsiteltävien tietojen, niiden taustalla toimivien tietojärjestelmien tai muiden suojattavien kohteiden (kuten henkilöstö, toimitilat) saatavuudesta ja eheydestä. Mikäli kyse on salassa pidettävästä tiedosta, on huolehdittava myös tiedon luottamuksellisuudesta ja organisaation toimintaympäristön tulee täyttää salassa pidettävän tiedon käsittelyltä edellytettävät vaatimukset tiedon, teknologian, toimitila- ja henkilöstöturvallisuuden osalta. (Väestörekisterikeskus 2019, 20.) Valtionvarainministeriön (2017b, 5) mukaan digitalisaation myötä tiedon ja palveluiden saatavuus ja eheys muodostuvat entistä merkittävämmäksi ja tiedon luottamuksellisuuden, eli salassapidon merkitys korostuu varsinkin tilanteissa, joissa asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa organisaatiolle (Väestörekisterikeskus 2019, 20). Tietoturvariskejä aiheutuu myös tietoteknisistä virheistä, väärin valituista lainsäädäntöön liittyvistä sopimusehdoista tai sopimussuhteen riskienarvioinnin puuttumisesta. Sopimuksiin liittyvät tietoturvariskit kohdistuvat erityisesti Suomen ulkopuolella tuotettaviin tai ylläpidettäviin palveluihin, joissa tiedon tai siihen pääsyn omaavan henkilöstön sijainti ei ole selvillä. (Lautjärvi 2018, 26.)

Paanasen (2019) mukaan tietoturvatyö voidaan jakaa esimerkiksi seuraaviin osa-alueisiin; palvelu- ja järjestelmätoimittajien tekemä tietoturvatyö, josta sovitaan henkilötietojen käsittelysopimuksissa, organisaation käyttämät tekniset suojausmenetelmät, joilla suojataan järjestelmiä, päätelaitteita ja näitä käyttävien toimintaa, organisaation yleiset tietoturvakäytännöt, joilla pyritään ohjaamaan henkilöstön toimintaa tietoturvan huomioivaan suuntaan (esimerkiksi. tietoturvapolitiikka, ohjeet ja koulutus). (Andreasson ym. 2019, 135.)

Jokaisen organisaation toiminnassa havaitaan jatkuvasti erilaisia teknisiä tietoturvatapahtumia, jotka kaikki tulee käsitellä organisaation sisäisellä menettelyllä ja ulkoistettujen palveluiden osalta sopimuksissa kuvattujen palveluhallintaprosessien mukaisesti palveluita tuottavassa organisaatiossa. Jokaisella organisaation henkilöstöön kuuluvalla, sekä palveluntuottajalla ja sen henkilöstöllä, tulee olla ohjeistus, kenelle havaituista tietoturvapoikkeamista ilmoitetaan. Johdon tulee määritellä ja nimetä tietoturvapoikkeamien käsittelyryhmä tai -toiminto, jonka tehtävänä on suunnitella tarvittavat toimenpiteet poikkeaman korjaamiseksi sekä toimia yhteistyössä ulkoisten ja sisäisten sidosryhmien kanssa. Käsittelyryhmän kokoonpano voi määräytyä tapauskohtaisesti poikkeaman perusteella, mutta ryhmään tulisi kuulua vakiohenkilöitä, jolloin erityyppisten poikkeamien mahdollinen yhteys toisiinsa havaitaan nopeasti. Jokaisella ryhmän jäsenellä tulee olla nimetty varahenkilö. Käsittelyryhmässä voi olla myös organisaation ulkopuolisia asiantuntijoita varsinkin toiminnoista, jotka on ulkoistettu palveluntarjoajille. Tietoturvapoikkeamien käsittelyryhmän tehtävänä on

varmistaa, että poikkeamiin reagoidaan ennalta tehtyjen suunnitelmien mukaisesti, selvitystyössä noudatetaan lakia ja kaikissa poikkeamien selvitystilanteissa mukana on riittävästi asiantuntemusta sekä asiaan liittyvät vastuuhenkilöt. (Valtiovarainministeriö 2017a, 17–18.)

Tietoturvapoikkeamienhallinta on prosessi, jonka tehtävänä on varmistaa organisaation kyvykkyys toimia tietoturvan vaarantavan haitallisen tilanteen selvittämiseksi ja hallitsemiseksi. Prosessi voidaan jakaa neljään vaiheeseen, joita ovat: tunnistaminen, selvittäminen, palauttaminen sekä jälkianalyysi. Prosessin kannalta on oleellista, että tietoturvasta vastaava johto on määritellyt organisaatiolle tavan ilmoittaa mahdollisista havaituista poikkeamista, jolloin prosessin ensimmäinen, eli poikkeaman tunnistamisvaihe voidaan aloittaa mahdollisimman aikaisessa vaiheessa. Tietoturvapoikkeamienhallinnan dokumentaation tulee sisältää vähintään seuraavat kuvaukset: tietoturvapoikkeamienhallinnan prosessin yleiskuvaus, vakavan häiriön määritelmä, tiedottamiskäytännöt sekä ajantasaiset yhteystiedot poikkeaman käsittelyn kannalta oleellisille tahoille. Johdon on syytä arvioida, onko tarpeen laatia vakaville häiriöille oma prosessi, jossa on huomioitu näiden selvittämiseen liittyvät vastuut. (Pirinen 2014, 5–6.) Poikkeamatilanteiden käsittelyä tulee harjoitella säännöllisesti, jolloin saadaan selville millaista osaamisen kehittämistä organisaation vastuuhenkilöille ja asiantuntijoille tarvitaan tietoturvapoikkeamien hallitsemiseksi. Johdon on myös huomioitava palvelutuottajien rooli ja kyvykkyys huolehtia näiden tuottamien palveluiden tietoturvallisuudesta. (Valtiovarainministeriö 2017a, 17, 31.)

Tietoturvapoikkeamista tulee raportoida organisaation johdolle, koska johdolla on organisaation tietoturvallisuuden varmistamisen lisäksi velvollisuus edistää tietoturvallisuuden kokonaiskehitystä sekä varmistaa tietoturvatyön riittävä resursointi. Tietoturvapoikkeamaraportti on toimitettava soveltuvilta osin myös toimintaan tai poikkeamaan liittyville sidosryhmille, tällä voidaan välttää vastaavien tilanteiden toistumista muissa organisaatioissa. Ilmoitusvelvollisuudesta on sovittu yleensä toiminta koskevassa turvallisuussopimuksessa. Tietoturvapoikkeamaraportti on myös arkistoitava myöhempää käyttöä varten. (Valtiovarainministeriö 2017a, 53)

Tietosuoja-asetus (EU 679/2016) velvoittaa 32 artiklassa rekisterinpitäjää toteuttamaan asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta henkilötietojen käsittely on turvattua. Henkilötiedot tulee suojata siirron, tallennuksen ja käsittelyn aikana oikeudetta tai vahingossa tapahtuvalta tuhoamiselta, muuttamiselta, luovuttamiselta tai pääsyltä. Johdon ja rekisterinpitäjien tulee tunnistaa organisaation toimintaan, tietojenkäsittelyyn ja suojattaviin tietoihin kohdistuvat tietoturvallisuuteen liittyvät vaatimukset, sekä toteuttaa organisaation toiminta näiden vaatimusten edellyttämällä tavalla. (Valtiovarainministeriö 2016, 24)

Tiedonhallintalain (906/2019) 4. pykälän 3 momentin luettelon 5 kohdan mukaan johdon olisi järjestettävä riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta. Näillä toimenpiteillä johto huolehtii siitä, että tiedonhallintayksikössä on olemassa riittävät kontrollit sen varmistamiseksi, että tiedonhallintayksikössä toimivat viranomaiset noudattavat tiedonhallintaa koskevia lainsäädännön vaatimuksia sekä organisaation sisäisiä määräyksiä ja ohjeita. Johdon valvontaan sisältyy myös henkilöstön riittävän tietoturvallisuuden ja tiedonhallinnan osaamisen kontrollointi. Valvonta on osa tiedonhallintayksikön sisäisen valvonnan järjestelyjä ja tietoturvallisuustoimenpiteiden toteuttamista. Vastaavalla tavalla on säädetty hyvän tiedonhallintatavan toteuttamisesta kumotussa julkisuuslain 18 pykälän 1 momentin 5 kohdassa.

6 Tutkimuksen toteutus

6.1 Tutkimusetiikka

Ammattikorkeakoulujen rehtorineuvoston Arenen julkaisemassa ammattikorkeakoulujen opinnäytetöiden eettisissä suosituksissa (2020a) ohjeistetaan opinnäytetyötä tekevää toimimaan hyvän tieteellisen käytännön mukaisesti. Hyvään tieteelliseen käytäntöön kuuluu muun muassa opinnäytetyön ja tutkimuksen aiheeseen perehtyminen, tutkimuseettisiin ohjeisiin tutustuminen, henkilötietojen käsittelyn arviointi ja tarvittaessa käsittelyn suunnitteleminen, tutkimusta koskevan sopimuksen laatiminen tilaajaorganisaation kanssa, opinnäytetyön viittauksia koskevan ohjeistuksen ja plagioinnin tarkastusmenettelyn noudattaminen, sekä opinnäytetyön julkaiseminen. (Arene 2020b, 3.)

Tutkija kuuluu tilaajaorganisaation tietosuojaryhmään ja tutkimuksen aihetta käsiteltiin sekä tilaajaorganisaation tietosuojaryhmässä, että opinnäytetyön ohjaajan kanssa ennen kuin lopullinen päätös aiheesta sekä opinnäytetyöhön liittyvät sopimukset tehtiin.

Opinnäytetyö on Opetus- ja kulttuuriministeriön ohjeistuksen mukaan julkinen eikä siihen saa sisältyä luottamuksellista tai salassa pidettävää tietoa (Arene 2020b, 27). Tutkimuksessa on käytetty vain sellaista tilaajaorganisaation aineistoa, joka on julkisesti saatavilla organisaation verkkosivuilla. Opinnäytetyön henkilöstöä koskevasta työpajasta tehdyt muistiinpanot on kirjattu siten, että keskusteluun osallistuneita ei voida tunnistaa. Organisaation tietoturvan ja tietosuojan johtamiseen liittyviin vastuisiin on dokumenttianalyysissä kirjattu tehtävänimike, rooli tai vastuuryhmä, jotka tiedot ovat julkisesti tilaajaorganisaation johtamisjärjestelmää koskevassa säännöstössä sekä verkkosivuilla.

6.2 Tutkimusmenetelmä

Tutkimuksellisen kehittämissuunnitelman tutkimusmetodina käytettiin laadullista tutkimusta, jonka tuloksena organisaation johdolle syntyy johtamisen teorian ja tietosuojan johtamisen yhdistävä malli. Laadullisessa tutkimuksessa tutkitaan pääasiassa yksittäistä tapausta tai prosessia ja tutkimusmenetelmä mahdollistaa uuden tavan ilmiön ymmärtämiseen. Laadullisessa tutkimuksessa kiinnostuksen kohteena ovat merkitykset, eli ihmisten kokemukset ja näkemykset reaalimaailman toiminnasta ja tutkimus toteutetaan aidossa kontekstissa ja suorassa kontaktissa tutkittavan ja tutkijan välillä. (Kananen 2017, 36.) Laadullinen tutkimus on kasvollista ja persoonallista tutkimusta, jossa tutkija on aina osa prosessia. Laadullisen tutkimuksen päättely lähtee johtoajatuksesta, josta se etenee eri suuntiin ja palaa takaisin johtoajatukseen, tutkimusmenetelmän tehtävänä on lisätä ymmärrystä,

antaa asioille merkityksiä ja mahdollistaa erilaisia tulkintoja, sekä tuottaa tutkittavasta asiasta uusia mallinnuksia. Laadullisen tutkimuksen avulla etsitään uutta tietoa ja sovelletaan sitä samalla verraten erilaisia vaihtoehtoja ja kehittäen työolosuhteita. (Pitkäranta 2014, 13–15.)

Pitkärannan (2014, 27) mukaan laadulliseen tutkimukseen tulee kerätä aineistoa laajasti ja monikanavaisesti, jolloin aineisto koostuu alkuperäisistä asiakirjoista, haastatteluista, havainnoinnista ja tutkijan muistiinpanoista. Tässä tutkimuksessa tutkimusaineisto koostui tilaajaorganisaation julkisista dokumenteista, työpajojen tuottamasta materiaalista ja henkilöstön kokemuksista. Havainnointia toteutettiin tietosuojasuunnitelman toteuttamista mallintavissa työpajoissa sekä aineistoanalyysin avulla läpikäytyjen organisaation johtamisjärjestelmää koskevien sääntöjen, määrittelyjen ja ohjeiden, sekä tietosuojaa ja tietoturvaa koskevien politiikkojen osalta. Työpajoissa käytettiin osallistujia osallistavia menetelmiä sekä suoraa ja osallistuvaa havainnointia tapahtumien seurantaan. Aineistoanalyysissä havainnoitiin, kuinka tietosuojaan liittyvää johdon ja päätöksenteon vastuita on kuvattu.

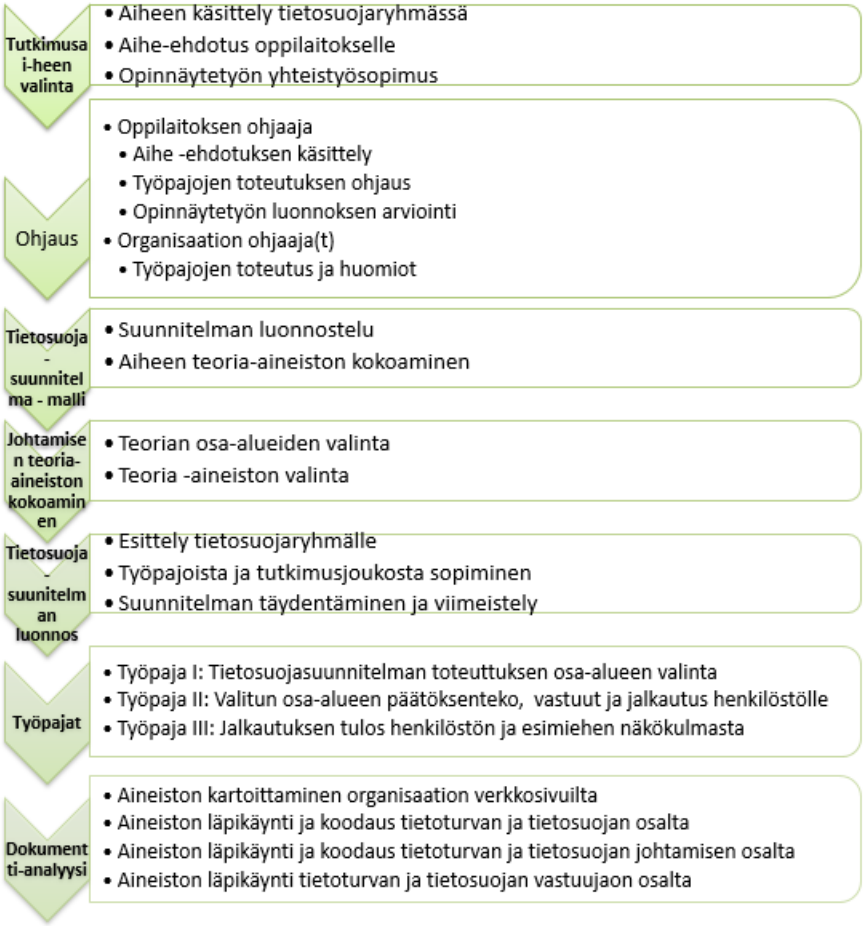
6.3 Tutkimusjoukko ja aikataulu

Tilaajaorganisaation tietosuojapolitiikan tietosuojavastuita kuvaavassa liitteessä 2 (Kotkan kaupunki 2017c) tietosuojasuunnitelman valmistelu on määritelty osaksi riskienhallintaa ja siitä vastaa tietoturvaorganisaationa toimiva riskienhallinnan johtoryhmä. Tämän kehittämishankkeen tilaajana toimii tilaajaorganisaation tietosuojaryhmä tietoturvaorganisaation sijaan. Osa tutkimukseen osallistuneista kuuluu molempiin edellä mainittuihin ryhmiin.

Tilaaja valitsi tutkimusjoukoksi tietosuojaryhmän jäsenet, joita on kahdeksan mukaan lukien tutkimusta tekevä. Tietosuojaryhmän jäsenet edustavat pääasiassa hallinto- ja talousyksikköjä, joiden vastuulle tietoturva ja tietosuoja on määritelty hallintosäännössä (Kotkan kaupunki 2020), lisäksi ryhmästä muodostuu kaksi linjaorganisaatiota sisältäen johdon, esimiehen ja kaksi alaista, sekä toisena johdon, esimiehen ja yhden alaisen.

Tutkimuksen aiheen valinta ja yhteistyösopimuksen laatiminen ajoittuivat marras- joulukuulle 2020 jonka jälkeen käynnistyi tietosuojasuunnitelmaan liittyvän aineiston kokoaminen ja suunnitelman luonnostelu, sekä muun teoria-aineiston valinta ja kokoaminen. Tietosuojasuunnitelman luonnosta käsiteltiin tietosuojaryhmän maaliskuun kokouksessa, jossa määriteltiin tutkimusjoukko ja työpajoihin osallistuminen. Työpajat toteutettiin huhti - kesäkuun aikana. Organisaation dokumenttien kartoittaminen alkoi kesäkuussa ja varsinainen aineiston analysointi toteutettiin heinäkuun aikana. Tutkimusta ohjattiin sekä oppilaitoksen, että tilaajaorganisaation puolelta käyden erilaisiin teemoihin keskittyviä tilannepalavereita

esimerkiksi työpajojen määrään ja toteuttamiseen sekä työpajojen kokemuksiin liittyen. Alla olevassa kuviossa 11 esitetään tutkimuksen eteneminen.



