

Sinikka Mickos

OSOITUSVELVOLLISUUS OSANA TIE- TOSUOJA- JA TIETOTURVAPOLITIIK- KAA

Opinnäytetyö
Tradenomi, Liiketalous

2020



**Kaakkois-Suomen
ammattikorkeakoulu**

Tekijä/Tekijät	Tutkinto	Aika
Sinikka Mickos	Tradenomi (AMK)	Toukokuu 2020
Opinnäytetyön nimi		
Osoitusvelvollisuus osana tietosuoja- ja tietoturvapoliittikkaa		43 sivua 0 liitesivua
Toimeksiantaja		
Lapinjärven kunta		
Ohjaaja		
Aarni Ahtola		
Tiivistelmä		
<p>Alati kiihtyvällä vauhdilla kehittyvä ja kansainvälistyvä teknologia ja digitaalisten palveluiden käytön kasvu velvoittavat myös rekisterinpitäjää muutoksiin henkilötietojen lainmukaisessa käsittelyssä. Suomessa on vuoden 2019 alusta astunut voimaan tietosuojalaki, joka täydentää kansallisen liikkumavaran osalta EU:n yleistä tietosuoja-asetusta (General Data Protection Regulation eli GDPR). GDPR toi mukanaan koko EU:n alueella huomattavia uudistuksia tietosuojan sääntelyyn. Yksi huomattavimmista uudistuksista on rekisterinpitäjän osoitusvelvollisuus. Vankan alustan organisaation rekisterinpitäjän osoitusvelvollisuuden noudattamiseksi luo kattava ja ajan tasalla oleva tietosuoja- ja tietoturvapoliittikka.</p> <p>Tässä opinnäytetyössä tutkittiin rekisterinpitäjän osoitusvelvollisuuden edellyttämien tietosuojaperiaatteiden toteutumista Lapinjärven kunnassa selvittämällä kunnan uudistetun tietosuoja- ja tietoturvapoliittikan lisäksi tehtyjen toimenpiteiden kattavuutta tietosuoja-asetuksen osoitusvelvollisuuden näkökulmasta. Osoitusvelvollisuus vaatii, että organisaation on kyettävä osoittamaan noudattavansa lainsäädäntöä kaikissa henkilötietojen käsittelyprosessien toiminnoissaan. Työn tutkimusmenetelmä oli kvalitatiivinen ja tutkimus- ja tiedonkeruumenetelminä hyödynnettiin kolmen kunnan tietosuojavastaavista ja ICT-johdosta muodostuvan GDPR-työryhmän ryhmäkeskusteluja ja sisäpiirihaastatteluja.</p> <p>Tutkimuksen tuloksena organisaatiolle tuotettiin kattava kartoitus nykytilasta rekisterinpitäjän osoitusvelvollisuuden toteuttamiseksi, jossa tärkeimpinä toimina esille nousivat tietosuojavastaavan nimeäminen ja toteutetut GDPR-projektit. Työn kehittämisehdotuksista kärkeen nousivat tietosuojavastaavan merkityksen korostaminen, sekä tietosuojan vuosikellon ja tietotilinpäätöksen toteuttamissuunnitelmat. Lisäksi työn tuloksena voidaan todeta, että tietosuojatyön siirtyessä tietosuojahankkeista osaksi koko organisaation jokapäiväistä arkea, voidaan tietosuoja-asetuksen noudattamisen todeta jatkossa olevan organisaatiolle yksi menestyksen tekijöistä.</p>		
Asiasanat		
osoitusvelvollisuus, tietosuojapolitiikka, tietoturvapoliittikka, tietosuoja-asetus, tietosuojalaki		

Author (authors)	Degree	Time
Sinikka Mickos	Bachelor of Business Administration	May 2020
Thesis title		43 pages
Accountability as part of data protection and data security policy		0 pages of appendices
Commissioned by		
The municipality of Lapinjärvi		
Supervisor		
Aarni Ahtola		
Abstract		
<p>The accelerating and internationalizing technology and growing use of digital services oblige the controller to make changes to the lawful processing of personal data. At the beginning of 2019, the Data Protection Act put this law into operation in Finland, fulfilling the EU's General Data Protection Regulation (GDPR) to complete these actions. The GDPR brought significant reforms to data protection regulation across the EU. One of the most significant reforms is the accountability of a controller. A robust platform for the organization is creating comprehensive and up-to-date data protection and security policy.</p>		
<p>This thesis examined the implementation of the data protection principles required by the registrar's accountability to provide information in the municipality of Lapinjärvi by finding out the scope of the measures taken in addition to the municipality's renewed data protection and data security policy of the municipality of Lapinjärvi from the controller's point of view on data protection regulation. According to the accountability principle, the organization must be able to follow fully the new legislation throughout the process of handling personal data. The research method of the work was qualitative and the research and data collection methods utilized the group discussions and interviews with the GDPR working groups, which consisted of data protection officers and ICT management of three different municipalities.</p>		
<p>As a result of this study, a comprehensive survey of the current status was produced for the organization in order to implement the controller's accountability, in which, the data protection officer and the implemented GDPR projects emerged as the most important activities. Among the proposals for the development of the work, the emphasis was in the role of the data protection officer, as well as the implementation plans for the annual clock and financial statements for data protection. In addition, it can be stated that as data protection work shifts from data protection projects to the daily life of the entire organization, compliance with the data protection regulation can become one of the key factors of success for the organization.</p>		
Keywords		
<p>accountability, data protection policy, data security policy, data protection regulation, data protection law</p>		

SISÄLLYS

1	JOHDANTO.....	9
2	OPINNÄYTETYÖN TARKOITUS JA TAVOITTEET	11
3	OPINNÄYTETYÖN TIETOPERUSTA.....	11
4	OPINNÄYTETYÖN TUTKIMUSMENETELMÄ	14
5	TOIMEKSIANTAJAN ESITTELY	15
6	OSOITUSVELVOLLISUUS.....	17
7	NYKYTILAN KUVAUS	19
8	TOTEUTETUT PROJEKTIT	20
8.1	Tietosuoja- ja tietoturvapoliittikka.....	21
8.1.1	Käyttäjän ohjeet	22
8.1.2	Muut ohjeet ja lomakkeet	24
8.2	GDPR-toteutus	24
9	ONGELMAT JA KRIITTISET PISTEET	27
10	TIETOSUOJAVASTAAVIEN SISÄPIIRIHAASTATTELUT JA GDPR- RYHMÄKESKUSTELUT	28
11	KEHITTÄMISEHDOTUS.....	32
12	JOHTOPÄÄTÖKSET	36
13	YHTEENVETO	37
	LÄHTEET.....	39

KÄYTETYT LYHENTEET JA TERMIT

Lyhenteet ja termit ovat pääosin Lapinjärven kunnan tietosuoja- ja tietoturva-politiikan liitteestä numero kaksi ”Käsitteet, Roolit ja Vastuut”, jossa nimensä mukaisesti kuvataan tietosuojaan ja tietoturvaan liittyvät, kunnan toiminnan kannalta keskeisimmät käsitteet, sekä roolit ja vastuut, ensi sijassa VAHTI-ohjeisiin perustuen.

Accountability	Rekisterinpitäjän osoitusvelvollisuus
Eheys	Tietojen, tai tietojärjestelmän sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käytökelpoisuus. Ominaisuus, joka ilmentää, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.
Fyysinen turvallisuus	Sisältää henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen, laittilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Lisäksi se sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden.
GDPR	General Data Protection Regulation (EU) 2016/679
Hallinnollinen tietoturvaluisuus	Tietoturvaluuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.
Henkilörekisteri	Kyseessä on mikä tahansa jäsenneilty tietojoukko, joka sisältää henkilötietoja. Tietojoukko on rekisteri,

josta tiedot ovat saatavilla tietyin perustein riippumatta siitä, onko tietojoukko keskitetty, hajautettu tai jaettu esimerkiksi toiminnallisin tai maantieteellisin perustein. Henkilötietoja voidaan tallettaa esimerkiksi sähköisiin tiedostoihin, tietokantoihin, paperisina, mappeihin, kortistoihin tai ääni- ja kuvataallenteisiin. Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan ihmiseen liittyviä tietoja.

Henkilötietojen käsittelijä

Henkilötietojen käsittelijä toimii rekisterinpitäjän ohjeiden mukaisesti sekä sen alaisuudessa ja rekisterinpitäjä määrittelee henkilötietojen käsittelyn keinot ja tarkoitukset. Käsittelijä voi olla esimerkiksi yksityinen elinkeinonharjoittaja, yritys, viranomainen tai yhdistys. Tämä ei kuitenkaan tarkoita rekisterinpitäjän alaisuudessa toimivia työntekijöitä, jotka käsittelevät henkilötietoja osana työtehtäviään.

Horisontaalinen verkosto

Verkosto toimii nimensä mukaisesti vaakasuunnassa; samalla tasolla olevat osastot tai yksiköt tekevät keskenään yhteistyötä.

JUHTA

Valtioneuvoston asettama julkisen hallinnon tietohallinnon neuvottelukunta

Luottamuksellisuus

Tietojen säilyminen luottamuksellisina (ettei kukaan sivullinen saa tietoa) ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

Oikeellisuus

Virheettömyys, yhtäpitävyys todellisen asiointilan kanssa.

Rekisterinpitäjä	Henkilö, yhteisö tai säätiö, jonka käyttöä varten rekisteri perustetaan, ja jolla on oikeus määrätä sen käytöstä, tai jonka tehtäväksi rekisterinpito on lailla säädetty.
Riski	Todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon. Uhkaan liittyvän vahingon rahallinen arvo tai odotusarvo. Riski voi olla myös mahdollisuus menettää päämääräksi asetettu seikka.
Riskienhallinta	Järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa. Erikseen organisoitu riskienhallintatoiminto tukee hallinnon johtamista. Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poistamisesta, alentamisesta tai pitämisestä omalla vastuulla, sekä riskienhallinnan organisointi.
Saatavuus	Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.
Tietoliikenneturvallisuus	Tiedonsiirtoyhteyksien turvaamisen, suojaamisen ja salaamisen, käyttäjän tunnistamisen ja verkon varmistamisen turvallisuustoimenpiteet, sekä lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus.
Tietosuojaseloste	Rekisteröidylle kohdistettu ja heidän saatavillaan oleva selkeä ja helposti ymmärrettävä kirjallinen selostus mm. siitä, mitä tietoja heistä kerätään ja miksi.
Tietosuojavastaava	Henkilö, joka on riippumaton, eikä hänellä voi olla eturistiriitoja tietosuojavastaavan tehtävien kanssa.

Tietosuojavastaava auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja mahdollisten erityislakien edellyttämän tietosuojan tason.

VAHTI

Valtiovarainministeriön asettama valtionhallinnon tietoturvallisuuden johtoryhmä

VPN

Virtual Private Network

VPN (MFA)

Virtual Private Network monivaiheinen tunnistautuminen

1 JOHDANTO

Suomessa on 1.1.2019 astunut voimaan uusi kansallinen tietosuojalaki 1050/2018 (Finlex 2018). Tietosuojalaki täydentää ja täsmentää kansallisen liikkumavaran osalta 28.5.2018 voimaan astunutta EU:n yleistä tietosuoja-asetusta, General Data Protection Regulation (EU) 2016/679 (myöhemmin GDPR), joka on yhtenäistänyt kaikkien EU-maiden tietosuojakäytännöt ja jota sovelletaan sekä julkisella että yksityisellä sektorilla. (Eduskunta 2018.) Tietosuojalaki ei siis ole itsenäinen ja kattava sääntelykokonaisuus, vaan sitä sovelletaan rinnakkain tietosuoja-asetuksen kanssa (HE 9/2018). Tietosuojalainsäädäntö sisältää parannuksia henkilötietojen suojaan sekä rekisteröidyn oikeuksiin ja sen tavoitteena on myös vastata uusiin, digitalisaation ja globalisaation tuomiin tietosuojahaasteisiin. (Tietosuojavaltuutetun toimisto 2020a.)

GDPR on kaikkien Euroopan unionin maiden yleinen tietosuoja-asetus, jonka soveltaminen on tuonut keskeisiä muutoksia tietosuojan sääntelyyn. Yksi keskeisimmistä periaatteista on osoitusvelvollisuus, jonka perusteella rekisterinpitäjän on kyettävä osoittamaan käsittelevänsä henkilötietoja tietosuojalainsäädännön mukaisesti. (Tietosuojavaltuutetun toimisto 2020b.) Osoitusvelvollisuus määritellään yleisessä tietosuoja-asetuksessa (5 art. 2 kohta) tärkeäksi alaksi ja nimenomaiseksi vaatimukseksi (Tietosuojavaltuutetun toimisto 2020c).

Rekisterinpitäjälle pelkkä lakien noudattaminen ei enää riitä, vaan asetuksen (5, 24 ja 25 artikla) perusteella sen pitää myös tämän jälkeen itse, aktiivisesti ja monin eri tavoin osoittaa, että organisaatioon kohdistuvat tietosuojavaatimukset on huomioitu ja otettu mukaan organisaation henkilötietojen käsittelyprosesseihin ja –käytäntöihin. Edellä kuvatusta mainittakoon erilaiset dokumentit, säännöt eri käytännöistä, kirjalliset suunnitelmat ja tietotilinpäätös. (Andreasson ym. 2019.) Tietosuoja-asetuksella halutaan myös varmistaa, että ihmisten oikeus henkilötietojen suojaan ja näin ollen yksityisyyteen, toteutuu myöskin digiaikana (Kuntaliitto 2019a).