Kuvio 11. Tutkimuksen eteneminen.

6.4 Tutkimuksen toteutus

Tutkimuksessa tilaajaorganisaatiolle toteutettiin kehittämissuunnitelmana organisaation johdon ja tietosuojaryhmän käyttöön tietosuojasuunnitelman malli. Malli perustuu Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) asettama työryhmän raporttiin EU – tietosuojan kokonaisuudistuksesta (Valtiovarainministeriö 2016) ja mallissa on syvennetty tietosuojan johtamiseen liittyviä tehtäviä ja vastuita tietosuojalainsäädännön, kansallisten ohjeiden sekä tietosuojaa koskevan kirjallisuuden avulla. Tietosuojasuunnitelman malli oli tutkimusjoukon käytettävissä tutkimuksen aikana. VAHTI – raportin (Valtiovarainministeriö 2016) tietosuojasuunnitelma on laaja yhdeksästä osa-alueesta ja niihin sisältyvistä tehtävistä muodostuva kokonaisuus, jota ei voida toteuttaa tutkimuksen puitteissa kokonaisuudessaan, joten tutkimuksen ensimmäisen työpajan avulla suunnitelmasta valitaan yksi osa-alue tai siihen liittyvä toimenpide, jota käsitellään tarkemmin kahdessa työpajassa; johdon ja esihenkilöiden työpajassa sekä henkilöstön työpajassa. Tietosuojasuunnitelman

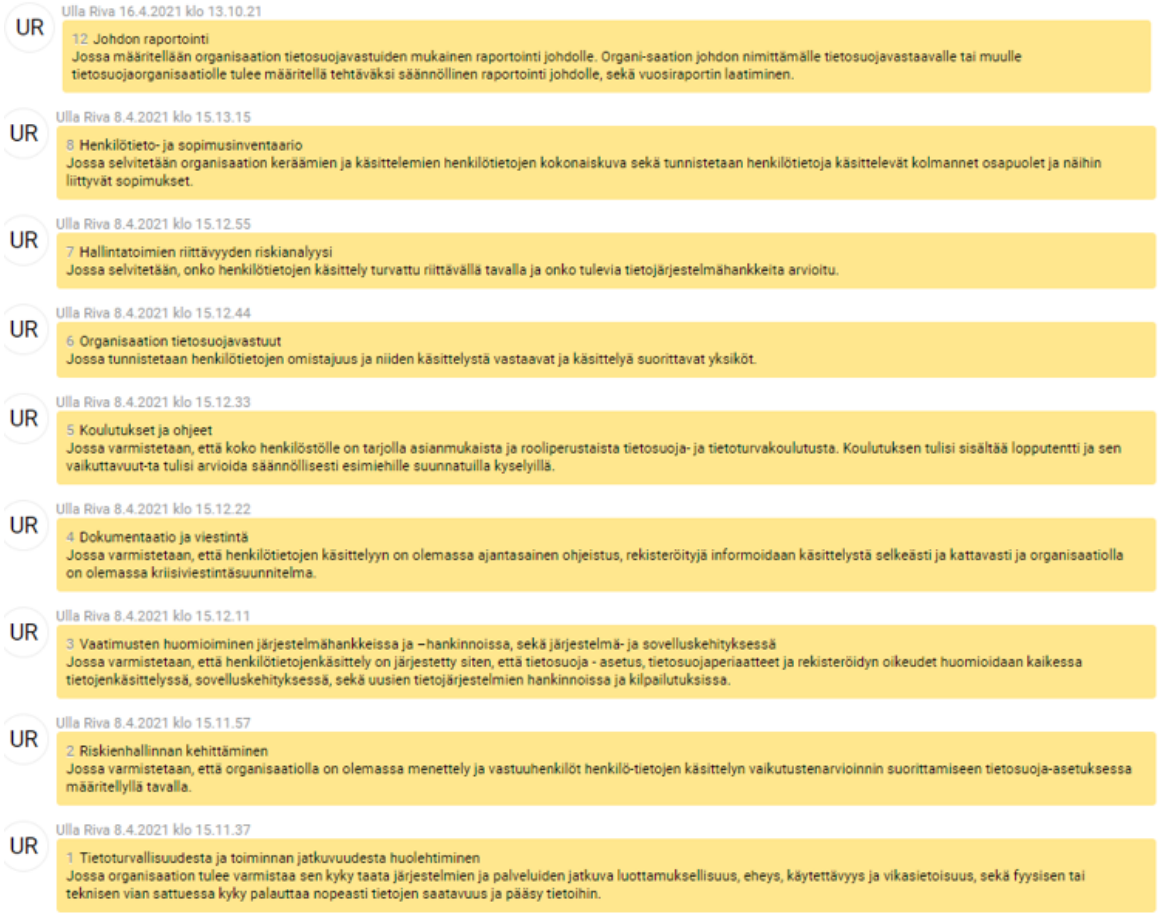
ja sen toteutukseen liittyvien työpajojen lisäksi tutkimukseen kuuluu tilaajaorganisaation johtamisjärjestelmän aineistoanalyysi, jossa aineiston avulla tutkitaan, kuinka tietosuojan johtaminen on määritelty, vastuutettu ja kuvattu. Tietoturvan johtaminen on myös arvioitu, koska tietoturva on osa tietosuojan toteutumista ja työpajoissa valittiin toteutettavaksi tietoturvaan liittyvä tietosuojasuunnitelman osa-alue.

Työpajat

Ensimmäisessä johdon ja esihenkilöiden työpajassa organisaation tietosuojaryhmä valitsi tietosuojasuunnitelman mallista osa-alueen, jota käsiteltiin tarkemmin kahdessa työpajassa; johdon ja esihenkilöiden työpajassa sekä henkilöstön työpajassa. Toisessa johdon ja esihenkilöiden työpajassa määriteltiin tietosuojasuunnitelmasta valitun osa-alueen toteutuksen edellyttämät päätökset ja toimenpiteet huomioiden organisaation johtamisjärjestelmän ja tietosuojavastaavan roolin. Kolmannessa, eli henkilöstön työpajassa johdon päätökset jalkautetaan johdon ja esihenkilöiden toimesta henkilöstötasolle. Valitun tietosuojasuunnitelman osa-alueen jalkautuksen kohteena oleva henkilöstö valittiin siten, että johtaja, esihenkilö ja henkilöstö ovat samasta linjaorganisaatiosta. Teamsissa pidetyt työpajat ajoittuivat huhti- kesäkuulle 2021 ja kukin työpaja kesti noin tunnin.

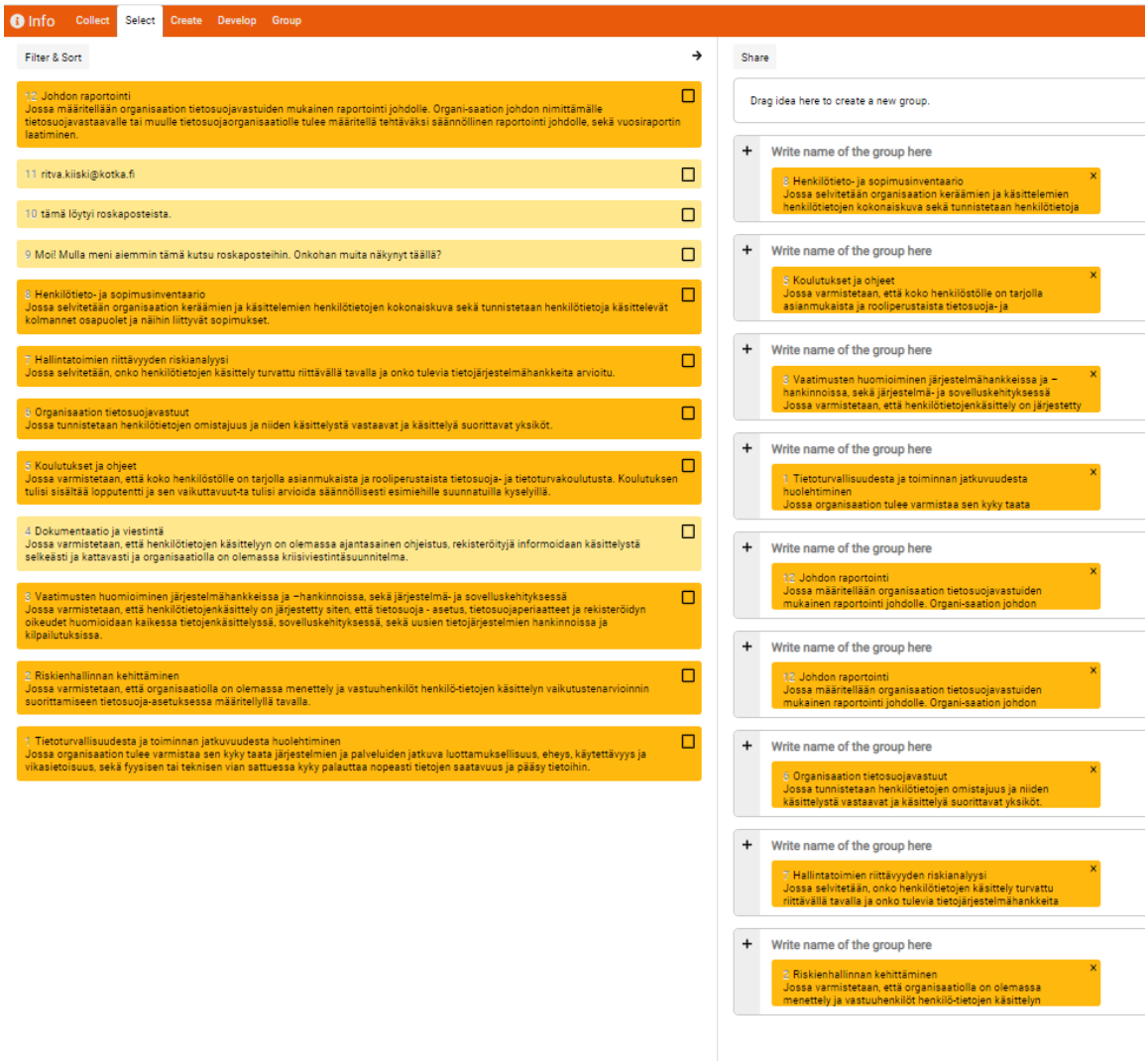
Tutkimuskohteen valinta toteutettiin kahdessa työpajassa käyttäen välineenä Orchidea Workshop – sovellusta, joka mahdollistaa useiden erityyppisten digitaalisten aivoriihityöpajojen toteuttamisen Teams – kokouksen yhteydessä.

Työpaja eteni kolmessa vaiheessa, joista ensimmäisessä työpajaan osallistuville on tutkijan toimesta kirjattu workshop- työkaluun tietosuojasuunnitelman yhdeksän osa-aluetta (kuvio 12). Työpajaan osallistujat olivat saaneet tietosuojasuunnitelman ensimmäisen luonnoksen perehdyttäväksi kolme viikkoa ennen työpajaa Teams - kutsun yhteydessä, joten osallistujilla oli käytettävissä tietoa kunkin osa-alueen sisällöstä.



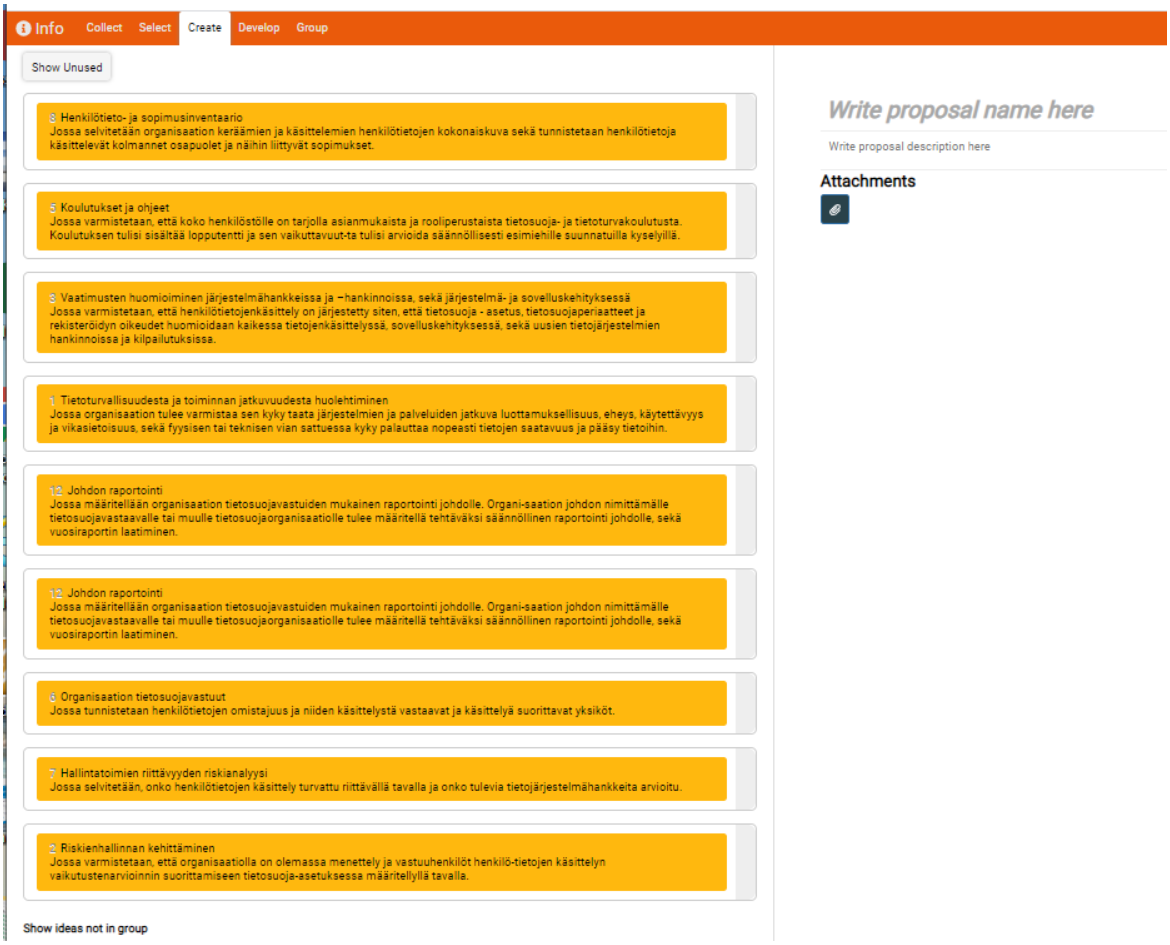
Kuvio 12. Näkymä osa-alueiden luettelosta työpajan alussa.

Toisessa, eli valinta vaiheessa osallistujat valitsivat omasta mielestään kolme tärkeintä tai merkityksellisintä tietosuojasuunnitelman osa-aluetta annetuista vaihtoehdoista. Valinta vaiheessa osallistujat siirsivät kolme valitsemaansa osa-aluetta sovelluksen vasemman-puoleisesta luettelosta oikealla olevalle tyhjälle riville, jolloin valinta tulee näkyviin kuviossa 13 oikeanpuolimmaisena näkyvään luetteloon. Tutkija ei osallistunut valintaan vaan toimi workshop- työkalun käyttäjänä.



Kuvio 13. Tietosuojasuunnitelman osa-alueiden valinta.

Työpajan kolmannessa vaiheessa (kuvio 14) laskettiin valintojen tuloksena saadusta luettelosta kunkin valitun osa-alueen saama valintojen määrä.



Kuvio 14. Valinnan tulokset.

Työryhmän jäsenten valinta kehitettäväksi tietosuojasuunnitelman osa-alueeksi viidellä äänellä (5 / 7) oli tietoturvallisuudesta ja toiminnan jatkuvuudesta huolehtiminen (kuvio 15). Valitun osa-alueen käsittelyä jatkettiin seuraavassa työpajassa.