Opinnäytetyön toimeksiantaja on Lapinjärven kunta, jossa GDPR on määrätietoisesti ja projektoidusti toimeenpantu. Kunnassa on perehdytty huolellisesti ja laajamittaisesti tietosuoja-asetuksen tuomiin velvoitteisiin ja panostettu tietoturva- ja tietosuojatyöhön olemassa olevin resurssein ja kuntayhteistyötä hyödyntäen. Koko henkilöstön tietosuojakoulutusta on pyritty aktiivisesti järjestämään mahdollisimman monipuolisesti ja samalla saattamaan tietosuojatyö kunnan kaikkiin toimintoihin luontevaksi osaksi jokapäiväistä työtä.

Tässä työssä tutkitaan, miten Euroopan parlamentin ja neuvoston asetuksen 2016/679 artiklan 5 mukaiset henkilötietojen käsittelyä koskevat periaatteet toteutuvat toimeksiantajan organisaatiossa. Kyseisen artiklan 1 kohdan mukaisesti henkilötietojen suhteen noudatettavat vaatimukset ovat käsittelyn lainmukaisuus, kohtuullisuus, läpinäkyvyys ja käyttösidonaisuus, sekä tietojen minimointi, täsmällisyys, eheys, luottamuksellisuus ja henkilötietojen säilytyksen rajoittaminen. Kyseisen artiklan kohdan 2 mukaisesti rekisterinpitäjän on pystyttävä vastaamaan myös siitä, että se pystyy osoittamaan, että kohtaa 1 on noudatettu ("osoitusvelvollisuus".)

Tämän opinnäytetyön tarkoitus, tavoitteet, tietoperusta sekä tutkimusmenetelmä kuvataan luvuissa kahdesta neljään ja työn toimeksiantaja esitellään tarkemmin luvussa viisi. Osoitusvelvollisuutta kuvataan luvussa kuusi ja luvussa seitsemän avataan laajemmin organisaation tietosuojan nykytilaa. Toimeksiantajan ICT-vastaavana, johtoryhmän ohjauksessa laatimani tietosuoja- ja tietoturvapoliittikka (Lapinjärven kunnanhallitus 2018), sekä muut rekisterinpitäjän osoitusvelvollisuuden täyttämiseksi tehdyt toimenpiteet selostetaan luvussa kahdeksan. Luvussa yhdeksän raportoidaan organisaation osoitusvelvollisuuden ongelmakohdat ja kipupisteet ja luvussa kymmenen analysoidaan tietosuojavastaavien sisäpiirihaastattelut ja tuodaan esille Myrskylän ja Lapinjärven kuntien, sekä Loviisan kaupungin välisen GDPR-työryhmän ryhmäkeskustelujen pääkohdat. Opinnäytetyön tietoperustan ja tutkimustulosten perusteella laaditut kehittämissuositukset ja johtopäätökset esitellään luvuissa yksitoista ja kaksitoista. Työn yhteenvedossa summataan tutkimuksen tavoitteiden saavuttaminen ja pohditaan tutkimuksen, sekä oman opiskeluni vaikutuksia toimeksiantajan organisaatiossa.

2 OPINNÄYTETYÖN TARKOITUS JA TAVOITTEET

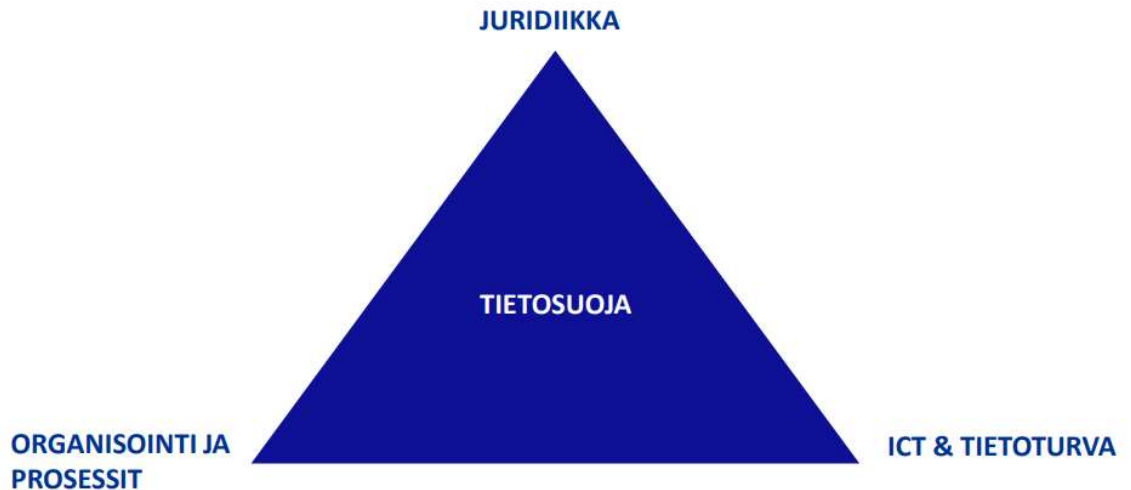
Tässä opinnäytetyössä tutkitaan rekisterinpitäjän osoitusvelvollisuuden edellyttämien tietosuojaperiaatteiden toteutumista Lapinjärven kunnassa. Osoitusvelvollisuus on GDPR:n yksi keskeisimmistä periaatteista ja se velvoittaa organisaatiota noudattamaan lainsäädäntöä kaikissa henkilötietojen käsittelyprosesseissa ja -käytännöissä. Työssä selvitetään kunnan uudistetun tietosuoja- ja tietoturvapoliitikan, sekä muiden GDPR:n velvoittamana tehtyjen toimien kattavuutta rekisterinpitäjän osoitusvelvollisuuden vaatimusten täyttämiseksi.

Tutkimuksen tavoitteena on kartoittaa Lapinjärven kunnan GDPR:n nykytilanne ja tutkimustulosten perusteella tuottaa kunnalle kehittämissuhteita tietosuojatason ylläpitämiseksi GDPR:n vaatimalla tasolla. Opinnäytetyön tutkimuksen aineistoa kerätään laadullisen tutkimuksen yleisimmin menetelmin, kuten havainnoimalla, koostamalla tietoa erityyppisistä dokumenteista, sekä hyödyntämällä vuorovaikutteisia ryhmäkeskusteluja ja sisäpiirihaastatteluja.

3 OPINNÄYTETYÖN TIETOPERUSTA

Tämän opinnäytetyön tietoperustana käytettiin sähköisiä ja kirjallisia lähteitä. Tutkimuksessa hyödynnettiin Lapinjärven kunnan tietoturva- ja tietosuojapolitiikan laadinnan sekä Loviisan kaupungin, Myrskylän ja Lapinjärven kuntien GDPR-yhteistyöprojektin tuloksia.

Tietosuojapolitiikan katsotaan olevan organisaatiossa ylin tietosuoja ohjaava dokumentti ja henkilötietojen käsittelyn tulee noudattaa sekä lainsäädäntöä että tietosuojapolitiikkaa. Henkilötietojen käsittelyyn liittyvät tärkeimmät perusperiaatteiden kuvaukset on suositeltavaa tehdä johdon määrittelemällä tietosuojapolitiikalla tai jollain muulla vastaavalla asiakirjalla ja samalla painottaa tietosuojan merkitystä organisaatiolle. (Rekisterinpitäjän velvollisuudet 2016.) Tietosuojan vaatimuksia ja siihen olennaisesti liittyviä kokonaisuuksia kuvataan ytimekkäästi seuraavan, Valtiovarainministeriön yhteishankkeen tietosuojatyöpajan kuvan mukaisesti.



Tietosuoja yhteishanke työpaja #1 - 12.6.2017

Kuva 1. Tietosuojan rakentuminen (Valtiovarainministeriö 2017)

Kuva kiteyttää tärkeimmät tietosuojaan liittyvät elementit, joita ovat lainsäädäntö, organisointi ja prosessit, sekä ICT & tietoturva.

Oikeusministeriön lausuntopyyntöön (Oikeusministeriö 2019), yleisen tietosuoja-asetuksen toimivuuteen ja sen soveltamiseen liittyviin kokemuksiin on kirjattu eri viranomaisten ja yritysten antamia vastauksia 74 kpl. Niissä on laajasti ja monipuolisesti hyödyllistä tietoa osoitusvelvollisuuteen ja tietosuoja-asetukseen liittyen. Vastauksia antaneista mainittakoon mm. Opetushallitus, Suomen Kuntaliitto, Kansaneläkelaitos, Verohallinto, Väestörekisterikeskus sekä Puolustusministeriö joista viimeisin mielestäni kiteyttää lausunnossaan juuri olennaisen seuraavasti:

”Tietosuoja-asetus on nostanut tietosuojan painoarvoa merkittävästi, ja tietoisuus tarpeesta käsitellä henkilötietoja oikein, on kasvanut. Samalla asetukset on edistänyt myös yleistä tietoturvallisuuden toteuttamista. Vaikka henkilötietojen käsittelyn ja suojaamisen edellytykset eivät tietosuoja-asetuksen myötä merkittävästi muuttuneet, on osoitusvelvollisuus ohjannut kiinnittämään henkilötietojen suojaan ja dokumentointiin enemmän huomiota. Toisena esimerkkinä tietosuojan edistämisestä konkreettisin toimin, on asetuksen velvoite nimittää tietosuojavastaava.”

Osoitusvelvollisuutta on erittäin kattavasti käsitellyt Vainio (2018) pro gradu -tutkielmassa, jossa hän muun muassa toteaa osoitusvelvollisuuden olevan

yleisluontoinen velvoite, jota ei ole sitä koskevissa artikloissa säädetty niin tarkkaan rekisterinpitäjän velvoitteiden täyttämisen keinojen osalta. Hänen työssään tarkastellaan mm. keskeisempiä käytäntöjä ja toimenpiteistä, joilla rekisterinpitäjä voi täyttää ositusvelvollisuuden.

Huomioitavaa siis on, että tietosuojan vaikutusten arviointi sekä selosteiden vaatimus toimivat olennaisina näyttöinä osoitusvelvollisuuden noudattamisessa. Haasteita vaikutuksen arviointiin tuo käytännön tuoreus, ja vaikka GDPR (35 artikla) säätelee raamit, jää rekisterinpitäjän omaan harkintaan käytännön toteutus. Lisähaasteen yleisen tietosuoja-asetuksen toteutukseen on vielä tuonut kansallisen lainsäädännön keskeneräisyys, johtuen henkilötietojen käsittelyyn liittyvien hallituksen esityksien, sekä monien aiheeseen liittyvien lakiluonnosten vireilläolosta. (Andreasson ym. 2019.)

Toukokuussa 2018 Tampereen kaupungille kvalitatiivisen, tulkintalainopillisen tutkielman, laatinut Himanka (2018) tuo esille, kuinka tietosuoja-asetus on tuonut mukanaan rekisterinpitäjälle uusia ja tarkemmin määriteltyjä vaatimuksia ja samanaikaisesti laajentanut rekisteröityjen oikeuksia. Lisäksi hän mainitsee rekisterinpitäjän lisääntyneet resurssitarpeet. Tulevaisuudessa uusien teknologioiden, esimerkiksi tekoälyn, oletetaan tuovan helpotusta organisaatioiden velvoitteiden toteuttamiseen tältäkin osin (Andreasson ym. 2019).

Suhteellisen uudesta aiheesta löytyy nyt tutkimuksia lisääntyvässä määrin, joista esimerkkinä Summen (2018) kvalitatiivinen tutkimus. Siinä tutkittiin mm. millaisilla teknisillä ja organisatorisilla toimilla osoitusvelvollisuuden voi täyttää. Työn johtopäätöksenä todettiin, että varsinkin dokumentaation osalta, vaihtoehtoja osoitusvelvollisuuden täyttämiseen on monia ja että jokainen organisaatio voi valita itselleen parhaiten soveltuvat ja toimintaa tukevat keinot.

Suurin osa aiheeseen liittyvistä tutkimusten toimeksiantajista on edelleen yrityksiä, joten ne eivät ole kaikilta osin suoraan verrannollisia julkishallinnolle tehtävään tutkimukseen, vaikkakin GDPR on yhtenäistänyt kaikkien EU-maiden tietosuojakäytännöt ja sitä sovelletaan sekä julkisella että yksityisellä sektorilla. (Eduskunta 2018.)

Julkishallinto on kiistatta merkittävä henkilötietojen käsittelijä ja omistaja. Valtiovarainministeriön alaisen julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) asettama asiantuntijatyöryhmä, on vuosina 2017-2018 toteuttanut kaksi yhteishanketta. Yhteishankkeiden tarkoituksena on tietosuojan ja tietoturvallisuuden osaamisen ja kehittämisen edistäminen julkishallinnossa. Erityisesti yhteishankkeilla on pyritty tukemaan julkishallinnon organisaatiota GDPR:n osoitusvelvollisuuden toteuttamisessa, mutta myös parantamaan organisaatioiden tietoturvapoikkeamien, sekä riskien- ja jatkuvuudenhallintaa. Yhteishankkeissa on ollut mukana myös Suomen Kuntaliitto, Tietosuojavaltuutetun toimisto, Oikeusministeriö, Valtori, Valtiovarainministeriö sekä Viestintävirastossa toimiva Kyberturvallisuuskeskus. (Valtioneuvosto 2018.) Lisäksi Valtiovarainministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) tuottaa ja kehittää kaikki tietoturvallisuuden osa-alueet kattavat ja voimassa olevat tietoturvaohjeet sekä tietoturvamääräykset (Valtiovarainministeriö 2020).