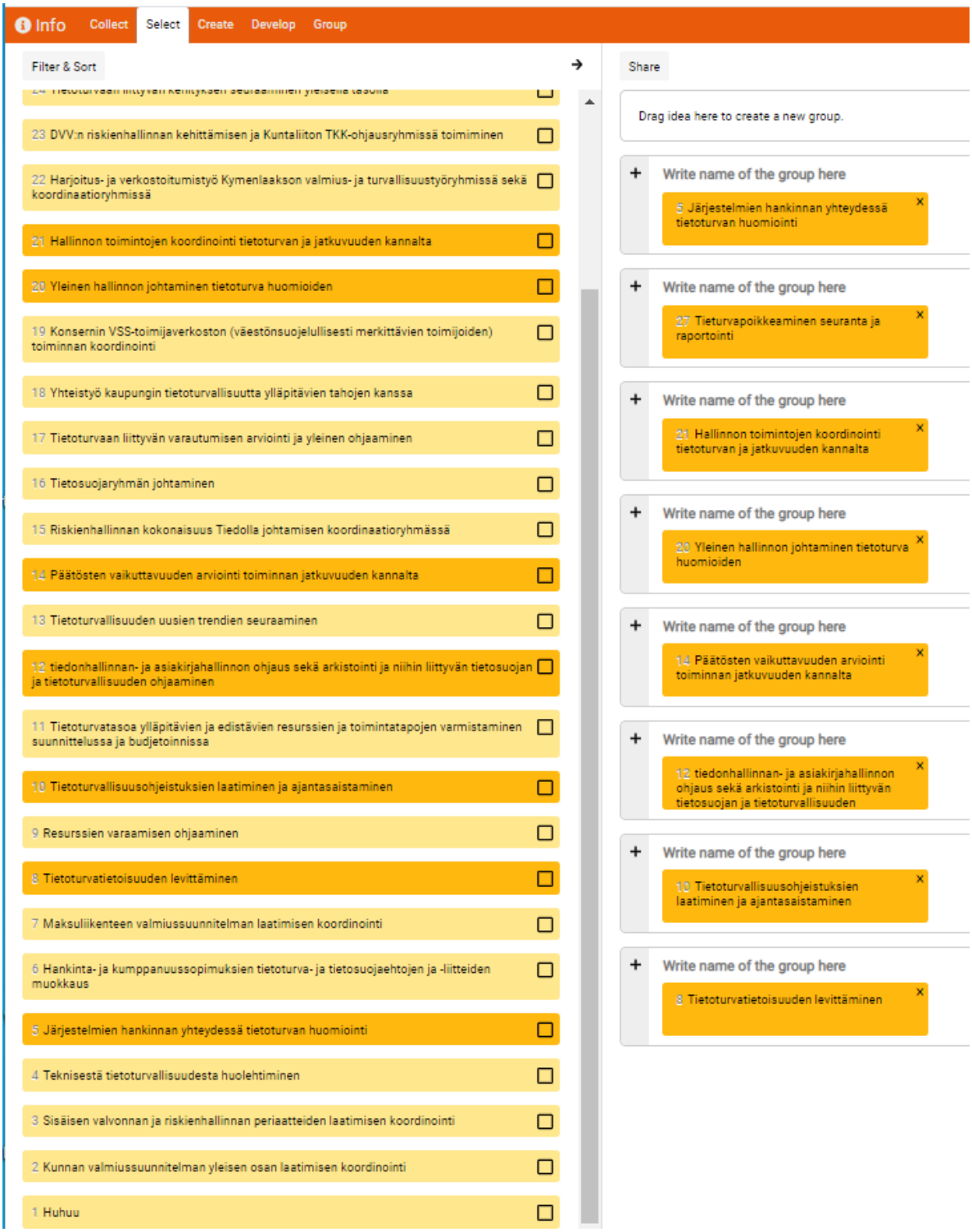
Kuvio 15. Tietosuojasuunnitelmasta valittu osa-alue Tietoturvallisuudesta ja toiminnan jatkuvuudesta huolehtiminen.

Osallistujilla oli edelleen mahdollisuus käyttää aikaisemmin saamaansa materiaalia ja tehtäväksi anto oli käyty sanallisesti läpi edellisen työpajan lopussa sekä Teams-kutsussa. Työvälineenä käytettiin edelleen Orchidea Workshop - sovellusta, johon osallistujat kirjasi-

vat työpajan ensimmäisessä vaiheessa tehtäväksi annon mukaisesti 1 - 3 omaan tehtäväänsä tai roolinsa liittyvää toimenpidettä, vastuuta tai päätöstä huomioiden organisaation johtamisjärjestelmän ja tietosuojavastaavan roolin, jotka liittyvät tietosuojasuunnitelman osa-alueeseen Organisaation tietoturvallisuudesta ja toiminnan jatkuvuudesta huolehtiminen. Toimenpiteitä / tehtäviä kertyi yhteensä 27 kappaletta, joista osa kuviossa 16.

Kuvio 16 Tehtävään liittyvät toimenpiteet ja vastuut

Työpajan toisessa vaiheessa osallistujat valitsivat edelleen kehitettävän ja henkilöstölle jalkautettavan vaihtoehdon kirjaamistaan tehtävistä (kuvio 17). Osallistujat valitsivat vaihtoehdot 8. Tietoturvatietoisuuden levittäminen ja 27. Tietoturvapoikkeamien seuranta ja raportointi.



Kuvio 17. Henkilöstölle jalkautettavan toimenpiteen valinta.

Tässä valinnassa ei laskettu kuinka paljon ääniä kukin valinta sai, vaan osallistujat tekivät valintapäätöksen keskinäisen keskustelun avulla. Valittujen vaihtoehtojen pohjalta osallistujat päättivät henkilöstölle jalkautettavaksi päätökseksi tilaajaorganisaation Intran etusivulla olevan Tietoturvapoikkeaman ilmoituslomakkeen jalkauttamisen henkilöstölle. Tietoturvapoikkeaman ilmoituslomakkeen linkki oli julkaistu organisaation intrassa joitakin viikkoja aikaisemmin, mutta sitä ei ollut vielä ohjeistettu tai tiedotettu henkilöstölle. Osallistujien näkemyksen mukaan tähän sopivat molemmat valinnat, samalla kun lomake jalkautetaan, lisätään tietoturvatietoisuutta, jonka lopputuloksena seurataan ja raportoidaan tietoturvapoikkeamia. Jalkautuksen tulosta käsiteltiin kolmannessa, eli henkilöstön työpajassa.

Kahdessa ensimmäisessä työpajassa tietosuojaryhmän jäsenet osallistuivat työpajatyöskentelyyn itseohjautuvasti aikaisemmin saamansa tietosuojasuunnitelman luonnoksen sekä lyhyen ohjeistuksen perusteella. Jokainen teki osan työpajojen tehtävistä yksin, mutta valintavaiheessa oli paljonkin yhteistä keskustelua sekä omista valinnoista, että työpajatyöskentelystä siihen tarkoitetun sovelluksen avulla.

Ensimmäisen työpajan tulos oli mielenkiintoinen, koska jatkokäsiteltäväksi tietosuojasuunnitelman osa-alueeksi valikoitui tietoturvaan liittyvä osa. Valinnan perusteella voidaan arvioida, että jokainen osallistuja teki valintansa oman arviointinsa perusteella eikä tutkija tai opinnäytetyön tietosuojanäkökulma vaikuttanut valinnan tulokseen.

Toisessa työpajassa jokaisen kuvaamien omaa tehtävää tai roolia koskevien päätösten ja vastuiden osalta ryhmä valitsi itsenäisesti kaksi toimenpidettä ja johti niistä hyvin yhden henkilöstölle eteenpäin vietävän kohteen. Työpajojen yhtenä tarkoituksena oli kerrata ja havainnollistaa kuinka päätöksen tulee jalkautua henkilöstölle saakka, joten jalkautus ja kolmannen työpajan edustajat valittiin siten, että jalkautukseen liittyvä johtaja, esihenkilö ja henkilöstö ovat samasta linjaorganisaatiosta. Päätöksen jalkautuksesta osallistujat sopivat, että tietoturvapoikkeaman ilmoituslomake esitellään ensin konsernipalvelualueen johtoryhmässä ja osallistujina olevat esimiehet velvoitetaan viestimään asia alaisilleen yksiköille. Työpajassa sovittiin, että seuranta kohdistuu Talousyksikköön, jonka esimies esittelee asian yksikön viikkopalaverissa ja muut johtoryhmään kuuluvat esimiehet esittelevät asian oman aikataulunsa mukaisesti. Tutkijan esimies kuuluu ao. johtoryhmään, joten jalkautuksen pitäisi näkyä myös tutkijan omassa yksikössä, vaikka yksikkö ei ole mukana tutkimuksessa.

Kolmannessa, eli henkilöstön työpajassa havainnoitiin keskustelun avulla tietosuojasuunnitelman osa-alueesta valitun käytännön toimenpiteen toteutuminen, eli johdon päätöksen jalkautuminen henkilöstölle. Työpajassa havainnointivälineenä oli teemahaastattelu, jossa pyrittiin löytämään vastauksia tutkimustehtävän mukaisesti ennakkoon määritellyn teeman

avulla, joka tässä perustui tutkimuksen avulla tuotettuun tietosuojasuunnitelman malliin ja sen käyttämiseen (Pitkäranta 2014, 93).

Työpajaan oli kutsuttu esimiehen lisäksi neljä esimiehen nimeämää henkilöstön edustajaa. Talousyksikössä tietoturvapoikkeaman ilmoituslomake tuli konsernipalvelualueen johtoryhmästä tiedoksi esimiehen sijaiselta heti seuraavassa viikkopalaverissa, eli yhtä viikkoa aikaisemmin kuin mitä toisessa työpajassa oli sovittu. Tästä johtuen asiaa käsiteltiin viikkopalaverissa lyhyesti sopien asian tarkempi läpikäynti seuraavaan viikkopalaveriin. Jalkauttamisen näkökulmasta tiedon kulku johtoryhmän kokouksesta toimi hyvin ja jalkautukselle saatiin käytännössä kaksi toteutusta (alustava sekä syventävä) samalle osallistujaryhmälle.

Henkilöstön työpajassa keskusteltiin lomakkeen jalkautuksesta ja saaduista kokemuksista. Keskustelun pohjana olivat kysymykset; Olitko huomannut tietoturvaloukkauksen ilmoituslomakkeen Intrassa? Olisitko tiennyt milloin ja miten lomaketta käytetään? Oliko asiasta kertominen yksikön palaverissa mielestäsi tärkeää vai turhaa? Tuletko käyttämään lomaketta ja madalsiko käyttökynnystä? sekä Heräsikö muita ajatuksia? Lisäksi esimieltä kysyttiin mitä ajatuksia hänelle tuli menettelystä?

Työpajassa käydyn keskustelun perusteella voidaan havaita, että tietoturvapoikkeaman ilmoituslomakkeen esittely ja läpikäynti kahdessa viikkopalaverissa oli herättänyt keskustelua, antanut tietoa sekä tietoturvapoikkeamista, että oikeasta tavasta reagoida havaitsemaansa poikkeamaan. Henkilöstöllä oli herännyt kiinnostus saada lisää tietoa tietoturvaan ja tietosuojaan liittyvistä asioista ja esimiehellä olisikin hyvä tilaisuus reagoida ja järjestää lisäkoulutusta. Esimiehen huomioissa nousi esille yksikön toimintaan liittyvän tiedon suuri määrä, josta on haastava poimia sekä toiminnan kannalta kriittinen tieto, että henkilöstöä kiinnostava tieto.

Tutkimuksessa ei ollut tarkoitus arvioida organisaation tietoturvan tai tietosuojan nykytilaa vaan tuottaa uutta tietoa tietosuojasuunnitelman muodossa ja testata suunnitelmasta valittua osa-aluetta kartoittamalla osa-alueeseen liittyvää päätöksentekoa ja vastuuta ja jalkauttamalla päätöksenteon kohde henkilöstölle. Talousyksikössä toteutettiin johdon ja esimiesten työpajassa tehdyn tietoturvaan liittyvän päätöksen perusteella organisaatiossa käyttöön otetun tietoturvapoikkeaman ilmoituslomakkeen jalkauttaminen. Jää myöhemmin nähtäväksi toteutetaanko tilaajaorganisaatiossa vastaavalla tavalla muiden tietosuojaan tai tietoturvaan liittyvien päätösten jalkauttaminen. Tämän pienen otannan perusteella henkilöstö koki viikkopalaverissa tehdyn jalkauttamisen hyväksi tavaksi tuoda uudet asiat tiedoksi.

Aineiston käsittely ja analyysi

Laadullisen aineiston analyysissä aineistosta luodaan kokonaisuus, jonka avulla voidaan tuottaa tulkinta ja tehdä johtopäätöksiä tutkittavasta ilmiöstä. Analyysi pitää sisällään aineiston osien analysointia eritellen, tiivistäen ja luokitellen sekä aineiston osien synteesin laatimisen, jossa aineistosta luodaan kokonaiskuva ja esitetään tutkimuskohde uudesta näkökulmasta. Tässä tutkimuksessa aineistoa analysoitiin teorialähtöisesti, jolloin analyysissä voidaan tunnistaa jo tiedetyn tiedon vaikutus ja aikaisemman tiedon tehtävänä on aukoa uusia ajatusuria eikä testata teoriaa. Aineistoanalyysissä tutkimusaineistoa pelkistettiin tutkimusaihetta koskevien ilmaisuiden ja niiden ryhmittelyn avulla, eli koodaamalla. Koodaaminen on yksinkertaisimmillaan samaa tarkoittavien sanojen tai yhtenäisiä merkityksiä sisältävien lauseiden tunnistamista ja merkitsemistä tutkijan valitsemilla koodeilla. Tutkimusaineisto luokiteltiin, mikä tarkoittaa analyysiyksiköiden ryhmittelyä ennalta määriteltyihin kategorioihin. Analyysissä käytettiin myös suppeasti määrällistä analyysiä, eli kvantifikointia, jossa aineistosta laskettiin koodien esiintyvyyttä. (Puusa & Juuti 2020, 151–154).

Aineistoanalyysissä käytetty dokumentaatio on tilaajaorganisaation verkkosivuilla joko suoraan julkaistua tai julkisten kokouspöytäkirjojen liitteenä olevaa julkista dokumentaatiota. Aineiston rajaaminen julkiseen dokumentaatioon perustuu EU:n yleisen tietosuoja-asetuksen (EU 679/2016) 5 ja 12 artikloissa määriteltyyn läpinäkyvyyden periaatteeseen, jonka mukaan henkilötietojen käsittelyn tulee olla rekisteröidyn kannalta läpinäkyvää. Periaatteen perusteella myös tietosuojaan liittyvän johto- ja päätöksentekovastuullisten sekä johtamis- ja päätöksenteko prosessien tulee olla rekisteröityjen saatavissa. Aineisto analysoitiin teoriaohjaavasti usealla lukukerralla jäsentäen, havainnoiden ja koodaten sitä kierros kierrokselta.

Aineistolähtöisessä analyysissä tutkimusaineistosta pyritään luomaan teoreettinen kokonaisuus, jossa analyysiyksiköt valitaan tutkimuksen tarkoituksen ja tehtävän mukaisesti. Aineistolähtöisessä analyysissä analyysiyksiköt eivät ole ennalta määriteltyjä tai harkittuja, jolloin teorian merkitys analyysin ohjaajana liittyy metodologiaan, ja tutkimuksessa julkilausutut metodologiset sitoumukset ohjaavat analyysiä. Aineistolähtöisen tutkimuksen problematiikka on, että puhtaita, ilman aikaisempaa teoriataustaa ja sen vaikutusta tehtäviä havaintoja on vaikea toteuttaa. Tätä ongelmaa pyritään tässä tutkimuksessa ratkaisemaan käyttämällä tutkimusmenetelmänä teoriaohjaavaa analyysiä, jossa teoria kytketään tutkimuksen avuksi, mutta tutkimus ei kokonaan pohjaudu teoriaan. Teoriaohjaavassa analyysissä analyysiyksiköt valitaan aineistosta, mutta aikaisempi tieto tai teoria ohjaa analyysiä. Aikaisemman tiedon merkitys ei ole teoriaa testaava vaan uusia ajatusuria aukova. (Tuomi & Sarajärvi 2018, 108–109).

Analyysikierroksilla luokitteluyksikkönä käytettiin kolmea värikoodia; vihreä: tietosuojan vastuu on nimetty, keltainen: tietosuojan johtamisen vastuu on määritelty välillisesti (vaatii tulkintaa lainsäädännöstä, organisaation hallinta, toiminta- ja muista säännöistä), sekä harmaa: Tietosuojan johtamisen vastuu on ilmaistu passiivissa (määritelty organisaatiolle tai oikeushenkilölle, ei roolille).

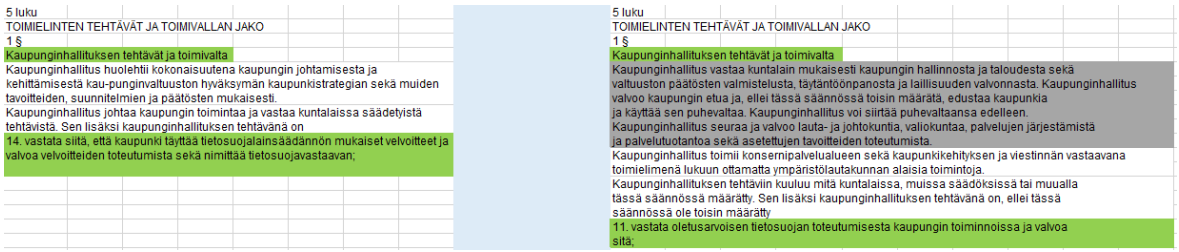
Ensimmäisellä analyysikierroksella käytiin läpi tilaajaorganisaation Määräykset, säännöt ja ohjeet - verkkosivuilla (Kotkan kaupunki 2021b) olevat hallintosäännöt (Kotkan kaupunki 2020, 2021) sekä 2020 vuoden hallintosäännön nojalla annetut toimintasäännöt, toiminta-ohjeet, organisaation asianhallintajärjestelmässä pöytäkirjan liitteenä (Kotkan kaupunki 2021c) olevat tietoturva ja tietosuojapolitiikat, tietotilinpäätös sekä henkilöstöohjelma (Kotkan kaupunki 2018), yhteensä kaksikymmentäneljä dokumenttia.

Tällä analyysikierroksella luokitteluyksikkönä toimi johtamista, sekä erityisesti tietosuojaa tai tietoturvaa kuvaava lause tai lausekokonaisuus. Yleisesti johtamista kuvaava lause tai lausekokonaisuus tai passiivimuodossa organisaation vastuulle määritelty tietoturvan tai tietosuojan vastuu sai harmaan värikoodin. Keltaisella värikoodilla merkittiin dokumentaatiosta kohdat, joissa johtamisen, tietoturvan tai tietosuojan vastuussa viitattiin ao. dokumentin tai jonkin toisen dokumentin sisältämään määrittelyyn. Vihreällä värikoodilla merkittiin kohdat, joissa kuvattiin selkeästi tietosuojaan liittyvä johtovastuu. Värikoodaamisen jälkeen havaitut lauseet tai lausekokonaisuudet kopioitiin havainnointipäiväkirjaan dokumentin nimen mukaisesti väliotsikoituna. Ensimmäisen analyysivaiheen aikana havainnointipäiväkirjaan siirrettyjen lauseiden ja lausekokonaisuuksien yhteyteen kirjattiin, liittyikö dokumentista ensimmäisellä kierroksella tehty havainto johtamiseen yleisesti, tietoturvan johtamiseen tai tietosuojan johtamiseen. Vain tietoturvan ja tietosuojan johtamiseen liittyväksi luokitellut dokumentit siirtyivät seuraavalle analyysikierrokselle. Toiselle analyysikierrokselle jäi yhdeksän dokumenttia.

Jatkoanalysoinnista pois karsitut dokumentit olivat; hallintosäännön nojalla annetut toimintasäännöt, joissa ei ollut kuvattu tietoturvaan tai tietosuojaan liittyvää johtamista, henkilöstöohjelma, joka on ainoa organisaation sisäinen ensimmäisen kierroksen läpikäynyt dokumentti, tietotilinpäätös (Kotkan kaupunki 2021d), joka ei ole tietosuojaa tai tietoturvaa ohjaava dokumentti vaan organisaation johdolle annettu raportti sekä käyttövaltuus- ja lokipolitiikat, jotka ovat tietosuojapolitiikan alipolitiikkoja. Tietosuojapolitiikka on tietoturvan alipolitiikka, joten sen alipolitiikat eivät kuvaa tietosuojan tai tietoturvan johtovastuuta vaan yksittäisiin tietojärjestelmiin liittyviä järjestelmän omistajan määrittely - ja dokumentointi vastuita. Henkilöstöohjelma analysoitiin ensimmäisellä kierroksella, koska henkilöstön osaamisen

kehittäminen on molemmissa hallintosäännöissä määritelty henkilöstöasioiden yksikölle. Henkilöstöohjelma ei kuitenkaan pitänyt sisällään tietosuojan tai tietoturvan osaamisen kehittämiseen tai perehdyttämiseen liittyviä vastuita tai toimenpiteitä, ohjelma on organisaation strategiaan perustuva henkilöstöstrategia dokumentti.

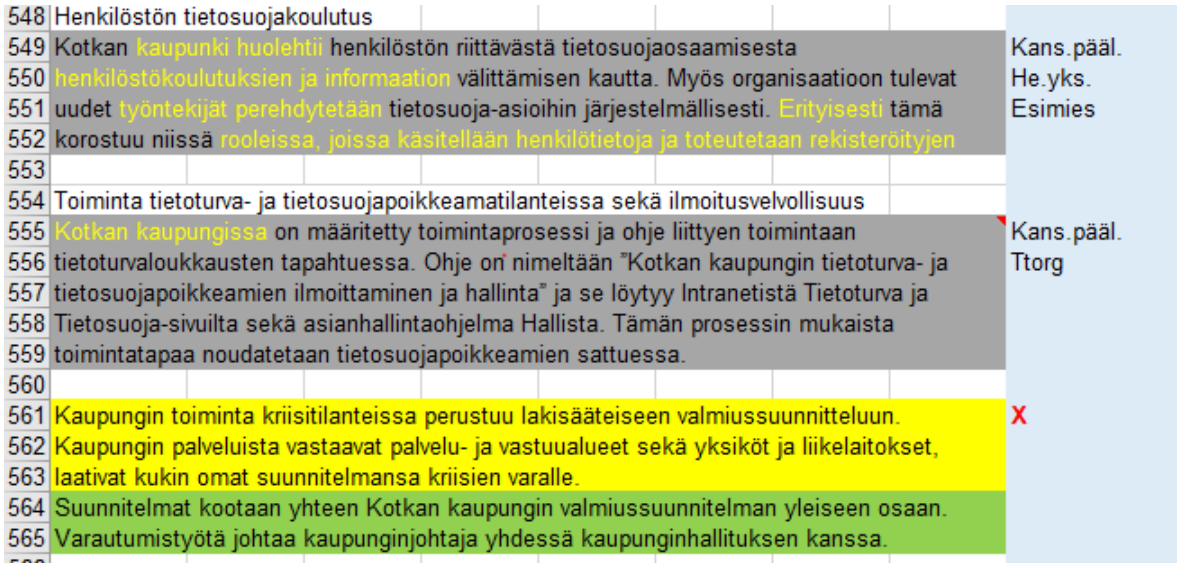
Toisella analyysikierroksella tietoturvan tai tietosuojan johtamista tai vastuiden määrittelyä koskevat tai niihin liittyvää tekstiä sisältäneet dokumentit tarkasteltiin uudelleen koodaamalla niistä Excel taulukon avulla tietoturvaan ja tietosuojaan liittyvä johtamisen ilmaus. Kuviossa 18 on esimerkki hallintosääntöjen (Kotkan kaupunki 2020a; 2021a) vertailusta. Vasemmalla vuoden 2020 ja oikealla vuoden 2021 hallintosääntö, jossa vihreällä on koodattu tietosuojan vastuun määrittely ja harmaalla vastuun ilmaiseminen passiivimuodossa.



Kuvio 18. Toisen analyysikierroksen koodaus hallintosääntöjen osalta.

Toisella analyysikierroksella läpikäydyt dokumentit olivat: hallintosääntö 3 2020, hallintosääntö 5 2021, kaupunginhallituksen alaisten toimintojen toimintasääntö, sisäisen tarkastuksen toimintasääntö, konserniohje, asiakirjahallinnon ja arkistotoimen toimintaohje, tiedonhallintalain mukaisten vastuiden määrittely, tietoturvapolitiikka ja tietosuojapolitiikka.

Kolmannella analyysikierroksella tarkasteltiin aiemmin mainitussa Excel - taulukossa olevia tietoturva ja tietosuojapolitiikoista poimittuja keltaisella tai harmaalla merkittyjä kohtia, joissa tietoturvan tai tietosuojan vastuu tai toimenpiteet on määritelty välillisesti tai ilmaistu passiivimuodossa. Näihin kohtiin haettiin edellä mainituista politiikoista vastuunjako -liitteessä kuvattujen tehtävien perusteella ja osin näitä soveltaen vastuutaho, joka merkittiin värikoodatun kohdan yhteyteen kuviossa 19 vaaleansinisellä pohjalla olevien lyhenteiden tapaan.



Kuvio 19. Kolmannen analyysikierroksen koodaus tietosuojapolitiikan osalta.

Aineistotutkimuksessa havainnoitiin, kuinka organisaation johdon tietosuojaan liittyviä vastuita on kuvattu johtamisjärjestelmään koskevissa dokumenteissa sekä muissa tietosuojaan tai tietoturvaan liittyvissä dokumenteissa. Tietosuojan johtamisjärjestelmän ja tietosuojasuunnitelman osalta tutkimuksen tuloksia käsitellään tarkemmin seuraavassa luvussa.

7 Tulokset

Tässä laadullisessa tutkimuksessa käytettiin tutkimusmenetelmänä suoraa ja osallistuvaa havainnointia, sekä teoriaohjaavaa aineistoanalyysiä. Aineistoanalyysissä tutustuttiin organisaation johtamisjärjestelmää sekä tietosuojaa ja tietoturvaa koskeviin sääntöihin ja politiikkoihin havainnoiden ja koodaten sitä, kuinka tietosuojaan liittyviä johdon ja päätöksenteon vastuita on kuvattu. Osallistuvaa havainnointia tehtiin kolmessa tietosuojasuunnitelman käytännön toteutukseen liittyvässä työpajassa. Tutkimuksen tarkoituksena oli kytkeä johtamisen teoria kehittävän tutkimuksen avulla käytännönläheiseksi osaksi kansallista tietosuojasuunnitelman mallia ja havainnollistaa millaisia toimenpiteitä ja päätöksiä johdon vastuulla on tietosuojasuunnitelman toteuttamisessa.

Tutkimuksen tuloksena organisaatiolle syntyi tietosuojasuunnitelma sekä työpajojen myötä käytännön toteutus tietosuojasuunnitelmasta valittuun osaan Tietoturvallisuudesta ja toiminnan jatkuvuudesta huolehtiminen. Tästä tietosuojasuunnitelman osasta edettiin johdon päätöksentekoa koskevan työpajan tuloksena valitsemaan kaksi henkilöstölle jalkautettavaa teemaa: tietoturvatietoisuuden levittäminen ja tietoturvapoikkeamien seuranta ja raportointi. Nämä päätöksenteon kautta valitut toimenpiteet jalkautettiin tilaajaorganisaation hallinto- ja toimintasäännöissä kuvatun johtamisjärjestelmän mukaisesti konsernipalvelualueen johtoryhmätasolta kolmanteen työpajaan valitun yksikön esimiehen kautta henkilöstölle. Jalkautusta seurattiin vain valitun yksikön osalta, mutta seurantaa on tarkoitus jatkaa tutkimuksen ulkopuolella kaikkien johtoryhmän yksiköiden osalta.

7.1 Tietoturvavastuu organisaatiossa

EU:n yleinen tietosuoja-asetus (EU 679/2016) edellyttää, että rekisterinpitäjä ja henkilötietoja käsittelevä organisaatio on huolehtinut henkilötietojen käsittelyn sisäänrakennetusta ja oletusarvoisesta tietosuojasta (25 artikla) sekä käsittelyn turvallisuudesta (32 artikla). Tietoturvan näkökulmasta tämä tarkoittaa että, rekisterinpitäjä on huolehtinut henkilötietojen käsittelyn luottamuksellisuudesta ja eheydestä ja henkilötietoja käsitellään tavalla, jolla varmistetaan niiden asianmukainen turvallisuus.

Aineiston analyysin perusteella voitiin havaita, että tietoturvaan liittyviä vastuita ja vastuussa olevia määritellään useassa dokumentissa.

Tilaajaorganisaation hallintosäännössä (Kotkan kaupunki 2020a, 12, 31) tietoturvallisuuden ohjaaminen määritellään konsernipalvelualueen hallintoyksikön vastuuksi ja tietoturvallisuuden tekninen kehittäminen talousyksikön vastuuksi, kaupunginhallitus vastaa tiedonhallinnan vastuiden, käytäntöjen ja valvonnan määrittelystä sekä tietoturvallisuusjärjestelyistä.

1.8.2021 voimaan tulevassa hallintosäännössä (Kotkan kaupunki 2021 13, 35) konsernipalvelualueen hallintoyksikkö vastaa kaupungin tiedonhallinnan- ja asiakirjahallinnon ohjauksesta sekä arkistoinnista ja niihin liittyvän tietosuojan ja tietoturvallisuuden ohjaamisesta. Talousyksikkö vastaa tietoturvallisuuden teknisestä kehittämisestä ja kaupunginhallitus vastaa on tiedonhallinnan vastuiden, käytäntöjen ja valvonnan määrittelystä sekä tietoturvallisuusjärjestelyistä kuten aikaisemmassakin hallintosäännössä. Uudessa hallintosäännössä jää siten tarkentamatta aikaisemman hallintosäännön mukaisen koko organisaatiota koskevan tietoturvallisuuden ohjaamisen vastuutaho. Vastuuta on mahdollista ohjata uuden hallintosäännön nojalla myöhemmin annettavalla toimintasäännöllä.

Tilaajaorganisaatiossa on kaupunginhallituksen hyväksymä tiedonhallintalain mukaisten vastuiden määrittely (Kotkan kaupunki 2020c, 3–4) jonka mukaan tiedonhallintalain (906/2019) mukaisista tietoturvallisuustoimenpiteiden kuvauksista vastaa talousjohtaja/tietohallinto jota auttaa toteutuksessa tietotyöryhmä ja tietosuojatyöryhmä. Saman määrittelydokumentin mukaan hallinto- ja kehittämispäällikkö ja talousjohtaja vastaavat tietoturvallisuusohjeiden ylläpidosta, riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden kokonaisuudesta. Työtä ohjaavat riskienhallinnan johtoryhmä sekä tietosuojatyöryhmä ja keskinäinen vastuu on määritelty hallintosäännössä. Määrittely vastaa aikaisemman hallintosäännön (Kotkan kaupunki 2020a) tietoturvallisuuden kokonaisvastuun määrittelyä.

Tietoturvapolitiikka (Kotkan kaupunki 2017d, 3) on organisaation johdon määrittely johtamista, palveluita ja toimintoja koskevista tietoturvallisuuden periaatteista sekä tavoitteista ja on perustana organisaation johdon antamille muille alapolitiikoille ja ohjeille, joita organisaatiossa sovelletaan tietoturvan toteutumiseksi. Tietoturvapolitiikassa määritellään muun muassa tietoturvatoimintaa ohjaavat tekijät, organisointi ja vastuut, tietoturvaosaamisen ja -tietoisuuden ylläpito, tietoriskien hallinta, poikkeustiloissa toimiminen, turvatoimien priorisointi sekä tietoturvallisuuden seuranta, ylläpito ja kehittäminen.

Aineistoanalyysissä tietoturvapolitiikka tarkasteltiin koodaamalla siitä Excel taulukon avulla tietoturvaan liittyvät johtamisen ilmaukset luokittelemalla nämä käyttäen kolmea värikoodia; vihreä: tietoturvan vastuu on nimetty, keltainen: tietoturvan johtamisen vastuu on määritelty välillisesti, eli määrittely edellyttää tulkintaa lainsäädännöstä, organisaation hallinta-, toiminta- ja muista säännöistä, sekä harmaa: tietoturvan johtamisen vastuu on ilmaistu passiivissa, eli vastuu on määritelty organisaatiolle tai oikeushenkilölle. Tietoturvapolitiikassa oli yhteensä kuusitoista määriteltyä vastuuta, kolme välillisesti määriteltyä ja seitsemäntoista passiivimuodossa ilmaistua vastuuta. Kolmannella analyysikierroksella harmaalla värikoodattuihin, eli passiivimuodossa esitettyihin kohtiin haettiin tietoturvapolitiikan vastuun-

jako - liitteessä kuvattujen vastuiden perusteella vastuutaho. Tietoturvapolitiikan ja sen liitteenä 2 olevan vastuunjakokuvauksen perusteella ylin toiminnallinen päätösvalta tietoturvassa kohdistuu kaupunginjohtajan johtoryhmälle, kansliapäällikölle sekä tietoturvaorganisaatiolle, joka vastuunjakotaulukon mukaan on riskienhallinnan johtoryhmä. Tietoturvapolitiikassa mainitaan rooli tietoturvasta vastaava, mutta tällaista roolia ei ole kuvattu vastuunjakokuvauksessa. Yksi politiikan kohta jäi koodauksen jälkeen ilman vastuutahoa. Tiedon ja tietojärjestelmien käyttöä koskevassa kappaleessa (Kotkan kaupunki 2017d, 6) mainitaan, että laiminlyönteihin puututaan tietoturvarikkomusten tulkinta ja seuraamussäännöstön mukaisesti. Säännöstö on tietosuojapolitiikan (Kotkan kaupunki 2017c) liite 4. Tietoturvapolitiikassa ja sen liitteenä olevassa vastuutaulukossa, tietosuojapolitiikassa ja sen liitteenä olevassa vastuutaulukossa tai seuraamussäännöstössä ei ole kuvattu minkä tahon tai roolin vastuulla seuraamusmenettely on.

Tietoturvaan liittyvää vastuuta kuvataan tilaajaorganisaatiossa hallintosäännöissä, sekä tiedonhallintalain mukaisten vastuiden määrittelyssä ja tietoturvapolitiikassa keskenään eri tavoilla. Tietoturvan päätöksentekoon liittyvien roolien ja vastuuhenkilöiden hahmottaminen on vaikeaa, koska vastuut on määritelty jokaisessa dokumentissa hieman eri tavalla. Pienessä organisaatiossa määrittelyn vaihtelevuus yleensä yhdistyy niihin vastuuhenkilöihin, jotka käytännössä hoitavat tietoturvavastuita. Tällaisen henkilöityneen vastuurakenteen perehdyttäminen henkilöstölle on toteutettava huolella. Kolmannen työpajan tuloksissa tuli selkeästi esille, että organisaation intranetin sivuilla jaettu tieto ei vielä muodosta toimivaa prosessia vaan henkilöstö tarvitsee konkreettisen vastuutahon, jolta voi kysyä lisätietoja ja saada neuvontaa ja ohjausta.

7.2 Tietosuojavastuu organisaatiossa

Organisaatiossa tulee määritellä tietosuojan kokonaisvastuu, joka pitää sisällään tietosuojan johtamisen ja koordinoinnin, sekä muun organisaation sisäisen järjestäytymisen tietosuojan toteuttamiseksi. Tietosuojan koordinoinnista vastaavan johdon tulee toimia organisaation ylimmän johdon antamalla toimivalla. (Andreasson ym. 2015, 83.) Tietosuojavelvoitteiden toteuttamiseen tarvittavat toimenpiteet tulee määritellä organisaation toimialan, koon, toiminnan ja henkilötietojen käsittelyn luonteen, käsiteltävien henkilötietojen arkaluonteisuuden, käsittelyn asiayhteyden ja tarkoitusten, organisaatiorakenteen ja yritysmuodon perusteella (Andreasson ym. 2019, 22.)