Tässä opinnäytetyössä hyödynnettiin opiskelemalla aihetta taustamateriaalin tyyppisesti myös Tietosuojavaltuutetun toimiston julkaisemaa teosta Miten valmistautua EU:n tietosuoja-asetukseen? (2017). Siinä käsitellään tietosuoja-asetuksessa säädettyjä henkilötietojen käsittelyä koskevia, rekisterinpitäjää ohjaavia tietosuojaperiaatteita, joista yksi merkittävimmistä on osoitusvelvollisuus.

4 OPINNÄYTETYÖN TUTKIMUSMENETELMÄ

Tämän opinnäytetyön tutkimusmenetelmä on kvalitatiivinen, eli laadullinen. Yleisimmät laadullisen tutkimuksen aineistonkeruumenetelmät ovat kysely, havainnointi, erityyppisistä dokumenteista koottu tieto, sekä haastattelut (Tuomi ym. 2018), joten menetelmä sopi hyvin omaan tutkimukseeni, jossa kyseisiä elementtejä käytettiin.

Tämän työn tutkimus- ja tiedonkeruumenetelminä hyödynnettiin ryhmäkeskustelun monipuolista vuorovaikutusta. Tyypillisesti ryhmäkeskusteluissa tietty ryhmä kokoontuu keskustelemaan ennalta päätetystä aiheesta. Lisäksi työssä

hyödynnettiin sisäpiirihaastatteluja, joissa sekä haastattelija että haastateltava ovat sitoutuneet ja kiinnostuneet yhteisestä aiheesta. (Juvonen ym. 2017.)

Ryhmäkeskustelua sovellettiin kuntien yhteisen GDPR-ryhmän puitteissa, jossa itse olen ryhmän jäsen. Sisäpiirihaastatteluissa haastateltiin Lapinjärven ja Myrskylän kuntien, sekä Loviisan kaupungin tietosuojavastaavia.

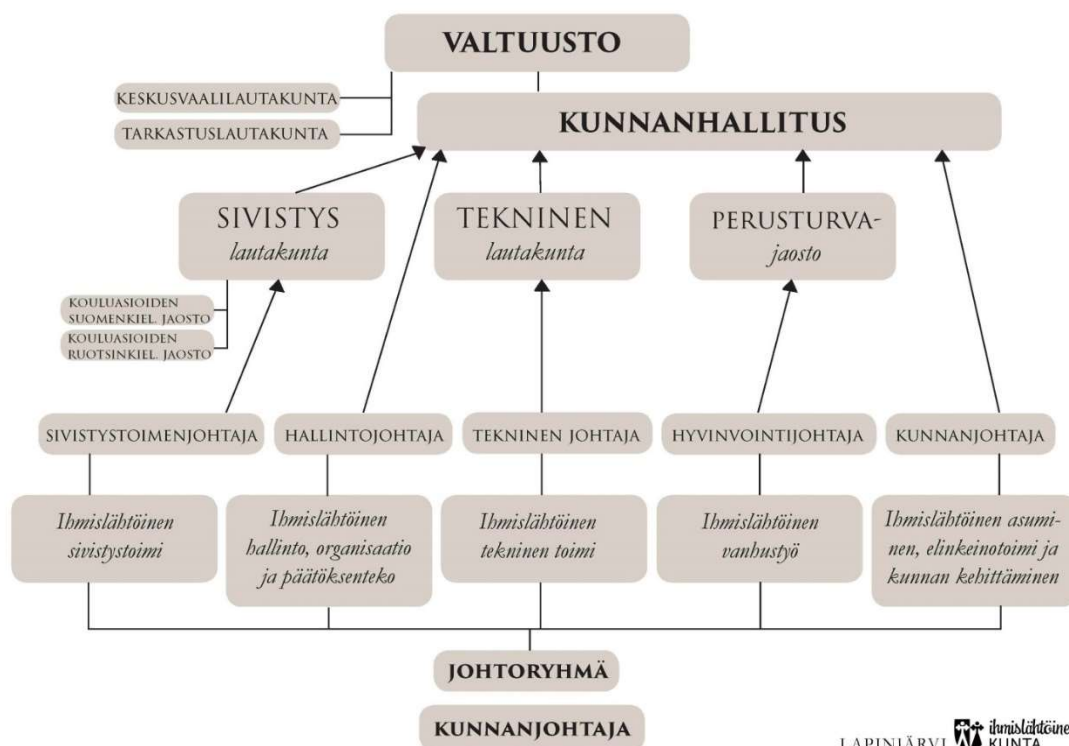
5 TOIMEKSIANTAJAN ESITTELY

Lapinjärven kunta on noin 2600 asukkaan, virallisesti kaksikielinen kunta, jossa ruotsinkielisten osuus on noin 33 %. Kuntaa kehitetään tuotteliaasti ketterän toimijan ja Suomen ensimmäisen ihmislähtöisen kunnan periaatteilla. Kunnanvaltuuston hyväksymän Ihmislähtöisen kunnan strategian mukaisesti, kuntaa kehitetään kansalaistoimijalähtöisesti, yhteisöllisesti ja luontaisin menetelmin sekä jähmeät organisaatiot ja byrokraatit unohtaen, siis ihminen edellä, nopeasti ja vastuullisesti. (Lapinjärvi 2017.)

Kunnassa toimii kaksi suomenkielistä ja yksi ruotsinkielinen alakoulu, sekä ko-keiluhankkeena toteutettu, 500 km päässä sijaitseva e-koulu (Tamminen 2018). Opetuksen ja koulutuksen lisäksi kunnassa tuotetaan kaksikielisesti hallintopalvelut, perusturva-, tekniset-, päivähoito-, varhaiskasvatus-, sekä nuoriso- ja kirjastopalvelut. Kunnan palveluksessa on noin 100 työntekijää. (Lapinjärvi 2020a.)

Lapinjärven kunta kuuluu Loviisan kaupungin yhteistoiminta-alueeseen, joka tarjoaa kuntien asukkaille sosiaali- ja terveystalvet ja jotka Loviisan kaupunki tuottaa isäntäkuntana. Lisäksi Loviisan kaupunki vastaa yhteistyöalueen maaseutuhallinnon tehtävistä Itäisen Uudenmaan maaseutuhallinnon alueella, johon kuuluvat Vantaan, Helsingin, Loviisan ja Porvoon kaupungit sekä Siipoon ja Lapinjärven kunnat. Kunnan yläkoulu- ja lukiopalvelut molemmille kieliryhmille, sekä rakennusvalvonnan ja ympäristönsuojelun viranomaistehtävät, tuottaa Loviisan kaupunki Lapinjärven kunnalle ostopalveluna. (Lapinjärvi 2020b.)

Oheinen organisaatiokuva (kuva 2) esittelee Lapinjärven eli Suomen ensimmäiseksi ihmislähtöiseksi kunnaksi julistautuneen kunnan hallinnollisen organisaation.



Kuva 2. Lapinjärven kunnan organisaatiokaavio (Lapinjärvi 2020c)

Lapinjärven kunta on ollut aktiivinen ja edistyksellinen toimija myös valokuidun saralla jo 1990-luvulta lähtien. Mediatiedotteessa (Lapinjärvi 2018) olen kertonut, kuinka kunnassa on määrätietoisesti rakennettu laajakaistastrategiaa, jonka tarkoituksena on ollut tuottaa kuntaan sellaiset tietoliikenteen kannalta toimivat järjestelmät, että kunnassa on mahdollista asua ja toimia, riippumatta siitä missä kylässä asuu tai missä yritys toimii. Strategiassa asetettujen tavoitteiden mukaisesti jatkuu laaja kuituyhteistyö myös kyläverkko-osuuskuntien ja operaattoreiden kanssa. Kaikki kunnan toiminnot ovat oman valokuituverkko-yhteyden piirissä, mikä on tuonut kunnalle huomattavia taloudellisia säästöjä ja mahdollistanut 100 Mbit/s laajakaistayhteydet ja kattavat, tietoturva edellä suunnitellut, langattomat verkot kaikissa kunnan palveluissa. (Lapinjärvi 2018.)

Viestintäviraston kuntakohtaisen Suomen nopeiden laajakaistayhteyksien listan kymmenen kärjessä valokuidutetuinta kuntaa on Lapinjärvi ollut vuonna 2014 sijalla 9, jolloin kunnassa oli jo 90 % kattavuus (Viestintävirasto 2014).

GDPR:n mukaan määrämuotoista tietosuoja-, tai rekisteriselostetta ei tarvitse laatia. Organisaatioiden tulee kuitenkin informoida rekisteröityjä henkilötietojen käsittelystä. Lapinjärven kunnan henkilörekisterit ovat julkisesti nähtävillä kunnan verkkosivuilla. Niistä esimerkkeinä mainittakoon mm. KuntaToimisto -ohjelmisto ja KTweb, oppilashallintojärjestelmä Visma InSchool Primus, Google Apps for Education –palvelu ja Helle-kirjastot.

6 OSOITUSVELVOLLISUUS

Tietosuojasetuksen artiklan 5 kohdassa 2 säädetään uusi henkilötietojen käsittelyn tietosuojaperiaatteen sääntely, eli osoitusvelvollisuus. Sen mukaan rekisterinpitäjälle ei enää riitä tietosuojaperiaatteiden noudattaminen, vaan sen on jatkuvasti pystyttävä myös osoittamaan, että tietosuojaperiaatteita on noudatettu. (Korpisaari ym. 2018.) Artikla 5 sisältää henkilötietojen käsittelyä koskevat periaatteet, joita olen alla olevan kuvan (kuva 3) mukaisesti havainnollistanut.



Kuva 3. Osoitusvelvollisuus

Osoitusvelvollisuuden toteutumiseksi henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Tietoja saa kerätä vain tiettyyn, lailliseen ja nimenomaiseen käyttötarkoitukseen. Tietojen keräämistä ja käyttämistä laillisesti määrittelee käyttötarkoitussidonnaisuus. Tietojen minimoinnilla rajataan henkilötietojen käsittely vain asianmukaisiin ja olennaisiin, sekä suhteutettuna käsittelyn tarkoituksiin. Jotta käsitellyt henkilötiedot ovat täsmällisiä, on ne tarvittaessa päivitettävä, jolloin on tehtävä kaikki kohtuudella mahdolliset toimenpiteet, että käsittelyn tarkoituksiin nähden poistetaan ne henkilötiedot, jotka ovat epätarkkoja ja virheellisiä, tai oikaistaan ne ensi tilassa. Säilytyksen rajoittaminen säätelee missä muodossa, kuinka kauan ja miten henkilötietoja säilytetään. Henkilötietojen käsittelyssä asianmukainen turvallisuus on hoidettava suojaamalla käsittely lainvastaisilta ja luvattomilta vahingoittumisilta sekä tietojen häviämislä tai tuhoutumiselta. Henkilötietojen käsittely on myös tapahduttava asianmukaisilla teknisillä ja organisatorisilla toimilla, jolloin taataan tiedon eheys ja luottamuksellisuus. (Korpisaari ym. 2018.)

Osoitusvelvollisuus on siis tietosuojasetuksessa erittäin keskeinen periaate. Jos organisaatiossa havaitaan esimerkiksi tietoturvaloukkaus, voi rekisterinpitäjä osoitusvelvollisuuteen liittyvien toimenpiteiden ja dokumenttien avulla todistaa, kuinka se on aktiivisesti pyrkinyt huomioimaan, ennakoimaan ja tunnistamaan tietosuojaan liittyvät riskit, sekä tehnyt niihin liittyviä tarvittavia toimenpiteitä suojatakseen henkilötiedot. Huomioitavaa on, että jos rekisterinpitäjä ei pysty osoittamaan noudattavansa tietosuojasetuksen velvoitteita, voi siitä syntyä hallinnollisia seuraamuksia, tai se voi aiheuttaa riskin organisaation maineelle. (Tietosuojavaltuutetun toimisto 2020a.)

Rekisterinpitäjää kohtaan kohdistuvaa luottamusta lisää osoitusvelvollisuuden toteuttaminen ja samalla on osoitettavissa, että rekisteröityjen, eli henkilötietojen käsittelyn kohteiden tietosuoja kunnioitetaan rekisterinpitäjän taholta. Tämä on myös yksi osoitusvelvollisuuden tarkoitus, ei siis ainoastaan lakisääteisten vaatimusten toteuttamisen analysointi. (Tietosuojavaltuutetun toimisto 2020a.)

Osoitusvelvollisuuteen liittyy myös dokumentointivelvollisuus, joka sisältää tiettyjen toimenpiteiden tekemistä ja kirjaamista. Osoitusvelvollisuuden vaatimuksiin liittyy, että rekisterinpitäjä toteuttaa tarpeelliset organisatoriset ja tekniset toimenpiteet niiden mukaisesti. (Tietosuojavaltuutetun toimisto 2020d.)

Tietotilinpäätöksellä vastataan GDPR:n osoitusvelvollisuuteen, artiklan 24 määrittelemän rekisterinpitäjän vastuun mukaisesti. Laatomalla tietotilinpäätöksen voi organisaatio osoittaa noudattavansa tietosuoja-asetusta ja tietosuoja-periaatteita henkilötietojen käsittelyssä ja osoittaa toimivansa niin myös käytännössä. Tietotilinpäätöksen yhtenä tärkeänä tehtävänä on antaa tietoa organisaation tietosuojan nykytilasta. Säännöllisen raportoinnin tulee sisältää tärkeimmät tietosuojaan ja henkilötietojen käsittelyyn liittyvät tekijät.

Tietosuoja-asetuksessa on myös sellaisia osoitusvelvollisuuteen liittyviä vaatimuksia, joita on analysoitava tapauskohtaisesti liittyen niiden velvoittavuuteen. Osoitusvelvollisuuden laajuus on myös kiinni organisaation koosta, siellä käsiteltävien henkilötietojen määrästä ja niiden tyypistä. Osoitusvelvollisuus on aina otettava huomioon jo suunniteltaessa henkilötietojen käsittelyä. (Tietosuojavaltuutetun toimisto 2020a.)