Aineiston analyysin perusteella voitiin havaita, että tietosuojaan liittyviä vastuita ja vastuussa olevia määritellään useassa dokumentissa.

Tilaajaorganisaation hallintosäännössä (Kotkan kaupunki 2020a, 16–17) määritellään kaupunginhallituksen tehtävään ja toimivaltaan vastata tietosuojalainsäädännön mukaisten velvoitteiden täyttämisestä ja velvoitteiden toteutumisen valvonnasta sekä nimittää tietosuojavastaava. 1.8.2021 voimaan tulevassa hallintosäännössä (Kotkan kaupunki 2021 17-18) kaupunginhallituksen tehtävään ja toimivaltaan kuuluu vastata oletusarvoisen tietosuojan toteutumisesta kaupungin toiminnoissa ja valvoa sitä. Kaupunginhallituksen tietosuojaa koskevaa vastuuta on supistettu uudessa hallintosäännössä, eikä koko organisaation tietosuojasta vastaavaa tahoa ole määritelty. Vastuuta on mahdollista ohjata uuden hallintosäännön nojalla myöhemmin annettavalla toimintasäännöllä.

Tietosuojapolitiikka (Kotkan kaupunki 2017c) on tietoturvapolitiikan alipolitiikka, jollaisena se toteuttaa johdon tietoturvapolitiikassa määrittelemiä johtamista, palveluita ja toimintoja koskevia tietoturvallisuuden periaatteita ja tavoitteita (Kotkan kaupunki 2017d, 3). Tietosuojapolitiikassa määritellään organisaation tietosuojan toteuttamisessa ja kehittämisessä noudatettavat periaatteet, toimintatavat, vastuut, sekä valvonnan ja seuraamusjärjestelmän. Tietosuojapolitiikan mukaan organisaatio toimii rekisterinpitäjänä. (Kotkan kaupunki 2017c, 3.)

Aineistoanalyysissä tietosuojapolitiikkaa tarkasteltiin koodaamalla Excel -taulukon avulla politiikasta tietosuojaan liittyvät johtamisen ilmaukset ja luokittelemalla nämä käyttäen kolmea värikoodia; vihreä: tietosuojan vastuu on nimetty, keltainen: tietosuojan johtamisen vastuu on määritelty välillisesti, eli määrittely edellyttää tulkintaa lainsäädännöstä, organisaation hallinta-, toiminta- ja muista säännöistä, sekä harmaa: tietosuojan johtamisen vastuu on ilmaistu passiivissa, eli vastuu on määritelty organisaatiolle tai oikeushenkilölle. Kolmannella analyysikierroksella harmaalla värikoodattuihin, eli passiivimuodossa esitettyihin kohtiin haettiin tietosuojapolitiikan vastuunjako - liitteessä kuvattujen vastuiden perusteella vastuutaho. Tietosuojapolitiikassa oli yhteensä neljä määriteltyä vastuuta, kolme välillisesti määriteltyä ja kaksikymmentäkaksi passiivimuodossa ilmaistua vastuuta. Neljätoista politiikan kohta jäi osin tai kokonaan koodauksen jälkeen ilman vastuutahoa mukaan lukien tietoturvapolitiikan (Kotkan kaupunki 2017d) analyysin yhteydessä havaittu tietoturvarikkomusten tulkinta ja seuraamussäännöstöä koskeva vastuutahon määrittelyn puutos. Tietosuojapolitiikan liitteenä 2 olevan vastuunjakokuvauksen perusteella ylin toiminnallinen päätösvalta tietosuojassa kohdistuu samalla tavalla kuin tietoturvapolitiikassa, eli kaupunginjohtajan johtoryhmälle, kansliapäällikölle sekä tietoturvaorganisaatiolle, joka vastuunjakotaulukon mukaan on riskienhallinnan johtoryhmä.

Kuten tietoturvan osalta havaittiin, myös tietosuojan osalta vastuuta kuvataan tilaajaorganisaatiossa hallintosäännöissä, sekä tiedonhallintalain mukaisten vastuiden määrittelyssä ja

tietosuojapolitiikassa keskenään eri tavoilla. Uudessa voimaan tulevassa hallintosäännössä tietosuojan kokonaisvastuullinen jää ilman määrittelyä ja kaupunginhallituksen tietosuojavastuuta on supistettu aikaisemmasta. Määrittelyn muutos aiheuttaa ainakin hetkellisesti dokumentoitujen vastuiden puutteellisuutta, mikä on hyvä tunnistaa henkilötietojen tietoturvapoikkeamatilanteiden käsittelyssä osoitusvelvollisuuden näkökulmasta. Tietosuojan osalta on havaittavissa myös tietosuojapolitiikan vastuunjakotaulukon yhtenevyys tietoturvapolitiikan vastaavan liitteen kanssa. Hallintosäännön pohjalta tehtävässä politiikan päivityksessä on hyvä tarkastella tietosuojan vastuunjakotaulukon tietojen ajantasaisuutta. Vastuunjakotaulukon sisällöllä voidaan merkittävästi helpottaa tietosuojavastuiden tulkitsemista ja ymmärrettävyyttä. Myös tietynlainen henkilöitynyt vastuunjako on havaittavissa nykyisestä tietosuojan vastuunjakotaulukosta. Tietosuojavastaavan rooli jää myös dokumentaatiossa avoimeksi, eikä tietosuojavastaavan ylimmälle johdolle annettavaa raportointia tai sen säännönmukaisuutta ole kuvattu. Organisaatiolla on käytössä tietotilinpäätös, mutta raportointitapaa tai raportin perustumista esimerkiksi tietosuojan nyytilakuvaukseen ja sen pohjalta tehtyyn tietosuojan tilan kehittämissuunnitelmaan ei voida havaita dokumentaatiosta.

7.3 Rekisterinpitäjä rooli

EU:n yleinen tietosuoja- asetus (EU 679/2016) määrittelee 4 artiklan 7 kohdassa rekisterinpitäjäksi luonnollisen henkilön tai oikeushenkilön, viranomaisen, viraston tai muun elimen, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisteinpitäjä voi siten olla organisaatio, mutta koska organisaatio ei itsessään toteuta tietosuoja-asetuksen 24 artiklassa rekisterinpitäjälle säädettyjä velvollisuuksia, joita ovat muun muassa sisäänrakennetun ja oletusarvoisen tietosuojan varmistaminen, sen osoittaminen, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta sekä tietosuojaa koskevien toimintaperiaatteiden täytäntöön paneminen, tulee organisaation johdon määritellä tarkemmin tietosuojan vastuut ja luoda tietosuojan johtamisjärjestelmä.

Tietosuoja-asetuksen (EU 679/2016) 38 artiklan 3. kohdassa määritellään tietosuojavastaavan raportoinnista, joka annetaan suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle. Tietosuojavastaavan tulee siis tietää mikä tai kuka organisaation johtamisjärjestelmän mukaan on raportoinnin vastaanottava taho. Tutkimuksen tilaajaorganisaatiossa tietotilinpäätöksen (Kotkan kaupunki 2021d) käsittelee ja hyväksyy kaupunginhallitus.

Tilaajaorganisaation asiakirjahallinnon ja arkistotoimen toimintaohjeessa (Kotkan kaupunki 2017a, 5, 8-9, 15) on määritelty, että kaupunginhallitus, lauta- ja johtokunnat ovat rekisterinpitäjiä henkilörekisteriasioissa ja vastuualueen/toimintayksikön/liikelaitoksen johtajalla on

yleisvastuu ao. organisaatioyksikön tiedonhallinnasta, tietosuojasta, asiakirjahallinnosta, arkistotoimesta ja resursseista, esimiehet vastaavat yksikkönsä tiedonhallinnasta, asiakirjahallinnosta ja arkistotoimesta ja tietosuojasta, lisäksi toimintaohjeen mukaan jokaisella kaupungin palveluksessa olevalla on vastuu huolehtia tietosuojaan liittyvien asioiden hoitamisesta oman tehtäväalueensa osalta. Tietosuojavastaavalle on määritelty valvontavastuu organisaation henkilörekisterien ja henkilötietojen käsittelyssä noudatettavien menettelyjen osalta.

Tilaajaorganisaatiossa on kaupunginhallituksen hyväksymä tiedonhallintalain mukaisten vastuiden määrittely (Kotkan kaupunki 2020c, 3–4). Vastuiden määrittely ei koske pelkästään tiedonhallintaa vaan myös muussa lainsäädännössä määriteltyjä tiedonhallintaan liittyviä vastuita, esimerkiksi EU:n tietosuoja-asetuksen (EU 679/2016) III ja IV lukujen rekisterinpitäjää koskevien vastuiden määrittelyä. Vastuumäärittelyssä tulee kuvata tietosuoja-asetuksen 30 artiklassa tarkoitetun henkilötietojen käsittelytoimia koskevan selosteen tiedoista vastaavat sekä rekisterinpitäjät tai tietovarannoista vastaavat viranhaltijat tai työntekijät, joilla on kokonaisvastuu rekisterinpidosta (rekisterinpitäjän edustaja) tai tietovarannosta. Tilaajaorganisaation osalta tietosuoja-asetuksen (EU 679/2016) mukaisesta käsittelytoimia koskevasta selosteesta on prosessinomistajilla, jotka toimivat tässä rekisterinpitäjän edustajina. Määrittelyn rekisterinpitäjiä tai tietovarannoista vastaavia koskevassa osassa vastuullisia ja näin rekisterinpitäjän edustajia, ovat prosessien omistajat, sekä vastuualueen tai toimintayksikön johtajat. Tiedonhallintalain mukaisten vastuiden määrittelyssä rekisterinpitäjän edustajien määrittely on toisistaan poikkeava.

Tilaajaorganisaation uudessa 1.8.2021 voimaan tulevassa hallintosäännössä (Kotkan kaupunki 2021a, 20, 21, 24, 39) rekisterinpitäjyys on määritelty lautakunnille sekä Kymenlaakson pelastuslaitoksen liikelaitoksen johtokunnalle. Konsernipalvelualueella on kolme kaupunginhallituksen alaista toimintayksikköä: hallintoyksikkö, henkilöstöasioiden yksikkö sekä talousyksikkö, jotka eivät toimi lautakuntien alaisina. Näiden osalta rekisterinpitäjyys on tutkimusta tehtäessä avoin, mutta rekisterinpitäjyyttä voidaan ohjata uuden hallintosäännön nojalla annettavalla toimintasäännöllä. Tietosuojapolitiikassa (Kotkan kaupunki 2017c) rekisterinpitäjyys on määritelty tilaajaorganisaatiolle, eikä vastuuta ole tarkennettu tietosuojapolitiikan liitteenä olevassa vastuunjakotaulukossa.

Vaikka rekisterinpitäjän rooli on henkilötietojen käsittelyä ja tietosuojaa koskevan lainsäädännön näkökulmasta ollut olemassa pitkään, on sen määrittely organisaatioiden säännöissä uutta ja edellyttää toimiakseen jalkauttamista niin rekisterinpitäjän rollissa toimiville kuin koko henkilöstölle. Kolmannen työpajan jalkautuskokeilu antoi johdolle ja esimiehille

hyvää palautetta konkreettisen lähiesimiehen toimesta annetun jalkautuksen tarpeesta sekä jalkautuksen avulla saadun tiedon vaikutuksesta toimintaan.

7.4 Tietosuojasuunnitelman toteutus

Tietosuojasuunnitelma (Privacy program) on jäsennelty suunnitelma, jonka avulla organisaatio voi täyttää lakisääteiset tietosuojaan kohdistuvat vaatimuksensa. Vahti – raportti (Valtiovarainministeriö 2016) sisältää useita suosituksia toimenpiteistä, joihin organisaation johto voi ryhtyä tunnistaakseen mahdolliset puutteet ja saattaakseen tietosuojan tilan lainsäädännön edellyttämälle tasolle sekä osaksi jokapäiväistä strategialähtöistä operatiivista toimintaa.

Tilaajaorganisaatiolle toteutettu tietosuojasuunnitelman malli perustuu Vahti – raportissa (Valtiovarainministeriö 2016) kuvattuun suunnitelmaan, jota on täydennetty tietosuojalainsäädännön ja kirjallisuuden avulla. Tietosuojasuunnitelma pitää sisällään yhdeksän kohtaa; henkilötieto- ja sopimusinventaario, hallintatoimien riittävyyden riskianalyysi, organisaation tietosuojavastuiden määrittely, johdon raportointi, koulutukset ja ohjeet, dokumentaatio ja viestintä, vaatimusten huomioiminen järjestelmähankkeissa ja -hankinnoissa, sekä järjestelmä- ja sovelluskehityksessä, riskienhallinnan kehittäminen, sekä tietoturvallisuudesta ja toiminnan jatkuvuudesta huolehtiminen.

Tilaajaorganisaation tietosuojaryhmä valitsi työpajatyöskentelyn avulla suunnitelmasta toteutettavan osa-alueen, jonka jälkeen ryhmään kuuluvat johtajat, esimiehet ja muut organisaation sääntöjen mukaan vastuulliset määrittelivät millaisia vastuita, toimenpiteitä tai päätöksiä kunkin rooliin kuului valitulla osa-alueella. Näistä määrittelyistä tuotettiin henkilöstölle jalkautettava päätös, jalkautus toteutettiin linjaorganisaation johtamisjärjestelmän mukaisesti konsernipalvelualueen johtoryhmästä johdon ja esimiehen kautta henkilöstölle, jonka kokemusta jalkautuksesta käsiteltiin kolmannessa työpajassa. Jalkautuksen kohteena oli tilaajaorganisaatiossa käyttöön otettu tietoturvapoikkeaman ilmoituslomake.

Työpajaan osallistunut henkilöstö piti saamansa tietoturvapoikkeaman ilmoituslomakkeen jalkautusta hyödyllisenä ja lomakkeen käyttökynnystä madaltavana. Haasteena koettiin suuri tietomäärä ja erityisesti esimiehen haasteena poimia ja nostaa esille ne asiat, joita henkilöstö ei ehkä ole huomannut intranetin julkaisuista.

Tietosuojasuunnitelman osalta tietosuojapolitiikan (Kotkan kaupunki 2017c) vastuunjakoa koskevassa liitteessä 2 tietosuojasuunnitelman valmisteluvastuu on määritelty tietoturvaorganisaatiolle, joka politiikan mukaan on riskienhallinnan johtoryhmä. Näin ollen tietoturvaorganisaation tehtäväksi jää arvioida ottaako tilaajaorganisaatio sille tehdyn tietosuojasuunnitelman käyttöön.

8 Johtopäätökset

8.1 Pohdinta

Pitkärannan (2014, 15) mukaan tutkiva asennoituminen pitää yllä organisaation tasapainoa sisäisen ja ulkoisen todellisuuden kanssa, jolloin organisaation toimintamallit ja toimintaympäristö ovat vuorovaikutuksessa keskenään. Tutkimuksella rakennetaan väyliä uutteen tietoon, uusiin kokemuksiin ja laajempaan ymmärrykseen, matkataan tulevaisuuteen.

Organisaatioiden johdolle on tarjolla tietoa siitä, kuinka se voi tukea organisaationsa tietosuojavastaavaa, mutta käytettyjen lähteiden perusteella on selkeästi tarve lisätä kansalliseen ohjeistukseen nimenomaan johdolle suunnattua ohjeistusta ja viestintää, jossa kuvataan nykyistä selvemmin organisaation johdon vastuu suhteessa organisaation jokaisen jäsenen vastuisiin. Nykyinen ohjeistus ja viestintä kohdistuvat pääasiassa organisaatiolle sekä tietosuojavastaavalle ja vaikka jokainen onkin vastuussa oman organisaationsa tietosuojan toteutumisesta ei tietosuojan johtaminen voi olla yhteisvastuullista. Organisaation johdon tulee tehdä tietosuojaa koskevat päätökset, tukea rooleja ja toimintoja, joiden tehtäväksi se on antanut päätösten toteuttamisen sekä seurata raportoinnin avulla ovatko tehdyt toimenpiteet riittäviä ja riittävän laadukkaita tietosuojan toteutumiseksi.

Valtioneuvoston kanslian (Pitkänen 2017, 11) teettämän tietosuojasäädösten muutostarpeita koskevassa selvityksessä havaittiin, että Suomen lainsäädäntö on valmiiksi varsin hyvin tietosuoja - asetuksen mukainen. Lainsäädännössä rekisterinpitäjälle ja henkilötietojen käsittelijälle määritellyt velvoitteet ovat nykyisessä tietosuojalainsäädännössä selkeämmin ja kattavammin kuvattuja kuin aikaisemmin. Lainsäädännön toteuttamisen problematiikka ei selvityksen havaintojen perusteella siten olisikaan lainsäädännössä vaan organisaation kyvyssä toteuttaa vaatimukset ja kehittää omaa osaamistaan toteuttamista varten.

Jurmun (2019, 20) väitöskirjatutkimuksen mukaan kuntasektorin muuttuvassa asiantuntijoiden osaamisessa korostuvat tulevaisuudessa erityisesti tiedon hyödyntämisen taidot, viestintä- ja vuorovaikutustaidot, verkostoitumistaidot, kokonaisuuksien hallinta, muutostilanteiden hoitaminen ja johtaminen. Myös substanssiin liittyvää osaamista tarvitaan, mutta sen rooli on tiedon helpon saatavuuden ja verkostojen aikakauden myötä muuttunut. Asiantuntijuuden osa-alueet liittyvät vahvasti eri toimijoiden välisen yhteistyön ja verkostojen merkityksen kasvuun.

Sote uudistuksen myötä syntyvät uudet hyvinvointialueet sekä niitä johtavat aluevaltuustot tuovat julkisen hallinnon johtamiskenttään uuden poliittisen johtamistason (Valtioneuvosto 2021). Jää nähtäväksi, kuinka aluevaltuustot vaikuttavat kuntaorganisaatioiden ja hyvin-

vointialueiden keskinäiseen työnjakoon palveluiden tuottamisessa. Työnjako vaikuttaa suoraan palveluiden henkilötietojen käsittelyyn, joten onkin mielenkiintoista nähdä yhtenevätkö maakuntien tietoturvaa- ja tietosuojaa ohjaavat dokumentit ja syntyykö alueellisia niin sanotusti virallisia tietosuojaryhmiä, joissa määritellään toimintaa laajemmasta näkökulmasta. Useissa maakunnissa on tai on ollut alueellisia epävirallisia tietosuojan yhteistoimintaryhmiä, joilla on pyritty yhtenäisiin toimintatapoihin.

Digitaalisten palveluiden käyttöön ja ylläpitoon liittyy merkittäviä henkilötietojen käsittelyn riskejä, esimerkiksi tietoja voidaan käsitellä laajemmin kuin käyttötarkoituksen mukaan on mahdollista, tietoja voi saada palvelusta rajoittamattomalle määrälle tai käsittelevät henkilöt, joilla ei ole työtehtävään perustuvaa oikeutta käsitellä tietoja, tiedot eivät ole saatavilla tietoliikennehäiriön tai palvelunestohyökkäyksen vuoksi silloin kun niitä tarvitaan, tiedot päätyvät tietomurron seurauksena sivulliselle tai katoavat palvelun tietosisällön tuhoutumisen vuoksi, tietoja säilytetään tarpeettomasti tai pidempään kuin on suunniteltu tai palvelun tietosisältö on vanhentunutta, virheellistä tai puutteellista (Voutilainen 2020, 69-70). Organisaatioiden tulisikin pohtia voiko sen tuottama digitaalinen palvelu toimia ilman, että digitalisaatio rakentuu tietoturvallisiin järjestelmiin, joissa henkilötietojen käsittely on asianmukaisesti suunniteltua ja dokumentoitua?

Tietosuojalainsäädännön noudattamatta jättämisen käytännön vaikutukset voivat tulla organisaatioille yllätyksinä, mikäli tarvittavia henkilötietojen käsittelyn riskien ja vaikutusten arviointeja ei ole tehty. Tietosuojavaltuutetun toimivaltaan (EU 679/2016) 58 artiklan mukaan kuuluvalla oikeudella antaa määräys henkilötietojen käsittelyn rajoittamisesta on organisaation päivittäisen toiminnan kannalta suurempi vaikutus kuin mahdollisella hallinnollisella sakolla. Mikäli organisaation ydintoimintaan liittyvää henkilötietojen käsittelyä joudutaan rajoittamaan tai käsittely joudutaan kokonaan lakkauttamaan, halvaantuu organisaation liiketoiminta siihen saakka, että käsittelyn lainmukaisuuden puutteet on korjattu. Tämä tarkoittaa merkittävää taloudellista vaikutusta ei pelkästään korjaustoimista vaan myös liiketoiminnan keskeytymisestä.

8.2 Vastaukset tutkimuskysymyksiin

Kehittämishankkeen lähtökohdaksi asetettiin tutkimuskysymykset mitä tietosuojan johtaminen tarkoittaa käytännössä, ja mikä on organisaation johdon vastuu tietosuojan toteutumisessa?

Tilaajaorganisaation johtamisjärjestelmää koskevan dokumenttianalyysin tarkoituksena oli selvittää, onko tietosuojan johtamista määritelty ja onko havaittavissa tietosuojan johtamis-

järjestelmä, jonka perusteella on nähtävissä mitä tietosuojan johtaminen tarkoittaa käytännössä. Huttusen (2018, 25) mukaan johtamisjärjestelmä on virallinen ja rakenteellinen kokonaisuus, jossa on määritelty ja organisoitu organisaation toiminnan valtuudet, päätöksenteko sekä asemavalta ja näiden jakautuminen niin vastuualueiden kuin yksittäisten henkilöiden osalta. Johtamisjärjestelmän ja johtamisen organisoitumisen lisäksi johtajuuteen vaikuttavat johdon strategiset linjaukset sekä johtajuus.

Kunnan johtamisjärjestelmä sekä sen sisältö määritellään kuntalaissa tehtäväksi hallintosäännöllä, johon tulisi koota kaikki johtosäännöllä määrättävät asiat, joita aikaisemmin on määritelty valtuuston työjärjestyksessä, hallintosäännössä, toimielinten johtosäännöissä, taloussäännössä ja tarkastussäännössä. Hallintosäännön määräyksiä voidaan jakaa eri asiakirjoihin, kun kunnan organisaation laajuuden vuoksi ei ole tarkoituksenmukaista koota määräyksiä yhteen. Kunnan johtaminen jakaantuu poliittiseen johtamiseen ja ammattijohtamiseen. Poliittisen johtamisen ja päätöksenteon tehtävä on asettaa tavoitteet sekä tehdä päätöksentekoa ohjaavat linjaukset. Ammatillinen johtaminen toimii poliittisen johtamisen ja päätöksenteon apuna vastaten valmistelu- ja täytäntöönpano-organisaation johtamisesta. Johtamisen rakenteiden ja toimintatapojen tulee olla määriteltyjä ja johtamisvastuussa olevien roolien tulee olla selkeitä. Toimintatapoihin ja määrittelyihin tulee sitoutua. Kunnan ylin johto muodostuu valtuustosta, kunnanhallituksesta ja kunnanjohtajasta tai pormestarista. (Myllymäki 2021, 3, 5, 14.)

Vuonna 2021 voimaan tulevassa hallintosäännössä tilaajaorganisaation tietosuojan ja tietoturvan vastuiden määrittelyä on päivitetty siten, että tietosuojan osalta hallintosäännössä määritellään organisaatiossa rekisterinpitäjä -vastuussa olevat tahot, joita ovat lautakunnat, pelastuslaitoksen johtokunta sekä kiinteistörekisteristä vastaava. Rekisterinpitäjyyden vastuu on uusi määrittely hallintosäännössä.

Hallintosäännön ulkopuolella määriteltäväksi jää konsernipalvelualueen kolmen toimintayksikön: hallintoyksikkö, henkilöstöasioiden yksikkö sekä talousyksikkö rekisterinpitäjyys. Ne eivät toimi lautakunnan alaisena, vaan niiden toimintaa ohjaa kaupunginhallitus sellaisilta osin mitä ei ole määritelty hallintosäännössä. Määrittely on mahdollista tehdä hallintosäännön nojalla annettavassa toimintasäännössä.

Hallintosäännön muutoksesta johtuen toimintasääntöjen lisäksi päivitettäväksi tulevat myös tietosuoja- ja tietoturvapolitiikat, joiden lisäksi on hyvä tarkastella myös tiedonhallinnan vastuukuvauksen ajantasaisuus kokonaisuuteen nähden. Organisaatiossa toteutetaankin käytännössä hallintosäännön päivityksellä ja sen perustalla tehtävien muutosten johdosta tietosuojasuunnitelman osaan 5.3 Organisaation tietosuojavastuut kuuluvia toimenpiteitä.

Vastuiden määrittelyn jälkeen organisaation tietosuojasta vastaava johto voi päättää kehittämishankkeessa luodun tietosuojasuunnitelman mallin käyttöönottamisesta ja toteuttamisesta, aikatalutusta ja toteutuksesta sekä sen raportoinnista vastaavista tahoista.

Toisena tutkimuskysymyksenä oli, mikä on organisaation johdon vastuu tietosuojan toteutumisessa?

Tässä opinnäytetyössä käytettyjen lähteiden perusteella voidaan havaita, että vastuu tietosuojasta ja tietoturvasta kuvataan politiikoissa kokonaisuudelle, eli organisaatiolle tai oikeushenkilölle ja varsinaisten vastuutahojen määrittely edellyttää organisaation johtamisjärjestelmän ja siihen liittyvä dokumentaatio kokonaisuuden hallintaa sekä organisaation toimijoiden hyvää tuntemusta. Nämä tiedot yhdistäen vastuutaho tai tahot ovat pääteltävissä. Johtamisjärjestelmän koostuminen useista dokumenteista ja vastuun kuvaaminen passiivimuodossa organisaatiolle, ei vastaa EU:n yleisen tietosuoja-asetuksen (EU 679/2016) 39 resitaalin läpinäkyvyyden periaatetta, jonka mukaan henkilötietojen käsittelyyn liittyvien tietojen on oltava helposti saatavilla ja ymmärrettävässä muodossa.

Vaikka jokainen onkin osaltaan vastuussa tietosuojan toteutumisesta ei tietosuojan johtaminen voi olla yhteisvastuullista. Organisaation johdolla on vastuu toiminnan suunnittelusta, määrittelystä sekä ohjeistamisesta. Tätä vastuuta johto ei voi ulkoistaa organisaatiolle tai tietosuojavastaavalle.

Tilaajaorganisaatiolle tuotetussa tietosuojasuunnitelman mallissa on pyritty konkretisoimaan ja kuvaamaan organisaation johdon vastuulla olevat toimenpiteet ja päätökset, joiden avulla tietosuojan johtaminen toteutetaan. Tietosuojan johtaminen on osa organisaation johtamisjärjestelmän toimintaa, jossa organisaation ylin johto määrittelee ylimmän tietosuojasta tilivelvollisen tahon ja tämä nimeää tietosuojan toimeenpanon kokonaisuudesta vastuulliset. Tietosuoja ei ole irrallinen toiminto, vaan osa jokaisen henkilötietoja käsittelevän organisaation toimintaa.

Tilaajaorganisaation hallintosäännössä kuvatut tietosuojaan liittyvät vastuut sitovat tietosuojan osaksi organisaation johtamisjärjestelmää. Johdon tulee kuitenkin arvioida tietosuojan johtamisen vastuita kokonaisuutena ja varmistaa, että toimintasääntöjen, politiikkojen ja muiden määrittelyjen päivityttyä tietosuojan kokonaisvastuullinen sekä osavastuulliset ja näiden tehtävät ja tietosuojavastaavan rooli ovat nähtävissä nykyistä selvemmin.

8.3 Kehittämishankkeen arviointi

Tämän tutkimuksellisen kehittämishankkeen suunnittelu ja toteutus perustuivat tutkimusmetodiksi valittuun laadullisen tutkimuksen menetelmään, jossa käytettiin toimintatutkimuksen, eli tutkimuksellisen kehittämistoiminnan keinoja. Kehittävässä tutkimuksessa konkreettista kehittämistoimintaa lähestytään tutkimuksellisen kysymyksenasettelun ja metodologisen tarkastelun kautta.

Laadullisen tutkimuksen luotettavuuskriteeristö koostuu Kanasen (2014, 150–154) mukaan vahvistettavuudesta, arvioitavuudesta tai dokumentaatiosta, tulkinnan ristiriidattomuudesta, luotettavuudesta ja saturaatiosta. Aineistoon perustuvassa laadullisessa tutkimuksessa vahvistettavuutta parannetaan keräämällä aineistoa eri lähteistä ja vertaamalla saatua tietoa tutkijan omaan tulkintaan katsoen tuottaako eri tietolähteet toisiaan tukevia tuloksia. Verrattavat lähteet voivat olla tutkimuksen aikana kerättyjä erilähteisiä tai eri muotoisia aineistoja. Tutkimuksen arvioitavuutta voidaan lisätä tutkimuksessa tehtyjen ratkaisujen dokumentaatiolla, jossa kuvataan tiedonkeruu ja analysointimenetelmiä sekä näiden perustelut. Tulkinnan ristiriidattomuudessa, eli sisäisessä validiteetissa eri lähteistä kerätyn tutkimusaineiston tulkinta tehdään monilähteisenä synteesinä. Samasta tutkimusaineistosta voidaan saada erilaisia tukintoja tarkastelukulmasta, tutkimusongelmasta, teemoittelusta ja koodaamisesta riippuen. Saturaatiossa eri lähteistä saadut tutkimustulokset alkavat toistua, kun havainnointia tehdään riittävän laajaan aineistoon. Tutkimuksessa otetaan uusia havaintoyksikköjä niin kauan kuin ne tuovat uutta tietoa tutkimukseen, kun vastaukset alkavat toistua on saavutettu saturaatio.

Tutkimuksen teoria-aineiston hankinnassa on lähdeaineistojen laajuudella pyritty varmistamaan erilaisten näkökulmien esille tuleminen niin johtamisen teorian kuin tietoturvan ja tietosuojankin osalta. Lähdeaineistona käytettiin uusinta kirjallisuutta ja tutkimusta, ellei erityisesti ollut tarpeen kuvata teemaa tai ilmiötä sen historian näkökulmasta. Vanhempaa lähdeaineistoa on käytetty perustellusti silloin, kun tieto on ollut tarpeellinen teeman tai ilmiön kokonaisuuden kuvaamisen kannalta, esimerkiksi tietoturvan ja osaamisen johtamisen teoriaosuudessa, joissa käsitellään teemojen perusteita. Aineistoanalyysissä havainnoitiin tilaajaorganisaation johtamisjärjestelmään kuuluva dokumentaatio, yhteensä kaksikymmentä neljä dokumenttia, jotka koostuivat voimassa olevasta hallintosäännöstä, sen perusteella annetuista kahdestatoista toimintasäännöstä, myöhemmin voimaan tulevasta hallintosäännöstä, konserniohjeistuksesta, henkilöstöohjelmasta, tiedonhallinnan vastuita koskevasta määrittelystä, asiakirjahallinnon ja arkistotoimen toimintaohjeesta sekä tietoturva ja tietosuojapolitiikoista.

Tutkimuksen työpajoista ja aineistoanalyysistä on pidetty havainnointipäiväkirjaa, johon on kuvattu aineistoanalyysissä arvioidut aineistot, havainnot, analyysikierrosten valinnat, koodaustavat sekä teemat ja käytetyt koodit ja tietojen yhdistelyn lopputulokset, sekä työpajojen vaiheet, sisällöt, lopputulokset ja havainnot. Tutkimuksen arvioitavuuden osalta tulee huomioida, että tutkimuksen tulokset ovat vahvasti organisaatio ja aikasidonnaisia. Tutkimuksessa analysoitu tilaajaorganisaation dokumentaatio on muuttumisvaiheessa. Analyysissä on käytetty tutkimushetkellä voimassa olevaa hallintosääntöä ja sen perusteella annettuja toimintasääntöjä ja politiikkoja, mutta uuden hallintosäännön tultua voimaan 1.8.2021 hallintosääntö muuttaa tietosuojan ja tietoturvan vastuita ja sen nojalla annetut toimintasäännöt sekä tietoturva- ja tietosuojapolitiikat tulevat muuttumaan.

Tutkimuksen tulkinnan ristiriidattomuutta on pyritty turvaamaan tietosuojaan, tietoturvaan ja johtamiseen rajatuilla tutkimuskysymyksillä, sekä kehittämishankkeen seurannalla tilaajaorganisaation tietosuojaryhmässä koko tutkimusprosessin ajan. Tutkimuksen luotettavuuden näkökulmasta tutkijan kuuluminen tietosuojaryhmään voisi tarkoittaa puolueellisuutta, mutta tutkijalla ei ole organisatorisen asemansa puitteissa mahdollisuutta vaikuttaa tutkimuksen tietosuojasuunnitelman käytännön toteutukseen, työpajoissa toteutettuun suunnitelman osan käyttökokeiluun tai organisaation johtamisjärjestelmää ohjaavien sääntöjen ja määräysten sisältöön. Kehittämishankkeen kohteena olevan tietosuojasuunnitelman sekä siihen liittyvän johtamisvastuun toimivuutta testattiin kolmella työpajalla. Osallistavassa työpajatyöskentelyssä osallistujille annettiin pohjatiedot sekä työpajatyöskentelyyn sopiva järjestelmäalusta, jolla osallistujat toteuttivat työpajalle suunnitellun sisällön mukaiset toimenpiteet itsenäisesti ilman tutkijan ohjausta ja vaikutusta lopputulokseen. Koska tutkija on osa tilaajaorganisaation tietosuojaryhmää, tällä työpajametodilla pyrittiin varmistamaan työpajojen tulosten objektiivisuus.