7 NYKYTILAN KUVAUS

Kunnassa on jo hyvissä ajoin ennen tietosuoja-asetuksen voimaan astumista, johtoryhmän ohjaamana, tehty suunnitelmallisesti, laajamittaisesti ja projektiluontoisesti töitä tietosuojan ja tietoturvan saattamiseksi asetuksen vaatimalle tasolle. Kunnassa on perehdytty huolellisesti ja laajamittaisesti tietosuoja-asetuksen tuomiin velvoitteisiin ja samalla pyritty aktiivisesti saattamaan tieto kunnan kaikkiin toimintoihin luontevana osana jokapäiväistä työtä.

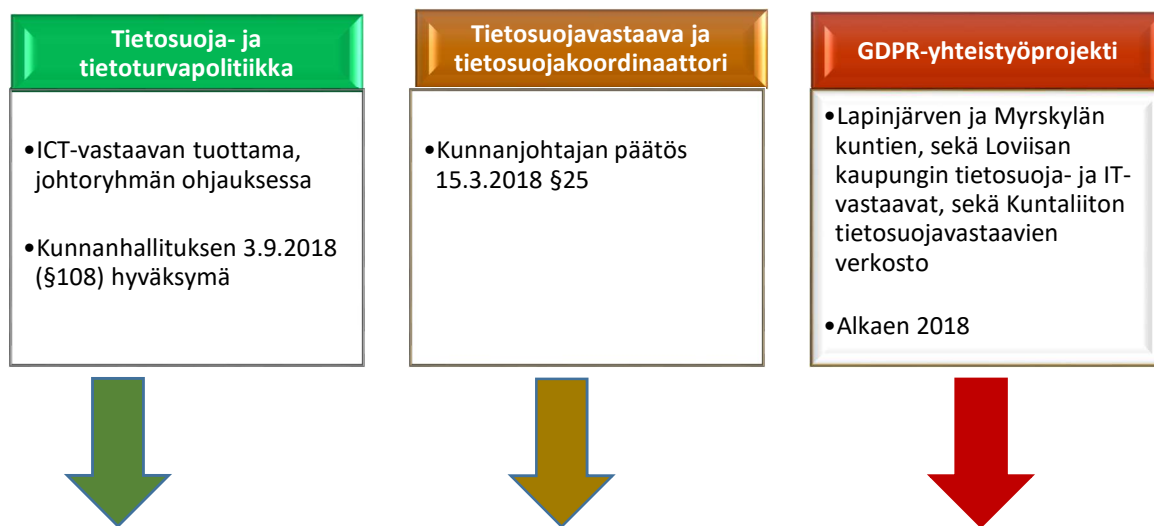
Työ sai hyvän pohjan tietosuoja- ja tietoturvapoliittikan laadinnasta, joka on ollut kattava toimenpide dokumentoitaessa myös osoitusvelvollisuuden toteuttamista tietosuoja-asetuksen 5. ja 25. artiklan mukaisesti (Tietosuojavaltuutetun toimisto 2020a). Siitä on myös ollut hyvä jatkaa jäljempänä esitettyihin, kunnassa jo toteutettuihin rekisterinpitäjän osoitusvelvollisuuden velvoitteiden noudattamiseksi tehtyihin toimenpiteisiin.

Tietosuojatyö on kuitenkin jatkuvaa, johdon vastuulla ja tietosuojavastaavan ohjaamana tehtävää työtä, joka parhaimmillaan saattaa koko henkilöstön tietosuojaosaamisen tasolle, jolla varmistetaan asiakastietojen joustava ja laillinen käsittely (Andreasson ym. 2019). Tätä työtä tehdään aktiivisesti Lapinjärven kunnassa.

8 TOTEUTETUT PROJEKTIT

Kunnassa on projektoidusti toteutettu suhteellisen kattavasti henkilötietojen käsittelyn tietosuojaperiaatteiden mukaisesti eri toimenpiteitä. Projekteissa on huomioitu henkilötietojen käsittelyn lainmukaisuus, kohtuullisuus, läpinäkyvyys ja käyttösidonaisuus, tietojen minimointi, täsmällisyys, eheys ja luottamuksellisuus sekä säilytyksen rajoittaminen (Euroopan parlamentin ja neuvoston asetus 2016/679).

Lapinjärvellä toteutettujen GDPR-projektien toimenpiteiden merkkipaaluja voidaan katsoa olleen alla olevan kuvan (kuva 4) mukaisesti seuraavat toimenpiteet:



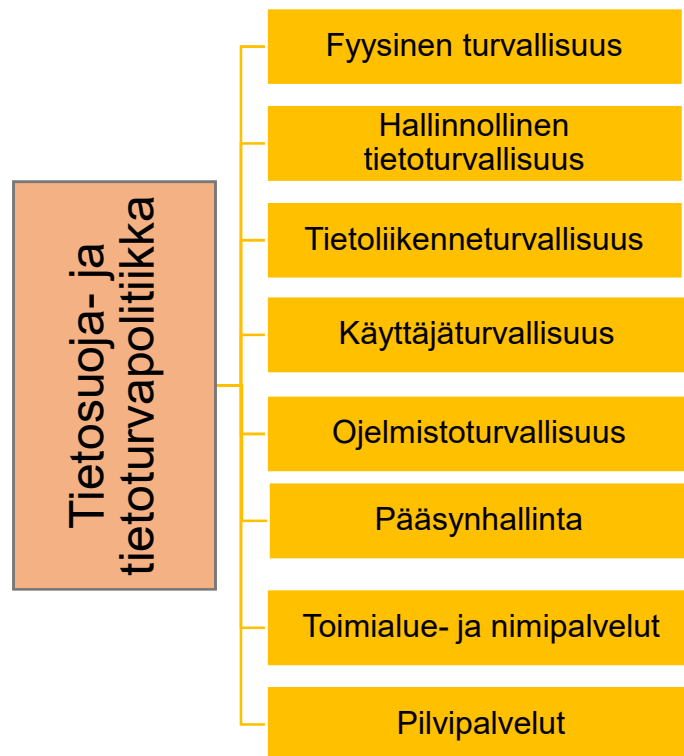
Kuva 4. GDPR-projektien merkkipaalut

Kuvan mukaisesti kunnassa on päätetty tietosuoja- ja tietoturvapoliittikan hyväksyminen kunnanhallituksessa, tietosuojavastaavan ja tietosuojakoordinaattorin määrääminen, sekä kuntien välisen, tiiviin GDPR-yhteistyön aloittaminen.

8.1 Tietosuoja- ja tietoturvapoliittikka

Tietosuojariskien hallinnan tulisi olla osana organisaation riskienhallintaprosessia, sillä henkilötietojen käsittelyn riskilähtöisyys on äärimmäisen oleellinen osa rekisterinpitäjän osoitusvelvollisuuden täyttymistä.

Riskien haitallisia vaikutuksia voidaan vähentää hallinnollisilla ja teknisillä ratkaisuilla. Yksi iso osa kokonaisvaltaista riskien hallintaa on ajantasainen tietosuojapolitiikka tai muu vastaava asiakirja, josta selviää organisaation henkilötietojen käsittelyyn liittyvät periaatteet ja tietosuojan merkitys organisaatiolle. (Rekisterinpitäjän velvollisuudet 2016). Osa Lapinjärven kunnan riskienhallintaa on uusi ja ajantasainen tietosuoja- ja tietoturvapoliittikka liitteineen, määräyksineen ja ohjeistuksineen. Sen rakenne on esitetty kuvassa 5.



Kuva 5. Tietosuoja- ja tietoturvaturvapolitiikan keskeiset elementit

Henkilöstön on tunnettava riittävästi organisaation tietoturvapoliittikka ja siihen kuuluva tietoturvat toimintaan liittyvä ohjeistus, sekä olla sitoutunut noudattamaan niitä (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen

täytäntöönpanosta 2010). Tietoturvapoliittikka on kattavasti tiedoksi ja noudatettavaksi tarkoitettu yrityksen sisäinen määräys, johon sisältyvät yleensä myös tietosuojaan ja tietoturvaan liittyvät ohjeet ja määräykset. Tietoturvallisuudella pyritään ensisijaisesti, ja kaikissa olosuhteissa, turvaamaan organisaation vastuulla olevien palveluiden jatkuvuus, eli tietoteknisesti mahdollistaa organisaation palveluihin liittyvien ICT-ratkaisujen käytettävyys. Organisaation tulee myös huolehtia, että sen kaikissa prosesseissa, rekistereissä sekä palveluissa tietojen luottamuksellisuus ja eheys taataan kaikissa olosuhteissa. Kun organisaatio hoitaa toimintalähtöisesti tietoturva- ja tietosuoja-asiat, tukee se näin sille asetettuja vaatimuksia tietojen ja tietojärjestelmien huolelliselle käsittelylle ja varmistaa kansalaisten yksityisyyden suojan. Tietoturvatoimintaa ohjataan monin tietoturvallisuuteen ja tietosuojaan liittyvien säädöksien, määräyksien ja ohjeiden kautta. (Periaatteet, politiikat ja suunnitelmat 2020.) Lapinjärven kunnan tietosuoja- ja tietoturvapoliittikka liitteineen on tarkoitettu, tietäin valtuuksin, kaikille kunnan työntekijöille toimeenpantavaksi.

8.1.1 Käyttäjän ohjeet

Tässä luvussa esitellään kunnan tietoturvapoliittikan ohjeet, joista osa on tarkoitettu kaikille kunnan työntekijöille ja osa esimiesasemassa olevien tai kunnan tietohallinnon käyttöön.

Henkilöstön tietoturvaohjeessa perustellaan tietoturvallisuuden tärkeys ja taustalla oleva lainsäädäntö. Ohjeessa selostetaan tarkemmin kyberturvallisuutta ja kohdistettuja hyökkäyksiä, sekä opastetaan sosiaalisen median käyttöä. Siinä käsitellään myös asianhallintaan ja tietojenkäsittelyyn liittyviä toimintoja, opastetaan päätelaitteiden käyttöä, käyttöoikeuksia, salasanoja, internet ja viestintäratkaisujen osalta, sekä fyysisten toimitilojen turvallisuutta. Lisäksi ohjeessa opastetaan tietoturvalliseen työskentelyyn kunnan tilojen ulkopuolella, etätyössä, matkoilla, julkisissa kulkuneuvoissa, nettikahviloissa ja mm. kotikoneella toimiessa. Lopuksi ohjeessa neuvotaan miten toimia ongelmatilanteissa, niihin liittyvissä ilmoitusvelvollisuudessa ja niiden mahdollisista seuraamuksista. Ohje on tarkoitettu kaikille kunnan työntekijöille.

Tietoturvasitoumus on asiakirja, joka allekirjoitetaan ja palautetaan kunnan tietoturvapäällikölle. Allekirjoituksellaan työntekijä sitoutuu noudattamaan määräyksiä, jotka liittyvät salassapitoon, käyttäjätunnus- ja salasanaohjeistuksiin, työaseman käyttöön, sähköpostin ja internet-yhteyksien käyttöön, tietoturvaohjeisiin ja tietojärjestelmien käyttöohjeisiin, sekä rikkomusten seuraamuksiin. Sitoumus on tarkoitettu kaikille kunnan työntekijöille.

Tiedon käsittely- ja luokittelu -ohje koskee asiakirjojen ja niiden sisältämän tiedon luokittelua sekä luokitellun tiedon käsittelyä. Luokittelun tavoitteena on varmistaa asiakirjojen ja niiden sisältämän tiedon oikeanlainen käsittely sen elinkaaren eri vaiheissa, jolloin tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat mm. tiedon luominen, käyttäminen, muuttaminen, tallentaminen, siirtäminen, jakelu, kopioiminen, arkistointi ja hävittäminen. Asiakirjan ja sen sisältämän tiedon luokittelulla tavoitellaan sitä, että asiakirjoja käsitellään julkisuusluokan mukaisella tavalla. Ohjeessa opastetaan myös kattavasti, miten käsitellä ja säilyttää salassa pidettävää ja arkaluontoista aineistoa ja opastetaan organisaation salatun sähköpostin käyttö. Kyseinen ohje on tarkoitettu kaikille kunnan työntekijöille.

Esimiehen tietoturvaohje on asiakirja, jossa kerrotaan esimiehen keskeiset tietoturvavastuut, työntekijän rekrytointiin, työsuhteen alkuun, työntekijän työsuhteen aikaiset ja työntekijän työtehtävien muuttumiseen ja työsuhteen päättymiseen liittyvät tietoturvavastuut. Ohje on tarkoitettu kaikille kunnassa esimiesasemassa toimiville.

Tietojärjestelmän omistajan tietoturvaohje käsittelee tietojärjestelmän omistajan velvollisuuksia ja tehtäviä. Ohjeen tarkoituksena on selkeyttää tietojärjestelmän elinkaaren aikaisia vastuita ja käytäntöjä kunnassa. Tavoitteena on varmistaa, että kunnassa käytössä olevien tietojärjestelmien hallinta on järjestetty siten, että tietojärjestelmiin ja niiden toimivuuteen voidaan luottaa. Ohjeessa käsitellään erikseen tietojärjestelmien omistus, siihen liittyvät omistajan vastuut, tietojärjestelmän omistajan yleiset tehtävät, sekä erilliset tietoturva-tehtävät. Lisäksi siinä opastetaan ostopalveluna hankittujen palvelujen tietojärjestelmien vastuut. Ohje on tarkoitettu kaikille kunnassa esimiesasemassa toimiville, sekä kunnan tietohallinnon käyttöön.