On kuitenkin syytä huomioida, että ensimmäisestä työpajasta puuttui yksi johdon edustaja, toisesta työpajasta tietosuojavastaava ja kolmannesta työpajasta yksi henkilöstön edustajista. Ensimmäisessä työpajassa osallistujat valitsivat jatkokäsiteltävän tietosuojasuunnitelman osa-alueen tekemällä kukin 1 - 3 valintaa ja näin saadun valintaluettelon kunkin valinnan saamat ”äänet” laskettiin. Valintaan osallistujia oli kuusi, valittu osa-alue sai viisi ääntä ja seuraava kolme, jolloin yhden henkilön äänestystuloksella ei olisi ollut merkittävää vaikusta tulokseen. Toisessa työpajassa osallistujat kirjasivat valittuun osa-alueeseen liittyviä vastuitaan tai päätöksiä. Valittu osa-alue oli tietoturvallisuudesta ja toiminnan jatkuvuudesta huolehtiminen, jonka toteutumisessa tietosuojavastaavalla ei ole erityistä roolia tai vastuuta, joten poissaololla ei ollut merkittävää vaikutusta työpajan lopputulokseen. Kolmannessa työpajassa arvioitiin keskustelun avulla toisen työpajan valinnan tuloksena päätetty tietotur-

vapoikkeamalomakkeen jalkautus talousyksikön henkilöstölle. Työpajasta poissa ollut henkilöstön edustaja on tilaajaorganisaation tietosuojaryhmän jäsen ja osallistunut siten kahteen edelliseen työpajaan ja ollut tietoinen viimeisen työpajan aiheesta. Poissaololla ei ollut merkitystä työpajassa käytyyn keskusteluun ja lopputulokseen.

8.4 Jatkotutkimus

Kehittämistehtävän puitteissa ei voitu toteuttaa koko tietosuojasuunnitelmaa, joten sen lopputulokset ja hyödyt jäivät vielä avoimiksi. Lisäksi organisaatio on ottamassa käyttöön uutta hallintosääntöä (08/2021), jolla tulee olemaan vaikutusta tietosuojan toteuttamisen vastuisiin.

Jatkotutkimuksena voisikin tilaajaorganisaation osalta olla tietosuojasuunnitelman toteuttamisen vaikutus organisaation tietosuojatoimintaan, esimerkiksi tietosuojan tasoon kohdistuvana seurantatutkimuksena, jossa kartoitetaan tietosuojan nykytila ennen ja jälkeen tietosuojasuunnitelman toteuttamista tai johtamisen jatkotutkimus, jossa kartoitetaan muuttuiko tietosuojan johtaminen vuonna 2021 annetun hallintosäännön ja sen perusteella annettujen muiden sääntöjen, ohjeiden ja politiikkojen johdosta.

Tilaajaorganisaation ulkopuolelta tutkimuskohteena voisi olla esimerkiksi dokumenttitutkimus kansallisesta ohjeistuksesta ja johdon roolin kuvaamisesta näissä ohjeissa tai tutkimus tietosuojajohtamisen laadusta ja vaikuttavuudesta.

Lähteet

Alasoini, T. 2016. Workplace Development Programmes as Institutional Entrepreneurs - Why They Produce Change and Why They Do Not. Aalto Yliopisto. Viitattu 28.5.2021. Saatavissa http://urn.fi/URN:ISBN:978-952-60-6625-7

Andreasson, A., Koivisto, J., Ylipartanen, A. 2014a. Tietosuojavastaavan käsikirja 1. Helsinki: Tietosanoma Oy

Andreasson, A., Koivisto, J., Ylipartanen, A. 2014b. Tietosuojavastaavan käsikirja 2. Helsinki: Tietosanoma Oy

Andreasson, A., Koivisto, J., Ylipartanen, A. 2015. 1. painos. Tietosuojakäsikirja johdolle. Helsinki: Tietosanoma Oy

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

Arene. 2020a. Ammattikorkeakoulujen opinnäytetöiden eettiset suositukset. Viitattu 22.7.2021. Saatavissa https://www.arene.fi/julkaisut/raportit/opinnaytetoiden-eettiset-suositukset/

Arene. 2020b. Vastuullinen opinnäytetyö. Viitattu 22.7.2021. Saatavissa https://www.arene.fi/julkaisut/raportit/opinnaytetoiden-eettiset-suositukset/

Bärlund, A., Perko, S. 2013. Kestävä johtajuus: bisneksen uusi elinehto. Helsinki: Talentum. Viitattu 3.4.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/b5ag28/alma991890523906254

Cisco Cybersecurity Series 2020. From Privacy to Proft: Achieving Positive Returns on Privacy Investments. Cisco Data Privacy Benchmark Study. Viitattu 16.1.2021. Saatavissa https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf

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). Viitattu 14.3.2021. Saatavissa https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679

Euroopan tietosuojaneuvosto, The European Data Protection Board (EDPB). 2021. Register of approved binding corporate rules. Viitattu 3.4.2021. Saatavissa https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en

Guan, B., Hsu, C. 2020. The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. Internet research. 30 (5), 1383–1405. Viitattu 27.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1hujjmv/cdi_crossref_primary_10_1108_INTR_06_2019_0260

Guhr, L. 2019. The impact of leadership on employees' intended information security behaviour: An examination of the full- range leadership theory. Information systems journal. Oxford, England. 29 (2), 340–362. Viitattu 4.4.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1n6in9k/cdi_proquest_journals_2177032676

Haapalehto, S. Tietosuojavastaavan nimittäminen, tehtävät ja asema. Yleiskirje 6/2018. Suomen Kuntaliitto. Viitattu 6.2.2021. Saatavissa https://www.kuntaliitto.fi/yleiskirjeet/2018/tietosuojavastaavan-nimittaminen-tehtavat-ja-asema

Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi HE 284/2018 vp. Viitattu 6.2.2021. Saatavissa https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_284+2018.pdf

Henkilörekisterilaki 471/1987. Viitattu 14.3.2021. Saatavissa https://www.finlex.fi/fi/laki/alkup/1987/19870471#Pidp446549040

Henkilötietolaki 523/1999. Viitattu 14.3.2021. Saatavissa https://www.finlex.fi/fi/laki/alkup/1999/19990523

Halme, J. 2018. Aivoriihi - toteutus ja perusperiaatteet. Orchidea Innovations. Viitattu 14.3.2021. Saatavissa https://info.orchideainnovations.com/innovaatio-blogi/aivoriihi

Huhtala, M. 2015. Asennejohtaja: arjen työkalut esimiehille. Helsinki: Kauppakamari. Viitattu 23.5.2021. Saatavilla https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/b5ag28/alma991567083906254

Huttunen, T. 2018. Johdetaan yhdessä - Hypeä vai työpaikan todellisuutta. Helsingin seudun kauppakamari. Viitattu 4.4.2021. Saatavissa https://kauppakamaritieto-fi.ezproxy.saimia.fi/ammattikirjasto/teos/johdetaan-yhdessa-2018#/kohta:Johdetaan((20)yhdess((e4)

Jabe, M. 2017. Erilaisten ihmisten johtaminen. 1. painos. Helsinki: Helsingin Kamari Oy / Helsingin seudun kauppakamari. Viitattu 18.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991638763906254

JHS – sanasto. Viitattu 16.1.2021. Saatavissa http://jhs-sanasto.jhs-suositukset.fi/JHS/fi/

Jurmu, L. 2019. Millaista asiantuntijuutta uudistuvissa kunnissa tarvitaan? Viitattu 27.7.2021. Saatavissa http://urn.fi/URN:NBN:fi:tuni-202004294473

Järvinen, P., Rousku, K. 2017. Työpaikan tietoturvaopas: tunnista uhat, hallitse riskit. Lietua: Talentum Media Oy. Viitattu 2.4.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991891003906254

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu

Kauhanen, J. 2018. Esimies tuottavuuden kehittäjänä. 1. painos. Helsinki: Kauppakamari. Viitattu 23.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991685603906254

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

Kotkan kaupunki. 2017a. Asiakirjahallinnon ja arkistotoimen toimintaohje 2017. Viitattu 7.7.2021. Saatavissa https://www.kotka.fi/kotkan-kaupunki/ohjeet-ja-saadokset/kaupunginhallituksen-antamat-toimintasaannot/

Kotkan kaupunki. 2020a. Hallintosääntö 3. Viitattu 20.7.2021. Saatavissa https://www.kotka.fi/kotkan-kaupunki/ohjeet-ja-saadokset/hallintosaanto/

Kotkan kaupunki. 2021a. Hallintosääntö 5. Viitattu 21.7.2021. Saatavissa https://www.kotka.fi/kotkan-kaupunki/ohjeet-ja-saadokset/hallintosaanto/

Kotkan kaupunki. 2018. Henkilöstöohjelma 2025. Viitattu 12.7.2021. Saatavissa http://hepake.kotka.fi/esimies/yleista/KOTKA2025Henkil%C3%B6st%C3%B6ohjelma.pdf

Kotkan kaupunki. 2020b. Kaupunginhallituksen alaisten toimintojen toimintasääntö 2020. Viitattu 22.7.2021. Saatavissa https://www.kotka.fi/kotkan-kaupunki/ohjeet-ja-saadokset/kaupunginhallituksen-antamat-toimintasaannot/

Kotkan kaupunki. 2017b. Konserniohje. Viitattu 23.7.2021. Saatavissa https://www.kotka.fi/kotkan-kaupunki/ohjeet-ja-saadokset/kaupunginhallituksen-antamat-toimintasaannot/

Kotkan kaupunki. 2021b. Määräykset, säännöt ja ohjeet. Viitattu 23.7.2021. Saatavissa https://www.kotka.fi/kotkan-kaupunki/ohjeet-ja-saadokset/hallintosaanto/

Kotkan kaupunki. 2021c. Esityslistat ja pöytäkirjat. Viitattu 23.7.2021. Saatavissa http://hallijulkaisu.kotka.fi/ktwebbin/dbisa.dll/ktwebscr/epj_tek_tweb.htm

Kotkan kaupunki. 2019. Sisäisen tarkastuksen toimintasääntö 2019. Viitattu 23.7.2021. Saatavissa https://www.kotka.fi/kotkan-kaupunki/ohjeet-ja-saadokset/kaupunginhallituksen-antamat-toimintasaannot/

Kotkan kaupunki. 2020c Tiedonhallintalain mukaisten vastuiden määrittely. Kh 28.9.2020 § 273. Viitattu 21.7.2021. Saatavissa http://hallijulkaisu.kotka.fi/ktwebbin/dbisa.dll/ktwebscr/epj_asil_tweb.htm?+bid=11081

Kotkan kaupunki. 2017c. Kotkan kaupungin tietosuojapolitiikka. Viitattu 22.7.2021. Saatavissa https://docplayer.fi/71310900-Tietosuojapolitiikka.html.

Kotkan kaupunki. 2021d. Tietotilinpäätös 2020. Viitattu 23.7.2021. Saatavilla http://hallijulkaisu.kotka.fi/ktwebbin/dbisa.dll/ktwebscr/pk_asil_tweb.htm?+bid=11914

Kotkan kaupunki. 2017d. Kotkan kaupungin tietoturvapolitiikka. Viitattu 22.7.2021. Saatavissa https://docplayer.fi/70640347-Tietoturvapolitiikka.html.

Kuitunen, M., Sutinen, M. 2018. Mahtava moka: uskalla, opi ja menesty. Helsinki: Alma Talent. Viitattu 29.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991890613906254

Kuntalaki 410/2015. Viitattu 10.6.2021. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2015/20150410#O2L4P14

Kupias, P. ym. 2013. Onnistu palautteessa. Helsinki: Talentum. Viitattu 26.6.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991641923906254

Laihonen, H., Hannula, M., Helander, N., Ilvonen, I., Jussila, J., Kukko, M., Kärkkäinen, H., Lönnqvist, A., Myllärniemi, J., Pekkola, S., Virtanen, P., Vuori, V.,Yliniemi, T., 2013. Tietojohtaminen. Tampereen teknillinen yliopisto, Tietojohtamisen tutkimuskeskus Novi

Laki digitaalisten palvelujen tarjoamisesta 306/2019. Viitattu 27.6.2021. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2019/20190306#L2P5

Laki julkisen hallinnon tiedonhallinnasta 906/2019. Viitattu 7.2.2021. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2019/20190906

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007. Viitattu 16.7.2021. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2007/200701599

Laki viranomaisten toiminnan julkisuudesta 621/1999. Viitattu 7.2.2021. Saatavissa https://finlex.fi/fi/laki/ajantasa/1999/19990621

Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista 661/2009. Viitattu 30.5.2021. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2009/20090661#L4

Lautjärvi, H. 2018. Business crime: yritysjohdon miinakenttä. Helsinki: Edita Publishing Oy. Viitattu 18.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991980773906254

Leclin, O. 2006. Laatu yrityksen menestystekijänä. Helsinki: Talentum.

Leclin, O., Laine, R.O. 2009. Laadunkehittäjän työkalupakki: Innovatiivisen johtamisjärjestelmän rakentaminen. Helsinki: Talentum.

Luukka, P. 2019. Yrityskulttuuri on kuningas: mikä, miksi, miten? Helsinki: Alma Talent. Viitattu 7.4.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991891103906254

Myllymäki, R. 2020. Kunnan hallintosääntö. Suomen kuntaliitto. Viitattu 24.1.2021. Saatavissa https://www.kuntaliitto.fi/julkaisut/2020/2072-kunnan-hallintosaanto

Myllymäki, R. 2021. Kunnan hallintosääntö. 2. uudistettu, täydennetty painos. Suomen kuntaliitto. Viitattu 28.7.2021. Saatavissa https://www.kuntaliitto.fi/julkaisut/2021/2072-kunnan-hallintosaanto

Mähönen, J. T. 2019. Osuuskuntien ohjaaminen kestävään liiketoimintaan: laki vai hallinnointikoodi, vai jotain muuta? Defensor Legis: Suomen asianajajaliiton äänenkannattaja, Vuosikerta. 100, Nro 4, Sivut 443-461. Viitattu 24.1.2021. Saatavissa http://hdl.handle.net/10138/305852

Mäenpää, O. 2021. Hallinto-oikeus. Helsinki: Talentum Media. Viitattu 4.4.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991596683906254

Oikeusministeriö. 2017. EU:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö. Julkaisunumero: 35/2017. Viitattu 16.1.2021. Saatavissa http://urn.fi/URN:ISBN:978-952-259-612-3

Osakeyhtiölaki 624/2006. Viitattu 10.6.2021. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2006/20060624#O2L5P1

Otala, L. 2018. Ketterä oppiminen: keino menestyä jatkuvassa muutoksessa. Helsinki: Helsingin Kamari Oy / Helsingin seudun kauppakamari. Viitattu 25.6.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991697833906254

Pirinen, A. 2014. Tietoturvallisuuden organisointi. Bonnier Pro (LAB). Bonnier Pro. Viitattu 4.4.2021. Saatavissa http://bonnierpro.fi.ezproxy.saimia.fi/fi/app/tietohallinto/tietoturvallisuuden-organisointi

Pirinen, H. 2015 Esimies muutoksen johtajana. Helsinki: Alma Talent. Viitattu 23.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991639783906254

Pitkänen, O. 2017. Tietosuojasäädösten muutostarve. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 41/2017. Viitattu 17.1.2021. Saatavissa http://urn.fi/URN:ISBN:978-952-287-389-7

Pitkäranta, A. 2014 Laadullinen tutkimus opinnäytetyönä: työkirja ammattikorkeakouluun. Jokioinen: e-Oppi. Viitattu 25.7.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/b5ag28/alma991599453906254

Puusa, A., Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Tallinna: Gaudeamus

Ratsula, N. 2016. Compliance – Eettinen ja vastuullinen liiketoiminta. Liettua: Talentum Media Oy

Ratsula, N., Ratsula, N. 2021. Sisäinen valvonta: käsikirja tulokselliseen organisaation ohjaukseen. Helsinki: Edita.

Riikonen, J. 2013. Johdon tuki tietosuojavastaavalle terveydenhuollon organisaatiossa. Itä-Suomen yliopisto. Viitattu 2.1.2021. Saatavissa http://urn.fi/urn:nbn:fi:uef-20130581

Rikosuhripäivystys.2021. Vastaamon tietomurto – Neuvoja uhreille. Viitattu 25.6.2021. Saatavissa https://www.riku.fi/toimi-nain-jos-tietojasi-on-vuodettu-verkkoon/

Rousku, K. 2018. Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma. Valtiovarainministeriön julkaisuja 32/2018. Viitattu 9.4.2021. Saatavissa http://urn.fi/URN:ISBN:978-952-251-975-7

Rousku, K. 2017. Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. Viitattu 23.1.2021. Saatavissa http://urn.fi/URN:ISBN:978-952-251-862-0

Seppo, T. 2020. Valmistaudu tiedonhallintalain ja digipalvelulain velvoitteisiin - työvälineitä tarjolla. Kuntaliitto. Ajankohtaista. Viitattu 27.6.2021. Saatavilla https://www.kuntaliitto.fi/ajankohtaista/2020/valmistaudu-tiedonhallintalain-ja-digipalvelulain-velvoitteisiin-tyovalineita

Silvola, H., Landau, T. 2019. Vastuullisuudesta ylituottoa sijoituksiin. Helsinki: Alma Talent. Viitattu 18.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991891033906254

Solomon, C. 2020. RACI 2.0: Use RACI to Avoid the 3 Pitfalls That Make It Almost Impossible for Teams to Perform. RACI Solutions Whitepaper. Viitattu 27.5.2021. Saatavissa https://www.racisolutions.com/free-raci-whitepaper

Sumkin, T., Tuomi, L. 2012. Osaamisen ja työn johtaminen: organisaation oppimisen oivalluksia. 1. p. Helsinki: Talentum Media. Viitattu 22.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991642063906254

Sydänmaanlakka, P. 2015. Älykäs julkinen johtaminen: miten rakentaa älykäs verkostoyhteiskunta? Helsinki: Talentum Pro. Viitattu 4.4.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991891113906254

Tienari, J., Harviainen, J. T. 2020. Strategiaopas kuntien päättäjille: osallista ja hallitse. Helsinki: Alma Talent Oy. Viitattu 22.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/b5ag28/alma9919882731062 54Tietosuojalaki 1050/2018. Viitattu 14.3.2021. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Tietosuojavaltuutetun toimisto. 2012. Laadi tietotilinpäätös. Viitattu 8.2.2021. Saatavissa https://tietosuoja.fi/julkaisut

Tietosuojavaltuutetun toimisto. 2018. Tietosuojavaltuutetun päätös luetteloksi käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi. Viitattu 8.5.2021. Saatavissa https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2021a. Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä. Viitattu 14.3.2021. Saatavissa https://tietosuoja.fi/tietosuoja

Tietosuojavaltuutetun toimisto. 2021b. Tietosuojavaltuutetun toimisto pyytää kommentteja uudesta tietosuojan vaikutustenarviointia koskevasta ohjeesta. Viitattu 24.8.2021. Saatavissa https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-pyytaa-kommentteja-uudesta-tietosuojan-vaikutustenarviointia-koskevasta-ohjeesta

Theseus. 2021. Tietosuoja - opinnäytetyöt. Viitattu 27.6.2021. Saatavissa https://www.theseus.fi/discover?filtertype_1=nimeke&filter_relational_operator_1=contains&filter_1=tietosuoja&query=tietosuoja&scope=%2F

Toikko, T., Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta: näkökulmia kehittämisprosessiin, osallistamiseen ja tiedontuotantoon. Tampere University Press. Viitattu 5.2.2021. Saatavissa http://urn.fi/URN:ISBN:978-951-44-7732-4

Tuomi, J., Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki: Kustannusosakeyhtiö Tammi. Viitattu 26.7.2021.