Ohjeessa sähköpostin ja salatun sähköpostin käytöstä kerrotaan säännöt milloin salatun sähköpostin käyttö on pakollista ja miten kunnan työntekijä saa salatun sähköpostin käyttöönsä. Ohje on tarkoitettu kaikille kunnan työntekijöille. **Suostumus sähköpostin avaamiseen** –lomake täytetään ja allekirjoitetaan kaikissa niissä tapauksissa, joissa käyttäjä antaa toiselle henkilölle oikeuden lukea omaa sähköpostiaan erityistapauksissa.

8.1.2 Muut ohjeet ja lomakkeet

Lomake käyttöoikeuksien tilaamisesta on tarkoitettu esimiehille, jotka anovat kunnan verkkojen ja tietojärjestelmien käyttöoikeuksia alaisilleen. Lisäksi asiantuntija- tai konsultointipalvelua ulkopuoliselta taholta ostettaessa, on esimiehille käytössä **Ulkopuolisen tahon salassapitositumus** -lomake. Samoin esimiehille on tarkoitettu myös **Tietoturvasopimus** -lomake, joka on liite sopimukseen. Se liitetään ulkopuolisen organisaation kanssa tehtävään sopimukseen silloin, kun kyseessä on toimeksianto, jonka aikana sopimuskumppani voi saada tietoonsa kunnan salassa pidettäviä tietoja joko IT-järjestelmistä tai muulla tavoin, eikä pääsopimuksessa ole tietoturvamääräyksiä.

Virhetilanteiden hallinta -liite liittyy riskianalyysin, jatkuvuussuunnitelman, sekä virhe- ja poikkeustilanteiden suunnitelmien ohjeistuksiin. Tietohallintoa ja perustietotekniikkaa koskevat liitteet ovat salassa pidettäviä, samoin kuin **Tietojärjestelmien pääkäyttäjän tietoturvaohje**, joka on tarkoitettu kaikille kunnassa tietojärjestelmän pääkäyttäjänä toimiville. Salainen on myös **ICT-henkilöstön tietoturvaohje**, joka on tarkoitettu vain kunnan tietohallinnon käyttöön.

8.2 GDPR-toteutus

Yhteistyössä Lapinjärven kunnan johtoryhmän, tietosuojavastaavan, tietosuojakoordinaattorin, muiden kuntien, sekä Kuntaliiton tietosuojavastaavien verkoston (Kuntaliitto 2019b) kanssa, on kunnan tietosuojatasoa vahvistettu entisestään. Kunnassa on toteutettu organisaation kaikilla toimialueilla ja toiminoissa GDPR:n edellyttämiä, seuraavaksi esiteltävien kuvan (kuva 7) koosteen mukaisesti tehtyjä toimenpiteitä.

Raakadatan keräysprojektin tulokset

- Tietosuojaselosteet
- Tietojärjestelmäluettelot
- Tietojärjestelmien pääkäyttäjät
- Tietojärjestelmien vastuuhenkilöt

Koko henkilöstön GDPR:n valmiustason nosto

- Monipuolinen tiedottaminen sähköisesti ja manuaalisesti
- Tietosuojan ja tietoturvan "huoneentaulut"
- Arjentietosuojaa.fi -pakollinen testi
- Tietoiskut, tilannekatsaukset virastopalavereissa ja muissa vastaavissa henkilökunnan kokoontumisissa
- O365 pilvipalvelut
- Salatun sähköpostin käytön laajennus

Kunnan verkkosivujen tietosuojatoimenpiteet

- Tietosuojaselosteet ja GDPR-sivustot
- Rekisteritietojen oikaisu -sivusto
- Rekisteritietojen tarkastus -sivusto
- Evästeiden ilmoitussivu
- Henkilötietoja sisältävien asiakirjojen poistot
- Some-jakonappien poisto
- Lomakkeisiin hyväksyminen henkilötietojen käsittelemiseksi
- "Tykkää meistä facessa" muutos linkiksi

Palvelimet, palomuurit, lan-, wlan- ja valokuituverkot, Internet-yhteydet, pääsynhallinnat

- Palvelinten kahdennusten käyttöönotto
- Laittilojen turvallisuustekijöiden kartoitukset
- Käyttäjä- ja sovelluslokiseurantojen kartoitukset
- Varmistusten siirto pilvipalveluun (palvelin Suomessa)
- Hakemistojen pääsynhallinnan tarkennukset
- VPN (MFA) todennuksen käyttöönotto

IT- ja mobiililaitteiden hankinta-, ylläpito- ja elinkaarenhallintamuutokset

- Hansel/3Step IT -sopimuskumppani -> valmiiksi kilpailutettu/leasing -> koko elinkaaren tietoturva
- Tiera/Atea -> Sopimuskumppani -> valmiiksi kilpailutettu/it-tuotteet
- Mobiilitietosuojan vahvistaminen -> Mobiili Secure

Muita toimenpiteitä

- Tietosuojattavan jätteen hävitysprosessien suojaukset
- Tietoturvaloukkauksien varautumisprosessi/Traficom/poliisi
- Sopimusten tietosuojapäivitykset
- Asiakirjahallintajärjestelmä/tekstinkäsittely; asiakirjojen yhtenäistäminen
- Turvatulostus monitoimilaitteille; tulostuksenhallinta
- Office 365 Advanced Threat Protection (ATP) käyttöönotto (liitteet, linkit, haitallisten linkkien jäljitys)

Kuva 7. Kooste GDPR:n edellyttämistä toimenpiteistä

Edellä kuvatut toimenpiteet ovat vaatineet tekijöiltä vahvaa sitoutumista prosessien etenemiseksi aikataulun mukaisesti ja ennalta sovitun tavoitetilan saavuttamiseksi. Se on vaatinut toteutuakseen myös laajaa yhteistyötä eri toimijoiden kesken, tiedon jakamista eri asiantuntijoiden välillä ja henkilöresurssien joustavuutta.

9 ONGELMAT JA KRIITTISET PISTEET

Niin kuin edellä on kuvattu, uutena asiana rekisterinpitäjälle on tullut todistaa, miten henkilötietojen käsittely ja suojaaminen on organisaatiossa toteutettu. Tähän on Lapinjärven kunnassa panostettu kaikilla sektoreilla, mutta väistämättä haasteena Lapinjärvelläkin toteutuksessa on ollut julkishallinnon niukat talous- ja henkilöresurssit kuntien alati lisääntyvien lakisääteisten velvoitteiden paineessa. Organisaatiossa on huomioitava osoitusvelvollisuuden vaatimusten edellyttämät hallinnolliset ja tekniset tasot. Kunnassa on tunnistettava henkilötietojen käyttötarkoitukset sekä henkilötietoja käsittelevät järjestelmät ja sovellukset, joiden pohjalta tehtävä riskianalyysi auttaa kartoittamaan tarvittavat hallintatoimenpiteet. Osoitusvelvollisuuden vaatima tietoturvan taso on taattava koko henkilötietojen käsittelyn elinkaaren ajan. Lapinjärven kunnan on haasteista huolimatta panostettava tietosuojatyöhön niin, että se voi jatkossakin taata tietosuojasetuksen mukaisen tietosuojan tason henkilötietojen käsittelyssä ja suojaamisessa.

Tietosuojaan liittyvää kansallista ja kansainvälistä viestintää tulisi aktiivisesti seurata ja tietosuojaa ylläpitää organisoidusti ja osana kunnan normaalia toimintaa. Työllä on oltava tarvittava johdon ymmärrys ja tuki. Olisi suuri riski, jos organisaation johto ei olisi tietoinen kokonaisuudesta ja sitoutunut työn toteuttamiseen.

Organisaation tietosuojavastaavan roolin merkitystä ei voi liikaa korostaa. Kunnan on huolehdittava, että tietosuojavastaavalla on työnsä hoitamiseksi tarpeellinen osaaminen. Osaamista ei synny ilman riittäviä resursseja. Riittävä resursointi luo myös hyvät edellytykset työssä jaksamiseen, joten luomalla tarvittavat edellytykset tietosuojavastaavan työn hoitamiseen, voidaan välttää myös tämä ennakoitu riskitekijä.

Henkilöstön riittävä tietosuoja- ja tietoturvaosaaminen on taattava huolehtimalla aktiivisesta koulutuksesta ja ohjeistuksesta. Erityisesti tähän olisi panostettava niiden henkilöiden osalta, jotka osallistuvat henkilötietojen käsittelyyn ja rekisteröidyn oikeuksien toteuttamiseen luotuihin prosesseihin, mutta myös koko henkilöstön osalta tuottamalla loppukäyttäjille suunnattua ohjeistusta ja

helppokäyttöisiä ohjeita (VAHTI-raportti 2016). Organisaation olisi erityisesti syytä ylläpitää opastusta ja tiedottamista salasanojen ja käyttöoikeuksien hallintaan, sekä henkilötietojen ja niihin liittyvien tietojärjestelmien asianmukaiseen käyttöön liittyen (Andreasson ym. 2019).

Kunnassa olisi suositeltavaa laatia tietotilinpäättös, jolloin tietovarannot, tietojohdaminen, tietojenkäsittely ja tietoturvallisuus nousisivat tilinpäätöstyyppisesti esille (Andreasson ym. 2019). Tietotilinpäättös olisi yksi tapa tuottaa organisaation tietojohdamiseen tarvittava dokumentti. Säännöllisesti laadittuna se tuottaisi johdolle selkeän kokonaiskuvan henkilötietojen käsittelyyn liittyvän tietoturvan ja tietosuojan tilanteesta ja sen avulla pystyttäisiin ohjaamaan tietosuojan kehitykseen tarvittavat resurssit. Tietotilinpäättöksellä on painava rooli osoitusvelvollisuuden toteuttajana. Tekemällä tietotilinpäättökseen kunta voi yhdellä tavalla toteuttaa GDPR:n osoitusvelvollisuuden mukaisia velvoitteita. Tietotilinpäättökseen päämääränä on lisätä läpinäkyvyyttä ja avoimuutta, sekä luottamusta siihen, että organisaatiossa vastuullisesti noudatetaan henkilötietojen käsittelyssä organisaation luomia tietosuoja- ja tietoturvaperiaatteita. Tietotilinpäättös toteuttaa accountability - eli tilintekovelvollisuusperiaatetta ja se toimii ajantasaisena tilannekuvana sekä omalle organisaatiolle, että ulkoisille sidosryhmille. (Kuntaliitto 2019c.)

10 TIETOSUOJAVASTAAVIEN SISÄPIIRIHAASTATTELUT JA GDPR-RYHMÄKESKUSTELUT

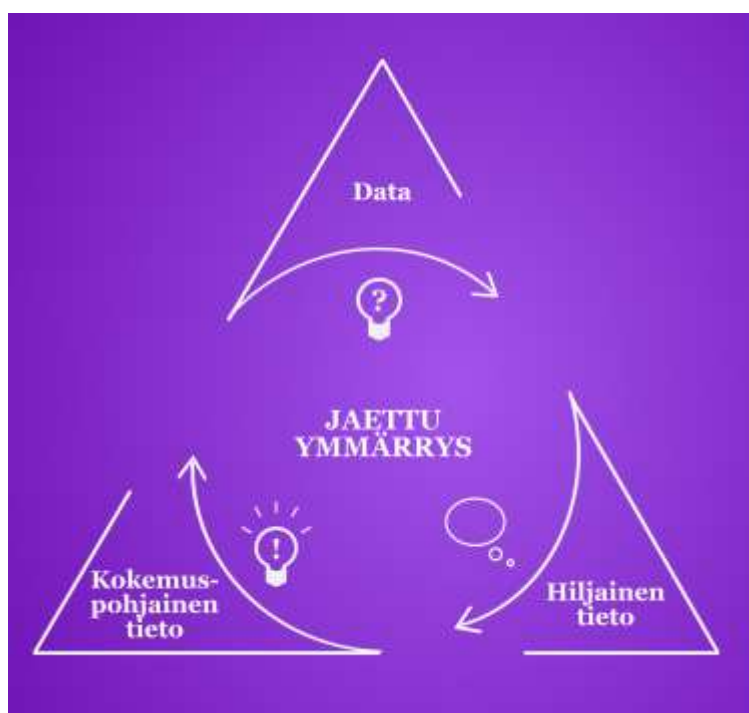
Lapinjärven ja Myrskylän kunnan sekä Loviisan kaupungin tietosuojavastavien sisäpiirihaastattelut toteutettiin Microsoft Teams -kokouksella. Kokouksen runkona toimi etukäteen osallistujille lähettämäni kysymykset, seuraavassa kuvatun sisäpiirihaastatteluun liittyvän ohjeen mukaisesti:

Tutkijan haastava tehtävä on pysyä hetken imusta huolimatta tilanteen tasalla ja muistaa, että hänen tehtävänä on tutkimusaineiston keruu. Tärkeää on ohjata intoutunutta keskustelua hienovaraisesti niin, että siinä pysytään itse asiassa ja tuotetaan tutkimuskysymykseen vastaamisen kannalta mielekästä tietoa. Tässä haastattelijaa auttaa esimerkiksi miellekartta tai yhdelle paperille kerätty listaus tutkimuskysymyksistä tai -teemoista, joita silmäilemällä voi varmistaa sen, että kaikki halutut asiat tulevat käsiteltyksi haastattelun kuluessa. (Juvonen 2017.)

Tietosuojavastavien ennakoon saamat kysymykset olivat seuraavat:

1. Onko tietosuojatyön tekemiseen organisaatiossanne mielestänne suunnattu riittävästi resursseja? Mahdollinen kehittämissuositus?
2. Onko organisaatiossanne tehty tietotilinpäätös ja jos ei, niin onko se suunniteltu tehtäväksi?
3. Onko organisaatiossanne olemassa prosessikuvaus tietoturvaloukkausten ilmoittamiseksi ja jos on, niin voiko sen jakaa ryhmän kaikille jäsenille käytettäväksi?
4. Onko organisaatiossanne olemassa prosessikuvaus rekisteröidyn oikeuksien toteuttamiseksi ja jos on, niin voiko sen jakaa ryhmän kaikille jäsenille käytettäväksi?
5. Onko organisaatioonne tullut pyyntöjä henkilötietojen oikaisemiseksi?
6. Onko organisaatioonne tullut henkilötietojen tarkastuspyyntöjä?
7. Onko organisaatioonne tullut pyyntöjä henkilötietojen poistamisesta?
8. Onko organisaatiossanne tehty tietosuojan vuosikello?

Alla oleva (kuva 7) kuva, joka tekijänsä mukaan kyseisessä artikkelissa esittää tiedolla johtamista, soveltuu mielestäni kuvaamaan myös tätä sisäpiirihaastattelua, jossa aiheesta saatavissa oleva lakisääteinen tieto, eli data ja ryhmän jäsenten kokemuspohjainen, sekä hiljainen tieto yhdistyvät ryhmän jaetuksi ymmärrykseksi (Juvonen 2017).



Kuva 7. Jaettu ymmärrys (Vuorela 2018)

Kokouksessa keskusteltiin kysymysten aiheista laajasti ja niistä yhteenvedona seuraavaksi muutamia tärkeimpiä poimintoja.

Todettiin, että julkishallinto rekisterinpitäjänä on käsitellyt henkilötietoja tietosuojalain kumoaman henkilötietolain mukaisesti jo aiemmin, joten pohja tietosuojalain mukanaan tuoman todistamisvelvoitteen toteuttamiseksi oli jo olemassa. Tältä pohjalta toimenpiteet rekisterinpitäjän osoitusvelvollisuuden toteuttamiseksi, oli kunnissa käynnistetty projektinomaisesti ja erityisesti ohjeiden ja periaatteiden osalta horisontaalisia verkostoja hyödyntäen.

Kaikissa kunnissa työ oli aloitettu kartoittamalla tietosuojan nykytila, jonka perusteella voitiin myös hahmottaa tavoitetilaan pääsemiseen tarvittavat toimenpiteet. Yhtenä tehtävänä oli kartoittaa ja dokumentoida kaikki organisaation henkilörekisterit. Kartoituksessa käytettiin Loviisan tietosuojavastaavan ohjeistamaa toimintamallia, jonka mukaisesti organisaatioissa kokoonnuttiin tietosuojakoordinaattorin ohjauksessa, erikseen jokaisen yksikön kanssa dokumentoimaan kaikki sähköiset ja paperilla olevat henkilörekisterit. Kaikista henkilörekistereistä koostettiin lomake, johon kirjattiin henkilörekisterin nimi, rekisterinpitäjä, rekisteristä vastaava omistaja, rekisterin pääkäyttäjät ja rekisterin tietojen käyttötarkoitus.

Kerätyn tiedon tuloksia hyödynnettiin myös sisäpiirihaastatteluissa ja käytyjen keskustelujen puitteissa huomattiin, että joistakin henkilörekistereistä puuttuivat tietosuojaselosteet. Puuttuneet tietosuojaselosteet julkaistiin kuntien verkkosivuilla ja GDPR:n mukainen rekisterinpitäjän velvollisuus informoida rekisteröityjä toteutui myös niiden osalta. Keskusteluissa vaihdettiin myös tietoa ja käytänteitä digiturvaan ja säännöllisiin avainasioihin liittyvistä vastuista, kuten mm. tietojärjestelmien pääkäyttäjien nimeämisiin liittyen.

Sisäpiirihaastattelun runkona olleiden ennakkokysymysten pohjalta käydyissä keskusteluissa ilmeni, ettei pyyntöjä henkilötietojen tarkastamiseksi, oikaisemiseksi tai poistamiseksi ollut juurikaan toistaiseksi tullut. Lisäksi ennakkoky-

symysten vastauksien perusteella sovittiin yhteistyössä laadittaviksi rekisteröidyn oikeuksien toteuttamiseen liittyvät prosessikuvaukset, sekä tietoturvaloukkausten ilmoittamiseen liittyvät prosessikuvaukset.

Kaikki sisäpiirihaastatteluun osallistuneet tietosuojavastaavat olivat pääsääntöisesti tyytyväisiä GDPR:n rekisterinpitäjän osoitusvelvollisuuden edellyttämien tietosuojaperiaatteiden toteuttamiseksi jo tehtyjen toimenpiteiden kattavuuteen omissa organisaatioissaan. Samalla kaikki kuitenkin painottivat myös tehtyjen toimenpiteiden seuraamisen, dokumentaation ja ajantasaisuuden säännöllisen arvioinnin tärkeyttä. Haastatteluissa tuli myös esille, kuinka GDPR-yhteistyö kuntatasolla on koettu hyödylliseksi ja tärkeäksi voimavaraksi ja että asiantuntijayhteistyötä halutaan ehdottomasti jatkaa ja näin vahvistaa yksittäisen kunnan niukkoja resursseja.

GDPR-työryhmä on ollut Lapinjärvelle tärkeä julkishallinnon asiantuntija- ja vertaistukiryhmä. Ryhmään kuuluvat Lapinjärven, Myrskylän ja Loviisan tietosuoja- ja ICT-vastaavat. Ryhmä on kokoontunut nykyisessä kokoonpanossaan vuodesta 2018 lähtien ja se on hyödyntänyt työssään aktiivisesti asiantuntijoita myös muista verkostoistaan. Esimerkiksi Tampereen kaupunki on ollut GDPR-edelläkävijä sekä hyödyllinen mallintaja ja Tammisaaren kaupungin asiantuntijoiden kanssa on usein vaihdettu vähintäänkin tilannekatsauksia puolin ja toisin. Kyseessä voidaan katsoa olevan ekosysteemi, joka perustuu arvoa luovaan vuorovaikutukseen ja yhteistyöhön.

GDPR-työryhmässä on käsitelty tietosuojan näkökulmasta henkilötietojen hallintointiin ja valvontaan sekä tiedon seurantaan ja raportointiin liittyviä toimenpiteitä. Yhdessä on myös kehitetty sopimusten ja alihankkijoiden hallintamalleja sekä käsitelty tiedon elinkaarenhallintaa. Lähitulevaisuuden toiminnan tavoitteena on selkeiden seuraamuskäytäntöjen sääntöjen valmistelu, joista esimerkkeinä mainittakoon tietoturva- ja tietosuojarikkomukset, rekisteröidyn oikeuksien toteuttaminen sekä tietoturvaloukkauksien ilmoittaminen. Tietosuojan vuosikellon toteuttamiseen ja tietotilinpäätöksen laadintaan liittyvien kunta-kohtaisten toimenpiteiden tukeminen kuuluvat työryhmän lähitulevaisuuden toiminnan kärkitavoitteisiin. Kaikki nämä ovat isoja kokonaisuuksia ja vaativat

pitkäjänteistä ja määrätietoista etenemistä ja ovat osa osoitusvelvollisuuden ohjaavaa riskilähtöistä toimintaa.

Näissä ryhmäkeskusteluissa voi katsoa olleen suurena etuna sen, että osallistujat tunsivat toisensa hyvin entuudestaan. Vuosien ajan jatkuneet, poikkihallinnollisetkin yhteistyökuviot ovat tutustuttaneet ryhmän jäsenet hyvin toisiinsa. Sillä oli merkittävästi vaikutusta ryhmän jäsenten näkemyksien ja vuorovaikutuksen ymmärtämiseen. Ryhmäkeskustelujen nimenomainen anti liittyykin juuri osallistujien väliseen vuorovaikutukseen ja sitä kautta yhteisen tiedon tuottamisen lopputulokseksi (Pietilä ym. 2017).

Henkilöstön koulutuksiin liittyvää suunnittelua ja toteutusta on kiitettävästi jaettu työryhmän kesken. Työryhmän jäsenistöllä on valmisteilla myös tietosuoja- ja tietoturvapoliittikan laadinta, joten Lapinjärven kunnan 2018 valmistuneet politiikat ovat kaikkien hyödynnettävissä soveltuvien osin. Niiden laadinnassa on myös aikoinaan hyödynnetty laajasti horisontaalisia verkostoja mm. Mäntsälän ja Hyvinkään kaupunkien kanssa.

Tämä ekosysteemi jatkaa kehittämistään ja kehittymistään jäsenistönsä hyväksi sekä muuttaa tarvittaessa muotoaan tilanteiden mukaan.

11 KEHITTÄMISEHDOTUS

Organisaation GDPR:n mukaiset toimintatavat ovat riippuvaisia hallinnollisen turvallisuuden johtamisesta ja kehittämisestä, aivan kuten muutkin kunnan prosessien toimintatavat. Tutkimuksessa ilmeni suhteellisen voimakkaana kunnan henkilöstön resurssipula. Siitä huolimatta on jo ennestään laajaan tehtäväkenttään sisällytettävä myös jatkuva tietosuojatyön huomioiminen jokapäiväisessä työssä, joten henkilöstölle on hyödyllistä aika ajoin päivittää toimintatapojaan myös kyseisiä ominaisuuksia kehittäville koulutuksilla. Koulutukset ylipäätään ovat siirtymässä enenevässä määrin verkkoon joka jo sinällään maldattaa koulutuksen järjestämisen ja osallistumisen kynnystä ja ovat myös kustannustehokkaimpia lähiopetukseen verrattuna. Organisaation johto on viime

kädessä vastuussa koulutuksen ja resurssien riittävydestä sekä siitä, että tietosuoja- ja tietoturvan mukaiset toimintatavat sisältyvät koko henkilöstön päivittäisiin prosesseihin positiivisena voimavarana.

Organisaation tulee laatia tietotilinpäätös, koska se kattaa kaikki tietosuoja-asetuksen velvoitteet ja velvoitteiden valvonnan ja se toimii sekä sisäisen että ulkoisen valvonnan apuna. Tietotilinpäätös antaa kokonaiskuvan organisaation henkilötietojen käsittelyn ja tietosuojan nykytilasta. Sen avulla organisaation johto voi valvoa ja arvioida nykytilaa sekä ohjata resursseja sen kehittämiseen. (Valtiovarainministeriö 2017b.) Tekemällä tietotilinpäätöksen, Lapinjärven kunta täyttää sisäisen suunnittelu- ja toimeenpanodokumentein GDPR:n accountability -periaatteen, jonka mukaan sen pitäisi itse osoittaa noudattavansa lakia, hyvää tietojenkäsittelytapaa ja hyvää tiedonhallintatapaa (Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus 2019).

Tietotilinpäätöksen tarkoitus on täydentää lakisääteistä tilinpäätöstä ja toimintakertomusta, mutta sen tarkoitus ei ole kuitenkaan aiheettomasti lisätä organisaation hallinnollista taakkaa (Tietosuojavaltuutetun toimisto 2012). Tietotilinpäätöksen laadintaa suunniteltaessa kannattaa pohtia, kuka sen kokoaa ja mitä mittareita käytetään. Lisäksi kannattaa miettiä miten usein se laaditaan ja kenelle siitä tiedotetaan. Kannattaa myös pohtia valmiiksi miten havaitut epäkohdat korjataan. Tietotilinpäätöksen laatimisen ohjeita ja mallipohjia löytyy esimerkiksi Valtiovarainministeriön sivustolta, jolle on koottu tietosuojan yhteishankkeiden materiaalit (Valtiovarainministeriö 2018). Vastaavia ohjeita ja mallipohjia on käytettävissä myös Kuntaliiton julkaisemana (Kuntaliitto 2019d).

Vaikka suhteellisen tuoreessa (Andreasson ym. 2019) kirjallisuudessa todetaankin, ettei tietotilinpäätöksiä toistaiseksi ole juurikaan kuntasektorilla toteutettu, on jo nyt nähtävissä, kuinka erityisesti suuret kaupungit ja kunnat ovat julkaisseet tietotilinpäätöksiään lisääntyvässä määrin. Kuten aikaisemmin tässä työssä on kuvattu, on kuntakohtaisen tietotilinpäätöksen laadinnan tukeminen myös yksi GDPR-työryhmän toiminnan kärkitavoitteista.

Lapinjärven kunnassa toimii GDPR:n mukaisesti nimetty tietosuojavastaava. Hän hoitaa tietosuojavastaavan tehtävät oman varsinaisen työn ohessa, joten

matka tietosuoja-asiantuntijaksi on siitäkin syystä pitkä ja vaivalloinen, mutta silti kiistatta ensiarvoisen tärkeä. Kunnan kannattaa jatkossa kiinnittää erityistä huomioita tietosuojavastaavan rooliin ja tehtävän hoidon kannalta riittävään resursointiin. Tietosuojavastaavan tehtävänä on mm. seurata, valvoa, neuvoa ja ohjeistaa tietosuoja-asioissa sekä toimia tarvittaessa yhteyshenkilönä rekisteröityjen ja valvontaviranomaisten kanssa. Tietosuojavastaaville on tarjolla runsaasti alan kirjallisuutta, koulutusohjelmia ja seminaareja. Lisäksi tietolähteinä kannattaa hyödyntää myös Oikeusministeriön, tietosuojavaltuutetun toimiston, Finlexin, Kyberturvallisuuskeskuksen, Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI), sekä tietosuojavastaavien internetsivustoja.