Työturvallisuuslaki 738/2002. Viitattu 14.4.2021. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2002/20020738

Valtioneuvosto. 2021. Mikä on hyvinvointialue? Viitattu 14.8.2021. Saatavissa https://libguides.lut.fi/LABlahdeviittaus

Valtiovarainministeriö. 2004. Tietoturvallisuus ja tulosohjaus. Valtiovarainministeriön julkaisuja 2/2004. Viitattu 30.5.2021. Saatavissa https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22004-tietoturvallisuus-ja-tulosohjaus

Valtiovarainministeriö. 2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. Valtiovarainministeriön julkaisuja 6/2006. Viitattu 30.5.2021. Saatavissa https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-62006-tietoturvatavoitteiden-asettaminen-ja-mittaaminen

Valtiovarainministeriö. 2016. EU-tietosuojan kokonaisuudistus VAHTI-raportti 1/2016. Viitattu 15.2.2021. Saatavissa http://urn.fi/URN:ISBN:978-952-251-778-4

Valtiovarainministeriö. 2017a. Tietoturvapoikkeamatilanteiden hallinta. Valtiovarainministeriön julkaisuja 8/2017. Viitattu 14.2.2021. Saatavissa http://urn.fi/URN:ISBN: 978-952-251-930-6

Valtiovarainministeriö. 2017b. Tietosuojan yhteishankkeet. Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) ja julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) yhteishankkeet 2017–2018. Viitattu 13.3.2021. Saatavissa https://vm.fi/tietosuojan-yhteishankkeet

Valtiovarainministeriö. 2020. Julkisen hallinnon digitaalinen turvallisuus. Valtiovarainministeriön julkaisuja 23/2020. Viitattu 10.6.2021. Saatavissa http://urn.fi/URN:ISBN:978-952-287-857-1

Valtiovarainministeriö. 2020. Suositus tiedonhallintamallista. Valtiovarainministeriön julkaisuja 29/2020. Viitattu 27.6.2021. Saatavissa http://urn.fi/URN:ISBN:978-952-367-328-1

Viitala, R. 2005. Johda osaamista!: Osaamisen johtaminen teoriasta käytäntöön. Helsinki: Inforviestintä.

Virtanen, P. ym. 2015. Tiedolla johtaminen hallinnossa: teoriaa ja käytäntöjä. Tampere: Tampere University Press.

Virtanen, P., Stenvall, J. 2019. Julkinen johtaminen. 2., uudistettu laitos. Helsinki: Tietosanoma.

Voutilainen, T. 2019. Oikeus tietoon: informaatio-oikeuden perusteet. 2., uudistettu painos. Helsinki: Edita Publishing Oy. Viitattu 2.4.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991980772906254

Voutilainen, T. 2020. Digitaalisten palvelujen sääntely. Helsinki: Alma Talent.

Vuorinen, T. 2013. Strategiakirja: 20 työkalua. Helsinki: Talentum. Viitattu 22.5.2021. Saatavissa https://lut.primo.exlibrisgroup.com/permalink/358FIN_LUT/1mu4kem/alma991890853906254

Väestörekisterikeskus, Digiturvapalvelut. 2019. Digiturvaopas – Judo - hanke sekä digitaalinen turvallisuus toiminnan mahdollistajana. JUDO - hanke | Digiturvan yhteishanke 2019-2021. Viitattu 13.2.2021. Saatavissa https://dvv.fi/documents/2252790/13076333/Digiturvaopas_1206_2019.pdf/f8d7e2ab-7395-2e4a-88e9-291cea4d0b41/Digiturvaopas_1206_2019.pdf

Liite 1. Tietosuojaan liittyvät käsitteet

Käsite	Kuvaus
Digitaalinen turvallisuus	Digitaalinen turvallisuus koostuu riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyvistä turvallisuuden kehittämistoimenpiteistä.
Henkilötieto	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto). Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.
Henkilötietojen käsittelijä	Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.
Henkilötietojen käsittely	Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.
Henkilötietojen käsittelyn vaikutustenarviointi	Ennen vaikutustenarviointia rekisterinpitäjän tulee tehdä käsittelyn riskienarviointi. Jos henkilötietojen käsittely todennäköisesti aiheuttaa yksilön oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ennen käsittelytoimien aloittamista toteutettava tietosuojan vaikutustenarviointi ja määriteltävä toimenpiteitä, joilla riskiä voidaan hallita.

	Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen.
Henkilötietojen tietoturvaloukkaus	Tietoturvaloukkaus, jonka seurauksena on henkilötietojen lainvastainen käsittely. Loukkauksesta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.
Jäännösriski	Riskiin käsittelyn jälkeen jäävä riski, jota ei voida tai ei haluta poistaa. Jäännösriskeihin voi sisältyä tunnistamattomia riskejä.
Kyberturvallisuus	Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan (organisaatiolle tai yhteiskunnalle) merkittävien ICT-toimintojen häiriöihin. Se yhdistää laaja-alaisesti riskienhallinnan, tietoturvallisuuden, tietosuojan, jatkuvuuden hallinnan, sekä varautumis- ja toipumissuunnittelun kokonaisuuksia
Osoitusvelvollisuus	Osoitusvelvollisuuden (”accountability”) avulla organisaation tulee kyetä osoittamaan, että se on huolehtinut seuraavista henkilötietojen käsittelyn osa-alueista: • lainmukaisuus, kohtuullisuus ja läpinäkyvyys • käyttötarkoitussidonnaisuus • tietojen minimointi • täsmällisyys • säilytyksen rajoittaminen ja • eheys ja luottamuksellisuus.
Pseudonymisointi	Henkilö tietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot tulee säilyttää erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei tällaista yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu.

Rekisterinpitäjä	Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
Rekisteröity	Henkilö, jonka henkilötietoja käsitellään.
Rekisteröidyn informointi (Henkilötietolaissa rekisteriseloste, rinnakkainen termi tietosuojaseloste)	Dokumentti, jossa rekisterinpitäjä kuvaa henkilötietojen käsittelyn perusteet ja tavat tiiviissä, avoimessa ja helposti ymmärrettävässä muodossa. Dokumentti tulee pitää yleisesti saatavilla.
Riskienhallinta	Järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet.
Tietosuoja	Ihmisten yksityisyyden suojeleminen ja yksilöä koskevien tietojen suojaaminen oikeudettomalta käytöltä henkilötietoja käsiteltäessä.
Tietosuojavastaava	Tietosuoja-asetuksen määrittelemä rooli, jonka rekisterinpitäjän ja henkilötiedon käsittelijän on nimettävä asetuksessa määritellyissä tilanteissa.
Tietoturvallisuus / tietoturva	Tiedon luottamuksellisuuden, eheyden ja saatavuuden takaaminen teknisten ja organisatoristen toimenpiteiden ja menettelyjen avulla.
Tietoturvaloukkaus / henkilötietojen tieoturvaloukkaus	Tietoturvaloukkaus, jonka seurauksena on henkilötietojen lainvastainen käsittely. Loukkauksesta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.
Varautuminen	Toiminta, jolla varmistetaan tehtävien häiriötön hoitaminen sekä mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa.

(Valtiovarainministeriö 2016, 10-13; Valtiovarainministeriö 2020, 16-17)

Liite 2. Henkilöstön työpajan yhteenveto

Seuraavassa on kirjattu yhteenvetoja henkilöstön työpajassa esitettyjen kysymysten tiimoilta käydystä keskustelusta:

Olitko huomannut tietoturvaloukkauksen ilmoituslomakkeen Intrassa?

Osa oli huomannut lomakkeen, mutta enemmistöllä yksikön henkilöstöstä ei ollut havaintoa lomakkeesta. Kun asia tuli tiedoksi talousyksikön viikkopalaverissa esimiehen sijaisena kokouksessa olleelta 31.5.2021 asia käytiin läpi alustavasti ja sovittiin tarkempi läpikäynti 7.6.2021 viikkopalaveriin. Yksi henkilö otti lomakkeen heti 31.5.2021 jälkeen käyttöön.

Olisitko tiennyt milloin ja miten lomaketta käytetään?

Yhdelle toimintatapa oli tuttu aikaisemmista työpaikoista, mutta suurimmalle osalle asia oli uusi eikä olisi tiennyt miten tai mihin lomaketta käytetään. Aikaisemmin on ollut tilanteita, joissa on herännyt ajatus, että ehkä pitäisi tehdä jotain, mutta koska toimintatapaa ei ollut kerrottu, jäi asian esille nostaminen tekemättä.

Oliko asiasta kertominen yksikön palaverissa mielestäsi tärkeää vai turhaa?

Tärkeää, koska intran kahlaamiseen ei ole aikaa eikä sinne julkaisemalla uuden asian havaitseminen toimi. Uuden asian jalkauttaminen nähdään tärkeäksi, kuten myös tässä tapauksessa sen ohjeistaminen mikä on poikkeama ja ymmärrämmekö mikä se on. Jollakin tasolla pitäisi käydä läpi erilaiset poikkeamat. Keskitetty koulutus, jossa on käytännönläheisiä esimerkkejä ja lomakkeen yhteyteen ohje.

Tuletko käyttämään lomaketta ja madalsiko käyttökynnystä?

Kyllä, nyt kun tietää, että on olemassa lomake ja mitä sillä tulee tehdä.

Heräsikö muita ajatuksia?

Meille ns. tietotyöläisille ei satu vastaavia läheltä piti tilanteita kuin teollisuudessa, mutta voisi olla käytäntö nostaa esille millaisia tietotyön läheltä piti tilanteita (poikkeamia) on tullut esille ja julkaista esimerkiksi “x päivää ilman poikkeamia” – tietoa.

Mitä ajatuksia esimiehelle tuli menettelystä?

Yksikössä on puhuttu paljon tiedon kulusta ja on tunnistettu yleisesti, että kaikki yksikön tarvitsema tieto ei tule esiin. On kokouksia, esimerkiksi konsernipalvelualueen ja kaupunginjohtajan johtoryhmät, joista tulee asioita tiedoksi. Esimiehen on vaikea suodattaa suu-

resta tietomäärästä mitä henkilöstölle tulee viedä tiedoksi, joten viikkopalaveriin voi jokainen nostaa asioita käsiteltäväksi. Opinnäytetyön työpajan esimies näki hyvänä mahdollisuutena testata, kuinka tieto kulkee organisaatiossa.

Liite 3. Johdon muistilista

Tietosuojakäsikirja johdolle (Andreasson ym. 2015) pitää sisällään liitteenä johdon muistilistan (Riva 2015), joka on pyritty tekemään toimialariippumattomaksi ja suuntaa antavaksi, eikä siinä luetella kattavasti organisaation toimintaa koskevaa sääntelyä. Johdon muistilista on kirjoitettu ennen tietosuoja-asetuksen (EU 679/2016) voimaantuloa, joten sitä on tässä yhteydessä päivitetty.

Johdon vastuu

Organisaation johdolla on aina viime kädessä vastuu toiminnan lainmukaisuudesta, tietosuojan ja tietoturvan toteutumisesta. Selvitä, mitkä lait, viranomaisvaatimukset ja standardit koskevat organisaation toimintaa ja aseta tietosuojan tavoitteet ja mittarit näiden vaatimusten perusteella. Tämän tilannekuvan perusteella voidaan edetä vastuiden toteuttamiseksi tarvittavien resurssien, joita ovat esimerkiksi henkilöt ja työvälineet, määrittelemiseen.

Resurssit ja tietoisuus

Organisaation johto on nimennyt tietosuoja- ja tietoturvavastaavat ja määritellyt heille tehtävänkuvan sekä tehtävän kannalta riittävät toimivaltuudet, vastuualueen ja työajan, sekä hankkinut vastuuvakuutuksen, mahdollistanut osaamisen ylläpitämisen henkilöhtaisella koulutussuunnitelmalla ja budjetilla, määritellyt yhteistyön ja verkostoitumisen tahot ja tarpeet sekä julkaissut yhteystiedot sekä henkilöstölle, että rekisteröidyille ja muille sidosryhmille.

Organisaation johto on määritellyt tarvittavat politiikat, esimerkiksi: tietoturva-, tietosuoja-, tietojen luokittelu, käyttövaltuus-, loki-, tietojärjestelmä- ja sähköpostipolitiikat, sekä laatinut näihin liittyvät alipolitiikat. Politiikat ovat organisaation johdon ilmaisemia tavoitteita ja vastuunjaon kuvauksia. Organisaation toimialasta riippuu, millaisia alipolitiikkoja se tarvitsee.

Politiikkoja täydennetään toimialaan ja toimintaa säätelevään lainsäädäntöön liittyvällä ohjeistuksella. Ohjeistusta tulisi olla vähintään henkilötietojen käsittelystä, tietojen luokittelusta ja tiedon elinkaaren hallinnasta, sekä tietojärjestelmien oikeasta käyttötarkoituksesta ja tavasta. Henkilötietojen käsittelyn ohjeistusta tulee antaa erikseen esimerkiksi henkilötietojen käsittelijälle, esimiehille (työntekijän yksityisyys) sekä henkilöstölle tehtäväkohtaisina työohjeina, digitaalisiin palveluihin sekä etätyöhön liittyen.

Organisaation johto on varmistanut sopimuspohjilla ja mallidokumenteilla toiminnan määrämuotoisuuden ja tietosuojan huomioimisen tilanteissa, joissa johto tai tietosuojavastaava ei ole mukana hankinnan tai sopimuksen valmistelussa. Sopimuspohjia ja malleja on hyvä

olla vähintään järjestelmähankintoja, pilvipalveluita sekä henkilötietojen käsittelyn ulkoistuksia varten.

Tietosuojatoiminnan tavoitteiden lisäksi johdon tulee määritellä tavoitteiden toteutumisen seurantaan ja mittaamiseen käytettävät mittarit, raportointijakso sekä tietojen keräämisestä vastaavat tahot, esimerkiksi palveluista vastaavat, esimiehet sekä tietosuojavastaava. Tietosuojavastaavalle on määritelty lakisääteinen oikeus raportoida suoraan organisaation ylimmälle johdolle, mikä mahdollistaa johdolle riittävän ja ajantasaisen tiedon tietosuojan tilanteesta päätöksiä varten.

Seuranta ja valvonta

Organisaation johdon tulee määritellä tarve ja sisältö; sitoumuksiin (esimerkiksi tietojen ja tietojärjestelmien salassapitositoumus) ja seuraamussäännöstöihin (tietoturva- ja tietosuojarikkomusten seuraamussäännöstö), käyttövaltuuspolitiikkaan ja käyttövaltuuskuvauksiin perustuva käyttövaltuuksien valvonta ja auditointi, virustorjuntaan ja välitystietojen manuaaliseen käsittelyyn liittyvä tekninen valvonta sekä tietosuojan / tietoturvan seuranta ja valvontasuunnitelma. Muun muassa sosiaali- ja terveydenhuollolla sekä eräillä niiden palveluiden tuottamiseen liittyvillä tahoilla on lakisääteinen velvollisuus omavalvonta, sekä seuranta ja valvontasuunnitelmien tekemiseen.

Henkilötietojen käsittely

Kaiken henkilötietojen käsittelyn, mukaan lukien niiden elinkaari, tulee olla suunniteltua, noudattaa tietosuoja-asetuksen (EU 679/2016) 5 artiklan käsittelyä koskevia periaatteita sekä tuottaa asetuksessa rekisterinpitäjälle tai henkilötietojen käsittelijälle määriteltyjä osoitusvelvollisuuteen sisältyviä dokumentteja ja ilmoituksia. Organisaation johdon tulee nimetä näistä vastuussa olevat sekä valvoa asetuksen noudattamista yhdessä tietosuojavastaavan kanssa. Henkilötietojen käsittelyn suunnittelu tulee huomioida jokaisessa järjestelmähankinnassa sekä käyttövaltuushallinnassa.

Asiakirjahallinto ja arkistointi

Organisaation tiedon elinkaarenhallinta on organisaation johdon vastuulla.

Lopuksi: Ole läsnä! Kiinnostu! Auta! Johda