Kuntien tietosuojaverkoston yhteistyötä, sekä GDPR-työryhmän yhteistyötä kannattaa ehdottomasti jatkaa niin, että ryhmä kokoontuu säännöllisesti jakamaan tietoa sekä käsittelemään ja kommentoimaan tietoturvaan, kyberturvallisuuteen ja tietosuojaan kuuluvia linjauksia. (Andreasson ym. 2019). Yhteistyötä kannattaa edelleen hyödyntää myös erilaisten ohjeistusten, dokumenttien ja käytännön ohjeiden laadinnassa ja jakamisessa. GDPR-työryhmä on tärkeässä roolissa myös viestittäessä johdolle. Työryhmissä kannattaa jatkossakin pyrkiä edistämään ja kehittämään organisaation tietosuojan ja tietoturvan toteutumista ja näin varmistaa organisaation onnistuminen tietosuojaosaamisessa ja siitä viestittämisessä. Jatkossa organisaation tulee päivittää tietosuoja-asetuksen mukaisia käytänteitä tekemällä säännöllisesti sisäisiä kartoituksia. Tämä voidaan tehdä jo organisoidun tietosuojatyön, eli kunnassa toteutettujen GDPR-projektien mukaisesti.

Vaikka henkilöresursseihin on saatu helpotusta kuntien yhteistyöstä ja taloudellisiin haasteisiin on vastattu välttämällä ylilyönnit palveluiden ostoissa mm. huolellisilla ostojen tarvearvioinneilla ja kilpailutuksilla, on jatkossa tarkkaan huolehdittava, että organisaation sisäinen tietosuoja- ja tietoturvaosaaminen varmistetaan. Haasteet on pyrittävä kääntämään voitoksi ja tietosuojatyökin yhdeksi ihmislähtöisen kunnan positiiviseksi voimavaraksi.

Koko henkilöstön tietosuojaosaamisen varmistaminen on ensisijaisen tärkeää. Kunnan tietosuoja- ja tietoturvapoliittikka liitteineen on tähän hyvä alusta. Se

on laaja kokonaisuus, jonka jokainen kunnan uusi työntekijä merkitsee allekirjoituksellaan tiedokseen tietosuojasitoumuksen ja työsopimuksen allekirjoituksen yhteydessä. Tietosuoja- ja tietoturvapoliittikka liitteineen on henkilökunnan saatavilla milloin tahansa luettavaksi, sekä digitaalisesti että paperimuodossa ja siitä kannattaakin henkilökuntaa muistuttaa säännöllisesti.

Tietosuojatyön sisällyttäminen koko henkilöstön päivittäisiin prosesseihin kannattaa tehdä säännöllisin väliajoin toteutettavilla tehotietoiskuilla. Siinä jaettaisiin samanaikaisesti tietoa kaikkien sähköisten kanavien kautta, sekä paperimuodossa henkilöstön sosiaalisiin tiloihin ja työyhteisöjen ilmoitustauluille ja samaan aikaan pyrittäisiin testaamaan koko henkilökunnan tietosuojaosaaminen. Tässä voitaisiin hyödyntää, kuten aikaisemminkin, Valtioneuvoston tarjoamaa jatkuvasti päivittyvää, ilmaista koulutusmateriaalia. Tarjolla on tietosuojatestien lisäksi myös erilaisia koulutusvideoita, joita organisaatiot voivat ottaa käyttöön milloin tahansa. (Valtioneuvosto 2017.)

Koko henkilöstön yhteiset ja pienempienkin ryhmien kokoontumiset voidaan niin ikään hyödyntää napakoilla tietosuojaiskuilla. Videotykin vapauduttua, voi tilaisuuden aluksi tai lopuksi esittää yksi tai muutama ote esim. tietosuoja- ja tietoturvapoliitikasta, tai muista valmiista ohjeistuksista esim. etätyöhön, sähköpostiin, internettiin, sosiaaliseen mediaan ym. liittyen ja näin myös madaltaa asiasta tiedottamisen kynnystä.

Hankintojen sopimukseen kannattaa kiinnittää erityistä huomioita ja varautua etupainotteisesti niihin liittyviin säännöksiin. Lapinjärven kunta on solminut muutamia hankintoihin liittyviä sopimuksia julkishallinnon sopimuskumppaneiden, Hanselin ja Sarastian kanssa. Nämä tarjoavat valmiiksi kilpailutetun yrityksen hankintakumppaniksi. Tällainen sopimus on voimassa esimerkiksi Hanselin ICT-laitteiden elinkaarenhallinnan ja irtaimen käyttöomaisuuden vuokrauspalvelun osalta ja palvelun tarjoaa 3StepIT. Kilpailutuksissa on huomioitu laitteiden elinkaarenhallinta, kiertotalouden kannattavuus, sekä GDPR:n mukainen tietosuoja. Kunnan kaikkien yksiköiden kannattaa jatkossakin aktiivisesti seurata julkisten hankintojen kilpailutuksen aikatauluja omien erityistarpeiden osalta. Tämä on sekä riskienhallintaa, että omien resurssien säästämistä. Vastaavasti, jos organisaatio itse tekee julkisen hankintaprosessin, on

sen erityisesti varmistettava henkilötietojen käsittelyn lainmukaisuus siinä tapauksessa, jos sopimuskumppanin hankintasopimuksen perusteella tullaan käsittelemään henkilötietoja. Hankintojen suunnittelun tueksi on tietosuoja-asetuksen keskeisiä velvoitteita laajasti opastettu (Hansel 2017) ohjeessa. Erittäin tärkeää on varmistaa myös sopimusliitteiden oikeellisuus ja erityisesti tämä kannattaa huomioida esimerkiksi vartiointi- ja siivouspalvelusopimuksissa, joissa henkilöstön vaihtuvuus voi olla suuri.

Organisaation on jatkossa kiinnitettävä erityistä huomiota myös tietojen sijaintiin. Toimeksiantajan tämän hetkisten palveluiden tietokannat sijaitsevat tois- taiseksi kaikki luotettavasti Suomessa. Mutta julkishallinto elää voimakkaassa murroksessa ja sitä ympäröivä maailma muuttuu ja digitalisoituu. Tietosuoja- työtä tulee tehdä lakkaamatta ja seurata aktiivisesti viestintää myös pilvipalve- luiden sopimusehtoihin liittyen. Uusien pilvipalveluiden osalta on tärkeää sel- vittää tietosuojan toteutuminen jo hankintavaiheessa, eli huomioida oikea-ai- kaisesti mm. rekisterinpitäjän ja tietojen käsittelijän vastuut, sekä tietojen da- tankäyttöoikeudet.

Organisaation tärkein voimavara on osaava ja motivoitunut henkilöstö, joten kunnassa tulisi jatkossakin huolehtia henkilökunnan osaamisen kehittämisestä ja pyrkiä kaikin tavoin luomaan arvostavaa, luottavaa ja avointa työskulttuuria.

12 JOHTOPÄÄTÖKSET

Tutkimuksen tuloksena voidaan todeta, että Lapinjärven kunnassa on tehty kattavasti sekä organisatorisia että teknisiä toimenpiteitä rekisterinpitäjän osoi- tusvelvollisuuden edellyttämien tietosuojaperiaatteiden toteuttamiseksi. Kun- nassa on uusittu tietosuoja- ja tietoturvapoliittikka, nimitetty tietosuojavastaava ja toteutettu sekä itsenäiset GDPR-projektit, kuin myös kuntien GDPR-yhteis- työprojektit. Tutkimuksen perusteella voidaan hyvin myös todeta, että tehtyjen toimenpiteiden ajoitus oli oikea ja niiden saattaminen kattavasti tiedoksi ja noudatettavaksi voitiin toteuttaa samanaikaisesti.

Tämän työn tutkimustulosten perusteella yksi tärkeimmistä kunnalle esitetyistä kehittämissuhteuksista on tietotilinpäättöksen laatiminen. Tietotilinpäättös noudattaa accountability- eli tilintekovelvollisuusperiaatetta ja sen mukaan organisaatio voi itse osoittaa noudattavansa lakia, hyvää tietojenkäsittelytapaa ja hyvää tiedonhallintatapaa. Työn kehittämissuhteuksissa esitetään myös organisaation resurssien kohdistamista tietosuojatyöhön niin, että varmistetaan tietosuojavastaavan erityisosaaminen sekä koko henkilöstön riittävä tietosuojiosaaminen. Lisäksi ehdotetaan jatkettavaksi sekä kuntien valtakunnallisen tietosuojaverkoston että lähikuntien välisen GDPR-työryhmän yhteistyötä ja tuodaan esille hankintoihin sekä tietovarantojen sijaintiin liittyvät kehittämissuhteukset.

Vaikka työn kartoituksessa ei varsinaisia puutteita organisaation GDPR:n toteutuksessa havaittukaan, on huomioitavaa, että tietosuojatyö on jatkuvaa työtä muuttuvissa olosuhteissa, eikä se työ saa pysähtyä. Pienenä mutta ketteränä kuntana Lapinjärvi pystyy varmasti jatkossakin toiminnoillaan takaamaan, että henkilötietojen käsittelyprosessi on saumaton, yhdenmukainen, läpinäkyvä, luotettava, eheä ja lainmukainen ja että kunnassa taataan GDPR:n mukaisten velvoitteiden toteutuminen.

13 YHTEENVETO

Opinnäytetyön tavoitteena oli selvittää, mitä toimeksiantajalla oli jo tehty ja mitä pitäisi vielä tehdä rekisterinpitäjän osoitusvelvollisuuden tietosuojaperiaatteiden noudattamiseksi. Lähtökohtaisesti tutkimuksen kivijalkana toimi organisaatiolle laatimani tietosuoja- ja tietoturvapoliittikka sekä välittömästi siitä jatkuneet GDPR-projektien toteutukset.

Opinnäytetyö noudatti kvalitatiivisen tutkimuksen linjaa, jossa tietoa kerättiin dokumenteista, haastattelemalla asiantuntijoita, sekä havainnoimalla kokonaisuuksia. Sisäpiirihaastattelut ja ryhmäkeskustelut osoittautuivat toimivaksi tavaksi tutkia olemassa olevia käytäntöjä ja kehitteillä olevia toteutuksia ja ne toimivat kiitettävästi työn tietoperustan tukena. Työn tietoperustasta saatiin myös asiantuntemusta ja ymmärrystä haastatteluille ja keskusteluille. Työn tuloksena saatiin laaja tilannekuva organisaation tietosuojan tilasta ja kehityksen

suunnasta. Tärkeää tutkimuksessa on sen kohdistuminen ydinasiaan ja tässä suhteessa työ onnistui mielestäni hyvin, vaikkakin se oli aihepiirin laajuuden vuoksi hetkittäin haasteellistakin.

Opinnäytetyön aihetta valittaessani halusin erityisesti linkittää sen omaan päivittäiseen työhöni. Tässä onnistuinkin loistavasti ja tämä opinnäytetyö on tuonut valtavasti hyödyllistä lisätietoa ja käytännön varmuutta hoitaa jatkossa tätäkin osa-aluetta työssäni hieman leveämmillä hartioilla. Erilaisiin tutkimusmenetelmiin tutustuminen oli myös avartava ja syventävä kokemus.

Opinnot ja tämä opinnäytetyö on tehty ICT-vastaavan kokopäivätyön ohessa. Yksi opiskelun suurimmista haasteista on ollut ajankäytön hallinta. Opiskelun lisäksi ovat kuitenkin oikealla ajankäytön suunnittelulla myös perhe, ystävät, lepo ja muut harrastukset saaneet vapaa-ajasta tärkeän paikkansa. Tukea opiskelun sujumiseen olen myös kaikilta tahoilta saanut kiitettävästi. Työnantajan tuki on ollut vuosilomien tai ylityövapaiden joustava sijoittaminen tarvittaessa lähiopetuspäiville. Tähän olin tyytyväinen, koska opiskelemaan olin lähtenytkin työnantajasta riippumattomalla päätöksellä. Opiskelijakavereista koen myös saaneeni valtavasti tukea ja synergiaa. Opiskelun sujuvuudesta saan myös kiittää elämän muiden osa-alueiden joustoa ja niiden virkistävää ja voimaannuttavaa vaikutusta.

Opiskelu on ollut enimmäkseen voimavara ja tietoa on voinut hyödyntää vuorovaikutteisesti työnantajan ja oppilaitoksen välillä. Opinnot ovat lisänneet ammattitaitoani ja siten myös hyödyntävät työnantajaani. Motivaatio on syntynyt halusta pitää huolta osaamisestani ja innostuksesta päivittää taitojani muuttuvassa maailmassa. Yhteenvetona todettakoon, että tämä on ollut erittäin antoisa, opettavainen ja palkitseva matka, jonka viitoittamaa tietä on mielenkiintoista jatkaa eteenpäin.

LÄHTEET

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

Eduskunta. 2018. EU:n yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano
– Uusi tietosuojalaki. WWW-dokumentti. Päivitetty 17.12.2018. Saatavissa:
https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojaudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx [viitattu 13.9.2019].

Euroopan komissio s.a. Mitkä ovat yleisen tietosuoja-asetuksen tärkeimmät
huomioon otettavat seikat julkishallinnossa? WWW-dokumentti. Saatavissa:
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_fi [viitattu 29.1.2020].

Euroopan parlamentin ja neuvoston asetukset (EU) 2016/679 luonnollisten henki-
löiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta
liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-ase-
tus). Saatavissa: [https://eur-lex.europa.eu/legal-con-
tent/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504](https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504)
[viitattu 16.1.2020].

Finlex. 2018. Tietosuojalaki. WWW-dokumentti. Saatavissa: [https://www.fin-
lex.fi/fi/laki/alkup/2018/20181050](https://www.finlex.fi/fi/laki/alkup/2018/20181050) [viitattu 2.5.2020].

Hansel. 2017. Tietosuoja-asetuksen huomioiminen kilpailutettaessa hankin-
toja. WWW-dokumentti. Saatavissa: [https://www.hansel.fi/media/filer_pub-
lic/1d/2c/1d2c32ab-bb9a-49c0-b75c-da64871d1df9/tietosuojaohje.pdf](https://www.hansel.fi/media/filer_public/1d/2c/1d2c32ab-bb9a-49c0-b75c-da64871d1df9/tietosuojaohje.pdf) [viitattu
12.3.2020].

HE 9/2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta
täydentäväksi lainsäädännöksi. WWW-dokumentti. Saatavissa:
<https://www.finlex.fi/fi/esitykset/he/2018/20180009> [viitattu 1.5.2020].

Himanka, P. 2018. EU:n yleisen tietosuoja-asetuksen mukainen vaikutus-
tenarviointi (DPIA) : riskit ja niiden vaikutukset luonnollisen henkilön oikeuksiin
ja vapauksiin. Tampereen ammattikorkeakoulu. Liiketalouden koulutusoh-
jelma. Opinnäytetyö. PDF-dokumentti. Saatavissa:
<http://urn.fi/URN:NBN:fi:amk-2018073014400> [viitattu 18.12.2019].

Juvonen, T., Sisäpiirihaastattelu. Teoksessa Hyvärinen, M., Nikander, P.,
Ruusuvoori, J. & Aho, A. 2017. Tutkimushaastattelijan käsikirja. E-kirja. Tam-
pere: Vastapaino. Saatavissa: <https://kaakkuri.finna.fi/Record/kaakkuri.223631>
[viitattu 14.1.2020].

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen E. Uusi tietosuojalainsäädäntö.

Alma Talent 2018. E-kirja. Saatavissa: [https://verkkokirjahylly-almatalent-fi.ezproxy.xamk.fi/teos/BAXBBXATHBBED#/kohta:l\(\(20\)Ylei-set\(\(20\)s\(\(e4\)\(\(e4\)nn\(\(f6\)kset/piste:tM](https://verkkokirjahylly-almatalent-fi.ezproxy.xamk.fi/teos/BAXBBXATHBBED#/kohta:l((20)Ylei-set((20)s((e4)((e4)nn((f6)kset/piste:tM) [viitattu 16.1.2020].

Kuntaliitto. 2019a. Tietosuoja-asetus. WWW-dokumentti 11.2.2019. Saatavissa: <https://www.kuntaliitto.fi/laki/julkisuus-ja-tietosuoja/tietosuoja-asetus> [viitattu 16.1.2020].

Kuntaliitto. 2019b. Kuntien tietosuojavastaavien verkosto. WWW-dokumentti. Saatavissa: <https://www.kuntaliitto.fi/laki/julkisuus-ja-tietosuoja/tietosuoja-asetus/kuntien-tietosuojavastaavien-verkosto> [viitattu 22.1.2020].

Kuntaliitto. 2019c. Kuntamarkkinat. Tietotilinpäätös -mitä ja miksi. WWW-dokumentti. Saatavissa: https://www.kuntaliitto.fi/sites/default/files/media/file/Sessio_11092019_1000_A3_8_Tietotilinp%C3%A4%C3%A4t%C3%B6s_1.pdf [viitattu 23.1.2020].

Kuntaliitto. 2019d. Tietotilinpäätös –mitä–miksi–miten. WWW-dokumentti. Saatavissa: https://www.kuntaliitto.fi/haku?s=tietotilinp%C3%A4%C3%A4t%C3%B6s+&created=&created_1= [viitattu 29.1.2020].

Lapinjärven kunnanhallitus. 2018. Lapinjärven kunnan tietoturva- ja tietosuoja-politiikka. Lapinjärven kunnanhallitus 3.9.2018 § 108. WWW-dokumentti. Saatavissa: http://lapinjarvi.ktweb.fi/ktwebbin/dbisa.dll/ktweb-scr/pk_asil.htm?+elin=KHALL&pvm=3%2e9%2e2018%2018%3a00 [viitattu 13.12.2019].

Lapinjärvi. 2017. Lapinjärvi kehittää ihmislähtöistä kuntaa. WWW-dokumentti. Saatavissa: <http://ihkulapinjarvi.blogspot.com/p/tervetuloa.html> [viitattu 28.1.2020].

Lapinjärvi. 2018. Ei maalla asuminen aina tarkoita huonoja yhteyksiä – Lapinjärvellä valokuitu on jo arkipäivää. WWW-dokumentti. Saatavissa: <https://www.sttinfo.fi/tiedote/ei-maalla-asuminen-aina-tarkoita-huonoja-yhteyksia--lapinjarvella-valokuitu-on-jo-arkipaivaa?publisherId=56401906&releaseId=68842000> [viitattu 28.1.2020].

Lapinjärvi. 2020a. Päivähoito ja koulutus. WWW-dokumentti. Saatavissa: <https://www.lapinjarvi.fi/paivahoito-ja-koulutus/opetus-ja-koulutus/> [viitattu 2.5.2020].

Lapinjärvi. 2020b. Sosiaali- ja terveystalot. WWW-dokumentti. Saatavissa: <https://www.lapinjarvi.fi/sosiaali-ja-terveyspalvelut/terveydenhuolto/> [viitattu 2.5.2020].

Lapinjärvi. 2020c. Organisaatiokaavio. WWW-dokumentti. Saatavissa: <https://www.lapinjarvi.fi/paatoksenteko/organisaatiokaavio-2/> [viitattu 2.5.2020].

Miten valmistautua EU:n tietosuoja-asetukseen? 2017. Selvityksiä ja ohjeita. 4/2017. Oikeusministeriö, Tietosuojavaltuutetun toimisto. PDF-dokumentti.

Saatavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79316/OMSO_04_2017_OM_TSV_EU_tietosuoja.pdf?sequence=1&isAllowed=y [viitattu 16.1.2020].

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. 2010. Vahti 2/2010. Valtiovarainministeriö. WWW-dokumentti. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229 [viitattu 22.1.2020].

Oikeusministeriö 2018. Uusi tietosuojalaki voimaan vuoden 2019 alusta. TIE-DOTE 5.12.2018. WWW-dokumentti. Saatavissa: https://valtioneuvosto.fi/artikkeli/-/asset_publisher/1410853/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta [viitattu 15.1.2020].

Oikeusministeriö 2019. Lausuntopyyntö: Yleisen tietosuoja-asetuksen toimitus ja sen soveltamiseen liittyvät kokemukset. WWW-dokumentti. Saatavissa: <https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=2df6ebd7-975e-4169-a0de-edd9ab3d7217> [viitattu 14.1.2020].

Periaatteet, politiikat ja suunnitelmat. 2020. OpiTietosuoja.fi. WWW-dokumentti. Saatavissa: <https://opitietosuoja.fi/fi/49-tyokalupakki/periaatteet-politiikat-ja-suunnitelmat> [viitattu 21.1.2020].

Pietilä, I. 2017. Ryhmäkeskustelu. Teoksessa Hyvärinen, M., Nikander, P. & Ruusuvoori, J. (toim.) Tutkimushaastattelun käsikirja. E-kirja. Tampere: Vastapaino. Saatavissa: <https://kaakkuri.finna.fi/Record/kaakkuri.223631> [viitattu 15.1.2020].

Rekisterinpitäjän velvollisuudet. 2016. Valtiovarainministeriö. WWW-dokumentti. Saatavissa: <https://www.vahtiohje.fi/web/guest/rekisterinpitajan-velvollisuudet> [viitattu 23.2.2020].

Summe, T. 2018. Todistustaakan täytyminen yrityksissä : yleinen tietosuoja-asetus. Turun ammattikorkeakoulu. Tietojenkäsittely. Opinnäytetyö. PDF-dokumentti. Saatavissa: <http://urn.fi/URN:NBN:fi:amk-201805026111> [viitattu 18.2.2020].

Tamminen, M. 2018. Eskolan kyläkoulusta tuli uusimaalaisen koulun satelliittipiste – Voisiko rahoitusmalli ratkaista kuolevien kyläkoulujen ongelman? Talouselämä 15.8.2018. WWW-dokumentti. Saatavissa: <https://www.talouselama.fi/uutiset/eskolan-kylakoulusta-tuli-uusimaalaisen-koulun-sateelliittipiste-voisiko-rahoitusmalli-ratkaista-kuolevien-kylakoulujen-ongelman/163c22bc-fd2c-34ca-950b-90cc6d649970> [viitattu 28.1.2020].

Tietosuojavaikuttetun toimisto. 2012. Laadi tietotilinpäätös. 2012. WWW-dokumentti. Saatavissa: <https://tietosuoja.fi/documents/6927448/10594424/Laadi+tietotilinp%C3%A4%C3%A4t%C3%B6s.pdf/4925bd9e-d07d-82fc-3f2d-71c5955310a0/Laadi+tietotilinp%C3%A4%C3%A4t%C3%B6s.pdf> [viitattu 12.3.2020].

Tietosuojavaltuutetun toimisto. 2020a. Osoita noudattavasi tietosuojasäännöksiä. WWW-dokumentti. Saatavissa: <https://tietosuoja.fi/osoitusvelvollisuus> [viitattu 22.1.2020].

Tietosuojavaltuutetun toimisto. 2020b. Mikä GDPR? WWW-dokumentti. Saatavissa: <https://tietosuoja.fi/gdpr> [viitattu 21.1.2020].

Tietosuojavaltuutetun toimisto. 2020c. 29 Artiklan mukainen tietosuojatyöryhmä. WWW-dokumentti. Saatavissa <https://tietosuoja.fi/documents/6927448/8316711/Automaattinen+p%C3%A4%C3%A4t%C3%B6ksenteko/28ae24f4-3345-4fb2-8708-c84abd8f57b0/Automaattinen+p%C3%A4%C3%A4t%C3%B6ksenteko.pdf> [viitattu 22.1.2020].

Tietosuojavaltuutetun toimisto. 2020d. Osoitusvelvollisuus tieteellisessä tutkimuksessa. WWW-dokumentti. Saatavissa: <https://tietosuoja.fi/osoitusvelvollisuus-tieteellisessa-tutkimuksessa> [viitattu 10.2.2020].

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällön analyysi. E-kirja. Helsinki: Kustannusosakeyhtiö Tammi. Saatavissa: <https://kaakkuri.finna.fi/Record/kaakkuri.223794> [viitattu 16.1.2020].

VAHTI-raportti 1/2016. WWW-dokumentti. Saatavissa: <https://www.vah-tiohje.fi/web/guest/suosituksia-toimenpiteista> [viitattu 9.3.2020].

Vainio, S. 2018. Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuojasetuksessa. Helsingin yliopisto, Oikeustieteellinen tiedekunta. Pro gradu. PDF-dokumentti. Saatavissa: <http://urn.fi/URN:NBN:fi:hulib-201802191291> [viitattu 4.10.2019].

Valtioneuvosto. 2017. Tietosuojaa ja tietoturvaa edistetään uusin keinoin – tutustu videokoulutukseen ja nettitestiin. Saatavissa: https://valtioneuvosto.fi/artikkeli/-/asset_publisher/10623/tietosuojaa-ja-tietoturvaa-edistetaan-uusin-keinoin-tutustu-videokoulutukseen-ja-nettitestiin [viitattu 12.3.2020].

Valtioneuvosto. 2018. Eduskunnan vastaus hallituksen esitykseen EU:n yleistä tietosuojasetusta täydentäväksi lainsäädännöksi Valtioneuvoston yleisistunto 5.12.2018 10.00. WWW-dokumentti. Saatavissa: <https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f805f5b62> [viitattu 7.10.2019].

Valtiovarainministeriö. 2017. Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet. WWW-dokumentti. Saatavissa: <https://vm.fi/documents/10623/4914009/Ty%C3%B6pajan+materiaalikooste/fbcb3a29-16c7-4006-a390-692a16b8d215/Ty%C3%B6pajan+materiaalikooste.pdf> [viitattu 12.3.2020].

Valtiovarainministeriö. 2017. Tietosuojan rakentuminen. Valtiovarainministeriön tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet -materiaalista. WWW-dokumentti. Saatavissa: <https://vm.fi/documents/10623/4914009/Ty%C3%B6pajan+materiaalikooste/fbcb3a29-16c7-4006-a390-692a16b8d215/Ty%C3%B6pajan+materiaalikooste.pdf> [viitattu 12.1.2020].

Valtiovarainministeriö. 2018. Yhteishankkeiden materiaalit. WWW-dokumentti. Saatavissa: <https://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit> [Viitattu 10.2.2020].

Valtiovarainministeriö. 2020. Voimassa olevat tietoturvaohjeet ja –määräykset. WWW-dokumentti. Saatavissa: <https://vm.fi/julkaisut/vahti> [Viitattu 16.1.2020].

Viestintävirasto 2014. WWW-dokumentti. Saatavissa: <https://legacy.viestinta-virasto.fi/hakutulos.html.stx> [viitattu 13.12.2019].

Vuorela, P. 2018. Ratkaisu Polanyin Paradoksiin - tiedolla johtamisella lisää ymmärrystä arkeen 2018. WWW-dokumentti. Saatavissa: <https://www.in-nolink.fi/ratkaisu-polanyin-paradoksiin-tiedolla-johtamisella-lisaa-ymmarrysta-arkeen/> [viitattu 13.3.2020].